Ристо Малчески

ТЕОРИЈА НА БРОЕВИ

Скопје, септември 2021

Рецензент

Д-р Павел Димовски, вон. проф
Технолошко-металуршки факултет
УКИМ Скопје

СОДРЖИНА

Предговор 7

I ГЛАВА
ДЕЛИВОСТ

1. Поим за деливост. Признаци за деливост 9
2. Делење со остаток 13
3. Најголем заеднички делител 18
4. Евклидов алгоритам 21
5. Најмал заеднички содржател 26

II ГЛАВА
ПРОСТИ БРОЕВИ

1. Поим за прост и сложен број 29
2. Основна теорема на аритметиката 34
3. Ферматови и Мерсенови броеви 39
4. Функциите $[x]$ и $\{x\}$ 44
5. Целобројни точки и функцијата $[x]$ 51
6. Белешка за распределбата на простите броеви 54

III ГЛАВА
МУЛТИПЛИКАТИВНИ ФУНКЦИИ

1. Поим за мултипликативна функција 58
2. Број на делители и збир на делители на природен број 60
3. Конволуциски производ 67
4. Функција на Мебиус 69
5. Ојлерова функција 73

IV ГЛАВА
КОНГРУЕНЦИИ

1. Поим за конгруенција 80
2. Системи остатоци 86
3. Теореми на Ојлер, Ферма, Кармајкл и Вилсон 94
4. Линеарна конгруентна равенка 102
5. Нелинеарни конгруентни равенки 110
6. Леми на Шур и Хенсел 115
7. Ред на број по модул 118

8. Лема за зголемување на степенот 122
9. Примитивни корени 125

V ГЛАВА
ЦИКЛОМАТИЧНИ ПОЛИНОМИ

1. Комплексни примитивни корени 130
2. Дефиниција и својства на цикломатични полиноми 133
3. Цикломатични полиноми и ред на број по прост модул 138
4. Теорема на Жигимонди 143

VI ГЛАВА
КВАДРАТНИ ОСТАТОЦИ

1. Квадратни остатоци по прост модул 148
2. Гаусов закон за реципроцитет 154
3. Квадратни конгруенции по сложен модул 157
4. Некои збирови на симболите на Лежандр 162

VII ГЛАВА
ДИОФАНТОВИ АПРОКСИМАЦИИ

1. Рационални и ирационални броеви 164
2. Теорема на Дирихле 168
3. Низи на Фарej 169
4. Поим за верижна дропка 174
5. Парцијални количници 176
6. Бесконечни верижни дропки 181
7. Ирационални броеви и верижни дропки 185
8. Периодични верижни дропки 193
9. Верижни дропки и квадратни остатоци 201
10. Алгебарски и трансцедентни броеви 203

VIII ГЛАВА
ДИОФАНТОВИ РАВЕНКИ

1. Линеарна Диофантова равенка 208
2. Питагорови тројки 210

3. Метод на Ферма 215
4. Збир од четири квадрати 219
5. Збир од два квадрати 221
6. Методи за решавање полиномни Диофантови равенки 228
7. Методи за решавање експоненцијални Диофантови равенки 232
8. Равенка на Туе 237
9. Равенка на Пел 239

IX ГЛАВА
КВАДРАТНИ ПОЛИЊА

1. Поим за квадратно поле. Основни својства 247
2. Квадратно цели броеви 250
3. Деливост во $\mathbb{Q}[\sqrt{d}]$ 253
4. Квадратно прости броеви и факторизација во $\mathbb{Q}[\sqrt{d}]$ 257
5. Единственост на факторизацијата во $\mathbb{Q}[\sqrt{d}]$ 259
6. Евклидски полиња 267
7. Множеството $\mathbb{Z}[\sqrt{d}]$ 271
8. Кинеска теорема за остатоци 273
9. Мала теорема на Ферма 275
10. Равенки од Пелов тип 277

Индекс на поими 285
Литература 288

ПРЕДГОВОР

> Ниту едно истражување на човекот не може да се нарече вистинска наука ако не е поткрепено со математички доказ.
>
> Проблематична е веродостојноста на тврдењата во науките каде што нема примена на ниту една математичка дисциплина, т.е. кои не се поврзани со математиката.
>
> Леонардо да Винчи

Корените на оваа се во далечната 1998 година, кога авторот направи неуспешен обид во коавторство со колеги од Институтот за математика при Природно-математичкиот факултет во Скопје да напише учебник по теорија на броеви за студентите од Институтот за математика. Овој обид заврши со оформување на нерецензирана скрипта која долги години беше основа за курсот Теорија на броеви при Природно-математичкиот факултет во Скопје. Предметнава книга суштински се разликува од споменатата скрипта, како по структура, така и по содржина.

Важен стимул за развојот на оваа книга се повеќе од триесетте години кои авторот ги помина работејќи во Сојузот на математичарите на Македонија, особено во делот на националните и меѓународните натпревари кои СММ ги организираше во периодот од 1988-2019 година, како и во списанието Сигма. Притоа, во оформувањето на оваа книга важна улога имаа бројните статии на авторот, кои десетици години наназад се пишувани, пред сé за да се премости недостатокот на литература за работа со надарените ученици по математика во Република Македонија, како и задачите кои беа разработувани на подготовките на учениците за учество на меѓународните математички натпревари (JBMO, BMO, EGMO, IMO, EMC, MeMO и APMO).

Материјалот кој е разработен во оваа книга е поделен на девет глави. Во книгава се содржани теми кои ретко се среќаваат во задачите кои се задаваат на математичките олимпијади, како што се темите: Ферматови броеви, Функција на Мебиус, Нелинеарни конгруентни равенки и теорема на Лагранж, Цикломатични полиноми и теорема на Жигимонди, Квадратни остатоци и квадратен закон на реципроцитет, Деливост на биномните коефициенти (теоремите на Лукас и Кумер), Диофантови апроксимации и Теореми на Чебишев и Дирихле.

Книгава е наменета пред се за учениците кои се интересираат за изучување и применета на теоријата на броеви и тоа на ниво потребно за успешно учество на престижните меѓународни математички олимпијади. Затоа, пред да се пристапи кон совладување на содржините кои се предмет на разработка на оваа книга е неопходно учениците да се стекнат со неопходните теориски знаења и техники за решавање на задачи на поелементарно ниво. Оттука, на читателите им препорачувам прво да ја проучат книгата Вовед во елементарна теорија на броеви ([76]), како и книгата Математички талент 26 – збирка задачи по елементарна теорија на броеви ([89]), која во целост соодвествува на споменатата книга, а потоа да преминат кон изучување на оваа книга.

Пожелно е оваа книга да ја совладаат и студенти од наставните групи по математика, кои во текот на својот работен век природно ќе се среќаваат со ученици надарени за математика, кои ученици учествуваат на математичките натпревари. Овде сакам да напоменам, ризикувајќи да бидам погрешно разбран, дека предметнава книга во целост може да се користи како основен учебник за почетен курс на студии по математика. Секако, истатане е доволна, па затоа на студентите по математика им препорачувам изучувајќи ги содржините од оваа книга да ја користат Збирката задачи по теорија на броеви, напишана од истиот автор.

При оформувањето на книгава важен допринос имаше колегата д-р Павел Димовски, кој со своите забелешки и предлози придонесе како да се намали бројот на грешките кои неминовно го пратат издавањето на секоја книга, така и да се подобрат решенијата на определен број задачи.

На крајот од книгава е наведена литературата која ја користев при пишувањето на оваа обемна збирка задачи. Во литературата, покрај книгите и статиите од други автори се наведени и моите книги и стручни статии од теорија на броеви, кои како што напоменав се резултат од мојата долгогодишна работа со надарените ученици за математика во Република Македонија.

За крај, и покрај вложениот напор, како од моја страна, така и од колегата д-р Павел Димовски, свесен сум дека се можни подобрувања на оваа збирка задачи, како и дека се присутни определен број грешки, кои за жал не го одминуваат издавањето на било кој ракопис. Затоа, однапред сум благодарен на секоја добронамерна критика и сугестија, која ќе придонесе како за отстранување на грешките, така и за подобрување на структурата и содржината на оваа збирка задачи.

Скопје Авторот
Септември, 2021 г.

I ГЛАВА
ДЕЛИВОСТ

Познати ни се множествата

$$\mathbb{N}=\{1,2,3,...,n,...\},\ \mathbb{N}_0=\mathbb{N}\cup\{0\}=\{0,1,2,3,...,n,...\} \text{ и}$$
$$\mathbb{Z}=\{...,-4,-3,-2,-1,0,1,2,3,4,...\}.$$

Операциите собирање и множење во овие множества се секогаш изводливи, т.е.

ако $m,n\in\mathbb{N}$, тогаш $m+n\in\mathbb{N}$ и $mn\in\mathbb{N}$;

ако $m,n\in\mathbb{N}_0$, тогаш $m+n\in\mathbb{N}_0$ и $mn\in\mathbb{N}_0$; и

ако $m,n\in\mathbb{Z}$, тогаш $m+n\in\mathbb{Z}$ и $mn\in\mathbb{Z}$.

Понатаму, за одземањето знаеме дека

ако $m,n\in\mathbb{N}$, тогаш $m-n\in\mathbb{N}$ ако и само ако $m>n$;

ако $m,n\in\mathbb{N}_0$, тогаш $m-n\in\mathbb{N}_0$ ако и само ако $m\geq n$; и

ако $m,n\in\mathbb{Z}$, тогаш $m-n\in\mathbb{Z}$.

Останува да ја разгледаме операцијата делење, која не е секогаш изводлива во множествата $\mathbb{N},\mathbb{N}_0$ и $\mathbb{Z}$. Имено, ако m и $n\neq 0$ се природни или цели броеви, тогаш количникот $m:n$ не е секогаш природен или цел број, соодветно. И токму тоа, прашањето кога бројот m е делив со бројот $n\neq 0$, т.е. прашањето за деливоста во множествата $\mathbb{N},\mathbb{N}_0$ и $\mathbb{Z}$ лежи во основата на теоријата на броеви.

Во следните разгледувања ќе се задржиме на прашањето за деливост во $\mathbb{N}$ и $\mathbb{Z}$, при што многу својства ќе бидат докажани само за природните броеви, со забелешка дека истите со мали надополнувања важат и во множеството на целите броеви $\mathbb{Z}$, при делители различни од нула.

1. ПОИМ ЗА ДЕЛИВОСТ. ПРИЗНАЦИ ЗА ДЕЛИВОСТ

1.1. Дефиниција. За бројот $a\in\mathbb{Z}$ ќе велиме дека е *делив* со бројот $b\in\mathbb{Z}$, $b\neq 0$, ако постои број $q\in\mathbb{Z}$ така што е исполнето равенството $a=bq$. Притоа ќе велиме дека b е *делител* на a, односно дека a е *содржател* на b и ќе пишуваме $b\mid a$.

Ако бројот $b\in\mathbb{Z},\ b\neq 0$ не е делител на бројот $a\in\mathbb{Z}$, т.е. ако не постои број $q\in\mathbb{Z}$ така што е исполнето равенството $a=bq$, тогаш ќе пишуваме $b\nmid a$.

Ќе велиме дека b е *вистински делител* на a ако $b\mid a$ и $b\neq a$.

1.2. Забележуваме дека ако $a,b\in\mathbb{N}$, тогаш и $q\in\mathbb{N}$. Понатаму, ако $b\mid a$, тогаш од $a=bq$ непосредно следуваат равенствата

$$a=(-b)(-q),\ -a=b(-q) \text{ и } -a=(-b)q,$$

од што согласно дефиницијата 1.1 следува дека

$$(-b)\mid a,\ b\mid(-a) \text{ и } (-b)\mid(-a).$$

Претходно изнесеното ни дава за право, при разгледувањето на деливоста, да се ограничиме на деливост на цел со природен број, односно на деливост на природните броеви.

1.3. Теорема. а) Нека $a,b\in\mathbb{N}$. Ако $a\mid b$ и $b\mid a$, тогаш $a=b$.

б) Нека $a,b,c\in\mathbb{N}$. Ако $a\mid b$ и $b\mid c$, тогаш $a\mid c$.

в) Ако $b\mid a$, тогаш $b\mid(ac)$, за секој $c\in\mathbb{N}$.

г) Нека $a=b+c$ и $d\mid b$. Тогаш $d\mid a$ ако и само ако $d\mid c$.

д) Ако $a\mid b$ и $a\mid c$, тогаш $a\mid(bx+cy)$ за секои $x,y\in\mathbb{Z}$.

ѓ) Ако $m\mid a$ и $n\mid b$, тогаш $mn\mid(ab)$.

Доказ. а) Нека $a,b\in\mathbb{N}$, $a\mid b$ и $b\mid a$. Од $a\mid b$ следува дека постои $q\in\mathbb{N}$ таков што $b=aq$, а од $b\mid a$ следува дека постои $p\in\mathbb{N}$ таков што $a=bp$. Понатаму, од равенствата $b=aq$ и $a=bp$ добиваме $b=aq=(bp)q=b(pq)$, т.е. $b=b(pq)$. Ако последното равенството го поделиме со $b\neq 0$ го добиваме равенството $pq=1$. Но, $p,q\in\mathbb{N}$ па затоа од последното равенство следува $p=q=1$. Конечно, $a=bp=b\cdot 1=b$.

б) Нека $a,b,c\in\mathbb{N}$, $a\mid b$ и $b\mid c$. Од $a\mid b$ следува дека постои $q\in\mathbb{N}$ таков што $b=aq$, а од $b\mid c$ следува дека постои $p\in\mathbb{N}$ таков што $c=bp$. Понатаму, од равенствата $c=bp$ и $b=aq$ добиваме $c=bp=(aq)p=a(qp)$, што според дефиниција 1.1 значи дека $a\mid c$.

в) Навистина, ако $b\mid a$, тогаш постои $q\in\mathbb{N}$ таков што $a=bq$. Сега, за секој $c\in\mathbb{N}$ добиваме $ac=(bq)c=b(qc)$. Значи, за бројот $ac\in\mathbb{N}$ постои број $qc\in\mathbb{N}$ таков што $ac=b(qc)$, па од дефиниција 1.1 имаме дека $b\mid(ac)$.

г) Нека $a=b+c$ и $d\mid b$, т.е. постои q таков што $b=dq$. Ако $d\mid c$, тогаш постои p таков што $c=dp$. Според тоа, $a=b+c=dq+dp=d(q+p)$, што според дефиниција 1.1 значи дека $d\mid a$. Ако $d\mid a$, тогаш постои r таков што $a=dr$. Според тоа, $c=a-b=dr-dq=d(r-q)$, што според дефиниција 1.1 значи дека $d\mid c$.

д) Нека $a\mid b$ и $a\mid c$. Од тврдењето под в) следува $a\mid(bx)$ и $a\mid(cy)$ за секои $x,y\in\mathbb{Z}$. Значи, постојат $p,q\in\mathbb{Z}$ такви што $bx=ap$ и $cy=aq$. Според тоа,

$$bx+cy=ap+aq=a(p+q),$$

т.е. $a\mid(bx+cy)$, за секои $x,y\in\mathbb{Z}$.

ѓ) Од $m\mid a$ и $n\mid b$ следува дека постојат p и q такви што $a=mp$ и $b=nq$. Според тоа, $ab=(mp)(nq)=(mn)(pq)$, што значи дека $mn\mid(ab)$. ■

1.4. Последица. а) Ако $k-1$ собирци во равенството $a_1+a_2+...+a_k=0$ се деливи со бројот d, тогаш и преостанатиот $k-$ти собирок е делив со d.

б) Ако $m_1\mid a_1, m_2\mid a_2,..., m_k\mid a_k$, тогаш $m_1m_2...m_k\mid a_1a_2...a_k$.

в) Ако $m\mid a$, тогаш $m^k\mid a^k$, за секој $k\in\mathbb{N}$.

Доказ. Непосредно следува од теорема 1.3. Деталите ги оставаме на читателот за вежба. ■

1.5. Пример. Нека се $1=d_1<d_2<...<d_k=n$ сите делители на природниот број $n>1$. Докажи, дека $d_1+d_2+...+d_k>k\sqrt{n}$.

Решение. Ако d е делител на природниот број n, тогаш јасно е дека и $\frac{n}{d}$ е исто така делител на n. Воведуваме ознака $S=d_1+d_2+...+d_k$. Бидејќи $n>1$ јасно е дека постои делител d_i, таков што $d_i\neq\frac{n}{d_i}$. Од друга страна

$$d_i+\tfrac{n}{d_i}>2\sqrt{d_i\cdot\tfrac{n}{d_i}}=2\sqrt{n}.$$

Сега,

$$2S=2(d_1+d_2+...+d_k)=\sum_{i=1}^{k}(d_i+\tfrac{n}{d_i})>\sum_{i=1}^{k}2\sqrt{n}=2k\sqrt{n}.$$

Значи, $S>k\sqrt{n}$ односно $d_1+d_2+...+d_k>k\sqrt{n}$ што и требаше да се докаже. ■

1.6. Пример. а) Нека $n\in\mathbb{N}_0$ и $k\in\mathbb{N}\setminus\{1\}$. Докажи, дека

$$(k-1)^2\mid(k^{n+1}-(k-1)n-k).$$

б) Нека $n\in\mathbb{N}$ и нека $a_1,a_2,...,a_n\in\{-1,1\}$ се такви што

$$a_1a_2+a_2a_3+...+a_{n-1}a_n+a_na_1=0.$$

Докажи, дека $4\mid n$.

Решение. а) Нека $n\in\mathbb{N}_0$, $k\in\mathbb{N}$ и нека $k=s+1$. Од Њутновата биномна формула следува

$$\begin{aligned}k^{n+1}-(k-1)n-k&=(s+1)^{n+1}-sn-s-1=(s+1)^{n+1}-(n+1)s-1\\&=s^{n+1}+\binom{n+1}{1}s^n+\binom{n+1}{2}s^{n-1}+...+\binom{n+1}{n-1}s^2+\binom{n+1}{n}s+1-(n+1)s-1\\&=s^{n+1}+\binom{n+1}{1}s^n+\binom{n+1}{2}s^{n-1}+...+\binom{n+1}{n-1}s^2\end{aligned}$$

$$= s^2[s^{n-1} + \binom{n+1}{1}s^{n-2} + \binom{n+1}{2}s^{n-3} + ... + \binom{n+1}{n-1}]$$
$$= (k-1)^2[(k-1)^{n-1} + \binom{n+1}{1}(k-1)^{n-2} + \binom{n+1}{2}(k-1)^{n-3} + ... + \binom{n+1}{n-1}],$$

што значи дека $(k-1)^2 \mid (k^{n+1} - (k-1)n - k)$.

б) Збирот $a_1a_2 + a_2a_3 + ... + a_{n-1}a_n + a_na_1$ има n собирци еднакви на 1 или -1, па бидејќи е еднаков на 0 заклучуваме дека $n = 2k$. Јасно, k собирци во збирот $a_1a_2 + a_2a_3 + ... + a_{n-1}a_n + a_na_1$ се еднакви на 1, а k на -1. Од друга страна

$$(a_1a_2)(a_2a_3)...(a_{n-1}a_n)(a_na_1) = a_1^2a_2^2...a_n^2 = 1,$$

па затоа $(-1)^k \cdot 1^k = 1$, што значи $k = 2t$. Конечно, $n = 2k = 2 \cdot 2t = 4t$, т.е. $4 \mid n$. ■

1.7. Пример. Определи го најголемиот природен број k за кој

$$1991^k \mid (1990^{1991^{1992}} + 1992^{1991^{1990}}).$$

Решение. Заради едноставноста на записот ставаме $a = 1991$. Треба да го определиме најголемиот природен број k за кој

$$a^k \mid ((a-1)^{a^{a+1}} + (a+1)^{a^{a-1}}) = ((a-1)^{a^{a+1}} + 1 + (a+1)^{a^{a-1}} - 1).$$

Бидејќи a е непарен број, очигледно првиот собирок во заградата дава остаток -1 при делење со a, додека другиот дава остаток 1. Затоа посебно ќе ги разгледаме најголемиот степен на a кој го дели $(a-1)^{a^{a+1}} + 1$ и најголемиот степен на a кој го дели $(a+1)^{a^{a-1}} - 1$. Притоа, ако овие два најголеми степени се различни, тогаш помалиот од нив е бараното k.

Ако $(a+1)^{a^n}$ го развиеме по Њутновата биномна формула, забележуваме дека последниот собирок е 1, претпоследниот е $\binom{a^n}{1}a = a^{n+1}$, а додека сите останати се деливи со a^{n+2}. Последното се докажува со индукција. Докажуваме дека за секој природен број n постои s_n таков што $a \nmid s_n$ и

$$(a+1)^{a^n} = 1 + s_na^{n+1}.$$

Навистина, за $n = 1$ имаме

$$(1+a)^a = 1 + \binom{a}{1}a + \binom{a}{2}a^2 + ... + \binom{a}{a}a^a$$
$$= 1 + a^2(1 + \binom{a}{2} + \binom{a}{3}a + ... + \binom{a}{a}a^{a-2}).$$

Сега, бидејќи a е непарен, важи $a \mid \binom{a}{2}$, па затоа a не е делител на

$$s_1 = 1 + \binom{a}{2} + \binom{a}{3}a + ... + \binom{a}{a}a^{a-2}.$$

Нека претпоставиме дека тврдењето важи за n. Тогаш

$$\begin{aligned}(1+a)^{a^{n+1}} &= (1+s_n a^{n+1})^a \\ &= 1+\binom{a}{1}s_n a^{n+1}+\binom{a}{2}s_n^2 a^{2n+2}+\ldots+\binom{a}{a}s_n^n a^{an+a} \\ &= 1+a^{n+2}(s_n+\binom{a}{2}s_n^2 a^n+\ldots+\binom{a}{a}s_n^n a^{an+a-n-2}) \\ &= 1+s_{n+1}a^{n+2}\end{aligned}$$

и како $a \nmid s_n$, добиваме дека $a \nmid s_{n+1}$.

На потполно аналоген начин се докажува дека за секој природен број n постои природен број t_n таков што $a \nmid t_n$ и важи

$$(a-1)^{a^n} = -1+t_n a^{n+1}.$$

Според тоа, од првото од горните две тврдења следува дека a^a е најголемиот степен со кој a го дели $(a+1)^{a^{a-1}}-1$, а од второто следува дека a^{a+2} е највисокиот степен со кој a го дели $(a-1)^{a^{a+1}}+1$.

Според тоа, бараниот број е $k_{\max} = a = 1991$. ■

2. ДЕЛЕЊЕ СО ОСТАТОК

2.1. На почетокот рековме дека операцијата делење не е секогаш изводлива во множествата $\mathbb{N}$ и $\mathbb{Z}$. Меѓутоа, во следната теорема ќе докажеме дека оваа операција, на определен начин сепак е изводлива во множествата $\mathbb{N}$ и $\mathbb{Z}$.

Теорема (за делење со остаток). За секој $a \in \mathbb{Z}$ и секој $b \in \mathbb{N}$ постојат единствени цели броеви q и r такви што

$$a = bq + r, \quad 0 \le r < b. \tag{1}$$

Доказ. Да го разгледаме множеството

$$A = \{\ldots, a-3b, a-2b, a-b, a, a+b, a+2b, a+3b, \ldots\}.$$

Ова множество содржи како негативни така и ненегативни цели броеви. Да го разгледаме множеството B од ненегативни цели броеви кои се содржат во множеството A. Множеството B има најмал елемент кој е природен број или е еднаков на нула. Нека тоа е бројот $a-qb$ и да го означиме со r. Тогаш важи (1), бидејќи во спротивно, ако $r \ge b$ тогаш бројот $a-(q+1)b$, кој е помал од $a-qb$, ќе биде природен број или еднаков на нула. Со тоа докажавме дека броевите q и r постојат и дека го задоволуваат условот (1).

Ќе докажеме дека броевите q и r се единствени. Да претпоставиме дека за броевите q_1 и r_1 важи

$$a = bq_1 + r_1, \quad 0 \le r_1 < b. \tag{2}$$

Ако од (1) го одземеме (2), добиваме

$$0 = b(q - q_1) + (r - r_1). \tag{3}$$

Според тоа, $b \mid (r - r_1)$ и $b > (r_1 - r)$, при што или $r - r_1 \geq 0$ или $r_1 - r \geq 0$. Ако $r - r_1 > 0$, тогаш од $b \mid (r - r_1)$ и $0 < r - r_1 < b$ добиваме дека природен број е делив со природен број кој е поголем од него, што не е можно. Значи $r - r_1 = 0$, т.е. $r = r_1$. Сега, од (3) добиваме $0 = b(q - q_1)$ и бидејќи $b \neq 0$ имаме $q - q_1 = 0$ т.е. $q = q_1$, што значи дека броевите q и r се единствени. ■

2.2. Дефиниција. Броевите a, b, q и r од теорема 2.1 ги нарекуваме *деленик, делител, количник* и *остаток*, соодветно.

2.3. Забелешка. Од теорема 2.1 непосредно следува дека $b \mid a$ ако и само ако остатокот r од делењето на a со b е 0, т.е. $r = 0$.

Количникот q од теоремата 2.1 може да биде кој било цел број, а r е некој број од множеството $\{0, 1, ..., b-1\}$, кое го нарекуваме *множество на остатоци при делење со бројот* b.

2.4. Теорема. а) Збирот на природните броеви a и b е делив со природниот број c ако и само ако збирот на остатоците на броевите a и b при делење со бројот c е делив со c.

б) Остатокот од делењето на збирот на броевите a и b со бројот c е еднаков на остатокот од делењето на збирот на остатоците на броевите a и b при делење со бројот c.

Доказ. а) Според теоремата за делење со остаток, за броевите a и b имаме $a = cq_1 + r_1$ и $b = cq_2 + r_2$. Според тоа,

$$a + b = (cq_1 + r_1) + (cq_2 + r_2) = c(q_1 + q_2) + r_1 + r_2, \tag{4}$$

што значи дека $a + b$ е делив со c ако и само ако $r_1 + r_2$ е делив со c.

б) Доказот непосредно следува од равенството (4). Деталите ги оставаме на читателот за вежба. ■

2.5. При докажување на некои својства на природните броеви често пати се користиме со записот на броевите со помош на цифри, т.е. со *декадниот систем* кој користи десет цифри. Меѓутоа, во употреба се и бројни системи со основа различна од бројот 10. Така, на пример, во информатиката најчесто користен е бинарниот броен систем, кој има основа 2. Користењето на бројните системи со различна основа се потпира на следнава теорема.

Теорема. Нека b е природен број поголем од 1. Тогаш секој природен број m може на единствен начин да се запише во обликот

$$m = a_n b^n + a_{n-1} b^{n-1} + ... + a_2 b^2 + a_1 b + a_0 , \qquad (5)$$

каде $0 < a_n < b$ и $0 \le a_i < b,$ за $i = 0,1,2,...,n-1$.

Доказ. Нека b и m се дадени. Од теоремата за делење со остаток следува дека постојат q_0 и a_0 такви што

$$m = q_0 b + a_0 , \ 0 \le a_0 < b .$$

Јасно, $q_0 \ge 0$. Ако $q_0 > 0$, тогаш за q_0 и b постојат q_1 и a_1 такви што

$$q_0 = q_1 b + a_1 , \ 0 \le a_1 < b .$$

Продолжувајќи ја постапката добиваме

$$\begin{aligned}
&m = q_0 b + a_0 , && 0 \le a_0 < b , && q_0 > 0 , \\
&q_0 = q_1 b + a_1 , && 0 \le a_1 < b , && q_1 > 0 \\
&q_1 = q_2 b + a_2 , && 0 \le a_2 < b , && q_2 > 0 \\
&\text{.....} \\
&q_{n-2} = q_{n-1} b + a_{n-1} , && 0 \le a_{n-1} < b , && q_{n-1} > 0 \\
&q_{n-1} = q_n b + a_n , && 0 \le a_n < b , && q_n = 0
\end{aligned}$$

Понатаму, од неравенствата

$$m > q_0 > q_1 > ... > 0$$

следува дека постои природен број q_{n-1} кој е позитивен и е помал од b. Сега од последното равенство следува $a_n = q_{n-1}$, што значи дека a_n е позитивен број. Со последователна замена од горната низа равенства добиваме:

$$\begin{aligned}
m &= q_0 b + a_0 \\
&= (q_1 b + a_1) b + a_0 \\
&= q_1 b^2 + a_1 b + a_0 \\
&\text{.....} \\
&= (q_{n-1} b + a_{n-1}) b^{n-1} + ... + a_1 b + a_0 \\
&= q_{n-1} b^n + a_{n-1} b^{n-1} + ... + a_1 b + a_0 \\
&= a_n b^n + a_{n-1} b^{n-1} + ... + a_1 b + a_0 .
\end{aligned}$$

Со тоа ја докажавме егзистенцијата на претставувањето (5). Останува уште да ја докажеме единственоста. Нека $n \ge s$ и

$$a_n b^n + a_{n-1} b^{n-1} + ... + a_2 b^2 + a_1 b + a_0 = c_s b^s + c_{s-1} b^{s-1} + ... + c_2 b^2 + c_1 b + c_0$$

$0 < c_s < b$ и $0 \le c_j < b,$ за $j = 0,1,2,...,s-1$. Тогаш

$$b(a_n b^{n-1} + a_{n-1} b^{n-2} + ... + a_2 b + a_1 - c_s b^{s-1} - c_{s-1} b^{s-2} - ... - c_2 b - c_1) = c_0 - a_0 ,$$

што значи дека $b \mid (c_0 - a_0)$, па затоа $c_0 = a_0$. Ако во горното равенство поделиме со b, тогаш повторувајќи ја постапката добиваме $c_1 = a_1$. Повторувајќи ја постапката, добиваме дека $c_i = a_i$, за $i = 0,1,2,...,s$. Ако $n > s$ имаме

$$a_n b^{n-(s+1)} + a_{n-1} b^{n-(s+2)} + ... + a_{s+2} b + a_{s+1} = 0,$$

и како $b > 0$ од последното равенство следува $a_i = 0$, за $i = s+1, s+2, ..., n$. Со тоа е докажана единствеността на претставувањето (5). ■

2.6. Последица. Секој позитивен цел број m на единствен начин може да се претстави како збир на степени бројот 2.

Доказ. Во теорема 2.5 земаме $b = 2$ и добиваме

$$m = 2^n a_n + 2^{n-1} a_{n-1} + ... + 2^2 a_2 + 2a_1 + a_0,$$

каде $a_n = 1$ и $a_i = 0$ или 1, за $i = 0, 1, 2, ..., n-1$, од што следува тврдењето. ■

2.7. Дефиниција. Ако се исполнети условите од теорема 2.5 и ако важи (5), тогаш ќе велиме дека m е претставен во *броен систем со основа* b. Бројот b го нарекуваме *основа* (*база*) на даденият броен систем, а бројот m го запишуваме во видот $m = a_n a_{n-1} ... a_2 a_1 a_{0_b}$.

Ако од контекстот е јасно во кој броен систем е запишан некој број, тогаш во записот на бројот го изоставуваме индексот b. Така, на пример, во секојдневната пракса подразбираме дека записот на бројот е даден во декаден броен систем, ако не е поинаку кажано.

2.8. Забелешка. Кај бројните системи со основа поголема од 10 неопходно е да се воведат ознаки за дополнителни цифри. На пример, во систем со основа 12 за цифрите 10 и 11 можеме да ги користиме ознаките a и b. На тој начин ги добиваме цифрите за бројниот систем со основа 12: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a и b.

Во информатиката често пати се користи систем со основа 16, при што за цифрите A, B, C, D, E и F се користат за означување на броевите 10, 11, 12, 13, 14, и 15. Овој систем е познат под називот *хексадецимален систем*, а додека системот со основа 2 во литературата е познат под називот *бинарен систем*.

2.9. Пример. Нека A и B се n-цифрени броеви, n е непарен број, кои при делење со бројот k даваат ист остаток $r \neq 0$. Најди барем еден број k, кој не зависи од n, таков што бројот C добиен со допишување на цифрите од A и B е делив со k.

Решение. Нека $A = ka + r,\ B = kb + r,\ 0 < r < k$. Тогаш

$$C = 10^n A + B = 10^n (ka + r) + kb + r = k(10^n a + b) + (10^n + 1)r.$$

Бројот C е делив со k ако и само ако бројот $10^n + 1$ е делив со k. Но, $n = 2m + 1$, па затоа

$$10^n + 1 = 10^{2m+1} + 1 = 11D.$$

Конечно, еден број k кој го задоволува условот на задачата е бројот 11. ■

2.10. Пример. Определи ги сите тројки природни броеви (a,b,c) такви што производот на секои два броја при делење со третиот дава остаток 1.

Решение. Условот на задачата можеме да го формулираме на следниов начин: за броевите a,b,c постојат цели броеви x,y,z така што

$$ab-1=cz,\ bc-1=ax,\ ca-1=by.$$

Притоа броевите a,b,c мора да се различни од 1. Со множење на горните равенства добиваме

$$xyzabc=(abc)^2-abc(a+b+c)+ab+bc+ca-1.$$

Ако на десната страна ги префрлиме сите членови кои содржат abc, заклучуваме дека постои природен број k таков што

$$kabc=ab+bc+ca-1. \tag{1}$$

Понатаму, имаме два случаја:

- некои два броја се еднакви, на пример $a=b$, тогаш важи $xa=ac-1$, од каде добиваме $a=1$, што не е можно,
- трите броја a,b,c се различни меѓу себе. Заради симетрија нека, на пример, $a<b<c$. Тогаш имаме $kabc<ab+bc+ca<3bc$, па затоа $ka<3$, и како $k,a\in\mathbb{N}$ добиваме $k=1$ и $a=2$. Ако замениме во (1) добиваме $bc=2(b+c)-1$, од каде следуваат неравенствата $bc<2(b+c)<4c$, т.е. $b<4$. Но, $b>a=2$, па затоа $b=3$. Конечно, од (1) имаме $6c=5+5c$, т.е. $c=5$.

Од претходните разгледувања следува дека сите решенија на задачата се добиваат како пермутација на тројката $(2,3,5)$. ■

2.11. Пример. За бројот n ќе велиме дека е *добар* ако може да се претстави како збир на природни броеви, не задолжително различни, чиј збир на реципрочни вредности е еднаков на 1. Ако е познато дека броевите 33, 34, ..., 73 се добри, докажи дека сите броеви поголеми или еднакви на 33 се добри.

Решение. Нека n е добар број, при што за некои природни броеви a_i важи

$$a_1+a_2+...+a_k=n,\ \ \frac{1}{a_1}+\frac{1}{a_2}+...+\frac{1}{a_k}=1.$$

Тогаш

$$\frac{1}{2a_1}+\frac{1}{2a_2}+...+\frac{1}{2a_k}=\frac{1}{2},$$

па заради $\frac{1}{2}=\frac{1}{4}+\frac{1}{4}=\frac{1}{3}+\frac{1}{6}$ низите $(4,4,2a_1,2a_2,...,2a_k)$ и $(3,6,2a_1,2a_2,...,2a_k)$ имаат збир на реципрочни вредности 1. Оттука добиваме дека броевите $2n+8$ и $2n+9$ се исто така добри. Меѓутоа, $2\cdot33+8=74$ и $2\cdot33+9=75$, па со индукција добиваме дека сите броеви поголеми или еднакви на 33 се добри. ■

3. НАЈГОЛЕМ ЗАЕДНИЧКИ ДЕЛИТЕЛ

3.1. Делителите на секој природен број a се помали или еднакви на бројот a, па затоа секој природен број, а со тоа и секој цел број различен од нула, има конечно многу делители. Оттука има смисла следнава дефиниција.

Дефиниција. Нека $a,b\in\mathbb{N}$. За бројот d ќе велиме дека е *заеднички делител* на броевите a и b ако $d\mid a$ и $d\mid b$.

Нека $d_1,d_2,...,d_k$ се заеднички делители на a и b, и d е најголемиот меѓу броевите $d_1,d_2,...,d_k$, во ознака $d=\max\{d_1,d_2,...,d_k\}$. За бројот d ќе велиме дека е *најголем заеднички делител* на a и b.

За најголемиот заеднички делител на броевите a и b стандардни ознаки се (a,b) или $\mathrm{NZD}(a,b)$. Ние ќе ја користиме ознаката (a,b).

За бројот d ќе велиме дека е *заеднички делител* на броевите $a_1,a_2,...,a_n$ ако $d\mid a_1,d\mid a_2,...,d\mid a_n$.

Нека $d_1,d_2,...,d_k$ се заеднички делители на броевите $a_1,a_2,...,a_n$. Бројот $d=\max\{d_1,d_2,...,d_k\}$ го нарекуваме *најголем заеднички делител* на $a_1,a_2,...,\ a_n$ и го означуваме со $(a_1,a_2,...,a_n)$.

3.2. Теорема. а) Ако $a=bq$ и $b>0$, тогаш $(a,b)=b$.

б) $(a,b)=(a,b+ax)$, за секој $x\in\mathbb{Z}$.

Доказ. а) Од $a=bq$ следува дека $b\mid a$ и бидејќи $b\mid b$, добиваме дека b е заеднички делител на a и b. Понатаму, бидејќи $(a,b)\le b$ и b е заеднички делител на a и b, добиваме дека $(a,b)=b$.

б) Ако $c\mid a$ и $c\mid b$, тогаш $c\mid(b+ax)$, за секој $x\in\mathbb{Z}$, што значи дека секој заеднички делител на a и b е заеднички делител и на a и $b+ax$. Обратно, ако $c\mid a$ и $c\mid(b+ax)$, тогаш $c\mid(b+ax-ax)=b$, т.е. c е заеднички делител на a и b. Значи, множеството заеднички делители на a и b се совпаѓа со множеството заеднички делители на a и $b+ax$, па затоа $(a,b)=(a,b+ax)$, за секој $x\in\mathbb{Z}$. ■

3.3. Последица. За секои $a,b\in\mathbb{N}$ точни се равенствата

$$(a,b)=(b,a)=(a,-b)=(a,a+b)=(a,b-a).$$

Доказ. Равенствата $(a,b)=(b,a)=(a,-b)$ се очигледни, а равенствата $(a,b)=(a,a+b)=(a,b-a)$ следуваат од теорема 3.2. ■

3.4. Дефиниција. За природните броеви a и b ќе велиме дека се *заемно прости* ако $(a,b)=1$.

За броевите $a_1, a_2, ..., a_n$ ќе велиме дека се *заемно прости во целина* ако $(a_1, a_2, ..., a_n) = 1$.

За броевите $a_1, a_2, ..., a_n$ ќе велиме дека се *заемно прости по парови* ако $(a_i, a_j) = 1$, за $i \neq j$, т.е. секои два броја се заемно прости.

3.5. Теорема. Ако $(a,b) = d$, $a = dx$ и $b = dy$, тогаш $(x,y) = 1$.

Доказ. Да претпоставиме дека $(x,y) = k > 1$. Тогаш постојат природни броеви x_1 и y_1 такви што $x = kx_1$ и $y = ky_1$. Од $a = dx$ и $b = dy$ добиваме

$$a = d(kx_1) = (kd)x_1 \text{ и } b = d(ky_1) = (kd)y_1 .$$

Според тоа $dk \mid a$ и $dk \mid b$. Значи, бројот dk е заеднички делител на a и b поголем од d, што не е можно бидејќи $(a,b) = d$. Конечно, од добиената противречност следува дека $k = 1$, т.е $(x,y) = 1$, што и требаше да се докаже. ■

3.6. Пример. Нека $a, b, c \in \mathbb{N}$, $(a,b,c) = 1$ и $c = \frac{ab}{a-b}$. Докажи дека $a-b$ е точен квадрат.

Решение. Нека $(a,b) = (a, a-b) = k$. Значи, постојат $a_1, b_1 \in \mathbb{N}$ такви што $a = a_1 k$, $a - b = b_1 k$ и $(a_1, b_1) = 1$. Според тоа,

$$b = a - kb_1 = ka_1 - kb_1 = k(a_1 - b_1)$$

и

$$ab = k^2 a_1 (a_1 - b_1) ,$$

па затоа

$$c = \frac{ab}{a-b} = \frac{k^2 a_1 (a_1 - b_1)}{b_1 k} = \frac{k a_1 (a_1 - b_1)}{b_1} . \qquad (1)$$

Значи, $(a_1, b_1) = (a_1, a_1 - b_1) = 1$ и бидејќи $c \in \mathbb{N}$, од (1) следува $b_1 \mid k$. Ако $k = mb_1$, тогаш $m \mid c, m \mid b$ и $m \mid a$, па од $(a,b,c) = 1$, следува $m = 1$, т.е. $b_1 = k$. Конечно, од $a - b = b_1 k$ и $b_1 = k$ следува $a - b = k^2$, што и требаше да се докаже. ■

3.7. Пример. Нека $a_1 = 1$, $a_2 = 1$ и $a_{n+2} = a_{n+1} + a_n$, за $n \in \mathbb{N}$. Докажи дека за секои $n, k \in \mathbb{N}$ броевите $ka_{n+2} + a_n$ и $ka_{n+3} + a_{n+1}$ се заемно прости.

Решение. Воведуваме ознака $b_n = ka_{n+2} + a_n$, $n \in \mathbb{N}$ и наоѓаме

$$\begin{aligned} b_n + b_{n-1} &= (ka_{n+2} + a_n) + (ka_{n+1} + a_{n-1}) \\ &= k(a_{n+2} + a_{n+1}) + a_n + a_{n-1} \\ &= ka_{n+3} + a_{n+1} = b_{n+1}. \end{aligned}$$

Од последното равенство имаме

$$b_{n+1}-b_n=b_{n-1}. \tag{2}$$

Ако $d=(b_{n+1},b_n)$, тогаш $d\mid b_{n+1}$ и $d\mid b_n$, па од (2) следува $d\mid b_{n-1}$. Понатаму, од $d\mid b_n$ и $d\mid b_{n-1}$ добиваме дека $d\mid(b_n-b_{n-1})=b_{n-2}$. Повторувајќи ја оваа постапка конечен број пати, наоѓаме дека $d\mid b_i,\ i=1,2,...,n$. Од друга страна имаме

$$b_2=ka_4+a_2=3k+1 \text{ и } b_1=ka_3+a_1=2k+1.$$

Бидејќи $d\mid b_2,\ d\mid b_1$ добиваме

$$\begin{aligned}0<d\le(b_2,b_1)&=(3k+1,2k+1)=(3k+1-2k-1,2k+1)\\&=(k,2k+1)=(k,2k+1-2k)=(k,1)=1.\end{aligned}$$

Според тоа, $d=1$ и b_n и b_{n+1} се заемно прости, т.е. за секои $n,k\in\mathbb{N}$ броевите $ka_{n+2}+a_n$ и $ka_{n+3}+a_{n+1}$ се заемно прости. ■

3.8. Пример. Нека $p(x)$ е полином со целобројни коефициенти таков што $p(0)=p(1)=1$. Нека a_1 е произволен цел број. Дифинираме низа $a_n, n=1,2,3,...$ таква што за секој $n\ge1$ важи $a_{n+1}=p(a_n)$. Докажи дека членовите на оваа низа се по парови заемно прости броеви.

Решение. Нека a_m и a_k, $m>k$ се два елементи на дадената низа. Ако $d=m-k$, тогаш

$$a_m=a_{k+d}=\underbrace{p(p(...(p}_{d}(a_k))...)=p^d(a_k).$$

Притоа $p^d(x)$ исто така е полином со целобројни коефициенти.

Од $p(0)=1$ следува дека слободниот член на $p(x)$ е еднаков на 1. Но, $p^2(0)=p(p(0))=p(1)$, па затоа истото важи и за $p^2(x)$. Сега, со индукција лесно се докажува дека слободниот член на полиномот $p^r(x)$ е еднаков на 1 за секој $r\ge1$, бидејќи од претпоставката $p^r(0)=1$ следува

$$p^{r+1}(0)=p(p^r(0))=p(1)=1.$$

За секој полином $f(x)$ со целобројни коефициенти постои полином $q(x)\in\mathbb{Z}[x]$ таков што $f(x)=xq(x)+f(0)$. Специјално, постои $q_d(x)\in\mathbb{Z}[x]$ таков што

$$p^d(x)=xq_d(x)+p^d(0)=xq_d(x)+1.$$

Оттука добиваме дека важи

$$a_m=p^d(a_k)=a_kq_d(a_k)+1=a_kQ+1,$$

каде $Q=q_d(a_k)$ е цел број. Сега од горното равенство непосредно следува

$$(a_m,a_k)=(a_kQ+1,a_k)=1,$$

што и требаше да се докаже. ■

4. ЕВКЛИДОВ АЛГОРИТАМ

4.1. Теорема. Ако $a = bq + r$, тогаш $(a,b) = (b,r)$.

Доказ. Ако $(a,b) = d$, тогаш постојат x и y такви што $a = dx$ и $b = dy$. Значи, $dx = dyq + r$, па од теорема 1.3 следува $d \mid r$ и бидејќи $d \mid b$ заклучуваме дека $d \mid (b,r)$.

Јасно, $d = (b,r)$, бидејќи ако $d < (b,r) = d_1$, тогаш според теорема 1.3, од равенството $a = bq + r$ следува $d_1 \mid a$ и бидејќи $d_1 \mid b$, добиваме дека постои заеднички делител на a и b кој е поголем од d, што е противречност. ■

4.2. Ќе докажеме како со помош на теоремата за делење со остаток и претходната теорема може да се конструира таканаречениот *Евклидов алгоритам* за наоѓање на НЗД на два броја a и b. Имаме

$$\begin{aligned}
&a = bq_1 + r_1 && 0 \le r_1 < b \\
&b = r_1q_2 + r_2 && 0 \le r_2 < r_1 \\
&r_1 = r_2q_3 + r_3 && 0 \le r_3 < r_2 \\
&\ldots\ldots\ldots\ldots && \ldots\ldots\ldots\ldots \\
&r_{k-2} = r_{k-1}q_k + r_k && 0 \le r_k < r_{k-1} \\
&r_{k-1} = r_kq_{k+1} + r_{k+1} && 0 \le r_{k+1} < r_k \\
&\ldots\ldots\ldots\ldots\ldots\ldots && \ldots\ldots\ldots\ldots\ldots
\end{aligned} \qquad (1)$$

Бидејќи остатоците r_i опаѓаат со секој следен чекор, т.е.

$$r_1 > r_2 > r_3 > \ldots > r_k > r_{k+1} > \ldots \ge 0$$

постапката дефинирана со равенствата (1) ќе заврши по конечен број чекори, т.е. по конечен број чекори ќе добиеме равенство од видот $r_{n-1} = r_nq_{n+1} + 0$, т.е. ќе важи $r_{n+1} = 0$, при што $r_n \neq 0$. Од равенството $r_{n-1} = r_nq_{n+1}$ следува $r_n \mid r_{n-1}$. Претходно кажаното и теорема 4.1 ни овозможуваат да ја докажеме следнава теорема.

4.3. Теорема. Последниот остаток r_n различен од нула, добиен со низата равенства (1) е еднаков на најголемиот заеднички делител на броевите a и b.

Доказ. Ако ги земеме предвид равенствата (1), тогаш од теоремата 4.1 непосредно ја добиваме следнава низа равенства

$$(a,b) = (b,r_1) = (r_1,r_2) = (r_2,r_3) = \ldots = (r_{n-1},r_n).$$

Но, $r_n \mid r_{n-1}$ што според теорема 3.2 значи дека $(r_{n-1},r_n) = r_n$. Конечно, од последните две равенства наоѓаме $(a,b) = (r_{n-1},r_n) = r_n$. ■

4.4. Теорема (Безу). Ако $d = (a,b)$, тогаш постојат цели броеви x и y такви што $d = ax + by$.

Доказ. Според теоремата 4.3, во системот равенства (1) на Евклидовиот алгоритам важи $d = r_n = (a,b)$, каде што r_n е последниот остаток различен од нула. Равенствата (1) ги запишуваме во видот:

$$\begin{aligned} r_n &= r_{n-2} - q_n r_{n-1} \\ r_{n-1} &= r_{n-3} - q_{n-1} r_{n-2} \\ r_{n-2} &= r_{n-4} - q_{n-2} r_{n-3} \\ &\cdots\cdots\cdots\cdots \\ r_2 &= b - r_1 q_2 \\ r_1 &= a - b q_1 \end{aligned} \qquad (2)$$

Сега, ако во првото равенство на (2) од второто равенство замениме за r_{n-1}, потоа од третото равенство во (2) во новодобиеното равенство замениме за r_{n-2}, па во секое новодобиено равенство последователно замениме за $r_{n-3},\ldots,r_3,r_2$ и r_1, добиваме равенство од вид $d = ax+by$. ■

4.5. Забелешка. Броевите x и y во претходната теорема се заемно прости, т.е. $(x,y)=1$.

Навистина, ако претпоставиме дека $(x,y)=k>1$, тогаш постојат $x_1, y_1 \in \mathbb{N}$ такви што $x = kx_1$ и $y = ky_1$. Слично, од $d=(a,b)$ следува дека постојат $a_1, b_1 \in \mathbb{N}$ такви што $a = da_1$ и $b = db_1$. Ако замениме во равенството $d = ax+by,$ добиваме

$$d = (da_1)(kx_1)+(db_1)(ky_1) = kd(a_1x_1+b_1y_1)\ ,$$

т.е. $kd \mid d$, што не е можно бидејќи $kd > d$. Од добиената противречност следува дека $(x,y)=1$.

Понатаму, ако $d=(a,b)$, тогаш броевите x и y во равенството $d = ax+by$ не се еднозначно определени. .

4.6. Теорема. а) Ако $c \mid a$ и $c \mid b$, тогаш $c \mid (a,b)$.

б) Ако $d \mid a,\ d \mid b$ и $d = ax+by$, за некои цели броеви x и y, тогаш $d=(a,b)$.

Доказ. а) Од теорема 4.4 следува дека постојат цели броеви x и y такви, што $(a,b) = ax+by$. Понатаму, од $c \mid a$ имаме $a = cm$ за некој цел број m, а од $c \mid b$ следува $b = cn$ за некој цел број n. Заменуваме во равенството $(a,b) = ax+by$ и добиваме $(a,b) = ax+by = (cm)x+(cn)y = c(mx+ny)$, што значи $c \mid (a,b)$.

б) Да претпоставиме дека $d \mid a, d \mid b$ и $d = ax+by$, за некои цели броеви x и y. Од тврдењето под а) следува дека $d \mid (a,b)$. Понатаму, постојат $a_1, b_1 \in \mathbb{N}$ такви што $a = a_1 \cdot (a,b)$ и $b = b_1 \cdot (a,b)$. Ако замениме во $d = ax+by$, добиваме

$$d = [a_1 \cdot (a,b)]x+[b_1 \cdot (a,b)]y = (a,b)\cdot(a_1x+b_1y)$$

што значи $(a,b)\mid d$.

Конечно, од $d\mid(a,b)$ и $(a,b)\mid d$ следува $d=(a,b)$. ■

4.7. Последица. а) $(m,n)=1$ ако и само ако постојат $x,y\in\mathbb{Z}$ такви што

$$mx+ny=1. \tag{3}$$

б) Ако $(a,k)=(b,k)=1$, тогаш $(ab,k)=1$.

Доказ. а) Нека $(m,n)=1$. Тогаш, од теорема 4.4 следува дека постојат $x,y\in\mathbb{Z}$ такви што $mx+ny=1$, т.е. важи (3).

Обратно, ако постојат $x,y\in\mathbb{Z}$ такви што важи (3), тогаш бидејќи $1\mid a$ и $1\mid b$, од теорема 4.6 б) следува дека $(m,n)=1$.

б) Од теорема 4.4 следува дека постојат $x,y,m,n\in\mathbb{Z}$ такви што $ax+ky=1$ и $bm+kn=1$, т.е. $ax=1-ky$ и $bm=1-kn$. Ако ги помножиме последните две равенства добиваме равенство кое е еквивалентно на равенството

$$(ab)(mx)+k(n+y-kny)=1.$$

Конечно, од тврдењето под а) следува $(ab,k)=1$. ■

4.8. Теорема. а) Ако $k>0$, тогаш $(ka,kb)=k\cdot(a,b)$.

б) Ако $c\mid a, c\mid b$ и $c>0$, тогаш $(\frac{a}{c},\frac{b}{c})=\frac{1}{c}\cdot(a,b)$.

Доказ. а) Нека $d=(a,b)$. Според тоа, $d\mid a$ и $d\mid b$ и постојат постојат x и y такви што $d=ax+by$. Но, тоа значи дека $kd\mid ka$, $kd\mid kb$ и постојат x и y такви што $kd=k(ax+by)=(ka)x+(kb)y$. Сега, од теорема 4.7 б) следува дека

$$(ka,kb)=kd=k\cdot(a,b).$$

б) Од $c\mid a$ и $c\mid b$ следува дека постојат m и n такви што $a=cm$ и $b=cn$. Сега од а) следува $(a,b)=(cm,cn)=c\cdot(m,n)=c\cdot(\frac{a}{c},\frac{b}{c})$, т.е. $(\frac{a}{c},\frac{b}{c})=\frac{1}{c}\cdot(a,b)$. ■

4.9. Теорема. а) Ако $q\mid ab$ и $(q,b)=1$, тогаш $q\mid a$.

б) Ако $q\mid a$, $p\mid a$ и $(q,p)=1$, тогаш $qp\mid a$.

Доказ. а) Според теорема 4.4, од $(q,b)=1$ следува дека постојат цели броеви m и n такви што $1=bm+qn$. Ако последното равенство го помножиме со a, добиваме дека постојат цели броеви m и n такви што

$$a=abm+qan. \tag{4}$$

Од условот на теоремата имаме дека $q\mid ab$, т.е. постои природен број k таков што $ab=qk$. Со замена во равенството (4), добиваме

$$a=(qk)m+qan=q(km+an).$$

Конечно, од последното равенство следува дека $q \mid a$.

б) Од $q \mid a$ и $p \mid a$ следува дека $a = qm$ и $a = pn$ за некои $m,n \in \mathbb{N}$. Според тоа, $qm = pn$ па затоа $q \mid pn$. Но, $(q,p) = 1$ и бидејќи $q \mid pn$, од тврдењето под а) следува $q \mid n$, што значи дека постои $k \in \mathbb{N}$ таков што $n = qk$. Конечно, $a = pn = p(qk) = (pq)k$, од што следува дека $pq \mid a$. ■

4.10. Последица. Ако за природните броеви a,b,c,d важи $ab = cd$, тогаш постојат природни броеви x,y,z,u такви што $a = xy, b = zu, c = xz$ и $d = yu$.

Доказ. Нека $x = (a,c)$. Тогаш постојат $y,z \in \mathbb{N}$ такви што $a = xy$, $c = zx$ и $(y,z) = 1$. Заменуваме во $ab = cd$ и добиваме $xyb = xzd$, односно $yb = zd$. Според тоа, $y \mid zd$ и како $(y,z) = 1$, од претходната теорема следува дека $y \mid d$, т.е. постои $u \in \mathbb{N}$ таков што $d = yu$. Сега, со замена во $yb = zd$ добиваме $yb = yzu$, т.е. $b = zu$. ■

4.11. На крајот од оваа точка ќе докажеме тврдење кое се однесува на бројот на чекорите n во Евклидовиот алгоритам.

Теорема. За бројот на чекорите n во Евклидовиот алгоритам важи $n < 2\log_2 b$.

Доказ. Да го разгледаме $i-$тиот чекор. Имаме $r_i \le \frac{r_{i-1}}{2}$ или $\frac{r_{i-1}}{2} < r_i < r_{i-1}$. Во вториот случај важи $\frac{r_{i-1}}{2} q_{i+1} + r_{i+1} < r_{i-1} < r_{i-1} q_{i+1} + r_{i+1}$, па затоа мора да е

$$q_{i+1} = 1 \text{ и } r_{i+1} = r_{i-1} - r_i < \frac{r_{i-1}}{2}.$$

Значи, во секој случај $r_{i+1} < \frac{r_{i-1}}{2}$. Оттука следува

$$1 \le r_n < \frac{r_{n-2}}{2} < \frac{r_{n-4}}{4} < \ldots < \frac{r_0}{2^{\frac{n}{2}}}$$

ако n е парен, а

$$1 \le r_{n-1} < \frac{r_{n-3}}{2} < \frac{r_{n-5}}{4} < \ldots < \frac{r_0}{2^{\frac{n-1}{2}}}$$

ако n е парен.

Според тоа, во секој случај важи $b = r_0 > 2^{\frac{n}{2}}$, па затоа $n < 2\log_2 b$. ■

4.12. Пример. Пресметај (f_{1960}, f_{1988}), каде f_n е низата на Фибоначи која е определена со $f_1 = f_2 = 1$ и $f_{n+2} = f_{n+1} + f_n$, за $n \ge 1$.

Решение. Имаме:

$$f_{n+3} = f_{n+2} + f_{n+1} = (f_{n+1} + f_n) + f_{n+1} = 2f_{n+1} + f_n,$$

$$f_{n+4} = f_{n+3} + f_{n+2} = (2f_{n+1} + f_n) + (f_{n+1} + f_n) = 3f_{n+1} + 2f_n,$$
$$f_{n+5} = f_{n+4} + f_{n+3} = (3f_{n+1} + 2f_n) + (2f_{n+1} + f_n) = 5f_{n+1} + 3f_n,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Сега, со индукција се докажува дека

$$f_{n+i} = f_i f_{n+1} + f_{i-1} f_n, \tag{5}$$

за секој $i \geq 2$. Ако ставиме $i = (k-1)n$ за $k \geq 2$ добиваме

$$f_{kn} = f_{(k-1)n} f_{n+1} + f_{(k-1)n-1} f_n,$$

од каде со индукција лесно се докажува дека важи

$$f_n \mid f_{kn}, \tag{6}$$

за секои $n, k \in \mathbb{N}$. Сега, непосредно се добива дека

$$(f_{n+1}, f_n) = (f_n, f_{n-1}) = \ldots = (f_2, f_1) = 1, \tag{7}$$

за секој $n \in \mathbb{N}$.

Од (5) следува

$$f_{1988} = f_{28} f_{1961} + f_{27} f_{1960}.$$

Сега, од (7) имаме $(f_{1960}, f_{1961}) = 1$, па затоа ако $d = (f_{1960}, f_{1988})$, тогаш $d \mid f_{28}$. Но, $1988 = 71 \cdot 28$ и $1960 = 70 \cdot 28$, па затоа од (6) следува $f_{28} \mid d$. Според тоа, $d \mid f_{28}$ и $f_{28} \mid d$, што значи $d = f_{28} = 317811$.

Коментар. Може да се докаже дека $(f_s, f_t) = f_{(s,t)}$. ■

4.13. Пример. Одреди го најголемиот заеднички делител на броевите

$$2^{2^2} + 2^{2^1} + 1,\ 2^{2^3} + 2^{2^2} + 1, \ldots, 2^{2^{n+1}} + 2^{2^n} + 1, \ldots \tag{8}$$

Решение. Со индукција по n ќе докажеме дека бројот $2^{2^2} + 2^{2^1} + 1 = 21$ е делител на секој од броевите во низата (5).

Ја воведуваме ознаката $a_k = 2^{2^{k+1}} + 2^{2^k} + 1,\ k = 1, 2, \ldots$. За $n = 1$ имаме

$$a_1 = 2^{2^2} + 2^{2^1} + 1 = 21,$$

па затоа $21 \mid a_1$, т.е. тврдењето важи за $n = 1$. Нека претпоставиме дека тврдењето важи за $n = k$, т.е. дека $21 \mid a_k$. За $n = k+1$ имаме

$$a_{k+1} = 2^{2^{k+2}} + 2^{2^{k+1}} + 1 = 2^{2^{k+1}}(2^{2^{k+1}} + 2^{2^k} + 1) - (2^{3 \cdot 2^k} - 1). \tag{9}$$

Од индуктивната претпоставка следува дека првиот собирок во (9) е делив со 21.

Ќе докажеме дека $2^{3 \cdot 2^k} - 1$ е делив со 21. Имаме,

$$2^{3 \cdot 2^k} - 1 = (2^3)^{2^k} - 1 = (2^3 - 1)[(2^3)^{2^k - 1} + (2^3)^{2^k - 2} + \ldots + 1],$$

па затоа $2^{3 \cdot 2^k} - 1$ е делив со 7. Исто така $2^{3 \cdot 2^k} - 1 = 2^{2m} - 1$, каде $m = 3 \cdot 2^{k-1}$, па затоа

$$2^{3\cdot 2^k}-1=(2^2-1)[(2^2)^{m-1}+(2^2)^{m-2}+\ldots+1],$$

што значи дека $2^{3\cdot 2^k}-1$ се дели со 3 . Но, $(7,3)=1$, па од теорема 4.9 б) следува дека $3\cdot 7=21\mid 2^{3\cdot 2^k}-1$. Според тоа,

$$21\mid 2^{2^{k+1}}(2^{2^{k+1}}+2^{2^k}+1) \text{ и } 21\mid (2^{3\cdot 2^k}-1),$$

па затоа $21\mid a_{k+1}$, т.е. тврдењето важи за $n=k+1$. Од принципот на математичка индукција следува дека $21\mid a_n$, за секој $n\in\mathbb{N}$.

Од претходно изнесеното и од $a_1=21$ следува дека најголемиот заеднички делител на броевите во низата (5) е еднаков на 21. ■

5. НАЈМАЛ ЗАЕДНИЧКИ СОДРЖАТЕЛ

5.1. Дефиниција. Нека $a,b\in\mathbb{N}$. За бројот $c\in\mathbb{N}$ ќе велиме дека е *заеднички содржател* на броевите a и b ако $a\mid c$ и $b\mid c$.

5.2. Од дефиниција 5.1 непосредно следува дека за секои $a,b\in\mathbb{N}$, броевите од видот $kab, k\in\mathbb{N}$ се заеднички содржатели на a и b. Според тоа, за секои a и b множеството од нивни заеднички содржатели е бесконечно, па затоа истото нема најголем елемент. Природно е да се запрашаме дали меѓу заедничките содржатели на a и b постои најмал содржател. Одговорот на ова прашање е потврден. Навистина, бројот $c_1=ab$ е заеднички содржател на a и b. Ако тој не е најмал, тогаш постои природен број c_2 таков што $c_2<c_1$ и $a\mid c_2$ и $b\mid c_2$. Ако c_2 не е најмал меѓу заедничките содржатели на a и b, тогаш постои заеднички содржател c_3 на a и b таков што $c_3<c_2$. Бидејќи природните броеви $c_1,c_2,c_3,\ldots$ се намалуваат, после конечен број чекори ќе најдеме најмал природен број c за кој важи $a\mid c$ и $b\mid c$. Јасно, ова е *најмалиот заеднички содржател* на a и b и за истиот се користи ознаката $c=\mathrm{NZS}(a,b)$. Да забележиме дека во литературата за најмалиот заеднички содржател на броевите a и b се користи и ознаката $[a,b]$, која ние ќе ја користиме во нашите разгледувања.

5.3. Теорема. Ако $[a,b]=s$ и S е произволен заеднички содржател на a и b, тогаш $s\mid S$, што значи дека сите заеднички содржатели на броевите a и b се од обликот $S=sk, k\in\mathbb{N}$.

Доказ. Од теоремата за делење со остаток следува дека постојат q и r такви што $S=sq+r,\quad 0\le r<s$. Ако $r\neq 0$, тогаш од $a\mid S$, $a\mid s$ и од претходното равен-

ство следува дека $a \mid r$. Слично $b \mid r$, што значи дека најдовме заеднички содржател на a и b кој е помал од s. Последното му противречи на фактот дека $[a,b]=s$. Од добиената противречност следува $r=0$, т.е. $S=sq$. ■

5.4. Теорема. Ако $(a,b)=1$, тогаш $[a,b]=ab$.

Доказ. Нека $[a,b]=s\le ab$. Тогаш, $s=am$, за некој $m\in\mathbb{N}$. Според тоа, $b \mid am$ и бидејќи $(a,b)=1$, од теорема 4.9 а) следува дека $b \mid m$, т.е. $m=bn$, за некој $n\in\mathbb{N}$. Од досега изнесеното имаме

$$s=am=a(bn)=(ab)n$$

и бидејќи $s\le ab$, од последното равенство следува $n=1$, што значи дека $s=ab$, т.е. $[a,b]=ab$. ■

5.5. Теорема. а) $[na,nb]=n\cdot[a,b]$, за секои $n,a,b\in\mathbb{N}$.

б) $[a,b]\cdot(a,b)=ab$, за секои $a,b\in\mathbb{N}$.

Доказ. а) Нека $[a,b]=x$. Значи, $a \mid x$ и $b \mid x$, па затоа $na \mid nx$ и $nb \mid nx$, т.е. nx е заеднички содржател на na и nb. Сега, од теорема 5.3 следува дека $[na,nb] \mid nx=n\cdot[a,b]$.

Нека $[na,nb]=s$. Тоа значи дека $na \mid s$, т.е. постои $q\in\mathbb{N}$ таков што $s=(na)q=n(aq)$, односно $s=ny$, $y=aq$. Јасно, $a \mid y$. Понатаму, $nb \mid s$, па затоа постои $k\in\mathbb{N}$ таков што $ny=s=(nb)k=n(bk)$, односно $y=bk$. Последното значи $b \mid y$, што заедно со $a \mid y$ повлекува дека y е заеднички содржател на a и b. Сега од теорема 4.3 следува дека $[a,b]=x \mid y$, односно

$$n\cdot[a,b]=nx \mid ny=s=[na,nb].$$

Конечно, $[na,nb] \mid n\cdot[a,b]$ и $n\cdot[a,b] \mid [na,nb]$ па затоа

$$[na,nb]=n\cdot[a,b].$$

б) Нека $(a,b)=d$ и m и n се такви што $a=md, b=nd$ и $(m,n)=1$. Од теорема 5.4 и од тврдењето под а) добиваме:

$$\begin{aligned} ab&=(md)(nd)=d\cdot d(mn)\\ &=(a,b)\cdot(d\cdot[m,n])\\ &=(a,b)\cdot[md,nd]\\ &=(a,b)\cdot[a,b]. \blacksquare \end{aligned}$$

5.6. Коментар. Во претходните разгледувања се задржавме на најмалиот заеднички содржател на два природни броја a и b. Аналогно се дефинира најмал заеднички содржател на конечно многу природни броеви $a_1, a_2, ..., a_k$. Притоа, тој

може да се определи и на следниов начин: најпрво определуваме $[a_1,a_2]=s_1$, а потоа определуваме $[s_1,a_3]=s_2$ итн. Последниот елемент s_{k-1} во низата $s_1,...,s_{k-1}$ е *најмалиот заеднички содржател* на броевите $a_1, a_2, ..., a_k$.

5.7. Пример. Нека a и b се природни броеви. Докажи дека

$$a^n+b^n \le (a,b)^n+[a,b]^n \text{, за секој } n\in\mathbb{N}.$$

Решение. Нека $d=(a,b)$ и $s=[a,b]$. Тогаш $s\ge a, s\ge b$ и $ab=ds$. Сега тврдењето на задаачата следува од неравенството

$$d^n+s^n-a^n-b^n=\frac{(ds)^n+s^{2n}-a^ns^n-b^ns^n}{s^n}=\frac{(s^n-a^n)(s^n-b^n)}{s^n}\ge 0. \blacksquare$$

5.8. Пример. Нека a и b се природни броеви такви што $a<b$. Докажи дека меѓу произволни b последователни природни броеви може да се најдат два броја чиј производ е делив со ab.

Решение. Нека $\{x_1,x_2,...,x_b\}$ е множество од b последователни природни броеви. Тогаш меѓу нив постои број x_i кој е делив со b и како $a<b$, постои број x_k кој е делив со a.

Ако $i\ne k$, тогаш производот x_ix_k е делив со ab.

Нека $i=k$. Да означиме $d=(a,b)$ и $s=[a,b]$. Тогаш $ds=ab$ и $s\mid x_i$. Ќе докажеме дека барем еден од броевите x_i+d и x_i-d, кои се деливи со d, припаѓа на множеството $\{x_1,x_2,...,x_b\}$. Навистина, ако двата броја не припаѓаат на ова множество, тогаш важи $x_i+d>x_b$ и $x_i-d<x_1$, па затоа $2d>x_b-x_1+1=b$. Но, $d\mid b$, па од последното неравенство ќе следува $d=b>a$, што противречи на $d=(a,b)$.

Ако $x_i+d\in\{x_1,x_2,...,x_b\}$, тогаш производот $x_i(x_i+d)$ е делив со $ds=ab$, а ако $x_i-d\in\{x_1,x_2,...,x_b\}$, тогаш производот $x_i(x_i-d)$ е делив со $ds=ab$. $\blacksquare$

II ГЛАВА
ПРОСТИ БРОЕВИ

1. ПОИМ ЗА ПРОСТ И СЛОЖЕН БРОЈ

1.1. Дефиниција. За природниот број p ќе велиме дека е *прост* ако p има точно два природни делители, т.е. единствени делители на p се 1 и p. Природниот број m кој има повеќе од два природни делители го нарекуваме *сложен број*.

1.2. Коментар. Според бројот на делителите, разликуваме три вида на природни броеви: броеви со еден делител (тоа е бројот 1), броеви со два делители (прости броеви) и броеви со повеќе од два делители (сложени броеви).

1.3. Теорема. Секој природен број n, поголем од 1, е делив барем со еден прост број.

Доказ. Ако природниот број n е прост, тогаш тврдењето е докажано. Имено, тој е делив со самиот себе, што значи со еден прост број.

Да претпоставиме дека n е произволен сложен број. Тогаш, тој мора да има барем еден делител различен од 1 и n, бидејќи во спротивно ќе биде прост број. Најмалиот од сите делители на n, различни од 1 и n, да го означиме со p. Ќе докажеме дека p е прост број. Навистина, ако p е сложен број, тогаш тој има делител q, $1<q<p$. Но, тогаш бројот q е делител на n, помал од p, што противречи на изборот на p. Од добиената противречност следува дека p е прост број. Конечно, сложениот број n е делив со простиот број p, што значи барем со еден прост број. ■

1.4. Според дефиниција 1.1 прости броеви се, на пример: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 и 37. Да забележиме дека единствен парен прост број е бројот 2. Имено, секој парен број поголем од 2 има најмалку три делители, и тоа 1, 2 и самиот број, што значи е сложен број.

Според теорема 1.3, за да утврдиме дали еден природен број, поголем од 1, е прост или сложен, доволно е да провериме дали тој е делив со последователните прости броеви 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ... Природно е да се запрашаме дали треба да делиме со сите прости броеви кои се помали од разгледуваниот број. Одговорот на ова прашање го дава следнава теорема.

1.5. Теорема. Ако природниот број p, $p>1$ не е делив со простите броеви чии квадрати се помали од p, тогаш p е прост број.

Доказ. Нека p е сложен број. Постои природен број $a \neq p$ и 1 таков што $a \mid p$. Значи, $p = ab$ каде што a и b се природни броеви помали од p. Нека $a \leq b$. Тогаш, $a^2 \leq ab = p$.

Можни се два случаи: a е прост број или a не е прост број.

Ако a е прост број, тогаш p е делив со прост број чиј квадрат е помал од p и во овој случај тврдењето е докажано.

Ако a не е прост број, тогаш постои прост број $q < a$ таков што $q \mid a$, па затоа $q \mid p$. Притоа $q^2 < a^2 \leq p$. Според тоа, p е делив со прост број чиј квадрат е помал од p, па и во овој случај тврдењето е докажано. ■

1.6. Коментар. Постапката за одредување на видот на еден природен број е доста сложена. Затоа се изготвуваат таблици на прости броеви. Едноставна постапка за изготвување на таблиците на прости броеви предложил Ератостен (III век пне.) и според него оваа постапка е наречена *Ератостеново сито*. Таа се состои во следново.

Ги испишуваме сите природни броеви помали или еднакви на бројот N. Најпрво ја прецртуваме единицата. Бидејќи првиот прост број е 2, ги прецртуваме сите природни броеви деливи со 2 и поголеми од 2 (тие се сложени). Следниот непрецртан број, кој е прост е бројот 3 и ги прецртуваме сите природни броеви деливи со 3 и поголеми од 3. Следниот непрецртан број е 5. Тој е прост, бидејќи ако не е ќе биде прецртан. Повторувајќи ја постапката јасно е дека можат да се определат сите прости броеви помали од даден природен број N. Според теоремата 1.5 доволно е проверката да ја направиме со прецртување на содржателите на простите броеви кои се помали или еднакви на $\sqrt{N}$.

1.7. Множеството сложени броеви е бесконечно, што може да се заклучи и од фактот дека множеството

$$A = \{4, 6, 8, 10, 12, 14, \ldots, 2k, \ldots\},$$

во кое сите броеви се сложени, е бесконечно.

Меѓутоа, одговорот на прашањето колку прости броеви има не е така едноставен. На ова прашање, во своето дело *Елементи*, дал одговор Евклид, III век пне. Имено, Евклид ја докажал следнава теорема.

1.8. Теорема. Постојат бесконечно многу прости броеви.

Доказ. Да претпоставиме дека постојат конечно многу прости броеви и да ги нумерираме по растечки редослед

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ \ldots,\ p_n = p\ . \tag{1}$$

Да го разгледаме бројот $N = p_1 p_2 p_3 \ldots p_n + 1$. Имаме, $N = p_i N_i + 1$, за $i = 1, 2, \ldots, n$ од што следува дека ниту еден од простите броеви во (1) не е делител на N. Зна-

чи, или бројот N е прост број или има прост делител кој не е меѓу броевите во (1). И во двата случаи заклучуваме дека постои прост број кој е поголем од најголемиот претпоставен прост број p, што противречи на претпоставката, па затоа постојат бесконечно многу прости броеви. ■

1.9. Дефиниција. За простиот број p ќе велиме дека p^{α} точно го дели n и ќе пишуваме $p^{\alpha} \| n$ ако $p^{\alpha} | n$ и $p^{\alpha+1} \nmid n$. Притоа ја користиме и ознаката $\alpha = v_p(n)$.

1.10. Теорема. Ако $p^{\alpha} \| n$ и $p^{\beta} \| m$, каде $\alpha > \beta$, тогаш $p^{\beta} \| n \pm m$.

Доказ. Нека $n = p^{\alpha} n_1$ и $m = p^{\beta} m_1$, при што $p \nmid m_1, n_1$. Имаме,

$$n \pm m = p^{\alpha} n_1 \pm p^{\beta} m_1 = p^{\beta}(p^{\alpha-\beta} n_1 \pm m_1),$$

при што $p^{\alpha-\beta} n_1 \pm m_1$ не е делив со p па затоа $p^{\beta} \| n \pm m$. ■

1.11. Коментар. Во теорема 1.8 докажавме дека множеството прости броеви е бесконечно, какво што е и множеството сложени броеви.

Во врска со сложените броеви ќе ја докажеме следнава теорема.

1.12. Теорема. За произволен природен број k, постојат k последователни сложени броеви.

Доказ. Да ги разгледаме броевите

$$a_1 = (k+1)k(k-1)\cdot \ldots \cdot 3 \cdot 2 + 2,$$
$$a_2 = (k+1)k(k-1)\cdot \ldots \cdot 3 \cdot 2 + 3,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_k = (k+1)k(k-1)\cdot \ldots \cdot 3 \cdot 2 + k + 1$$

Ова се k последователни природни броеви и сите се сложени бидејќи a_1 е делив со 2, a_2 е делив со 3, ... , a_k е делив со $k+1$. ■

1.13. Пример. Докажи, дека за секој парен број $n \geq 5$ постојат прости броеви p и q помали од $n-1$ такви што $(n-p, n-q) = 1$.

Решение. Нека $p = 2, q = 3$. Тогаш од $n \geq 5$ следува $p < q < n-1$ при што $n - p = n-2, n-q = n-3$. Јасно,

$$(n-p, n-q) = (n-2, n-3) = 1. \blacksquare$$

1.14. Пример. За кои природни броеви n бројот

$$3^{2n+1} - 2^{2n+1} - 6^n$$

е сложен?

Решение. Дадениот израз може да се запише во видот

$$\begin{aligned} 3^{2n+1}-2^{2n+1}-6^n &= 3\cdot(3^n)^2-2\cdot(2^n)^2-3^n\cdot 2^n \\ &= 3\cdot(3^n)^2+2\cdot 3^n\cdot 2^n-3\cdot 3^n\cdot 2^n-2\cdot(2^n)^2 \\ &= 3^n(3\cdot 3^n+2\cdot 2^n)-2^n(3\cdot 3^n+2\cdot 2^n) \\ &= (3^n-2^n)(3^{n+1}+2^{n+1}). \end{aligned}$$

Бидејќи за секој $n>1$ важи $3^n-2^n>1$, заклучуваме дека дадениот број е сложен за секој природен број $n>1$. За $n=1$ тој е еднаков на простиот број 13. ■

1.15. Пример Природните броеви a и b се такви што $a>b$, $a\neq 1$, $b\neq 1$ и b^2+a-1 е делител на a^2+b-1. Докажи, дека b^2+a-1 има барем два различни прости делители.

Решение. Нека претпоставиме дека a и b се броеви кои го исполнуваат условот на задачата. Од равенството

$$(b^2-1)^2-a^2=(b^2-a-1)(b^2+a-1),$$

добиваме дека

$$(b^2+a-1)\,|\,[(b^2-1)^2-a^2]. \tag{2}$$

Јасно,

$$(b^2-1)^2+(b-1)=[(b^2-1)^2-a^2]+[a^2+(b-1)].$$

Од (2) и условот на задачата $(b^2+a-1)\,|\,(a^2+b-1)$, добиваме дека

$$(b^2+a-1)\,|\,[(b^2-1)^2+(b-1)]=b(b-1)(b^2+b-1). \tag{3}$$

За секој природен број b се точни равенствата

$$(b,b-1)=1,\ (b,b^2+b-1)=1,\ (b-1,b^2+b-1)=1. \tag{4}$$

Јасно, точни се и неравенствата

$$\begin{aligned} &b<b^2+a-1, \\ &b-1<b^2+a-1, \\ &b^2+b-1<b^2+a-1, \end{aligned} \tag{5}$$

при што точноста на третото неравенство е последица од неравенството $b<a$.

Нека претпоставиме дека $p=b^2+a-1$ е прост број. Заради (3) добиваме $p\,|\,b$ или $p\,|\,(b-1)$ или $p\,|\,(b^2+b-1)$, што не е можно заради (5). Според тоа b^2+a-1 не е прост број, што значи дека има најмалку два прости делителa. ■

1.16. Пример. Природните броеви a, b, c и d се такви што

$$ab^2+ad^2+cb^2=ba^2+bd^2+ca^2$$

и $a^2+b^2+c^2+d^2$ е прост број. Докажи, дека $a=b$.

Решение. Нека $a\neq b$. Условот на задачата можеме да го запишеме во облик

$$(a-b)d^2-ab(a-b)-ac(a-b)-(a-b)bc=0,$$

т.е.

$$(a-b)(d^2-ab-ac-bc)=0.$$

Но $a-b\neq 0$, па според тоа

$$d^2-ab-ac-bc=0,$$

односно

$$d^2=ab+bc+ca. \tag{6}$$

Тогаш

$$\begin{aligned} a^2+b^2+c^2+d^2 &= a^2+b^2+c^2+ab+bc+ca \\ &= a^2+b^2+c^2+2ab+2bc+2ca-ab-bc-ca \\ &= (a+b+c)^2-(ab+bc+ca)=(a+b+c)^2-d^2 \\ &= (a+b+c-d)(a+b+c+d). \end{aligned}$$

Бидејќи $a^2+b^2+c^2+d^2$ е прост број и $a+b+c-d<a+b+c+d$, добиваме $a+b+c-d=1$, односно

$$d=a+b+c-1. \tag{7}$$

Сега од (6) и (7) последователно добиваме

$$\begin{aligned} &d^2=(a+b+c-1)^2 \\ &ab+bc+ca=a^2+b^2+c^2+2ab+2bc+2ca-2a-2b-2c+1 \\ &a(a+b-2)+b(b+c-2)+c(c+a-2)+1=0. \end{aligned}$$

Во последното равенство сите собироци се ненегативни и освен тоа последниот е поголем од нула, што е противречност.

Конечно, од добиената противречност следува дека $a=b$. ■

1.17. Пример. Нека p е прост број, а n е природен број. Докажи дека постои најмногу еден природен број d таков што важи $d\mid pn^2$ и n^2+d е точен квадрат.

Решение. Нека

$$n^2+d=m^2, \tag{2}$$

и нека $z=(m,n)$. Тогаш имаме $n=xz$ и $m=yz$, каде $(x,y)=1$, па од (2) следува дека $d=az^2$ за некој природен број a. Притоа $az^2=d\mid pn^2=px^2z^2$, па затоа $a\mid px^2$. Ако замениме во (2) и скратиме со z^2 добиваме $x^2+a=y^2$. Последното равенство го множиме со p и добиваме

$$px^2+pa=py^2.$$

Бидејќи $a \mid px^2$, левата страна на последното равенство е делива со a, па затоа $a \mid py^2$. Сега, од $(x,y)=1$ следува $(x^2,y^2)=1$, па затоа постојат цели броеви α,β такви што $\alpha x^2+\beta y^2=1$. Но, тогаш

$$a \mid (\alpha px^2+\beta py^2)=p(\alpha x^2+\beta y^2)=p,$$

па затоа $a=1$ или $a=p$.

Ако $a=1$, тогаш $x^2+1=y^2$, од каде добиваме $x=0$ и $n=xz=0$, што не е можно. Значи, можно е само $a=p$. Тогаш важи $x^2+p=y^2$, односно

$$p=y^2-x^2=(y-x)(y+x),$$

па затоа $y-x=1$ и $y+x=p$, т.е. $y=\frac{p+1}{2}$ и $x=\frac{p-1}{2}$. Оттука $n=xz=\frac{1}{2}(p-1)z$.

Значи, егзистенцијата на бројот d со наведените својства повлекува дека $\frac{p-1}{2} \mid n$. Од друга страна, ако ова важи, тогаш постои единствен d за кој се исполнети бараните услови, и тоа

$$d=pz^2=p(\tfrac{n}{z})^2=p(\tfrac{2n}{p-1})^2.$$

Со тоа тврдењето е докажано. ■

2. ОСНОВНА ТЕОРЕМА НА АРИТМЕТИКАТА

2.1. Честопати одделни аритметички задачи можеме едноставно да ги решиме ако даден природен број го разложиме на производ од прости множители. Притоа, се поставува прашањето дали секој природен број може да се претстави како производ од прости броеви. Се докажува дека секој сложен број е производ од прости броеви. За мали броеви тоа лесно се проверува: $4=2\cdot 2, 12=2\cdot 2\cdot 3$ итн. Пред да го докажеме ова тврдење, кое е познато како *основна теорема на аритметиката,* ќе ја докажеме следнава теорема.

2.2. Теорема. Ако p е прост број и $p \mid ab$, тогаш $p \mid a$ или $p \mid b$.

Доказ. Да претпоставиме дека $p \nmid a$. Тогаш a и p се заемно прости броеви. Но, $p \mid ab$, па од теорема I 4.9 а) следува дека $p \mid b$.

Аналогно се докажува дека ако $p \nmid b$, тогаш $p \mid a$. ■

2.3. Теорема (основна теорема на аритметиката). Секој природен број N на единствен начин може да се запише како производ на прости множители (редоследот на множителите не е важен).

Доказ. Најпрво ќе докажеме дека природниот број N може да се запише како производ на прости множители.

Ако N е прост број, тогаш $N = p$ и теоремата е докажана.

Да претпоставиме дека N не е прост број. Тогаш $N = n_1 n_2$. Ако n_1 и n_2 се прости броеви, тогаш доказот е завршен. Ако n_1 или n_2 не е прост број, тогаш постапката ја повторуваме и по конечен број чекори (сложен број е делив само со простите броеви чии квадрати се помали или еднакви на самиот број) го добиваме претставувањето

$$N = p_1 p_2 ... p_n, \tag{1}$$

каде што $p_i, i = 1,2,...,n$ се прости броеви.

Да претпоставиме дека постојат две претставувања:

$$N = p_1 p_2 ... p_n = q_1 q_2 ... q_k,\ n \le k .$$

Тогаш $p_1 \mid q_1 q_2 ... q_k$ и бидејќи два прости броеви се или меѓусебно еднакви или се заемно прости, добиваме дека $p_1 = q_j$ за некој $j = 1,2,...,k$. Повторувајќи ја постапката за $p_2, ..., p_n$ добиваме дека

$$N = p_1 p_2 ... p_n = (p_1 p_2 ... p_n) q_{n+1} ... q_k ,$$

од што следува $q_{n+1} = ... = q_k = 1$, па значи $n = k$ и претставувањето е единствено со точност до редоследот на множителите. ■

2.4. При разложувањето на даден број на прости множители, некои од множителите може повеќекратно да се повторуваат. Ако во разложувањето (1) некои од множителите се еднакви меѓу себе, на пример p_1 се јавува a_1 пати, p_2 се јавува a_2 пати итн., p_k се јавува a_k пати, тогаш за n добиваме

$$n = p_1^{a_1} p_2^{a_2} ... p_k^{a_k} . \tag{2}$$

Ваквиот запис на бројот n го нарекуваме *каноничен запис*.

Да забележиме дека со помош на каноничниот запис можеме да дадеме едноставен критериум кога еден природен број е точен квадрат. Имено, од теорема 2.3 и од својствата на степените, следува дека:

Природниот број n е точен квадрат ако и само ако степеновите показатели a_i, $i = 1,2,...,k$ во каноничниот запис (2) *се парни броеви.*

2.5. Забелешка. Со помош на каноничниот запис на дадени природни броеви n и m лесно се определуваат најголемиот заеднички делител и најмалиот заеднички содржател на n и m. Имено, ако $n = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$ и $m = p_1^{b_1} p_2^{b_2} ... p_k^{b_k}$, $a_i \ge 0$, $b_j \ge 0, i, j \in \{1,2,...,k\}$, тогаш

$(m,n) = p_1^{c_1} p_2^{c_2} ... p_k^{c_k}$, каде што $c_i = \min\{a_i, b_i\}, i = 1,2,...,k$ и

$[m,n]=p_1^{d_1}p_2^{d_2}...p_k^{d_k}$, каде што $d_i=\max\{a_i,b_i\}, i=1,2,...,k$.

2.6. Следнава теорема е последица од каноничниот запис и истата често пати се користи при решавање на задачи.

Теорема. Ако $ab=c^n$, $(a,b)=1$, тогаш $a=a_1^n$ и $b=b_1^n$.

Доказ. Случајот кога еден од броевите a или b е единица е тривијален. Затоа ќе го разгледаме случајот кога $a>1$ и $b>1$. Бидејќи $(a,b)=1$, факторите во каноничното претставување на a и b се различни. Според тоа, имаме

$$a=p_1^{a_1}p_2^{a_2}...p_s^{a_s} \text{ и } b=p_{s+1}^{a_{s+1}}p_{s+2}^{a_{s+2}}...p_{s+r}^{a_{s+r}} ,$$

каде $p_1,p_2,...,p_{s+r}$ се различни прости броеви, $s\geq 1, r\geq 1$. Нека каноничното претставување на бројот *c* е дадено со

$$c=q_1^{b_1}q_2^{b_2}q_3^{b_3}\ldots q_k^{b_k} .$$

Тогаш

$$p_1^{a_1}p_2^{a_2}\ldots p_{s+r}^{a_{s+r}}=q_1^{nb_1}q_2^{nb_2}\ldots q_k^{nb_k} .$$

Според основната теорема на аритметиката, $k=s+r$ и простиот број q_j се совпаѓа со некој прост број p_i , а исто така се совпаѓаат и нивните експоненти. Ако ги пренумерираме простите броеви q_j добиваме

$$q_j=p_j,\ j=1,2,...,s+r \text{ и } a_j=nb_j,\ j=1,2,...,s+r .$$

Конечно, $a=(p_1^{b_1}p_2^{b_2}...p_s^{b_s})^n$ и $b=(p_{s+1}^{b_{s+1}}p_{s+2}^{b_{s+2}}...p_{s+r}^{b_{s+r}})^n$. ■

2.7. Теорема. Нека $m,n\in\mathbb{N}$ и $(m,n)=1$. Ако $d\in\mathbb{N}$ и $d\mid mn$, тогаш постојат единствени природни броеви d_1 и d_2 такви што $d=d_1d_2,\ d_1\mid m,\ d_2\mid n$.

Доказ. Претпоставуваме дека $d\mid mn$. Нека $d_1=(d,m),\ d_2=(d,n)$. Бидејќи $d\mid mn$, имаме $(d,mn)=d$. Но, како $(m,n)=1$ добиваме

$$d=(d,mn)=(d,m)\cdot(d,n)=d_1d_2,\ d_1\mid m,\ d_2\mid n ,$$

т.е. d_1 и d_2 се броеви со бараните својства.

Нека d_1' и d_2' се природни броеви такви што $d=d_1'd_2'$, $d_1'\mid m,\ d_2'\mid n$. Бидејќи $d_1=(d,m),\ d_2=(d,n)$ добиваме $d_1'\leq d_1$ и $d_2'\leq d_2$, па затоа $d=d_1'd_2'\leq d_1d_2=d$, што е можно ако и само ако $d_1=d_1',\ d_2=d_2'$. ■

2.8. Теорема. Ако $x^a=y^b$ за некои природни броеви x,y,ab, тогаш постои природен број z таков што $x=z^m$ и $y=z^n$, каде $b=m\cdot(a,b)$ и $a=n\cdot(a,b)$.

Доказ. Нека $b=m\cdot(a,b)$, $a=n\cdot(a,b)$ и $(m,n)=1$. Имаме $x^{n\cdot(a,b)}=y^{m\cdot(a,b)}$, па затоа $x^n=y^m$. Нека $p_i^{\alpha_i}$ и $p_i^{\beta_i}$ се степените на простиот број p_i во x и y соодветно. Од $x^n=y^m$ следува $p_i^{n\alpha_i}=p_i^{m\beta_i}$, па затоа $n\alpha_i=m\beta_i$, што значи дека за секој i важи $\frac{\alpha_i}{m}=\frac{\beta_i}{n}=r_i$. Сега, ако ставиме $z=\prod p_i^{r_i}$, добиваме

$$x=\prod p_i^{\alpha_i}=\prod p_i^{mr_i}=(\prod p_i^{r_i})^m=z^m \text{ и } y=\prod p_i^{\alpha_i}=\prod p_i^{nr_i}=(\prod p_i^{r_i})^n=z^n. \blacksquare$$

2.9. Пример. За даден $c\in\mathbb{N}$, нека n_0 е најмалиот природен број таков што $2^{n_0}>c$. Докажи дека, тогаш за секој $n\geq n_0$ важи:

$$a^n \mid cb^n \qquad \Rightarrow \qquad a \mid b,$$

каде $a,b\in\mathbb{N}$.

Решение. Нека p е прост број и нека α,β,γ се соодветно најголемите степени со кои p ги дели a,b,c, соодветно. Сега од $a^n \mid cb^n$ следува

$$n\alpha\leq n\beta+\gamma.$$

Од друга страна, бидејќи $p^{n_0}\geq 2^{n_0}>c$, важи $\gamma<n_0\leq n$. Оттука, следува

$$n\alpha<n\beta+n=n(\beta+1),$$

па затоа $\alpha<\beta+1$, т.е. $\alpha\leq\beta$. Конечно, од произволноста на простиот број p следува $a \mid b$. $\blacksquare$

2.10. Пример. Одреди ги сите рационални броеви x, за кои $\sqrt{8x^2-2x-3}$ исто така е рационален број.

Решение. Нека $x=\frac{a}{b}$, каде $a,b\in\mathbb{Z}, b\neq 0$ и $(a,b)=1$. Јасно, $\sqrt{8x^2-2x-3}$ е рационален број ако $8a^2-2ab-3b^2$ е полн квадрат. Имаме,

$$8a^2-2ab-3b^2=(4a-3b)(2a-b) \text{ и } (4a-3b,2a-b)=1,$$

па затоа од теорема 2.6 следува дека $4a-3b=u^2$ и $2a+b=v^2$, т.е. $a=\frac{u^2+3v^2}{10}$ и $b=\frac{2v^2-u^2}{5}$. Според тоа, $x=\frac{u^2+3v^2}{2(v^2-u^2)}$, $u,v\in\mathbb{N}$ и $(u,v)=1$. $\blacksquare$

2.11. Пример. Докажи дека производ на пет последователни природни броеви не може да биде точен квадрат.

Решение. Нека претпоставиме дека $x,x+1,x+2,x+3,x+4$ се последователни природни броеви чиј производ е точен квадрат. Нека $p\geq 5$ е прост број. Прво да забележиме дека најмногу еден од наведените броеви може да е делив со p. Ако

$p\,|\,(x+i)$, $0\le i\le 4$, тогаш од претпоставката следува дека најголемиот степен на кој p е делител на $x+i$ е парен. Последното значи дека секој од петте разгледувани броеви мора да биде од видот $2^{\alpha}3^{\beta}t_0^2$, за некој $t_0\in\mathbb{N}$. Сега, секој број од видот $2^{\alpha}3^{\beta}t_0^2$ може да се запише во видот $2^{\alpha_1}3^{\beta_1}t_1^2$, каде α_1,β_1 се непарни или 0, па затоа секој од петте броја може да биде прикажан во еден од следниве облици $t^2,2t^2,3t^2,6t^2$ за соодветен број $t\in\mathbb{N}$. Од принципот на Дирихле следува дека два од овие пет броја може да се прикажат како au^2 и av^2 за некои различни $u,v\in\mathbb{N}$ и некој фиксен $a\in\{1,2,3,6\}$. Ако, на пример, $u>v$, тогаш

$$au^2-av^2=a(u^2-v^2)\le(x+4)-x=4\text{, т.е. } u^2-v^2\le\tfrac{4}{a}.$$

Последното е можно само ако $a=1,u=2,v=1$, па затоа 1 и 4 се меѓу разгледуваните броеви, т.е. станува збор за броевите 1, 2, 3, 4, 5. Но, $1\cdot2\cdot3\cdot4\cdot5=120$ не е точен квадрат. Конечно, од добиената противречност следува тврдењето на задачата. ■

2.12. Пример. Нека $a_1,\ldots,a_k,b_1,\ldots,b_k$ се природни броеви такви што $(a_i,b_i)=1$ за секој $i\in\{1,2,\ldots,k\}$. Нека m е најмалиот заеднички содржател на броевите $b_1,\ldots,b_k$, а $c_i=a_i\frac{m}{b_i}$, за $i\in\{1,2,\ldots,k\}$. Докажи дека

$$(a_1,\ldots,a_k)=(c_1,\ldots,c_k).$$

Решение. Нека p е прост број кој е делител на барем еден од броевите $a_1,\ldots,a_k,b_1,\ldots,b_k$. Нека α_i и β_i се соодветно највисоките степени на p кои ги делат a_i и b_i. Тогаш највисокиот степен на кој p го дели m е еднаков на $\mu=\max\limits_j\beta_j$, додека највисокиот степен на p кој го дели c_i е еднаков на $\gamma_i=\alpha_i+\mu-\beta_i$. Ако се земе е предвид дека p е произволен прост фактор, тврдењето на задачата е еквивалентно со равенството

$$\min_i\alpha_i=\min_i(\alpha_i+\mu-\beta_i)=\mu+\min_i(\alpha_i-\beta_i). \tag{3}$$

Притоа, заради $(a_i,b_i)=1$ важи $\alpha_i\ne0\Rightarrow\beta_i=0$.

Заради пократок запис дефинираме $\delta_i=\alpha_i-\beta_i$. Сега, од воочениот однос на експонентите α_i и β_i следува

$$\delta_i=\begin{cases}-\beta_i, & \text{ако } \alpha_i=0\\ \alpha_i, & \text{ако } \alpha_i\ne0.\end{cases}$$

Разликуваме два случаја. Ако постои индекс i_0 таков што $\alpha_{i_0}=0$, тогаш $\min\limits_i\alpha_i=0$. Од друга страна, $\min\limits_i\delta_i=-\max\limits_i\beta_i=-\mu$, па тогаш и десната страна во

(3) има вредност 0. Во спротивно, $\alpha_i > 0$ за $i \in \{1,2,...,k\}$. Но, тогаш $\beta_i = 0$ за $i \in \{1,2,...,k\}$, па е $\mu = 0$ и $\delta_i = \alpha_i$ за $i \in \{1,2,...,k\}$. Последното значи дека равенството (3) е точно и во овој случај, со што задачата е решена. ■

2.13. Пример. Нека $a,b,c \in \mathbb{N}$. Докажи дека

$$[(a,b),(b,c),(c,a)] = ([a,b],[b,c],[c,a]), \tag{4}$$

$$[a,(b,c)] = ([a,b],[a,c]). \tag{5}$$

Решение. Нека $p_1, p_2, ..., p_n$ се сите прости броеви кои учествуваат во каноничните разложувања на a,b,c. Тогаш

$$a = p_1^{a_1} p_2^{a_2} ... p_n^{a_n},\ b = p_1^{b_1} p_2^{b_2} ... p_n^{b_n} \text{ и } c = p_1^{c_1} p_2^{c_2} ... p_n^{c_n},$$

каде $a_i \geq 0, b_i \geq 0, c_i \geq 0$, за $i = 1,2,...,n$. Од забелешка 2.7 следува дека

$$[(a,b),(b,c),(c,a)] = \prod_{i=1}^{n} p_i^{\max\{\min\{a_i,b_i\},\min\{b_i,c_i\},\min\{c,a_i\}\}}$$

$$([a,b],[b,c],[c,a]) = \prod_{i=1}^{n} p_i^{\min\{\max\{a_i,b_i\},\max\{b_i,c_i\},\max\{c,a_i\}\}}.$$

Сега равенството (4) следува од претходните две равенства и фактот дека за секои три броја k,l,m важи

$$\max\{\min\{k,l\},\min\{l,m\},\min\{m,k\}\} = \min\{\max\{k,l\},\max\{l,m\},\max\{m,k\}\},$$

кое лесно се докажува. Равенството (5) се докажува аналогно. Деталите ги оставаме на читателот за вежба. ■

3. ФЕРМАТОВИ И МЕРСЕНОВИ БРОЕВИ

3.1. Многу математичари безуспешно се обидувале да најдат општа формула која ќе генерира само прости броеви, т.е. функција $f(n)$ чии вредности, за сите природни броеви n, ќе бидат прости броеви. Во овој дел интересно е да ја спомнеме неточната хипотеза на Ферма. Тој ги проучувал броевите од видот $f_n = 2^{2^n} + 1$, каде n е природен број. Овие броеви, во негова чест, се наречени *Фрматови броеви*. За првите пет вредности на бројот n, Ферма ги добил броевите $f_0 = 3$, $f_1 = 5$, $f_2 = 17$, $f_3 = 257$, $f_4 = 65537$ и со проверка утврдил дека тие се прости броеви. Ферма ја искажал хипотезата дека и за секој природен број $n \geq 5$, бројот f_n е прост. Меѓутоа, Ојлер докажал дека бројот f_5 е производ на два прости броја, т.е. дека

$$f_5 = 2^{32}+1 = 2^{28}(5^4+2^4)-(5\cdot 2^7)^4+1 = 2^{28}\cdot 641-(640^4-1)$$
$$= 641(2^{28}-639(640^2+1)) = 641\cdot 6700417 = 4294967297.$$

Да споменеме дека до денес не е најден ниту еден прост Ферматов број поголем од f_4. Затоа се добило впечаток дека Ферматовите броеви не се од посебен интерес, но се покажало тие имаат низа интересни својства, без разлика дали се прости или сложени. Во следната теорема ќе дадеме едно такво својство.

3.2. Теорема. Ако $m \neq n$, тогаш Ферматовите броеви f_m и f_n се заемно прости.

Доказ. Нека се f_n и f_{n+k}, $k>0$, два различни Ферматови броја и нека претпоставиме дека m е природен број, таков да $m \mid f_n$ и $m \mid f_{n+k}$. Земаме $x = 2^{2^n}$ и добиваме

$$\frac{f_{n+k}-2}{f_n} = \frac{2^{2^{n+k}}+1-2}{2^{2^n}+1} = \frac{2^{2^n 2^k}-1}{2^{2^n}+1} = \frac{(2^{2^n})^{2^k}-1}{2^{2^n}+1} = \frac{x^{2^k}-1}{x+1} = x^{2^k-1}-x^{2^k-2}+\ldots-1,$$

што значи дека $f_n \mid (f_{n+k}-2)$, па од $m \mid f_n$ следува дека $m \mid (f_{n+k}-2)$. Но, од $m \mid f_{n+k}$ и $m \mid (f_{n+k}-2)$ следува дека $m \mid 2$ и како Ферматовите броеви се непарни добиваме дека $m=1$, што значи дека броевите f_n и f_{n+k}, $k>0$ се заемно прости. ■

3.3. Прашање дали Ферматовиот број е прост или сложен е тесно поврзано со проблемот за конструкција на правилен многуаголник само со помош на шестар и линијар. Имено, Гаус ја докажал следнава теорема, чиј доказ нема да го презентираме бидејќи излегува надвор од рамките на нашите разгледувања.

Теорема. Правилен n-аголник може да се конструира со линијар и шестар ако и само ако $n = 2^s p_1 p_2 \ldots p_k$, $k>0$, каде $s \in \mathbb{N}_0$, а $p_1, p_2, \ldots, p_k$ се различни Ферматови прости броеви или $n = 2^s$, каде $s \in \mathbb{N}\setminus\{1\}$. ■

3.4. Интересно е дека Ферматовите броеви можат да се искористат и за докажување на бесконечноста на множеството прости броеви. Во таа насока ќе дадеме уште еден доказ на ова тврдење.

Доказ на теорема 1.12. Според теорема 3.2 Ферматовите броеви се по парови заемно прости, па затоа секој Ферматов број е делив со некој непарен прост број кој не е делител на ниту еден друг Ферматов број. Но, Ферматови броеви има бесконечно многу, па оттука следува дека и прости броеви има бесконечно многу. ■

3.5. Нека претпоставиме дека бројот n не е степен на бројот 2 и да го разгледаме бројот 2^n+1. Можни се два случаја: n е прост број или n е сложен,

односно $n=2^s r$, каде r е непарен број поголем од 1. Во вториот случај, ако $s>1$, тогаш r е непарен број поголем од 1, а ако $s=0$, тогаш r е непарен сложен број.

Ако $n\geq 5$ е прост број, тогаш $n=6k\pm 1, k\in\mathbb{N}$, па затоа

$$2^n+1=2^{6k+1}+1=(2+1)(2^{6k}-2^{6k-1}+\ldots-2+1), \text{ т.е. } 3\,|\,(2^n+1)$$

или

$$2^n+1=2^{6k-1}+1=(2+1)(2^{6k-2}-2^{6k-3}+\ldots-2+1), \text{ т.е. } 3\,|\,(2^n+1),$$

што значи дека и во двата случаја 2^n+1 е сложен број.

Ако $n=2^s r$, каде r е непарен број поголем од 1, тогаш

$$2^n+1=2^{2^s r}+1=(2^{2^s})^r+1=(2^{2^s}+1)[(2^{2^s})^{r-1}-(2^{2^s})^{r-2}+\ldots-2^{2^s}+1]$$

т.е. $(2^{2^s}+1)\,|\,(2^n+1)$, што значи дека 2^n+1 е сложен број. Со тоа ја докажавме следнава теорема.

Теорема. Ако природниот број $n>1$ не е степен на бројот 2, тогаш 2^n+1 е сложен број. ■

3.6. Последица. Бројот 2^n+1, $n\in\mathbb{N}$ е прост само ако е Ферматов број.

Доказ. Непосредно следува од теорема 3.5. ■

3.7. Покрај Ферматовите броеви, забележително внимание кај математичарите предизвикале и таканаречените Мерсенови броеви, а тоа се броевите од видот $M_n=2^n-1$, $n\in\mathbb{N}$. За Мерсеновите броеви точна е следнава теорема.

Теорема. Ако n е природен број и 2^n-1 е прост број, тогаш и n е прост број.

Доказ. Ќе го докажеме еквивалентното тврдење, т.е. ќе го докажеме тврдењето: ако n е сложен број, тогаш и 2^n-1 е сложен број.

Нека $n=mk$, каде $m,k>1$. Тогаш

$$2^n-1=2^{mk}-1=(2^m)^k-1=(2^m-1)[(2^m)^{k-1}+(2^m)^{k-2}+\ldots+2^m+1],$$

т.е. $(2^m-1)\,|\,(2^n-1)$, што значи дека 2^n-1 е сложен број. ■

3.8. Според претходната теорема, бројот од облик 2^n-1 не може да биде прост ако n не е прост број. Пишуваме $M_p=2^p-1$, при што подразбираме дека p е прост број. Броевите M_p, ги нарекуваме *Мерсенови прости броеви*. Ферматовите и Мерсеновите прости броеви се од посебно значење, бидејќи истите наоѓаат примена во многу други математички дисциплини.

Во воведот на својата книга *Cogitata physico mathematica* од 1644 година Мерсен изнел посебно интересно тврдење за Мерсеновите прости броеви. Тој тврдел

дека M_p е прост број за $p = 2,3,5,7,13,17,19,31,67,127,257$ и дека M_p е сложен за сите останати прости броеви $p < 257$. Тврдењето на Мерсен предизвикало голем интерес од причина што наведените броеви се толку големи што што неколку стотина години никој не можел ниту да го потврди ниту да го негира неговото тврдење. На тогашните математичари им било јасно дека Мерсен не можел да го провери тврдењето за сите наведени броеви, но тоа не можеле и другите да го направат. Во 1772 година Ојлер докажал дека бројот M_{31} е прост, а Лукас во 1876 година докажал дека и бројот M_{127} е прост. Американскиот математичар Кол во 1903 година докажал дека

$$2^{67} - 1 = 193707721 \cdot 761838257287,$$

што значи дека бројот M_{67} не е прост. До 1947 година се тестирани сите Мерсенови броеви M_n за $n \le 257$ и се покажало дека Мерсен направил пет грешки: погрешно заклучил дека M_{67} и M_{257} се прости и дека M_{61}, M_{89} и M_{107} се сложени.

До денес не е докажана, ниту е негирана хипотезата дека постојат бесконечно многу Мерсенови прости броеви. Во следната теорема ќе дадеме критериум за проверка дали еден Мерсенов број е прост или не е прост број. Овој критериум е познат како Лукас-Лемеров тест и доказот на истиот нема да го презентираме, бидејќи далеку ги надминува рамките на нашите разгледувања.

Теорема. Дефинираме низа природни броеви $\{s_n\}$ со $s_1 = 4$ и $s_{n+1} = s_n^2 - 2$. Нека p е непарен прост број. Мерсеновиот број M_n е прост ако и само ако M_n е делител на s_{n-1}. □

Наоѓањето на што е можно поголем прост број денес се сведува на наоѓање на што е можно поголем Мерсенов прост број. Триесет и осмиот Мерсенов прост број $2^{6972593} - 1$ е откриен во 1999 година и тоа бил првиот откриен прост број со повеќе од 1000000 цифри. Во неговиот декаден запис има 2098960 цифри. Во 2001 година е откриен Мерсеновиот прост број $2^{13466917} - 1$ кој има 4053946 цифри, во 2003 година е откриен Мерсеновиот прост број $2^{20996011} - 1$ во чиј декаден запис има 6320430 цифри, а во 2006 година е откриен Мерсеновиот прост број $2^{32582657} - 1$ кој има 9808358 цифри.

3.9. Пример. Докажи дека за Ферматовите броеви важи $f_n \mid (2^{f_n} - 2)$.

Решение. Ако го искористиме познатото неравенство $2^n \ge n + 1$, за секој $n \in \mathbb{N}$, добиваме дека $2^{n+1} \mid 2^{2^n}$, од што следува дека $(2^{2^{n+1}} - 1) \mid (2^{2^{2^n}} - 1)$. Но, $(2^{2^n} + 1) \mid (2^{2^{n+1}} - 1)$, па затоа $(2^{2^n} + 1) \mid (2^{2^{2^n}} - 1)$, што значи

$(2^{2^n}+1) \mid 2(2^{2^n}-1) = 2^{2^{2^n}+1}-2$, т.е. $f_n \mid (2^{f_n}-2)$. ■

3.10. Пример. Докажи дека ниту еден од Ферматовите броеви

$$f_n = 2^{2^n}+1, n = 2,3,...$$

не може да се запише како збир на два прости броја.

Решение. Броевите $f_n, n = 2,3,...$ се непарни. Затоа, ако бројот f_n може да се запише како збир на два прости броја, тогаш едниот од нив мора да е парен, т.е. бројот 2, па другиот е бројот $f_n - 2$. Но, ако $n > 1$ тогаш

$$f_n - 2 = 2^{2^n} - 1 = (2^{2^{n-1}} - 1)(2^{2^{n-1}} + 1)$$

не е прост број. ■

3.11. Пример. Докажи дека Ферматовиот прост број $p = 2^{2^n}+1$, $n \in \mathbb{N}$ не може да биде запишан како разлика на петти степени на два природни броја.

Решение. Нека

$$p = a^5 - b^5 = (a-b)(a^4 + a^3b + a^2b^2 + ab^3 + b^4),\ a,b \in \mathbb{N}.$$

Бидејќи p е прост број $a-b=1$, т.е. $a = b+1$, $b \in \mathbb{N}$. Сега

$$a^5 - b^5 = (b+1)^5 - b^5 = 5b^5 + 10b^3 + 10b^2 + 5b + 1,$$

па затоа $5b^5 + 10b^3 + 10b^2 + 5b = 2^{2^n}$, што не е можно, бидејќи левата страна на последното равенство е делива со 5, а десната не е делива со 5. ■

3.12. Преимер. Нека $f_i, i = 2,3,...,1985$ се Ферматови броеви. Најди ја цифрата на единиците во декадниот запис на бројот $[f_2, f_3, ..., f_{1985}]$.

Решение. Од теорема 3.2 имаме $(f_m, f_n) = 1$, за $m \neq n$, па затоа

$$[f_2, f_3, ..., f_{1985}] = f_2 f_3 \cdots f_{1985}.$$

Понатаму,

$$\begin{aligned} f_n = 2^{2^n}+1 &= (2^{2^n}-1)+2 \\ &= [(2^4)^{2^{n-2}} - 1] + 2 = (2^4 - 1)a_n + 2 \\ &= (2^2+1)(2^2-1)a_n + 2 = 5q_n + 2, \end{aligned}$$

за секој $n \geq 2$. Според тоа,

$$\begin{aligned} [f_2, f_3, ..., f_{1985}] &= f_2 f_3 \cdots f_{1985} \\ &= (5q_2+2)(5q_3+2)...(5q_{1985}+2) \\ &= 5b + 2^{1984} = 5b + 4^{992} \\ &= 5b + (5-1)^{992} = 5m+1. \end{aligned}$$

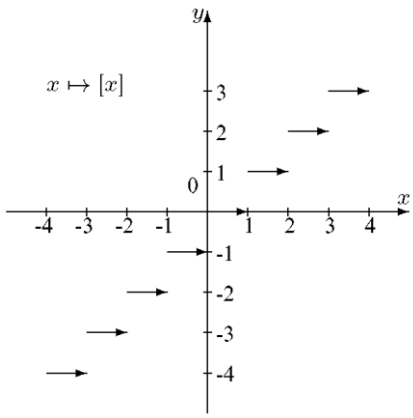
Притоа, бидејќи секој од броевите $f_i, i = 2,3,...,1985$ е непарен, добиваме дека $[f_2, f_3, ..., f_{1985}]$ е непарен број, што значи дека m е парен број, т.е. $m = 2p$. Ко-

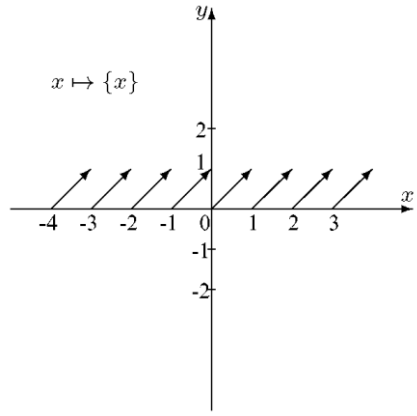
нечно, од $[f_2, f_3, ..., f_{1985}] = 10p+1$ следува дека цифрата на единиците на бројот $[f_2, f_3, ..., f_{1985}]$ е 1. ■

4. ФУНКЦИИТЕ $[x]$ И $\{x\}$

4.1. Дефиниција. Функцијата $[\cdot]: \mathbb{R} \to \mathbb{Z}$ определена со: ако x е меѓу последователните цели броеви k и $k+1$, т.е. $k \le x < k+1$, тогаш $[x] = k$ ја нарекуваме *цел дел од* x.

4.2. Дефиниција. Функцијата $\{\cdot\}: \mathbb{R} \to [0,1)$ определена со $\{x\} = x - [x]$ ја нарекуваме *дробен дел од* x.





4.3. Теорема. Нека x и y се реални броеви. Тогаш

а) $[x] \le x < [x]+1$, $x-1 < [x] \le x$, $0 \le x-[x] < 1$

б) $[x]+[-x] = \begin{cases} 0, & \text{ако } x \text{ е цел број,} \\ -1, & \text{ако } x \text{ не е цел број.} \end{cases}$

в) $[x+m] = [x]+m$, ако m е цел број.

г) $[x]+[y] \le [x+y] \le [x]+[y]+1$.

д) $[x-y] \le [x]-[y] \le [x-y]+1$.

ѓ) $[x][y] \le [xy] \le [x][y]+[x]+[y]$, ако $x, y \ge 0$.

е) $[\frac{[x]}{m}] = [\frac{x}{m}]$, ако m е природен број.

ж) $[\sqrt{[x]}] = [\sqrt{x}]$, ако $x \ge 0$.

Доказ. а) Секој дел од тврдењето следува од дефиниција 7.1.

б) Ако x е цел број, тогаш $[-x] = -[x]$. Ако x не е цел број, тогаш од $[-x] = y$ следува $-y-1 < x < -y$ или $[x] = -y-1$ и $[-x] = -[x]-1$.

в) Од а) следува дека

$$x+m-1<[x+m]\le x+m \text{ и } x+m-1<[x]+m\le x+m.$$

Бидејќи $[x+m]$ и $[x]+m$ се цели броеви, од претходните две неравенства следува $[x+m]=[x]+m$.

г) Нека $x=n+\alpha$, $y=m+\beta$, каде $m,n\in\mathbb{Z}$ и $0\le\alpha,\beta<1$. Тогаш

$$[x]+[y]=m+n\le[n+\alpha+m+\beta]=[x+y]$$
$$=m+n+[\alpha+\beta]\le n+m+1=[x]+[y]+1.$$

д) Според г) имаме $[x-y]+[y]\le[(x-y)+y]\le[x-y]+[y]+1$, т.е.

$$[x-y]\le[x]-[y]\le[x-y]+1.$$

ѓ) Според а) имаме $[x][y]\le xy<([x]+1)([y]+1)$. Значи,

$$[x][y]\le[xy]\le([x]+1)([y]+1)-1=[x][y]+[x]+[y].$$

е) Нека $x=n+\alpha,\ n=qm+r,\ 0\le\alpha<1,\ 0\le r<m-1$. Имаме

$$[\tfrac{x}{m}]=[\tfrac{qm+r+\alpha}{m}]=q+[\tfrac{r+\alpha}{m}]=q.$$

Од друга страна, бидејќи $0\le r+\alpha<m$ добиваме

$$[\tfrac{[x]}{m}]=[\tfrac{n}{m}]=[q+\tfrac{r}{m}]=q.$$

Конечно, од (1) и (2) следува $[\tfrac{[x]}{m}]=[\tfrac{x}{m}]$.

ж) Бидејќи $x\ge0$, x може да се запише во облик

$$x=n^2+r+\{x\}$$

каде n и r се ненегативни цели броеви, $0\le r\le2n$. Тогаш,

$$[\sqrt{[x]}]=[\sqrt{n^2+r}]=[\sqrt{n^2+r}-n+n]=n+[\sqrt{n^2+r}-n]=n+[\tfrac{r}{\sqrt{n^2+r}+n}]=n.$$

Слично,

$$[\sqrt{x}]=[\sqrt{n^2+r+\{x\}}-n+n]=n+[\sqrt{n^2+r+\{x\}}-n]=n+[\tfrac{r+\{x\}}{\sqrt{n^2+r+\{x\}}+n}]=n$$

бидејќи $0\le r+\{x\}<2n+1<\sqrt{n^2+r+\{x\}}+n$. Значи, $[\sqrt{[x]}]=[\sqrt{x}]$. ■

4.4. Лема. За секој $x\in\mathbb{R}$ важи

$$[x+\tfrac{1}{2}]=[2x]-[x]. \qquad (1)$$

Доказ. Секој реален број x може да се запише во облик $x=k+\alpha$ или $x=k+\frac{1}{2}+\alpha$ каде што $k\in\mathbb{Z}$ и $0\le\alpha<\frac{1}{2}$.

Ако $x=k+\alpha$, тогаш

$$[k+\alpha+\tfrac{1}{2}]=k;\ [2k+2\alpha]=2k;\ [k+\alpha]=k,$$

па затоа точно е равенството (1).

Ако $x=k+\alpha+\frac{1}{2}$, тогаш

$$[k+\alpha+\tfrac{1}{2}+\tfrac{1}{2}]=k+1;\ [2k+2\alpha+1]=2k+1;\ [k+\alpha+\tfrac{1}{2}]=k,$$

па затоа точно е равенството (1). ■

4.5. Лема. Ако $n\in\mathbb{N}$ и $x\geq 0$, тогаш постојат точно $[\frac{x}{n}]$ природни броеви помали или еднакви на x деливи со n.

Доказ. Броеви деливи со n се: $n, 2n, 3n, \ldots$.

Нека има j природни броеви помали или еднакви на x деливи со n. Тогаш

$$jn\leq x<(j+1)n\text{, т.е. } j\leq\tfrac{x}{n}<j+1.$$

Според тоа, $j\leq[\frac{x}{n}]<j+1$, односно $[\frac{x}{n}]=j$. ■

4.6. Теорема (Лежандр). Нека p е прост број, n е природен број и a е најголемиот степен на бројот p таков што $p^a\mid n!$, т.е. $p^a\parallel n!$. Тогаш,

$$a=[\tfrac{n}{p}]+[\tfrac{n}{p^2}]+\ldots+[\tfrac{n}{p^k}]+\ldots \qquad (2)$$

Доказ. Според лема 4.5 во низата $1,2,\ldots,n$ има $[\frac{n}{p}]$ броеви деливи со p, па затоа

$$n!=p\cdot 2p\cdot\ldots\cdot[\tfrac{n}{p}]pM_1=p^{[\frac{n}{p}]}\cdot[\tfrac{n}{p}]!\cdot M_1$$

и M_1 е природен број кој не е делив со p.

Ако претходното размислување го примениме на низата $1,2,\ldots,[\frac{n}{p}]$ и ако земеме во предвид дека $[\frac{[n/p]}{p}]=[\frac{n}{p^2}]$, добиваме дека

$$n!=p^{[n/p]+[n/p^2]}\cdot[\tfrac{n}{p^2}]!\cdot M_2$$

и M_2 е природен број кој не е делив со p.

Продолжувајќи ја постапката добиваме дека

$$n!=Mp^{[n/p]+[n/p^2]+[n/p^3]+\ldots}$$

каде M е природен број кој не е делив со p, т.е. точно е равенството (2). ■

4.7. Забелешка. Постапката во претходниот доказ ќе заврши по конечен број чекори, бидејќи постои $k_0\in\mathbb{N}$ таков што $\frac{n}{p^{k_0}}<1$, па затоа $[\frac{n}{p^k}]=0$ за $k\geq k_0$.

4.8. Лема. Ако $a,b\in\mathbb{R}^+$. Тогаш $[2a]+[2b]\geq[a]+[b]+[a+b]$

Доказ. Нека $a=[a]+\alpha$ и $b=[b]+\beta$, каде што $0\leq\alpha<1$ и $0\leq\beta<1$.

Ако $\alpha+\beta<1$, тогаш

$$[a+b]=[a]+[b]$$

и затоа

$$[2a]+[2b]\geq 2[a]+2[b]=[a]+[b]+[a+b]$$

Ако $\alpha+\beta\geq 1$, тогаш $2\alpha\geq 1$ или $2\beta\geq 1$. Нека $2\alpha\geq 1$. Тогаш

$$[a+b]=[a]+[b]+1 \text{ и } [2a]=2[a]+1,$$

па затоа

$$[2a]+[2b]\geq 2[a]+1+2[b]=[a]+[b]+[a+b]. \blacksquare$$

4.9. Лема (равенство на Ермит). Ако $x\in\mathbb{R}$ и $n\in\mathbb{N}$, тогаш

$$[x]+[x+\tfrac{1}{n}]+[x+\tfrac{2}{n}]+...+[x+\tfrac{n-1}{n}]=[nx].$$

Доказ. Бидејќи

$$[x]+[x+\tfrac{1}{n}]+...+[x+\tfrac{n-1}{n}]=n[x]+[\{x\}]+[\{x\}+\tfrac{1}{n}]+...+[\{x\}+\tfrac{n-1}{n}]$$

и $[nx]=n[x]+[n\{x\}]$, доволно е даденото неравенство да го докажеме кога x е реален број од интервалот $[0,1)$.

Нека $x\in[0,1)$ и $k\in\{0,1,2,...,n-1\}$ е таков што $\frac{k}{n}\leq x<\frac{k+1}{n}$. Тогаш од

$$x+\tfrac{n-k-1}{n}<\tfrac{k+1}{n}+\tfrac{n-k-1}{n}=1$$

следува

$$[x]=[x+\tfrac{1}{n}]=[x+\tfrac{2}{n}]=...=[x+\tfrac{n-k-1}{n}]=0,$$

а од

$$x+\tfrac{n-k}{n}\geq\tfrac{k}{n}+\tfrac{n-k}{n}=1 \text{ и } x+\tfrac{n-1}{n}<\tfrac{k+1}{n}+\tfrac{n-1}{n}\leq\tfrac{n}{n}+\tfrac{n-1}{n}<2$$

следува

$$[x+\tfrac{n-k}{n}]=[x+\tfrac{n-k+1}{n}]=...=[x+\tfrac{n-1}{n}]=1.$$

Според тоа,

$$[x]+[x+\tfrac{1}{n}]+...+[x+\tfrac{n-k-1}{n}]+[x+\tfrac{n-k}{n}]+[x+\tfrac{n-k+1}{n}]+...+[x+\tfrac{n-1}{n}]=$$
$$=\underbrace{0+0+...+0}_{n-k \text{ пати}}+\underbrace{1+1+...+1}_{k \text{ пати}}=k=[nx]. \blacksquare$$

4.10. На крајот од овој параграф ќе докажеме едно тврдење кое има значителна примена при пресметување на некои релации поврзани со функцијата цел дел.

Теорема. Нека p и q се заемно прости броеви. Ако функцијата $f:\mathbb{Z}^+\to\mathbb{R}$ е таква што

1) $\frac{f(k)}{p}$ не е цел број, за $k=1,2,...,p-1$,

2) $f(k)+f(p-k)$ е цел број делив со p за $k=1,2,...,p-1$,

тогаш

$$\sum_{k=1}^{p-1}[f(k)\frac{q}{p}]=\frac{q}{p}\sum_{k=1}^{p-1}f(k)-\frac{p-1}{2}. \tag{3}$$

Доказ. Нека $k\in\{1,2,...,p-1\}$. Од 2) следува дека

$$\frac{qf(k)}{p}+\frac{qf(p-k)}{p}\in\mathbb{Z}, \tag{4}$$

а од 1) дека $\frac{qf(k)}{p}\notin\mathbb{Z}$ и $\frac{qf(p-k)}{p}\notin\mathbb{Z}$. Затоа

$$0<\{\frac{qf(k)}{p}\}+\{\frac{qf(p-k)}{p}\}<2.$$

Но според (4), важи $\{\frac{qf(k)}{p}\}+\{\frac{qf(p-k)}{p}\}\in\mathbb{Z}$, па затоа

$$\{\frac{qf(k)}{p}\}+\{\frac{qf(p-k)}{p}\}=1, \text{ за } k=1,2,...,p-1.$$

Ако ги собереме претходните $p-1$ равенство и поделиме со 2 добиваме

$$\sum_{k=1}^{p-1}\{\frac{q}{p}f(k)\}=\frac{p-1}{2}.$$

Од последното равенство следува равенството

$$\sum_{k=1}^{p-1}\frac{q}{p}f(k)-\sum_{k=1}^{p-1}[\frac{q}{p}f(k)]=\frac{p-1}{2},$$

кое е еквивалентно на равенството (3). ■

4.11. Последица (равенство на Гаус). Ако p и q се заемно прости броеви, тогаш

$$\sum_{k=1}^{p-1}[k\frac{q}{p}]=\frac{(p-1)(q-1)}{2}.$$

Доказ. Функцијата $f(x)=x$ ги задоволува условите 1) и 2) од теорема 4.10, па затоа

$$\sum_{k=1}^{p-1}[k\frac{q}{p}]=\frac{q}{p}\sum_{k=1}^{p-1}k-\frac{p-1}{2}=\frac{q}{p}\cdot\frac{p(p-1)}{2}-\frac{p-1}{2}=\frac{(p-1)(q-1)}{2}. \blacksquare$$

4.12. Последица. Ако p е непарен прост број, тогаш

$$\sum_{k=1}^{p-1}[\frac{k^3}{p}]=\frac{(p-2)(p-1)(p+1)}{4}. \tag{5}$$

Доказ. Фукцијата $f(x)=x^3$ ги задоволува условите од теорема 4.10, па затоа за секој природен број q кој не е делив со p важи

$$\sum_{k=1}^{p-1}[\frac{q}{p}k^3]=\frac{q}{p}\sum_{k=1}^{p-1}k^3-\frac{p-1}{2}=\frac{q}{p}\cdot\frac{(p-1)^2p^2}{4}-\frac{p-1}{2}=\frac{(p-1)(p^2q-pq-2)}{4}.$$

Ако во последното равенство земеме $q=1$, го добиваме равенството (5). ■

4.13. Пример. Ако природниот број $A>3$ не е точен квадрат, тогаш постои природен број n таков што $A=[n+\sqrt{n}+\frac{1}{2}]$. Докажи!

Решение. Нека претпоставиме дека бројот A_0 не може да се прикаже во саканиот облик. Тоа значи дека интервалот $[A_0, A_0+1)$ не содржи ниту еден член од низата $n+\sqrt{n}+\frac{1}{2}$. Значи, постои $n_0\in\mathbb{N}$ таков што

$$n_0+\sqrt{n_0}+\tfrac{1}{2}<A_0 \text{ и } A_0+1\le n_0+1+\sqrt{n_0+1}+\tfrac{1}{2}.$$

Од последните две неравенства последователно следува

$$\sqrt{n_0}<A_0-n_0-\tfrac{1}{2}\le\sqrt{n_0+1},$$
$$n_0<(A_0-n_0)^2-(A_0-n_0)+\tfrac{1}{4}\le n_0+1,$$
$$A_0<(A_0-n_0)^2+\tfrac{1}{4}\le A_0+1.$$

Но, броевите A_0 и n_0 се природни, па од последните неравенства следува дека $A_0=(A_0-n_0)^2$. Значи, A_0 е квадрат на природен број, со што тврдењето на задачата е докажано. ■

4.14. Пример. Нека $n>1$. Докажи дека полиномот

$$p_n(x)=\sum_{k=0}^{n}\frac{x^k}{k!}$$

нема рационални нули.

Решение. Нека претпоставиме дека $\alpha=\frac{q}{r}$, $(q,r)=1$, е рационална нула на полиномот $p_n(x)$. Тогаш

$$\sum_{k=0}^{n}\frac{n!}{k!}(\frac{q}{r})^k=n!\,p_n(\alpha)=0,$$

па ако помножиме со r^n добиваме

$$q^n+r\sum_{k=0}^{n-1}\frac{n!}{k!}q^kr^{n-1-k}=0.$$

Значи, $r\mid q^n$ и како $(q,r)=1$ добиваме $r=1$. Значи, горното равенство го добива обликот

$$q^n+\sum_{k=0}^{n-1}\frac{n!}{k!}q^k=0. \qquad (6)$$

Бидејќи за $0 \le k \le n-1$ бројот $\frac{n!}{k!}$ е делив со n, па заклучуваме дека $n \mid q^n$. Последното значи дека за произволен прост множител p на бројот n имаме $p \mid q^n$, од каде што следува дека $p \mid q$.

Сега, нека m е највисокиот степен со кој p го дели $n!$. Бидејќи $p^k \mid q^k$, добиваме дека $p^{m+k} \mid n!q^k$ за секој $k \in \{1,2,...,n-1\}$. Од друга страна, според формулата на Лежандр (2) степенот со кој p го дели $k!$ е еднаков на

$$[\frac{k}{p}]+[\frac{k}{p^2}]+...+[\frac{k}{p^s}] \le \sum_{i=1}^{s} \frac{k}{p^i} \le \sum_{i=1}^{s} \frac{k}{2^i} < k .$$

Затоа $p^k \nmid k!$, т.е. степенот со кој p го дели $k!$ не е поголем од $k-1$. Затоа

$$p^{m+1} \mid \frac{n!}{k!} q^k ,$$

каде $1 \le k \le n$. Со разгледување на членот во (6) кој соодветствува на $k=0$ заклучуваме дека $p^{m+1} \mid n!$, што противречи на изборот на m. Конечно, од добиената противречност следува дека разгледуваниот полином нема рационални нули. ■

4.15. Пример. Нека $f(m)$ е најголемиот цел број k за кој $2^k \mid m!$. Докажи дека за секој природен број n постојат бесконечно многу природни броеви m такви што $m - f(m) = n$.

Решение. Според теоремата на Лежандр имаме $f(m) = \sum_{k \ge 1} [\frac{m}{2^k}]$. Понатаму, ако $\overline{a_r a_{r-1} ... a_1 a_0}$ е бинарниот запис на бројот m, т.е.

$$m = a_r 2^r + a_{r-1} 2^{r-1} + ... + a_1 2^1 + a_0,$$

тогаш за $1 \le k \le r$ важи

$$[\frac{m}{2^k}] = a_r 2^{r-k} + a_{r-1} 2^{r-k-1} + ... + a_{k+1} 2^1 + a_k = \overline{a_r a_{r-1} ... a_{k+1} a_k}$$

(за $k > r$ разгледуваниот цел дел е 0). Значи,

$$f(m) = \sum_{k=1}^{r} \sum_{i=k}^{r} a_i 2^{i-k} = \sum_{i=1}^{r} \sum_{k=1}^{i} a_i 2^{i-k} = \sum_{i=1}^{r} 2^i a_i \sum_{k=1}^{i} 2^{-k} = \sum_{i=1}^{r} 2^i a_i - \sum_{i=1}^{r} a_i .$$

Затоа

$$m - f(m) = a_r + a_{r-1} + ... + a_1 + a_0 .$$

Според тоа, $m - f(m) = n$ ако и само ако m во бинарниот запис има точно n единици. Такви броеви очигледно има бесконечно многу. ■

4.16. Пример. Нека n и p се природни броеви такви што $p > 2^n$. Докажи де-

ка целиот дел на бројот $\sum_{k=0}^{n} \sqrt[p]{1+\binom{n}{k}}$ е еднаков на $n+1$.

Решение. Доволно е да докажеме дека

$$n+1 \le \sum_{k=0}^{n} \sqrt[p]{1+\binom{n}{k}} < n+2 . \tag{7}$$

Левото неравенство во (1) е очигледно, бидејќи $\sqrt[p]{1+\binom{n}{k}} > 1$ за $k = 0,1,...,n$. За да го докажеме десното неравенство, ќе го користиме неравенството на Бернули. Имаме:

$$(1+\tfrac{1}{p}\binom{n}{k})^p \ge 1+p\cdot\tfrac{1}{p}\binom{n}{k} = 1+\binom{n}{k}, \text{ за } k = 0,1,...,n,$$

па затоа

$$1+\tfrac{1}{p}\binom{n}{k} \ge \sqrt[p]{1+\binom{n}{k}}, \text{ за } k = 0,1,...,n.$$

Ако ги собереме претходните неравенства и искористиме дека $p > 2^n$ добиваме

$$\sum_{k=0}^{n} \sqrt[p]{1+\binom{n}{k}} \le n+1+\tfrac{1}{p}\sum_{k=0}^{n}\binom{n}{k} = n+1+\tfrac{2^n}{p} < n+2 . \blacksquare$$

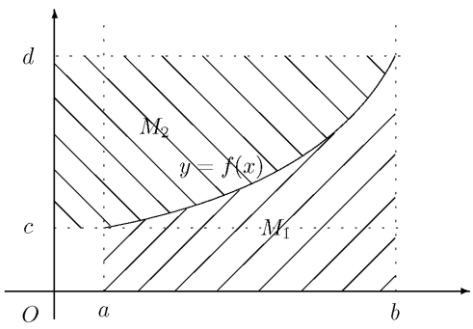
5. ЦЕЛОБРОЈНИ ТОЧКИ И ФУНКЦИЈАТА $[x]$

5.1. Теорема. Нека $a,b,c,d \in \mathbb{R}$, $b > a \ge 0, d > c \ge 0$ и нека $f:[a,b] \to [c,d]$ е биективна растечка функција. Тогаш

$$\sum_{a\le k\le b} [f(k)] + \sum_{c\le k\le d} [f^{-1}(k)] - n(G_f) = [b]\cdot[d] - \alpha(a)\alpha(c) \tag{1}$$

каде k е цел број, $n(G_f)$ е бројот на точките со ненегативни целобројни координати на графикот на f и функцијата $\alpha:\mathbb{R}\to\mathbb{Z}$ е определена со

$$\alpha(x) = \begin{cases} [x], & \text{ако } x \in \mathbb{R}\setminus\mathbb{Z} \\ 0, & \text{ако } x = 0 \\ x-1, & \text{ако } x \in \mathbb{Z}\setminus\{0\}. \end{cases}$$



Доказ. За секоја ограничена област M во рамнината со $n(M)$ да го означиме бројот на точките со ненегативни целобројни координати во M.

Функцијата f е растечка и биективна, па затоа таа е непрекина-

та. Да ги разгледаме множествата

$$M_1 = \{(x,y) \in \mathbb{R}^2 \mid a \le x \le b, 0 \le y \le f(x)\},$$
$$M_2 = \{(x,y) \in \mathbb{R}^2 \mid c \le y \le d, 0 \le x \le f^{-1}(y)\},$$
$$M_3 = \{(x,y) \in \mathbb{R}^2 \mid 0 \le x \le b, 0 \le y \le d\},$$
$$M_4 = \{(x,y) \in \mathbb{R}^2 \mid 0 \le x \le a, 0 \le y \le c\}.$$

Тогаш

$$n(M_1) = \sum_{a \le k \le b} [f(k)], \qquad n(M_2) = \sum_{c \le k \le d} [f^{-1}(k)],$$
$$n(M_3) = [b] \cdot [d], \qquad n(M_4) = \alpha(a)\alpha(c).$$

Понатаму,

$$n(M_1) + n(M_2) - n(M_1 \cap M_2) = n(M_1 \cup M_2),$$

па затоа

$$n(M_1) + n(M_2) - n(G_f) = n(M_3) - n(M_4),$$

од каде следува равенството (1). ■

5.2. Лема. Нека $m,n,s \in \mathbb{N}$, $m \le n$. Тогаш низата $\frac{m}{n}, \frac{2m}{n}, ..., \frac{sm}{n}$ содржи точно $[\frac{s \cdot (m,n)}{n}]$ цели броеви.

Доказ. Нека $d = (m,n)$. Тогаш $m = ad, n = bd$ каде $(a,b) = 1$ и низата е

$$\frac{a}{b}, \frac{2a}{b}, ..., \frac{sa}{b}.$$

Но, $(a,b) = 1$, па затоа последната низа содржи точно $[\frac{s}{b}]$ цели броеви. Понатаму, $b = \frac{n}{d}$ што значи дека низата содржи точно

$$[\frac{s}{b}] = [\frac{sd}{n}] = [\frac{s \cdot (m,n)}{n}]$$

цели броеви. ■

5.3. Последица. Нека $m,n,s \in \mathbb{N}$, $m \le n$. Тогаш

$$\sum_{k=1}^{s} [\frac{km}{n}] + \sum_{1 \le k \le \frac{ms}{n}} [\frac{kn}{m}] = s[\frac{ms}{n}] + [\frac{s \cdot (m,n)}{n}]. \qquad (2)$$

Доказ. Функцијата $f : [1,s] \to [\frac{m}{n}, \frac{ms}{n}]$ определена со $f(x) = \frac{m}{n}x$ е растечка, биективна и важи $f^{-1}(y) = \frac{n}{m}y$. Од лемата 5.2 следува дека $n(G_f) = [\frac{s \cdot (m,n)}{n}]$, па затоа од теоремата 5.1 следува равенството

$$\sum_{k=1}^{s} [\frac{km}{n}] + \sum_{1 \le k \le \frac{ms}{n}} [\frac{kn}{m}] - [\frac{s \cdot (m,n)}{n}] = s[\frac{ms}{n}],$$

кое е еквивалентно со равенството (2). ■

5.4. Забелешка. Ако во последицата 5.3 земеме $s=n$ добиваме дека за секои природни броеви m и n е точно равенството

$$\sum_{k=1}^{n}[\tfrac{km}{n}]+\sum_{k=1}^{m}[\tfrac{kn}{m}]=mn+(m,n)\,. \tag{3}$$

5.5. Теорема. Нека $a,b,c,d\in\mathbb{R}$, $b>a\geq 0, d>c\geq 0$ и нека $f:[a,b]\to[c,d]$ е биективна опаѓачка функција. Тогаш

$$\sum_{a\leq k\leq b}[f(k)]-\sum_{c\leq k\leq d}[f^{-1}(k)]=[b]\cdot\alpha(c)-[d]\cdot\alpha(a) \tag{4}$$

каде k е цел број и функцијата $\alpha:\mathbb{R}\to\mathbb{Z}$ е определена како во теоремата 5.1.

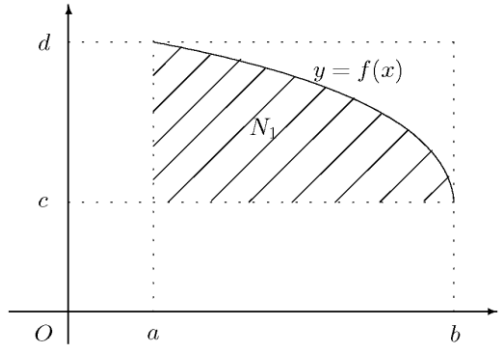
Доказ. Повторно, за секоја ограничена област M во рамнината со $n(M)$ да го означиме бројот на точките со ненегативни целобројни координати во M.

Функцијата f е опаѓачка и биективна, па затоа таа е непрекината. Да ги разгледаме множествата

$$N_1=\{(x,y)\in\mathbb{R}^2\mid a\leq x\leq b, c\leq y\leq f(x)\},$$
$$N_2=\{(x,y)\in\mathbb{R}^2\mid c\leq y\leq d, a\leq x\leq f^{-1}(y)\},$$
$$N_3=\{(x,y)\in\mathbb{R}^2\mid a\leq x\leq b, 0\leq y\leq c\},$$
$$N_4=\{(x,y)\in\mathbb{R}^2\mid 0\leq x\leq a, c\leq y\leq d\}.$$

Тогаш

$$\sum_{a\leq k\leq b}[f(k)]=n(N_1)+n(N_3),$$
$$\sum_{c\leq k\leq d}[f^{-1}(k)]=n(N_2)+n(N_4),$$
$$n(N_1)=n(N_2),$$
$$n(N_3)=([b]-\alpha(a))\alpha(c),$$
$$n(N_4)=([d]-\alpha(c))\alpha(a).$$



Според тоа,

$$\sum_{a\leq k\leq b}[f(k)]-\sum_{c\leq k\leq d}[f^{-1}(k)]=n(N_3)-n(N_4)=[b]\cdot\alpha(c)-[d]\cdot\alpha(a),$$

т.е. точно е равенството (4). ■

5.6. Забелешка. Од теоремата 5.5 применета на функцијата $f:[1,n]\to[0,m-\frac{m}{n}]$, определена со $f(x)=-\frac{m}{n}x+m, m\leq n$ и равенството (3) со едноставни пресметувања следува равенството

$$\sum_{k=1}^{n}[\tfrac{km}{n}]=\tfrac{1}{2}(mn+m-n+(m,n)), \qquad (5)$$

т.е. равенството

$$(m,n)=2\sum_{k=1}^{n}[\tfrac{km}{n}]-mn-m+n.$$

Понатаму, од равенството (5) и релацијата $x-[x]=\{x\}$ следува

$$\begin{aligned}\sum_{k=1}^{n-1}\{\tfrac{km}{n}\}&=\sum_{k=1}^{n-1}\tfrac{km}{n}-\sum_{k=1}^{n-1}[\tfrac{km}{n}]=\tfrac{m}{n}\cdot\tfrac{n(n-1)}{2}+m-\sum_{k=1}^{n}[\tfrac{km}{n}]\\&=\tfrac{m}{n}\cdot\tfrac{n(n-1)}{2}+m-\tfrac{1}{2}(mn+m-n+(m,n))\\&=\tfrac{1}{2}(n-(m,n)).\end{aligned}$$

6. БЕЛЕШКА ЗА РАСПРЕДЕЛБА НА ПРОСТИТЕ БРОЕВИ

6.1. Во претходните разгледувања докажавме повеќе својства на простите броеви. Притоа, докажавме дека множеството прости броеви е бесконечно и видовме дека со помош на Евклидовиот алгоритам може да се провери дали еден природен број е прост или сложен. Понатаму, природно се наметнуваат прашањето како простите броеви се распределени во множеството природни броеви? Во потрагата по одговор на распределбата на простите броеви, една од најчесто користените функции е функцијата $\pi(x)$, која се дефинира како што следува:

Дефиниција. За секој реален број x со $\pi(x)$ го означуваме бројот на простите броеви p такви што $p\le x$.

Всушност, функцијата $\pi(x)$ ја дава распределбата на простите броеви, за која може да се каже дека е прилично нерамномерна. Меѓутоа, додека на мали интервали распределбата на простите броеви изгледа крајно нерегуларна, за големи интервали случајот не е таков и постојат едноставни формули кои даваат приближни вредности на $\pi(x)$ кога x е многу голем број. Така во 1896 година Хадамард и Вапе Поусин докажале дека $\pi(x)\sim\frac{x}{\ln x}$ кога $x\to\infty$. Во следната лема ќе докажеме едно својство на функцијата $\pi(x)$, но истата нема детално да ја изучуваме бидејќи доказите на својствата на оваа функција излегуваат од рамките на нашите разгледувања.

6.2. Лема. Нека p_n е $n-$тиот прост број ($p_1=2, p_2=3,\ldots$) и нека $\pi(n)$ е бројот на простите броеви кои се помаили или еднакви на n. Ако

$$A=\{n+p_n \mid n\in\mathbb{N}\} \text{ и } B=\{n+\pi(n)+1 \mid n\in\mathbb{N}\},$$

тогаш $A\cap B=\varnothing$ и $A\cup B=\mathbb{N}\setminus\{1\}$.

Доказ. Од дефиницијата на функцијата π следува:

i) $\pi(p_k)=k$ за секој $k\in\mathbb{N}$,

ii) $\pi(n)\le\pi(n+1)$, за секој $n\in\mathbb{N}$,

iii) $\pi(n)<\pi(n+1)$, ако $n+1$ е прост број.

Нека претпоставиме дека за некои *m* и *n* важи

iv) $m+p_m=n+\pi(n)+1$.

Можни се два случаи: $p_m\le n$ и $p_m>n$. Ако $p_m\le n$, тогаш ако се земе предвид дека $m=\pi(p_m)\le\pi(n)$ добиваме

$$m+p_m\le n+\pi(n)<n+\pi(n)+1,$$

што противречи на *iv*). Ако $p_m>n$, тогаш од $m=\pi(p_m)>\pi(n)$ следува $m\ge\pi(n)+1$ и $m+p_m>n+\pi(n)+1$ што противречи на *iv*). Според тоа $A\cap B=\varnothing$.

Ќе докажеме дека $A\cup B=\mathbb{N}\setminus\{1\}$. Јасно, $1\notin A,B$ и $2\in B$. Нека $n>2$ е произволен природен број кој не припаѓа на множеството A. Ќе докажеме дека $n\in B$. Бидејќи постои $m\in\mathbb{N}$ т.ш. $m+p_m<n<m+1+p_{m+1}$, т.е. $p_m\le n-m-1<p_{m+1}$, добиваме дека $\pi(n-m-1)=m$, па значи

$$n=\pi(n-m-1)+(n-m-1)+1\in B.\ \blacksquare$$

6.3. Во врска со распределбата на простите броеви е и следната теорема на Чебишев, чиј доказ излегува од рамките на нашите разгледувања, па затоа истиот нема да го презентираме.

Теорема (Чебишев). Ако $n>5$, тогаш меѓу броевите n и $2n$ постојат најмалку два прости броја. □

6.4. Пример. Ако $k>3$, тогаш $p_{k+2}<2p_k$, каде p_k е $k-$тиот прост број. Докажи!

Решение. Бидејќи $k>3$ имаме $p_k>p_3=5$. Сега од теорема 6.3 следува дека постојат барем два прости броја q и r такви, да $p_k<q<r<2p_k$. Но, $p_{k+1}\le q$ и $p_{k+2}\le r$, па затоа $p_{k+2}<2p_k$. ■

6.5. Последица (постулат на Бертран). Ако $n>3$, тогаш меѓу броевите n и $2n-2$ постои најмалку еден прост број.

Доказ. Навистина, ако $n=4$, тогаш 5 е меѓу 4 и 6, а ако $n=5$, тогаш 7 е меѓу 5 и 8.

Ако $n>5$, тогаш од теоремата 6.3 следува дека меѓу n и $2n$ има најмалку два прости броја. Ако поголемиот од овие прости броеви е $2n-1$, тогаш бидејќи

$2n-2=2(n-1)$ е сложен број, помалиот прост број ќе биде помал или еднаков на $2n-3$. Тоа значи дека меѓу n и $2n-2$ постои најмалку еден прост број. ■

6.6. Пример. Ако $n>1$, тогаш во каноничното разложување на $n!$ има најмалку еден прост број со степен еден.

Решение. За $n\le 7$ тврдењето на задачата е очигледно.

Ако $n=2k$, $k\ge 4$, тогаш согласно постулатот на Бертран постои барем еден прост број p таков што $k<p<2k-2<n$. Но, тогаш $2p>2k=n$, што значи дека $p<n<2p$, од што следува дека простиот број p во каноничното разложување на $n!$ е со степен еден.

Ако $n=2k+1, k\ge 4$, тогаш повторно од постулатот на Бертран следува дека постои прост број p таков што $k<p<2k-2<n$. И во овој случај $2k<2p$, па значи и $2k+1<2p$, т.е. $p<n<2p$, од што следува дека простиот број p во каноничното разложување на $n!$ е со степен еден. ■

6.7. На крајот од овој дел, во врска со распределбата на простите броеви, ќе дадеме уште една теорема, чиј доказ излегува надвор од рамките на нашите разгледувања.

Теорема (Дирихле). Секоја аритметичка прогресија $ak+b, k=0,1,\ldots$, каде a, b се заемно прости природни броеви, содржи бесконечно многу прости броеви. □

6.8. Последица. Секоја аритметичка прогресија $ak+b, k=0,1,2,\ldots$, каде a,b се заемно прости природни броеви, за секој природен број s содржи бесконечно многу членови кои се производ на s различни прости броеви.

Доказ. За $s=1$ тврдењето следува од теоремата на Дирихле.

Нека претпоставиме дека тврдењето важи за природниот број $s\ge 1$. Од $(a,b)=1$ следува дека постои број k_0 таков што

$$ak_0+b=q_1q_2\ldots q_s$$

каде $q_1<q_2<\ldots<q_s$ се прости броеви. Согласно теоремата на Дирихле постојат бесконечно многу природни броеви k, такви што $ak+1=q$ е прост број поголем од q_s. За

$$t=q_1q_2\ldots q_sk+k_0$$

имаме

$$at+b=q_1q_2\ldots q_sak+ak_0+b=q_1q_2\ldots q_s(ak+1)=q_1q_2\ldots q_sq,$$

т.е тврдењето важи за $s+1$.

Конечно, од принципот на математичка индукција следува дека тврдењето важи за секој $s\in\mathbb{N}$. ■

6.9. Пример. Докажи, дека за секој природен број m постои прост број чиј збир на цифри е поголем од $9m$.

Решение. Нека m е природен број. Бидејќи $(10^m, 10^m - 1) = 1$, според теоремата на Дирихле, постои природен број k таков што $p = 10^m k + 10^m - 1$ е прост број. Бидејќи последните m цифри на p се еднакви на 9, добиваме дека збирот на цифрите на p е поголем од $9m$. ■

6.10. Пример. Определи ги сите природни броеви m такви што важи

$$1!3!5!...(2m-1)! = (\tfrac{m(m+1)}{2})! . \qquad (1)$$

Решение. Бидејќи за произволен прост број p и природен број n важи $p \nmid n!$ ако и само ако $n < p$, заклучуваме дека постоењето на прост број p таков што

$$2m-1 < p \le \tfrac{m(m+1)}{2}$$

повлекува дека m не може да биде решение на (1), бидејќи десната страна е делива со p, а левата страна не е делива со p. Од постулатот на Бертран следува дека таков број ќе постои секогаш кога

$\tfrac{m(m+1)}{2} \ge 2(2m-1)$, т.е. $m^2 - 7m + 4 \ge 0$.

Но последното неравенство очигледно е точно за $m \ge 7$, односно за $m \ge 7$ равенката (1) нема решение. Останува да ги разгледаме броевите $m \le 6$.

За $m = 6$ е $2m-1 = 11 < 13 < 21 = \tfrac{6\cdot 7}{2}$, а за $m = 5$ е $2m-1 = 9 < 11 < 15 = \tfrac{5\cdot 6}{2}$, па затоа овие вредности не се решение.

Од друга страна, $m = 1, 2$ очигледно се решенија. Решение е и $m = 3$, бидејќи

$$1!3!5! = 6\cdot 5! = 6! = (\tfrac{3\cdot(3+1)}{2})!,$$

а исто така и $m = 4$, бидејќи

$$1!3!5!7! = 6!7! = 720\cdot 7! = 10\cdot 9\cdot 8\cdot 7! = 10! = (\tfrac{4\cdot(4+1)}{2})! . \blacksquare$$

III ГЛАВА
МУЛТИПЛИКАТИВНИ ФУНКЦИИ

1. ПОИМ ЗА МУЛТИПЛИКАТИВНА ФУНКЦИЈА

1.1. Дефиниција. Функцијата $f:\mathbb{N}\to\mathbb{C}$, $\mathbb{C}$ е множеството комплексни броеви, ја нарекуваме *аритметичка функција*.

За аритметичката функција $f:\mathbb{N}\to\mathbb{C}$ ќе велиме дека е *мултипликативна* ако

а) постои $n_0\in\mathbb{N}$ таков што $f(n_0)\neq 0$ и

b) ако $(m,n)=1$, тогаш $f(mn)=f(m)f(n)$.

Ако условот б) е исполнет за секои $m,n\in\mathbb{N}$, заемно прости или не, тогаш ќе велиме дека функцијата f е *потполно мултипликативна*.

1.2. Забелешка. а) Ако $f:\mathbb{N}\to\mathbb{C}$ е мултипликативна, тогаш $f(1)=1$. Навистина, постои $a\in\mathbb{N}$ е таков што $f(a)\neq 0$, па затоа од $f(a)=f(a\cdot 1)=f(a)f(1)$ следува $f(1)=1$.

б) Ако f е милтипликативна и $n=p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}$ е каноничното претставување на n, тогаш $f(n)=f(p_1^{a_1})f(p_2^{a_2})\ldots f(p_k^{a_k})$.

в) Ако f е потполно милтипликативна и $n=p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}$ е каноничното претставување на n, тогаш

$$f(n)=f(p_1)^{a_1}f(p_2)^{a_2}\ldots f(p_k)^{a_k}.$$

1.3. Теорема. Ако f е мултипликативна функција, тогаш функцијата h дефинирана со

$$F(n)=\sum_{d|n}f(d)$$

е мултипликативна.

Функцијата F ја нарекуваме *функција сума* за функцијата f.

Доказ. Нека $m>1, n>1$ и $(m,n)=1$. Имаме

$$F(n)F(m)=\sum_{d_1|m}f(d_1)\sum_{d_2|n}f(d_2)=\sum_{d_1|m,\,d_2|n}f(d_1)f(d_2).$$

Ако $d_1\mid m, d_2\mid n$ и $(m,n)=1$, тогаш $(d_1,d_2)=1$, па затоа

$$F(n)F(m)=\sum_{d_1|m,\,d_2|n}f(d_1d_2).$$

Понатаму, множеството од сите броеви d_1d_2, каде d_1 и d_2 се позитивни делители на m и n соодветно, се совпаѓа со множеството од сите позитивни делители на mn и притоа не се повторува ниту еден делител на mn. Значи,

$$F(n)F(m)=\sum_{d_1|m,\,d_2|n} f(d_1d_2)=\sum_{d|mn} f(d)=F(mn)\ .\ \blacksquare$$

1.4. Последица. Нека f е мултипликативна функција и F е нејзината функција сума. Ако $n=p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}$, тогаш

$$F(n)=\prod_{i=1}^{k}(1+f(p_i)+\ldots+f(p_i^{a_i}))\,. \tag{1}$$

Доказ. Имаме,

$$\prod_{i=1}^{k}(1+f(p_i)+\ldots+f(p_i^{a_i}))=\sum_{\substack{0\le b_1\le a_1,\\ \ldots\ldots\ldots\\ 0\le b_k\le a_k}} f(p_1^{b_1})f(p_2^{b_2})\ldots f(p_k^{b_k})$$

$$=\sum_{\substack{0\le b_1\le a_1,\\ \ldots\ldots\ldots\\ 0\le b_k\le a_k}} f(p_1^{b_1}p_2^{b_2}\ldots p_k^{b_k})=\sum_{d|n} f(d)=F(n),$$

што и требаше да се докаже. ■

1.5. Пример. Ако $f_1, f_2, \ldots, f_k$ се мултипликативни функции, тогаш функцијата $f_1f_2\ldots f_k$ е мултипликативна. Докажи!

Решение. Нека $(m,n)=1$. Тогаш

$$\begin{aligned}(f_1f_2\ldots f_k)(mn)&=f_1(mn)f_2(mn)\ldots f_k(mn)\\&=f_1(m)f_1(n)f_2(m)f_2(n)\ldots f_k(m)f_k(n)\\&=f_1(m)f_2(m)\ldots f_k(m)\cdot f_1(n)f_2(n)\ldots f_k(n)\\&=(f_1f_2\ldots f_k)(m)(f_1f_2\ldots f_k)(n),\end{aligned}$$

што значи дека функцијата $f_1f_2\ldots f_k$ е мултипликативна. ■

1.6. Пример. За секој природен број n со $\delta(n)$ да го означиме производот на различните природни делители на n. Докажи дека функцијата $\delta(n)$ не е мултипликативна.

Решение. Имаме, $(2,3)=1$ и $\delta(2)\delta(3)=2\cdot3=6\neq36=\delta(6)=\delta(2\cdot3)$, што значи дека функцијата $\delta(n)$ не е мултипликативна. ■

1.7. Пример. Со $\sigma_2(n)$ да го означиме збирот на квадратите на сите делители на природниот број n. Докажи дека постојат бесконечно многу природни броеви

n такви што $n \mid \sigma_2(n)$.

Решение. Нека $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Лесно се докажува дека

$$\sigma_2(n) = \prod_{i=1}^{k} (1 + p_i^2 + \ldots + p_i^{2\alpha_i}).$$

Забележуваме дека функцијата σ_2 е мултипликативна, односно дека од $(a,b)=1$ следува $\sigma_2(ab) = \sigma_2(a)\sigma_2(b)$.

Бројот 10 ги задоволува условите на задачата бидејќи $10 \mid \sigma_2(10) = 130$. Ќе докажеме дека од било кој број n кој ги задоволува условите на задачата можеме да добиеме поголем број кој ги задоволува условите на задачата, од што ќе следува тврдењето. Со $v_p(x)$ да го означиме најголемиот i таков што $p^i \mid x$. Бидејќи $\sigma_2(n) > n^2$, постои прост број p таков што $v_p(n) = r$ и $v_p(\sigma_2(n)) > 2r$, т.е. $p^{r+1} \mid \frac{\sigma_2(n)}{n}$. Нека $n = p^r m$, $p \nmid m$. Бидејќи

$$\begin{aligned}
\sigma_2(p^{2r+1}) &= 1 + p^2 + \ldots + p^{2r} + p^{2r+2} + \ldots + p^{4r+2} \\
&= 1 + p^2 + \ldots + p^{2r} + p^{2r+2}(1 + p^2 + \ldots + p^{2r}) \\
&= (p^{2r+2} + 1)(1 + p^2 + \ldots + p^{2r}) \\
&= (p^{2r+2} + 1)\sigma_2(p^r),
\end{aligned}$$

добиваме

$$p^{r+1} n \mid \sigma_2(n) = \sigma_2(p^r)\sigma_2(m) \mid \sigma_2(p^{2r+1})\sigma_2(m) = \sigma_2(p^{2r+1}m) = \sigma_2(p^{r+1}n),$$

што значи дека и бројот $p^{r+1}n$ ги задоволува условите на задачата. Со ова доказот е завршен. ■

2. БРОЈ НА ДЕЛИТЕЛИ И ЗБИР НА ДЕЛИТЕЛИ НА ПРИРОДЕН БРОЈ

2.1. Дефиниција. Нека $n \in \mathbb{N}$. Со $\tau(n)$ го означуваме *бројот од сите природни делители* на n. Со $\sigma(n)$ го означуваме *збирот од сите природни делители* на n.

Во следнава табела се презентирани вредностите на $\tau(n)$ и $\sigma(n)$, за $n = 1,2,3,\ldots,17$.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$\tau(n)$	1	2	2	3	2	4	2	4	3	4	2	6	2	4	4	5	2
$\sigma(n)$	1	3	4	7	6	12	8	15	13	18	12	28	14	24	24	31	18

Јасно, $\tau(n)=2$ и $\sigma(n)=n+1$ ако и само ако n е прост број.

2.2. Теорема. Функциите $\tau(n)$ и $\sigma(n)$ се мултипликативни.

Доказ. Функцијата $f(n)=1$ е мултипликативна. Бидејќи

$$\tau(n)=\sum_{d|n}1=\sum_{d|n}f(d),$$

од теорема 1.3 следува дека функцијата $\tau(n)$ е мултипликативна.

Функцијата $f(n)=n$ е мултипликативна. Бидејќи

$$\sigma(n)=\sum_{d|n}d=\sum_{d|n}f(d),$$

од теорема 1.3 следува дека функцијата $\sigma(n)$ е мултипликатвна. ■

2.3. Теорема. Ако $n=p_1^{a_1}p_2^{a_2}...p_k^{a_k}$, тогаш

$$\tau(n)=(1+a_1)(1+a_2)...(1+a_k),\ \sigma(n)=\frac{p_1^{a_1+1}-1}{p_1-1}\cdot\frac{p_2^{a_2+1}-1}{p_2-1}\cdot...\cdot\frac{p_k^{a_k+1}-1}{p_k-1}. \qquad (1)$$

Доказ. Ако p е прост број и $a\geq 1$, тогаш делители на p^a се $1, p, p^2, ..., p^a$, па затоа

$$\tau(p^a)=1+a \text{ и } \sigma(p^a)=1+p+p^2+...+p^a=\frac{p^{a+1}-1}{p-1}.$$

Конечно, равенствата (1) следуваат од мултипликативноста на функциите $\tau(n)$ и $\sigma(n)$. ■

2.4. Лема. За секој природен број $n\geq 2$ важи

$$\sigma(n)<n(1+\ln n).$$

Доказ. Од дефиницијата на $\sigma(n)$ и својствата на определениот интеграл следува:

$$\sigma(n)=\sum_{d|n}d=\sum_{d|n}\frac{n}{d}\leq n\sum_{d\leq n}\frac{1}{d}<n(1+\int_1^n\frac{dx}{x})=n(1+\ln n). \text{ ■}$$

2.5. Дефиниција. За природниот број n ќе велиме дека е *совршен* ако важи $\sigma(n)=2n$.

2.6. Броевите 6 и 28 се совршени. До сега не е познато дали постои непарен совршен број. За парните совршени броеви точна е следнава теорема..

Теорема (Ојлер). Парен број n е совршен ако и само ако има може да се претстави во видот $2^{p-1}(2^p-1)$ каде 2^p-1 е прост број.

Доказ. Нека $n=2^{p-1}(2^p-1)$, каде 2^p-1 е прост број. Тогаш, бидејќи бројот 2^p-1 е прост имаме

$$\sigma(n)=\sigma(2^{p-1}(2^p-1))=\sigma(2^{p-1})\sigma(2^p-1)=\frac{2^p-1}{2-1}\cdot(2^p-1+1)=2^p(2^p-1)=2n$$

т.е. n е совршен број.

Обратно, нека претпоставиме дека $\sigma(n)=2n$. Бројот n е парен, па затоа може да се претстави во видот $n=2^k m$, каде $k,m\in\mathbb{N}$ и m е непарен број. Од

$$\begin{aligned}2^{k+1}m=2n=\sigma(n)=\sigma(2^k m)=\sigma(2^k)\sigma(m)\\=(2^{k+1}-1)\sigma(m)\end{aligned}$$

следува дека $2^{k+1}-1$ е делител на m, па затоа $m=(2^{k+1}-1)t$ за некој непарен број t. Сега лесно се добива дека $\sigma(m)=2^{k+1}t$. Ако $t>1$, тогаш бидејќи 1, t и m се различни делители на m, добиваме

$$\sigma(m)\geq t+m+1=2^{k+1}t+1>2^{k+1}t=\sigma(m),$$

што е противречност. Затоа $t=1$ и $\sigma(m)=2^{k+1}=m+1$, што значи дека m е прост број. ■

2.7. Пример. Докажи дека:

а) $\sum_{d|n}d^k=\sum_{d|n}(\frac{n}{d})^k$, б) $\tau(n)<2\sqrt{n}$, и в) $\sqrt{n}\leq\frac{\sigma(n)}{\tau(n)}$, $n>1$.

Решение. а) Равенството следува од фактот дека ако d е делител на бројот n, тогаш и $\frac{n}{d}$ е делител на бројот n, и обратно.

б) Ако n не е точен квадрат, тогаш неговите делители ги групираме во парови од видот $(d,\frac{n}{d})$, $d<\frac{n}{d}$, кои ги има помалку од $\sqrt{n}$. Ако n е точен квадрат, тогаш $\tau(n)\leq 2(\sqrt{n}-1)+1<2\sqrt{n}$.

в) Од

$$\sigma(p^a)=\frac{p^{a+1}-1}{p-1}=1+p+p^2+\ldots+p^a\geq(a+1)p^{\frac{a}{2}}=\tau(p^a)p^{\frac{a}{2}}$$

добиваме $\frac{\sigma(p^a)}{\tau(p^a)}\geq\sqrt{p^a}$ и ако ја искористиме мултипликативноста на функциите $\tau(n)$ и $\sigma(n)$ добиваме $\sqrt{n}\leq\frac{\sigma(n)}{\tau(n)}$. ■

2.8. Пример. Бројот 9 може да се претстави како збир на два последователни природни броја $9=4+5$, а уште повеќе тој може да се претстави како збир на барем два последователни природни броја на точно два начина

$$9=4+5=2+3+4.$$

Дали постои природен број кој може да се претстави како збир на 1990 последователни природни броеви и кој може да се претстави како збир на барем два последователни броја на точно 1990 начини?

Решение. Нека претпоставиме дека бројот N ги има саканите својства. Првиот од двата услови на задачата може да се запише како

$$N = m + (m+1) + ... + (m+1989) = 995(2m+1989),$$

за некој m, па затоа N е непарен број делив со 5 и 199. Вториот услов е дека постојат точно 1990 парови природни броеви (n,k) за кои

$$N = n + (n+1) + ... + (n+k) = \frac{(k+1)(2n+k)}{2}.$$

Според тоа, постојат точно 1990 начини бројот $2N$ да го прикажеме во видот

$$2N = (k+1)(2n+k),$$

при што $k \geq 1$. Бидејќи N е непарен број, заклучуваме дека еден од двата множители во последното равенство е непарен број, а другиот е делив со 2, но не и со 4. Бидејќи $k+1 < 2n+k$, добиваме дека секоја опишана факторизација на бројот $2N$ еднозначно го определува бараниот пар (n,k). Ако ставиме

$$2N = 2 \cdot 5^{s_1} 199^{s_2} p_3^{s_3} ... p_r^{s_r},$$

каде p_i се прости броеви различни од 2, 5 и 199, добиваме дека бројот на делители на бројот $2N$ е еднаков на

$$(1+1)(s_1+1)(s_2+1)...(s_r+1).$$

Според тоа, факторизации $2N = uv, u < v$ има $(s_1+1)(s_2+1)...(s_r+1)$, а бидејќи тривијалната факторизација $2N = 1 \cdot 2N$ дава $k = 0$, бројот на опишаните парови е

$$(s_1+1)(s_2+1)...(s_r+1) - 1.$$

Последното значи дека

$$(s_1+1)(s_2+1)...(s_r+1) = 1991 = 11 \cdot 181.$$

Но, $5 \cdot 199 \mid N$, па затоа $s_1, s_2 > 0$, од што следува

$$s_1 = 10, s_2 = 180 \text{ или } s_1 = 180, s_2 = 10,$$

а $s_3 = s_4 = ... = s_r = 0$. Според тоа, $N = 5^{10} 199^{180}$ или $N = 5^{180} 199^{10}$, што значи дека ова се единствените два броја кои се решение на задачата. ■

2.9. Пример. Нека $\sigma(n)$ е збирот на позитивните делители на природниот број n. За природниот број m ќе велиме дека е *силен* ако за секој $1 \leq k < m$ важи

$$\frac{\sigma(k)}{k} < \frac{\sigma(m)}{m}.$$

Докажи дека постојат бесконечно многу силни броеви.

Решение. Нека $a_m = \frac{\sigma(m)}{m}$. Јасно, бројот m е силен ако и само ако $a_k < a_m$ за секој $k < m$. Сега, доволно е да докажеме дека низата $a_n, n \in \mathbb{N}$ нема најголем

елемент, бидејќи тогаш лесно се покажува дека постојат бесконечно многу силни броеви. Имено, ако бројот m е силен, тогаш го наоѓаме најмалиот $m'>m$ таков што $a_m < a_{m'}$. Тогаш и бројот m' очигледно е силен.

Нека n е произволен природен број. За секој негов делител $d:1$ важи $2d \mid 2n$. Бидејќи, освен тоа тривијално важи $1 \mid 2n$, го добиваме неравенството

$$\sigma(2n) \geq 2\sigma(n)+1.$$

Оттука, ако поделиме со $2n$ добиваме дека $a_{2n} > a_n$, т.е. низата $a_n, n \in \mathbb{N}$ нема најголем елемент. ■

2.10. Пример. Нека n е природен број. Определи го бројот на паровите природни броеви (x,y) за кои важи $\frac{1}{x}+\frac{1}{y}=\frac{1}{n}$.

Решение. Од $\frac{1}{x}+\frac{1}{y}=\frac{1}{n}$ следува $nx+ny=xy$, т.е. $(n-x)(n-y)=n^2$. За $n=1$ имаме $(x-1)(y-1)=1$, од каде се добива единствено решение $(x,y)=(2,2)$. Нека $n \geq 2$ и $n=p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$ е канонична факторизација на бројот n. Нека

$$1=d_1<d_2<...<d_s=n^2$$

се сите делители на n^2. Бидејќи n^2 е точен квадрат, добиваме дека s е непарен број, и притоа важи

$$d_1d_s=d_2d_{s-1}=...=d_{\frac{s+1}{2}}^2=n^2.$$

Според тоа, постои биекција меѓу решенијата (x,y) на $\frac{1}{x}+\frac{1}{y}=\frac{1}{n}$ и паровите делители на n^2, па затоа бројот на паровите природни броеви (x,y) за кои важи $\frac{1}{x}+\frac{1}{y}=\frac{1}{n}$ е еднаков на

$$\tau(n^2)=(2\alpha_1+1)(2\alpha_2+1)...(2\alpha_k+1). \blacksquare$$

2.11. Пример. Нека n е совршен број. Докажи дека $\sum_{d|n}\frac{1}{d}=2$.

Решение. Ако d е делител на бројот n, тогаш и $\frac{n}{d}$ е делител на n. Бидејќи n е совршен број, за збирот на неговите делители важи $\sigma(n)=2n$. Сега имаме,

$$\sum_{d|n}\frac{1}{d}=\sum_{d|n}\frac{1}{\frac{n}{d}}=\sum_{d|n}\frac{d}{n}=\frac{1}{n}\sum_{d|n}d=\frac{1}{n}\cdot 2n=2. \blacksquare$$

2.12. Пример. Докажи дека секој непарен совршен број има најмалку три различни прости делители.

Решение. Нека претпоставиме дека n е непарен број кој има само еден прост

делител, т.е. нека $n=p^k$, каде $p\geq 3$ и k е природен број. Јасно, броевите $1, p, p^2,..., p^k$ се сите делители на n па нивниот збир е:

$$\sigma(n)=1+p+p^2+...+p^k=\frac{p^k-1}{p-1}+p^k<p^k+p^k=2p^k=2n.$$

Бидејќи $\sigma(n)\neq 2n$ следува дека бројот n не е совршен.

Сега, нека n има два прости делители $p,q\geq 3$, т.е. $n=p^aq^b, a,b\geq 1$. Имаме:

$$\begin{aligned}\sigma(n)&=\sigma(p^aq^b)=\sigma(p^a)\sigma(q^b)=(1+p+p^2+...+p^a)(1+q+q^2+...+q^b)\\&=p^a(1+\tfrac{1}{p}+...+\tfrac{1}{p^a})q^b(1+\tfrac{1}{q}+...+\tfrac{1}{q^b})<p^aq^b\sum_{i=0}^{\infty}\frac{1}{p^i}\sum_{s=0}^{\infty}\frac{1}{q^s}\\&=p^aq^b\,\frac{1}{1-\frac{1}{p}}\cdot\frac{1}{1-\frac{1}{q}}\leq p^aq^b\,\frac{1}{1-\frac{1}{3}}\cdot\frac{1}{1-\frac{1}{5}}=\frac{15}{8}\,p^aq^b<2p^aq^b=2n,\end{aligned}$$

па затоа бројот n не е совршен. Оттука следува дека секој непарен совршен број има најмалку три различни прости делители. ■

2.13. Пример. Нека n е природен број. Докажи дека збирот на сите позитивни делители на бројот $n!$ (вклучувајќи ги 1 и $n!$) не е поголем од $\frac{1}{2}(n+1)!$.

Решение. За збирот на делителите на бројот $m=p_1^{r_1}p_2^{r_2}...p_k^{r_k}$ имаме

$$\sigma(m)=\prod_{i=1}^{k}\frac{p_i^{r_i+1}-1}{p_i-1}<\prod_{i=1}^{k}\frac{p_i^{r_i+1}}{p_i-1}=m\prod_{i=1}^{k}\frac{p_i}{p_i-1}.$$

За $m=n!$ важи $p_1=2$ и $p_i\geq 2i-1$, т.е. $\frac{p_i}{p_i-1}\leq\frac{2i-1}{2i-2}\leq\frac{i+3}{i+2}$ за $2\leq i\leq k\leq\frac{n+2}{2}$. Затоа за $n>10$ имаме

$$\frac{\sigma(n!)}{n!}\leq\frac{2}{1}\cdot\frac{3}{2}\cdot\frac{5}{4}\cdot\prod_{i=4}^{k}\frac{2i-1}{2i-2}\leq\frac{15}{4}\prod_{i=4}^{k}\frac{i+3}{i+2}=\frac{15}{4}\cdot\frac{k+3}{6}\leq\frac{15}{4}\cdot\frac{n+8}{12}<\frac{n+1}{2}.$$

Тврдењето важи и за $n\leq 10$. Навистина,

$$\begin{aligned}&\frac{\sigma(2!)}{2!}=\frac{3}{2}, \qquad \frac{\sigma(3!)}{3!}=2, \qquad \frac{\sigma(4!)}{4!}=\frac{5}{2},\\&\frac{\sigma(5!)}{5!}=3, \qquad \frac{\sigma(6!)}{6!}=\frac{403}{120}<\frac{7}{2}, \quad \frac{\sigma(7!)}{7!}=\frac{403}{105}<4,\\&\frac{\sigma(8!)}{8!}=\frac{221}{56}<\frac{9}{2}, \frac{\sigma(9!)}{9!}=\frac{2057}{504}<5, \frac{\sigma(10!)}{10!}=\frac{273823}{64800}<\frac{11}{2}.\end{aligned}$$ ■

2.14. Пример. Определи ги сите природни броеви n таквиа што $\tau(n)^3=4n$.

Решение. Нека $n=p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$ е каноничната факторизација на бројот n и $p_1<p_2<...<p_k$. Бројот $4n$ е точен куб, па затоа $2\mid n$, т.е. $p_1=2$. Значи $\tau(n)^3=2^{\alpha_1+2}p_2^{\alpha_2}...p_k^{\alpha_k}$, па затоа $\alpha_1=3\beta_1+1, \alpha_2=3\beta_2,..., \alpha_k=3\beta_k$, каде $\beta_i\geq 0$. Од

$$\tau(n)=(\alpha_1+1)(\alpha_2+1)...(\alpha_k+1)=(3\beta_1+2)(3\beta_2+1)...(3\beta_k+1)$$

следува

$$(3\beta_1+2)^3(3\beta_2+1)^3...(3\beta_k+1)^3=2^{3(\beta_1+1)}p_2^{3\beta_2}...p_k^{3\beta_k}$$

$$(3\beta_1+2)(3\beta_2+1)...(3\beta_k+1)=2^{\beta_1+1}p_2^{\beta_2}...p_k^{\beta_k}. \qquad (2)$$

Јасно, ниту еден од броевите на левата страна на (2) не е делив со 3, па следува дека $p_i\geq 5$ за секој $i\in\{2,3,...,k\}$. Равенката (2) е еквивалентна на равенката

$$\frac{3\beta_1+2}{2^{\beta_1+1}}=\frac{p_2^{\beta_2}}{3\beta_2+1}\cdot...\cdot\frac{p_k^{\beta_k}}{3\beta_k+1}. \qquad (3)$$

За $i\in\{2,3,...,k\}$ важи $p_i^{\beta_i}\geq 5^{\beta_i}=(1+4)^{\beta_i}\geq 1+4\beta_i\geq 1+3\beta_i$. Сега, од (3) следува $\frac{3\beta_1+2}{2^{\beta_1+1}}\geq 1$. Лесно се докажува дека за $\beta_1>2$ важи $2^{\beta_1+1}>3\beta_1+2$, па затоа $\beta_1\leq 2$.

Ако $\beta_1=0$ или $\beta_1=2$, тогаш $\frac{3\beta_1+2}{2^{\beta_1+1}}=1$, т.е. $\frac{p_i^{\beta_i}}{3\beta_i+1}=1$ за $i\in\{2,3,...,k\}$. Последното е можно само ако $\beta_i=0$, бидејќи во спротивно важи

$$p_i^{\beta_i}\geq 5^{\beta_i}\geq 1+4\beta_i>1+3\beta_i.$$

Ако $\beta_1=0$, тогаш $\alpha_1=1$ и бидејќи $\beta_i=0$ за $i\in\{2,3,...,k\}$ следува $\alpha_i=0$ за $i\in\{2,3,...,k\}$. Оттука $n=2^1=2$.

Ако $\beta_1=2$, тогаш $\alpha_1=7$, па следува дека $n=2^7=128$.

Ако $\beta_1=1$, тогаш левата страна на (3) е еднаква на $\frac{5}{4}$. Од друга страна, ако $p_i>5$ или $\beta_i>1$, тогаш $\frac{p_i^{\beta_i}}{3\beta_i+1}>\frac{5}{4}$. Значи $p_2=5$, од каде следува дека $\frac{5^{\beta_2}}{3\beta_2+1}=\frac{5}{4}$, т.е $\beta_2=1$. Според тоа, $n=2^{\alpha_1}5^{\alpha_2}=2^{3\beta_1+1}5^{3\beta_2}=2^4\cdot 5^3=2000$.

Значи, $n=2, n=128, n=2000$ се бараните броеви. ■

2.15. Пример (теорема на Луивил). Докажи го идентитетот

$$\sum_{d|n}\tau^3(d)=(\sum_{d|n}\tau(d))^2. \qquad (4)$$

Решение. Според пример 1.5 и принципот на математичка индукција од мултипликативноста на функцијата $f(n)$ следува за секој $m\in\mathbb{N}$ функцијата $(f(n))^m$ е мултипликативна. Понатаму, бидејќи функцијата $\tau(n)$ е мултипликативна, добиваме дека функциите $\sum_{k|n}\tau^3(k)$ и $(\sum_{k|n}\tau(k))^2$ се мултипликативни. Затоа, доволно е идентитетот (4) да го докажеме за броеви од обликот $n=p^a$, каде p е прост број и $a\in\mathbb{N}_0$. Имаме

$$\sum_{d|p^a} \tau^3(d) = \sum_{i=0}^{a} \tau^3(p^i) = \sum_{i=1}^{a+1} i^3 = [\frac{(a+1)(a+2)}{2}]^2$$

$$= (\sum_{i=1}^{a+1} i)^2 = (\sum_{i=0}^{a} \tau(p^i))^2 = (\sum_{d|p^a} \tau(d))^2,$$

што и требаше да се докаже. ■

3. КОНВОЛУЦИСКИ ПРОИЗВОД

3.1. Теорема. Нека $f(n)$ и $g(n)$ се мултипликативни функци. Тогаш и функцијата

$$h(n) = \sum_{d|n} f(d)g(\frac{n}{d}) \tag{1}$$

е мултипликативна.

Доказ. Нека m и n се заемно прости броеви. Ако d_1 се менува во множеството делители на m и d_2 се менува во множеството делители на n, тогаш $d_1 d_2$ се менува во множеството делители на mn и обратно. Затоа

$$h(m)h(n) = \sum_{d_1|m} f(d_1)g(\frac{m}{d_1}) \cdot \sum_{d_2|m} f(d_2)g(\frac{n}{d_2})$$

$$= \sum_{d_1 d_2|mn} f(d_1)f(d_2)g(\frac{m}{d_1})g(\frac{n}{d_2})$$

$$= \sum_{d_1 d_2|mn} f(d_1 d_2)g(\frac{mn}{d_1 d_2}) = h(mn),$$

т.е. функцијата h е мултипликативна. ■

3.2. Дефиниција. Нека f и g се аритметички функции. Функцијата h определена со равенството (1) ја нарекуваме *конволуциски производ* или *производ на Дирихле* за функциите f и g. Притоа ја прифаќаме ознаката $h = f * g$.

3.3. Непосредна последица од претходната теорема е теорема 1.3. Навистина, доволно е да забележиме дека функцијата $g(n) = 1, n \in \mathbb{N}$ е мултипликативна. Понатаму, аналогно на доказот на теоремата 3.1 може да се докаже следнава теорема. Деталите ги оставаме на читателот за вежба.

Теорема. Нека $f(n)$ и $g(n)$ се мултипликативни функци. Тогаш и функцијата

$$h(n) = \sum_{d^k|n} f(d)g(\frac{n}{d^k})$$

е мултипликативна. ■

3.4. Теорема. а) Ако f, g и h се аритметички функции, тогаш

$$f*g = g*f \text{ и } (f*g)*h = f*(g*h),$$

т.е. конволуцискиот производ е комутативен и асоцијативен.

б) За секоја аритметичка функција f важи $f*e = e*f = f$, каде функцијата $e:\mathbb{N}\to\mathbb{C}$ е определена со

$$e(n) = \begin{cases} 1, & \text{ако } n = 1, \\ 0, & \text{ако } n \neq 1. \end{cases}$$

Доказ. а) Нека f и g се аритметички функции. Тогаш

$$(f*g)(n) = \sum_{d|n} f(d)g(\tfrac{n}{d}) = \sum_{d_1|n} f(\tfrac{n}{d_1})g(d_1) = (g*f)(n),$$

бидејќи ако d се менува во множеството делители на n, тогаш $d_1 = \frac{n}{d}$ се менува во множеството делители на n и обратно.

Нека f, g и h се аритметички функции. Тогаш за секој $n\in\mathbb{N}$ важи

$$(f*(g*h))(n) = \sum_{a|n} f(a)(g*h)(\tfrac{n}{a}) = \sum_{a|n} f(a)\sum_{b|\frac{n}{a}} g(b)h(\tfrac{n}{ab}) = \sum_{abc=n} f(a)g(b)h(c)$$

$$((f*g)*h)(n) = \sum_{c|n}(f*g)(\tfrac{n}{c})h(c) = \sum_{c|n} h(c)\sum_{b|\frac{n}{c}} g(b)f(\tfrac{n}{bc}) = \sum_{abc=n} f(a)g(b)h(c),$$

па затоа $(f*g)*h = f*(g*h)$.

б) За секој $n\in\mathbb{N}$ важи

$$(e*f)(n) = \sum_{d|n} e(d)f(\tfrac{n}{d}) = f(n),$$

па затоа $f*e = e*f = f$. ■

3.5. Теорема. Нека f е аритметичка функција. Ако $f(1)\neq 0$, тогаш постои единствена аритметичка функција g таква што $f*g = e$.

Доказ. Нека f е аритметичка функција таква што $f(1)\neq 0$.

Индуктивно ќе конструираме аритметичка функција g за која важи

$$(f*g)(n) = e(n), \text{ за секој } n\in\mathbb{N}.$$

За $n=1$ имаме $f(1)g(1) = (f*g)(1) = e(1) = 1$, па затоа $g(1) = \frac{1}{f(1)}$.

Нека $n>1$ и да претпоставиме дека $g(1), g(2), ..., g(n-1)$ се еднозначно определени така што важи $(f*g)(k) = e(k)$ за $k = 1,2,...,n-1$. Тогаш

$$f(1)g(n) + \sum_{\substack{d|n \\ d>1}} f(d)g(\tfrac{n}{d}) = \sum_{d|n} f(d)g(\tfrac{n}{d}) = (f*g)(n) = e(n) = 0,$$

па затоа

$$g(n) = -\frac{1}{f(1)} \sum_{\substack{d|n \\ d>1}} f(d) g(\tfrac{n}{d}),$$

што значи дека $g(n)$ е еднозначно определен. Конечно, од принципот на математичка индукција следува дека постои единствена аритметичка функција g таква што $f * g = e$. ■

3.6. Дефиниција. Нека f е аритметичка функција таква што $f(1) \neq 0$. Единствената аритметичка функција g таква што $f * g = e$ ја нарекуваме *конволуциска инверзија* на f.

Притоа, ја користиме ознаката $g = f^{-1}$.

3.7. Коментар. Во забелешка 1.2. а) видовме дека за секоја мултипликативна функција f важи $f(1) = 1 \neq 0$, што според теорема 3.5 значи дека секоја мултипликативна функција f има конволуциска инверзија.

4. ФУНКЦИЈА НА МЕБИУС

4.1. Дефиниција. Функција $\mu : \mathbb{N} \to \mathbb{R}$ определена со

$$\mu(n) = \begin{cases} 1, & n = 1 \\ 0, & \text{ако } n \text{ е делив со квадрат на природен број поголем од 1,} \\ (-1)^r, & \text{ако } n \text{ е производ на } r \text{ различни прости броеви,} \end{cases}$$

за $n \in \mathbb{N}$ ја нарекуваме *функција на Мебиус*.

4.2. Теорема. Функцијата на Мебиус е мултипликативна.

Доказ. Нека m и n се заемно прости броеви. Ако $m = 1$ или $n = 1$, тогаш равенството $\mu(mn) = \mu(m)\mu(n)$ е исполнето, бидејќи $\mu(1) = 1$. Ако $m > 1, n > 1$ и барем еден од броевите m и n се дели со квадрат на природен број поголем од 1, тогаш равенството е исполнето бидејќи $\mu(mn) = 0$ и $\mu(m) = 0$ или $\mu(n) = 0$. Нека $m = p_1 p_2 ... p_r$ и $n = q_1 q_2 ... q_s$, каде $p_1, p_2, ..., p_r, q_1, q_2, ... q_s$ се различни прости броеви. Тогаш $\mu(mn) = (-1)^{r+s} = (-1)^r (-1)^s = \mu(m)\mu(n)$.

Конечно, од претходно изнесеното следува дека функцијата μ е мултипликативна. ■

4.3. Теорема. Ако $f : \mathbb{N} \to \mathbb{R}$ е мултипликативна функција, тогаш

$$\sum_{d|n}\mu(d)f(d)=(1-f(p_1))(1-f(p_2))...(1-f(p_r)),$$

каде $n=p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}$ е каноничното претставување на природниот број $n>1$.

Доказ. Функциите f и μ се мултипликативни, па затоа функцијата $\mu(n)f(n)$ е мултипликативна и од последица 1.4 следува

$$\sum_{d|n}\mu(d)f(d)=\prod_{i=1}^{r}(1+\mu(p_i)f(p_i))(1+\mu(p_i^2)f(p_i^2))...(1+\mu(p_i^{\alpha_i})f(p_i^{\alpha_i})).$$

Но,

$$\begin{aligned}(1+\mu(p_i)f(p_i))(1+\mu(p_i^2)f(p_i^2))...(1+\mu(p_i^{\alpha_i})f(p_i^{\alpha_i}) &= \\ =(1+(-1)f(p_i))(1+0\cdot f(p_i^2))...(1+0\cdot f(p_i^{\alpha_i}) &\\ =1-f(p_i),&\end{aligned}$$

па затоа точно е равенството (1). ■

4.4. Теорема. Нека f е мултипликативна функција и нека $F(n)=\sum_{d|n}f(d)$. Тогаш за секој $N\in\mathbb{N}$ важи

$$\sum_{n=1}^{N}F(n)=\sum_{k=1}^{N}f(k)[\tfrac{N}{k}].$$

Доказ. Имаме

$$\sum_{n=1}^{N}F(n)=\sum_{n=1}^{N}\sum_{d|n}f(d). \qquad (1)$$

Нека $k\le N$ е даден природен број. Тогаш $f(k)$ се појкавува во $\sum_{d|n}f(d)$ ако и само ако $k\mid n$. Бројот на појавувања на $f(k)$ од десната страна на (1) е еднаков на бројот на броевите од множеството $\{1,2,...,N\}$ кои се деливи со k и овој број е еднаков на $[\frac{N}{k}]$. Според тоа,

$$\sum_{n=1}^{N}F(n)=\sum_{n=1}^{N}\sum_{d|n}f(d)=\sum_{k=1}^{N}f(k)[\tfrac{N}{k}]. \blacksquare$$

4.5. Последица. За секој $N\in\mathbb{N}$ важи

$$\sum_{n=1}^{N}\tau(n)=\sum_{n=1}^{N}[\tfrac{N}{n}].$$

Доказ. Имаме $\tau(n)=\sum_{d|n}1$, па затоа тврдењето следува од претходната теорема применета на мултипликативната функција $f(n)=1$ за $n\in\mathbb{N}$. ■

4.6. Последица. За секој $N \in \mathbb{N}$ важи

$$\sum_{n=1}^{N} \sigma(n) = \sum_{n=1}^{N} n[\tfrac{N}{n}].$$

Доказ. Имаме $\sigma(n) = \sum_{d|n} d$, па затоа тврдењето следува од претходната теорема применета на мултипликативната функција $f(n) = n$ за $n \in \mathbb{N}$. ■

4.7. Последица. За секој $n \in \mathbb{N}$ важи

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{ако } n = 1, \\ 0, & \text{ако } n > 1. \end{cases}$$

Доказ. За $n = 1$ равенството следува од дефиницијата на μ. Нека $n > 1$. Доволно е да претпоставиме дека $n = p_1 p_2 ... p_r$. Во спротивно $\mu(n) = 0$. Функцијата $f(n) = 1$ е мултипликативна и важи $f(p) = 1$, за секој прост број p. Сега, од теорема 4.3 следува

$$\sum_{d|n} \mu(d) = \sum_{d|n} \mu(d) f(d) = (1 - f(p_1))(1 - f(p_2))...(1 - f(p_r))$$
$$= (1-1) \cdot (1-1)...(1-1) = 0. \blacksquare$$

4.8. Последица. За секој $N \in \mathbb{N}$ важи

$$\sum_{n=1}^{N} \mu(n)[\tfrac{N}{n}] = 1.$$

Доказ. Ако во теорема 4.4 земеме $f(n) = \mu(n)$ и ја примениме последица 4.7, добиваме

$$\sum_{n=1}^{N} \mu(n)[\tfrac{N}{n}] = \sum_{n=1}^{N} \sum_{d|n} \mu(d) = \mu(1) + \sum_{n=2}^{N} \sum_{d|n} \mu(d) = \mu(1) = 1. \blacksquare$$

4.9. Последица. За секој $N \in \mathbb{N}$ важи

$$|\sum_{n=1}^{N} \frac{\mu(n)}{n}| \le 1.$$

Доказ. Од последица 4.8 последователно добиваме

$$\sum_{n=1}^{N} \mu(n)(\tfrac{N}{n} - \{\tfrac{N}{n}\}) = 1,$$
$$\sum_{n=1}^{N} \mu(n) \tfrac{N}{n} = 1 + \sum_{n=1}^{N} \mu(n)\{\tfrac{N}{n}\} = 1 + \{N\} + \sum_{n=2}^{N} \mu(n)\{\tfrac{N}{n}\},$$
$$N|\sum_{n=1}^{N} \frac{\mu(n)}{n}| \le 1 + \{N\} + \sum_{n=2}^{N} \{\tfrac{N}{n}\} \le 1 + \{N\} + \sum_{n=2}^{N} 1 = 1 + 0 + N - 1 = N,$$

од каде следува бараното неравенство. ■

4.10. Теорема (Мебиусова инверзна формула). Нека $f:\mathbb{N}\to\mathbb{N}$ е произволна мултипликативна функција и

$$F(n)=\sum_{d|n} f(d)$$

е нејзината функција сума. Тогаш

$$f(n)=\sum_{d|n} F(d)\mu(\tfrac{n}{d}). \tag{1}$$

Формулата (1) ја нарекуваме *Мебиусова инверзна формула*.

Доказ. Имаме

$$\sum_{d|n} F(d)\mu(\tfrac{n}{d})=\sum_{d|n}\mu(\tfrac{n}{d})(\sum_{t|d} f(t))=\sum_{d|n}\sum_{t|d} f(t)\mu(\tfrac{n}{d}).$$

Нека t е фиксиран делител на n. Од сите собирци во горниот збир, во кои фигурира t, пред заграда го вадиме $f(t)$. Во заградата остануваат сите собирци од видот $\mu(\frac{n}{d})$, каде d е делител на n и d се дели со t. Нека $d=tk$, $k\in\mathbb{N}$. Тогаш $\frac{n}{d}=\frac{\frac{n}{t}}{k}$ и условот $d\mid n$ е еквивалентен на условот $k\mid\frac{n}{t}$. Значи, во заградите остануваат сите собирци од видот $\mu(\frac{\frac{n}{t}}{k})$, за кои $k\mid\frac{n}{t}$. Според тоа, коефициентот пред $f(t)$ е

$$\sum_{k|\frac{n}{t}}\mu(\tfrac{\frac{n}{t}}{k})=\sum_{l|\frac{n}{t}}\mu(l),$$

при што искористивме, дека ако k се менува во делителите на $\frac{n}{t}$, тогаш бројот $l=\frac{\frac{n}{t}}{k}$ повторно се менува во делителите на $\frac{n}{t}$. Но, од последица 4.7 следува, дека

$$\sum_{l|\frac{n}{t}}\mu(l)=\begin{cases}1, & \text{ако } t=n,\\ 0, & \text{ако } t<n.\end{cases}$$

Значи,

$$\sum_{d|n} F(d)\mu(\tfrac{n}{d})=\sum_{t|n} f(t)(\sum_{l|\frac{n}{t}}\mu(l))=\sum_{t|n,\,t<n} f(t)\cdot 0+f(n)\cdot 1=f(n).$$ ■

4.11. Теорема. Нека $f:\mathbb{N}\to\mathbb{N}$ е произволна мултипликативна функција и

$$F(n)=\prod_{d|n} f(d).$$

Тогаш

$$f(n)=\prod_{d|n}(F(\tfrac{n}{d}))^{\mu(d)}.$$

Доказ. Како и во доказот на теорема 4.10, за произволен t ги разгледуваме собирците на кои $\mu(d)$ е степен. Со аналогни размислувања добиваме

$$\prod_{d|n}(F(\tfrac{n}{d}))^{\mu(d)} = \prod_{d|n}(\prod_{t|\frac{n}{d}} f(t))^{\mu(d)} = (\prod_{t|n} f(t))^{\sum_{d|\frac{n}{t}}\mu(d)} = f(n)\ .\ \blacksquare$$

4.12. Теорема. Нека f е аритметичка функција и F е нејзината функција сума. Ако F е мултипликативна функција, тогаш функцијата f е мултипликативна.

Доказ. Нека $m,n\in\mathbb{N}$ се такви што $(m,n)=1$ и нека d е делител на mn. Тогаш $d=ab$, каде $a\,|\,m, b\,|\,n$ и $(a,b)=1$. Сега, од Мебиусовата инверзна формула следува

$$\begin{aligned} f(mn) &= \sum_{d|mn} F(\tfrac{mn}{d})\mu(d) = \sum_{a|m,b|n} F(\tfrac{mn}{ab})\mu(ab) \\ &= \sum_{a|m,b|n} F(\tfrac{m}{a})F(\tfrac{n}{b})\mu(a)\mu(b) \\ &= (\sum_{a|m} F(\tfrac{m}{a})\mu(a))(\sum_{b|n} F(\tfrac{n}{b})\mu(b)) = f(m)f(n), \end{aligned}$$

што значи дека функцијата f е мултипликативна. $\blacksquare$

4.13. Пример. а) Докажи дека за секој природен број n важи

$$\sum_{d|n}\mu(d)\tau(d) = (-1)^k,$$

каде $k=\nu(n)$ е бројот на различните прости делители на n.

б) Ако $n=p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$ е каноничната факторизација на природниот број n, докажи дека

$$\sum_{d|n}\mu(d)\sigma(d) = (-1)^k\, p_1p_2...p_k\,.$$

Решение. а) Равенството непосредно следува од теоремата 4.3, применета на мултипликативната функција $f(n)=\tau(n)$.

б) Равенството непосредно следува од теоремата 4.3, применета на мултипликативната функција $f(n)=\sigma(n)$. $\blacksquare$

4.14. Пример. а) Докажи дека за секој природен број n важи

$$\sum_{d|n}\mu(\tfrac{n}{d})\tau(d) = 1.$$

б) Докажи дека за секој прирдоен број n важи

$$\sum_{d|n} \mu(\tfrac{n}{d})\sigma(d) = n .$$

Решение. а) Равенството непосредно следува од Мебиусовата инверзна формула, применета на мултипликативната функција $f(n)=1$ чија функција сума е $\tau(n)$.

б) Равенството непосредно следува од Мебиусовата инверзна формула, применета на мултипликативната функција $f(n)=n$ чија функција сума е $\sigma(n)$.

5. ОЈЛЕРОВА ФУНКЦИЈА

5.1. Дефиниција. За секој природен број n со $\varphi(n)$ да го означиме бројот од сите природни броеви m такви што $m \le n$ и $(m,n)=1$. Аритметичката функција φ ја нарекуваме *Ојлерова функција*.

Јасно, $\varphi(1)=1$ и $\varphi(n)=n-1$ ако и само ако n е прост број.

Вредностите на функцијата φ за првите 17 природни броеви се дадени во следнава табела:

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$\varphi(m)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16

Забележуваме дека $\varphi(12)=4=2\cdot 2=\varphi(3)\varphi(4)$, што укажува на мултипликативноста на функцијата φ, која покасно ќе ја докажеме.

5.2. Теорема (Гаус). Ако $n \in \mathbb{N}$, тогаш $\sum_{d|n} \varphi(d) = n$, при што сумирањето е по сите позитивни делители на n.

Доказ. Нека d е позитивен делител на n и со $C(d)$ да го означиме множеството од сите природни броеви $m, m \le n$ такви што $(m,n)=d$. Ако $d \ne d'$, тогаш бидејќи цел број m со бројот n може да има најмногу еден најголем заеднички делител добиваме дека множествата $C(d)$ и $C(d')$ немаат заеднички елементи. Понатаму, множеството $C(d)$ е еднакво на множеството од сите природни броеви m, $m \le n$ такви што $(\frac{m}{d},\frac{n}{d})=1$, што значи дека тоа ги содржи природните броеви $\frac{m}{d}$ кои се помали или еднакви на $\frac{n}{d}$ и се заемно прости со $\frac{n}{d}$, па затоа бројот на елементите на множеството $C(d)$ е еднаков на $\varphi(\frac{n}{d})$. Но, унијата на сите овие множества е еднаква на множеството природни броеви помали или еднакви на n, па

затоа $\sum_{d|n}\varphi(\frac{n}{d})=n$. Конечно, бидејќи за секој d делител на n бројот $\frac{n}{d}$ е делител на n и обратно, од последното равенство следува

$$n=\sum_{d|n}\varphi(\frac{n}{d})=\sum_{d|n}\varphi(d)\ .\ \blacksquare$$

5.3. Теорема. Функцијата φ е мултипликативна.

Доказ. Според теоремата 5.2. функцијата $F(n)=n$ е функција сума на Ојлеровата функција φ. Но, функцијата F е мултипликативна, па од теоремата 4.12 следува дека Ојлеровата функција φ е мултипликативна. ■

5.4. Теорема. Ако $n=p_1^{a_1}p_2^{a_2}...p_k^{a_k}$ е каноничниот запис на број n, тогаш

$$\begin{aligned}\varphi(n)&=p_1^{a_1}p_2^{a_2}...p_k^{a_k}(1-\tfrac{1}{p_1})(1-\tfrac{1}{p_2})...(1-\tfrac{1}{p_k})\\&=n(1-\tfrac{1}{p_1})(1-\tfrac{1}{p_2})...(1-\tfrac{1}{p_k}).\end{aligned}$$

Доказ. Единствени броеви меѓу 1 и p^a кои не се заемно прости со p се броевите што се деливи со p, а такви се: $p,2p,3p,...,p^{a-1}p$ и нив ги има p^{a-1}. Според тоа,

$$\varphi(p^a)=p^a-p^{a-1}=p^a(1-\tfrac{1}{p})\ .$$

Сега, од теорема 5.3. следува

$$\begin{aligned}\varphi(n)&=\varphi(p_1^{a_1}p_2^{a_2}...p_k^{a_k})=\varphi(p_1^{a_1})\varphi(p_2^{a_2})...\varphi(p_k^{a_k})\\&=p_1^{a_1}(1-\tfrac{1}{p_1})p_2^{a_2}(1-\tfrac{1}{p_2})...p_k^{a_k}(1-\tfrac{1}{p_k})\\&=p_1^{a_1}p_2^{a_2}...p_k^{a_k}(1-\tfrac{1}{p_1})(1-\tfrac{1}{p_2})...(1-\tfrac{1}{p_k})\\&=n(1-\tfrac{1}{p_1})(1-\tfrac{1}{p_2})...(1-\tfrac{1}{p_k}),\end{aligned}$$

што и требаше да се докаже. ■

5.5. Последица. Ако $n>2, n\in\mathbb{N}$, тогаш $\varphi(n)$ е парен број.

Доказ. Нека $n=2^k m$, $k>1$ и m е непарен број. Тогаш

$$\varphi(n)=\varphi(2^k m)=\varphi(2^k)\varphi(m)=2^{k-1}\varphi(m)\ ,$$

па затоа $\varphi(n)$ е парен број. Понатаму, ако $n=p^k m$, p е непарен прост број, m е непарен број и $(p,m)=1$, тогаш

$$\varphi(n)=\varphi(p^k m)=\varphi(p^k)\varphi(m)=(p^k-p^{k-1})\varphi(m)=p^{k-1}(p-1)\varphi(m)$$

па затоа $\varphi(n)$ е парен број. ■

5.6. Последица. За секој природен број n важи

$$\varphi(n) = n\sum_{d|n}\frac{\mu(d)}{d}.$$

Доказ. *Прв начин*. Очигледно за $n=1$ равенството (1) е исполнето. Нека $n>1$ и $n = p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}$ е каноничното претставување на n. Функцијата $f(n)=\frac{1}{n}$ е мултипликативна, па од теоремата 4.3 следува, дека

$$\sum_{d|n}\frac{\mu(d)}{d} = (1-\tfrac{1}{p_1})(1-\tfrac{1}{p_2})...(1-\tfrac{1}{p_r})$$

$$= \tfrac{1}{n}n(1-\tfrac{1}{p_1})(1-\tfrac{1}{p_2})...(1-\tfrac{1}{p_r}) = \frac{\varphi(n)}{n}.$$

Втор начин. Според теоремата 5.2 важи $\sum_{d|n}\varphi(d)=n$. Сега, од теоремата 4.10 следува равенството $\varphi(n)=\sum_{d|n}\mu(d)\frac{n}{d}$. ■

5.7. Лема. За секој природен број $n>2$ важи

$$\varphi(n) > \frac{n}{4\ln n}.$$

Доказ. Функцијата $f(n)=\frac{\sigma(n)\varphi(n)}{n^2}$ е мултипликативна. Понатаму, ако p е прост број, тогаш за секој $j\in\mathbb{N}$ важи:

$$f(p^j) = \frac{(p^{j+1}-1)p^{j-1}(p-1)}{(p-1)p^{2j}} = 1-\frac{1}{p^{j+1}} \geq 1-\frac{1}{p^2}. \qquad (1)$$

Според тоа, ако $n = p_1^{a_1}p_2^{a_2}...p_k^{a_k}$ е каноничното претставување на n, тогаш бидејќи f е мултипликативна од (1) следува

$$f(n) = f(p_1^{a_1}p_2^{a_2}...p_k^{a_k}) = f(p_1^{a_1})f(p_2^{a_2})...f(p_k^{a_k})$$

$$\geq (1-\tfrac{1}{p_1^2})(1-\tfrac{1}{p_2^2})...(1-\tfrac{1}{p_k^2})$$

$$> \prod_{m=2}^{\infty}(1-\tfrac{1}{m^2}) = \prod_{m=2}^{\infty}\frac{(m-1)(m+1)}{m^2} = \frac{1}{2}.$$

Значи, $\varphi(n) > \frac{n^2}{2\sigma(n)}$. Но, од лемата 2.4 следува дека за секој природен број $n\geq 2$ важи $\frac{1}{\sigma(n)} > \frac{1}{n(1+\ln n)}$, па затоа за секој природен број $n>2$ важи

$$\varphi(n) > \frac{n^2}{2\sigma(n)} > \frac{n^2}{2n(1+\ln n)} = \frac{n}{2(1+\ln n)} > \frac{n}{4\ln n}. \blacksquare$$

5.8. Пример. Ако n е парен совршен број, тогаш $\varphi(n) = 2^{p-1}(2^{p-1}-1)$, за некој прост број p. Докажи!

Решение. Парен природен број n е совршен ако и само ако има облик

$$n = 2^{p-1}(2^p - 1),$$

каде $2^p - 1$ е Мерсенов прост број. Според тоа,

$$\begin{aligned}\varphi(n) &= \varphi(2^{p-1})\varphi(2^p - 1) = 2^{p-2}(2^p - 1 - 1) \\ &= 2^{p-2} \cdot 2(2^{p-1} - 1) = 2^{p-1}(2^{p-1} - 1),\end{aligned}$$

што и требаше да се докаже. ■

5.9. Пример. Докажи дека $\varphi(n) \geq \frac{\sqrt{n}}{\sqrt{2}}$ за секој природен број n.

Решение. Нека $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ е канонична факторизација на бројот n каде $p_1 < p_2 < \ldots < p_k$ се прости броеви и $\alpha_i \geq 1$ за $i = 1, 2, \ldots, k$. Имаме

$$\varphi(n) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \ldots p_k^{\alpha_k - 1}(p_1 - 1)(p_2 - 1)\ldots(p_k - 1).$$

За $p_i \geq 3$ имаме $p_i^2 \geq 3p_i$, т.е. $p_i^2 + 1 > 3p_i$, па затоа $(p_i - 1)^2 > p_i$, односно $p_i - 1 > \sqrt{p_i}$. Ќе разгледаме два случаја.

Ако $p_1 = 2$, тогаш бидејќи $\alpha_i - \frac{1}{2} \geq \frac{\alpha_i}{2}$ за секој природен број α_i добиваме

$$\begin{aligned}\varphi(n) &= 2^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \ldots p_k^{\alpha_k - 1}(2 - 1)(p_2 - 1)\ldots(p_k - 1) \\ &> 2^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \ldots p_k^{\alpha_k - 1} \sqrt{p_2}\sqrt{p_3}\ldots\sqrt{p_k} = \frac{1}{\sqrt{2}} \cdot 2^{\alpha_1 - \frac{1}{2}} p_2^{\alpha_2 - \frac{1}{2}} \ldots p_k^{\alpha_k - \frac{1}{2}} \\ &\geq \frac{1}{\sqrt{2}} \cdot 2^{\frac{\alpha_1}{2}} p_2^{\frac{\alpha_2}{2}} \ldots p_k^{\frac{\alpha_k}{2}} = \frac{1}{\sqrt{2}} \sqrt{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}} = \frac{\sqrt{n}}{\sqrt{2}}.\end{aligned}$$

Ако $p_1 > 2$, тогаш

$$\begin{aligned}\varphi(n) &= p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \ldots p_k^{\alpha_k - 1}(p_1 - 1)(p_2 - 1)\ldots(p_k - 1) \\ &\geq p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \ldots p_k^{\alpha_k - 1} \sqrt{p_1}\sqrt{p_2}\ldots\sqrt{p_k} = p_1^{\alpha_1 - \frac{1}{2}} p_2^{\alpha_2 - \frac{1}{2}} \ldots p_k^{\alpha_k - \frac{1}{2}} \\ &\geq p_1^{\frac{\alpha_1}{2}} p_2^{\frac{\alpha_2}{2}} \ldots p_k^{\frac{\alpha_k}{2}} = \sqrt{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}} = \sqrt{n} > \frac{\sqrt{n}}{\sqrt{2}},\end{aligned}$$

што и требаше да се докаже. ■

5.10. Пример (Шинцел). Докажи дека постојат бесконечно многу природни броеви k такви што равенката $\varphi(n) = k$ нема решение.

Решение. Нека $k = 2 \cdot 7^m$, $m \geq 1$. Ако $n = p_1^{a_1} p_2^{a_2} \ldots p_t^{a_t}$, тогаш

$$\begin{aligned}\varphi(n) &= p_1^{a_1} p_2^{a_2} \ldots p_t^{a_t}(1 - \tfrac{1}{p_1})(1 - \tfrac{1}{p_2})\ldots(1 - \tfrac{1}{p_t}) \\ &= p_1^{a_1 - 1} p_2^{a_2 - 1} \ldots p_t^{a_t - 1}(p_1 - 1)(p_2 - 1)\ldots(p_t - 1).\end{aligned}$$

Ако најмалку два од простите броеви $p_1, p_2, ..., p_t$ се непарни, тогаш $4 \mid \varphi(n)$, па затоа $\varphi(n) \neq k$. Ако $n = 2^a p^b$, каде $p \geq 3$, тогаш

$$\varphi(n) = 2^a p^b (1-\tfrac{1}{2})(1-\tfrac{1}{p}) = 2^{a-1} p^{b-1}(p-1)$$

и лесно се покажува дека и во овој случај $\varphi(n) \neq k$. ■

5.11. Пример. Нека $n > 4$ е сложен број таков што $n \mid \varphi(n)\sigma(n)+1$. Докажи дека n има најмалку три различни прости делители.

Решение. За секој сложен број $n > 4$ бројот $\varphi(n)$ е парен, па затоа $\varphi(n)\sigma(n)+1$ е непарен број. Сега од $n \mid \varphi(n)\sigma(n)+1$ следува дека n е непарен број. Ќе докажеме дека во каноничната факторизација на n степенот на секој прост делител p е еднаков на еден.

Нека претпоставиме спротивно, т.е. дека степенот на некој прост делител p е најмалку 2, односно $n = p^{\alpha} a, \alpha \geq 2$. Од $p \mid n$ следува $p \mid \varphi(n)\sigma(n)+1$. Имаме, $\varphi(n) = p^{\alpha-1}(p-1)q$. Јасно $p \mid \varphi(n)$. Сега, од $p \mid \varphi(n)$ и $p \mid \varphi(n)\sigma(n)+1$ следува $p = 1$, што е противречност. Значи, $\alpha = 1$.

Сега нека претпоставиме дека n има најмногу два прости делители, т.е. нека $n = pq$. Имаме, $\varphi(n) = (p-1)(q-1)$ и $\sigma(n) = (1+p)(1+q)$, па затоа

$pq \mid (p-1)(q-1)(p+1)(q+1)+1 = p^2q^2 - p^2 - q^2 + 2$, т.е. $\frac{p^2+q^2-2}{pq} = k \in \mathbb{Z}$.

Нека (a,b) е пар од природни броеви за кои важи $a^2 + b^2 - 2 = kab$ и притоа збирот $a+b$ е најмал. Без ограничување на општоста можеме да земеме дека $a \geq b$. Ја разгледуваме квадратната равенка $a^2 - kab + b^2 - 2 = 0$ по непозната a. Од Виетовите формули следува дека $\frac{b^2-2}{a}$ е решение на оваа равенка. Оттука $(\frac{b^2-2}{a}, b)$ е нов пар кој е решение на равенката. Од минималноста на $a+b$ следува дека $a+b \leq \frac{b^2-2}{a}+b$, од каде следува дека $a < b$, што е противречност.

Конечно, од добиената противречност следува дека n има најмалку три различни прости делители. ■

5.12. Пример. Докажи, дека $\varphi(n)+\sigma(n) \geq 2n$, при што знак за равенство важи ако и само ако $n = 1$ или n е прост број.

Решение. Нека $n = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$. Имаме

$$\varphi(n)+\sigma(n) = p_1^{a_1} p_2^{a_2} ... p_k^{a_k} (1-\tfrac{1}{p_1})(1-\tfrac{1}{p_2})...(1-\tfrac{1}{p_k}) + \frac{p_1^{a_1+1}-1}{p_1-1} \cdot \frac{p_2^{a_2+1}-1}{p_2-1} \cdot ... \cdot \frac{p_k^{a_k+1}-1}{p_k-1}$$

$$= n[(1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_k}) + \frac{(1-p_1^{-(a_1+1)})(1-p_2^{-(a_2+1)})...(1-p_k^{-(a_k+1)})}{(1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_k})}]$$

$$\geq 2n\sqrt{(1-p_1^{-(a_1+1)})(1-p_2^{-(a_2+1)})...(1-p_k^{-(a_k+1)})} \geq 2n,$$

при што знак за равенство важи ако и само ако $n=1$ или n е прост број. ■

5.13. Пример. Докажи, дека

$$\sum_{k|n} \varphi(k)\sigma(\frac{n}{k}) = n\tau(n). \qquad (2)$$

Решение. Функциите $\varphi(n)$ и $\sigma(n)$ се мултипликативни, па затоа левата страна на (2) е мултипликативна функција. Јасно, функцијата $n\tau(n)$ е мултипликативна, па затоа доволно е да докажеме дека (2) важи за броеви од облик $n = p^a$, каде p е прост број и $a \in \mathbb{N}$. Од својствата на функциите φ и σ следува:

$$\sum_{k|p^a} \varphi(k)\sigma(\frac{p^a}{k}) = \sum_{i=0}^{a} \varphi(p^i)\sigma(p^{a-i}) = \sigma(p^a) + \sum_{i=1}^{a} \varphi(p^i)\sigma(p^{a-i})$$

$$= \sigma(p^a) + \sum_{i=1}^{a} (p^i - p^{i-1})(1 + p + ... + p^{a-i})$$

$$= \sigma(p^a) + \sum_{i=1}^{a} (p^a - p^{i-1}) = \sum_{i=0}^{a} p^i + ap^a - \sum_{i=0}^{a-1} p^i$$

$$= (a+1)p^a = p^a\tau(p^a),$$

што и требаше да се докаже. ■

IV ГЛАВА
КОНГРУЕНЦИИ

1. ПОИМ ЗА КОНГРУЕНЦИЈА

1.1. Во претходните разгледувања видовме дека броевите кои што при делење со еден број даваат ист остаток се од посебен интерес во теоријата на броеви. Токму затоа тие биле предмет на истражување на многу знаменити математичари, што довело до поимот конгруенција во множеството на целите броеви, т.е. до методот на конгруенции во множеството на целите броеви. Овој метод е формален аритметички метод заснован на разгледување на својствата на целите броеви кои имаат еднакви остатоци при делење со еден број. Методот прв го разработил германскиот математичар Гаус, но многу резултати биле познати и пред Гаус.

1.2. Дефиниција. Нека $a,b\in\mathbb{Z}$ и $m\in\mathbb{N}$. Ако $m|(a-b)$, тогаш ќе велиме дека бројот a *е конгруентен* со бројот b по модул m и ќе пишуваме $a\equiv b\,(\mathrm{mod}\,m)$.

Ако $m\nmid(a-b)$, тогаш ќе велиме дека бројот a *не е конгруентен* со бројот b по модул m и ќе пишуваме $a\not\equiv b\,(\mathrm{mod}\,m)$.

1.3. Теорема. Нека $a,b\in\mathbb{Z}$ и $m\in\mathbb{N}$. Тогаш:

а) $a\equiv b\,(\mathrm{mod}\,m)$ ако и само ако постои цел број k таков што $a=b+km$,

б) $a\equiv b\,(\mathrm{mod}\,m)$ ако и само ако при делење со m броевите a и b имаат еднакви остатоци,

в) ако $a\equiv b\,(\mathrm{mod}\,m)$ и $d\,|\,m$, тогаш $a\equiv b\,(\mathrm{mod}\,d)$,

г) ако $a\equiv b\,(\mathrm{mod}\,m)$ и $c\neq 0$, тогаш $ac\equiv bc\,(\mathrm{mod}\,mc)$.

Доказ. а) Од дефиницијата 1.2 следува дека $a\equiv b\,(\mathrm{mod}\,m)$ ако и само ако $m|(a-b)$. Понатаму, $m|(a-b)$ ако и само ако постои цел број k таков што $a-b=km$, т.е. постои цел број k таков што $a=b+km$.

б) Нека $a=mp+r$ и $b=mq+s$, $p,q,r,s\in\mathbb{Z}$, $0\le r,s<m$. Тогаш $a\equiv b\,(\mathrm{mod}\,m)$ ако и само ако $m|(a-b)$, што значи ако и само ако

$$m|[(mp+r)-(mq+s)].$$

Според тоа, $a\equiv b\,(\mathrm{mod}\,m)$ ако и само ако $m|[m(p-q)+(r-s)]$.

Значи, $a\equiv b\,(\mathrm{mod}\,m)$ ако и само ако $m|(r-s)$. Но, $-m<r-s<m$, па затоа $a\equiv b\,(\mathrm{mod}\,m)$ ако и само ако $r-s=0$, т.е. ако и само ако $r=s$.

в) Од $a\equiv b\,(\mathrm{mod}\,m)$ следува $m|(a-b)$ и како $d\,|\,m$, следува дека $d|(a-b)$.

Сега, од дефиницијата 1.2 следува дека $a \equiv b (\mathrm{mod}\, d)$.

г) Од $a \equiv b \,(\mathrm{mod}\, m)$ следува $m \mid a-b$. Понатаму, $c \neq 0$ па од $m \mid a-b$ следува $mc \mid (a-b)c = ac-bc$, што според дефиницијата 1.2 значи $ac \equiv bc \,(\mathrm{mod}\, mc)$. ■

1.4. Теорема. Нека $m \in \mathbb{N}$ и $a, b \in \mathbb{Z}$. Тогаш

а) $a \equiv a \,(\mathrm{mod}\, m)$,

б) Ако $a \equiv b \,(\mathrm{mod}\, m)$, тогаш $b \equiv a \,(\mathrm{mod}\, m)$,

в) Ако $a \equiv b \,(\mathrm{mod}\, m)$ и $b \equiv c \,(\mathrm{mod}\, m)$, тогаш $a \equiv c \,(\mathrm{mod}\, m)$.

Доказ. а) Од $a-a=0$, за секој $a \in \mathbb{Z}$ следува $a \equiv a \,(\mathrm{mod}\, m)$, за секој $a \in \mathbb{Z}$.

б) Ако $a \equiv b \,(\mathrm{mod}\, m)$, тогаш $m \mid (a-b)$. Од $b-a = (-1)(a-b)$ следува $m \mid (b-a)$, па од дефиницијата 1.2 заклучуваме дека $b \equiv a \,(\mathrm{mod}\, m)$.

в) Ако $a \equiv b \,(\mathrm{mod}\, m)$ и $b \equiv c \,(\mathrm{mod}\, m)$, тогаш $m \mid (a-b)$ и $m \mid (b-c)$. Според тоа, $m \mid [(a-b)+(b-c)] = a-c$ па затоа $a \equiv c \,(\mathrm{mod}\, m)$. ■

1.5. Теорема. Ако $a \equiv b \,(\mathrm{mod}\, m)$ и $c \equiv d \,(\mathrm{mod}\, m)$, тогаш

$$a+c \equiv b+d \,(\mathrm{mod}\, m),\ a-c \equiv b-d \,(\mathrm{mod}\, m) \text{ и } ac \equiv bd \,(\mathrm{mod}\, m).$$

Доказ. Нека $a \equiv b \,(\mathrm{mod}\, m)$ и $c \equiv d \,(\mathrm{mod}\, m)$. Од дефиниција 1.2 имаме дека $m \mid (a-b)$ и $m \mid (c-d)$. Според тоа

$$m \mid [(a-b)+(c-d)] = (a+c)-(b+d),$$
$$m \mid [(a-b)-(c-d)] = (a-c)-(b-d) \text{ и}$$
$$m \mid [c(a-b)+b(c-d)] = ac-bd,$$

што значи дека

$$a+c \equiv b+d \,(\mathrm{mod}\, m),\ a-c \equiv b-d \,(\mathrm{mod}\, m) \text{ и } ac \equiv bd \,(\mathrm{mod}\, m).$$ ■

1.6. Последица. а) Ако $a \equiv b \,(\mathrm{mod}\, m)$, тогаш

$$a+c \equiv b+c \,(\mathrm{mod}\, m),\ a-c \equiv b-c \,(\mathrm{mod}\, m) \text{ и } ac \equiv bc \,(\mathrm{mod}\, m)$$

за секој $c \in \mathbb{Z}$.

б) Ако $a \equiv b \,(\mathrm{mod}\, m)$, тогаш $a^n \equiv b^n \,(\mathrm{mod}\, m)$ за секој $n \in \mathbb{N}$.

Доказ. Непосредно следува од теоремите 1.4 и 1.5. ■

1.7. Последица (Лагранж). Нека

$$f(x) = a_k x^k + a_{k-1} x^{k-1} + \ldots + a_1 x + a_0,\ a_i \in \mathbb{Z},\ i = 0,1,2,\ldots,k.$$

Ако $a \equiv b \,(\mathrm{mod}\, m)$, тогаш

$$f(a) \equiv f(b) \,(\mathrm{mod}\, m).$$

Доказ. Од последицата 1.6 б) следува $a^t \equiv b^t \pmod m$ за $t = 0,1,...,k$. Сега од последицата 1.6 а) следува

$$a_t a^t \equiv a_t b^t \pmod m \text{ за } t = 0,1,...,k$$

$$a_k a^k + a_{k-1}a^{k-1} + ... + a_1 a + a_0 \equiv a_k b^k + a_{k-1}b^{k-1} + ... + a_1 b + a_0 \pmod m$$

односно $f(a) \equiv f(b) \pmod m$. ■

1.8. Коментар. Да забележиме дека теорема 1.5 всушност покажува дека релацијата $\equiv$ по даден модул е согласна со операциите собирање, одземање и множење на конгруенции.

Меѓутоа, релацијата $\equiv$ не е согласна со релацијата делење на цели броеви (дури и кога последната е дефинирана). Имено, во конгруенцијата $8 \equiv -4 \pmod{12}$ броевите 8 и -4 се деливи со 2 и со 4, меѓутоа ако поделиме со 2, односно со 4 добиваме $4 \equiv -2 \pmod{12}$ односно $2 \equiv -1 \pmod{12}$, што не е точно.

1.9. Теорема. а) Ако $(a,m) = d$, $q = \frac{m}{d}$ и $ab \equiv ac \pmod m$, тогаш $b \equiv c \pmod q$.

б) Ако $(a,m) = 1$ и $ab \equiv ac \pmod m$, тогаш $b \equiv c \pmod m$.

в) Ако $(a,m) = d$, $q = \frac{m}{d}$ и $b \equiv c \pmod q$, тогаш $ab \equiv ac \pmod m$.

Доказ. а) Нека $(a,m) = d$ и $ab \equiv ac \pmod m$. Постојат цели броеви p и q такви што $m = dq$ и $a = dp$, $(p,q) = 1$. Од $ab \equiv ac \pmod m$ следува дека постои $k \in \mathbb{Z}$ таков што $ab = ac + mk$. Ако последното равенство го поделиме со d го добиваме равенството $pb = pc + qk$ од што следува $p(b-c) = qk$. Но, $(p,q) = 1$ од каде следува $q \mid (b-c)$, т.е. $b \equiv c \pmod q$.

б) Следува од тврдењето под а) за $d = 1$.

в) Бидејќи $(a,m) = d$, добиваме $a = dp$ и $m = dq$, за некои цели броеви p и q. Понатаму, од $b \equiv c \pmod q$ следува дека постои $k \in \mathbb{Z}$ таков што $b = c + qk$. Последното равенство го множиме со a и добиваме дека $ab = ac + aqk$ и ако замениме за $a = dp$ добиваме дека

$$ab = ac + (dq)(pk) = ac + m(pk),$$

односно $ab - ac = m(pk)$. Конечно, $m \mid (ab-ac)$, т.е. $ab \equiv ac \pmod m$. ■

1.10. Теорема. Ако $a \equiv b \pmod m$, $a \equiv b \pmod n$ и $[m,n] = k$, тогаш

$$a \equiv b \pmod k.$$

Доказ. Нека $(m,n) = t$. Тогаш $n = pt$ и $m = qt$, каде $(p,q) = 1$ и $[m,n] = pqt$. Од $n \mid (a-b)$ и $m \mid (a-b)$ следува дека $pt \mid (a-b)$ и $qt \mid (a-b)$, т.е. $a - b = ptr$ и

$a-b=qts$. Значи, $ptr=qts$, т.е. $pr=qs$ и бидејќи $(p,q)=1$ добиваме $p\mid s$ т.е. $s=pu$. Со замена во $a-b=qts$ добиваме $a-b=qtpu$, т.е. $pqt\mid(a-b)$. Но, $[m,n]=pqt=k$, па затоа $a\equiv b\pmod k$. ■

1.11. Теорема. Ако $x\equiv y(\mathrm{mod}\,m)$, тогаш $(x,m)=(y,m)$.

Доказ. Од $x\equiv y(\mathrm{mod}\,m)$ следува дека постои $z\in\mathbb{Z}$ таков, што $y-x=mz$. Бидејќи $(x,m)\mid x$ и $(x,m)\mid m$, добиваме $(x,m)\mid y$, што значи $(x,m)\mid(y,m)$. На потполно ист начин се добива $(y,m)\mid(x,m)$, па затоа $(x,m)=(y,m)$. ■

1.12. Теорема. Нека $a\in\mathbb{Z}$ и $m,n\in\mathbb{N}$. Тогаш $(a^m-1,a^n-1)=a^{(m,n)}-1$.

Доказ. Нека $d=(a^m-1,a^n-1)$ и $(m,n)=k$, т.е. $m=km_1, n=kn_1$. Тогаш

$$a^m-1=(a^k-1)(a^{k(m_1-1)}+\ldots+a^k+1),$$
$$a^n-1=(a^k-1)(a^{k(n_1-1)}+\ldots+a^k+1),$$

па затоа $a^k-1=a^{(m,n)}-1$ е делител на $d=(a^m-1,a^n-1)$. Од друга страна, постојат природни броеви x и y такви што $k=mx-ny$, па како $a^m\equiv 1(\mathrm{mod}\,d)$ и $a^n\equiv 1(\mathrm{mod}\,d)$, добиваме $1\equiv a^{mx}\equiv a^{nx}\cdot a^k\equiv a^k(\mathrm{mod}\,d)$. Значи, $d=(a^m-1,a^n-1)$ е делител на $a^k-1=a^{(m,n)}-1$, што повлекува

$$(a^m-1,a^n-1)=a^{(m,n)}-1.\ ■$$

1.13. Последица. Нека $a,b\in\mathbb{Z}$, $(a,b)=1$ и $m,n\in\mathbb{N}$. Тогаш

$$(a^m-b^m,a^n-b^n)=a^{(m,n)}-b^{(m,n)}.$$

Доказ. Доказот е аналоген на доказот на теоремата 1.12. Деталите ги оставаме на читателот за вежба. ■

1.14. Пример. Докажи, дека $41\mid(1+3+3^2+\ldots+3^{1991})$.

Решение. Да забележиме дека

$$1+3+3^2+\ldots+3^{1991}=(1+3+3^2+\ldots+3^7)(1+3^8+3^{12}+\ldots+3^{1984}). \qquad (1)$$

Од друга страна имаме

$$1\equiv 1(\mathrm{mod}\,41),\ 3\equiv 3(\mathrm{mod}\,41),\ 3^2\equiv 9(\mathrm{mod}\,41),\ 3^3\equiv 27(\mathrm{mod}\,41),$$
$$3^4\equiv -1(\mathrm{mod}\,41),\ 3^5\equiv -3(\mathrm{mod}\,41),\ 3^6\equiv -9(\mathrm{mod}\,41)\ \text{и}\ 3^7\equiv -27(\mathrm{mod}41).$$

Значи,

$$1+3+3^2+\ldots+3^7\equiv 0(\mathrm{mod}\,41). \qquad (2)$$

Конечно, од (1) и (2) следува $41|(1+3+3^2+...+3^{1991})$. ■

1.15. Пример. Природните броеви m и n се такви што бројот $m-n$ е непарен. Докажи дека бројот $(m+3n)(5m+7n)$ не е точен квадрат.

Решение. Нека го претпоставиме спротивното и $d=(m,n)$. Тогаш $m=dx$, $n=dy$, $(x,y)=1$ и

$$(m+3n)(5m+7n)=d^2(x+3y)(5x+7y).$$

Бидејќи $m-n$ е непарен, истото важи и за $x-y$. Нека c е најголемиот заеднички делител на $x+3y$ и $5x+7y$. Броевите $x+3y$ и $5x+7y$ се непарни, па затоа и c е непарен. Јасно, c е делител на броевите

$$3(5x+7y)-7(x+3y)=8x \text{ и } 5(x+3y)-(5x+7y)=8y,$$

па затоа тој е делител на x и y. Но, $(x,y)=1$, па затоа $c=1$.

Сега од претпоставката следува дека $x+3y=a^2$ и $5x+7y=b^2$, каде a и b се непарни природни броеви. Бидејќи броевите a и b се непарни добиваме

$$b^2-a^2\equiv 0(\mathrm{mod}\,8).$$

Од друга страна

$$b^2-a^2=4(x+y),$$

каде $x+y=2x-(x-y)$ е непарен број. Значи, 8 не е делител на b^2-a^2 што е противречност. Конечно, од добиената противречност следува тврдењето на задачата. ■

1.16. Пример. Нека $p_1<p_2<p_3<p_4$ и $q_1<q_2<q_3<q_4$ се прости броеви такви што $p_4-p_1=8$ и $q_4-q_1=8$. Нека $p_1>5, q_1>5$. Докажи дека $30\mid p_1-q_1$.

Решение. За секој прост број $p>3$ важи $p\equiv\pm 1(\mathrm{mod}\,6)$. Ако $p_1\equiv 1(\mathrm{mod}\,6)$, тогаш $p_4\equiv 3(\mathrm{mod}\,6)$, што не е можно бидејќи p_4 е прост број. Значи, $p_1\equiv -1(\mathrm{mod}\,6)$. Аналогно важи $q_1\equiv -1(\mathrm{mod}\,6)$, па оттука

$$p_1-q_1\equiv 0(\mathrm{mod}\,6). \tag{3}$$

Два од броевите p_1+2, p_1+4, p_1+6 се прости бидејќи се непарни и се наоѓаат меѓу p_1 и $p_4=p_1+8$. Бидејќи $p_1+4\equiv 3(\mathrm{mod}\,6)$ добиваме дека p_1+4 не е прост број. Значи $p_2=p_1+2, p_3=p_1+6$. Аналогно се добива дека $q_2=q_1+2$ и $q_3=q_1+6$.

Ако $p_1\equiv 2(\mathrm{mod}\,5)$, тогаш $p_4\equiv 0(\mathrm{mod}\,5)$ што не е можно. Ако $p_1\equiv 3(\mathrm{mod}\,5)$, тогаш $p_2\equiv 0(\mathrm{mod}\,5)$, а ако $p_1\equiv 4(\mathrm{mod}\,5)$, тогаш $p_3\equiv 0(\mathrm{mod}\,5)$ што исто така не е можно. Значи, $p_1\equiv 1(\mathrm{mod}\,5)$. Аналогно, $q_1\equiv 1(\mathrm{mod}\,5)$. Затоа

$$p_1-q_1\equiv 0(\mathrm{mod}\,5). \tag{4}$$

Од (3) и (4) следува $30 \mid p_1 - q_1$. ■

1.17. Пример. Нека герданот A има 14 бисери, а герданот B има 19 бисери. Докажи дека за секој непарен природен број n постои начин да ги нумерираме сите бисери со броеви од множеството

$$\{n, n+1, ..., n+32\}$$

така што секој број ќе се употреби само еднаш и броевите кои соодветствуваат на соседните бисери се заемно прости.

Решение. Основната идеја на решението е што е можно повеќе да користиме последователни броеви за означување на соседни бисери, бидејќи соседните броеви се заемно прости. Ќе се обидеме од даденото множество на погоден начин да одделиме 14 последователни броеви со кои ќе ги означиме бисерите од герданот A, т.е.

$$n+m, n+m+1, ..., n+m+13$$

(каде бројот $m, 1 \le m \le 18$ дополнително ќе го определиме), додека преостанатите броеви формираат две низи последователни броеви со должина m, односно $19-m$. Тоа се броевите

$$n, n+1, ..., n+m-1, n+m+14, ..., n+32$$

и со нив без да им се менува редоследот ќе ги означиме бисерите од герданот B. Прво да забележиме дека бидејќи n е непарен број за герданот B е исполнет условот $(n, n+32) = (n, 32) = 1$. Според тоа, условите од кои го определуваме бројот m се

$$(n+m, n+m+13) = 1 \text{ и } (n+m-1, n+m+14) = 1.$$

Точни се следниве равенства

$$(n+m, n+m+13) = (n+m, 13) \text{ и}$$
$$(n+m-1, n+m+14) = (n+m-1, 15),$$

па затоа m го определуваме од следниве три услови

1) $m \not\equiv -n \pmod{13}$,
2) $m \not\equiv 1-n \pmod{3}$ и
3) $m \not\equiv 1-n \pmod{5}$.

Меѓутоа, од броевите 1, 2, ..., 18 најмногу два не го задоволуваат првиот услов, точно шест не го задоволуваат вториот услов и најмногу четири не го задоволуваат третиот услов. Според тоа, меѓу нив постои број m_0 кој ги задоволува сите услови. Ако сега ставиме $m = m_0$, тогаш нумерирањата на двата гердана го имаат саканото својство. ■

1.18. Пример. Нека $f_1(x)$ е еднаков на квадратот на збирот на цифрите на природниот број x, а $f_n(x) = f_1(f_{n-1}(x))$. Пресметај $f_{1991}(2^{1990})$.

Решение. Прво да забележиме дека

$$2^{1990} < 8^{700} < 10^{700},$$

па затоа

$$f_1(2^{1990}) < (9\cdot 700)^2 < 5\cdot 10^7 .$$

Оттука следува

$$f_2(2^{1990}) \le (4+7\cdot 9)^2 < 5000$$

и

$$f_3(2^{1990}) < (4+3\cdot 9)^2 = 31^2 = 961 .$$

Од друга страна, од $2^6 \equiv 1 (\mathrm{mod}\, 9)$ следува

$$2^{1990} \equiv 2^4 \equiv 7 (\mathrm{mod}\, 9) .$$

Бидејќи секој број дава ист остаток по модул 9 како и неговиот збир на цифри, добиваме дека $f_1(x) \equiv x^2 (\mathrm{mod}\, 9)$ за секој $x \in \mathbb{N}$, па затоа

$$f_1(2^{1990}) \equiv 7^2 \equiv 4 (\mathrm{mod}\, 9)$$

и

$$f_2(2^{1990}) \equiv 4^2 \equiv 7 (\mathrm{mod}\, 9) .$$

Најпосле, имаме $f_3(2^{1990}) = n^2$, при што $n < 31$ и

$$n \equiv f_2(2^{1990}) \equiv 7 (\mathrm{mod}\, 9) .$$

Според тоа,

$$f_3(2^{1990}) \in \{49, 256, 625\} .$$

Меѓутоа, во сите три случаи е $f_4(2^{1990}) = 169$, па за $n \ge 2$ имаме:

$$f_{2n}(2^{1990}) = 169 \text{ и } f_{2n+1}(2^{1990}) = 256 .$$

Значи, $f_{1991}(2^{1990}) = 256$. ■

2. СИСТЕМИ ОСТАТОЦИ

2.1. Од својствата на конгруенциите следува дека релацијата „... е конгруентен со ... по модул m ...“ е релација за еквиваленција. Во однос на оваа релација множеството $\mathbb{Z}$ го разбиваме на m дисјунктни класи на еквиваленција. Во врска со претходно изнесеното ја имаме следнава дефиниција.

Дефиниција. Ако $x \equiv y (\mathrm{mod}\, m)$, тогаш y го нарекуваме *остаток* од x по модул m. Множеството $y_1, y_2, ..., y_m$ го нарекуваме *комплетен систем остатоци* по модул m ако за секој $x \in \mathbb{Z}$ постои еден и само еден y_i, $i = 1, 2, ..., m$, таков што $x \equiv y_i (\mathrm{mod}\, m)$.

2.2. Теорема. Секој цел број е конгруентен по модул m со еден и само еден од броевите $0,1,2,...,m-1$.

Доказ. Нека a е цел број. Јасно, $a \equiv r \pmod m$ за некој r, $0 \le r < m$. Да претпоставиме дека $a \equiv r \pmod m$ и $a \equiv s \pmod m$, $0 \le r, s < m$. Тогаш, $s \equiv r \pmod m$, т.е. $m \mid (s-r)$ и бидејќи $-m < s-r < m$, добиваме дека $s-r=0$, односно $s=r$, што и требаше да се докаже. ■

2.3. За секој $r \in \{0,1,2,...,m-1\}$ со $C_m(r)$ да го означиме множеството од сите цели броеви кои се конгруентни со r по модул m. Од претходната теорема следува дека

$$C_m(r) \cap C_m(s) = \varnothing \text{ за } r \ne s$$

и дека

$$C_m(0) \cup C_m(1) \cup ... \cup C_m(m-1) = \mathbb{Z}.$$

Дефиниција. Множествата $C_m(r)$, $r \in \{0,1,2,...,m-1\}$ ги нарекуваме *класи на конгруенции по модул* m.

2.4. Теорема. Множеството $\{a_0, a_1, ..., a_{m-1}\}$ е комплетен систем на остатоци по модул m ако и само ако

$$a_r \in C_m(r) \text{ за } r = 0,1,...,m-1.$$

Доказ. Непосредно следува од претодните разгледувања. ■

2.5. Теорема. Нека $(a,m)=1$ и $S=\{a_1, a_2, ..., a_m\}$ е комплетен систем остатоци по модул m. Тогаш за секој $b \in \mathbb{Z}$ множеството $T=\{aa_1+b, aa_2+b, ..., aa_m+b\}$ е комплетен систем остатоци по модул m.

Доказ. Од $(a,m)=1$ следува дека постојат $c,k \in \mathbb{Z}$ такви што $ac+mk=1$, што значи $ac \equiv 1 \pmod m$. Ако $d \in \mathbb{Z}$, тогаш постои единствен $t \in \{1,2,...,m\}$ таков што $c(d-b) \equiv a_t \pmod m$. Но, тогаш

$$d-b \equiv ac(d-b) \equiv aa_t \pmod m,$$

т.е. $d \equiv (aa_t+b) \pmod m$.

Ако $d \equiv (aa_i+b) \pmod m$, тогаш

$$(aa_i+b) \equiv (aa_t+b) \pmod m,$$

па затоа $aa_i \equiv aa_t \pmod m$. Но, $(a,m)=1$ и од последната конгруенција и својствата на конгруенциите следува $a_i \equiv a_t \pmod m$, што значи $i=t$. Според тоа, T е комплетен систем остатоци по модул m. ■

2.6. Од теоремите 2.2 и 2.4 следува дека *секое множество од* m *последователни цели броеви е комплетен систем на остатоци по модул* m. Така на при-

мер, множеството $\{1, 2, ..., m\}$ е комплетен системи на остатоци по модул m. Ако m е непарен број, тогаш и множеството

$$\{-\tfrac{m-1}{2}, -\tfrac{m-1}{2}+1, ..., -1, 0, 1, ..., \tfrac{m-1}{2}\}$$

е комплетен систем на остатоци по модул m.

Фактот дека $\{0, 1, ..., m-1\}$ е комплетен систем на остатоци по модул m значи дека секоја комбинација на збирови, производи и разлики од овие броеви, по модул m е повторно некој од тие броеви. Ова доведува до таканаречената *модуларна аритметика*. Во следните две табели се дадени операциите собирање и множење по модул 5.

$a \setminus b$	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$a+b \pmod 5$

$a \setminus b$	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$ab \pmod 5$

Од таблицата за множење по модул 5 следува дека $0^2, 1^2, 2^2, 3^2$ и 4^2 се конгруентни по модул 5 само со некој од броевите 0, 1 и 4. Но, 0, 1, 2, 3 и 4 е комплетен систем на остатоци по модул 5, па заклучуваме дека квадрат на природен број при делење со 5 не дава остаток 2 и 3.

2.7. Дефиниција. Нека $S = \{a_1, a_2, ..., a_m\}$ е комплетен систем остатоци по модул m и нека $S' \subseteq S$ се состои од сите броеви од S кои се заемно прости со m. Тогаш S' го нарекуваме *редуциран систем остатоци* по модул m.

2.8. Теорема. Ако $(a, m) = 1$ и S' е редуциран систем остатоци по модул m, тогаш a е конгруентен со единствен број од S'. Ако S'' е друг редуциран систем остатоци по модул m, тогаш S' и S'' имаат еднаков број елементи.

Доказ. Од дефиницијата 2.7 следува дека $S' \subseteq S = \{a_1, a_2, ..., a_m\}$, каде S е комплетен систем остатоци по модул m. Затоа постои единствен број $b \in S$ таков да $a \equiv b \pmod m$. Од $(a, m) = 1$ следува $(b, m) = 1$, па значи $b \in S'$. Јасно, бидејќи b е единствен во S тој е единствен и во S'.

Нека S'' е друг редуциран систем остатоци по модул m. Секој елемент од S'' е конгруентен со точно еден елемент од S', а бидејќи два различни елементи од S' не се конгруентни, добиваме дека бројот на елементите на S' е поголем или еднаков со бројот на елементите на S''. Ако ги замениме местата на S'' и S' до-

биваме дека бројот на елементите на S'' е поголем или еднаков на бројот на елементите на S'. Значи, S' и S'' имаат еднаков број елементи. ■

2.9. Теорема. Ако $m>1$ и S' е редуциран систем остатоци по модул m, тогаш бројот на сите природни броеви помали или еднакви на m и заемно прости со m е еднаков на бројот на елементите на S'.

Доказ. Бидејќи $S=\{1,2,...,m\}$ е комплетен систем остатоци по модул m, добиваме дека $S'=\{k \mid k\in S,(m,k)=1\}$ е редуциран систем остатоци по модул m. Сега тврдењето следува од теорема 2.8. ■

2.10. Во точка III 5 за секој природен број n вредноста $\varphi(n)$ на Ојлеровата функција ја дефинираме како бројот на природните броеви m такви што $m\le n$ и $(m,n)=1$. Според тоа, $\varphi(n)$ е еднаков на бројот на елементите на редуцираниот систем на остатоци по модул n добиен од комплетниот систем на остатоци $\{0,1,2,...,n-1\}$ по модул n. Сега од теоремите 2.8 и 2.9 следува дека $\varphi(n)$ е еднаков на бројот на елементите на произволен редуциран систем на остатоци по модул n и секој редуциран систем на остатоци S' по модул n може да се запише во видот $S'=\{a_1, a_2,..., a_{\varphi(m)}\}$.

2.11. Теорема. Ако $(a,m)=1$ и $S'=\{a_1, a_2,..., a_{\varphi(m)}\}$ е редуциран систем остатоци по модул m, тогаш и множеството $T'=\{aa_1, aa_2,..., aa_{\varphi(m)}\}$ е редуциран систем остатоци по модул m.

Доказ. Од дефиницијата 2.7 имаме $S'\subseteq S=\{a_1,a_2,...,a_m\}$, каде S е комплетен систем остатоци по модул m. Според теоремата 2.5 при $b=0$ множеството $T=\{aa_1,aa_2,...,aa_m\}$ е комплетен систем остатоци по модул m. Сите броеви aa_j, $j=1,2,...,m$ се различни меѓу себе по модул m, па затоа доволно е да докажеме дека

$$(aa_j,m)=1, \text{ за } j=1,2,...,\varphi(m).$$

Последното тврдење следува од равенствата

$$(a,m)=(a_j,m)=1, \text{ за } j=1,2,...,\varphi(m). \blacksquare$$

2.12. Коментар. Горните разгледувања ни овозможуваат да дадеме е друг доказ дека функцијата φ е мултипликативна, т.е. друг доказ на теоремата III 5.3, кој овде ќе го презентираме.

***Доказ на теорема* III 5.3.** Јасно $\varphi(1)=1\neq 0$. Нека $(m,n)=1$. Во следнава табела ќе го определиме бројот $\varphi(mn)$ на елементите кои се заемно прости со mn. Имаме

$$\begin{array}{ccccccc} 1 & 2 & 3 & \ldots & k & \ldots & n \\ n+1 & n+2 & n+3 & \ldots & n+k & \ldots & 2n \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ (m-1)n+1 & (m-1)n+2 & (m-1)n+3 & \ldots & (m-1)n+k & \ldots & mn \end{array}$$

Да забележиме дека ако за фиксиран k и за некој $i \in \{0,1,2,\ldots,m-1\}$ бројот $in+k$ е заемно прост со n ако и само ако и за секој $j \in \{0,1,2,\ldots,m-1\}$ бројот $jn+k$ е заемно прост со n. Со други зборови, во било која колона на дадената таблица или сите елементи се заемно прости со n или ниту еден не е заемно прост со n. Колони во кои сите елементи се заемно прости со n се $\varphi(n)$ на број. Бидејќи $(m,n)=1$, во секоја колона има $\varphi(m)$ елементи кои се заемно прости со m. Затоа вкупниот број елементи во табелата кои се заемно прости со m и n, односно со mn, е еднаков на $\varphi(m)\varphi(n)$, од што следува $\varphi(m)\varphi(n)=\varphi(mn)$. ■

Понатаму, теоремата III 5.4, т.е. формулата

$$\begin{aligned} \varphi(n) &= p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k} (1-\tfrac{1}{p_1})(1-\tfrac{1}{p_2})\ldots(1-\tfrac{1}{p_k}) \\ &= n(1-\tfrac{1}{p_1})(1-\tfrac{1}{p_2})\ldots(1-\tfrac{1}{p_k}), \end{aligned}$$

каде $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ е каноничниот запис на број n се докажува на потполно ист начин како во точка III 5, но теоремата на Гаус III 5.2, т.е. формулата

$$\sum_{d|n} \varphi(d) = n, \ n \in \mathbb{N}$$

е непосредна последица од горните разгледувања.

***Доказ на теорема* III 5.2.** Нека $f(n)=\sum_{d|n}\varphi(d)$. Функцијата $f(n)$ е мултипликативна, односно $f(nm)=f(n)f(m)$, за секои m и n такви што $(m,n)=1$. Нека p е прост број и $a \geq 1$. Тогаш

$$\begin{aligned} f(p^a) &= \sum_{d|p^a} \varphi(d) = \varphi(1)+\varphi(p)+\ldots+\varphi(p^a) \\ &= 1+(p-1)+(p^2-p)+\ldots+(p^a-p^{a-1}) = p^a. \end{aligned}$$

Според тоа, ако $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$, тогаш

$$f(n) = f(p_1^{a_1}) f(p_2^{a_2}) \ldots f(p_k^{a_k}) = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k} = n \,.\ ■$$

2.13. Пример. Нека m и r се заемно прости броеви и $m>0$. Докажи дека множеството $\{c, c+r, c+2r, \ldots, c+(m-1)r\}$ е комплетен систем на остатоци по модул m.

Решение. Множеството $\{0,1,2,...,m-1\}$ е комплетен систем на остатоци по модул m и $(m,r)=1$, па ако во теоремата 2.5 ставиме

$$a_i = i-1,\ \ i=1,2,..,m,\ a=r \text{ и } b=c$$

добиваме дека множеството

$$\{c, c+r, c+2r, ..., c+(m-1)r\}$$

е комплетен систем на остатоци по модул m. ■

2.14. Пример. Нека $\{a_1, a_2, ..., a_m\}$ е комплетен систем на остатоци по модул m, $\{b_1, b_2, ..., b_n\}$ е комплетен систен на остатоци по модул n и $(m,n)=1$. Докажи, дека множеството

$$A=\{a_i n + b_j n \mid i=1,2,...,m;\ j=1,2,...,n\}$$

е комплетен систем на остатоци по модул mn.

Решение. Од $a_i n + b_j m \equiv a_k n + b_t m \pmod{mn}$, тогаш $a_i n \equiv a_k n \pmod{m}$, па затоа $a_i \equiv a_k \pmod{m}$. Бидејќи $\{a_1, a_2, ..., a_m\}$ е комплетен систем на остатоци по модул m добиваме дека $i=k$. На потполно ист начин се добива $j=t$. Значи сите mn елементи на множеството A не се меѓусебно конгруентни по модул mn, па затоа множеството A е комплетен систем на остатоци по модул mn. ■

2.15. Пример. Нека

$$S_n = \{\binom{n}{n}, \binom{2n}{n}, \binom{3n}{n}, ..., \binom{n^2}{n}\}, n \in \mathbb{N}.$$

а) Докажи дека постојат бесконечно многу сложени природни броеви n такви што S_n не е комплетен систем на остатоци по модул n.

б) Докажи дека постојат бесконечно многу сложени природни броеви n такви што S_n е комплетен систем на остатоци по модул n.

Решение. а) Ќе докажеме дека $n=2p$, каде $p>2$ е прост број го задоволува условот. Имаме

$$\binom{2kp}{2p} \equiv k(2k-1) \pmod{2p}.$$

Конкретно, одовде следува дека $\binom{2kp}{2p}$ е делив со p за $k \in \{\frac{p+1}{2}, p, 2p\}$, т.е. S_{2p} има три елементи деливи со p, па затоа не е комплетен систем на остатоци по модул n.

б) Ќе докажеме дека $n=p^2$, каде $p>2$ е прост број го задоволува условот. Имаме

$$\binom{kp^2}{p^2} = \prod_{i=0}^{p^2-1} \frac{kp^2-i}{p^2-i} = k \prod_{j=1}^{p-1} \frac{kp^2-jp}{jp} \cdot \prod_{p \nmid i} \frac{kp^2-i}{p^2-i},$$

па затоа по модул p^2

$$\binom{kn}{n} \equiv k\prod_{j=1}^{p-1}\frac{kp-j}{j} = k\prod_{j=1}^{p-1}(1-\frac{kp}{j}) \equiv k-k^2p\sum_{j=1}^{p-1}\frac{1}{j}.$$

Бидејќи

$$\sum_{j=1}^{p-1}\frac{1}{j} = \sum_{j=1}^{\frac{p-1}{2}}(\frac{1}{j}+\frac{1}{p-j}) = \sum_{j=1}^{\frac{p-1}{2}}\frac{p}{j(p-j)} \equiv 0(\mathrm{mod}\ p)$$

добиваме $\binom{kn}{n} \equiv k(\mathrm{mod}\ p^2)$. ■

2.16. Пример. Докажи дека постојат цели броеви $a_1, a_2, ..., a_m$ и $b_1, b_2, ..., b_k$ такви што броевите a_ib_j, $1 \le i \le m, 1 \le j \le k$, формираат комплетен систем остатоци по модул mk ако и само ако важи $(m,k)=1$.

Решение. Нека броевите a_ib_j, $1 \le i \le m, 1 \le j \le k$ формираат комплетен систем остатоци по модул mk. Тогаш точно еден од нив е делив со mk. На пример, нека $mk \mid a_1b_1$. Според тоа, постојат броеви $a' \mid a_1$ и $b' \mid b_1$ такви што $mk = a'b'$. Не може да важи $a' \mid (a_i - a_s)$ за некои индекси $i \ne s$, бидејќи во спротивно ќе важи $mk = a'b' \mid (a_ib_1 - a_sb_1)$, што противречи на претпоставката. Оттука следува дека $a' \ge m$, бидејќи во спротивно од m броеви a_i, најмалку два ќе даваат еднаков остаток по модул a'. Слично, $b' \ge k$, па од $mk = a'b'$ ќе следува $a' = m, b' = k$, што значи дека броевите a_i, односно b_j соодветно формираат комплетен систем на остатоци по модул m, односно k.

Нека претпоставиме дека $(m,k) > 1$ и нека p е прост број таков што $p \mid (m,k)$. Тогаш меѓу броевите a_i има $m - \frac{m}{p}$ кои не се деливи со p. Аналогно, меѓу броевите b_j има $k - \frac{k}{p}$ кои не се деливи со p. Значи, $(m - \frac{m}{p})(k - \frac{k}{p})$ броеви a_ib_j не се деливи со p. Меѓутоа, бидејќи овие броеви формираат комплетен систем на остатоци по модул mk заклучуваме дека меѓу нив има $mk - \frac{mk}{p}$ броеви кои не се деливи со p. Значи, треба да важи $(m - \frac{m}{p})(k - \frac{k}{p}) = mk - \frac{mk}{p}$, што е противречност.

Конечно, од добиената противречност следува дека $(m,k) = 1$.

Нека $(m,k) = 1$. Треба да најдеме две низи цели броеви $a_1, a_2, ..., a_m$ и $b_1, b_2, ..., b_k$ такви што броевите a_ib_j, $1 \le i \le m, 1 \le j \le k$, формираат комплетен систем остатоци по модул mk.

Како што веќе докажавме, тогаш $a_i, 1 \le i \le m$, мора да формираат комплетен систем

на остатоци по модул m, додека броевите b_j, $1 \le j \le k$, мора да ги даваат сите различни остатоци по модул k. Сакаме да видиме во каков однос се броевите a_i и бројот k. Случајот $k=1$ е тривијален. Нека $k>1$ и нека q е прост делител на k. Нека меѓу броевите a_i има точно x броеви кои не се деливи со q. Аналогно како погоре, меѓу броевите b_j има $k-\frac{k}{q}$ кои не се деливи со q. Од друга страна, меѓу производите $a_i b_j$ има $mk-\frac{mk}{q}$ кои не се деливи со q. Оттука, $x(k-\frac{k}{q}) = mk-\frac{mk}{q}$, т.е. $x=m$. Затоа, ниту еден од броевите a_i не е делив со q. Сега, од произволноста на простиот делител q на k, следува $(a_i,k)=1$ за секој $1 \le i \le m$. Аналогно се докажува дека $(b_j,m)=1$ за секој $1 \le j \le k$.

Претходните разгледувања сугерираат да ги разгледаме броевите

$$a_i = ki+1, \quad 1 \le i \le m,$$
$$b_j = mj+1, \quad 1 \le j \le k.$$

Очигледно, $a_r - a_s = k(r-s)$, што $(a_i,k)=1$ и $|r-s|<m$ повлекува дека сите a_i се различни по модул m. Слично, броевите b_j се различни по модул k. Ако броевите $a_i b_j$ и $a_r b_s$ даваат ист остаток при делење со mk, тогаш

$$\begin{aligned} mk \mid (a_i b_j - a_r b_s) &= (ki+1)(mj+1)-(kr+1)(ms+1) \\ &= km(ij-rs)+m(j-s)+k(i-r). \end{aligned}$$

Бидејќи $(m,k)=1$, мора да е $k \mid (j-s)$ и $m \mid (i-r)$, што значи $i=r$ и $j=s$, па затоа наведените броеви го имаат саканото својство. ■

2.17. Пример. Нека $(a,n)=1$. Определи го збирот

$$\sum_{\substack{1 \le k \le n \\ (k,n)=1}} \{\tfrac{ak}{n}\}.$$

Решение. Од $(a,n)=1$, следува дека кога k се менува во редуциран систем остатоци по модул n, тогаш ak се менува во редуциран систем остатоци по модул n. Затоа важи

$$\sum_{\substack{1 \le k \le n \\ (k,n)=1}} \{\tfrac{ak}{n}\} = \sum_{\substack{1 \le m < n \\ (m,n)=1}} \{\tfrac{m}{n}\} = \frac{1}{n} \sum_{\substack{1 \le m < n \\ (m,n)=1}} m.$$

Бидејќи $(m,n)=1$ ако и само ако $(n-m,n)=1$, добиваме

$$2 \sum_{\substack{1 \le m \le n \\ (m,n)=1}} m = \sum_{\substack{1 \le m \le n \\ (m,n)=1}} m + \sum_{\substack{1 \le m \le n \\ (n-m,n)=1}} m$$

$$= \sum_{\substack{1\le m\le n\\(m,n)=1}} m + \sum_{\substack{1\le m\le n\\(m,n)=1}} (n-m)$$
$$= \sum_{\substack{1\le m\le n\\(m,n)=1}} n = n\varphi(n)$$

,

па затоа

$$\sum_{\substack{1\le k\le n\\(k,n)=1}} \{\frac{ak}{n}\} = \frac{1}{n} \sum_{\substack{1\le m\le n\\(m,n)=1}} m = \frac{1}{2}\varphi(n) . \blacksquare$$

3. ТЕОРЕМИ НА ОЈЛЕР, ФЕРМА, КАРМАЈКЛ И ВИЛСОН

3.1. Теорема (Ојлер). Ако $(a,m)=1$, тогаш

$$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m) .$$

Доказ. Нека $\{a_1, a_2, ..., a_{\varphi(m)}\}$ е редуциран систем остатоци по модул m. Според теоремата 2.11 и $\{aa_1, aa_2, ..., aa_{\varphi(m)}\}$ е редуциран систем остатоци по модул m. Значи, за секој a_i постои еден и само еден a_j така што $a_i \equiv aa_j (\mathrm{mod}\, m)$. Ако ги помножиме сите конгруенции од овој вид, ги има точно $\varphi(m)$, добиваме

$$a^{\varphi(m)} a_1 a_2 ... a_{\varphi(m)} \equiv a_1 a_2 ... a_{\varphi(m)} (\mathrm{mod}\, m) .$$

Бидејќи $(a_i, m)=1$, за $i=1,2,...,\varphi(m)$, од последната конгруенција добиваме $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$. ■

3.2. Теорема (мала теорема на Ферма). Ако p е прост број и $(a,p)=1$, тогаш

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p) .$$

Доказ. Од $(a,p)=1$, според теоремата 3.1 добиваме

$$a^{\varphi(p)} \equiv 1 (\mathrm{mod}\, p)$$

и како $\varphi(p) = p-1$ имаме $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$. ■

3.3. Последица. Ако p е прост број, тогаш за секој цел број a важи

$$a^p \equiv a (\mathrm{mod}\, p) .$$

Доказ. Ако $p \mid a$, тогаш јасно $a^p \equiv a (\mathrm{mod}\, p)$. Ако $p \nmid a$, тогаш од малата теорема на Ферма следува $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$, и ако последната конгруенцијата ја помножиме со a добиваме $a^p \equiv a (\mathrm{mod}\, p)$. ■

3.4. Последица. Ако p и q се различни прости броеви, тогаш

$$p^{q-1}+q^{p-1}\equiv 1 \pmod{pq}.$$

Докажи!

Доказ. Од малата теорема на Ферма имаме $q\mid(p^{q-1}-1)$ и $p\mid(q^{p-1}-1)$. Според тоа, $pq\mid(p^{q-1}-1)(q^{p-1}-1)$, т.е.

$$pq\mid(p^{q-1}q^{p-1}-p^{q-1}-q^{p-1}+1). \tag{1}$$

Бидејќи p и q се прости броеви имаме

$$pq\mid p^{q-1}q^{p-1}. \tag{2}$$

Од (1) и (2) непосредно следува дека $pq\mid(p^{q-1}+q^{p-1}-1)$, т.е.

$$p^{q-1}+q^{p-1}\equiv 1 \pmod{pq}. \blacksquare$$

3.6. Да го разгледаме бројот $n=561=3\cdot 11\cdot 17$. Според малата теорема на Ферма за секој a кој не е делив со 3, 11 или 17 важи

$$a^2\equiv 1 \pmod 3,\ a^{10}\equiv 1 \pmod{11} \text{ и } a^{16}\equiv 1 \pmod{17}. \tag{3}$$

Ако овие три конгруенции ги степенуваме соодветно со степените 280, 56 и 35, добиваме

$$a^{560}\equiv 1 \pmod 3,\ a^{560}\equiv 1 \pmod{11} \text{ и } a^{560}\equiv 1 \pmod{17},$$

па затоа $a^{560}\equiv 1 \pmod{561}$.

Претходните разгледувања покажуваат дека не е точно обратното тврдење на малата теорема на Ферма, т.е. дека од тоа што за секој $a\in\mathbb{Z}$ заемно прост со n важи $a^{n-1}\equiv 1 \pmod n$ не следува дека n е прост број.

Дефиниција. За сложениот број n ќе велиме дека е *Кармајклов број* ако за секој $a\in\mathbb{Z}$ заемно прост со n важи $a^{n-1}\equiv 1 \pmod n$.

Да забележиме дека единствен Кармајклов број помал од 1000 е бројот 561. Понатаму, ако конгруенциите (3) ги степенуваме соодветно со степените 40, 8 и 5 добиваме

$$a^{80}\equiv 1 \pmod 3,\ a^{80}\equiv 1 \pmod{11} \text{ и } a^{80}\equiv 1 \pmod{17},$$

па затоа $a^{80}\equiv 1 \pmod{561}$, што е појако тврдење од тврдењето на теоремата на Ојлер според која од $\varphi(561)=\varphi(3\cdot 11\cdot 17)=2\cdot 10\cdot 16=320$ следува $a^{320}\equiv 1 \pmod{561}$. Последното сугерира дека во општ случај експонентот $\varphi(n)$ во теоремата на Ојлер може да се подобри.

3.7. Дефиниција. Функцијата $\lambda : \mathbb{N} \to \mathbb{N}$ определена со:

$\lambda(1)=1, \lambda(2)=1, \lambda(4)=2, \lambda(2^k)=2^{k-2}$ за $k \geq 3$,

$\lambda(p^k)=p^{k-1}(p-1)$ за непарен прост број p и природен број k, и

$\lambda(n)=[\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), ..., \lambda(p_r^{\alpha_r})]$ за $n=p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}$

ја нарекуваме *функција на Кармајкл*.

3.8. Лема. За секој $n \in \mathbb{N} \setminus \{1\}$ важи $\lambda(n) \mid \varphi(n)$, при што $\lambda(n)=\varphi(n)$ ако и само ако $n=2,4,p^k$ или $2p^k$ каде p е непарен прост број и k е природен број.

Доказ. Непосредно следува од својствата на Ојлеровата функција и дефиниција 3.7. Деталите ги оставаме на читателот за вежба. ■

3.9. Теорема (Кармајкл). Ако n е природен број и a е цел број таков што $(a,n)=1$, тогаш

$$a^{\lambda(n)} \equiv 1 (\mathrm{mod}\, n).$$

Доказ. Доволно е да докажеме дека

$$a^{\lambda(p^k)} \equiv 1 (\mathrm{mod}\, p^k)$$

за секој прост број p и $k \geq 0$. Навистина, бидејќи од $p^k \mid n$ следува $\lambda(p^k) \mid \lambda(n)$, ако последната конгруенција ја степенуваме со $\frac{\lambda(n)}{\lambda(p^k)}$ добиваме

$$a^{\lambda(n)} \equiv 1 (\mathrm{mod}\, p^k),$$

а оттука ќе следува $a^{\lambda(n)} \equiv 1 (\mathrm{mod}\, n)$.

Ако p е непарен прост број, тогаш од дефиницијата 3.7 и теоремата на Ојлер следува $p^k \mid a^{\varphi(p^k)}-1=a^{\lambda(p^k)}-1$. Ако $p=2$ и $k=1,2$, тогаш тврдењето следува од дефиницијата 3.7 и теоремата на Ојлер, а ако $p=2$ и $k \geq 3$, тогаш

$$a^{\lambda(2^k)}-1=a^{2^{k-2}}-1=(a^2-1)\prod_{i=1}^{k-3}(a^{2^i}+1),$$

при што $2^3 \mid a^2-1$ и сите останати множители се парни, па оттука следува тврдењето. ■

3.10. Коментар. Ако n е прост број, тогаш теоремата на Кармајкл не дава подобрување на малата теорема на Ферма, т.е. на теоремата на Ојлер, бидејќи во тој случај важи $\lambda(n)=\varphi(n)=n-1$. Покасно ќе докажеме дека теоремата 3.9 е оптимална во смисол дека експонентот $\lambda(n)$ не може да се подобри.

3.11. Теорема. Ако n е производ на различни прости множители, тогаш за секој a важи

$$a^{\lambda(n)+1} \equiv a \pmod{n}.$$

Доказ. Нека $n = p_1 p_2 ... p_s$, $p_i \neq p_k$, за $i \neq k$. Доволно е да докажеме дека

$$a^{\lambda(n)+1} \equiv a \pmod{p_i}, \text{ за } i = 1,2,...,s. \quad (4)$$

Ако $p_i \mid a$, тогаш конгруенцијата (4) е очигледна. Нека $p_i \nmid a$, т.е. $(p_i, a) = 1$. Тогаш од теоремата на Ферма следува $a^{p_i - 1} \equiv 1 \pmod{p_i}$. Бидејќи

$$p_i - 1 \mid \lambda(n) = [p_1 - 1, p_2 - 1, ..., p_s - 1],$$

добиваме $a^{\lambda(n)} \equiv 1 \pmod{n}$ од каде следува (1). ■

3.12. Теорема. (Вилсон). Ако p е прост број, тогаш

$$(p-1)! \equiv -1 \pmod{p}. \quad (5)$$

Доказ. За $p = 2$ и $p = 3$ непосредно се проверува дека тврдењето важи. Нека претпоставиме дека $p \geq 5$.

Да забележиме дека $1 \equiv 1 \pmod{p}$ и $p - 1 \equiv -1 \pmod{p}$. За секој j, $2 \leq j \leq p-2$ важи $(j, p) = 1$, па затоа постои еден и само еден i така што $ij \equiv 1 \pmod{p}$ и $0 \leq i \leq p-1$. Очигледно $i \notin \{0, 1, p-1\}$, па затоа за секој j, $2 \leq j \leq p-2$, постои еден и само еден i така што $ij \equiv 1 \pmod{p}$ и $2 \leq i \leq p-2$. Притоа $i \neq j$, бидејќи за секој $j, 2 \leq j \leq p-2$, важи $(j-1, p) = (j+1, p) = 1$ и затоа

$$j^2 - 1 = (j-1)(j+1) \not\equiv 0 \pmod{p}.$$

Така, броевите $2, 3, ..., p-2$ ги поделивме на $\frac{p-3}{2}$ дисјунктни двоелементни множества $\{i, j\}$ за кои важи $ij \equiv 1 \pmod{p}$. Ако ги помножиме овие конгруенции добиваме $2 \cdot 3 \cdot 4 \cdot ... \cdot (p-2) \equiv 1 \pmod{p}$ и како $1 \equiv 1 \pmod{p}$ и $p - 1 \equiv -1 \pmod{p}$ од последните три конгруенции следува

$$(p-1)! \equiv -1 \pmod{p}. \blacksquare$$

3.13. Лема. Ако $(m-1)! \equiv -1 \pmod{m}$, тогаш m е прост број.

Решение. Нека m не е прост број, т.е. нека $m = ks, 1 < k < m$. Тогаш, k е делител на $(m-1)!$ и како k е делител на $(m-1)!+1$ добиваме дека k е делител на 1, што е противречност. ■

3.14. Пример. Определи ги сите цели броеви a, b, c, d кои не се деливи со 5 и за кои важи

$$a^4 + b^4 + c^4 + d^4 = 2012. \quad (6)$$

Решение. Имаме, $(a,5)=1$, па затоа од малата теорема на Ферма следува дека $a^4 \equiv 1(\mathrm{mod}\,5)$. Аналогно се добива $b^4 \equiv 1(\mathrm{mod}\,5), c^4 \equiv 1(\mathrm{mod}\,5)$ и $d^4 \equiv 1(\mathrm{mod}\,5)$. Според тоа, $a^4+b^4+c^4+d^4 \equiv 4(\mathrm{mod}\,5)$ и како $2012 \equiv 2(\mathrm{mod}\,5)$ заклучуваме дека не постојат цели броеви a,b,c,d такви што важи (6). ■

3.15. Пример. Определи ги сите природни броеви n за кои бројот

$$1^{\varphi(n)}+2^{\varphi(n)}+\ldots+n^{\varphi(n)}$$

е заемно прост со бројот n.

Решение. Нека p прост делител на бројот n. Нека природниот број a не е делив со p. Од теоремата на Ојлер следува $a^{\varphi(n)} \equiv 1(\mathrm{mod}\,p)$. Бидејќи бројот на природните броеви помали или еднакви на n кои не се деливи со p е еднаков на $n-\frac{n}{p}$, добиваме

$$1^{\varphi(n)}+2^{\varphi(n)}+\ldots+n^{\varphi(n)} \equiv n-\frac{n}{p} \equiv -\frac{n}{p}(\mathrm{mod}\,p).$$

Според тоа, p не е делител на $1^{\varphi(n)}+2^{\varphi(n)}+\ldots+n^{\varphi(n)}$ ако и само ако p не е делител на $\frac{n}{p}$, што значи ако и само ако p^2 не е делител на n. Последното значи дека n и $1^{\varphi(n)}+2^{\varphi(n)}+\ldots+n^{\varphi(n)}$ се заемно прости ако и само ако n е производ на различни прости броеви. ■

3.16. Пример. Ако $(p,q)=1$, $p \geq 2$, тогаш низата $\{\frac{p^n}{qn+1}, n \in \mathbb{N}\}$ содржи бесконечно многу цели броеви. Докажи!

Решение. Од $(p,q)=1$ следува $(p^k,q)=1$, за секој $k \in \mathbb{N}$. Значи, за секој природен број k ќе важи $q \mid p^{k\varphi(q)}-1$. Нека $n_k=\frac{p^{k\varphi(q)}-1}{q}$. Тогаш важи

$$\frac{p^{n_k}}{qn_k+1}=\frac{p^{n_k}}{p^{k\varphi(q)}}=p^{n_k-k\varphi(q)}.$$

Бидејќи $p \geq 2$, за доволно големо k ќе важи $n_k \geq k\varphi(q)$. ■

3.17. Пример. Докажи дека

$$1989 \mid (n^{n^{n^n}}-n^{n^n})$$

за секој природен број n.

Решение. Воведуваме ознаки

$$a=n^{n^{n^n}}-n^{n^n}=n^{n^n}(n^{n^{n^n}-n^n}-1),$$
$$b=n^{n^n}-n^n=n^n(n^{n^n-n}-1),$$

$$c = n^n - n.$$

Сега

$$a = n^{n^n}(n^b - 1), \quad b = n^n(n^c - 1), \quad c = n(n^{n-1} - 1).$$

Бидејќи $1989 = 9 \cdot 13 \cdot 17$ идејата на решението е да докажеме дека $\varphi(d) \mid b$ за секој $d \in \{9,13,17\}$, бидејќи тогаш важи:

$$(n,d) = 1 \quad \Rightarrow \quad d \mid (n^{\varphi(d)} - 1 \mid n^b - 1 \mid a.$$

Од друга страна, ако $d \in \{13,17\}$ и $(n,d) \neq 1$, тогаш $d \mid n \mid a$, а додека од $(n,9) \neq 1$ следува $3 \mid n$, па затоа $9 \mid n^2 \mid a$. Според тоа, задачата ќе биде решена ако докажеме дека

$$[\varphi(9), \varphi(13), \varphi(17)] = [6,12,16] = 48 \mid b.$$

Прво, $3 \mid n \Rightarrow 3 \mid b$. Од друга страна ако 3 не е делител на n, тогаш $(n,3) = 1$. Но, $2 \mid c$ (јасно ако n е парен; а ако n е непарен, тогаш $n^{n-1} - 1$ е парен). Значи, $\varphi(3) = 2 \mid c$, па од теоремата на Ојлер следува $3 \mid (n^c - 1) \mid b$.

Понатаму, ако n е парен, тогаш $2^n \mid b$, па затоа од $n \geq 4$ следува $16 \mid b$. Ако $n = 2k+1$, тогаш

$$\begin{aligned} c &= (2k+1)((2k+1)^{2k} - 1) = (2k+1)((4k(k+1)+1)^k - 1 \\ &= (2k+1)4k(k+1)N = 8(2k+1)\tfrac{k(k+1)}{2} N. \end{aligned}$$

Значи, $\varphi(16) = 8 \mid c$ и затоа повторно од теоремата на Ојлер следува $16 \mid (n^c - 1) \mid b$. Со тоа задачата е решена. ■

3.18. Пример. Нека a и b се природни броеви такви што $a^n + n$ е делител на $b^n + n$ за секој природен број n. Докажи дека $a = b$.

Решение. Нека $a \neq b$. Од $a^n + n \mid b^n + n$ следува $a < b$. Нека $p > b$ е прост број и $n = (a+1)(p-1) + 1$. Јасно, $n \equiv 1 \pmod{p-1}$. Од

$$n = (a+1)(p-1) + 1 = ap + p - a$$

следува дека $n \equiv -a \pmod{p}$. Оттука, за секој цел број r заемно прост со p, од малата теорема на Ферма следува $r^n \equiv r(r^{p-1})^{a+1} \equiv r \pmod{p}$. Од $p > b > a$ следува $(a, p) = 1$.

Земаме $r = a$. Значи, $a^n \equiv a \pmod{p}$ и како $n \equiv -a \pmod{p}$, добиваме $a^n + a \equiv 0 \pmod{p}$. Следува $b^n + b \equiv 0 \pmod{p}$ и бидејќи $(p,b) = 1$ од малата теорема на Ферма следува $b^n \equiv b \pmod{p}$. Според тоа, $0 \equiv b^n + b \equiv 2b \pmod{p}$, па затоа $p \mid b$, што е противречност. ■

3.19. Пример. а) Докажи дека постојат бесконечно многу парови природни броеви (m,n) такви што $4mn-m-n+1$ е точен квадрат.

б) Докажи дека не постои ниту еден пар природни броеви (m,n) таков што $4mn-m-n$ е точен квадрат.

Решение. а) Ја разгледуваме равенката

$$4mn-m-n+1=k^2,$$

која е еквивалентна со равенката

$$(4m-1)(4n-1)=4k^2-3.$$

Иёбираме k таков што $k=t^2-1$ и добиваме

$$4k^2-3=4(t^2-1)^2-3=4t^4-8t^2+1=(2t^2-1)^2-4t^2$$
$$=(2t^2-2t-1)(2t^2+2t-1),$$

што значи

$$(4m-1)(4n-1)=(2t^2-2t-1)(2t^2+2t-1),$$

од каде добиваме

$$4m-1=2t^2-2t-1,\ \ 4n-1=2t^2+2t-1,$$

односно

$$m=\tfrac{t^2-t}{2},\ \ n=\tfrac{t^2+t}{2},\ t\in\mathbb{N}.$$

Притоа важи

$$4mn-m-n+1=(t^2-1)^2.$$

б) Слично како во решението под а) равенството $4mn-m-n=k^2$ е еквивалентно на равенството

$$(4m-1)(4n-1)=4k^2+1. \tag{7}$$

Нека претпоставиме дека постојат природни броеви m,n,k за кои важи (7). Нека p е прост број кој е делител на $4m-1$. Тогаш

$$(2k)^2\equiv -1(\mathrm{mod}\,p).$$

Од друга страна, од малата теорема на Ферма следува

$$(2k)^{p-1}\equiv 1(\mathrm{mod}\,p).$$

Бројот p е непарен, па затоа

$$1\equiv(2k)^{p-1}\equiv((2k)^2)^{\frac{p-1}{2}}\equiv(-1)^{\frac{p-1}{2}}(\mathrm{mod}\,p),$$

од каде следува $p\equiv 1(\mathrm{mod}\,4)$. Бидејќи во претходните разгледувања простиот множител p на $4m-1$ е произволен, заклучуваме дека

$$4m-1\equiv 1(\mathrm{mod}\,4),$$

што е противречност. ■

3.20. Пример. Нека p е прост број. Докажи, дека за секој $k = 0,1,2,..., p-1$ важи

$$k!(p-k-1)!+(-1)^k \equiv 0 (\mathrm{mod}\ p).$$

Решение. Означуваме $a_k = k!(p-k-1)+(-1)^k$. Имаме

$$\begin{aligned} a_k + a_{k+1} &= k!(p-k-1)!+(-1)^k + (k+1)!(p-k-2)!+(-1)^{k+1} \\ &= k!(p-k-2)![p-k-1+k+1] \\ &= k!(p-k-2)!\,p \end{aligned}$$

па затоа

$$a_k + a_{k+1} \equiv 0 (\mathrm{mod}\ p),$$

за $k = 0,1,2,..., p-2$. Од теоремата на Вилсон следува дека

$$a_0 = (p-1)!+1 \equiv 0 (\mathrm{mod}\ p).$$

Добиваме $a_0 + a_1 \equiv 0 (\mathrm{mod}\ p)$, т.е. $a_1 \equiv 0 (\mathrm{mod}\ p)$. Повторувајќи ја постапката за $k = 1,2,..., p-2$ добиваме $a_{k+1} \equiv 0 (\mathrm{mod}\ p)$, што и требаше да се докаже. ■

3.21. Пример. Ако p е прост број, тогаш $\binom{p^n}{p} \equiv p^{n-1} (\mathrm{mod}\ p^n)$. Докажи!

Решение. Нека $p > 2$. Најпрво ќе го докажеме идентитетот $\binom{p^n}{p} = p^{n-1}\binom{p^n-1}{p-1}$. Имаме,

$$\begin{aligned} p^{n-1}\binom{p^n-1}{p-1} &= p^{n-1} \cdot \frac{(p^n-1)!}{(p^n-p)!(p-1)!} = p^{n-1} \cdot \frac{p^n}{p^n} \cdot \frac{(p^n-1)!}{(p^n-p)!(p-1)!} \\ &= \frac{(p^n-1)!\cdot p^n}{(p^n-p)!(p-1)!\cdot p} = \binom{p^n}{p}. \end{aligned}$$

Сега добиваме

$$\begin{aligned} \binom{p^n}{p} = p^{n-1}\binom{p^n-1}{p-1} &= p^{n-1}\,\frac{(p^n-1)(p^n-2)...(p^n-(p-1))}{1\cdot 2\cdot ...\cdot (p-1)} \\ &\equiv p^{n-1}\,\frac{(-1)^{p-1}(p-1)!}{(p-1)!} = p^{n-1} (\mathrm{mod}\ p^n). \end{aligned}$$

За $p = 2$ добиваме

$$\binom{2^n}{2} = 2^{n-1}\binom{2^n-1}{1} = 2^{n-1}(2^n-1) \equiv -2^{n-1} \equiv 2^{n-1} (\mathrm{mod}\, 2^n). \blacksquare$$

3.22. Пример. а) Нека $(a, 65520) = 1$. Од $65520 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$ следува

$$\varphi(65520) = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot (1-\tfrac{1}{2})(1-\tfrac{1}{3})(1-\tfrac{1}{5})(1-\tfrac{1}{7})(1-\tfrac{1}{13}) = 13824 \text{ и}$$

$$\lambda(n) = [\lambda(2^4), \lambda(3^2), \lambda(5), \lambda(7), \lambda(13)] = [2^2, 6, 4, 6, 12] = 12.$$

Според тоа, ако $(a, 65520) = 1$, тогаш од теоремата на Кармајкл следува $a^{12} \equiv 1 (\mathrm{mod}\, 65520)$, а од теоремата на Ојлер имаме $a^{13824} \equiv 1 (\mathrm{mod}\, 65520)$.

б) Според теоремата на Кармајкл имаме $a^{60} \equiv 1 (\mathrm{mod}\, N)$ за $(a, N) = 1$, каде $N = 2^4 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 61$, бидејќи $\lambda(N) = 60$. Колку за споредба, според теоремата на Ојлер $\varphi(N) = 2^{13} \cdot 3^5 \cdot 5^4 = 1244160000$, од што се гледа предноста на теоремата на Кармајкл во однос на теоремата на Ојлер. ■

4. ЛИНЕАРНИ КОНГРУЕНТНИ РАВЕНКИ

4.1. Дефиниција. Нека $f(x)$, $\deg f = n$, е полином со целобројни коефициенти и $m \in \mathbb{N}$. Равенката од облик

$$f(x) \equiv 0 (\mathrm{mod}\, m) \tag{1}$$

ја нарекуваме *полиномна конгруентна равенка од* $n-ти\ ред$. Ако $\deg f = 1$, тогаш за (1) ќе велиме дека е *линеарна конгруентна равенка*. Решение на (1) е секој цел број x кој ја задоволува. За две решенија x и x' ќе велиме дека се *еквивалентни* ако $x \equiv x' (\mathrm{mod}\, m)$.

Број на решенија на (1) го нарекуваме бројот на нееквивалентните решенија на (1).

Според последица 1.17 од $x \equiv x' (\mathrm{mod}\, m)$ следува $f(x) \equiv f(x') (\mathrm{mod}\, m)$, па затоа претходната дефиниција за решение на (1) е коректна. Понатаму, еквивалентните решенија на (1) припаѓаат на исти класи на остатоци, а нееквивалентните решенија припаѓаат на различни класи на остатоци $x_k, k = 0,1,2,...,m-1$ по модул m. Бидејќи бројот на класите на остатоци по модул m е конечен, равенката (1) може да се реши со непосредна проверка на било кој комплетен систем на остатоци по модул m. Навистина, доволно е да земеме произволен комплетен систем на остатоци x_k, $k = 0,1,...,m-1$ по модул m и да провериме кои од броевите $f(x_k)$, $k = 0,1,...,m-1$, се деливи со m.

4.2. Лема (Ојлер). Ако $(a, m) = 1$, тогаш

$$x_1 \equiv b a^{\varphi(m)-1} (\mathrm{mod}\ m) \tag{2}$$

е решение на линеарната конгруентна равенка $ax \equiv b (\mathrm{mod}\, m)$.

Општото решение на равенката $ax \equiv b (\mathrm{mod}\, m)$ е дадено со $x = x_1 + jm,\ j \in \mathbb{Z}$.

Доказ. Бидејќи $(a, m) = 1$ од теоремата на Ојлер следува $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$, па затоа $a^{\varphi(m)} b \equiv b (\mathrm{mod}\, m)$, т.е. $a a^{\varphi(m)-1} b \equiv b (\mathrm{mod}\, m)$, што значи дека (2) е решение на линеарната конгруентна равенка $ax \equiv b (\mathrm{mod}\, m)$.

Ако x е произволно решение на равенката $ax \equiv b (\mathrm{mod}\, m)$, тогаш

$$ax - ax_1 \equiv 0 (\mathrm{mod}\ m), \text{ т.е. } a(x - x_1) \equiv 0 (\mathrm{mod}\ m),$$

па затоа

$$x - x_1 \equiv 0 (\mathrm{mod}\ m), \text{ т.е. } x = x_1 + jm,\ j \in \mathbb{Z}. \blacksquare$$

4.3. Во лемата 4.2 докажавме, дека ако $(a,m)=1$, тогаш линеарната конгруентна равенка $ax \equiv b (\mathrm{mod} m)$ има точно едно решение $x \equiv x_1 (\mathrm{mod} m)$.

Нека $d=(a,m)$. Можни се два случаи:

а) $d \nmid b$. Во овој случај равенката нема решение бидејќи $ax \equiv 0 (\mathrm{mod} d)$, за секој $x \in \mathbb{Z}$, а $b \not\equiv 0 (\mathrm{mod} d)$.

б) $d \mid b$. Нека $a = a_1 d,\ m = m_1 d,\ b = b_1 d$. Тогаш равенката го добива обликот

$$(a_1 d)x \equiv d b_1 (\mathrm{mod}\, d m_1)$$

и од теоремата 1.9 следува дека $a_1 x \equiv b_1 (\mathrm{mod} m_1),\ (a_1, m_1) = 1$. Според лемата 4.2 последната равенка има единствено решение $x \equiv x_1 (\mathrm{mod} m_1)$. Потоа, решенијата на равенката $ax \equiv b (\mathrm{mod} m)$ се сите цели броеви v такви што $v \equiv x_1 (\mathrm{mod} m_1)$ односно $v = x_1 + k m_1,\ k \in \mathbb{Z}$. Ако k ги прима вредностите $0,1,...,d-1$, тогаш v прима d вредности при што било кои две од нив не се конгруентни по модул m, т.е. не се еквивалентни. Ако k ги прима сите вредности, тогаш соодветните v ќе бидат конгруентни по модул m на овие d вредности.

Така решенијата на конгруентната равенка $ax \equiv b (\mathrm{mod} m)$ се

$$x \equiv x_1 + k \tfrac{m}{d} (\mathrm{mod} m),\ 0 \le k \le d-1. \tag{3}$$

Од претходната дискусија следува следната теорема.

Теорема. Линеарната конгруентна равенка $ax \equiv b (\mathrm{mod} m)$ има решение ако и само ако $d=(a,m)$ е делител на b. Притоа решението е единствено по модул $\frac{m}{d}$, односно решенијата на равенката се дадени со (3) каде x_1 е некое решение на равенката $\frac{a}{d} x \equiv \frac{b}{d} (\mathrm{mod} \frac{m}{d})$. $\blacksquare$

4.4. Коментар. Претходната теорема ја докажавме користејќи ја лемата 4.2, за чиј доказ ја искористивме теоремата на Ојлер. Но, оваа теорема може да се докаже и без користење на теоремата на Ојлер. Во продолжение ќе дадеме еден ваков доказ.

***Доказ на теорема* 4.3.** Ако линеарната конгруентна равенка $ax \equiv b (\mathrm{mod} m)$ има решение, тогаш постои $y \in \mathbb{Z}$ таков што $ax - my = b$, па затоа $d=(a,m)$ е делител на b.

Обратно, нека претпоставиме дека $d=(a,m)$ е делител на b и нека $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ и $m' = \frac{m}{d}$. Сега треба да ја решиме линеарната конгруентна равенка

$a'x \equiv b'(\mathrm{mod}\, m')$. Но, таа има точно едно решение по модул m'. Навистина, бидејќи $(a', m') = 1$, според теоремата 2.5 кога x се менува во комплетен систем остатоци по модул m', тогаш $a'x$ се менува во комплетен систем остатоци по модул m', т.е. секој остаток по модул m' (па така и b') се добива точно за еден x од комплетниот систем остатоци по модул m'.

Јасно, ако x' е некое решение на $a'x \equiv b'(\mathrm{mod}\, m')$, тогаш во множеството цели броеви сите решенија на $ax \equiv b(\mathrm{mod}\, m)$ се дадени со $x = x' + nm'$, за $n \in \mathbb{Z}$, Сите решенија кои не се еквивалкентни, т.е. не се конгруентни по модул m се дадени со $x = x' + nm'$ каде $n = 0, 1, 2, ..., d-1$. Според тоа, ако $d \mid b$, тогаш линеарната конгруентна равенка $ax \equiv b(\mathrm{mod}\, m)$ има точно d решенија по модул m. ■

Лема 4.2 експлицитно го дава решението на равенката $a'x \equiv b'(\mathrm{mod}\, m')$, кога $(a', m') = 1$, што не е случај кога теорема 4.3 ја докажавме без користењето на теоремата на Ојлер. Затоа, се поставува прашањето како на друг начин да се реши линеарната конгруентна равенка $a'x \equiv b'(\mathrm{mod}\, m')$, кога $(a', m') = 1$. Одговорот на ова прашање е едноставен. Имено, од $(a', m') = 1$ следува дека постојат броеви $u, v \in \mathbb{Z}$ такви што $a'u + m'v = 1$ и u, v може да се определат со Евклидовиот алгоритам. Сега имаме $a'u \equiv 1(\mathrm{mod}\, m')$, па затоа $x \equiv ub'(\mathrm{mod}\, m')$.

4.5. Претходно се осврнавме на решавањето на линеарната конгруентна равенка од видот $ax \equiv b(\mathrm{mod}\, m)$, $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Друг начин за решавање на оваа равенка е со помош на факторизацијата на модулот $m = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$.

Нека $m_i = p_i^{\alpha_i}$, $i = 1, 2, ..., k$. Јасно, броевите m_i, $i = 1, 2, ..., k$ се по парови заемно прости и важи $[m_1, m_2, ..., m_k] = m$. Сега, од теоремата 1.10 следува дека проблемот за наоѓање на решенијата на равенката $ax \equiv b\,(\mathrm{mod}\, m)$ е еквивалентен на решавање на системот линеарни конгруентни равенки $ax \equiv b\,(\mathrm{mod}\, m_i), i = 1, 2, ..., k$. Секоја од равенките на последниот систем може многу полесно да се реши, бидејќи најчесто броевите m_i, $i = 1, 2, ..., k$ се многу помали од m. Нека претпоставиме дека линеарните конгруентни равенки $ax \equiv b(\mathrm{mod}\, m_i), i = 1, ..., k$ имаат решенија $x \equiv b_i(\mathrm{mod}\, m_i)$, $i = 1, ..., k$. Тогаш почетниот проблем се сведува на решавање на системот линеарни конгруентни равенки од видот

$$x \equiv b_1(\mathrm{mod}\, m_1), x \equiv b_2(\mathrm{mod}\, m_2), ..., x \equiv b_k(\mathrm{mod}\, m_k), \qquad (4)$$

со една непозната и со заемно прости модули, односно $(m_i, m_j) = 1$ за $i \neq j$. За да го решиме системот (4) ќе ја користиме следнава теорема.

4.6. Теорема (Кинеска теорема за остатоци). Нека $m=m_1...m_k$, $(m_i,m_j)=1$, за $i\neq j$, броевите M_s и $M_s^{'}$, $s=1,2,...,k$ се определени со условите

$$m_1m_2...m_k=M_sm_s,\ M_sM_s^{'}\equiv 1(\mathrm{mod}\, m_s) \tag{5}$$

и

$$x_0=M_1M_1^{'}b_1+M_2M_2^{'}b_2+...+M_kM_k^{'}b_k.$$

Тогаш постои единствено решение на системот (4) по модул m дадено со

$$x\equiv x_0(\mathrm{mod}\, m_1m_2...m_k). \tag{6}$$

Доказ. Нека x е определено со условот (6). Од условите (5) следува дека $m_s\mid M_j$, за $j\neq s$ и $M_sM_s^{'}b_s\equiv b_s\ (\mathrm{mod}\, m_s)$. Затоа за секој $s=1,2,...,k$ последователно добиваме

$$\begin{aligned}
&x\equiv M_1M_1^{'}b_1+M_2M_2^{'}b_2+...+M_kM_k^{'}b_k\ (\mathrm{mod}\, m_1m_2...m_k),\\
&x\equiv M_1M_1^{'}b_1+M_2M_2^{'}b_2+...+M_kM_k^{'}b_k\ (\mathrm{mod}\, m_s),\\
&x\equiv M_sM_s^{'}b_s\ (\mathrm{mod}\, m_s),\\
&x\equiv b_s\ (\mathrm{mod}\, m_s),
\end{aligned}$$

што значи дека x е решение на системот (4). Понатаму, нека x' е друго решение на системот (4). Тогаш $x-x'\equiv 0\ (\mathrm{mod}\, m_i)$ за $i=1,2,...,k$. Од $(m_i,m_j)=1$ за $i\neq j$ добиваме $x\equiv x'\ (\mathrm{mod}\, m_1m_2...m_k)$ што значи дека решението x е единствено по модул $m=m_1m_2...m_k$. ■

4.7. Кинеската теорема за остатоци може да се обопшти за модули $m_1,m_2,...,m_k$ кои не се заемно прости.

Теорема. Системот линеарни конгруентни равенки (4) има решение ако и само ако $(m_i,m_j)\mid(b_i-b_j)$ за секои $i,j=1,2,...,k,\ i\neq j$. Ако системот (4) има решение, тогаш тоа е единствено по модул $[m_1,m_2,...,m_k]$. ■

4.8. Во досегашните изложувања разгледувавме линеарна конгруентна равенка и систем линеарни конгруентни равенки со една непозната. Во следната теорема ќе докажеме кога систем од две линеарни конгруентни равенки со две непознати има единствено решение.

Теорема. Ако $(cf-ed,m)=1$, тогаш системот равенки

$$\begin{cases} cx+ey\equiv a(\mathrm{mod}\, m)\\ dx+fy\equiv b(\mathrm{mod}\, m)\end{cases} \tag{7}$$

има единствено решение за *x* и *y* по модул *m*.

Доказ . Нека претпоставиме дека постои решение на системот равенки (4).

Ако првата равенка ја помножиме со *f*, втората со *e* и добиените равенки ги одземеме, добиваме

$$(cf-de)x \equiv af-be \pmod{m}. \tag{8}$$

Ако ја помножиме првата равенка со *d*, втората со *c* и ја одземеме првата од втората равенка добиваме

$$(cf-de)y \equiv bc-ad \pmod{m}. \tag{9}$$

Бидејќи $(cf-ed,m)=1$ постои единствен *x* по модул *m* кој ја задоволува (8) и постои единствен *y* по модул *m* кој ја задоволува (9). Затоа, ако постои решение на системот (7), тоа е единствено по модул *m*.

Бидејќи $(cf-ed,m)=1$ следува дека постои $z \in \mathbb{Z}$ таков што

$$z(cf-ed) \equiv 1 \pmod{m}. \tag{10}$$

Вака определеното z ќе го искористиме за да ги решиме равенките (8) и (9). Ако x и y ги задоволуваат (8) и (9), тогаш

$$\begin{cases} x \equiv z(cf-de)x \equiv z(af-be) \pmod{m} \\ y \equiv z(cf-de)y \equiv z(bc-ad) \pmod{m}. \end{cases} \tag{11}$$

Ќе докажеме дека (7) има решение. Нека x, y и z се дадени со (10) и (11). Тогаш

$$\begin{aligned} cx+ey &\equiv cz(af-be)+ez(bc-ad) \equiv azcf-azed \\ &\equiv az(cf-de) \equiv a \pmod{m} \\ dx+fy &\equiv dz(af-be)+fz(bc-ad) \equiv fzbc-dzbc \\ &\equiv bz(cf-de) \equiv b \pmod{m}. \end{aligned}$$

Според тоа, постои решение на (7) и освен тоа докажавме дека тоа е единствено по модул m. ■

4.9. Пример. Реши ја линеарната конгруентна равенка

$$3x \equiv 20 \pmod{35}.$$

Решение. Имаме $(3,35)=1$, па затоа

$$x \equiv 20 \cdot 3^{\varphi(35)-1} \equiv 30 \cdot 3^{23} \equiv 30 \pmod{35}$$

е решение на дадената равенка. ■

4.10. Пример. Реши ја линеарната конгруентна равенка

$$42x \equiv 50 \pmod{76}.$$

Решение. Од $(42,76)=2 \mid 50$ следува дека дадената равенка има решение. Сега, можеме да скратиме со $(42,76)=2$ и добиваме

$$21x \equiv 25 \pmod{38}.$$

Понатаму, $0 \equiv 38 \pmod{38}$, па ако ги собереме последните две конгруенции наоѓаме $21x \equiv 63 \pmod{38}$. Но, $(21,38)=1$, па затоа во последната конгруенција мо-

жеме да скратиме со 21, со што добиваме $x \equiv 3 \pmod{38}$. Јасно, решенијата по модул 76 се дадени со

$$x \equiv 3 \pmod{76} \text{ и } x \equiv 41 \pmod{76}. \blacksquare$$

4.11. Пример. Реши ја линеарната конгруентна равенка

$$11x \equiv 25 \pmod{60}.$$

Решение. Бидејќи $(11,60)=1$, равенката има точно едно решение. Решението x мора да биде деливо со 5 бидејќи $11x = 25 + 60k$ за некој $k \in \mathbb{Z}$. Нека $x = 5y$. Тогаш

$$55y \equiv 25 \pmod{60}$$

и ако поделиме со 5 добиваме

$$\begin{aligned} 11y &\equiv 5 \pmod{12} \\ -y &\equiv 5 \pmod{12} \\ y &\equiv -5 \pmod{12} \\ y &\equiv 7 \pmod{12}. \end{aligned}$$

Затоа $x \equiv 35 \pmod{60}$. $\blacksquare$

4.12. Пример. Реши го системот линеарни конгруентни равенки

$$x \equiv b_1 \pmod{4},\ x \equiv b_2 \pmod{5},\ x \equiv b_3 \pmod{7}.$$

Решение. Имаме $4 \cdot 5 \cdot 7 = 35 \cdot 4 = 28 \cdot 5 = 20 \cdot 7$ и притоа важи

$$35 \cdot 3 \equiv 1 \pmod{4}, \quad 28 \cdot 2 \equiv 1 \pmod{5}, \quad 20 \cdot 6 \equiv 1 \pmod{7},$$

па затоа

$$x_0 = 35 \cdot 3b_1 + 28 \cdot 2b_2 + 20 \cdot 6b_3 = 105b_1 + 56b_2 + 120b_3,$$

и општото решение на дадениот систем е

$$x \equiv 105b_1 + 56b_2 + 120b_3 \pmod{140}.$$

На пример, општото решение на системот

$$x \equiv 1 \pmod{4}, \quad x \equiv 3 \pmod{5}, \quad x \equiv 2 \pmod{7}$$

е дадено со $x \equiv 105 \cdot 1 + 56 \cdot 3 + 120 \cdot 2 \equiv 93 \pmod{140}$, а општото решение на системот

$$x \equiv 3 \pmod{4}, \quad x \equiv 2 \pmod{5}, \quad x \equiv 6 \pmod{7}$$

е дадено со $x \equiv 105 \cdot 3 + 56 \cdot 2 + 120 \cdot 6 \equiv 27 \pmod{140}$. $\blacksquare$

4.13. Пример. Реши го системот линеарни конгруентни равенки

$$x \equiv 5 \pmod{6},\ x \equiv 3 \pmod{10},\ x \equiv 8 \pmod{15}.$$

Решение. Очигледно дадениот систем ги исполнува условите од воопштената Кинеска теорема за остатоци, па затоа тој има решение. Решението на равенката

$$x \equiv 5 \pmod{6}$$

има вид $5+6t, t\in\mathbb{Z}$. Со замена во втората равенка ја добиваме равенката

$$5+6t\equiv 3\,(\mathrm{mod}\,10),$$

која е еквивалентна со равенката $6t\equiv 8\,(\mathrm{mod}\,10)$, односно со равенката

$$3t\equiv 4\,(\mathrm{mod}\,5),$$

чие решение е $t\equiv 3\,(\mathrm{mod}\,5)$. Оттука $t=3+5u, u\in\mathbb{Z}$, а $x=23+30u, u\in\mathbb{Z}$. Со замена во третата равенка ја добиваме равенката

$$23+30u\equiv 8\,(\mathrm{mod}\,15)$$

која е еквивалентна со равенкта $30u\equiv 0\,(\mathrm{mod}\,15)$ и чие решение е $u=0+v, v\in\mathbb{Z}$, па затоа решението на даденият систем е

$$x=23+30v, v\in\mathbb{Z}.\ \blacksquare$$

4.14. Пример. Определи ги сите природни броеви $n\geq 2$ за кои важи следниот услов: За сите цели броеви a,b заемно прости со n е исполнето

$$a\equiv b(\mathrm{mod}\,n) \text{ ако и само ако } ab\equiv 1(\mathrm{mod}\,n).$$

Решение. Ако од $a\equiv b(\mathrm{mod}\,n)$ следува $ab\equiv 1(\mathrm{mod}\,n)$, тогаш

$$a^2\equiv ab\equiv 1(\mathrm{mod}\,n).$$

Обратно, ако $a^2\equiv 1(\mathrm{mod}\,n)$, тогаш од $ab\equiv 1(\mathrm{mod}\,n)$ следува $a^2\equiv ab(\mathrm{mod}\,n)$, односно $a\equiv b(\mathrm{mod}\,n)$.

Значи доволно е да ги најдеме сите цели броеви a заемно прости со n за кои $a^2\equiv 1(\mathrm{mod}\,n)$. Нека $n=p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$ е канонична факторизација на бројот n. Од $p_i^{\alpha_i}\mid n$ следува $a^2\equiv 1(\mathrm{mod}\,p_i^{\alpha_i})$ за $i=1,2,...,k$. Доволно е да ги определиме сите цели броеви заемно прости со p_i за кои важи

$$a^2\equiv 1(\mathrm{mod}\,p_i^{\alpha_i}).$$

Во тој случај, од Кинеската теорема за остатоци следува дека системот конгруентни равенки

$$\begin{cases} a^2\equiv 1(\mathrm{mod}\,p_1^{\alpha_1}),\\ a^2\equiv 1(\mathrm{mod}\,p_2^{\alpha_2}),\\ .....\\ a^2\equiv 1(\mathrm{mod}\,p_k^{\alpha_k}) \end{cases}$$

има единствено решение по модул $p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}=n$.

Ако $p_i\geq 3$, тогаш $(2,p_i)=1$, па важи $2^2\equiv 1(\mathrm{mod}\,p_i^{\alpha_i})$. Од последната конгруенција имаме $p_i=3$ и $\alpha_i=1$.

Ако $p_i = 2$, од $(2,3)=1$ следува $3^2 \equiv 1 (\mathrm{mod}\, 2^{\alpha_i})$, од каде $\alpha_i \in \{1,2,3\}$.

Според тоа, $n \in \{2,3,4,6,8,12,24\}$. ■

4.15. Пример. Нека m и n се природни броеви такви што за секој природен број k важи $(11k-1,m)=(11k-1,n)$. Докажи дека за некој цел број s важи $\frac{m}{n}=11^s$.

Решение. Нека $m=11^a p, n=11^b q$ при што $a,b \geq 0$ и броевите p,q не се деливи со 11. Ќе докажеме дека $p=q$, од каде што ќе следува тврдењето на задачата.

Бидејќи $(p,11)=1$ според Кинеската теорема за остатоци постои природен број x таков што

$$x \equiv 0 (\mathrm{mod}\, p),\ x \equiv -1 (\mathrm{mod} 11).$$

Но, тогаш $x=11k-1$ за некој природен број k, па затоа

$$p=(x,11^a p)=(11k-1,m)=(11k-1,n)=(x,11^b q) \leq q.$$

На потполно идентичен начин се докажува дека $q \leq p$, па затоа $p=q$. ■

4.16. Пример. Докажи, дека системот

$$5x+y \equiv 3 (\mathrm{mod} 33),$$
$$x+2y \equiv 1 (\mathrm{mod} 21)$$

нема решение.

Решение. Имаме $[33,21]=231$. Од првата конгруенција следува

$$y \equiv 3-5x+33i (\mathrm{mod}\, 231), i=0,1,2,...,6.$$

Заменуваме во втората конгруенција и добиваме $9x \equiv 5+66i (\mathrm{mod}\, 21)$ што не е можно бидејќи $5+66i \not\equiv 0 (\mathrm{mod}\, 3)$ за секој $i \in \mathbb{N}$. ■

4.17. Пример. Определи критериум за решливост на системот

$$\begin{cases} a_1x+b_1y \equiv c_1 (\mathrm{mod}\, m_1) \\ a_2x+b_2y \equiv c_2 (\mathrm{mod}\, m_2). \end{cases}$$

Решение. Нека $[m_1,m_2]=m$ и $m=m_1q_1=m_2q_2$. Дадениот систем е еквивалентен на системот

$$\begin{cases} a_1q_1x+b_1q_1y \equiv c_1q_1 (\mathrm{mod}\, m) \\ a_2q_2x+b_2q_2y \equiv c_2q_2 (\mathrm{mod}\, m) \end{cases}$$

од кој следува

$$\begin{cases} (a_1b_2-b_1a_2)x \equiv c_1b_2-b_1c_2 (\mathrm{mod}\, d) \\ (a_1b_2-b_1a_2)y \equiv c_2a_1-a_2c_1 (\mathrm{mod}\, d), \end{cases}$$

каде $d=(m_1,m_2)$. Нека $(a_1b_2-b_1a_2,d)=\delta$. Тогаш бараниот критериум е

$$0 \equiv c_1b_2-b_1c_2 \equiv c_2a_1-a_2c_1 (\mathrm{mod}\, \delta).$$ ■

5. НЕЛИНЕАРНИ КОНГРУЕНТНИ РАВЕНКИ

5.1. Теорема. Нека p е прост број. Конгруентната равенка

$$x^2 \equiv -1 (\mathrm{mod}\, p)$$

има решение ако и само ако $p = 2$ или $p \equiv 1 (\mathrm{mod}\, 4)$.

Доказ. Ако $p = 2$, тогаш $x = 1$ е едно решение на дадената равенка.

Ако $p \equiv 1 (\mathrm{mod}\, 4)$, тогаш од теоремата на Вилсон следува

$$\begin{aligned} -1 &\equiv (1 \cdot 2 \cdot \ldots \cdot \tfrac{p-1}{2}) \cdot (\tfrac{p+1}{2} \cdot \ldots (p-2)(p-1)) \\ &= (1 \cdot 2 \cdot \ldots \cdot \tfrac{p-1}{2}) \cdot ((p - \tfrac{p-1}{2}) \cdot \ldots (p-2)(p-1)) \\ &\equiv (1 \cdot 2 \cdot \ldots \cdot \tfrac{p-1}{2}) \cdot (\tfrac{p-1}{2} \cdot \ldots \cdot 2 \cdot 1) = ((\tfrac{p-1}{2})!)^2 (\mathrm{mod}\, p), \end{aligned}$$

што значи дека $x = (\frac{p-1}{2})!$ е едно решение на дадената равенка.

Нека $p \equiv 3 (\mathrm{mod}\, 4)$. Да претпоставиме дека постои $x \in \mathbb{Z}$ таков што $x^2 \equiv -1 (\mathrm{mod}\, p)$. Тогаш

$$x^{p-1} = (x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} = -1 (\mathrm{mod}\, p),$$

што противречи на малата теорема на Ферма. ■

5.2. Последица. Постојат бесконечно многу прости броеви од видот $4k+1$, $k \in \mathbb{N}$.

Доказ. Нека претпоставиме дека има конечно многу прости броеви од видот $4k+1$ и нека се тоа броевите $p_1, p_2, \ldots, p_n$. Нека p е прост делител на бројот

$$m = 4p_1^2 p_2^2 \ldots p_n^2 + 1.$$

Тогаш конгрунетната равенка $x^2 \equiv -1 (\mathrm{mod}\, p)$ има решение $2p_1 p_2 \ldots p_n$, па од теоремата 5.1 следува дека $p \equiv 1 (\mathrm{mod}\, 4)$. Јасно, $p \neq p_i$, за $i = 1, 2, \ldots, n$, што противречи на претпоставката. Конечно, од добиената противречност следува дека постојат бесконечно многу прости броеви од видот $4k+1$. ■

5.3. Дефиниција. За полиномните конгруентни равенки

$$f(x) \equiv 0 (\mathrm{mod}\, m) \text{ и } g(x) \equiv 0 (\mathrm{mod}\, m)$$

ќе велиме дека се *еквивалентни* ако имаат исти решенија.

5.4. Лема. Ако $b_i \equiv a_i (\mathrm{mod}\, m)$, $i = 0, 1, 2, \ldots, n$, тогаш равенките

$$\sum_{i=0}^{n} b_i x^{n-i} \equiv 0 (\mathrm{mod}\, m) \text{ и } \sum_{i=0}^{n} a_i x^{n-i} \equiv 0 (\mathrm{mod}\, m)$$

се еквивалентни.

Доказ. Од $b_i \equiv a_i \pmod m$, $i = 0,1,2,...,n$ следува дека $b_i x^{n-i} \equiv a_i x^{n-i} \pmod m$, $i = 0,1,2,...,n$, па затоа

$$\sum_{i=0}^{n} b_i x^{n-i} \equiv \sum_{i=0}^{n} a_i x^{n-i} \pmod m .$$

Според тоа, u е решение на $\sum_{i=0}^{n} b_i x^{n-i} \equiv 0 \pmod m$ ако и само ако u е решение на

$$\sum_{i=0}^{n} a_i x^{n-i} \equiv 0 \pmod m ,$$

што значи дека дадените равенки се еквиваленsни. ■

5.5. Нека $m = p_1^{t_1} p_2^{t_2} ... p_r^{t_r}$ е каноничното претставување на m. Тогаш конгруентната равенка

$$f(x) \equiv 0 \pmod m , \tag{1}$$

е еквивалентна на системот конгруентни равенки

$$f(x) \equiv 0 \pmod{p_i^{t_i}} , \ i = 1,2,...,r . \tag{2}$$

Навистина, бидејќи $[p_1^{t_1}, p_2^{t_2}, ..., p_r^{t_r}] = m$ важи $f(u) \equiv 0 \pmod m$ ако и само ако $f(u) \equiv 0 \pmod{p_i^{t_i}}$, $i = 1,2,...,r$.

Нека секоја равенка од системот конгруентни равенки (2) има решение и да претпоставиме дека $i-$тата конгруентна равенка има точно k_i решенија: $a_i^{(1)}, a_i^{(2)}, ..., a_i^{(k_i)}$. Сега u е решение на (1) ако и само ако за секој i постои j_i таков што $u \equiv a_i^{(j_i)} \pmod{p_i^{t_i}}$. Бидејќи модулите $p_i^{t_i}$ се по парови заемно прости од Кинеската теорема за остатоци следува дека постои b_i таков што $mp_i^{-t_i} b_i \equiv 1 \pmod{p_i^{t_i}}$ и за u добиваме

$$u \equiv \sum_{i=1}^{r} mp_i^{-t_i} b_i a_i^{(j_i)} \pmod m .$$

Според тоа, за секоја вредност $j_1, j_2, ..., j_r$ имаме различен u по модул m и секој j_i прима точно k_i вредности. Значи, точна е следнава теорема.

Теорема. Ако $m = p_1^{t_1} p_2^{t_2} ... p_r^{t_r}$ е каноничното претставување на m и $N(m)$ е бројот на решенијата на конгруентната равенка (1), тогаш $N(m) = \prod_{i=1}^{r} N(p_i^{t_i})$. ■

5.6. На крајот од овој параграф ќе разгледаме нелинеарни конгруентни равенки по прости модули. Претходно ќе ја докажеме следнава лема.

Лема. Конгруентната равенка $\sum_{i=0}^{n} a_i x^{n-i} \equiv 0 (\mathrm{mod}\, m)$, $(a_0, m) = 1$ е еквивалентна на конгруентна равенка од видот

$$x^n + \sum_{i=1}^{n} b_i x^{n-i} \equiv 0 (\mathrm{mod}\, m). \tag{3}$$

Доказ. Линеарната конгруентна равенка $a_0 x \equiv 1 (\mathrm{mod}\, m)$ има единствено решение $x \equiv b (\mathrm{mod}\, m)$ и притоа $(b, m) = 1$. Според тоа, дадената равенка е еквивалентна на равенката

$$\sum_{i=0}^{n} b a_i x^{n-i} \equiv 0 (\mathrm{mod}\, m).$$

Ставаме $b a_i = b_i$ и од лемата 5.4 следува дека дадената равенка е еквивалентна на равенката (3). ■

5.7. Теорема. Нека p е прост број. Ако редот на конгруентната равенка

$$f(x) \equiv 0 (\mathrm{mod}\, p), \tag{4}$$

е поголем или еднаков на p, тогаш секој цел број е решение на (4) или постои полином $g(x)$ со целобројни коефициенти и коефициент 1 пред највисокиот степен, таков што равенката $g(x) \equiv 0 (\mathrm{mod}\, p)$ е еквивалентна на равенката (4). Притоа $\deg g < p$.

Доказ. Од $n \geq p$ имаме $f(x) = (x^p - x) q(x) + r(x)$, каде $q(x)$ и $r(x)$ се полиноми со целобројни коефициенти и $\deg r < p$. Од малата теорема на Ферма следува

$$f(x) \equiv r(x) (\mathrm{mod}\, p), \text{ за секој } x \in \mathbb{Z}. \tag{5}$$

Да го разгледаме полиномот

$$r(x) = b_0 x^k + b_1 x^{k-1} + \ldots + b_k,\ k < p.$$

Ако $b_i = 0,\ i = 0,1,2,\ldots,k$, тогаш $f(x) \equiv 0 (\mathrm{mod}\, p)$ за секој $x \in \mathbb{Z}$. Ако $b_0 \neq 0$, тогаш бидејќи p е прост број $(b_0, p) = 1$ или p, па согласно лемата 5.4 можеме да претпоставиме дека $(b_0, p) = 1$. Според лемата 5.6 равенката $r(x) \equiv 0 (\mathrm{mod}\, p)$ е еквивалентна на равенка $g(x) \equiv 0 (\mathrm{mod}\, p)$, при што коефициентот пред највисокиот степен на полиномот $g(x)$ е 1 и $\deg g < p$. Според (5) равенките $g(x) \equiv 0 (\mathrm{mod}\, p)$ и (4) се еквивалентни. ■

5.8. Теорема (Лагранж). Нека p е прост број. Ако $f(x)$ е полином од $n-$ти степен со целобројни коефициенти и водечки коефицинт a_0, заемно прост со p, тогаш конгруентната равенка $f(x) \equiv 0 (\mathrm{mod}\, p)$ има најмногу n решенија.

Доказ. Ако $n=0$, тогаш $f(x)=a_0\not\equiv 0(\mathrm{mod}\,p)$, т.е. $f(x)\equiv 0(\mathrm{mod}\,p)$ нема решение. Ако $n=1$, тогаш според лемата 4.2 конгруентната равенка $f(x)\equiv 0(\mathrm{mod}\,p)$ има точно едно решение.

Нека тврдењето е точно за секоја конгруентна равенка со степен помал од n и нека постојат повеќе од n решенија на конгруентната равенка $f(x)\equiv 0(\mathrm{mod}\,p)$, чиј степен е n. Нека $f(x)=\sum_{i=0}^{n} a_i x^{n-i}$ и $u_i, i=1,2,...,n+1$ се решенија на равенката $f(x)\equiv 0(\mathrm{mod}\,p)$ такви што $u_i\not\equiv u_j\ (\mathrm{mod}\,p), i\neq j$. Дефинираме полином

$$g(x)=f(x)-a_0(x-u_1)...(x-u_n).$$

Полиномот $g(x)$ е идентичен со нултиот полином или е полином со степен k, $0\le k<n$.

Ќе докажеме дека $f(x)$ е идентичен на нула или е полином чии коефициенти се деливи со p. Нека $g(x)=\sum_{i=0}^{k} b_i x^{k-i}$ и нека b_j е коефициентот со најмал индекс кој не е делив со p. Земаме $h(x)=b_j x^{k-j}+b_{j+1}x^{k-j-1}+...+b_k$. Тогаш степенот на конгруентната равенка $h(x)\equiv 0(\mathrm{mod}\,p)$ е $k-j, 0\le k-j<n$ и $h(u_i)\equiv 0(\mathrm{mod}\,p)$, за $i=1,2,...,n$ што противречи на индуктивната претпоставка.

Според тоа, $g(x)\equiv 0(\mathrm{mod}\,p)$ за секој $x\in\mathbb{Z}$, а оттука следува дека

$$f(x)\equiv a_0(x-u_1)...(x-u_n)(\mathrm{mod}\,p).$$

Во случајов $a_0(u_{n+1}-u_1)...(u_{n+1}-u_n)\equiv f(u_{n+1})(\mathrm{mod}\,p)$ што противречи на

$$(a_0,p)=1,\ u_{n+1}\not\equiv u_i(\mathrm{mod}\,p), i=1,2,...,n \text{ и } f(u_{n+1})\equiv 0(\mathrm{mod}\,p).$$

Конечно, од добиената противречност следува дека не постојат повеќе од n решенија на конгруентната равенка $f(x)\equiv 0(\mathrm{mod}\,p)$ чиј степен е n. ■

5.9. Последица. Ако конгруентната равенка

$$\sum_{i=0}^{n} a_i x^{n-i}\equiv 0(\mathrm{mod}\,p),$$

p е прост број, има повеќе од n решенија, тогаш $p\mid a_i, i=0,1,2,...,n$.

Доказ. Непосредно следува од теоремата 5.8. ■

5.10. Последица. Ако $p\ge 5$ е прост број, тогаш броителот на рационалниот број

$$1+\tfrac{1}{2}+\tfrac{1}{3}+...+\tfrac{1}{p-1} \tag{6}$$

е делив со p^2.

Доказ. Нека $f(x)=x^{p-1}-1-(x-1)(x-2)...(x-p+1)$. Конгруентната равенка $f(x)\equiv 0(\mathrm{mod}\, p)$ има $p-1$ решение и тоа се броевите $1,2,...,p-1$. Понатаму, $\deg f \le p-2$, па од последицата 5.9 следува дека сите коефициенти на полиномот

$$f(x)=a_{p-2}x^{p-2}+...+a_1x+a_0$$

се деливи со p, односно $a_n\equiv 0(\mathrm{mod}\, p)$ за $n=0,1,..,p-2$. Сега,

$$f(p)=p^{p-1}-1-(p-1)!=a_{p-2}p^{p-2}+...+a_1p+a_0, \qquad (7)$$

па како $a_0=-1-(p-1)!$, со замена во (7), по делењето со p добиваме

$$p^{p-2}-a_{p-2}p^{p-3}-...-a_2p-a_1=0.$$

Сега, од $p\mid a_2$ и од претходното равенство следува дека $p^2\mid a_1$. Меѓутоа, лесно се гледа дека

$$\frac{a_1}{(p-1)!}=1+\frac{1}{2}+\frac{1}{3}+...+\frac{1}{p-1},$$

од што следува бараното тврдење. ■

5.11. Коментар. Во доказот на претходната последица имаме $a_0=-1-(p-1)!$ и како $p\mid a_0$, ова дава друг доказ на теоремата на Вилсон.

5.12. Последица. Нека $f(x), g(x)$ и $h(x)$ се полиноми со целобројни коефициенти и степени n,m и s соодветно, такви што $f(x)=g(x)h(x)$ и нека p е прост број. Ако равенката $f(x)\equiv 0(\mathrm{mod}\, p)$ има n решенија, тогаш равенките $g(x)\equiv 0(\mathrm{mod}\, p)$ и $h(x)\equiv 0(\mathrm{mod}\, p)$ имаат m и s решенија, соодветно.

Доказ. Непосредно следува од теоремата 5.8. ■

5.13. Последица (Лагранж). Нека p е прост број. Конгруентната равенка

$$f(x)=x^n+\sum_{i=1}^{n}a_ix^{n-i}\equiv 0(\mathrm{mod}\, p),\ n<p,\ (a_n,p)=1$$

има точно n решенија ако и само ако сите коефициенти на остатокот од делењето на $x^{p-1}-1$ со $f(x)$ се деливи с p.

Доказ. Нека $x^{p-1}-1=f(x)q(x)+r(x)$, каде $q(x)$ и $r(x)$ се полиноми со целобројни коефициенти и степенот на $q(x)$ е $p-1-n$, а степенот на $r(x)$ е помал од n.

Ако конгруентната равенка $f(x)\equiv 0(\mathrm{mod}\, p)$ има n решенија, тогаш сите тие се решенија и на равенката $r(x)\equiv 0(\mathrm{mod}\, p)$, што според последицата 5.9 е можно ако и само ако сите коефициенти на $r(x)$ се деливи со p.

Ако сите коефицинти на $r(x)$ се деливи со p, тогаш равенките

$$x^{p-1}-1\equiv 0(\mathrm{mod}\, p) \text{ и } f(x)q(x)\equiv 0(\mathrm{mod}\, p)$$

се еквивалентни. Сега, од малата теорема на Ферма следува дека конгруентната равенка $x^{p-1}-1\equiv 0(\mathrm{mod}\, p)$ има $p-1$ решенија. Но, според теоремата 5.8 равенките $q(x)\equiv 0(\mathrm{mod}\, p)$ и $f(x)\equiv 0(\mathrm{mod}\, p)$ имаат најмногу по $p-1-n$ и n решенија соодветно, па од последицата 5.10 следува дека овие равенки имаат точно $p-1-n$ и n решенија. ■

5.14. Пример. Реши ги равенките

а) $x^5+2x^4-2x^3-2x^2+2x-1\equiv 0(\mathrm{mod}3)$,

б) $x^6+x^5-2x^2-x\equiv 0(\mathrm{mod}5)$,

в) $x^{14}-x^{13}-x^2+2x+1\equiv 0(\mathrm{mod}13)$.

Решение. а) Бидејќи

$$x^5+2x^4-2x^3-2x^2+2x-1=(x^3-x)(x^2+2x-1)+x-1$$

дадената равенка е еквивалентна на равенката $x-1\equiv 0(\mathrm{mod}3)$, т.е. на равенката $x\equiv 1(\mathrm{mod}3)$.

б) Дадената равенка е еквивалентна на равенката $-x^2\equiv 0(\mathrm{mod}5)$, т.е. на равенката $x\equiv 0(\mathrm{mod}5)$.

в) Дадената равенка е еквивалентна на равенката $x\equiv -1(\mathrm{mod}13)$. ■

5.15. Пример. Реши ја конгруентната равенка $3x^3-4x^2-2x-4\equiv 0(\mathrm{mod}7)$.

Решение. Дадената равенка е еквивалентна на равенката

$$x^3+x^2-3x+1\equiv 0(\mathrm{mod}7). \qquad (8)$$

Сите коефициенти на остатокот $-49x^2+70x-21$ од делењето на x^7-x со x^3+x^2-3x+1 се деливи со 7, па затоа равенката (8) има три решенија. Конечно, $x\equiv 1,2,3(\mathrm{mod}7)$. ■

6. ЛЕМИ НА ШУР И ХЕНСЕЛ

6.11. Теорема (лема на Шур). Ако f е неконстантен полином со целобројни коефициенти, тогаш за бесконечно многу прости броеви p постои цел број x таков што $p\mid f(x)$.

Доказ. Нека $f(x)=b_m x^m+b_{m-1}x^{m-1}+...+b_1x+b_0$, и да претпоставиме дека $p_1, p_2,..., p_s$ се сите прости броеви кои се делители на $f(x)\neq 0,\ x\in\mathbb{Z}$. Тогаш бројот

$$\begin{aligned} f(b_0p_1p_2...p_s) &= b_0(b_m b_0^{m-1}(p_1p_2...p_s)^m+...+\ b_1p_1p_2...p_s+1)\\ &= b_0(Ap_1p_2...p_s+1), \end{aligned}$$

каде A е цел број делив со прост број различен од $p_1,..., p_s$, што е противречност. ■

6.2. Теорема (лема на Хенсел). Нека p е прост број, $f(x)$ е полином со целобројни коефициенти и $f'(x)$ е неговиот прв извод. Ако $f(a)\equiv 0(\mathrm{mod}\, p^j)$ и $f'(a)\not\equiv 0(\mathrm{mod}\, p)$, тогаш постои еден и само еден $t\in\{0,1,2,..., p-1\}$ таков што

$$f(a+tp^j)\equiv 0(\mathrm{mod}\, p^{j+1}).$$

Доказ. Ако се искористи Тејлоровиот развој на полиномот $f(x)$ во околина на точката a добиваме

$$f(a+tp^j)=f(a)+tp^j f'(a)+t^2p^{2j}\frac{f''(a)}{2!}+...+t^np^{nj}\frac{f^{(n)}(a)}{n!}. \qquad (1)$$

Ќе докажеме дека броевите $\frac{f^{(k)}(a)}{k!}$ се цели. Доволно е тврдењето да го докажеме за полиноми од видот $g(x)=x^m$, каде $m\geq k$. Тогаш имаме:

$$\frac{g^{(k)}(a)}{k!}=\frac{m(m-1)...(m-k+1)}{k!}a^{m-k}=\binom{m}{k}a^{m-k}\in\mathbb{Z}.$$

Затоа од (1) следува

$$f(a+tp^j)\equiv f(a)+tp^j f'(a)(\mathrm{mod}\, p^{j+1}).$$

Според тоа, за да биде $f(a+tp^j)\equiv 0(\mathrm{mod}\, p^{j+1})$, потребно и доволно е да важи

$$tf'(a)\equiv -\frac{f(a)}{p^j}(\mathrm{mod}\, p). \qquad (2)$$

Но,

$$f'(a)\not\equiv 0(\mathrm{mod}\, p),$$

па затоа од теоремата 4.3 следува дека линеарната конгруентна равенка (2) има единствено решение $t\in\{0,1,2,..., p-1\}$. ■

6.3. Последица. Конгруентната равенка

$$x^{p-1}-1\equiv 0(\mathrm{mod}\, p^j)$$

има точно $p-1$ решение за секој прост број p и секој природен број j.

Доказ. За $j=1$ тврдењето следува од малата теорема на Ферма. Нека претпоставиме дека тврдењето важи за некој $j\in\mathbb{N}$, т.е. дека $x_1, x_2,..., x_{p-1}$ се сите решенија на конгруентната равенка

$$f(x) = x^{p-1} - 1 \equiv 0 (\mathrm{mod}\, p^j).$$

Тогаш за секој i важи

$$f(x_i) \equiv 0 (\mathrm{mod}\, p^j) \text{ и } f'(x_i) = (p-1)x_i^{p-2} \not\equiv 0 (\mathrm{mod}\, p),$$

па од лемата на Хенсел следува дека постои единствен $t_i \in \{0,1,2,...,p-1\}$ таков што

$$f(x_i + t_i p^j) \equiv 0 (\mathrm{mod}\, p^{j+1}).$$

Тоа значи дека $y_i = x_i + t_i p^j$, $i = 1,2,...,p-1$ се решенија на конгруентната равенка $f(x) \equiv 0 (\mathrm{mod}\, p^{j+1})$. Останува да докажеме дека ова се сите решенија. Навистина, ако y' е некое решение на разгледуваната равенка, тогаш $f(y') \equiv 0 (\mathrm{mod}\, p^j)$, па затоа од индуктивната претпоставка следува дека $y' \equiv x_i (\mathrm{mod}\, p^j)$ за некој $i = 1,2,...,p-1$. Сега од единствеността на t_i следува дека $y' \equiv y_i (\mathrm{mod}\, p^{j+1})$. ■

6.4. Пример. Реши ја конгруентната равенка

$$x^2 + x + 47 \equiv 0 (\mathrm{mod}\, 7^3). \tag{3}$$

Решение. Прво ќе ја решаваме конгруентната равенка $x^2 + x + 47 \equiv 0 (\mathrm{mod}\, 7)$. Решнијата на оваа равенка се $x \equiv 1 (\mathrm{mod}\, 7)$ и $x \equiv 5 (\mathrm{mod}\, 7)$. Нека $f(x) = x^2 + x + 47$. Тогаш $f'(x) = 2x + 1$, па затоа $f'(1) = 3 \not\equiv 0 (\mathrm{mod}\, 7)$ и $f'(5) = 11 \not\equiv 0 (\mathrm{mod}\, 7)$. Тоа значи дека можеме да ја примениме лемата на Хенсел.

За да ја решиме конгруентната равенка (3) треба да решиме

$$f'(a)t \equiv -\frac{f(a)}{7} (\mathrm{mod}\, 7) \text{ за } a = 1,5.$$

Имаме:

1) $3t \equiv -7 (\mathrm{mod}\, 7)$, од каде следува $t = 0$, односно $a + 7t = 1$,

2) $11t \equiv -11 (\mathrm{mod}\, 7)$, од каде следува $t = 6$, односно $a + 7t = 47$.

Конечно, за да ја решиме конгруенцијата (3) треба да решиме

$$f'(a)t \equiv -\frac{f(a)}{49} (\mathrm{mod}\, 7) \text{ за } a = 1,47.$$

Имаме

1) $3t \equiv -1 (\mathrm{mod}\, 7)$, од каде следува $t = 2$, односно $a + 49t = 99$,

2) $11t \equiv -47 (\mathrm{mod}\, 7)$, од каде следува $t = 4$, односно $a + 49t = 243$.

Значи, решенија на (3) се

$$x \equiv 99 (\mathrm{mod}\, 7^3) \text{ и } x \equiv 243 (\mathrm{mod}\, 7^3). \blacksquare$$

7. РЕД НА БРОЈ ПО МОДУЛ

7.1. Обратното тврдење на теоремата на Ферма не важи. Така, на пример, $3^{90} \equiv 1 (\mathrm{mod}\, 91)$, меѓутоа $91 = 7 \cdot 13$ е сложен број. Од друга страна ако p е природен број и $0 < p < a$ е таков што $a^{p-1} \not\equiv 1 (\mathrm{mod} p)$, тогаш p не е прост број. Затоа, теоремата на Ферма содржи парцијален тест дали бројот е прост или не, т.е. може да се искористи да се докаже дека бројот p не е прост без наоѓање на нетривијален делител на p. Во натамошните разгледувања ќе се осврнеме на конгруенцијата $a^k \equiv 1 (\mathrm{mod}\, n)$, за $k \in \mathbb{N}$.

7.2. Дефиниција. Нека n е природен број и a е цел број таков што $(a,n) = 1$. *Ред на бројот* a *по модул* n, го нарекуваме најмалиот природен број $\delta = \delta(a,n)$ таков што $a^{\delta} \equiv 1 (\mathrm{mod}\, n)$.

Од $3^5 \equiv 1 (\mathrm{mod} 11)$ и $3^i \not\equiv 1 (\mathrm{mod} 11)$, за $i \in \{1,2,3,4\}$ следува дека $\delta(3,11) = 5$.

7.3. Теорема. Нека n е природен број, $(a,n) = 1$ и нека $\delta = \delta(a,n)$. Тогаш:

а) $a^m \equiv 1 (\mathrm{mod}\, n)$ за $m \in \mathbb{N}$ ако и само ако $\delta \mid m$,

б) $\delta \mid \varphi(n)$,

в) ако $r, s \in \mathbb{N}$, тогаш $a^r \equiv a^s (\mathrm{mod}\, n)$ ако и само ако $r \equiv s (\mathrm{mod}\, \delta)$,

г) $a^i \not\equiv a^j (\mathrm{mod}\, \delta)$ за $i, j \in \{1,2,...,\delta\}$, $i \neq j$,

д) ако m е природен број, тогаш редот на a^m по модул n е еднаков на $\frac{\delta}{(\delta,m)}$,

ѓ) редот за a^m по модул n е δ ако и само ако m и δ се заемно прости броеви.

е) низата $1, a, a^2, a^3, ...$ е периодична по модул n со минимален период δ.

Доказ. а) Ако $a^m \equiv 1 (\mathrm{mod}\, n)$ за некој природен број m, тогаш од $m = \delta q + r$, $0 \leq r < \delta$ добиваме $a^m = a^{\delta q + r} = a^{\delta q} a^r$, па затоа $a^r \equiv 1 (\mathrm{mod}\, n)$. Ако $r > 0$, тогаш претходната конгруенција противречи на фактот дека редот на a по модул n е δ, па затоа $r = 0$. Значи, $m = \delta q$, т.е. $\delta \mid m$.

Обратно, ако $m = \delta q$, тогаш

$$a^m \equiv a^{q\delta} \equiv (a^{\delta})^q \equiv 1 (\mathrm{mod}\, n).$$

б) Според теоремата на Ојлер имаме $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$ па од тврдењето под а) следува $\delta \mid \varphi(n)$.

в) Нека $r > s$. Бидејќи a и n се заемно прости добиваме $a^r \equiv a^s \pmod n$ ако и само ако $a^{r-s} \equiv 1 (\mathrm{mod}\, n)$. Според а) последното е возможно ако и само ако $\delta \mid (r-s)$ т.е. ако и само ако $r \equiv s (\mathrm{mod}\, \delta)$.

г) Непосредно следува од тврдењето под в)

д) Нека $d = (\delta, m)$. Тогаш $\delta = ud$ и $m = vd$, $(u,v) = 1$, па затоа

$$(a^m)^{\frac{\delta}{(\delta,m)}} = (a^m)^{\frac{ud}{d}} = a^{mu} = a^{uvd} = a^{(ud)v} = a^{\delta v} \equiv 1 (\mathrm{mod}\, n)$$

Нека претпоставиме t е таков што $(a^m)^t \equiv 1 (\mathrm{mod}\, n)$. Тогаш $a^{mt} \equiv 1 (\mathrm{mod}\, n)$ па од $\delta = \delta(a,n)$ и тврдењето под а) следува $\delta \mid mt$. Затоа $ud \mid vdt$ и како u и v се заемно прости добиваме $u \mid t$. Бидејќи $\delta = ud$, односно $u = \frac{\delta}{d} = \frac{\delta}{(\delta,m)}$ добиваме дека $\frac{\delta}{(\delta,m)}$ е делител на произволниот број t со својство $(a^m)^t \equiv 1 (\mathrm{mod}\, n)$, па од дефиницијата на ред по модул следува дека $\frac{\delta}{(\delta,m)}$ е ред за a^m по модул n.

ѓ) Непосредно следува од тврдењето под д).

е) Непосредно следува од в) и г). ■

7.4. Последица. Ако $p > 2$ е прост број и $a \in \mathbb{Z}$, тогаш за секој прост делител q на бројот $a^{p-1} + a^{p-2} + ... + a + 1$ важи $p \mid q-1$ или $p = q$.

Доказ. Ако $q \mid a-1$, тогаш $q \mid a^{p-1} + ... + a + 1 \equiv 1 + ... + 1 + 1 = p (\mathrm{mod}\, q)$, па затоа $q = p$.

Од друга страна, ако $q \nmid a-1$, тогаш редот на бројот a по модул q е делител на p, што значи дека е еднаков на p. Бидејќи овој ред е делител на $q-1$, следува дека $p \mid q-1$. ■

7.5. Теорема. Ако $(a,n) = (b,n) = 1$ и $\delta(a,n)$ е заемно прост со $\delta(b,n)$, тогаш

$$\delta(ab,n) = \delta(a,n) \cdot \delta(b,n).$$

Доказ. Нека $\delta(a,n) = R$ и $\delta(b,n) = S$. Тогаш

$$(ab)^{RS} = a^{RS} b^{RS} = (a^R)^S (b^S)^R \equiv 1 \cdot 1 \equiv 1 (\mathrm{mod}\, n)$$

Според теорема 7.3 а) имаме $\delta(ab,n) \mid RS$. Бидејќи R и S се заемно прости, постојат цели броеви r и s за кои $\delta(ab,n) = rs, rw = R$ и $sx = S$. Ќе докажеме дека $r = R$ и $s = S$. Од дефиницијата на r и s имаме

$$(ab)^{rs} = a^{rs} b^{rs} \equiv 1 (\mathrm{mod}\, n)$$
$$(a^{rs} b^{rs})^w \equiv 1 (\mathrm{mod}\, n)$$
$$(a^{rw})^s (b^{rw})^s \equiv 1 (\mathrm{mod}\, n)$$

Меѓутоа, бидејќи $a^{rw} \equiv 1 (\mathrm{mod}\, n)$ и $rw = R$ имаме $b^{Rs} \equiv 1 (\mathrm{mod}\, n)$. Од теорема 7.3 а) имаме $S = \delta(b,n) \mid Rs$ и како $(R,S) = 1$ следува $S \mid s$. Но, $s \mid S$, па затоа $S = s$. Аналогно се докажува дека $r = R$, па затоа $\delta(ab,n) = RS = \delta(a,n) \cdot \delta(b,n)$. ■

7.6. Теорема (Лукас). Ако n е природен број и ако постои цел број a таков што $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ и $a^{\frac{n-1}{p}} \not\equiv 1 (\mathrm{mod}\, n)$ за секој прост делител p на $n-1$, тогаш n е прост број.

Доказ. Од $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ следува $(a,n) = 1$ и од теоремата 3 а) имаме $\delta(a,n) \mid n-1$. Ако p е прост број таков што $p \mid n-1$, тогаш од $a^{\frac{n-1}{p}} \not\equiv 1 (\mathrm{mod}\, n)$ следува дека $\delta(a,n) \nmid \frac{n-1}{p}$. Навистина, ако $\delta(a,n) \mid \frac{n-1}{p}$, тогаш $a^{\frac{n-1}{p}} \equiv 1 (\mathrm{mod}\, n)$, што е противречност. Меѓутоа, $\delta(a,n) \mid n-1$ и $\delta(a,n) \nmid \frac{n-1}{p}$ за секој p кој е делител на $n-1$ повлекува $\delta(a,n) = n-1$. Сега од теоремата 7.3 б) следува $n-1 \mid \varphi(n)$ и како $\varphi(n) \le n-1$ добиваме $\varphi(n) = n-1$, што значи дека бројот n е прост. ■

7.7. Пример. Определи го редот на 2 по модул 53.

Решение. Од теорема 7.3 б) следува дека $\delta(a,n)$ треба да го бараме меѓу делителите на $\varphi(n)$. Според тоа, за да го определиме $\delta(a,n)$ треба да ги определиме делителите на $\varphi(n)$, а потоа последователно (во растечки редослед) за $d \mid \varphi(n)$ да провериме дали $a^d \equiv 1 (\mathrm{mod}\, n)$.

Првиот делител за кој е точна последната конгруенција е $\delta(a,n)$.

Во случајов имаме, $\varphi(53) = 53$ и делители на 52 се: 1, 2, 4, 13, 26 и 52. Бидејќи

$$2^1 \equiv 2 (\mathrm{mod}\, 53), \quad 2^2 \equiv 4 (\mathrm{mod}\, 53), \quad 2^4 \equiv 16 (\mathrm{mod}\, 53),$$
$$2^{13} \equiv 30 (\mathrm{mod}\, 53), \quad 2^{26} \equiv -1 (\mathrm{mod}\, 53)$$

заклучуваме дека $\delta(2,53) = 52$. ■

7.8. Пример. Нека $n, a > 1$ се природни броеви. Докажи дека $n \mid \varphi(a^n - 1)$.

Решение. Јасно, $a^n \equiv 1 (\mathrm{mod}\, a^n - 1)$ и $a^m \not\equiv 1 (\mathrm{mod}\, a^n - 1)$ за $0 < m < n$. Според тоа, редот на бројот a по модул $a^n - 1$ е n, па затоа $n \mid \varphi(a^n - 1)$. ■

7.9. Пример. Докажи дека секој прост делител на Ферматовиот број $2^{2^n} + 1$ за $n \ge 1$ има облик $p = 2^{n+1}k + 1$ за $k \in \mathbb{N}$.

Решение. Од $2^{2^n}+1\equiv 0(\mathrm{mod}\, p)$ следува $2^{2^n}\equiv -1(\mathrm{mod}\, p)$ и $2^{2^{n+1}}\equiv 1(\mathrm{mod}\, p)$. Нека $\delta(2,p)$ е редот на бројот 2 по модул p. Тогаш $\delta(2,p)\,|\,2^{n+1}$, па затоа $\delta(2,p)=2^m, m\le n+1$. Но, ако $m\le n$, тогаш $2^{2^m}\equiv 1(\mathrm{mod}\, p)$, од каде после степенување на 2^{n-m} добиваме $2^{2^n}\equiv 1(\mathrm{mod}\, p)$, што противречи на $2^{2^n}\equiv -1(\mathrm{mod}\, p)$, бидејќи $p\neq 2$. Значи, $m=n+1$ и $\delta(2,p)=2^{n+1}$. Конечно,

$$\delta(2,p)=2^{n+1}\,|\,\varphi(p)=p-1,$$

т.е. постои $k\in\mathbb{N}$ таков што $p=2^{n+1}k+1$. ■

7.10. Пример. Докажи, дека ако $(a,n)=1$ и $n=p_1^{a_1}p_2^{a_2}...p_t^{a_t}$ е каноничното разложување на n, тогаш редот на бројот a по модул n е еднаков на најмалиот заеднички содржател на редовите на a по модулите $p_i^{a_i}$, $i=1,2,...,t$.

Решение. Нека k_i ередот на a по модул $p_i^{a_i}$, k е ред на a по модул n и $m=[k_1,k_2,...,k_t]$. Тогаш, од конгруенцијата $a^k\equiv 1(\mathrm{mod}\, n)$ следуваат конгруенциите $a^k\equiv 1(\mathrm{mod}\ p_i^{a_i})$, $i=1,2,...,t$, па затоа $k_i\,|\,k$, за секој $i=1,2,...,t$, т.е. $m\le k$. Но, од друга страна од $a^{k_i}\equiv 1(\mathrm{mod}\ p_i^{a_i})$, $i=1,2,...,t$ следува $a^m\equiv 1(\mathrm{mod}\ p_i^{a_i})$ за $i=1,2,...,t$ од каде добиваме $a^m\equiv 1(\mathrm{mod}\, n)$. Но, тоа значи дека $k\le m$, па затоа $k=m$, што и требаше да се докаже. ■

7.11. Пример. Нека $a,b\in\mathbb{N}$ и $d=(a,b)$. Докажи дека ако n е произволен природен број и $\frac{b}{d}$ е непарен број, тогаш $(n^a+1,n^b-1)\le 2$.

Решение. Нека $m=n^d$, $a=dx, b=dy$. Според условот на задачата y е непарен број. Тогаш $n^a+1=n^{dx}+1=m^x+1$, $n^b-1=n^{dy}-1=m^y-1$.

Нека $(m^x+1,m^y-1)=l$. Ако $l>1$ и k е ред на m по модул l (јасно $(m,l)=1$), тогаш од конгруенцијата $m^y\equiv 1(\mathrm{mod}\, l)$ следува дека $k\,|\,y$, па значи k е непарен број. Понатаму, од конгруенцијата $m^x\equiv -1(\mathrm{mod}\, l)$ следува $m^{2x}\equiv 1(\mathrm{mod}\, l)$, па значи $k\,|\,2x$ и како k е непарен број добиваме дека $k\,|\,x$. Но, $(x,y)=1$ и k е заеднички делител на x и y, па затоа $k=1$. Меѓутоа, $k=1$ е ред на m по модул l и затоа $m\equiv 1(\mathrm{mod}\, l)$, односно $m^x\equiv 1(\mathrm{mod}\, l)$. Но, $m^x\equiv -1(\mathrm{mod}\, l)$ па затоа $2\equiv 0(\mathrm{mod}\, l)$, т.е. $l\le 2$. ■

8. ЛЕМА ЗА ЗГОЛЕМУВАЊЕ НА СТЕПЕНОТ

8.1. Теорема. Нека n е природен број, $p>2$ е прост број и $a\neq 1$ е цел број.

1) Ако $p^k \parallel a-1,\ k>0$ и $p^l \parallel n$, тогаш $p^{k+l} \parallel a^n-1$, односно

$$v_p(a^n-1)=v_p(a-1)+v_p(n)$$

2) Ако n е непарен, $p^k \parallel a+1,\ k>0$ и $p^l \parallel n$, тогаш $p^{k+l} \parallel a^n+1$, односно

$$v_p(a^n+1)=v_p(a+1)+v_p(n).$$

Доказ. 1) Имаме $a=p^kB+1$ за некој цел број B кој не е делив со p. Тогаш

$$a^n-1=(1+p^kB)^n-1=np^kB+\binom{n}{2}p^{2k}B^2+\binom{n}{3}p^{3k}B^3+\ldots+p^{nk}B^n. \quad (1)$$

Тврдењето ќе го докажеме со индукција по l. За $l=0$ и $l=1$, очигледно сите собирци, освен првиот, на десната страна на (1) се деливи со p^{k+l+1}, а првиот собирок е делив со p^{k+l}, па затоа $p^{k+l} \parallel a^n-1$.

Нека претпоставиме дека, тврдењето важи за $l=0,1,2,\ldots,t-1$ и нека $l=t$. Тврдењето важи за $l=1$, па затоа $p^{k+1} \parallel a^p-1$. Понатаму, бидејќи $p^{t-1} \parallel N=\frac{n}{p}$, од индуктивната претпоставка применета на $A=a^p$ и N добиваме

$$p^{k+t}=p^{(k+1)+(t-1)} \parallel A^N-1=(a^p)^{\frac{n}{p}}-1=a^n-1.$$

Конечно, од принципот на математичка индукција следува дека тврдењето важи за секој природен број l.

2) Следува од тврдењето под 1) со замена на a со $-a$. ■

8.2. Последица. Ако $\delta=\delta(p,a)$ и $p^k \parallel a^\delta-1$, тогаш $\delta(p^{k+l},a)=p^l\delta$.

Доказ. Непосредно следува од теоремата 8.1, применета на a^δ. ■

8.3. Последица. 1) Нека $a,b\in\mathbb{Z}$ и $n\in\mathbb{N}$. За секој прост број $p>2$ таков што $p\mid a-b,\ p\nmid a,\ p\nmid b$ важи, ако $p^k \parallel a-b$ и $p^l \parallel n$, тогаш $p^{k+l} \parallel a^n-b^n$, односно

$$v_p(a^n-b^n)=v_p(a-b)+v_p(n).$$

2) Нека $a,b\in\mathbb{Z}$ и $n\in\mathbb{N}$ е непарен. За секој прост број $p>2$ таков што $p\mid a+b,\ p\nmid a,\ p\nmid b$ важи, ако $p^k \parallel a+b$ и $p^l \parallel n$, тогаш $p^{k+l} \parallel a^n+b^n$, односно

$$v_p(a^n+b^n)=v_p(a+b)+v_p(n).$$

Доказ. 1) За секој $b\in\mathbb{Z},\ p\nmid b$, постои цел број c таков што

$$bc\equiv 1(\mathrm{mod}\ p^{k+l}).$$

Во теоремата 8.1 го заменуваме a со ac. Условите $p^k \| ac-1$ и $p^{k+l} \| (ac)^n - 1$ се еквивалентни со условите $p^k \| a-b$ и $p^{k+l} \| a^n - b^n$, од што следува тврдењето.

2) Следува од тврдењето а) применето на $(a,-b)$. ■

8.4. Тврдењата искажани во теоремата 8.1 и последицата 8.3 се познати како лема за зголемување на степенот. За $p=2$ теоремата 8.1 и нејзината последица не се точни. На пример, $2\|3-1$ и $2\|2$, но $2^3 \mid 3^2-1$. Затоа случајот $p=2$ ќе го разгледаме посебно. Прво ќе ја докажеме следнава лема која важи за секој прост број p.

Лема. а) Нека $x,y\in\mathbb{Z}$ и $n\in\mathbb{N}$. За секој прост број p таков што $(n,p)=1$, $p\mid x-y$, $p\nmid x$ и $p\nmid y$ важи

$$v_p(x^n-y^n)=v_p(x-y).$$

б) Нека $x,y\in\mathbb{Z}$ и $n\in\mathbb{N}$ е непарен. За секој прост број p таков што $(n,p)=1$, $p\mid x+y$, $p\nmid x$ и $p\nmid y$ важи

$$v_p(x^n+y^n)=v_p(x+y).$$

Доказ. а) Имаме

$$x^n-y^n=(x-y)(x^{n-1}+x^{n-2}y+x^{n-3}y^2+\ldots+y^{n-1}),$$

па затоа доволно е да докажеме дека $p\nmid x^{n-1}+x^{n-2}y+x^{n-3}y^2+\ldots+y^{n-1}$. Навистина, од $x\equiv y(\mathrm{mod}\, p)$ следува

$$x^{n-1}+x^{n-2}y+x^{n-3}y^2+\ldots+y^{n-1}\equiv nx^{n-1}\not\equiv 0(\mathrm{mod}\, p).$$

б) Следува од тврдењето под а) применето на $(x,-y)$. ■

8.5. Теорема. Нека $x,y\in\mathbb{Z}$ се непарни броеви такви што $4\mid x-y$. Тогаш за секој природен број n важи

$$v_2(x^n-y^n)=v_2(x-y)+v_2(n).$$

Доказ. Нека $n=2^k m$, каде m е непарен број. Од лемата 8.4 следува

$$\begin{aligned} v_2(x^n-y^n) &= v_2(x^{2^k m}-y^{2^k m}) \\ &= v_2((x^{2^k})^m-(y^{2^k})^m) \\ &= v_2(x^{2^k}-y^{2^k}). \end{aligned}$$

Според тоа, треба да докажеме дека

$$v_2(x^{2^k}-y^{2^k})=v_2(x-y)+k. \qquad (1)$$

Понатаму, имаме

$$x^{2^k} - y^{2^k} = (x^{2^{k-1}} + y^{2^{k-1}})(x^{2^{k-2}} + y^{2^{k-2}})...(x^2 + y^2)(x+y)(x-y). \quad (2)$$

Сега, од $4 \mid x-y$ следува $x \equiv y \equiv \pm 1 (\mathrm{mod}\, 4)$ следува $x^{2^t} \equiv y^{2^t} \equiv 1 (\mathrm{mod}\, 4)$ за секој $t \in \mathbb{N}$, па затоа $x^{2^t} + y^{2^t} \equiv 2 (\mathrm{mod}\, 4)$, од каде добиваме

$$v_2(x^{2^t} + y^{2^t}) = 1 \text{ за секој } t \in \mathbb{N}. \quad (3)$$

Сега, бидејќи x, y се непарни и меѓусебно конгруентни по модул 4, добиваме $x + y \equiv 2 (\mathrm{mod}\, 4)$, од каде следува

$$v_2(x+y) = 1. \quad (3)$$

Конечно, ако ја примениме функцијата v_2 на (2) и потоа ги искористиме (3) и (4) ја добиваме формуата (1). ■

8.6. Последица. Нека x, y се непарни цели броеви и $n \in \mathbb{N}$ е парен број. Тогаш

$$v_2(x^n - y^n) = v_2(x-y) + v_2(x+y) + v_2(n) - 1.$$

Доказ. Јасно, $4 \mid x^2 - y^2$. Понатаму, за $n = 2^k m$, каде m е непарен број и $k \in \mathbb{N}$, од теоремата 8.5 следува

$$\begin{aligned} v_2(x^n - y^n) &= v_2(x^{2^k m} - y^{2^k m}) \\ &= v_2((x^2)^{2^{k-1} m} - (y^2)^{2^{k-1} m}) \\ &= v_2(x^2 - y^2) + k - 1 \\ &= v_2(x-y) + v_2(x+y) + v_2(n) - 1, \end{aligned}$$

што и требаше да се докаже. ■

8.7. Пример. Докажи дека за секој $n \in \mathbb{N}$ бројот $2^{3^n} + 1$ е делив со 3^{n+1}, но не е делив со 3^{n+2}.

Решение. Имаме $3^1 \,\|\, (-2) - 1$ и $3^n \,\|\, 3^n$. Сега, од теорема 7.7 следува дека $3^{n+1} \,\|\, (-2)^{3^n} - 1 = -(2^{3^n} + 1)$. ■

8.8. Пример. Докажи дека $4^m - 4^n, m > n$ е делив со 3^{k+1} ако и само ако $m-n$ е делив со 3^k.

Решение. Доволно е да докажеме дека $3^{k+1} \mid 4^{m-n} - 1$ ако и само ако $3^k \mid m-n$. Ако $v_3(m-n) = s$ и $v_3(4^{m-n} - 1) = t$, тогаш од теоремата 8.1 следува дека $t = s+1$.

Ако $3^{k+1} \mid 4^{m-n} - 1$, тогаш $k+1 \le t = s+1$, т.е. $k \le s$ и значи $3^k \mid m-n$.

Обратно, ако $3^k \mid m-n$, тогаш $k \le s$, $k+1 \le s+1 = t$ и затоа $3^{k+1} \mid 4^{m-n} - 1$. ■

9. ПРИМИТИВНИ КОРЕНИ

9.1. Во теорема 7.3 докажавме дека $\delta(a,n)\,|\,\varphi(n)$. Логично е да се запрашаме дали за даден природен број n може да се избере a таков што $\delta(a,n)=\varphi(n)$?

Во врска со ова прашање ја имаме следнава дефиниција.

Дефиниција. Нека $n\in\mathbb{N}$ и $(a,n)=1$. Ако $\delta(a,n)=\varphi(n)$, тогаш ќе велиме дека a е *примитивен корен по модул* n.

9.2. Теорема. Ако a е примитивен корен од n, тогаш $\{a,a^2,...,a^{\varphi(n)}\}$ е редуциран систем на остатоци по модул n.

Доказ. Имаме $(a,n)=1$. Оттука следува дека $(a^i,n)=1$, за секој $1\le i\le\varphi(n)$. Понатаму, броевите a^i, $i\in\{1,2,...,\varphi(n)\}$ не се меѓусебно конгруентни по модул n (зошто?). Бидејќи имаме само $\varphi(n)$ природни броеви помали од n кои се заемно прости со n, заклучуваме дека елементите на множеството $\{a,a^2,...,a^{\varphi(n)}\}$ мора да се конгруентни со нив. Според тоа, $\{a,a^2,...,a^{\varphi(n)}\}$ е редуциран систем на остатоци по модул. ■

9.3. Во теоремата 5.8 докажавме дека за полином од $n-$ти степен $f(x)$, конгруентната равенка $f(x)\equiv 0(\mathrm{mod}\,p)$ има најмногу n решенија. Притоа, да споменеме дека во случајов ние всушност работевме во $\mathbb{Z}_p$ - полето остатоци по модул прост број p.

Лема. Нека p е прост број. Ако $n\,|\,p-1$, тогаш конгруентната равенка

$$x^n\equiv 1(\mathrm{mod}\,p)$$

има n решенија.

Доказ. Според теоремата 5.8 равенката $x^n\equiv 1(\mathrm{mod}\,p)$ има најмногу n решенија. Од друга страна, степенот на полиномот $\frac{x^{p-1}-1}{x^n-1}$ е еднаков на $p-1-n$, па затоа равенката $\frac{x^{p-1}-1}{x^n-1}\equiv 1(\mathrm{mod}\,p)$ има најмногу $p-1-n$ решенија. Понатаму, од теоремата на Ферма следува дека равенката $x^{p-1}\equiv 1(\mathrm{mod}\,p)$ има точно $p-1$ решение. Конечно, тврдењето на лемата следува од последицата 5.12. ■

9.4. Теорема. За секој прост број p постои примитивен корен по модул p.

Доказ. Со индукција по делителите d на бројот $p-1$, ќе докажеме дека постојат $\varphi(d)$ елементи на $\mathbb{Z}_p$ со ред d. Тврдењето е тривијално за $d=1$. Нека

претпоставиме дека тврдењето е точно за сите делители на бројот $p-1$ помали од d. Од лемата 9.3 следува дека постојат точно d елементи на $\mathbb{Z}_p$ чиј ред е делител на d. Од индуктивната претпоставка следува дека меѓу тие d елементи точно $\varphi(m)$ имаат ред m, каде m е произволен делител на d помал од d. Преостанатите $d-\sum_{d>m|d}\varphi(m)$ имаат ред d, а од теоремата III 5.2 следува дека

$$d-\sum_{d>m|d}\varphi(m)=\varphi(d),$$

со што е завршен индуктивниот доказ. ■

9.5. Последица. Ако p е прост број, тогаш постојат точно $\varphi(p-1)$ примитивни корени по модул p.

Доказ. Непосредно следува од теоремата 9.4. Деталите ги оставаме на читателот за вежба. ■

9.6. Последица. Нека p е прост број и $n\in\mathbb{N}$. Ако за секој a таков што $(a,p)=1$ важи $p\mid a^n-1$, тогаш $p-1\mid n$.

Доказ. Доволно е да земеме $a=u$ каде u е примитивен корен по модул p. ■

9.7. Според теоремата 9.2 егзистенцијата на примитивен корен u по прост модул p значи дека мултипликативната група $\mathbb{Z}_p^*$ е циклична и е генерирана од елементот u. Понатаму, во теоремата 9.4 докажавме дека за секој прост број p постои примитивен корен по модул p. Логично се поставува прашањето за кои природни броеви n постои примитивен корен по модул n. Одговор на ова прашање ќе дадеме во следните разгледувања.

9.8. Теорема. Нека p е непарен прост број. Тогаш за секој $n\in\mathbb{N}$ постои примитивен корен по модулите p^n и $2p^n$.

Доказ. Според теоремата 9.4 постои примитивен корен u по модул p. Прво ќе докажеме дека барем еден од броевите $u, u+p$ е примитивен корен по модул p^2, т.е. дека има ред $\varphi(p^2)=p(p-1)$ по модул p^2. Секој од овие два броја има ред $p-1$ по модул p, па затоа нивните редови по модул p^2 се деливи со $p-1$, што значи дека тие се еднакви на $p-1$ или $p(p-1)$. Ако ниту u ниту $u+p$ не е примитивен корен по модул p^2, тогаш $u^{p-1}\equiv(u+p)^{p-1}\equiv 1(\mathrm{mod}\,p^2)$. Меѓутоа, од Њутновата биномна формула следува дека

$$0 \equiv (u+p)^{p-1} - u^{p-1} \equiv (p-1)pu^{p-2} \not\equiv 0 (\mathrm{mod}\, p^2),$$

што е противречност.

Сега нека u е примитивен корен по модул p^2. Ќе докажеме дека u е примитивен корен по модул p^n. Бидејќи p точно го дели $u^{p-1}-1$, од теоремата 8.1 следува, дека $p^n \mid u^m - 1$ ако и само ако $p^{n-1}(p-1) \mid m$, т.е. редот на u по модул p^n е еднаков на $\varphi(p^n)$, што значи дека u е примитивен корен по модул p^n.

Конечно, бидејќи $\varphi(2p^n) = \varphi(p^n)$, секој непарен примитивен корен по модул p^n е и примитивен корен по модул $2p^n$. Според тоа, u или $u+p$ е примитивен корен по модул $2p^n$. ■

9.9. Теорема. Примитивен корен по модул $n, n \in \mathbb{N}$ постои ако и само ако $n = p^k$ или $n = 2p^k$, каде p е непарен прост број и $k \in \mathbb{N}$, или $n \in \{2,4\}$.

Доказ. Ако постои природен број a таков што $\delta(a,n) = \varphi(n)$, тогаш од теоремата на Кармајкл следува дека $\lambda(n) = \varphi(n)$. Но, тоа значи дека n не може да биде од облик $2^k, k > 2$. Исто така, од теоремата на Кармајкл следува дека n не може да биде и производ на два заемно прости броеви n_1 и n_2 поголеми од 2, бидејќи $\lambda(n_1)$ и $\lambda(n_2)$ по дефиниција се парни, па затоа

$$\begin{aligned}\lambda(n) = [\lambda(n_1), \lambda(n_2)] &\le \tfrac{1}{2}\lambda(n_1)\lambda(n_2) \\ &\le \tfrac{1}{2}\varphi(n_1)\varphi(n_2) = \tfrac{1}{2}\varphi(n) < \varphi(n),\end{aligned}$$

Секој $n \in \mathbb{N}$ кој е запишан во некој од наведените облици или содржи степен на бројот 2 поголем од 4 или е производ на два заемно прости броеви поголеми од 2, па затоа тврдењето следува од претходните разгледувања. ■

9.10. Теорема. Нека $m, n \in \mathbb{N}$. Ако $n \mid a^m - 1$ за секој цел број a таков што $(a,n) = 1$, тогаш $\lambda(n) \mid m$, каде λ е функцијата на Кармајкл.

Доказ. Нека $n = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, каде p_i се различни непарни прости броеви и $\alpha_i > 0$. Од теоремата 9.9 следува дека за секој i постои u_i чиј ред по модул $p_i^{\alpha_i}$ е еднаков на $\varphi(p_i^{\alpha_i})$. За $\alpha > 3$ примитивен корен по модул 2^α не постои, но редот на бројот 5 по модул 2^α е еднаков на $2^{\alpha-2}$ (Зошто?).

Од Кинеската теорема за остатоци следува дека постои a таков што $a \equiv 5 (\mathrm{mod}\, 2^\alpha)$ и $a \equiv u_i (\mathrm{mod}\, p_i^{\alpha_i})$, за $i = 1,2,\ldots,r$. Тогаш $n \mid a^m - 1$ ако и само ако

$2^{\alpha} \mid a^m - 1$ и $p_i^{\alpha_i} \mid a^m - 1$, за $i = 1,2,...,r$, а тоа важи ако и само ако $\lambda(2^{\alpha}) \mid m$ и $\lambda(p_i^{\alpha_i}) \mid m$, за $i = 1,2,...,r$, што значи ако и само ако $\lambda(n) \mid m$. ■

9.11. Пример. Докажи дека броевите 1, 2, ..., 100 можат да се распоредат во полињата на табела 10×10 така, што во секој 2×2 квадрат производите на броевите на дијагоналите се еднакви по модул 101.

Решение. Нека u е примитивен корен по модул 101. Во полето на $i-$тата редица и $j-$тата колона, $i, j = 1,2,...,10$, да го запишеме остатокот на u^{10i+j} при делење со 101. Во секој квадрат определен со редиците $i, i+1$ и колоните $j, j+1$, производот на броевите на секоја од дијагоналите е еднаков на

$$k \equiv u^{10(2i+1)+(2j+1)} \pmod{101}. \blacksquare$$

9.12. Пример. Нека p е прост број и $S_n = \sum_{x=0}^{p-1} x^n$, $n \in \mathbb{N}$. Докажи дека $S_n \equiv p-1 \pmod{p}$ ако $p-1 \mid n$ и $S_n \equiv 0 \pmod{p}$ ако $p-1 \nmid n$.

Решение. Нека $p-1 \mid n$, т.е. $n = (p-1)q$. Бидејќи $(x, p) = 1$ за $x = 1,2,..., p-1$ од малата теорема на Ферма следува

$$S_n = \sum_{x=0}^{p-1} x^n = \sum_{x=1}^{p-1} (x^{p-1})^q \equiv \sum_{x=1}^{p-1} 1^q = p-1 \pmod{p}.$$

Нека $p-1 \nmid n$. Тогаш $n = (p-1)q + k$ за некој $k \in \{1,2,..., p-2\}$, па затоа

$$S_n = \sum_{x=0}^{p-1} x^n = \sum_{x=1}^{p-1} (x^{p-1})^q x^k \equiv \sum_{x=1}^{p-1} x^k \pmod{p}, \qquad (1)$$

за некој $k \in \{1,2,..., p-2\}$. Според теоремата 9.4 постои примитивен корен u по модул p. Според теоремата 9.2 множеството $\{u, u^2, ..., u^{p-1}\}$ е редуциран систем на остатоци по модул p, па затоа од (1) следува

$$S_n \equiv \sum_{x=1}^{p-1} x^k \pmod{p} \equiv \sum_{i=1}^{p-1} (u^i)^k \equiv \sum_{i=1}^{p-1} (u^k)^i \pmod{p}$$

$$u^k S_n \equiv \sum_{i=1}^{p-1} (u^k)^{i+1} \equiv \sum_{i=2}^{p} (u^k)^i \equiv \sum_{i=1}^{p-1} (u^k)^i \equiv S_n \pmod{p}.$$

Но, за $k \in \{1,2,..., p-2\}$ важи $u^k \not\equiv 1 \pmod{p}$, па затоа од последните конгруенции следува $S_n \equiv 0 \pmod{p}$. ■

9.13. Пример. Нека p е непарен прост број и $f(x) = a_0 + a_1 x + ... + a_{p-1} x^{p-1}$ е полином со целобројни коефициенти таков што е исполнето: за целите броеви a и

b бројот $a-b$ не е делив со p ако и само ако $f(a)-f(b)$ не е делив со p. Докажи дека $p \mid a_{p-1}$.

Решение. Од условот следува дека $f(0), f(1),..., f(p-1)$ формираат комплетен систем на остатоци по модул p. Сега од пример 9.12 добиваме

$$0 \equiv \sum_{i=0}^{p-1} f(i) = pa_0 + \sum_{k=0}^{p-1} a_k \sum_{i=0}^{p-1} i^k \equiv (p-1)a_{p-1} (\mathrm{mod}\, p),$$

од каде следува тврдењето на задачата. ■

V ГЛАВА
ЦИКЛОМАТИЧНИ ПОЛИНОМИ

1. КОМПЛЕКСНИ ПРИМИТИВНИ КОРЕНИ

1.1. Дефиниција. Нека се дадени комплексен број $z \neq 0$ и природен број n. $n-ти\ корен$ од z го нарекуваме комплексниот број w за кој важи

$$w^n = z. \tag{1}$$

Притоа ја користиме ознаката $w = \sqrt[n]{z}$. Понатаму, ако $z = |z|(\cos\varphi + i\sin\varphi)$, тогаш

$$w = \sqrt[n]{z} = \sqrt[n]{|z|}(\cos\frac{\varphi+2k\pi}{n} + i\sin\frac{\varphi+2k\pi}{n}),\ k = 0, \pm1, \pm2, ... \tag{2}$$

Ако во формулата (2) ставиме $k = 0,1,2,...,n-1$ за w добиваме n различни вредности $w_0, w_1, ..., w_{n-1}$. Ставајќи $k = n$, заради периодичноста на тригонометриските функции повторно го добиваме бројот w_0 итн. Според тоа, $n-$тиот корен од комплексниот број z, има точно n различни вредности, кои се добиваат од формулата (2) за $k = 0,1,2,...,n-1$.

Ако $z = 1$, тогаш $\varphi = 0$ и според (2) $n-$те различни корени на бројот 1 се зададени со

$$u_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n},\ k = 0,1,2,...,n-1. \tag{3}$$

Ако ставиме $u = u_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, тогаш од Моавровата формула добиваме

$$u_k = u^k,\ k = 0,1,...,n-1.$$

1.2. Лема. Нека $S_p = \sum_{k=0}^{n-1} u_k^p$ е збирот на $p-$тите степени на $n-$тите корени на единицата, $n \in \mathbb{N}$. Тогаш

$$S_p = \begin{cases} n, & \text{ако } n \mid p \\ 0, & \text{ако } n \nmid p. \end{cases}$$

Доказ. Од $u_k = u^k$, $k = 0,1,...,n-1$ и $u = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, добиваме

$$S_p = 1 + u^p + u^{2p} + ... + u^{(n-1)p}. \tag{4}$$

Ако $n \mid p$ и $\frac{p}{n} = m$, тогаш $u^p = u^{mn} = (u^n)^m = 1^m = 1$ и од (4) следува $S_p = n$. Нека $n \nmid p$. Притоа важи $u^{np} = (u^n)^p = 1^p = 1$. Од $n \nmid p$ следува $u^p - 1 \neq 0$, па затоа

$$S_p = 1+u^p+u^{2p}+\ldots+u^{(n-1)p} = \frac{u^{np}-1}{u^p-1} = 0. \blacksquare$$

1.3. Дефиниција. Нека u е $n-$ти корен на единицата, $n \in \mathbb{N}$. Најмалиот природен број k таков што важи $u^k = 1$ го нарекуваме *ред на бројот* u и го означуваме со $\mathrm{ord}(u)$.

1.4. Лема. Нека $n \in \mathbb{N}$ и u е $n-$ти корен на единицата. Тогаш $u^k = 1$ за некој $k \in \mathbb{N}$ ако и само ако $\mathrm{ord}(u) \mid k$. Специјално, $\mathrm{ord}(u) \mid n$.

Доказ. Нека $d = \mathrm{ord}(k)$. Ако $d \mid k$, тогаш $u^k = (u^d)^{\frac{k}{d}} = 1^{\frac{k}{d}} = 1$.

Обратно, ако $u^k = 1$ и $k = qd + r$, $0 \le r < d$, тогаш од

$$1 = u^{qd+r} = (u^d)^q u^r = u^r$$

следува дека $u^r = 1$. Но, $r < d = \mathrm{ord}(u)$, па затоа $r = 0$, т.е. $d \mid k$. $\blacksquare$

1.5. Последица. Нека $n \in \mathbb{N}$, u е $n-$ти корен на единицата и $d = \mathrm{ord}(u)$. Тогаш $u^k = u^m$ ако и само ако $k \equiv m (\mathrm{mod}\, d)$.

Доказ. Следува од лемата 1.4. Деталите ги оставаме на читателот за вежба. $\blacksquare$

1.6. Дефиниција. Нека u е $n-$ти корен на единицата. Ако $\mathrm{ord}(u) = n$, тогаш ќе велиме дека u е *примитивен* $n-$*ти корен* на единицата.

1.7. Лема. Ако u е примитивен $n-$ти корен на единицата, тогаш $u, u^2, \ldots, u^n$ се сите $n-$ти корени на единицата.

Доказ. Имаме $\mathrm{ord}(u) = n$, па затоа $(u^k)^n = (u^n)^k = 1$, за $k = 1, 2, \ldots, n$, што според дефиницијата 1.1 значи дека комплексните броеви u^k, $k = 1, 2, \ldots, n$ се $n-$ти корени на единицата. Ако $u^k = u^m$, $k, m \in \{1, 2, \ldots, n\}$, тогаш од последицата 1.5 следува $k \equiv m (\mathrm{mod}\, n)$, па затоа $k = m$. Според тоа, броевите $u, u^2, \ldots, u^n$ се различни меѓу себе, па затоа тоа се сите $n-$ти корени на единицата. $\blacksquare$

1.8. Лема. Нека $n, k \in \mathbb{N}$ и u е примитивен $n-$ти корен на единицата. Тогаш u^k е примитивен $n-$ти корен на единицата ако и само ако $(n, k) = 1$.

Доказ. Нека u е примитивен $n-$ти корен на единицата и $d = \mathrm{ord}(u^k)$. Тогаш $u^{kd} = 1$ и бидејќи $\mathrm{ord}(u) = n$ од лемата 1.4 следува дека $n \mid kd$. Ако $(n, k) = 1$, тогаш од $n \mid kd$ следува $n \mid d$. Од друга страна бидејќи u^k е $n-$ти корен на едини-

цата, повторно од лемата 1.4 следува дека $d \mid n$. Сега, од $n \mid d$ и $d \mid n$, следува $d = n$, т.е. u^k е примитивен $n-$ти корен на единицата.

Ако $(n,k) \neq 1$, тогаш од $1 = (u^n)^{\frac{k}{(n,k)}} = (u^k)^{\frac{n}{(n,k)}}$, па од лемата 1.4 следува дека $d \mid \frac{n}{(n,k)}$. Според тоа, $d < n$, па затоа u^k не е примитивен $n-$ти корен на единицата. ■

1.9. Последица. Нека $n \in \mathbb{N}$. Тогаш постојат $\varphi(n)$ примитивни $n-$ти корени на единицата.

Доказ. Непосредно следува од лемата 1.8. ■

1.10. Теорема. Збирот на сите примитивни $n-$ти корени на единицата е еднаков на $\mu(n)$.

Доказ. Нека

$$f(n) = \sum_{\substack{1 \le k \le n \\ (k,n)=1}} e^{\frac{2\pi i k}{n}},$$

каде $u = e^{\frac{2\pi i}{n}}$ е примитивен $n-$ти корен на единицата. Ќе докажеме дека функцијата f е мултипликативна. Прво ќе докажеме дека сите $\varphi(m)\varphi(n)$ собирци од $f(m)f(n)$ се по парови различни. Нека го претпоставиме спротивното, т.е. нека

$$e^{\frac{2\pi i a}{n}} e^{\frac{2\pi i b}{m}} = e^{\frac{2\pi i c}{n}} e^{\frac{2\pi i d}{m}}.$$

Од последицата 1.5 следува

$$am + nb \equiv cm + nd \pmod{mn},$$

односно

$$m(a-c) + n(b-d) \equiv 0 \pmod{mn}.$$

Но, $(m,n) = 1$, па од последната конгруенција следува дека $n \mid a-c$ и $m \mid b-d$, и како $1 \le a,c \le n$ и $1 \le b,d \le m$, заклучуваме дека $a = c$ и $b = d$, што значи дека сите $\varphi(m)\varphi(n)$ собирци од $f(m)f(n)$ се по парови различни. Понатаму, од $(a,n) = (b,m) = 1$ следува $(am+bn, mn) = 1$, па затоа секој од горните собирци се појавува и во $f(mn)$, кој има $\varphi(mn) = \varphi(n)\varphi(m)$ собирци. Последното значи дека функцијата f е мултипликативна.

Сега, бидејќи

$$\begin{aligned} f(p) &= u + u^2 + \ldots + u^{p-1} \\ &= \frac{u(u^{p-1}-1)}{u-1} = \frac{u(u^{p-1}-u^p)}{u-1} \\ &= \frac{u^p(1-u)}{u-1} = -1, \end{aligned}$$

а за $k>1$ важи

$$f(p^k)=u+u^2+\ldots+u^{p^k}-(u^p+u^{2p}+\ldots+u^{p^{k-1}p})$$
$$=\frac{u(u^{p^k}-1)}{u-1}-\frac{u^p((u^p)^{p^{k-1}}-1)}{u^p-1}$$
$$=\frac{u(u^{p^k}-1)}{u-1}-\frac{u^p(u^{p^k}-1)}{u^p-1}=0,$$

од мултипликативноста на f следува $f(n)=\mu(n)$. ■

2. ДЕФИНИЦИЈА И СВОЈСТВА НА ЦИКЛОМАТИЧНИТЕ ПОЛИНОМИ

2.1. Дефиниција. Нека $n\in\mathbb{N}$. Полиномот

$$\Phi_n(x)=\prod_{\mathrm{ord}(\theta)=n}(x-\theta)$$

го нарекуваме $n-$*ти цикломатичен полином*.

2.2. Забелешка. Од дефиниција 2.1 следува дека:

- водечкиот коефициент на $n-$тиот цикломатичен полином е еднаков на 1,
- $n-$тиот цикломатичен полином има само еднократни нули и тоа се примитивните $n-$ти корени на единицата, и
- бидејќи бројот на примитивни $n-$ти корени на единицата е еднаков на $\varphi(n)$, важи $\deg\Phi_n=\varphi(n)$.

2.3. Теорема. Ако $n\in\mathbb{N}$, тогаш

$$x^n-1=\prod_{k|n}\Phi_k(x). \qquad (1)$$

Доказ. Нули на полиномот x^n-1 се $n-$тите корени на единицата. Нека θ е еден од тие корени и нека $\mathrm{ord}(\theta)=k$. Тогаш θ е примитивен $k-$ти корен, па затоа е нула на полиномот $\Phi_k(x)$. Но, според лемата 1.4 важи $k\mid n$, па затоа θ е нула на полиномот $\prod_{k|n}\Phi_k(x)$.

Обратно, ако θ е нула на полиномот $\prod_{k|n}\Phi_k(x)$, тогаш постои $k_0, k_0\mid n$ и θ е нула на полиномот $\Phi_{k_0}(x)$. Сега, од дефиниција 1.1 следува $\theta^{k_0}=1$ и бидејќи $k_0\mid n$ добиваме $\theta^n=1$, односно θ е нула на полиномот x^n-1.

Значи, двата полиноми во (1) имаат исти нули и водечки коефициенти еднакви на 1, па затоа тие се идентични. ■

2.4. Забелешка. Од теоремата 2.3 непосредно следува, дека

$$n = \deg(x^n - 1) = \deg(\prod_{k|n} \Phi_k(x)) = \sum_{k|n} \deg \Phi_k(x) = \sum_{k|n} \varphi(k),$$

и ова е уште еден доказ на теоремата III 5.2.

2.5. Пред да преминеме на разгледување на други својства на цикломатичните полиноми ќе докажеме едно помошно тврдење за моничните полиноми, т.е. полиномите со водечки коефициент 1. .

Теорема. Нека f и g се два монични полиноми со рационални коефициенти. Ако сите коефициенти на полиномот fg се цели броеви, тогаш и сите коефициенти на полиномите f и g се цели броеви.

Доказ. Нека

$$f(x) = x^m + a_{m-1}x^{m-1} + ... + a_0 \text{ и } g(x) = x^n + b_{n-1}x^{n-1} + ... + b_0$$

се разгледуваните полиноми. Нека M и N се соодветно најмалите заеднички содржатели на именителите на броевите $a_{m-1},...,a_0$ и $b_{n-1},...,b_0$ запишани со заемно прости броители и именители. Тогаш M и N се најмалите природни броеви за кои $Mf(x)$ и $Ng(x)$ се полиноми со целобројни коефициенти. Ставаме $A_i = Ma_i$, за $0 \le i \le m-1$ и $B_j = Nb_j$, за $0 \le j \le n-1$, и нека $A_m = M, B_n = N$. Тогаш

$$MNf(x)g(x) = A_m B_n x^{m+n} + ... + A_0 B_0.$$

Сега, бидејќи $f(x)g(x) \in \mathbb{Z}[x]$, добиваме дека сите коефициенти на полиномот $MNf(x)g(x)$ се деливи со MN.

Нека претпоставиме дека $MN > 1$. Нека p е прост број таков што $p \mid MN$. Ќе докажеме дека постои $i \in \{0,1,2,...,m\}$ таков што $p \nmid A_i$. Навистина, ако $p \nmid M$, тогаш $p \nmid A_m$. Ако $p \mid M$ и $p \mid A_i$ за секој $i \in \{0,1,...,m-1\}$, тогаш $(\frac{M}{p})a_i = \frac{A_i}{p} \in \mathbb{Z}$ за секој $i \in \{0,1,...,m-1\}$ и $\frac{M}{p} < M$, што противречи на минималноста на M. Аналогно се докажува дека постои $j \in \{0,1,2,...,n\}$ таков што $p \nmid B_j$. Нека I, J се најголемите индекси i, j за кои $p \nmid A_i$, $p \nmid B_j$. Тогаш коефициентот во полиномот $MNf(x)g(x)$ пред членот x^{I+J} е број од видот $A_I B_J + S$ и притоа важи $p \mid S$. Навистина, од

$$S = \sum_{\substack{k+l=I+J \\ k \neq I, l \neq J}} A_k B_l$$

следува дека за секој собирок во овој збир важи или $k > I$ или $l > J$, па затоа ќе важи $p \mid A_k$ или $p \mid B_l$, т.е. секој собирок во овој збир ќе биде делив со p, па затоа $p \mid S$. Последното значи дека коефициентот пред членот x^{I+J} не е делив со MN што е противречност. Од добиента противречност следува $MN = 1$, па затоа $M = 1, N = 1$, со што тврдењето е докажано. ■

2.6. Теорема. Ако $n \in \mathbb{N}$, тогаш $\Phi_n(x)$ е полином со целобројни коефициенти, односно $\Phi_n(x) \in \mathbb{Z}[x]$, при што слободниот член е $\Phi_n(0) = \pm 1$.

Доказ. Тврдењето ќе го докажеме со индукција. За $n = 1$ имаме $\Phi_1(x) = x - 1$. Нека претпоставиме дека тврдењето е точно за сите броеви помали од n. Тогаш $\Phi_n(x) = \frac{x^n - 1}{\prod\limits_{\substack{k \mid n \\ k \neq n}} \Phi_k(x)}$. Полиномите $x^n - 1$ и $\prod\limits_{\substack{k \mid n \\ k \neq n}} \Phi_k(x)$ се со целобројни коефициенти, па затоа полиномот $\Phi_n(x)$ е со рационални коефициенти. Сега, од теорема 2.5 следува дека полиномот $\Phi_n(x)$ е со целобројни коефициенти. Во случајот слободниот член на $\Phi_n(x)$ е цел број. Од Виетовите формули следува дека тој број е производ на сите корени на $\Phi_n(x)$. Бидејќи корените се ненулти и имаат модул 1 (како комплексни броеви), нивниот производ е ± 1. ■

2.7. Теорема. За секој $n \in \mathbb{N}$ важи

$$\Phi_n(x) = \prod_{d \mid n} (x^{\frac{n}{d}} - 1)^{\mu(d)} .$$

Доказ. Непосредно следува од теоремите 2.3 и III 4.6. Деталите ги оставаме на читателот за вежба. ■

2.8. Теорема. Нека $n \in \mathbb{N}$ и p е прост број. Тогаш

$$\Phi_{np}(x) = \begin{cases} \Phi_n(x^p), & \text{ако } p \mid n, \\ \frac{\Phi_n(x^p)}{\Phi_n(x)}, & \text{ако } p \nmid n. \end{cases}$$

Доказ. Нека $p \mid n$. Од теоремата 2.7 следува

$$\begin{aligned} \Phi_{np}(x) &= \prod_{d \mid np} (x^{\frac{np}{d}} - 1)^{\mu(d)} \\ &= (\prod_{d \mid n} (x^{\frac{np}{d}} - 1)^{\mu(d)})(\prod_{\substack{d \mid np \\ d \nmid n}} (x^{\frac{np}{d}} - 1)^{\mu(d)}) \qquad (2) \\ &= \Phi_n(x^p)(\prod_{\substack{d \mid np \\ d \nmid n}} (x^{\frac{np}{d}} - 1)^{\mu(d)}). \end{aligned}$$

За множителите во последната заграда на горниот израз важи $d \mid pn$ и $d \nmid n$, па бидејќи p е прост број добиваме $p \mid d$. Понатаму, од $p \mid n$ следува $p^2 \mid d$. Навистина, ако $d = pa$ и $p \nmid a$, тогаш од $d \mid pn$ ќе следува $a \mid n$. Но, $(a, p) = 1$, па затоа од $p \mid n$ и $a \mid n$ добиваме $d = ap \mid n$, што е противречност. Според тоа, $p^2 \mid d$ и од дефиницијата III 4.1 следува $\mu(d) = 0$, што значи дека

$$\prod_{\substack{d \mid np \\ d \nmid n}} (x^{\frac{np}{d}} - 1)^{\mu(d)} = 1,$$

па од (2) добиваме дека $\Phi_{np}(x) = \Phi_n(x^p)$.

Доказот во случајот кога $p \nmid n$ е аналоген, со тоа што од теоремата 2.7, мултипликативноста на функцијата $\mu(n)$ и дефиницијата III 4.1 добиваме

$$\Phi_{np}(x) = \prod_{d \mid np} (x^{\frac{np}{d}} - 1)^{\mu(d)} = (\prod_{d \mid n} (x^{\frac{np}{d}} - 1)^{\mu(d)})(\prod_{d \mid n} (x^{\frac{np}{dp}} - 1)^{\mu(pd)})$$

$$= \Phi_n(x^p)(\prod_{d \mid n} (x^{\frac{n}{d}} - 1)^{-\mu(d)}) = \frac{\Phi_n(x^p)}{\Phi_n(x)}. \blacksquare$$

2.9. Последица. Нека $n, k \in \mathbb{N}$ и p е прост број. Тогаш

$$\Phi_{np^k}(x) = \begin{cases} \Phi_n(x^{p^k}), & \text{ако } p \mid n, \\ \dfrac{\Phi_n(x^{p^k})}{\Phi_n(x^{p^{k-1}})}, & \text{ако } p \nmid n. \end{cases}$$

Доказ. Од теорема 2.8 следува

$$\Phi_{np^k}(x) = \Phi_{np^{k-1}}(x^p) = \ldots = \Phi_{np}(x^{p^{k-1}}) = \begin{cases} \Phi_n(x^{p^k}), & \text{ако } p \mid n, \\ \dfrac{\Phi_n(x^{p^k})}{\Phi_n(x^{p^{k-1}})}, & \text{ако } p \nmid n. \end{cases} \blacksquare$$

2.10. Теорема. Ако $a, n \in \mathbb{N}$ и $(a, n) = 1$, тогаш

$$\Phi_n(x^a) = \prod_{d \mid a} \Phi_{nd}(x). \tag{3}$$

Доказ. Според забелешката 2.2 и својствата на полиномите имаме

$$\deg \Phi_n(x^a) = a\varphi(n) \text{ и } \deg \prod_{d \mid a} \Phi_{nd}(x) = \sum_{d \mid a} \varphi(nd) = \varphi(n) \sum_{d \mid a} \varphi(d) = a\varphi(n).$$

Според тоа, полиномите во (3) имаат еднакви степени и бидејќи тие се монични, па за да го докажеме тврдењето доволно е да докажеме дека секој $a-$ти корен на примитивен $n-$ти корен на единицата е корен на полиномот $\prod_{d \mid a} \Phi_{nd}(x)$.

Нека θ е примитивен $n-$ти корен на единицата. Тогаш

$$\Phi_n(x^a)=\prod_{(k,n)=1}(x^a-\theta^k). \tag{4}$$

Значи, секоја нула на полиномот $\Phi_n(x^a)$ е од облик ω^k, каде ω е примитивен $an-$ти корен на единицата и $(k,n)=1$. Нека сега $b=(k,a)$. Тогаш ω^k е примитивен $\frac{an}{b}-$ти корен на единицата. Ако $d=\frac{a}{b}$, тогаш ω^k е корен на полиномот $\Phi_{nd}(x)$. Според тоа, нулите на полиномот $\Phi_n(x^a)$ се еднакви на нулите на полиномот $\prod_{d|a}\Phi_{nd}(x)$. ■

2.11. Теорема. Ако p е прост број, тогаш полиномот $\Phi_p(x)$ е иредуцибилен.

Доказ. За да докажеме дека $\Phi_p(x)$ е иредуцибилен, доволно е да докажеме дека $\Phi_p(x+1)$ е иредуцибилен. Од теоремата 2.8 следува

$$\begin{aligned}\Phi_p(x+1)=\Phi_{p\cdot1}(x+1)&=\frac{\Phi_1((x+1)^p)}{\Phi_1(x+1)}=\frac{(x+1)^p-1}{(x+1)-1}\\&=\frac{x^p+\binom{p}{1}x^{p-1}+\ldots+\binom{p}{p-2}x^2+\binom{p}{p-1}x}{x}\\&=x^{p-1}+\binom{p}{1}x^{p-2}+\ldots+\binom{p}{p-2}x+\binom{p}{p-1},\end{aligned}$$

па од Ајзенштајновиот критериум (види [167], стр. 207) следува дека $\Phi_p(x+1)$ е иредуцибилен. ■

2.12. Пример. Докажи дека низата

$$10001,\ 100010001,\ 1000100010001,\ldots$$

не содржи прости броеви.

Решение. Имаме $10001=73\cdot137$, а вториот член на низата е делив со 3, па затоа првите два члена на низата не се прости броеви. Понатаму, секој член на оваа низа е од видот $1+10^4+10^8+\ldots+10^{4n}$, па затоа треба да докажеме дека за секој природен број n овој број е сложен.

Ако $n+1$ е сложен број, тогаш од $m+1\,|\,n+1$ следува $10^{4(m+1)}-1\,|\,10^{4(n+1)}-1$, т.е. $1+10^4+10^8+\ldots+10^{4m}\,|\,1+10^4+10^8+\ldots+10^{4n}$, што значи дека во овој случај $n-$тиот член на низата е сложен број.

Ако $n+1$ е прост број, тогаш од теорематафсзаз 2.3 следува

$$\begin{aligned}1+10^4+10^8+\ldots+10^{4n}&=\frac{10^{4(n+1)}-1}{10^4-1}=\frac{(10^4)^{n+1}-1}{10^4-1}\\&=\frac{\Phi_1(10^4)\Phi_{n+1}(10^4)}{\Phi_1(10^4)}=\Phi_{n+1}(10^4),\end{aligned}$$

Сега, од теорема 2.10 следува

$$\Phi_{n+1}(10^4) = \Phi_{n+1}(10)\Phi_{2(n+1)}(10)\Phi_{4(n+1)}(10),$$

од каде што во овој случај следува тврдењето на задачата. ■

3. ЦИКЛОМАТИЧНИ ПОЛИНОМИ И РЕД НА БРОЈ ПО ПРОСТ МОДУЛ

3.1. Теорема. Нека p е прост број. Ако постојат цел број a и полином $f \in \mathbb{Z}[x]$ такви што

$$x^n - 1 \equiv (x-a)^2 f(x) (\mathrm{mod}\, p), \tag{1}$$

тогаш $p \mid n$.

Доказ. Ако во (1) ставиме $x = a$ добиваме $a^n - 1 \equiv 0 (\mathrm{mod}\, p)$, што значи дека $p \nmid a$. Во (1) ставаме $x = y + a$ и добиваме

$$(y+a)^n - 1 \equiv y^2 f(y+a) (\mathrm{mod}\, p). \tag{2}$$

Сега, ако во полиномите на (2) ги споредиме коефициентите пред y, добиваме дека $na^{n-1} \equiv 0 (\mathrm{mod}\, p)$. Но, $p \nmid a$, па затоа од последната конгруенција следува дека $p \mid n$. ■

3.2. Лема. Нека $n \in \mathbb{N}, x \in \mathbb{Z}$ и $d < n$ е делител на n. Ако p е заеднички прост делител на $\Phi_n(x)$ и $\Phi_d(x)$, тогаш $p \mid n$.

Доказ. Според теоремата 2.3 имаме $x^n - 1 = \prod_{k \mid n} \Phi_k(x)$, што значи дека $x^n - 1$ е делив со $\Phi_n(x)\Phi_d(x)$. Според тоа, полиномот $x^n - 1$ има двократна нула по модул p, па од теоремата 3.1 следува дека $p \mid n$. ■

3.3. Лема. Нека $m, n \in \mathbb{N}$ и p е прост број таков, што $p \nmid mn$. Тогаш броевите $\Phi_m(x)$ и $\Phi_n(x)$ не може и двата да бидат деливи со p за иста вредност на $x \in \mathbb{Z}$.

Доказ. Ако за некој $x \in \mathbb{Z}$ важи $p \mid \Phi_m(x)$ и $p \mid \Phi_n(x)$, тогаш полиномот $x^{mn} - 1$ има двократна нула по модул p, па од теоремата 3.1 следува дека $p \mid mn$, што е противречност. ■

3.4. Теорема. Нека $f(x)$ е полином со целобројни коефициенти. Постои неконстантен полином $m(x)$ таков што $(m(x))^2 \mid f(x)$ ако и само ако полиномот

$(f(x), f'(x))$ не е константен. Тврдењето важи и кога $f(x)$ е полином над полето $\mathbb{Z}_p$.

Доказ. Нека $m(x)$ е неконстантен полином таков што $(m(x))^2 \mid f(x)$. Од правилата за диференцирање следува дека $m(x) \mid f'(x)$, па затоа $m(x)$ е заеднички делител на $f(x)$ и $f'(x)$, т.е. полиномот $(f(x), f'(x))$ не е константен.

Нека полиномот $(f(x), f'(x))$ не е константен. Нека $m(x) \mid (f(x), f'(x))$ е иредуцибилен и не е константен. Ставаме $f(x) = m(x)r(x)$ и добиваме

$$f'(x) = m'(x)r(x) + m(x)r'(x).$$

Но, $m(x)$ е деител на $f'(x)$, па затоа $m(x) \mid m'(x)r(x)$. Понатаму, полиномот $m(x)$ е иредуцибилен, па затоа $(m(x), m'(x))$ е константен полином и како $m(x) \mid m'(x)r(x)$ заклучуваме дека $m(x) \mid r(x)$. Според тоа, постои полином $q(x)$ таков што $r(x) = m(x)q(x)$. Конечно, постои неконстантен полином $m(x)$ таков што $f(x) = (m(x))^2 q(x)$, т.е. $(m(x))^2 \mid f(x)$.

Случајот со полиноми над полето $\mathbb{Z}_p$ е малку поспецифичен. Ако $m'(x) \neq 0$, тогаш разгледувањата се како погоре. Ако $m'(x) = 0$, тогаш од малата теорема на Ферма добиваме

$$m(x) = \sum_{k \geq 0} a_k x^k = (\sum_{k \geq 0} a_k x^k)^p \pmod{p},$$

што противречи на иредуцибилноста на $m(x)$. ■

3.5. Теорема. Нека m и n се различни природни броеви и p е прост број таков, што $p \nmid mn$. Тогаш

$$(\Phi_m(x), \Phi_n(x)) = 1$$

над $\mathbb{Z}_p[x]$.

Доказ. Нека претпоставиме дека $(\Phi_m(x), \Phi_n(x)) \neq 1$. Ако земеме предвид дека $\Phi_m(x)\Phi_n(x) \mid x^{mn} - 1$ следува дека постои полином $g(x)$ над $\mathbb{Z}_p[x]$ таков што $g^2(x) \mid x^{mn} - 1$. Но, тогаш од теоремата 3.4 следува дека $(mnx^{mn-1}, x^{mn} - 1) \neq 1$, што е противречност. ■

3.6. Теорема. Нека p е прост број. Тогаш за секои $n \in \mathbb{N}$ и $a \in \mathbb{Z}$ такви што $(n, p) = 1$ важи $p \mid \Phi_n(a)$ ако и само ако $\delta(a, p) = n$.

Доказ. Тврдењето ќе го докажеме со математичка индукција по n.

Од $\Phi_1(x) = x - 1$ следува дека тврдењето важи за $n = 1$. Нека претпоставиме дека тврдењето важи за сите природни броеви $k < n$.

Нека претпоставиме дека за некој $a \in \mathbb{Z}$ важи $p \mid \Phi_n(a)$. Тогаш, од теорема 2.3 следува дека $a^n \equiv 1 (\mathrm{mod}\, p)$. Нека претпоставиме дека $\delta(a, p) = k < n$. Тогаш од индуктивната претпоставка следува $p \mid \Phi_k(a)$. Значи, $p \mid \Phi_n(a)$ и $p \mid \Phi_k(a)$, па бидејќи $k \mid n$ од лемата 3.2 следува $p \mid n$, што противречи на $(n, p) = 1$.

Нека $\delta(a, p) = n$. Тогаш од теоремата 2.3 следува

$$0 \equiv a^n - 1 \equiv \prod_{k \mid n} \Phi_k(a) (\mathrm{mod}\, p),$$

па затоа $p \mid \Phi_k(a)$, за некој $k \mid n$. Меѓутоа, не може да биде $k < n$, бидејќи тогаш повторно од теоремата 2.3 ќе следува $p \mid a^k - 1$, што противречи на $\delta(a, p) = n$. Според тоа, $k = n$, т.е. $p \mid \Phi_n(a)$.

Значи, тврдењето важи и за $k = n$, па од принципот на математичка индукција следува дека важи за секој природен број n. ■

3.7. Теорема. Нека $n \in \mathbb{N}$ и $x \in \mathbb{Z}$. Тогаш за секој прост делител p на $\Phi_n(x)$ важи или $p \equiv 1 (\mathrm{mod}\, n)$ или $p \mid n$.

Доказ. Нека p е прост делител на $\Phi_n(x)$. Тогаш $p \nmid x$ бидејќи $p \mid \Phi_n(x) \mid x^n - 1$. Нека $k = \delta(x, p)$. Бидејќи $p \mid x^n - 1$, добиваме $x^n \equiv 1 (\mathrm{mod}\, p)$, па од теоремата IV 7.3 следува дека $k \mid n$.

Ако $k = n$, тогаш од малата теорема на Ферма следува $x^{p-1} \equiv 1 (\mathrm{mod}\, p)$, па затоа од теоремата IV 7.3 добиваме $n \mid p - 1$, т.е. $p \equiv 1 (\mathrm{mod}\, n)$.

Ако $k < n$, тогаш од теоремата 2.3 и дефиницијата на ред по модул следува

$$0 \equiv x^k - 1 = \prod_{d \mid k} \Phi_d(x) \, (\mathrm{mod}\, p),$$

па затоа за некој $d \mid k$ важи $p \mid \Phi_d(x)$. Конечно, бидејќи $p \mid \Phi_d(x)$ и $p \mid \Phi_n(x)$, од лемата 3.2 следува $p \mid n$. ■

3.8. Во втората глава без доказ ја дадовме теоремата на Дирихле. Во следната последица ќе докажеме специјален случај на оваа теорема.

Последица (теорема на Дирихле). Нека $n \in \mathbb{N}$. Тогаш постојат бесконечно многу прости броеви p такви што $p \equiv 1 (\mathrm{mod}\, n)$.

Доказ. За $n = 1$ тврдењето е тривијално, па затоа нека $n > 1$.

Нека претпоставиме дека постојат конечно многу прости броеви p такви што $p \equiv 1 (\mathrm{mod}\, n)$. Нека M е производ на овие прости броеви и простите броеви кои се делители на n. Јасно, $M > 1$. Бидејќи $\Phi_n(x)$ е неконстантен моничен полином,

постои $k \in \mathbb{N}$ таков што $\Phi_n(M^k) > 1$. Нека q е прост делител на бројот $\Phi_n(M^k)$. Тогаш $q \mid \Phi_n(M^k) \mid M^{kn} - 1$, па затоа $q \nmid M$. Но, тогаш од начинот на кој е определен M следува $q \nmid n$ и $q \not\equiv 1 (\mathrm{mod}\, n)$, што противречи на теоремата 3.7.

Конечно, од добиената противречност следува дека постојат бесконечно многу прости броеви p такви што $p \equiv 1 (\mathrm{mod}\, n)$. ■

3.9. Во продолжение ќе дадеме друг доказ на последицата IV 7.4.

Последица. Нека $a \in \mathbb{Z}$ и $p > 2$ е прост број. Тогаш за секој прост делител q на $1 + a + ... + a^{p-1}$ важи $q \equiv 1 (\mathrm{mod}\, p)$ или $q = p$.

Доказ. Нека q е прост делител на $1 + a + ... + a^{p-1}$. Бидејќи

$$1 + a + ... + a^{p-1} = \frac{a^p - 1}{a - 1} = \frac{a^p - 1}{\Phi_1(a)} \quad \text{и} \quad a^p - 1 = \Phi_1(a)\Phi_p(a)$$

добиваме дека

$$\Phi_p(a) = 1 + a + ... + a^{p-1}.$$

Сега од теоремата 3.7 следува $q \equiv 1 (\mathrm{mod}\, p)$ или $q \mid p$, т.е. $q = p$. ■

3.10. Пример. Нека $a, b \in \mathbb{N}$ и $x > 1$ е природен број. Докажи дека

$$(x^a - 1, x^b - 1) = x^{(a,b)} - 1.$$

Решение. Нека $M = (x^a - 1, x^b - 1)$ и $m = (a, b)$. Од $x^m - 1 \mid x^a - 1$ и $x^m - 1 \mid x^b - 1$ следува $x^m - 1 \mid M$.

Јасно, $(x, M) = 1$. Нека $\delta(x, M) = d$. Тогаш $M \mid x^d - 1$ и од $x^a \equiv x^b \equiv 1 (\mathrm{mod}\, M)$, добиваме $d \mid a$ и $d \mid b$, па затоа $d \mid m$. Така, $x^d - 1 \mid x^m - 1$, па затоа $M \mid x^m - 1$.

Според тоа, $x^m - 1 \mid M$ и $M \mid x^m - 1$, од каде $M = x^m - 1$. ■

3.11. Теорема. Нека $a, b \in \mathbb{N}$. Нека $(\Phi_a(x), \Phi_b(x)) > 1$ за некој $x \in \mathbb{Z}$. Тогаш $\frac{a}{b}$ е степен на прост број, т.е. $\frac{a}{b} = p^k$, каде p е прост број и $k \in \mathbb{Z}$.

Доказ. Нека p е заеднички прост делител на $\Phi_a(x)$ и $\Phi_b(x)$. Ќе докажеме дека $\frac{a}{b}$ е степен на бројот p, т.е. ако $a = p^\alpha A$ и $b = p^\beta B$, каде $\alpha, \beta \geq 0$ и A и B се природни броеви кои не се деливи со p, тогаш $A = B$.

Од $p \mid \Phi_a(x) \mid x^a - 1$ следува дека $(x, p) = 1$. Ќе докажеме дека $p \mid \Phi_A(x)$.

Од $(\Phi_a(x), \Phi_b(x)) > 1$ следува дека $\alpha > 0$. Сега, од последицата 2.9 следува дека

$$0 \equiv \Phi_a(x) = \Phi_{p^\alpha A}(x) = \frac{\Phi_A(x^{p^\alpha})}{\Phi_A(x^{p^{\alpha-1}})} (\mathrm{mod}\, p),$$

па затоа $0 \equiv \Phi_A(x^{p^\alpha}) (\mathrm{mod}\, p)$. Понатаму, бидејќи $p^\alpha - 1$ е делив со $p-1$, а од теоремата на Ферма следува дека $x^{p^\alpha - 1} \equiv 1 (\mathrm{mod}\, p)$, па затоа $x^{p^\alpha} \equiv x (\mathrm{mod}\, p)$. Значи,

$$0 \equiv \Phi_A(x^{p^\alpha}) \equiv \Phi_A(x) (\mathrm{mod}\, p),$$

т.е. $p \mid \Phi_A(x)$. Аналогно се докажува дека $p \mid \Phi_B(x)$.

Нека претпоставиме дека $A > B$. Ако $m = (A, B)$, тогаш $m < A$. Бидејќи $p \mid \Phi_A(x) \mid x^A - 1$ и $p \mid \Phi_B(x) \mid x^B - 1$ заклучуваме, дека $p \mid (x^A - 1, x^B - 1)$. Сега од пример 3.10 следува $p \mid x^m - 1 = \prod_{d \mid m} \Phi_d(x)$. Според тоа, постои делител d на m таков што $p \mid \Phi_d(x)$. Значи, $d \mid m \mid A, d < A$, $p \mid \Phi_A(x)$ и $p \mid \Phi_d(x)$, па од лема 3.2 следува $p \mid A$, што противречи на претпоставката дека $p \nmid A$.

Конечно, од добиената противречност следува $A = B$, па затоа $\frac{a}{b} = p^{\alpha - \beta} = p^k$, за $k \in \mathbb{Z}$. ■

3.12. Пример. Определи ги сите цели броеви x и y такви што

$$\frac{x^7 - 1}{x - 1} = y^5 - 1. \tag{3}$$

Решение. Равенството (3) е еквивалентно со равенството

$$1 + x + x^2 + x^3 + x^4 + x^5 + x^6 = (y-1)(1 + y + y^2 + y^3 + y^4).$$

Јасно, секој прост број p кој е делител на левата страна на последното равенство е непарен, т.е. $p > 2$. Сега, од последицата 3.9 следува дека за секој прост број p кој е делител на $y - 1$ важи или $p = 7$ или $p \equiv 1 (\mathrm{mod}\, 7)$, па затоа важи или $y - 1 \equiv 0 (\mathrm{mod}\, 7)$ или $y - 1 \equiv 1 (\mathrm{mod}\, 7)$, т.е. или $y \equiv 1 (\mathrm{mod}\, 7)$ или $y \equiv 2 (\mathrm{mod}\, 7)$.

Ако $y \equiv 1 (\mathrm{mod}\, 7)$, тогаш $1 + y + y^2 + y^3 + y^4 \equiv 5 \not\equiv 0, 1 (\mathrm{mod}\, 7)$.

Ако $y \equiv 2 (\mathrm{mod}\, 7)$, тогаш $1 + y + y^2 + y^3 + y^4 \equiv 31 \not\equiv 0, 1 (\mathrm{mod}\, 7)$.

Според тоа, не постојат цели броеви x и y такви што важи (3). ■

3.13. Пример. Нека $p_1, p_2, ..., p_n$ се различни прости броеви поголеми од 3. Докажи дека бројот $2^{p_1 p_2 \cdots p_n} + 1$ има најмалку $2^{2^{n-1}}$ делител.

Решение. Доволно е да се докаже дека бројот $2^{p_1 p_2 \cdots p_n} + 1$ има најмалку 2^{n-1} заемно прости делители. Имаме:

$$(2^{p_1p_2\cdots p_n}-1)(2^{p_1p_2\cdots p_n}+1)=2^{2p_1p_2\cdots p_n}-1=\prod_{d\mid 2p_1p_2\cdots p_n}\Phi_d(2)$$
$$=(\prod_{d\mid p_1p_2\cdots p_n}\Phi_d(2))(\prod_{d\mid p_1p_2\cdots p_n}\Phi_{2d}(2))$$
$$=(2^{p_1p_2\cdots p_n}-1)(\prod_{d\mid p_1p_2\cdots p_n}\Phi_{2d}(2)),$$

па затоа

$$2^{p_1p_2\cdots p_n}+1=\prod_{d\mid p_1p_2\cdots p_n}\Phi_{2d}(2).$$

Според теоремата 3.11, ако $\Phi_a(x)$ и $\Phi_b(x)$ не се заемно прости, тогаш $\frac{a}{b}$ е степен на прост број. Оттука следува дека доволно е да докажеме дека може да се земат 2^{n-1} различни делители на бројот $p_1p_2...p_n$ такви што количникот на никои два не е прост број. Изборот на делители на бројот $p_1p_2...p_n$ кои имаат парен број делители очигледно ги задоволува условите на задата, со што доказот е завршен. ■

4. ТЕОРЕМА НА ЖИГИМОНДИ

4.1. Лема. Нека $a,n>1$ се природни броеви. Ако сите прости делители на $\Phi_n(a)$ се делители и на n, тогаш $\Phi_n(a)$ е прост број кој е делител на n или $n=2$.

Доказ. Нека p е произволен прост делител на $\Phi_n(a)$. Бидејќи слободниот член на секој цикломатичен полином е ±1, заклучуваме дека $(p,a)=1$. Нека $k=\delta(a,p)$. Од теорема 3,6 следува $p\mid\Phi_k(a)$. Сега, од теорема 3.11 следува дека $\frac{n}{k}=p^t$ за некој природен број t, што значи $p\mid n$. Понатаму,

$$x^n-1=\Phi_n(x)Q(x)$$

за некој полином $Q(x)$. Сега, од теорема 2.3 следува дека $x^{\frac{n}{p}}-1\mid Q(x)$. Освен тоа од лемата за зголемување на експонентот следува дека ако p е непарен прост број тогаш $v_p(a^n-1)=v_p(a^{\frac{n}{p}}-1)+1$, освен ако $n=2$. Значи, $v_p(\Phi_n(a))=1$, освен ако $n=2$.

Нека q е друг прост број кој е делител на $\Phi_n(a)$. Тогаш, ако $y=\delta(a,q)$, аналогно како погоре се добива дека $\frac{n}{y}=q^s$. Сега, од $kp^t=n=yq^s$ следува $p\mid y$ и $q\mid k$, од каде добиваме $q\mid p-1$ и $p\mid q-1$, што е противречност. ■

4.2. Лема. Нека $a,n>1$ се природни броеви. Нека $n=p^k r$, каде $p\nmid r$. Тогаш

$$\Phi_n(a)>(b^{p-2}(b-1))^{\varphi(r)}, \tag{1}$$

каде $b=a^{p^{k-1}}$.

Доказ. Од последицата 2.9 следува

$$\Phi_n(a)=\frac{\Phi_r(b^p)}{\Phi_r(b)}.$$

Бидејќи b^p е барем за b^p-1 поголем од било кој корен на полиномот $\Phi_r(x)$, лесно се докажува дека $\Phi_r(b^p)>(b^p-1)^{\varphi(r)}$. Слично, лесно се докажува дека $\Phi_r(b)<(b+1)^{\varphi(r)}$. Според тоа,

$$\Phi_n(a)>(\tfrac{b^p-1}{b+1})^{\varphi(r)},$$

па ако земеме предвид дека

$$b^p-1>b^p-b^{p-2}=b^{p-2}(b^2-1),$$

го добиваме неравенството (1). ■

4.3. Теорема (Жигимонди). Нека a и n се природни броеви поголеми од 1. Тогаш постои прост делител q на a^n-1 таков што q не е делител на a^j-1 за $j\in\{1,2,...,n-1\}$, освен ако

1) $n=2, a=2^s-1$, каде $s\geq 2$ или
2) $n=6, a=2$.

Доказ. Треба да докажеме дека за секои a и n, освен во случаите 1) и 2), кои лесно се проверуваат, постои прост број p таков што $\delta(a,p)=n$.

Ако $n=2$, точноста на теоремата лесно се проверува и се констатира исклучокот. Нека $n>2$. Ако претпоставиуме дека не постои таков прост број q за кој $\delta(a,q)=n$, тогаш од лемата 4.1 следува дека $\Phi_n(a)=p$ за некој прост број p. Навистина, не може да важи $q\mid\Phi_n(a)$ и $q\nmid n$, за некој прост број q, бидејќи тогаш од теоремата 3.6 следува $\delta(a,q)=n$, што очигледно не е можно.

Ако $n=p^k r$, каде k и r се природни броеви и $(p,r)=1$, тогаш од лемата 4.2 следува

$$p>(b^{p-2}(b-1))^{\varphi(r)},$$

каде $b=a^{p^{k-1}}$. Ако $p\geq 5$, тогаш $b^{p-2}>p$, па добиваме противречност. Значи, $p=3$. Но, тогаш $a=2,k=1,r=1$ или $r=2$. Оттука ги добиваме случаите $n=3$ или $n=6$. Лесно се проверува дека случајот $n=3, a=2$ важи, а за $n=6, a=2$ веќе констатиравме дека спаѓа во исклучоците. ■

4.4. Последица. Нека a и n се природни броеви поголеми од 1. Тогаш постои прост делител q на a^n+1 таков што q не е делител на a^j-1 за $j\in\{1,2,...,n-1\}$, освен ако $n=3, a=2$.

Доказ. Нека $n\in\mathbb{N}\setminus\{1\}$. Нека p е прост број таков што $\delta(a,p)=2n$, кој според теоремата на Жигимонди сигурно постои. Тогаш мора да важи $p\mid a^n+1$ и не постои $j<n$ таков што $p\mid a^j+1$, бидејќи во спротивно би важело $p\mid a^{2j}-1$, при што $2j<2n$, што е противречност. Со проверка на оние вредности кои се исклучоци во теоремата на Жигимонди, добиваме дека во случајов искочок е $n=3, a=2$. ■

4.5. Пример. Определи ги сите петорки (a,n,p,q,r) природни броеви такви што важи

$$a^n-1=(a^p-1)(a^q-1)(a^r-1). \qquad (1)$$

Решение. Ако $a=1$, тогаш сите петорки $(1,n,p,q,r)$ ја задоволуваат равенката (1). Ако $n>p,q,r\ (a\neq 1)$, тогаш според теоремата на Жигимонди a^n-1 има делител кој не е делител на ниту еден од множителите на десната страна на (1). Заради исклучоците во теоремата имаме два можни подслучаи.

а) $n=2, a=2^s-1$, каде $s\geq 2$. Тогаш мора да е $p=q=r=1$. Ако овие вредности ги замениме во (1) добиваме $a=3$. Значи, петорката $(3,2,1,1,1)$ е решение на (1).

б) $n=6, a=2$. Со едноставна провека на делителите на бројот $63=2^6-1$ ги добиваме решенијата $(2,6,2,2,3),(2,6,2,3,2),(2,6,3,2,2)$.

Нека барем еден од p,q,r важи дека е еднаков на n, на пример $p=n$. Тогаш $(a^q-1)(a^r-1)=1$, па затоа $a=2, q=1, r=1$. Аналогно постапуваме во случаите кога q или r е еднаков на n, па затоа во овие три случаи решенија се петорките $(2,n,n,1,1),(2,n,1,n,1),(2,n,1,1,n)$, каде $n\in\mathbb{N}$. ■

4.6. Пример. Определи ги сите тројки природни броеви (a,m,n) такви што важи $a^m+1\mid(a+1)^n$.

Решение. Ако $a,m>1$, тогаш од последицата 4.4 следува дека постои прост број p кој е делител на a^m+1, но не е делител на $a+1$, што значи и на $(a+1)^n$. Исклучоци се $n=3, a=2$ и со непосредна проверка добиваме дека сите тројки од видот $(2,3,n)$, $n\geq 2$ се решение на задачата. Ако $a=1$ или $m=1$, добиваме нови решенија $(1,m,n),(a,1,n)$ каде m,n, т.е. a,n се произволни природни броеви. ■

4.7. Во претходните разгледувања се осврнавме на специјален случај на теоремата на Жигимонди, кој е погоден за цикломатичните полиноми. Сега, без доказ, ќе го презентираме општиот облик на теоремата на Жигимонди, а исто така без доказ ќе ја презентираме и генерализацијата на последицата 4.4. Притоа, покасно ќе разгледаме примери за чие решавање се искористени овие тврдења.

Теорема (Жигимонди). Нека a,b и n се природни броеви такви што $n>1$ и $a>b>0$. Тогаш постои прост делител q на a^n-b^n таков што q не е делител на a^j-b^j, за $j\in\{1,2,...,n-1\}$, освен ако:

1) $n=2, a+b=2^s$, каде $s\geq 2$ или
2) $n=6, a=2, b=1$. □

4.8. Последица. Нека a,b и n се природни броеви такви што $n>1$, $a,b>0$ и $a\neq b$. Тогаш постои прост делител q на a^n+b^n таков што q не е делител на a^j+b^j за $j\in\{1,2,...,n-1\}$, осве ако $n=3, a=2, b=1$. □

4.9. Пример. Докажи дека низата $a_n=3^n-2^n$, $n\in\mathbb{N}$, не содржи три члена кои формираат геометриска прогресија.

Решение. Нека претпоставиме дека за природните броеви x,y,z важи

$$q(3^x-2^x)=3^y-2^y \text{ и } q^2(3^x-2^x)=3^z-2^z.$$

Јасно, бројот q е рационален, т.е. $q=\frac{a}{b}$, $(a,b)=1$. Според тоа, важи

$$a(3^x-2^x)=b(3^y-2^y) \text{ и } a^2(3^x-2^x)=b^2(3^z-2^z). \qquad (2)$$

Нека p е прост број кој е делител на a_z, а не е делител на a_x и a_y. Тогаш од второто равенство во (2) следува $p\mid a$, но тогаш за да биде исполнето првото равенство во (2) мора да важи $p\mid b$. Според тоа, имаме противречност за сите вредности x,y,z, бидејќи 3 и 2 не се исклучоци во теоремата на Жигимонди 4.5. ■

4.10. Пример. Докажи дека не постојат природни броеви x,y и прост број z такви што

$$x^{2013}+y^{2013}=z^{2013}. \qquad (3)$$

Решение. Од $x+y\mid x^{2013}+y^{2013}$ и последицата 4.8 следува дека $x^{2013}+y^{2013}$ има најмалку два различни прости делители и тоа прост делител p на $x+y$ и прост делител q на $x^{2013}+y^{2013}$ кој не е делител на a^j+b^j за $j\in\{1,2,...,2012\}$.

Но, z е прост број, па затоа десната страна на (3) има само еден прост делител, што значи дека равенката (3) нема решение.

Да забележиме дека равенката (3) е специјален случај на големата теорема на Ферма за која покасно ќе стане збор, па затоа одма можевме да заклучиме дека истата нема решение. ■

VI ГЛАВА
КВАДРАТНИ ОСТАТОЦИ

1. КВАДРАТНИ ОСТАТОЦИ ПО ПРОСТ МОДУЛ

1.1. Нека $p>2$ е прост број. Да ја разгледаме конгруенцијата од втор степен

$$c_0x^2+c_1x+c_2\equiv 0(\mathrm{mod}\,p), \tag{1}$$

каде $(c_0,p)=1$. Како што знаеме оваа конгруенција има најмногу две решенија, но во ваков облик истата потешко се решава. Затоа ќе ја докажеме следнава лема.

Лема. Конгруенцијата (1) е еквивалентна на конгруенција од видот

$$(x+c)^2\equiv a(\mathrm{mod}\,p).$$

Доказ. Бидејќи $(c_0,p)=1$, ако конгруенцијата (1) ја помножиме со c_0^{p-2} и ја искористиме малата теорема на Ферма, добиваме еквивалентна конгруенција

$$x^2+b_1x+b_2\equiv 0(\mathrm{mod}\,p).$$

Понатаму, ако бројот b_1 е парен, со одделување на точен квадрат ја добиваме еквивалентната конгруенција

$$(x+\tfrac{b_1}{2})^2\equiv \tfrac{b_1^2}{4}-b_2(\mathrm{mod}\,p),$$

а ако бројот b_1 е непарен, тогаш b_1+p е парен и ја добиваме еквивалентната конгруенција

$$(x+\tfrac{b_1+p}{2})^2\equiv \tfrac{(b_1+p)^2}{4}-b_2(\mathrm{mod}\,p),$$

со што доказот е завршен. ■

Во конгруенцијата $(x+c)^2\equiv a(\mathrm{mod}\,p)$ можеме да ставиме $x+c=y$. Последното значи дека за да ги проучиме конгруенциите од видот (1), доволно е да ги проучиме конгруенциите од видот $x^2\equiv a(\mathrm{mod}\,p)$. Уште повеќе, ако класата x_0 е решение на последната конгруенција, тогаш и класата $-x_0$ е нејзино решение, при што од $p>2$ следува дека двете класи се различни. Според тоа, конгруенцијата (1) или нема решение, или има единствено решение 0 (случајот кога $p\mid a$) или има две решенија кои зависат од a и p.

1.2. Дефиниција. Нека $(a,p)=1$. Ако конгруенцијата $x^2\equiv a(\mathrm{mod}\,p)$ има решение, тогаш велиме дека a е *квадратен остаток* по модул p. Во спротивно велиме дека a е *квадратен неостаток* по модул p.

1.3. Теорема. Нека p е непарен прост број. Редуцираниот систем на остатоци по модул p се состои од $\frac{p-1}{2}$ квадратни остатоци и $\frac{p-1}{2}$ квадратни неостатоци по модул p.

Доказ. Секој квадратен остаток по модул p е конгруентен на квадратот на некој од броевите

$$-\frac{p-1}{2}, -\frac{p-3}{2}, ..., -2, -1, 1, 2, ..., \frac{p-3}{2}, \frac{p-1}{2},$$

т.е. конгруентен е на некој од броевите $1^2, 2^2, ..., (\frac{p-1}{2})^2$. Останува да докажеме дека овие $\frac{p-1}{2}$ броеви меѓусебно не се конгруентни по модул p. Нека претпоставиме дека $k^2 \equiv t^2 (\mathrm{mod}\, p)$, каде $1 \le t < k \le \frac{p-1}{2}$. Тогаш $(k-t)(k+t) \equiv 0 (\mathrm{mod}\, p)$, па затоа $k-t \equiv 0 (\mathrm{mod}\, p)$ или $k+t \equiv 0 (\mathrm{mod}\, p)$, што не е можно бидејќи $0 < k-t < p$ и $0 < k+t < p$. ■

1.4. Дефиниција. За даден прост број p и цел број a *симболот на Лежандр* $(\frac{a}{p})$ е определен со

$$(\frac{a}{p}) = \begin{cases} 1, & \text{ако } p \nmid a \text{ и } a \text{ е квадратен остаток по модул } p \\ -1, & \text{ако } p \nmid a \text{ и } a \text{ е квадратен неостаток по модул } p \\ 0, & \text{ако } p \mid a. \end{cases}$$

Според тоа, бројот на решенијата на конгруенцијата $x^2 \equiv a (\mathrm{mod}\, p)$ е еднаков на $1 + (\frac{a}{p})$.

1.5. Теорема (критериум на Ојлер). Нека a е цел број и p е непарен прост број. Тогаш

$$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} (\mathrm{mod}\, p). \qquad (2)$$

Доказ. Ако $(\frac{a}{p}) = 0$, тогаш $p \mid a$, што значи дека е точна конгруенцијата (2).

Ако $(\frac{a}{p}) = 1$, тогаш $p \nmid a$ и постои $x_0 \in \mathbb{Z}$ таков што $x_0^2 \equiv a (\mathrm{mod}\, p)$. Сега, од малата теорема на Ферма следува $a^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1 = (\frac{a}{p}) (\mathrm{mod}\, p)$, т.е. точна е конгруенцијата (2).

Нека $(\frac{a}{p}) = -1$. Од теоремата IV 2.5 следува дека за секој $i \in \{1, ..., p-1\}$ можеме да избереме $j \in \{1, ..., p-1\}$ таков што важи $ij \equiv a (\mathrm{mod}\, p)$. Притоа, бидејќи конгру-

енцијата $x^2 \equiv a(\mathrm{mod}\, m)$ нема решение важи $i \neq j$. Значи, множеството $\{1,...,p-1\}$ го разбивме на $\frac{p-1}{2}$ подмножества $\{i, j\}$ такви што $ij \equiv a(\mathrm{mod}\, p)$. Ако ги помножиме овие $\frac{p-1}{2}$ конгруенции и ја примениме теоремата на Вилсон, добиваме

$$a^{\frac{p-1}{2}} \equiv (p-1)! \equiv -1 = (\frac{a}{p})(\mathrm{mod}\, p),$$

т.е. точна е конгруенцијата (2). ■

1.6. Теорема. Нека p е непарен прост број.

а) Ако $a \equiv b(\mathrm{mod}\, p)$, тогаш $(\frac{a}{p}) = (\frac{b}{p})$.

б) $(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$, за секои цели броеви a и b.

в) Ако $(a, p) = 1$, тогаш $(\frac{a^2}{p}) = 1$.

г) $(\frac{1}{p}) = 1$, $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$.

Доказ. а) Ако $a \equiv b(\mathrm{mod}\, p)$, тогаш конгруенцијата $x^2 \equiv a(\mathrm{mod}\, p)$ има решение ако и само ако конгруенцијата $x^2 \equiv b(\mathrm{mod}\, p)$ има решение, па затоа $(\frac{a}{p}) = (\frac{b}{p})$.

б) Согласно Критериумот на Ојлер, за секои цели броеви a и b важи

$$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}}(\mathrm{mod}\, p),\ (\frac{b}{p}) \equiv b^{\frac{p-1}{2}}(\mathrm{mod}\, p) \text{ и } (\frac{ab}{p}) \equiv (ab)^{\frac{p-1}{2}}(\mathrm{mod}\, p),$$

па затоа

$$(\frac{a}{p})(\frac{b}{p}) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} \equiv (\frac{ab}{p})(\mathrm{mod}\, p),$$

од каде следува

$$(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p}).$$

в) Конгруенцијата $x^2 \equiv a^2(\mathrm{mod}\, p)$ има решение $x = a$, па затоа $(\frac{a^2}{p}) = 1$.

г) Равенството $(\frac{1}{p}) = 1$ непосредно следува од тврдењето под в) за $a = 1$.

Ако во критериумот на Ојлер ставиме $a = -1$ добиваме $(\frac{-1}{p}) \equiv (-1)^{\frac{p-1}{2}}(\mathrm{mod}\, p)$, од каде следува $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$. ■

1.7. Последица. Нека p е непарен прост број. Тогаш

$$(\frac{-1}{p}) = \begin{cases} 1, & p \equiv 1(\mathrm{mod}\, 4), \\ -1, & p \equiv 3(\mathrm{mod}\, 4). \end{cases}$$

Доказ. Секој непарен прост број p е од видот $p=4k+1$ или $p=4k+3$. Ако $p=4k+1$, тогаш од теоремата 1.6 следува

$$(\tfrac{-1}{p})=(-1)^{\frac{p-1}{2}}=(-1)^{2k}=1,$$

а ако $p=4k+3$, тогаш повторно од теоремата 1.6 следува

$$(\tfrac{-1}{p})=(-1)^{\frac{p-1}{2}}=(-1)^{2k+1}=-1,$$

што и требаше да се докаже. ■

1.8. Теорема. Нека x,y се заемно прости цели броеви и a,b,c се произволни цели броеви. Ако p е непарен прост делител на бројот $ax^2+bxy+cy^2$ кој не е делител на ниту еден од коефициентите a,b,c, тогаш $D=b^2-4ac$ е квадратен остаток по модул p.

Специјално, ако $p\mid x^2-Dy^2$ и $(x,y)=1$, тогаш D е квадратен остаток по модул p.

Доказ. Нека $N=ax^2+bxy+cy^2$. Од $4aN=(2ax+by)^2-Dy^2$ и $p\mid N$ следува

$$(2ax+by)^2\equiv Dy^2 (\mathrm{mod}\, p).$$

Понатаму, y не е делив со p, бидејќи во спротивно и $2ax+by$, а со тоа и x ќе биде делив со p, што противречи на претпоставката дека x,y се заемно прости цели броеви.

Бидејќи y не е делив со p, постои цел број y_1 таков што $yy_1\equiv 1(\mathrm{mod}\, p)$. Горната конгруенција ја ножиме со y_1^2 и добиваме

$$(2axy_1+byy_1)^2\equiv D(yy_1)^2\equiv D(\mathrm{mod}\, p),$$

од каде што следува тврдењето. ■

1.9. Теорема (лема на Гаус). Нека p е непарен прост број и a е цел број таков што $(a,p)=1$. Нека a_j за $1\le j\le\frac{p-1}{2}$ е најмалиот ненегативен остаток на бројот aj по модул p. Тогаш

$$(\tfrac{a}{p})=(-1)^n,$$

каде n е бројот на остатоците кои се поголеми од $\frac{p}{2}$.

Доказ. Нека $r_1,r_2,...,r_n$ се остатоците кои се поголеми од $\frac{p}{2}$, а $s_1,s_2,...,s_k$ се пресотанатите остатоци. Според теоремата IV 2.5 овие броеви се по парови раз-

лични и ниту еден од нив не е еднаков на нула. Значи, $n+k=\frac{p-1}{2}$. Понатаму, броевите $p-r_i, i=1,2,..,n$ се различни и $0<p-r_i<\frac{p}{2}$ за $i=1,2,..,n$. Исто така, ниту еден $p-r_i$ не е еднаков на некој s_j. Навистина, ако $p-r_i=s_j$, тогаш

$$r_i \equiv \alpha a (\mathrm{mod}\, p),\ s_j \equiv \beta a (\mathrm{mod}\, p)$$

за некои $\alpha,\beta \in \{1,2,...,\frac{p-1}{2}\}$, па од $(a,p)=1$ и $a(\alpha+\beta) \equiv r_i + s_j \equiv 0 (\mathrm{mod}\, p)$ следува $\alpha+\beta \equiv 0 (\mathrm{mod}\, p)$ што не е можно бидејќи $2 \le \alpha+\beta \le p-1$.

Според тоа, броевите $p-r_1, p-r_2, ..., p-r_n, s_1, ..., s_k$ се некоја пермутација на броевите $1,2,...,\frac{p-1}{2}$. Затоа

$$\begin{aligned}(\tfrac{p-1}{2})! &= (p-r_1)(p-r_2)...(p-r_n)s_1...s_k \\ &\equiv (-1)^n r_1 r_2 ... r_n s_1 s_2 ... s_k \\ &\equiv (-1)^n a \cdot 2a \cdot ... \cdot \tfrac{p-1}{2} a \\ &= (-1)^n (\tfrac{p-1}{2})! a^{\frac{p-1}{2}} (\mathrm{mod}\, p).\end{aligned}$$

Последната конгруенција ја кратиме со $(\frac{p-1}{2})!$ и добиваме $(-1)^n a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$, т.е. $a^{\frac{p-1}{2}} \equiv (-1)^n (\mathrm{mod}\, p)$. Од критериумот на Ојлер следува $(\frac{a}{p}) \equiv (-1)^n (\mathrm{mod}\, p)$, па затоа $(\frac{a}{p}) = (-1)^n$. ■

1.10. Забелешка. Лемата на Гаус може да се формулира и на следниов начин: Нека p е непарен прост број и a е цел број таков што $(a,p)=1$. Нека a_j за $1 \le j \le \frac{p-1}{2}$ е најмалиот остаток на бројот aj по модул p. Тогаш $(\frac{a}{p}) = (-1)^n$, каде n е бројот на негативните броеви меѓу броевите a_j, $1 \le j \le \frac{p-1}{2}$.

1.11. Теорема (правило на двојката). Нека p е непарен прост број. Тогаш

$$(\tfrac{2}{p}) = (-1)^{\frac{p^2-1}{8}},$$

т.е. бројот 2 е квадратен остаток по модул p ако и само ако $p = 8k \pm 1$.

Доказ. Ако $p = 8k+1$ за некој природен број k, тогаш бројот n од лемата на Гаус е еднаков на бројот на броевите меѓу $2,4,6,..., p-1 = 8k$ кои се поголеми од $\frac{p-1}{2} = 4k$. Според тоа, $n = 2k$ и $(\frac{2}{p}) = 1 = (-1)^{\frac{p^2-1}{8}}$.

Случаите $p=8k-1, p=8k+3$ и $p=8k-3$ се разгледуваат аналогно. Деталите ги оставаме на читателот за вежба. ■

1.12. Аналогно на доказот на теоремата 1.11 може да се докаже следнава теорема. Деталите ги оставаме на читателот за вежба.

Теорема. а) Бројот -2 е квадратен остаток по модул p ако и само ако $p\equiv 1(\mathrm{mod}8)$ или $p\equiv 3(\mathrm{mod}8)$.

б) Бројот -3 е квадратен остаток по модул p ако и само ако $p\equiv 1(\mathrm{mod}6)$.

в) Бројот 3 е квадратен остаток по модул p ако и само ако $p\equiv \pm 1(\mathrm{mod}12)$.

г) Бројот 5 е квадратен остаток по модул p ако и само ако $p\equiv \pm 1(\mathrm{mod}10)$. □

1.13. Пример. Нека p е непарен прост број. Постои природен број $a<\sqrt{p}+1$ кој е квадратен неостаток по модул p. Докажи!

Решение. Нека a е најмалиот квадратен неостаток по модул p и $b=[\frac{p}{a}]+1$. Бидејќи $0<ab-p<a$ и a е најмалиот квадратен неостаток, добиваме дека $ab-p$ е квадратен остаток. Затоа

$$1=(\tfrac{ab-p}{p})=(\tfrac{a}{p})(\tfrac{b}{p})=-(\tfrac{b}{p}).$$

Според тоа, b е квадратен неостаток, па затоа $a\le b<\frac{p}{a}+1$, од каде следува тврдењето. ■

1.14. Пример. Докажи дека за $n\in\mathbb{N}$ секој прост делител на бројот n^4-n^2+1 е од видот $12k+1$.

Решение. Имаме

$$n^4-n^2+1=(n^2-1)^2+n^2 \text{ и } n^4-n^2+1=(n^2+1)^2-3n^2.$$

Користејќи ги теоремите 1.6 г), 1.8 и 1.12, од првото равенство добиваме дека $p\equiv 1(\mathrm{mod}4)$, а од второто дека $p\equiv \pm 1(\mathrm{mod}12)$. Конечно, од овие конгруенции следува дека $p\equiv 1(\mathrm{mod}12)$. ■

1.15. Пример. Докажи дека постојат бесконечно многу прости броеви од видот $8k+3$.

Решение. Нека $p_1, p_2, ..., p_n$ се сите прости броеви од видот $8k+3$. Да го разгледаме бројот

$$m=p_1^2p_2^2...p_n^2+2.$$

Од теоремата 1.12 а) следува дека сите прости делители на бројот m се од видот $8k+1$ или $8k+3$. Но, $m\equiv 3(\mathrm{mod}8)$, па затоа не може сите прости делители на m

да се од видот $8k+1$. Значи, постои прост делител p на m од видот $8k+3$. Очигледно, $p \neq p_i$, $i=1,2,...,n$, што е противречност. ■

1.16. Пример. Нека $p \equiv 1 (\mathrm{mod}\, 4)$. Пресметај го збирот на сите квадратни остатоци r по модул p такви што $1 \leq r \leq p-1$.

Решение. Според теоремата 1.3 имаме $\frac{p-1}{2}$ квадратни остатоци по модул p. Понатаму, од теоремата 1.6 следува

$$(\frac{p-r}{p}) = (\frac{-r}{p}) = (\frac{-1}{p})(\frac{r}{p}) = (-1)^{\frac{p-1}{2}}(\frac{r}{p}) = (-1)^{\frac{4k+1-1}{2}}(\frac{r}{p}) = (\frac{r}{p}).$$

Тоа значи дека r е квадратен остаток по модул p ако и само ако $p-r$ е квадратен остаток по модул p. Затоа важи

$$2\sum_{\substack{1\leq r\leq p-1\\(\frac{r}{p})=1}} r = \sum_{\substack{1\leq r\leq p-1\\(\frac{r}{p})=1}} r + \sum_{\substack{1\leq r\leq p-1\\(\frac{r}{p})=1}} (p-r) = \frac{p(p-1)}{2}, \text{ т.е. } \sum_{\substack{1\leq r\leq p-1\\(\frac{r}{p})=1}} r = \frac{p(p-1)}{4}. \blacksquare$$

1.17. Пример. Докажи дека постојат бесконечно многу непарни броеви n, за произволен парен број x такви што ниту еден од броевите на бесконечната низа

$$x^x+1, x^{x^x}+1, x^{x^{x^x}}+1, \ldots,$$

не е делив со n.

Решение. Такви се, на пример, сите прости броеви p од облик $4k+3$. Навистина, ако x е парен број, тогаш секој член на низата $x, x^x, x^{x^x}, \ldots$ е парен број. Затоа, ако некој член на низата $x^x+1, x^{x^x}+1, x^{x^{x^x}}+1, \ldots$ е делив со p, тогаш за некој природен број m ќе имаме $p \mid x^{2m}+1$, па затоа

$$(x^m)^2 \equiv -1 (\mathrm{mod}\, p),$$

што не е можно бидејќи според последицата 1.7 бројот -1 не е квадратен остаток на простиот број $p=4k+3$. ■

2. ГАУСОВ ЗАКОН ЗА РЕЦИПРОЦИТЕТ

2.1. Теорема. Ако p е непарен прост број и $(a,2p)=1$, тогаш $(\frac{a}{p}) = (-1)^t$, каде $t = \sum_{j=1}^{\frac{p-1}{2}} [\frac{ja}{p}]$.

Доказ. Нека при делење со p на броевите aj, $j=1,2,...,\frac{p-1}{2}$ најмалите ненега-

тивни остатоци кои се поголеми од $\frac{p}{2}$ се $r_1, r_2, ..., r_n$, а $s_1, s_2, ..., s_k$ се преостанатите остатоци. При овие делења количници се броевите $[\frac{ja}{p}]$, па затоа ако $(a, p) = 1$ добиваме

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p[\frac{ja}{p}] + \sum_{i=1}^{n} r_i + \sum_{i=1}^{k} s_i$$

и

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{i=1}^{n} (p - r_i) + \sum_{i=1}^{k} s_i = np - \sum_{i=1}^{n} r_i + \sum_{i=1}^{k} s_i \ .$$

Ако ги одземеме овие равенства добиваме

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = p(\sum_{j=1}^{\frac{p-1}{2}} [\frac{ja}{p}] - n) + 2\sum_{i=1}^{n} r_i \ .$$

Понатаму,

$$\sum_{j=1}^{\frac{p-1}{2}} j = \frac{\frac{p-1}{2}(\frac{p-1}{2}+1)}{2} = \frac{p^2-1}{8},$$

па затоа

$$(a-1)\frac{p^2-1}{8} \equiv \sum_{j=1}^{\frac{p-1}{2}} [\frac{ja}{p}] - n \pmod 2 \ . \qquad (1)$$

Сега, ако a е непарен, т.е. $(a, 2p) = 1$, тогаш оттука следува

$$\sum_{j=1}^{\frac{p-1}{2}} [\frac{ja}{p}] \equiv n \pmod 2 \ ,$$

па тврдењето на теоремата следува од лемата на Гаус (теорема 1.9). ■

2.2. Забелешка. Ако во претходната теорема земеме $a = 2$, тогаш бидејќи $[\frac{2j}{p}] = 0$ за $j = 1, 2, ..., \frac{p-1}{2}$ од (1) добиваме $\frac{p^2-1}{8} \equiv n \pmod 2$, па од лемата на Гаус (теорема 1.9) следува $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$ и ова е уште еден доказ на правилото на двојката (теорема 1.10).

2.3. Теорема (Гаусов закон за реципроцитет). Ако p и q се различни непарни прости броеви, тогаш важи

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \ .$$

Доказ. Нека

$$S=\{(x,y)\mid x,y\in\mathbb{Z},1\le x\le\tfrac{p-1}{2},1\le y\le\tfrac{q-1}{2}\}.$$

Множеството S има $\frac{p-1}{2}\cdot\frac{q-1}{2}$ елементи. Множеството S го делиме на две дисјунктни множества S_1 и S_2 во зависност од тоа дали $qx>py$ или $qx<py$. Јасно, не е можне да биде $qx=py$. Значи, S_1 е множеството од сите парови $(x,y)\in\mathbb{Z}^2$ такви што $1\le x\le\frac{p-1}{2}$ и $1\le y<\frac{qx}{p}$. Такви парови има $\sum_{x=1}^{\frac{p-1}{2}}[\frac{qx}{p}]$. Слично, S_2 е множеството од сите парови $(x,y)\in\mathbb{Z}^2$ такви што $1\le y\le\frac{q-1}{2}$ и $1\le x<\frac{py}{q}$, а такви парови има $\sum_{y=1}^{\frac{q-1}{2}}[\frac{py}{q}]$. Според тоа,

$$\sum_{x=1}^{\frac{p-1}{2}}[\frac{qx}{p}]+\sum_{y=1}^{\frac{q-1}{2}}[\frac{py}{q}]=\frac{p-1}{2}\cdot\frac{q-1}{2},$$

па од теоремата 2.1 следува

$$(\frac{p}{q})(\frac{q}{p})=(-1)^{\sum_{y=1}^{\frac{q-1}{2}}[\frac{py}{q}]}(-1)^{\sum_{x=1}^{\frac{p-1}{2}}[\frac{qx}{p}]}=(-1)^{\sum_{y=1}^{\frac{q-1}{2}}[\frac{py}{q}]+\sum_{x=1}^{\frac{p-1}{2}}[\frac{qx}{p}]}=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.\ \blacksquare$$

2.4. Една од можните корисни формулации на Гаусовиот закон за реципроцитет е следнава последица.

Последица. Нека p и q се различни прости броеви. Ако p и q се двата од облик $4k+3$, тогаш една од равенките

$$x^2\equiv p(\mathrm{mod}\,q),\ y^2\equiv q(\mathrm{mod}\,p) \tag{2}$$

е решлива, а другата не е решлива. Ако барем еден од p и q е од облик $4k+1$, тогаш или двете равенки (2) се решливи или ниту една од нив не е решлива. □

2.5. Пример. Пресметај $(\frac{-42}{61})$.

Решение. Имаме:

$$(\frac{-42}{61})=(\frac{-1}{61})(\frac{2}{61})(\frac{3}{61})(\frac{7}{61}),\ (\frac{-1}{61})=(-1)^{\frac{61-1}{2}}=1\ \text{и}\ (\frac{2}{61})=(-1)^{\frac{61^2-1}{8}}=-1.$$

Понатаму, од Гаусовиот закон за реципроцитет следува $(\frac{3}{61})(\frac{61}{3})=1$, па затоа $(\frac{3}{61})=(\frac{61}{3})=(\frac{1}{3})=1$. Слично, $(\frac{7}{61})=(\frac{61}{7})=(\frac{5}{7})=(\frac{7}{5})=(\frac{2}{5})=(-1)^{\frac{5^2-1}{8}}=-1$. Конечно, $(\frac{-42}{61})=(\frac{-1}{61})(\frac{2}{61})(\frac{3}{61})(\frac{7}{61})=1\cdot(-1)\cdot1\cdot(-1)=1$, што значи дека -42 еквадратен остаток по модул 61. ■

2.6. Пример. Нека p и q се *прости броеви близнаци*, т.е. $q = p+2$. Докажи дека постои $a \in \mathbb{Z}$ таков што $p \mid (a^2 - q)$ ако и само ако постои $b \in \mathbb{Z}$ таков што $q \mid (b^2 - p)$.

Решение. Прво да забележиме дека едниот од броевите p, q има вид $4k+1$, а другиот $4k+3$. Од теорема 2.3 следува $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{4k+1-1}{2}\cdot\frac{4k+3-1}{2}} = 1$. Затоа, постои $a \in \mathbb{Z}$ таков што $a^2 \equiv q \pmod p$ ако и само ако $(\frac{q}{p}) = 1$ ако и само ако $(\frac{p}{q}) = 1$ ако и само ако постои $b \in \mathbb{Z}$ таков што $b^2 \equiv p \pmod q$. ■

3. КВАДРАТНИ КОНГРУЕНЦИИ ПО СЛОЖЕН МОДУЛ

3.1. Дефиниција. Нека се дадени цел број a и непарен природен број b и нека $b = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ е каноничниот запис на бројот b. *Симболот на Јакоби* $(\frac{a}{b})$ е определен со

$$(\frac{a}{b}) = (\frac{a}{p_1})^{\alpha_1} (\frac{a}{p_2})^{\alpha_2} \ldots (\frac{a}{p_r})^{\alpha_r}.$$

3.2. Забелешка. а) Фактот дека симболот на Јакоби и симболот на Лежандр имаат иста ознака не доведува до конфузија, бидејќи кога b е прост број претходната дефиниција се сведува на дефиницијата 1.4.

б) Лесно се гледа дека од $(\frac{a}{b}) = -1$ следува дека a е квадратен неостаток по модул b. Навистина, ако $(\frac{a}{b}) = -1$, тогаш по дефиниција $(\frac{a}{p_i}) = -1$ за барем еден $p_i \mid b$, па a не е квадратен остаток по модул p_i. Меѓутоа, ако $(\frac{a}{b}) = 1$, тогаш не мора a да е квадратен остаток по модул b. Навистина, иако

$$(\frac{2}{15}) = (\frac{2}{3})(\frac{2}{5}) = (-1)(-1) = 1,$$

бројот 2 не е квадратен остаток по модул 15, бидејќи тоа не е ниту по неговите прости множители.

3.3. Теорема. Нека a е цел број и $b = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ е каноничниот запис на природниот број b. Тогаш a е квадратен остаток по модул b ако и само ако a е квадратен остаток по модул $p_i^{\alpha_i}$ за секој $i = 1, 2, \ldots, r$.

Доказ. Ако a е квадратен остаток по модул b, тогаш очигледно мора да е

квадратен остаток по модул $p_i^{\alpha_i}$ за секој $i=1,2,...,r$.

Нека претпоставиме дека a е квадратен остаток по модул $p_i^{\alpha_i}$ и нека x_i е цел број таков што $x_i^2 \equiv a(\mathrm{mod}\, p_i^{\alpha_i})$. Според Кинеската теорема за остатоци постои број x таков што $x \equiv x_i(\mathrm{mod}\, p_i^{\alpha_i})$ за $i=1,2,...,r$. Тогаш $x^2 \equiv x_i^2 \equiv a(\mathrm{mod}\, p_i^{\alpha_i})$ за секој $i=1,2,...,r$, па затоа $x^2 \equiv a(\mathrm{mod}\, b)$. ■

3.4. Теорема. Ако p е прост број, тогаш квадратни остатоци по модул p^n ($n>0$) има точно $[\frac{2^{n-1}-1}{3}]+2$ за $p=2$, односно $[\frac{p^{n+1}-1}{2(p+1)}]+1$ за $p>2$.

Доказ. Со k_n да го означиме бројот на квадратните остатоци по модул p^n.

Нека p е непарен и $n \geq 2$. Бројот a е квадратен остаток по модул p^n ако и само ако $p \nmid a$ и a е квадратен остаток по модул p, или $p^2 \mid a$ и $\frac{a}{p^2}$ е квадратен остаток по модул p^{n-2}. Според тоа, точно е равенството $k_n = k_{n-2} + \frac{p-1}{2} p^{n-1}$.

Нека $p=2$ и $n \geq 3$. Бројот a е квадратен остаток по модул 2^n ако и само ако $a \equiv 1(\mathrm{mod}8)$ или $4 \mid a$ и $\frac{a}{4}$ е квадратен остаток по модул 2^{n-2}. Според тоа, точно е равенството $k_n = k_{n-2} + 2^{n-3}$.

Сега тврдењето се докажува со математичка индукција. ■

3.5. Теорема. Нека a и a' се цели броеви и b и b' се непарни природни броеви. Тогаш

а) $(\frac{a}{b})(\frac{a}{b'}) = (\frac{a}{bb'})$,

б) $(\frac{a}{b})(\frac{a'}{b}) = (\frac{aa'}{b})$,

в) ако $(a,b)=1$, тогаш $(\frac{a^2}{b}) = (\frac{a}{b^2}) = 1$, и

г) ако $a \equiv a'(\mathrm{mod}\, b)$, тогаш $(\frac{a}{b}) = (\frac{a'}{b})$.

Доказ. Непосредно следува од дефиницијата на симболот на Јакоби и теоремата 1.6. Деталите ги оставаме на читателот за вежба. ■

3.6. Теорема. Ако b е непарен природен број, тогаш

$$(\frac{-1}{b}) = (-1)^{\frac{b-1}{2}} \text{ и } (\frac{2}{b}) = (-1)^{\frac{b^2-1}{8}}.$$

Доказ. Нека $b = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$. Имаме

$$(\frac{-1}{b}) = \prod_{i=1}^{r} (\frac{-1}{p_i})^{\alpha_i} = \prod_{i=1}^{r} (-1)^{\alpha_i \frac{p_i-1}{2}} = (-1)^{\sum_{i=1}^{r} \alpha_i \frac{p_i-1}{2}}.$$

Ако x и y се непарни броеви, тогаш

$$\frac{xy-1}{2} - (\frac{x-1}{2} + \frac{y-1}{2}) = \frac{(x-1)(y-1)}{2} \equiv 0 (\mathrm{mod}\, 2),$$

па затоа

$$\frac{xy-1}{2} \equiv \frac{x-1}{2} + \frac{y-1}{2} (\mathrm{mod}\, 2).$$

Ако повеќекратно ја примениме последната релација добиваме

$$\sum_{i=1}^{r} \alpha_i \frac{p_i-1}{2} \equiv \sum_{i=1}^{r} \frac{p_i^{\alpha_i}-1}{2} \equiv \frac{1}{2} (\prod_{i=1}^{r} p_i^{\alpha_i} - 1) \equiv \frac{b-1}{2} (\mathrm{mod}\, 2), \qquad (1)$$

па затоа

$$(\frac{-1}{b}) = (-1)^{\sum_{i=1}^{r} \alpha_i \frac{p_i-1}{2}} = (-1)^{\frac{b-1}{2}}.$$

Имаме

$$(\frac{2}{b}) = \prod_{i=1}^{r} (\frac{2}{p_i})^{\alpha_i} = \prod_{i=1}^{r} (-1)^{\alpha_i \frac{p_i^2-1}{8}} = (-1)^{\sum_{i=1}^{r} \alpha_i \frac{p_i^2-1}{8}}.$$

Ако x и y се непарни броеви, тогаш

$$\frac{x^2y^2-1}{8} - (\frac{x^2-1}{8} + \frac{y^2-1}{8}) = \frac{(x^2-1)(y^2-1)}{8} \equiv 0 (\mathrm{mod}\, 2),$$

па затоа

$$\frac{x^2y^2-1}{8} \equiv \frac{x^2-1}{8} + \frac{y^2-1}{8} (\mathrm{mod}\, 2).$$

Ако повеќекратно ја примениме последната релација добиваме

$$\sum_{i=1}^{r} \alpha_i \frac{p_i^2-1}{8} \equiv \sum_{i=1}^{r} \frac{(p_i^{\alpha_i})^2-1}{8} \equiv \frac{1}{8} ((\prod_{i=1}^{r} p_i^{\alpha_i})^2 - 1) \equiv \frac{b^2-1}{8} (\mathrm{mod}\, 2),$$

па затоа

$$(\frac{2}{b}) = (-1)^{\sum_{i=1}^{r} \alpha_i \frac{p_i^2-1}{8}} = (-1)^{\frac{b^2-1}{8}}. \blacksquare$$

3.7. Теорема (закон за реципроцитет). Ако a и b се непарни природни броеви и $(a,b)=1$, тогаш

$$(\frac{a}{b})(\frac{b}{a}) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$$

Доказ. Нека

$$a = q_1^{\beta_1} q_2^{\beta_2} \ldots q_s^{\beta_s} \text{ и } b = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$$

се каноничните записи на a и b. Тогаш од теоремата 3.5, теоремата 2.3 и равенството (1) следува

$$\begin{aligned}
(\tfrac{a}{b})(\tfrac{b}{a}) &= (\prod_{i=1}^{r}(\tfrac{a}{p_i})^{\alpha_i})(\prod_{j=1}^{s}(\tfrac{b}{q_j})^{\beta_j}) \\
&= (\prod_{i=1}^{r}(\tfrac{q_1^{\beta_1}q_2^{\beta_2}\ldots q_s^{\beta_s}}{p_i})^{\alpha_i})(\prod_{j=1}^{s}(\tfrac{p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r}}{q_j})^{\beta_j}) \\
&= (\prod_{i=1}^{r}\prod_{j=1}^{s}(\tfrac{q_j}{p_i})^{\beta_j\alpha_i})(\prod_{j=1}^{s}\prod_{i=1}^{r}(\tfrac{p_i}{q_j})^{\beta_j\alpha_i}) \\
&= \prod_{i=1}^{r}\prod_{j=1}^{s}((\tfrac{q_j}{p_i})(\tfrac{p_i}{q_j}))^{\beta_j\alpha_i} \\
&= \prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{\alpha_i\frac{p_i-1}{2}.\beta_j\frac{q_j-1}{2}} \\
&= (-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}\alpha_i\frac{p_i-1}{2}.\beta_j\frac{q_j-1}{2}} \\
&= (-1)^{\sum_{i=1}^{r}\alpha_i\frac{p_i-1}{2}.\sum_{j=1}^{s}\beta_j\frac{q_j-1}{2}} \\
&= (-1)^{\frac{a-1}{2}.\frac{b-1}{2}},
\end{aligned}$$

што и требаше да се докаже. ■

3.8. Пример. Докажи дека не постојат цели броеви x, y такви што $x^2 = y^3 - 5$.

Решение. Ако y е парен број, тогаш $x^2 = y^3 - 5 \equiv 3 (\mathrm{mod}\, 8)$, што не е можно.

Нека y е непарен број. Ако $y \equiv 3 (\mathrm{mod}\, 4)$, тогаш $x^2 = y^3 - 5 \equiv 3^3 - 5 \equiv 2 (\mathrm{mod}\, 4)$ што повторно не е можно. Според тоа, $y = 4k+1, k \in \mathbb{Z}$. Тогаш со замена во $x^2 = y^3 - 5$ добиваме

$$x^2 + 4 = 64k^3 + 48k^2 + 12k = 4k(16k^2 + 12z + 3).$$

Според тоа,

$$x^2 \equiv -4 (\mathrm{mod}\, 16k^2 + 12z + 3).$$

Меѓутоа, вредноста на симболот на Јакоби

$$(\tfrac{-4}{16k^2+12z+3}) = (\tfrac{-1}{16k^2+12z+3})$$

е еднаква на -1 бидејќи $16k^2 + 12z + 3 \equiv 3 (\mathrm{mod}\, 4)$, што повторно е противречност. ■

3.9. Пример. Низата на Фибоначи е определена со $f_0 = 0,\ f_1 = 1$ и

$$f_{n+2} = f_{n+1} + f_n, \text{ за } n \geq 0.$$

Докажи:

а) ако p е прост број од видот $10k \pm 1$, тогаш $f_{p-1} \equiv 0 (\mathrm{mod}\, p)$.

б) ако p е прост број од видот $10k\pm 3$, тогаш $f_{p+1}\equiv 0(\mathrm{mod}\, p)$.

Решение. За Фибоначиевите броеви точна е таканаречената Бинетова формула (види [150], страна 154):

$$f_n=\frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^n-(\frac{1-\sqrt{5}}{2})^n],\ \text{за}\ n\geq 0. \qquad (2)$$

а) Од (2) имаме

$$f_{p-1}=\frac{1}{2^{p-2}}[\binom{p-1}{1}+\binom{p-1}{3}\cdot 5+\ldots+\binom{p-1}{p-2}\cdot 5^{\frac{p-3}{2}}].$$

За $0<k<p$ важи

$$\binom{p-1}{k-1}+\binom{p-1}{k}=\binom{p}{k}=\frac{p(p-1)\ldots(p-k+1)}{k!}\equiv 0(\mathrm{mod}\, p).$$

Според тоа,

$$\binom{p-1}{0}\equiv -\binom{p-1}{1}\equiv\binom{p-1}{2}\equiv -\binom{p-1}{3}\equiv\ldots\equiv\binom{p-1}{p-1}(\mathrm{mod}\, p),$$

па како $\binom{p-1}{0}=1$, добиваме

$$\binom{p-1}{1}\equiv\binom{p-1}{3}\equiv\ldots\equiv\binom{p-1}{p-2}\equiv -1(\mathrm{mod}\, p).$$

Затоа важи

$$2^{p-1}f_{p-1}\equiv -2(1+5+\ldots+5^{\frac{p-3}{2}})\equiv -\frac{5^{\frac{p-1}{2}}-1}{2}\equiv -\frac{1}{2}[(\frac{5}{p})-1](\mathrm{mod}\, p).$$

Бидејќи $(\frac{5}{p})=(\frac{p}{5})$, а квадратни остатоци по модул 5 се 1 и 4, добиваме дека $(\frac{5}{p})=1$ ако $p\equiv\pm 1(\mathrm{mod}10)$, додека $(\frac{5}{p})=-1$ ако $p\equiv\pm 3(\mathrm{mod}10)$. Оттука следува дека

$$f_{p-1}\equiv 0(\mathrm{mod}\, p)\ \text{за}\ p=10k\pm 1.$$

б) Од (2) имаме:

$$f_{p+1}=\frac{1}{2^p}[\binom{p+1}{1}+\binom{p+1}{3}\cdot 5+\ldots+\binom{p+1}{p}\cdot 5^{\frac{p-1}{2}}].$$

Од $\binom{p+1}{k}=\binom{p}{k}+\binom{p}{k-1}$ следува $\binom{p+1}{k}\equiv 0(\mathrm{mod}\, p)$ за $1<k<p$. Затоа важи

$$2^p f_{p+1}\equiv 1+5^{\frac{p-1}{2}}\equiv 1+(\frac{5}{p})\equiv 0(\mathrm{mod}\, p),$$

кога $p\equiv\pm 3(\mathrm{mod}10)$. ■

4. НЕКОИ ЗБИРОВИ НА СИМБОЛИТЕ НА ЛЕЖАНДР

4.1. Во некои случаи е потребно да се определи бројот на вредностите $x\in\{0,1,\ldots,p-1\}$ за кои $f(x)$ е квадратен остаток по модул p каде p е непарен

прост број, а $f(x)$ е полином со целобројни коефициенти. Одговорот на ова прашање е непосредно поврзан со вредноста на збирот

$$\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right).$$

Ако $f(x)$ е полином од прв степен, тогаш точна е следнава теорема

Теорема. За произволни цели броеви a,b и непарен прост број $p\nmid a$ важи

$$\sum_{x=0}^{p-1}\left(\frac{ax+b}{p}\right)=0.$$

Доказ. Бидејќи $p\nmid a$ броевите $ax+b$ за $x=0,1,2,...,p-1$ формираат комплетен систен на остатоци по модул p. Бидејќи меѓу нив има точно $\frac{p-1}{2}$ квадратни остатоци кои не се деливи со p, точно $\frac{p-1}{2}$ квадратни неостатоци и точно еден делив со p, следува дека

$$\sum_{x=0}^{p-1}\left(\frac{ax+b}{p}\right)=\frac{p-1}{2}+(-1)\frac{p-1}{2}+0=0. \blacksquare$$

4.2. Теорема. Нека $f(x)$ е полином со целобројни коефициенти, $\deg f=k$ и p е непарен прост број. Ставаме $p'=\frac{p-1}{2}$ и нека

$$f(x)^{p'}=a_0+a_1x+...+a_{kp'}x^{kp'}.$$

Тогаш

$$\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right)\equiv -(a_{p-1}+a_{2(p-1)}+...+a_{k'(p-1)})\pmod p, \text{ каде } k'=[\tfrac{k}{2}].$$

Доказ. Да означиме $S_n=\sum_{x=0}^{p-1}x^n, n\in\mathbb{N}$ и $S_0=p$. Според примерот IV 9.12 имаме $S_n\equiv -1(\mathrm{mod}\,p)$ за $n>0$, $p-1\mid n$ и $S_n\equiv 0(\mathrm{mod}\,p)$ во останатите случаи. Сега од критериумот на Ојлер следува

$$\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right)\equiv\sum_{x=0}^{p-1}f(x)^{p'}=\sum_{i=0}^{kp'}a_iS_i\equiv -(a_{p-1}+a_{2(p-1)}+...+a_{k'(p-1)})\pmod p. \blacksquare$$

4.3. Теорема. Нека a,b,c се цели броеви и p е непарен прост број кој не е делител на a. Тогаш

$$\sum_{x=0}^{p-1}\left(\frac{ax^2+bx+c}{p}\right)=\begin{cases}-\left(\frac{a}{p}\right), & p\nmid b^2-4ac,\\ (p-1)\left(\frac{a}{p}\right), & p\mid b^2-4ac.\end{cases} \tag{1}$$

Доказ. Имаме:

$$(\frac{4a}{p})\sum_{x=0}^{p-1}(\frac{ax^2+bx+c}{p})=\sum_{x=0}^{p-1}(\frac{(2ax+b)^2-D}{p}),$$

каде $D=b^2-4ac$. Бидејќи броевите $ax+b$ за $x=0,1,...,p-1$ формираат комплетен систем на остатоци по модул p, добиваме

$$\sum_{x=0}^{p-1}(\frac{ax^2+bx+c}{p})=(\frac{a}{p})\sum_{x=0}^{p-1}(\frac{x^2-D}{p})=S(\frac{a}{p}).$$

Од теоремата 4.2. следува $S\equiv -1(\mathrm{mod}\, p)$, па како $|S|\le p$ следува дека $S=-1$ или $S=p-1$. Ќе докажеме дека $S=p-1$ ако и само ако $p\mid D$. Нека претпоставиме дека $S=p-1$. Тогаш $p-1$ вредност на симболите на Лежандр $(\frac{x^2-D}{p})$ за $x=0,...,p-1$ се еднакви на 1, а еден, да кажеме за $x=x_0$ е еднаков на 0, т.е. $p\mid x_0^2-D$. Но, тогаш $p\mid(-x_0)^2-D=x_0^2-D$, па мора да е $x_0=0$, од каде ќе следува дека $p\mid D$. Обратно, ако $p\mid D$, тогаш од теоремата 1.6 следува

$$S=\sum_{x=0}^{p-1}(\frac{x^2-D}{p})=\sum_{x=0}^{p-1}(\frac{x^2}{p})=p-1.$$

Но, $S=-1$ или $S=p-1$, па од претходните разгледувања следува: ако $p\nmid D$, тогаш $S=-1$.

Конечно, од претходните разгледувања следува формулата (1). ■

4.4. Пример. Нека p е непарен прост број и k е цел број таков што $(k,p)=1$ Пресметај го збирот

$$\sum_{x=0}^{p-1}(\frac{x(x+k)}{p}).$$

Решение. Имаме,

$$\sum_{x=0}^{p-1}(\frac{x(x+k)}{p})=\sum_{x=0}^{p-1}(\frac{x^2+kx}{p}).$$

Сега, ако во теорема 4.3 земеме $a=1, b=k$ и $c=0$, добиваме $D=k^2$ и како $p\nmid D$ следува дека

$$\sum_{x=0}^{p-1}(\frac{x(x+k)}{p})=\sum_{x=0}^{p-1}(\frac{x^2+kx}{p})=-(\frac{1}{p})=-1.\ ■$$

VII ГЛАВА
ДИОФАНТОВИ АПРОКСИМАЦИИ

Теоријата на Диофантовите апроксимации е гранка од теоријата на броеви во која се проучуваат апроксимациите на реалните броеви со рационалните. Познато е дека секој реален број може произволно добро да се апроксимира со рационални броеви. Меѓутоа, ако при апроксимирањето се бара броевите со кои се врши апроксимацијата да задоволуваат некој дополнителен услов, на пример, на определен начин да им се ограничи именителот, тогаш бараната точност не може секогаш да се постигне.

Пред да ги разгледаме Диофантовите апроксимации ќе се задржиме на рационалните и ирационалните броеви, при што ќе разгледаме неколку критериуми за докажување дали еден реален број е рационален или е ирационален. Притоа ќе сметаме дека читателот е запознаен со конструкцијата на реалните броеви, која може да се реализира на повеќе начини, од кои еден може да се види во [85]. Во нашите разгледувања за множествата природни, цели, рационални и реални броеви ќе ги користиме стандардните ознаки $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ и $\mathbb{R}$, соодветно.

1. РАЦИОНАЛНИ И ИРАЦИОНАЛНИ БРОЕВИ

1.1. Секој рационален број α може да се запише во обликот

$$\alpha = \frac{p}{q},\ p \in \mathbb{Z}, q \in \mathbb{N}, (p,q) = 1. \tag{1}$$

Постоењето на ирационалните брови им било познато уште на античките математичари. На пример, се смета дека ирационалноста на бројот $\sqrt{2}$ ја докажал Питагора или некој од неговите ученици. Меѓутоа, утврдувањето дали некој реален број е рационален или ирационален секогаш не е едноставна задача. На пример, за добро познатата од математичката анализа Ојлерова константа C не се знае дали е рационален или е ирационален број. Сепак, за рационалните броеви се знае многу повеќе и постојат определени критериуми со кои може да се определи дали некој реален број е рационален. Во следната теорема ќе докажеме еден ваков критериум, при што ќе се задржиме на позитивните броеви бидејќи пренесувањето на резултатите на негативните броеви е едноставно. Да се потсетиме, секој позитивен реален број α на единствен начин меже да се претстави со децимален запис:

$$\alpha = a_0, a_1 a_2 \ldots a_n \ldots \tag{2}$$

каде a_0 е ненегативен цел број, $a_i \in \{0,1,2,3,4,5,6,7,8,9\}$ за $i \geq 1$ и не се сите a_n почнувајќи од некој n еднакви на 9. Последниот услов е потребен за да се обезбе-

ди единственоста на записот, бидејќи без овој услов некои броеви би имале два децимални записа. На пример, $2,129999\ldots = 2,13000\ldots$, $1,999\ldots = 2,000\ldots$ итн. Понатаму, меѓу децималните записи на реалните броеви постојат *периодични* записи, т.е. записи кај кои почнувајќи од некое место, група цифри периодично се повторува. Во врска со периодичните децимални записи ќе ја докажеме следнава теорема.

1.2. Теорема. Реалниот број α е рационален ако и само ако неговиот децимален запис (2) е периодичен.

Доказ. Нека $\alpha = \frac{p}{q}$, $p \in \mathbb{Z}, q \in \mathbb{N}, (p,q) = 1$ е произволен рационален број. При делење на целиот број p со природниот број q можни остатоци се $0,1,\ldots,q-1$. Ако при делењето на p со q се појави остаток 0, тогаш делењето завршува и α има *конечен децимален запис*, кој всушност е периодичен децимален запис со периода цифрата 0. Ако при делењето на p со q не се појавува остаток 0, тогаш по најмногу q чекори, ќе се повтори остатокот кој се добива (принцип на Дирихле: имаме q делења и $q-1$ можни остатоци). Тоа значи дека ќе имаме повторување на цифрите кои се наоѓаат меѓу првите две повторувања на остатокот кој прв се повторува и со оваа постапка ќе добиеме *бесконечен периодичен децимален број*.

Обратно, да разгледаме реален број кој има бесконечен периодичен децимален запис

$$\alpha = a_0, a_1 a_2 \ldots a_k (a_{k+1} a_{k+2} \ldots a_{k+s}), \tag{3}$$

каде со $(a_{k+1} a_{k+2} \ldots a_{k+s})$ е означена периодата која содржи најмалку цифри (со најмала должина) која за прв пат се јавува по цифрата a_k во децималниот запис на бројот α. Тогаш

$$\alpha(10^{k+s} - 10^k) = (10^s - 1)(10^k a_0 + \overline{a_1 a_2 \ldots a_k}) + \overline{a_{k+1} a_{k+2} \ldots a_{k+s}},$$

па затоа

$$\alpha = a_0 + \frac{\overline{a_1 a_2 \ldots a_k}}{10^k} + \frac{\overline{a_{k+1} a_{k+2} \ldots a_{k+s}}}{10^{k+s} - 10^k},$$

што значи дека α е рационален број. ■

1.3. Се поставуваат прашањата кога даден рационален број има конечен децимален запис, а кога има *чист периодичен децимален запис*, т.е. децимален запис во кој во (3) ја нема „*претпериодата*“ $a_1 a_2 \ldots a_k$, т.е. кога $k = 0$. Во врска со овие две прашања точни се следниве теореми.

Теорема А. Нека $\alpha = \frac{p}{q}$, $p \in \mathbb{Z}, q \in \mathbb{N}, (p,q) = 1$ е рационален број. Бројот α има конечен децимален запис ако и само ако $q = 2^a 5^b$, каде $a,b \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Доказ. Нека α има конечен децимален запис, т.е. $\frac{p}{q}=a_0,a_1a_2...a_k$. Според тоа, $\frac{p}{q}=\frac{10^n a_0+\overline{a_1a_2...a_k}}{10^n}$, од каде по евентуално кратење во дропката на десната страна на последното равенство добиваме дека $q=2^a5^b$ каде $a,b\in\mathbb{N}_0=\mathbb{N}\cup\{0\}$.

Обратно, нека $q=2^a5^b$ каде $a,b\in\mathbb{N}_0=\mathbb{N}\cup\{0\}$. Имаме, $\frac{p}{q}=\frac{p}{2^a5^b}$ и ако дропката ја проширime со 5^{a-b} или 2^{b-a} (во зависност од тоа дали $a\geq b$ или $a<b$) добиваме $\frac{p}{q}=\frac{r}{10^n}$ каде r и n се природни броеви. Нека

$$r=\overline{c_kc_{k-1}...c_1c_0}=10^kc_k+10^{k-1}c_{k-1}+...+10c_1+c_0$$

е декадниот запис на r. Тогаш

$$\frac{p}{q}=\frac{r}{10^n}=10^{k-n}c_k+10^{k-1-n}c_{k-1}+...+10^{1-n}c_1+10^{-n}c_0,$$

што значи дека $\frac{p}{q}$ во децимален запис се запишува со помош на истите цифри како и бројот r и, можда, определен број нули пред нив, во случај кога $k<n$. Според тоа, бројот $\frac{p}{q}$ има конечен децимален запис. ■

Теорема Б. Нека $\alpha=\frac{p}{q}$, $p\in\mathbb{Z}, q\in\mathbb{N}, (p,q)=1$ е рационален број. Бројот α има бесконечен чист периодичен децимален запис ако и само ако $(q,10)=1$. □

1.4. Теорема. Нека $P(x)=x^n+a_1x^{n-1}+...+a_{n-2}x^2+a_{n-1}x+a_n$ е полином со целобројни коефициенти и реалниот број α е корен на $P(x)$. Тогаш, или α е цел број или α е ирационален број.

Доказ. Бидејќи 0 е цел број, ќе го разгледуваме само случајот кога $\alpha\neq 0$. Нека претпоставиме дека α е рационален број, т.е. $\alpha=\frac{p}{q}$, $p\in\mathbb{Z}, q\in\mathbb{N}, (p,q)=1$. Заменуваме $\alpha=\frac{p}{q}$ во равенката $P(x)=0$ и последователно добиваме

$$\frac{p^n}{q^n}+a_1\frac{p^{n-1}}{q^{n-1}}+...+a_{n-2}\frac{p^2}{q^2}+a_{n-1}\frac{p}{q}+a_n=0,$$
$$p^n=-q(a_1p^{n-1}+...+a_{n-2}p^2q^{n-3}+a_{n-1}pq^{n-2}+a_nq^{n-1}).$$

Од последното равенство следува $q\mid p^n$ и како $(p,q)=1$ добиваме $q=1$, т.е. $\alpha=\frac{p}{q}=p$ е цел број. ■

1.5. Последица. Ако природниот број p не е $n-$ти степен на ниту еден приро-

ден број, тогаш $\sqrt[n]{p}$ е ирационален број.

Доказ. Следува од теоремата 1.4 применета на равенката $x^n - p = 0$. ■

1.6. Теорема. Ако $\alpha \in \mathbb{Q}$, тогаш постои реален број $c > 0$ таков што за секој рационален број $\frac{p}{q} \neq \alpha$ важи

$$|\alpha - \frac{p}{q}| \geq \frac{c}{q}.$$

Доказ. Нека $\alpha = \frac{a}{b}, b \geq 1$. Ако $\frac{p}{q}$ е произволен рационален број таков што $\frac{p}{q} \neq \frac{a}{b}$, тогаш $aq - bp \neq 0$, па затоа за целиот број $|aq - bp|$ важи $|aq - bp| \geq 1$. Сега, ако земеме $c = \frac{1}{b}$, добиваме

$$|\alpha - \frac{p}{q}| = |\frac{a}{b} - \frac{p}{q}| = \frac{|aq-bp|}{bq} \geq \frac{1}{bq} = \frac{c}{q},$$

што и требаше да се докаже. ■

1.7. Последица. Нека α е реален број. Ако за секој позитивен реален број c постои барем еден рационален број $\frac{p}{q} \neq \alpha$ таков што $|\alpha - \frac{p}{q}| < \frac{c}{q}$, тогаш α е ирационален број.

Доказ. Непосредно следува од теоремата 1.6. ■

1.8. Важни математички константи π и e се ирационални броеви. Ламберт прв докажал дека бројот π е ирационален. Во следниот пример ќе ја докажеме ирационалноста на бројот e.

Пример. Докажи дека бројот e е ирационален.

Решение. Од математичката анализа е познато дека

$$\frac{1}{e} = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!} + \ldots.$$

Нека претпоставиме дека $e = \frac{p}{q}$, $p, q \in \mathbb{N}, (p,q) = 1$. Од $e = \frac{p}{q}$ следува дека $\frac{1}{e} p!$ е цел број, па затоа и

$$A = p!(\frac{1}{e} - (1 - \frac{1}{1!} + \frac{1}{2!} - \ldots + (-1)^p \frac{1}{p!}))$$

е цел број. Меѓутоа, $A = p!(\frac{1}{(p+1)!} - \frac{1}{(p+2)!} + \ldots)$, па затоа

$$0 < A < p! \cdot \frac{1}{(p+1)!} = \frac{1}{p+1} < 1,$$

што е противречност. Конечно, од добиената противречност следува дека бројот e е ирационален. ■

2. ТЕОРЕМА НА ДИРИХЛЕ

2.1. Теорема (Дирихле). Нека $\alpha \in \mathbb{R}$ и $n \in \mathbb{N}$. Тогаш постои рационален број $\frac{p}{q}$ таков што важи

$$|\alpha - \tfrac{p}{q}| < \tfrac{1}{qn} \text{ и } 0 < q \le n \ .$$

Доказ. Без ограничување на општоста можеме да земеме дека $\alpha \in [0,1)$. Разгледуваме $n+1$ броеви $0, \{\alpha\}, \{2\alpha\}, ..., \{n\alpha\}$ од интервалот $[0,1)$. Овој интервал да го делиме на n интервали:

$$[0, \tfrac{1}{n}),\ [\tfrac{1}{n}, \tfrac{2}{n}),\ ...,\ [\tfrac{n-1}{n}, 1).$$

Од принцип на Дирихле следува дека барем еден од овие интервали содржи два од дадените броеви. Нека се тоа броевите $\{k\alpha\} = k\alpha - [k\alpha]$ и $\{m\alpha\} = m\alpha - [m\alpha]$ и нека, на пример, $m > k$. Значи,

$$\tfrac{1}{n} > |\{m\alpha\} - \{k\alpha\}| = |\alpha(m-k) - ([m\alpha] - [k\alpha])| .$$

Земаме $q = m - k$ и $p = [m\alpha] - [k\alpha]$. Јасно, $0 < q \le n$ и притоа важи

$$|\alpha q - p| < \tfrac{1}{n}, \text{ т.е. } |\alpha - \tfrac{p}{q}| < \tfrac{1}{qn} . \blacksquare$$

2.2. Последица. Ако α е ирационален број, тогаш неравенката

$$|\alpha - \tfrac{p}{q}| < \tfrac{1}{q^2} \tag{1}$$

има бесконечно многу решенија по $p \in \mathbb{Z}$ и $q \in \mathbb{N}$.

Доказ. Тврдењето на теоремата 2.1 важи и ако го додадеме условот $(p,q) = 1$, бидејќи условите за p и q ќе останат задоволени и ако поделиме со нивен заеднички делител. Значи, за $n > 1$ постојат заемно прости броеви $p \in \mathbb{Z}$ и $q \in \mathbb{N}$ такви што $|\alpha - \tfrac{p}{q}| < \tfrac{1}{nq} < \tfrac{1}{q^2}$. Бидејќи α е ирационален број, важи $\alpha q - p \neq 0$.

Нека претпоставиме дека постојат само конечномногу рационални броеви $\frac{p}{q}$ кои се решенија на (1) и нека тоа се броевите $\frac{p_i}{q_i}, i = 1,2,...,k$. Земаме природен број m таков што $\frac{1}{m} < |aq_i - p_i|$ за $i = 1,2,...,k$. Сега, ако во теоремата 2.1 земеме $n = m$, добиваме дека постои рационален број $\frac{p}{q}$ кој е решение на (1) и за кој важи $|aq - p| \le \frac{1}{m}$. Според тоа, $\frac{p}{q}$ е различен од $\frac{p_i}{q_i}, i = 1,2,...,k$, што е противречност. $\blacksquare$

2.3. Забелешка. Тврдењето на последицата 2.2 не е точно ако α е рационален број. Навистина, нека $\alpha=\frac{a}{b}$. Ако $\frac{p}{q}\neq\alpha$, тогаш

$$|\alpha-\frac{p}{q}|=|\frac{a}{b}-\frac{p}{q}|=|\frac{aq-bp}{bq}|\geq\frac{1}{bq},$$

па од (1) следува $q<b$. Според тоа, неравенката (1) може да биде задоволена само за конечно многу парови заемно прости броеви $p\in\mathbb{Q}$ и $q\in\mathbb{N}$.

3. НИЗИ НА ФАРЕЈ

3.1. Дефиниција. *Низа на Фарej* F_n *од ред* $n\in\mathbb{N}$ е монотоно растеча низа од нескратливи дропки $\frac{a}{b}$ во интервалот $[0,1]$ за кои $b\leq n$.

Така, низите на Фарej од ред 2, ред 3 и ред 5 се:

$$F_2:\frac{0}{1},\frac{1}{2},\frac{1}{1};\ F_3:\frac{0}{1},\frac{1}{3},\frac{1}{2},\frac{2}{3},\frac{1}{1}\ \text{и}\ F_5:\frac{0}{1},\frac{1}{5},\frac{1}{4},\frac{1}{3},\frac{2}{5},\frac{1}{2},\frac{3}{5},\frac{2}{3},\frac{3}{4},\frac{4}{5},\frac{1}{1}.$$

3.2. Лема. Бројот на членови на низа на Фарej F_n е еднаков на

$$1+\varphi(1)+\varphi(2)+...+\varphi(n),$$

каде φ е Ојлеровата функција.

Доказ. Ако $\frac{a}{b}$ е елемент од низата на Фарej, тогаш $(a,b)=1$ и за секој $b,1\leq b\leq n$, можните вредности на a за кои $\frac{a}{b}$ е елемент од низата на Фарej се точно $\varphi(b)$. Според тоа, вкупниот број членови на низата на Фарej е еднаков на $1+\varphi(1)+\varphi(2)+...+\varphi(n)$. ■

3.3. Теорема. Нека $\frac{a}{b}\in F_n$. Нека $y\in\mathbb{Z}$ е таков што $n-b<y\leq n$ и

$$ay\equiv-1(\mathrm{mod}\,b)$$

и нека $x=\frac{ay+1}{b}$. Тогаш $\frac{x}{y}$ е дропката која во F_n следува непосредно по $\frac{a}{b}$.

Доказ. Од $x=\frac{ay+1}{b}$ следува $bx-ay=1$ и $(x,y)=1$. Од $y\leq n$ следува $\frac{x}{y}\in F_n$ и $\frac{x}{y}=\frac{a}{b}+\frac{1}{by}>\frac{a}{b}$. Нека $\frac{c}{d}$ е дропка во F_n која непосредно следува по $\frac{a}{b}$ и нека претпоставиме дека $\frac{a}{b}<\frac{c}{d}<\frac{x}{y}$. Тогаш $xd-yc\geq1$, $cb-ad\geq1$ и

$$\frac{1}{by}=\frac{bx-ay}{by}=\frac{x}{y}-\frac{a}{b}=(\frac{x}{y}-\frac{c}{d})+(\frac{c}{d}-\frac{a}{b})=\frac{xd-cy}{yd}+\frac{cb-ad}{bd}\geq\frac{1}{dy}+\frac{1}{db}=\frac{b+y}{bdy},$$

па затоа бидејќи $\frac{c}{d}\in F_n$ добиваме $b+y\leq d\leq n$, односно $y\leq n-b$ што противре-

чи на изборот на бројот y. ■

3.4. Забелешка. Од својствата на линеарните конгруенции непосредно следува дека броевите x и y кои ги задоволуваат условите во теоремата 3.3 се еднозначно определени. На читателот, за вежба, му оставаме ова тврдење самостојно да го провери.

3.5. Последица. Ако $\frac{a}{b} < \frac{c}{d}$ се соседни дропки во F_n, тогаш

1) $b+d > n$,
2) $bc-ad=1$ и
3) $(b,d)=1$.

Доказ. Сите три тврдења непосредно следуваат од

$$n-b < d \le n,\ ad \equiv -1 (\mathrm{mod}\, b) \text{ и } c = \frac{ad+1}{b}.$$

Деталите ги оставаме на читателот за вежба. ■

3.6. Дефиниција. Нека $\frac{a}{b}$ и $\frac{c}{d}$ се нескратливи дропки. Дропката $\frac{a+c}{b+d}$ ја нарекуваме *медијанта* на дропките $\frac{a}{b}$ и $\frac{c}{d}$.

3.7. Последица. Ако $\frac{a}{b} < \frac{x}{y} < \frac{c}{d}$ се три последователни членови на F_n, тогаш $\frac{x}{y}$ е медијанта на $\frac{a}{b}$ и $\frac{c}{d}$.

Доказ. Од последица 3.5 следува $bx-ay=1$ и $cy-dx=1$. Ако ги одземеме овие равенства добиваме $x(b+d)-y(a+c)=0$, односно $\frac{x}{y} = \frac{a+c}{b+d}$, ■

3.8. Последица. Секоја дропка помала од 1 од F_{n+1} со именител $n+1$ се наоѓа меѓу две соседни дропки од F_n и е нивна медијанта.

Доказ. Непосредно следува од последицата 3.7. ■

3.9. Забелешка. Од претходните разгледувања следува дека, знаејќи ја низата на Фарej F_n, низата на Фарej од $(n+1)-$ви ред ја конструираме така што во F_n ги наоѓаме оние соседни дропки чиј збир на именители е $n+1$ и меѓу нив ја запишуваме нивната медијанта.

На пример, со овој алгоритам од низата $F_3 : \frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}$ ја добиваме низата $F_4 : \frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}$, а од низата $F_5 : \frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}$ ја добиваме низата $F_6 : \frac{0}{1}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{1}{1}$.

3.10. Со помош на низите на Фарej ќе дадеме друг доказ на теоремата 2.1.

Доказ. Повторно ќе претпоставиме дека $\alpha \in [0,1)$. Нека $\frac{p}{q}$ и $\frac{c}{d}$ се соседни членови на низата F_n и нека $\frac{p}{q} \le \alpha \le \frac{c}{d}$. Нека, на пример, $\frac{p}{q} \le \alpha \le \frac{p+c}{q+d}$. Тогаш

$$|\alpha - \frac{p}{q}| < \frac{p+c}{q+d} - \frac{p}{q} = \frac{qc-pd}{q(q+d)} < \frac{1}{qn},$$

бидејќи според последицата 3.5 важи $qc - pd = 1$ и $q + d > n$, а притоа $0 < q \le n$. ■

3.11. Дефиниција. За рационалниот број $\frac{a}{b}$ ќе велиме дека е *најдобра апроксимација* на реалниот број α, ако не постои рационален број $\frac{x}{y}$ за кој $y \le b$ и $|\alpha - \frac{x}{y}| \lhd |\alpha - \frac{a}{b}|$.

3.12. Теорема. Ако $\alpha \in \mathbb{R} \cap (0,1)$ се наоѓа меѓу два соседни члена во F_n, тогаш барем еден од нив е најдобра апроксимација за α.

Доказ. Нека $\frac{a}{b}$ и $\frac{c}{d}$ се два последователни членови на F_n и $\frac{a}{b} < \alpha < \frac{c}{d}$. Нека притоа важи $|\alpha - \frac{a}{b}| \trianglelefteq |\alpha - \frac{c}{d}|$. Ако постои $\frac{x}{y}$ таков што $|\alpha - \frac{x}{y}| \lhd |\alpha - \frac{a}{b}|$, тогаш $\frac{x}{y} \in (\frac{a}{b}, \frac{c}{d})$. Бидејќи $\frac{a}{b}$ и $\frac{c}{d}$ се последователни членови на F_n, дропката $\frac{x}{y}$ не припаѓа на F_n, па затоа мора да важи $y > n \ge b$, што значи дека $\frac{a}{b}$ е најдобра апроксимација за α. ■

3.13. Теорема. Нека $\frac{a}{b}$ и $\frac{c}{d}$ се два последователни членови на F_n и $\frac{a}{b} < \alpha < \frac{c}{d}$. Тогаш меѓу нескратливите дропки со именител $n+1$ најдобра апроксимација за α може да биде само медијантата $\frac{a+c}{b+d}$. Таа е најдобра апроксимација за α ако и само ако $b + d = n + 1$ и $|\frac{a+c}{b+d} - \alpha| \le \min\{|\frac{a}{b} - \alpha|, |\frac{c}{d} - \alpha|\}$.

Доказ. Според последицата 3.8, во множеството $F_n \cap (\frac{a}{b}, \frac{c}{d})$ може да се наоѓа само еден елемент од F_{n+1}, а тоа е медијантата $\frac{a+c}{b+d}$, и тоа само кога $b + d = n + 1$. Ако последниот услов е исполнет и ако важи $|\frac{a+c}{b+d} - \alpha| \le \min\{|\frac{a}{b} - \alpha|, |\frac{c}{d} - \alpha|\}$, тогаш $|\frac{a+c}{b+d} - \alpha| \trianglelefteq |\frac{x}{y} - \alpha|$ за секој $\frac{x}{y} \in F_{n+1}$.

Обратното тврдење е очигледно. ■

3.14. Следната теорема дава значително подобрување на последицата 2.2.

Теорема (Хурвиц). а) За секој ирационален број α неравенката

$$|\alpha-\frac{p}{q}|\leq\frac{1}{\sqrt{5}q^2} \tag{1}$$

има бесконечно многу решенија по $p\in\mathbb{Z}$ и $q\in\mathbb{N}$.

б) Константата во неравенството (1) не може да се подобри.

Доказ. а) Без ограничување на општоста можеме да претпоставиме дека $\alpha\in[0,1)$ (Зошто?). Нека претпоставиме дека тврдењето не е точно, т.е. дека неравенката (1) има конечно многу решенија и нека n е природен број кој е поголем од именителите на сите решенија $\frac{p}{q}$ на (1). Тоа значи не постојат p,q, $q>n$ такви што важи (1). Нека $\frac{a}{b}$ и $\frac{c}{d}$, ($\frac{a}{b}<\frac{c}{d}$) се соседни членови на низата F_m меѓу кои се наоѓа α. За доволно голем m ќе важи $b,d>n$. Од претпоставката следува дека

$$|\alpha-\frac{a}{b}|>\frac{1}{\sqrt{5}b^2}\ \text{ и }\ |\alpha-\frac{c}{d}|>\frac{1}{\sqrt{5}d^2},$$

па затоа

$$\frac{1}{bd}=\frac{bc-ad}{bd}=\frac{c}{d}-\frac{a}{b}=|\alpha-\frac{a}{b}|+|\frac{c}{d}-\alpha|>\frac{1}{\sqrt{5}b^2}+\frac{1}{\sqrt{5}d^2},$$

од каде следува

$$\frac{\sqrt{5}-1}{2}<\frac{d}{b}<\frac{\sqrt{5}+1}{2}. \tag{1}$$

Сега да ја разгледаме медијантата $\frac{a+c}{b+d}$ на $\frac{a}{b}$ и $\frac{c}{d}$. Без ограничување на општоста можеме да претпоставиме дека $\frac{a}{b}<\alpha<\frac{a+c}{b+d}$. Јасно, $b,b+d>n$. Од претпоставката следува $|\alpha-\frac{a}{b}|>\frac{1}{\sqrt{5}b^2}$, $|\alpha-\frac{a+c}{b+d}|>\frac{1}{\sqrt{5}(b+d)^2}$, па затоа

$$\frac{1}{b(b+d)}=\frac{b(a+c)-a(b+d)}{b(b+d)}=\frac{a+c}{b+d}-\frac{a}{b}=|\alpha-\frac{a}{b}|+|\frac{a+c}{b+d}-\alpha|>\frac{1}{\sqrt{5}b^2}+\frac{1}{\sqrt{5}(b+d)^2},$$

од каде следува $\frac{\sqrt{5}-1}{2}<\frac{b+d}{b}=1+\frac{d}{b}<\frac{\sqrt{5}+1}{2}$, што противречи на неравенствата (1).

Конечно, од добиената противречност следува точноста на тврдењето.

б) Нека $\varphi=\frac{\sqrt{5}-1}{2}$ и $\varepsilon>0$. Дропки $\frac{p}{q}>\varphi+\varepsilon$ за кои $|\varphi-\frac{p}{q}|\leq\frac{1}{(\sqrt{5}+\varepsilon)q^2}$ има само конечно многу, бидејќи тогаш $\varepsilon<\frac{1}{(\sqrt{5}+\varepsilon)q^2}$, т.е. $q^2<\frac{1}{\varepsilon(\sqrt{5}+\varepsilon)}$. Од друга страна, ако $\frac{p}{q}<\varphi+\varepsilon$, тогаш може да се докаже дека $|\varphi-\frac{p}{q}|>\frac{1}{(\sqrt{5}+\varepsilon)q^2}$.

Според тоа, за секој $\varepsilon>0$ неравенката $|\varphi-\frac{p}{q}|\leq\frac{1}{(\sqrt{5}+\varepsilon)q^2}$ има само конечно многу решенија по $p,q\in\mathbb{N}$, што значи дека константата $\sqrt{5}$ во тврдењето под а) не може да се подобри. ■

3.15. Како што видовме, во општ случај константата $\sqrt{5}$ од теоремата на Хур-

виц не може да се подобри, но може да се докаже дека за сите ирационални броеви α кои не се од облик $\frac{a+b\varphi}{c+d\varphi}$, $a,b,c,d\in\mathbb{Z}$, $|ad-bc|=1$, теоремата на Хурвиц е точна и ако $\sqrt{5}$ се замени со $\sqrt{8}$.

3.16. Пример. Нека $n\in\mathbb{N}$, $m=1+\sum_{i=1}^{n}\varphi(i)$ и $a_i, i=1,...,m$ се именителите на дропките на низата F_n. Докажи дека

$$\sum_{i=1}^{m-1}\frac{1}{a_i a_{i+1}}=1.$$

Решение. Нека

$$F_n:\frac{b_1}{a_1},\frac{b_2}{a_2},\frac{b_3}{a_3},...,\frac{b_{m-1}}{a_{m-1}},\frac{b_m}{a_m}.$$

Според последица 3 имаме $a_i b_{i+1}-b_i a_{i+1}=1$ за $i=0,1,...,m-1$, па затоа

$$\sum_{i=1}^{m-1}\frac{1}{a_i a_{i+1}}=\sum_{i=1}^{m-1}\frac{b_{i+1}a_i-a_{i+1}b_i}{a_i a_{i+1}}=\sum_{i=1}^{m-1}\left(\frac{b_{i+1}}{a_{i+1}}-\frac{b_i}{a_i}\right)=\frac{b_m}{a_m}-\frac{b_1}{a_1}=1-0=1.\ \blacksquare$$

3.17. Пример. Низата $\{a_n\}$ е зададена со $a_1=1$ и $a_{2n}=a_n$ и $a_{2n+1}=a_{n+1}+a_n$, за секој $n\in\mathbb{N}$. Нека m е природен број. Докажи дека бројот m во низата $\{a_{2k-1}\}_{k=1}^{\infty}$ се појавува точно $\varphi(m)$ пати.

Решение. Нека

$$S=\{\frac{k}{2^n}\mid k,n\in\mathbb{N}_0,k\le 2^n\}$$

и да го разгледаме пресликувањето $f:\mathbb{Q}\cap[0,1]\to S$ определено со

$$f(\tfrac{0}{1})=0,\ f(\tfrac{1}{1})=1 \text{ и } f(\tfrac{a+c}{b+d})=\tfrac{1}{2}(\tfrac{a}{b}+\tfrac{c}{d})$$

секогаш кога $\frac{a}{b}$ и $\frac{c}{d}$ се соседни членови на низа на Фарej од некој ред. Може да се докаже дека ова пресликување е биекција.

Со помош на индукција по n лесно се докажува дека ако $f(\frac{p}{q})=\frac{k}{2^r}$ за $k,r\in\mathbb{N}_0$ $(0\le p\le q,(p,q)=1)$, тогаш $a_{2^r+k}=q$. Навистина, ако $k=2l$, $l\in\mathbb{N}_0$, тогаш од $f(\frac{p}{q})=\frac{l}{2^{r-1}}$ заради индуктивната претпоставка имаме $a_{2^r+k}=a_{2^{r-1}+l}=q$. Од друга страна, ако $k=2l+1$, нека $\frac{a}{b}$ и $\frac{c}{d}$ се такви што $f(\frac{a}{b})=\frac{l}{2^{r-1}}$ и $f(\frac{c}{d})=\frac{l+1}{2^{r-1}}$. Тогаш по дефиниција $f(\frac{a+c}{b+d})=\frac{k}{2^r}$, па затоа $a+c=p$ и $b+d=q$, а тогаш според индуктивната претпоставка имаме

$$a_{2^r+k}=a_{2^{r-1}+l}+a_{2^{r-1}+l+1}=b+d=q.$$

Според тоа, $a_m = n$ за непарно m ако и само ако $m = 2^r + k$, при што $f(\frac{p}{n}) = \frac{k}{2^r}$. Сега тврдењето на задачата следува од фактот дека нескратливи дропки $\frac{p}{n}$ има $\varphi(n)$.

Пресликувањето f е познато и како функција на Минковски. ■

3.18. Пример. Определи ја дропка $\frac{p}{q}$, каде p и q се природни броеви помали од 100 и која е најблиску до $\frac{1}{\sqrt{2}}$

Решение. Имаме, $\frac{41}{29} < \sqrt{2} < \frac{99}{70}$. Ако $\frac{q}{p}$ е дропка за која важи $\frac{41}{29} < \frac{q}{p} < \frac{99}{70}$, тогаш $\frac{70}{99} < \frac{p}{q} < \frac{29}{41}$. Сега, бидејќи $99 \cdot 29 - 41 \cdot 70 = 1$, заклучуваме дека дропките $\frac{29}{41}$ и $\frac{70}{99}$ се соседни членови во низата F_{99}. Според тоа, барем една од дропките $\frac{29}{41}$ и $\frac{70}{99}$ е најдобра апроксимација за бројот $\frac{1}{\sqrt{2}}$. Со непосредна проверка се добива дека бараната дропка е $\frac{70}{99}$. ■

4. ПОИМ ЗА ВЕРИЖНА ДРОПКА

4.1. Дефиниција. Изразот од облик

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \ldots}}} = \left\langle a_0; \frac{b_1}{a_1}, \frac{b_2}{a_2}, \frac{b_3}{a_3}, \ldots \right\rangle \tag{1}$$

го нарекуваме *верижна* или *непрекината дропка*.

За верижната дропка (1) често пати се користи и записот

$$a_0 + \frac{b_1|}{|a_1} + \frac{b_2|}{|a_2} + \frac{b_3|}{|a_3} + \ldots \tag{2}$$

4.2. Коментар. Во општ случај елементите на верижната дропка a_0, a_i, b_i, $(i = 1,2,\ldots)$ можат да бидат реални и комплексни броеви, функции од една или повеќе променливи, елементи од апстрактни простори во кои се дефинирани операциите собирање и делење и слично. Дропките

$$a_0 = \frac{a_0}{1}, \frac{b_i}{a_i}, (i = 1,2,3,\ldots)$$

ги нарекуваме *делови* на верижната дропка (1), соодветно нулти или слободен член, прв, втор, итн. член, а елементите a_i и b_i $(i \geq 1)$ членови на $i-$тиот дел, ги

нарекуваме соодветно *делумен именител* и *делумен броител*. Во натамошните разгледувања ќе претпостауваме дека $a_i \neq 0$ и дека $\frac{b_i}{a_i}$ не може да се скрати.

4.3. Дефиниција. Ако верижната дропка (1) содржи конечен број на дропки (на пример n, не сметајќи го нултиот), тогаш истата ја нарекуваме *конечна* или *n-делна верижна дропка* и скратено ја означуваме со

$$\left\langle a_0; \frac{b_1}{a_1}, \frac{b_2}{a_2}, ..., \frac{b_n}{a_n} \right\rangle = \left\langle a_0; \frac{b_i}{a_i} \right\rangle_{i=1}^{n} \tag{3}$$

Верижната дропка (1), која има бесконечно делови ја нарекуваме *бесконечна верижна дропка* и притоа ја користиме ознаката

$$\left\langle a_0; \frac{b_i}{a_i} \right\rangle_{i=1}^{\infty} \tag{4}$$

Верижната дропка во која сите делумни броители се еднакви на 1 ја нарекуваме *обична* или *стандардна* верижна дропка.

За обичните верижни дропки ја користиме ознаката

$$\langle a_0; a_1, a_2, a_3, ... \rangle = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + ...}}} \tag{5}$$

4.4. Теорема. а) Секоја конечна верижна дропка со рационални броителии именители a_0, a_i, b_i, $i = 1,2,...,n$ е рационален број.

б) Секој рационален број можеме на единствен начин да го претставиме како конечна стандардна верижна дропка таква што $a_0 \in \mathbb{Z}$ и $a_i \in \mathbb{N}, i = 1,2,...,n$, при што $a_n > 1$.

Доказ. а) Доволно е да ги извршиме назначените операции во конечната верижна дропка (3).

б) Нека $\frac{u_0}{u_1}$ е рационален број таков што $(u_0, u_1) = 1$ и $u_1 > 0$. Да го примениме Евклидовиот алгоритам. Имаме

$$\begin{aligned}
&u_0 = u_1 a_0 + u_2, && 0 < u_2 < u_1 \\
&u_1 = u_2 a_1 + u_3, && 0 < u_3 < u_2 \\
&u_2 = u_3 a_2 + u_4, && 0 < u_4 < u_3 \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&u_{n-1} = u_n a_{n-1} + u_{n+1}, && 0 < u_{n+1} < u_n \\
&u_n = u_{n+1} a_n.
\end{aligned} \tag{6}$$

Ако за секој $i = 1,2,...,n$ ставиме $\alpha_i = \frac{u_i}{u_{i+1}}$, тогаш равенствата (6) го добиваат обликот

$$\alpha_i = a_i + \frac{1}{\alpha_{i+1}}, \ 0 \leq i \leq n-1 \text{ и } \alpha_n = a_n.$$

Но, тоа значи

$$\alpha_0 = a_0 + \frac{1}{\alpha_1} = a_0 + \frac{1}{a_1 + \frac{1}{\alpha_2}}.$$

Со последователна елиминација на $\alpha_2, \alpha_3, \ldots, \alpha_n$ добиваме

$$\frac{u_0}{u_1} = \alpha_0 = \langle a_0; a_1, a_2, a_3, \ldots, a_n \rangle.$$

Јасно, заради Евклидовиот алгоритам претставувањето е единствено. ■

4.5. Забелешка. Во теоремата 4.4 условот $a_n > 1$ е суштински. Навистина, ако го испуштиме овој услов, тогаш на пример за бројот $\frac{26}{11}$ ги имаме следниве две претставувања

$$\frac{26}{11} = 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{3}}} = 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1}}}}.$$

5. ПАРЦИЈАЛНИ КОЛИЧНИЦИ

5.1. Дефиниција. Нека е дадена верижната дропка

$$\left\langle a_0; \frac{b_1}{a_1}, \frac{b_2}{a_2}, \frac{b_3}{a_3}, \ldots \right\rangle. \tag{1}$$

Конечната дропка

$$\frac{P_k}{Q_k} = \left\langle a_0; \frac{b_1}{a_1}, \frac{b_2}{a_2}, \ldots, \frac{b_k}{a_k} \right\rangle, \ k = 1, 2, \ldots \tag{2}$$

ја нарекуваме $k-$*ти парцијален количник* на верижната дропка (1).

Да забележиме дека при конечна верижна дропка

$$\left\langle a_0; \frac{b_1}{a_1}, \frac{b_2}{a_2}, \ldots, \frac{b_n}{a_n} \right\rangle = \left\langle a_0; \frac{b_i}{a_i} \right\rangle_{i=1}^{n} \tag{3}$$

имаме $k \le n$. Во натамошните разгледувања ќе ги користиме Ојлеровите ознаки

$$P_{-1} = 1, Q_{-1} = 0, P_0 = a_0 \text{ и } Q_0 = 1.$$

5.2. Теорема. Броевите P_k, Q_k, $k = 1, 2, 3, \ldots$ определени со

$$P_k = a_k P_{k-1} + b_k P_{k-2} \tag{4}$$

$$Q_k = a_k Q_{k-1} + b_k Q_{k-2} \tag{5}$$

каде

$$P_{-1} = 1, \ Q_{-1} = 0, P_0 = a_0 \text{ и } Q_0 = 1,$$

се соодветно броителот и именителот на парцијалниот количник $\frac{P_k}{Q_k}$ на верижната дропка (1).

Доказ. Нека R_k, $k=1,2,...$ е низата од парцијални количници на верижната дропка (1). Треба да докажеме дека $R_k=\frac{P_k}{Q_k}$, $k=1,2,....$

За $k=1$ имаме $R_1=a_0+\frac{b_1}{a_1}=\frac{a_0a_1+b_1}{a_1}$. Од друга страна, од (4) и (5) имаме $P_1=a_0a_1+b_1$ и $Q_1=1\cdot a_1+b_1\cdot 0=a_1$. Значи, $R_1=\frac{P_1}{Q_1}$, односно за $k=1$ тврдењето е точно.

Нека сега претпоставиме дека теоремата е точна за сите природни броеви помали или еднакви на *k*. Од релациите на (4) и (5) имаме

$$P_{k+1}=a_{k+1}P_k+b_{k+1}P_{k-1}$$
$$Q_{k+1}=a_{k+1}Q_k+b_{k+1}Q_{k-1}.$$

Согласно со индуктивната претпоставка имаме

$$R_k=\frac{P_k}{Q_k}=\frac{a_kP_{k-1}+b_kP_{k-2}}{a_kQ_{k-1}+b_kQ_{k-2}}.$$

Од дефиницијата на верижната дропка (1) парцијалниот количник R_{k+1} се добива од парцијалниот количник R_k ако членот a_k се замени со сумата $a_k+\frac{a_{k+1}}{b_{k+1}}$. Затоа,

$$R_{k+1}=\frac{(a_k+\frac{b_{k+1}}{a_{k+1}})P_{k-1}+b_kP_{k-2}}{(a_k+\frac{b_{k+1}}{a_{k+1}})Q_{k-1}+b_kQ_{k-2}}=\frac{a_{k+1}(a_kP_{k-1}+b_kP_{k-2})+b_{k+1}P_{k-1}}{a_{k+1}(a_kQ_{k-1}+b_kQ_{k-2})+b_{k+1}Q_{k-1}}=\frac{a_{k+1}P_k+b_{k+1}P_{k-1}}{a_{k+1}Q_k+b_{k+1}Q_{k-1}}=\frac{P_{k+1}}{Q_{k+1}}.$$

Конечно, тврдењето следува од принципот на математичка индукција. ■

5.3. Последица. а) За обичната дропка $\langle a_0;a_1,a_2,...\rangle$ броителот и именителот на парцијалниот количник $\frac{p_k}{q_k}$, $k=1,2,...$ можеме да ги определиме од релациите

$$p_k=a_kp_{k-1}+p_{k-2} \tag{6}$$
$$q_k=a_kq_{k-1}+q_{k-2} \tag{7}$$

Каде $p_0=a_0$, $p_{-1}=1$, $q_0=1$ и $q_{-1}=0$.

б) Ако $\langle a_0;a_1,a_2,...,a_n\rangle=\frac{p_n}{q_n}$, тогаш $\langle a_n;a_{n-1},a_{n-2},...,a_0\rangle=\frac{p_n}{p_{n-1}}$.

Доказ. а) Кај обичните верижни дропки важи $b_k=1$, $k=1,2,...$. Сега точноста на тврдењето следува ако замениме во (4) и (5).

б) За $n=0$ тврдењето е тривијално. Нека претпоставиме дека за $n-1$ важи

$$\langle a_{n-1};a_{n-2},a_{n-3},...,a_0\rangle=\frac{p_{n-1}}{p_{n-2}}.$$

Тогаш од индуктивната претпоставка и од тврдењето под а) следува

$$\langle a_n;a_{n-1},a_{n-2},...,a_0\rangle=a_n+\frac{1}{\langle a_{n-1};a_{n-2},...,a_0\rangle}=a_n+\frac{p_{n-2}}{p_{n-1}}=\frac{a_np_{n-1}+p_{n-2}}{p_{n-1}}=\frac{p_n}{p_{n-1}}.$$

Конечно, точноста на тврдењето следува од принципот на математичка индукција. ■

5.4. Теорема. За два соседни парцијални количници $\frac{P_{k-1}}{Q_{k-1}}$ и $\frac{P_k}{Q_k}$ на верижната дропка (1) важи релацијата

$$\frac{P_k}{Q_k}-\frac{P_{k-1}}{Q_{k-1}}=(-1)^{k-1}\frac{b_1b_2..b_k}{Q_kQ_{k-1}},\ k\geq 1. \tag{8}$$

Доказ. Имаме

$$\frac{P_k}{Q_k}-\frac{P_{k-1}}{Q_{k-1}}=\frac{\Delta_k}{Q_kQ_{k-1}}, \tag{9}$$

каде $\Delta_k=\begin{vmatrix}P_k & P_{k-1}\\ Q_k & Q_{k-1}\end{vmatrix}$. Ако ги искористиме релациите (4) и (5) добиваме

$$\Delta_k=\begin{vmatrix}a_kP_{k-1}+b_kP_{k-2} & P_{k-1}\\ a_kQ_{k-1}+b_kQ_{k-2} & Q_{k-1}\end{vmatrix}=-b_k\Delta_{k-1}. \tag{10}$$

Со последователна примена на релацијата (10) добиваме

$$\Delta_k=(-1)^kb_1b_2...b_k\Delta_0$$

каде

$$\Delta_0=\begin{vmatrix}P_0 & P_{-1}\\ Q_0 & Q_{-1}\end{vmatrix}=\begin{vmatrix}a_0 & 1\\ 1 & 0\end{vmatrix}=-1.$$

Според тоа, $\Delta_k=(-1)^{k-1}b_1b_2...b_k$ и со замена во (9) ја добиваме релацијата (8). ■

5.5. Последица. Ако $\frac{P_{k-1}}{Q_{k-1}}$ и $\frac{P_k}{Q_k}$, $k\geq 1$ се два соседни парцијални количници на верижната дропка (1), тогаш

$$P_kQ_{k-1}-P_{k-1}Q_k=(-1)^{k-1}b_1b_2...b_k.$$

Доказ. Следува од доказот на теоремата 5.4. ■

5.6. Последица. Ако $\frac{p_{k-1}}{q_{k-1}}$ и $\frac{p_k}{q_k}$, $k\geq 1$ се два соседни парцијални количници на обичната верижна дропка $\langle a_0;a_1,a_2,...\rangle$, тогаш

$$\frac{p_k}{q_k}-\frac{p_{k-1}}{q_{k-1}}=\frac{(-1)^{k-1}}{q_kq_{k-1}}\ \text{ и }\ p_kq_{k-1}-p_{k-1}q_k=(-1)^{k-1}.$$

Доказ. Следува од теоремата 5.4 и последицата 5.5 за $b_1=b_2=...=b_k=1$. ■

5.7. Последица. За два соседно парцијални количници $\frac{P_{k-2}}{Q_{k-2}}$ и $\frac{P_k}{Q_k}$, $k\geq 2$ со иста парност на верижната дропка (1) важи

$$\frac{P_k}{Q_k}-\frac{P_{k-2}}{Q_{k-2}}=(-1)^k\frac{b_1b_2..b_{k-1}a_k}{Q_kQ_{k-2}}. \tag{11}$$

Доказ. Имаме

$$\frac{P_k}{Q_k}-\frac{P_{k-2}}{Q_{k-2}}=\frac{D_k}{Q_kQ_{k-2}}, \tag{12}$$

каде $D_k = \begin{vmatrix} P_k & P_{k-2} \\ Q_k & Q_{k-2} \end{vmatrix}$. Ако се искористат релациите (4) и (5) добиваме

$$D_k = \begin{vmatrix} a_k P_{k-1} + b_k P_{k-2} & P_{k-2} \\ a_k Q_{k-1} + b_k Q_{k-2} & Q_{k-2} \end{vmatrix} = a_k \Delta_{k-1} ,$$

каде Δ_{k-1} е детерминантата од теоремата 5.4. Значи, $\Delta_{k-1} = (-1)^k b_1 b_2 ... b_{k-1}$, па затоа $D_k = (-1)^k b_1 b_2 ... b_{k-1} a_k$ и ако замениме во (12) ја добиваме релацијата (11). ■

5.8. Последица. Ако $\frac{p_{k-2}}{q_{k-2}}$ и $\frac{p_k}{q_k}$, $k \geq 2$ се два соседни парцијални количници со иста парност на обичната верижна дропка $\langle a_0; a_1, a_2, ... \rangle$, тогаш

$$\frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = (-1)^k \frac{a_k}{q_k q_{k-2}}. \tag{13}$$

Доказ. Следува од последицата 5.7 за $b_1 = b_2 = ... = b_k = 1$. ■

5.9. Теорема. Ако сите елементи на конечната верижна дропка се позитивни, тогаш нејзините парцијални количници со парен индекс формираат монотоно растечка низа, а парцијалните количници со непарен индекс формираат монотоно опаѓачка низа. Притоа секој парцијален количник со парен индекс е помал од секој парцијален количник со непарен индекс, а бројот α, вредноста на конечната верижна дропка, лежи меѓу два соседни парцијални количници.

Доказ. Нека е дадена верижната дропка

$$\alpha = \left\langle a_0; \frac{b_1}{a_1}, \frac{b_2}{a_2}, ..., \frac{b_n}{a_n} \right\rangle \tag{14}$$

со позитивни елементи a_k и b_k и нека $\frac{P_k}{Q_k}$, $k = 0,1,2,\ldots n$, се нејзините последователни парцијални количници. Јасно $P_k > 0$ и $Q_k > 0$.

Ако $k = 2m$, тогаш од (11) следува $\frac{P_{2m}}{Q_{2m}} - \frac{P_{2m-2}}{Q_{2m-2}} > 0$, односно $\frac{P_{2m}}{Q_{2m}} > \frac{P_{2m-2}}{Q_{2m-2}}$, за $m = 1,2,3,...$. Значи, $\frac{P_0}{Q_0} < \frac{P_2}{Q_2} < \frac{P_4}{Q_4} < ...$.

Ако пак $k = 2m+1$, тогаш од (11) следува $\frac{P_{2m-1}}{Q_{2m-1}} > \frac{P_{2m+1}}{Q_{2m+1}}$, за $m = 1,2,3,...$.

Според тоа, $\frac{P_1}{Q_1} > \frac{P_3}{Q_3} > \frac{P_5}{Q_5} > ...$.

Понатаму, ако во релацијата (8) земеме $k = 2m$ добиваме $\frac{P_{2m}}{Q_{2m}} < \frac{P_{2m-1}}{Q_{2m-1}}$. Нека $s \leq m$. Тогаш $\frac{P_{2m}}{Q_{2m}} < \frac{P_{2m-1}}{Q_{2m-1}} \leq \frac{P_{2s-1}}{Q_{2s-1}}$. Ако пак $s > m$, тогаш $\frac{P_{2m}}{Q_{2m}} < \frac{P_{2s}}{Q_{2s}} < \frac{P_{2s-1}}{Q_{2s-1}}$. Значи, за секои s и m имаме $\frac{P_{2m}}{Q_{2m}} < \frac{P_{2s-1}}{Q_{2s-1}}$, односно секој парцијален количник со непарен индекс е поголем од секој парцијален количник со парен индекс.

На крајот, од дефиницијата на верижна дропка (14) очигледни се неравенствата: $\alpha > \frac{P_0}{Q_0}$, $\alpha < \frac{P_1}{Q_1}$, $\alpha > \frac{P_2}{Q_2}$ итн. Значи, ако k е парен број, тогаш $\frac{P_k}{Q_k} < \alpha < \frac{P_{k+1}}{Q_{k+1}}$ и ако k е непарен број, тогаш $\frac{P_k}{Q_k} > \alpha > \frac{P_{k+1}}{Q_{k+1}}$. Очигледно, за последниот парцијален количник наместо строги неравенства на десната страна во последните неравенства важи знак за равенство. ■

5.10. Последица. Ако елементите на верижната дропка (1) се позитивни и $\frac{P_k}{Q_k}$ се нејзините парцијални количници, тогаш точна е оценката

$$|\alpha - \frac{P_k}{Q_k}| \leq \frac{b_1 b_2 .. b_{k+1}}{Q_k Q_{k+1}} \tag{15}$$

Доказ. Од теоремите 5.9 и 5.4 следува

$$|\alpha - \frac{P_k}{Q_k}| \leq |\frac{P_{k+1}}{Q_{k+1}} - \frac{P_k}{Q_k}| = \frac{b_1 b_2 .. b_{k+1}}{Q_k Q_{k+1}} . \blacksquare$$

5.11. Последица. Ако елементите на обичната верижна дропка $\langle a_0; a_1, a_2, ... \rangle$ се позитивни и $\frac{p_k}{q_k}$ се нејзини парцијални количници, тогаш точна е оценката

$$|\alpha - \frac{p_k}{q_k}| \leq \frac{1}{q_k q_{k+1}} .$$

Доказ. За обичните верижни дропки имаме $b_k = 1, k = 1, 2, ...$, па сега точноста на оценката следува од последицата 5.10. ■

5.12. Пример За обичната верижна дропка $\langle 2; 1, 2, 1, 2, 2, 3 \rangle$ парцијалните количници се:

$$\frac{p_0}{q_0} = \frac{2}{1}, \ \frac{p_1}{q_1} = \frac{3}{1}, \ \frac{p_2}{q_2} = \frac{8}{3}, \ \frac{p_3}{q_3} = \frac{11}{4}, \ \frac{p_4}{q_4} = \frac{30}{11}, \text{ и } \frac{p_6}{q_6} = \frac{243}{89} .$$

Последниот парцијален количник е вредноста на конечната обична верижна дропка, односно $\langle 2; 1, 2, 1, 2, 2, 3 \rangle = \frac{243}{89}$. ■

5.13. Пример. За конечната верижна дропка $\langle 0; \frac{1}{2}, \frac{3}{4}, \frac{5}{8}, \frac{7}{16} \rangle$ парцијалните количници се:

$$\frac{P_0}{Q_0} = \frac{0}{1}, \ \frac{P_1}{Q_1} = \frac{1}{2}, \ \frac{P_2}{Q_2} = \frac{4}{11}, \ \frac{P_3}{Q_3} = \frac{37}{98} \text{ и } \frac{P_4}{Q_4} = \frac{620}{1645} .$$

Последниот парцијален количник е еднаков на конечната верижна дропка, односно $\langle 0; \frac{1}{2}, \frac{3}{4}, \frac{5}{8}, \frac{7}{16} \rangle = \frac{620}{1645}$. ■

6. БЕСКОНЕЧНИ ВЕРИЖНИ ДРОПКИ

6.1. Нека е дадена бесконечната верижна дропка

$$\left\langle a_0; \frac{b_1}{a_1}, \frac{b_2}{a_2}, ..., \frac{b_n}{a_n}, ... \right\rangle \tag{1}$$

и низата парцијални количници

$$\left\langle a_0; \frac{b_1}{a_1}, \frac{b_2}{a_2}, ..., \frac{b_n}{a_n} \right\rangle = \frac{P_n}{Q_n},\ n = 1, 2, 3, ... \tag{2}$$

Дефиниција. За бесконечната верижна дропка (1) ќе велиме дека е *конвергентна*, ако постои конечна граница

$$\lim_{n\to\infty} \frac{P_n}{Q_n} = \alpha \tag{3}$$

и притоа за бројот α ќе велиме дека е *вредност* на верижната дропка (1). Ако пак границата (3) не постои, тогаш верижната дропка (1) ја нарекуваме *дивергентна* и на неа не и придружуваме бројна вредност.

6.2. Пример. Определи ги сите низи $R_n = \frac{P_n}{Q_n},\ n = 1, 2, ...$ кои се парцијални количници на некоја верижна дропка.

Решение. Прво да претпоставиме дека $R_{k-1} \neq R_{k-2}$ за секој $k \geq 2$. Тоа значи дека

$$\begin{vmatrix} P_{k-1} & P_{k-2} \\ Q_{k-1} & Q_{k-2} \end{vmatrix} \neq 0, \tag{4}$$

за секој $k \geq 2$. За $k = 1$ неравенството (4) е исто така точно. Затоа системот равенки

$$\begin{cases} P_k = a_k P_{k-1} + b_k P_{k-2} \\ Q_k = a_k Q_{k-1} + b_k P_{k-2} \end{cases}$$

има единствено решение по a_k и b_k. Според тоа, $R_n = \frac{P_n}{Q_n}$ се парцијални количници на верижната дропка $\left\langle a_0; \frac{b_1}{a_1}, \frac{b_2}{a_2}, ... \right\rangle$, каде $a_0 = R_1 - \frac{b_1}{a_1}$.

Сега да претпоставиме дека *k* е најмалиот број поголем од 2 таков што $R_{k-1} = R_{k-2}$. Тоа значи дека

$$\begin{vmatrix} P_{k-1} & P_{k-2} \\ Q_{k-1} & Q_{k-2} \end{vmatrix} = 0$$

т.е. $R_k = R_{k-1}$. Продолжувајќи ја постапката добиваме

$$R_{k-2} = R_{k-1} = R_k = R_{k+1} = ...$$

Јасно, во случајов низата $\{R_n\}$ е низа од парцијални количници за некоја верижна дропка.

Ако ги земеме предвид претходните дискусии, добиваме дека бараните низи $\{R_n\}$ се низите кои го имаат следново својство: ако $R_n = R_{n+1}$, за некој n, тогаш $R_n = R_{n+k}$, за $k \geq 1$. ■

6.3. Пример. Определи верижна дропка која конвергира кон бројот e.

Решение. Бројот e е гранична вредност на низата $\frac{(n+1)^n}{n^n}$. Затоа нека $a_0 = 1$ и да ставиме

$$P_{-1} = 1 \qquad Q_{-1} = 0$$
$$P_0 = 1 \qquad Q_0 = 1$$
$$P_k = (k+1)^k \qquad Q_k = k^k$$

за $k \geq 1$. Лесно се проверува дека $\frac{P_k}{Q_k} \neq \frac{P_{k+1}}{Q_{k+1}}$ за $k \geq 0$. Затоа според примерот 6.2 постои верижна дропка $\left\langle a_0; \frac{b_1}{a_1}, \frac{b_2}{a_2}, \ldots \right\rangle$ чии парцијални количници се $\frac{P_n}{Q_n} = (1+\frac{1}{n})^n$ и кои конвергираат кон бројот e. Притоа $a_0 = 1$, а за $k \geq 1$ членовите a_k и b_k се решенија на системот

$$\begin{cases} P_k = a_k P_{k-1} + b_k P_{k-2} \\ Q_k = a_k Q_{k-1} + b_k Q_{k-2}. \end{cases}$$

Согласно со Кошиевиот критериум низата $\frac{P_n}{Q_n}, n = 1,2,3,\ldots$ конвергира ако и само ако за секој $\varepsilon > 0$ постои $n_0 = n_0(\varepsilon)$ таков што

$$\left| \frac{P_{n+m}}{Q_{n+m}} - \frac{P_n}{Q_n} \right| < \varepsilon, \text{ за } n > n_0(\varepsilon) \text{ и } m > 0.$$

Ако $Q_k \neq 0$, тогаш очигледно имаме

$$\frac{P_n}{Q_n} = \frac{P_0}{Q_0} + \sum_{k=1}^{n} \left(\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} \right) = \frac{P_0}{Q_0} + \sum_{k=1}^{n} (-1)^{k-1} \frac{b_1 b_2 .. b_{k+1}}{Q_k Q_{k-1}}$$

односно

$$\lim_{n \to \infty} \frac{P_n}{Q_n} = \frac{P_0}{Q_0} + \sum_{k=1}^{\infty} (-1)^{k-1} \frac{b_1 b_2 .. b_{k+1}}{Q_k Q_{k-1}} \tag{5}$$

т.е. редот (5) конвергира ако и само ако конвергира верижната дропка (1). Притоа ако верижната дропка (1) конвергира, тогаш од (5) непосредно следува оценката

$$\left| e - \frac{P_n}{Q_n} \right| \leq \sum_{k=n+1}^{\infty} \left| \frac{b_1 b_2 .. b_{k+1}}{Q_k Q_{k-1}} \right| . \blacksquare$$

6.4. Теорема. Ако сите елементи $a_0, a_k, b_k, k = 1,2,\ldots$ на верижната дропка (1) се позитивни, при што

$$b_k \leq a_k, \; a_k \geq d > 0, \; k = 1,2,3,\ldots \tag{6}$$

тогаш верижната дропка (1) е конвергентна.

Доказ. При доказот на првиот дел на теоремата 5.9 не користевме дека верижната дропка е конечна. Затоа, повторувајќи го овој доказ констатираме дека ако елементите на верижната дропка (1) се позитивни, тогаш нејзините парни парцијални количници $\frac{P_{2k}}{Q_{2k}}$, $k=1,2,...$ формираат монотоно растечка низа ограничена од горе. Според тоа, постои $\lim\limits_{k\to\infty}\frac{P_{2k}}{Q_{2k}}=\alpha$. Аналогно, непарните парцијални количници $\frac{P_{2k+1}}{Q_{2k+1}}$, $k=1,2,...$ на верижната дропка (1) формираат монотоно опаѓачка низа ограничена од долу. Затоа постои $\lim\limits_{k\to\infty}\frac{P_{2k+1}}{Q_{2k+1}}=\beta$, при што $\beta\geq\alpha$. Освен тоа, за секој $k\geq 0$ имаме $\frac{P_{2k}}{Q_{2k}}<\alpha\leq\beta<\frac{P_{2k+1}}{Q_{2k+1}}$.

Според теоремата 5.4 имаме

$$0\leq\beta-\alpha<\frac{P_{2k+1}}{Q_{2k+1}}-\frac{P_{2k}}{Q_{2k}}=\frac{b_1b_2..b_{2k+1}}{Q_{2k}Q_{2k+1}}=\xi_k. \tag{7}$$

Ќе докажеме дека $\xi_k\to 0$ кога $k\to\infty$. Имаме

$$Q_k=a_kQ_{k-1}+b_kQ_{k-2} \text{ и } Q_{k-1}=a_{k-1}Q_{k-2}+b_{k-1}Q_{k-3}.$$

Од (6) добиваме

$$Q_k\geq b_k(Q_{k-1}+Q_{k-2}) \text{ и } Q_{k-1}\geq dQ_{k-2}.$$

Значи,

$$Q_k\geq b_k(1+d)Q_{k-2}. \tag{8}$$

Од неравенството (8) последователно добиваме

$$Q_{2k}\geq b_{2k}(1+d)Q_{2k-2}\geq...\geq b_{2k}...b_2(1+d)^kQ_0=b_2...b_{2k}(1+d)^k \tag{9}$$

$$Q_{2k+1}\geq b_{2k+1}(1+d)Q_{2k-1}\geq...\geq b_{2k+1}...b_3(1+d)^kQ_1\geq b_1...b_{2k+1}(1+d)^k \tag{10}$$

бидејќи $Q_1=a_1\geq b_1$. Од (9) и (10) добиваме

$$Q_{2k}Q_{2k+1}\geq b_1...b_{2k+1}(1+d)^{2k} \tag{11}$$

па значи

$$\xi_k=\frac{b_1b_2...b_{2k+1}}{Q_{2k}Q_{2k+1}}\leq\frac{1}{(1+d)^{2k}}$$

од каде $\xi_k\to 0$ кога $k\to\infty$.

Според тоа, од неравенството (7), ако преминеме кон граница добиваме $0\leq\beta-\alpha\leq 0$. Значи, $\alpha=\beta=\lim\limits_{n\to\infty}\frac{P_n}{Q_n}$ односно верижната дропка (1) конвергиа. ■

6.5. Забелешка. За конвергентна дропка (1) со позитивни елементи нејзината вредност α се наоѓа меѓу два парцијални количници $\frac{P_{n-1}}{Q_{n-1}}$ и $\frac{P_n}{Q_n}$. Притоа важи

$$|\alpha-\frac{P_n}{Q_n}|\lhd|\frac{P_{n-1}}{Q_{n-1}}-\frac{P_n}{Q_n}|=\frac{b_1b_2...b_n}{Q_{n-1}Q_n}.$$

6.6. Последица. Обична верижна дропка со природни коефициенти е секогаш конвергентна.

Доказ. Следува од теорема 6.4. Деталите ги оставаме на читателот за вежба. ■

6.7. Теорема (Принсгејм). Ако за бесконечната верижна дропка

$$\left\langle 0;\frac{b_1}{a_1},\frac{b_2}{a_2},...,\frac{b_n}{a_n},...\right\rangle \tag{12}$$

се исполнети равенствата

$$|b_n|+1\trianglelefteq|a_n|,\ n=1,2,..., \tag{13}$$

тогаш таа конвергира, при што нејзината апсолутна вредност е помала или еднаква на 1.

Доказ. Нека $\frac{P_k}{Q_k}, k=1,2,...$ се парцијални количници на верижната дропка (12).

Бидејќи $Q_k=a_kQ_{k-1}+b_kQ_{k-2}, k=1,2,...$, добиваме

$$|Q_k|\trianglerighteq|a_k|\cdot|Q_{k-1}|-|b_k|\cdot|Q_{k-2}|.$$

Од неравенствата (13) добиваме

$$|Q_k|\geq(|b_k|+1)|Q_{k-1}|-|b_k|\cdot|Q_{k-2}|,$$

односно

$$|Q_k|-|Q_{k-1}|\trianglerighteq|b_k|\cdot(|Q_{k-1}|-|Q_{k-2}|) \tag{14}$$

Од (14) со последователна примена, ако се има предвид дека $Q_0=1$ и $Q_{-1}=0$ добиваме

$$|Q_k|-|Q_{k-1}|\trianglerighteq|b_k|\cdot|b_{k-1}|\cdot...\cdot|b_1|, \tag{*}$$

односно $|Q_k|\trianglerighteq|Q_0|=1.$

Конвергентноста на верижната дропка (12) е еквивалентна со конвергентноста на редот

$$\frac{P_0}{Q_0}+\sum_{k=1}^{\infty}(\frac{P_k}{Q_k}-\frac{P_{k-1}}{Q_{k-1}})=\sum_{k=1}^{\infty}(-1)^{k-1}\frac{b_1b_2...b_{k+1}}{Q_{k-1}Q_k} \tag{15}$$

Да го разгледаме редот

$$\sum_{k=1}^{\infty}\frac{|b_1|\cdot|b_2|...|b_k|}{|Q_{k-1}|\cdot|Q_k|} \tag{16}$$

Од неравенството (*) имаме

$$\sum_{k=1}^{n}\frac{|b_1|\cdot|b_2|...|b_k|}{|Q_{k-1}|\cdot|Q_k|}\leq\sum_{k=1}^{n}\frac{|Q_k|-|Q_{k-1}|}{|Q_{k-1}|\cdot|Q_k|}=\sum_{k=1}^{n}(\frac{1}{|Q_{k-1}|}-\frac{1}{|Q_k|})=\frac{1}{|Q_0|}-\frac{1}{|Q_n|}<\frac{1}{|Q_0|}=1,$$

за $n=1,2,...$.

Според тоа, парцијалните суми на редот (16) се ограничени, па затоа овој ред конвергира и

$$\sum_{k=1}^{n} \frac{|b_1|\cdot|b_2|\cdot..|b_k|}{|Q_{k-1}|\cdot|Q_k|} \le 1. \qquad (17)$$

Но, тоа значи дека редот (15) конвергира апсолутно, па значи и обично, т.е. постои

$$\lim_{n\to\infty} \frac{P_n}{Q_n} = \sum_{k=1}^{\infty} \left(\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}}\right) = \alpha .$$

Освен тоа, од неравенството (17) имаме $|\alpha| \le 1$. ■

6.8. Пример. Пресметај ја вредноста на верижната дропка $\langle 1; \frac{1}{1}, \frac{1}{1}, \frac{1}{1}, ... \rangle$.

Решение. Забележуваме дека тоа е обична верижна дропка каде $a_0 = a_1 = a_2 = ... = 1$. Според последицата 6.6 оваа верижна дропка е конвергентна. Нека нејзината граница е α. Јасно, бројот α мора да го задоволува равенството $\alpha = \frac{1}{1+\alpha}$. Затоа α е корен на равенката $x^2 + x - 1 = 0$, од каде е $\alpha = x_1 = \frac{-1+\sqrt{5}}{2}$ или $\alpha = x_2 = \frac{-1-\sqrt{5}}{2}$. Сите парцијални количници за дадената верижна дропка се позитивни, па затоа $\alpha \ne x_2 < 0$. Конечно, $\alpha = \frac{-1+\sqrt{5}}{2}$. ■

6.9. Пример. Пресметај ја вредноста на верижната дропка $\langle 1; \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, ... \rangle$.

Решение. Бројот α мора да го задоволува равенството $\alpha = 1 + \frac{1}{1+\alpha}$, кое е еквивалентно со равенството $\alpha^2 = 2$. Од последното равенство добиваме $\alpha = \sqrt{2}$ или $\alpha = -\sqrt{2}$. Бидејќи парцијалните количници се позитивни броеви, не е можно да е $\alpha = -\sqrt{2}$. Затоа $\alpha = \sqrt{2}$. ■

7. ИРАЦИОНАЛНИ БРОЕВИ И ВЕРИЖНИ ДРОПКИ

7.1. Секоја низа од цели броеви $a_0, a_1, a_2, ...$, сите позитивни освен можеби a_0, определува бесконечна обична верижна дропка $\langle a_0; a_1, a_2, ... \rangle$. Вредноста на $\langle a_0; a_1, a_2, ... \rangle$ е определена со $\lim_{n\to\infty} \langle a_0; a_1, a_2, ..., a_n \rangle$.

Според последицата 6.6 границата

$$\lim_{n\to\infty} \langle a_0; a_1, a_2, ..., a_n \rangle = \lim_{n\to\infty} \frac{P_n}{Q_n}$$

постои. Парцијалниот количник

$$\langle a_0; a_1, a_2, ..., a_n \rangle = \frac{P_n}{Q_n}$$

го нарекуваме $n-та$ *конвергента* на обичната бесконечна верижна дропка.

7.2. Теорема. Секоја обична бесконечна верижна дропка е ирационален број.

Доказ. Нека $\alpha = \langle a_0; a_1, a_2, ... \rangle$. Според теоремата 5.9 α се наоѓа меѓу $\frac{p_n}{q_n}$ и $\frac{p_{n+1}}{q_{n+1}}$, а според последицата 5.6 имаме

$$|\alpha - \frac{p_n}{q_n}| < |\frac{p_{n-1}}{q_{n-1}} - \frac{p_n}{q_n}| = \frac{1}{q_{n-1}q_n}.$$

Ако помножиме со q_n, добиваме

$$0 < |q_n\alpha - p_n| < \frac{1}{q_{n+1}}. \quad (1)$$

Нека претпоставиме дека α е рационален број, т.е. $\alpha = \frac{a}{b}$, $a \in \mathbb{Z}, b \in \mathbb{N}$. Ако замениме во (1) и помножиме со b добиваме

$$0 < |q_n a - p_n b| < \frac{b}{q_{n+1}}.$$

Но, низата $\{q_n\}$ е монотоно растечка, па затоа постои $n_0 \in \mathbb{N}$ таков, што $\frac{b}{q_{n_0+1}} < 1$. Значи, добиваме дека $|q_{n_0}a - p_{n_0}b|$ е поголем од 0 и е помал од 1, што е противречност. ■

7.3. Теорема. Нека $\alpha = \langle a_0; a_1, a_2, ... \rangle$. Важи $a_0 = [\alpha]$ и ако $\alpha_1 = \langle a_1; a_2, ... \rangle$, тогаш $\alpha = a_0 + \frac{1}{\alpha_1}$.

Доказ. Од теоремата 5.9 следува дека $\frac{p_0}{q_0} < \alpha < \frac{p_1}{q_1}$, односно

$$a_0 < \alpha < a_0 + \frac{1}{a_1}.$$

Бидејќи $a_1 \geq 1$ добиваме дека $a_0 < \alpha < a_0 + 1$ и затоа $a_0 = [\alpha]$. Исто така,

$$\alpha = \lim_{n\to\infty} \langle a_0; a_1, a_2, ... \rangle = \lim_{n\to\infty} (a_0 + \frac{1}{\langle a_1; a_2, ..., a_n \rangle}) = a_0 + \frac{1}{\lim_{n\to\infty} \langle a_1; a_2, ..., a_n \rangle} = a_0 + \frac{1}{\alpha_1}. \quad ■$$

7.4. Теорема. Две различни бесконечни обични верижни дропки конвергираат кон различни вредности.

Доказ. Нека претпоставиме дека

$$\langle a_0; a_1, a_2, ... \rangle = \langle b_0; b_1, b_2, ... \rangle = \alpha.$$

Според теорема 7.3. имаме $a_0 = [\alpha] = b_0$ и од тука

$$\alpha = a_0 + \frac{1}{\langle a_1; a_2, a_3, ... \rangle} = b_0 + \frac{1}{\langle b_1; b_2, b_3, ... \rangle}.$$

Затоа $\langle a_1;a_2,a_3,\ldots\rangle=\langle b_1;b_2,b_3,\ldots\rangle$. Добиваме $a_1=b_1$ и со математичка индукција лесно се докажува $a_i=b_i$, $i=1,2,3,\ldots$. ■

7.5. Во теоремата 7.2 докажавме дека секоја обична бескоенчна верижна дропка е ирационален број. Ќе докажеме дека секој ирационален број α_0 може да се претстави како обична бесконечна верижна дропка. Ставаме $a_0=[\alpha_0]$, $\alpha_1=\frac{1}{\alpha_0-a_0}$ и

$$a_i=[\alpha_i],\ \alpha_{i+1}=\frac{1}{\alpha_i-a_i}\text{, за } i=1,2,3,\ldots \tag{2}$$

Јасно, a_i е цел број и α_i е ирационаелен број. Освен тоа, од $a_{i-1}=[\alpha_{i-1}]$ и фактот дека α_{i-1} е ирационален број имаме

$$a_{i-1}<\alpha_{i-1}<a_{i-1}+1\text{, т.е. } 0<\alpha_{i-1}-a_{i-1}<1,$$

односно $\alpha_i=\frac{1}{\alpha_{i-1}-a_{i-1}}>1$, па затоа $a_i=[\alpha_i]\geq 1$ за секој $i\geq 1$.

Понатаму, од (2) имаме $\alpha_i=a_i+\frac{1}{\alpha_{i+1}}$ и со последователна примена добиваме

$$\alpha_0=a_0+\frac{1}{\alpha_1}=a_0+\frac{1}{a_1+\frac{1}{\alpha_2}}=a_0+\frac{1}{a_1+\frac{1}{a_2+\frac{1}{\alpha_3}}}=\ldots=a_0+\frac{1}{a_1+\frac{1}{a_2+\frac{1}{a_3+\ldots+\frac{1}{\alpha_n}}}}$$

$$=\langle a_0;a_1,a_2,\ldots a_{n-1},\alpha_n\rangle.$$

Според последицата 5.3 последната верижна дропка може да се запише во облик

$$\alpha=\langle a_0;a_1,a_2,\ldots a_{n-1},\alpha_n\rangle=\frac{\alpha_n p_{n-1}+p_{n-2}}{\alpha_n q_{n-1}+q_{n-2}}, \tag{3}$$

каде $p_k=a_k p_{k-1}+p_{k-2}$ и $q_k=a_k q_{k-1}+p_{k-2}$, за $k=1,2,\ldots,n-1$. Според последицата 5.6 имаме

$$\alpha-\frac{p_{n-1}}{q_{n-1}}=\frac{\alpha_n p_{n-1}+p_{n-2}}{\alpha_n q_{n-1}+q_{n-2}}-\frac{p_{n-1}}{q_{n-1}}=\frac{-(p_{n-1}q_{n-2}-p_{n-2}q_{n-1})}{q_{n-1}(\alpha_n q_{n-1}+q_{n-2})}=\frac{(-1)^{n-1}}{q_{n-1}(\alpha_n q_{n-1}+q_{n-2})}. \tag{4}$$

Но, $\alpha_n>0$ и кога $n\to\infty$ важи $q_n\to\infty$ добиваме $\alpha-\frac{p_{n-1}}{q_{n-1}}\to 0$ кога $n\to\infty$, т.е.

$$\lim_{n\to\infty}\frac{p_n}{q_n}=\lim_{n\to\infty}\langle a_0;a_1,a_2,\ldots,a_n\rangle=\lim_{n\to\infty}\langle a_0;a_1,a_2,\ldots\rangle.$$

Со тоа ја докажавме следната теорема.

Теорема. Секој ирационален број α_0, со алгоритамот опишан со равенствата (2) може да се претстави како обична бесконечна верижна дропка со елементи $a_i>0$, за $i\geq 1$. Ако α_i е определен со (2), тогаш

$$\langle a_0;a_1,a_2,\ldots\rangle=\langle a_0;a_1,a_2,\ldots a_{n-1},\alpha_n\rangle \text{ и } \alpha_n=\langle a_n;a_{n+1},a_{n+2},\ldots\rangle. \blacksquare$$

7.6. Последица. За секој $n\geq 0$ важи

$$|\alpha_0-\frac{p_n}{q_n}|<\frac{1}{q_n q_{n+1}} \text{ и } |q_n\alpha_0-p_n|<\frac{1}{q_{n+1}}. \tag{5}$$

Доказ. Од (4) имаме

$$|\alpha_0 - \tfrac{p_n}{q_n}| = \tfrac{1}{q_n(\alpha_{n+1}q_n + q_{n-1})}$$

и како $0 < a_i < \alpha_i$ добиваме

$$|\alpha_0 - \tfrac{p_n}{q_n}| < \tfrac{1}{q_n(a_{n+1}q_n + q_{n-1})} = \tfrac{1}{q_n q_{n+1}}.$$

Второто неравенство го добиваме од првото, ако помножиме со q_n. ■

7.7. Последица. За конвергентите $\frac{p_n}{q_n}$ важат неравенствата

$$|\alpha_0 - \tfrac{p_n}{q_n}| \lhd |\alpha_0 - \tfrac{p_{n-1}}{q_{n-1}}| \text{ и } |q_n\alpha_0 - p_n| \lhd |q_{n-1}\alpha_0 - p_{n-1}|. \qquad (6)$$

Доказ. Да забележиме дека $a_n + 1 > \alpha_n$, односно

$$\alpha_n q_{n-1} + q_{n-2} < (a_n + 1)q_{n-1} + q_{n-2} = q_n + q_{n-1} \le a_{n+1}q_n + q_{n-1} = q_{n+1}.$$

Ако ја искористиме релацијата (4) и последните неравенства добиваме

$$|\alpha_0 - \tfrac{p_{n-1}}{q_{n-1}}| = \tfrac{1}{q_{n-1}(\alpha_n q_{n-1} + q_{n-2})} > \tfrac{1}{q_{n-1}q_{n+1}}.$$

Ако помножиме со q_{n-1}, тогаш според последицата 7.6 добиваме

$$|q_{n-1}\alpha_0 - p_{n-1}| > \tfrac{1}{q_{n+1}} \rhd |q_n\alpha_0 - p_n|,$$

т.е. точно е второто неравенство во (6).

За да го докажеме првото неравенство доволно е да забележиме дека $q_{n-1} \le q_n$ и да го примениме второто неравенство. Имено,

$$|\alpha_0 - \tfrac{p_n}{q_n}| = \tfrac{1}{q_n}|\alpha_0 q_n - p_n| < \tfrac{1}{q_n}|\alpha_0 q_{n-1} - p_{n-1}| \le \tfrac{1}{q_{n-1}}|\alpha_0 q_{n-1} - p_{n-1}| = |\alpha_0 - \tfrac{p_{n-1}}{q_{n-1}}|. \blacksquare$$

7.8. Пример. Претстави го бројот $\sqrt{3}$ како обична верижна дропка.

Решение. Според алгоритамот опишн со равенствата (2) добиваме

$$a_0 = [\sqrt{3}] = 1, \qquad \alpha_1 = \tfrac{1}{\sqrt{3}-1} = \tfrac{\sqrt{3}+1}{2},$$

$$a_1 = [\alpha_1] = 1, \qquad \alpha_2 = \tfrac{2}{\sqrt{3}-1} = \sqrt{3}+1,$$

$$a_2 = [\alpha_2] = 2, \qquad \alpha_3 = \tfrac{1}{\sqrt{3}+1-2} = \tfrac{\sqrt{3}+1}{2},$$

$$a_3 = [\alpha_3] = 1, \qquad \alpha_4 = \tfrac{2}{\sqrt{3}-1} = \sqrt{3}+1.$$

Забележуваме дека доаѓа до периодично повторување на последните два чекори, па добиваме $\sqrt{3} = \langle 1; 1, 2, 1, 2, \ldots \rangle$. ■

7.9. Пример. Претстави го бројот $e = 2,71828182...$ како обична верижна дропка.

Решение. Имаме

$a_0 = [e] = 2,$ $\alpha_1 = \frac{1}{2{,}71828182\ldots - 2} = 1{,}39221119\ldots,$

$a_1 = 1,$ $\alpha_2 = \frac{1}{1{,}39221119\ldots - 1} = 2{,}54964677\ldots,$

$a_2 = 2,$ $\alpha_3 = \frac{1}{2{,}54964677\ldots - 2} = 1{,}81935024\ldots,$

$a_3 = 1,$ $\alpha_4 = \frac{1}{1{,}81935024\ldots - 1} = 1{,}22047928\ldots,$

$a_4 = 1,$ $\alpha_5 = \frac{1}{1{,}22047928 - 1} = 4{,}53557347\ldots,$

$a_5 = 4,$ $\alpha_6 = \frac{1}{4{,}53557347\ldots - 4} = 1{,}867157\ldots,$

$a_6 = 1,$ $\alpha_7 = \frac{1}{1{,}867157\ldots - 1} = 1{,}153193\ldots,$

$a_7 = 1,$ $\alpha_8 = \frac{1}{1{,}153193\ldots - 1} = 6{,}527707\ldots,$

$a_8 = 6,$ $\alpha_9 = \frac{1}{6{,}527707\ldots - 6} = 1{,}8949\ldots,$

$a_9 = 1,$ $\alpha_{10} = \frac{1}{1{,}8949\ldots - 1} = 1{,}1173\ldots$

$a_{10} = 1,$ .....

....

Значи, $e = \langle 2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, \ldots \rangle$. ■

7.10. Теорема. Ако $\frac{a}{b}$ е рационален број со позитивен именител таков што $|\alpha - \frac{a}{b}| \lhd |\alpha - \frac{p_n}{q_n}|$ за некој $n \geq 1$, тогаш $b > q_n$.

Ако $\frac{a}{b}$ е рационален број со позитивен именител таков што $|\alpha b - a| \lhd |\alpha q_n - p_n|$ за некој $n \geq 1$, тогаш $b > q_n$.

Доказ. Прво ќе го докажеме вториот дел од теоремата. Нека претпоставиме дека $|\alpha b - a| \lhd |\alpha q_n - p_n|$ и $b \leq q_n$. Бидејќи $q_n < q_{n+1}$ за $n \geq 1$ добиваме $b < q_{n+1}$. Да го разгледаме системот линеарни равенки

$$\begin{cases} xq_n + yq_{n+1} = b \\ xp_n + yp_{n+1} = a. \end{cases} \tag{7}$$

Детерминантата на системот е еднаква на ± 1 и затоа овој систем има единствено целобројно решение. Притоа $x \neq 0$ и $y \neq 0$. Јасно, ако $x = 0$, тогаш $b = yq_{n+1}$, па значи $y > 0$, односно $b \geq q_{n+1}$, што е противречност. Ако $y = 0$, тогаш $a = xp_n$, $b = xq_n$ и бидејќи $|x| \geq 1$ добиваме

$$|\alpha b - a| \rightleftharpoons |x| \cdot |\alpha q_n - p_n| \trianglerighteq |\alpha q_n - p_n|,$$

што повторно е противречност.

Ќе докажеме дека x и y имаат спротивни знаци. Имено, ако $y<0$, тогаш од $xq_n = b - yq_{n+1}$ следува, дека $x>0$. Ако $y>0$, тогаш од $b<q_{n+1}$ следува $b<yq_{n+1}$ односно $xq_n<0$, што значи $x<0$. Но, сега од теоремата 5.9 следува дека $\alpha q_n - p_n$ и $\alpha q_{n+1} - p_{n+1}$ имаат спротивни знаци. Од системот (7) имаме:

$$\alpha b - a = x(\alpha q_n - p_n) + y(\alpha q_{n+1} - p_{n+1})$$

и затоа

$$|\alpha b - a| \geq |x| \cdot |\alpha q_n - p_n| + |y| \cdot |\alpha q_{n+1} - p_{n+1}| > |x| \cdot |\alpha q_n - p_n| \geq |\alpha q_n - p_n|,$$

што противречи на условот на теоремата. Од добиената противречност следува, дека ако $|\alpha b - a| < |\alpha q_n - p_n|$ за некој $n \geq 1$, тогаш $b > q_n$.

Нека препоставиме дека $|\alpha - \frac{a}{b}| < |\alpha - \frac{p_n}{q_n}|$ и $b \leq q_n$. Тоа значи, дека

$$b|\alpha - \frac{a}{b}| < q_n|\alpha - \frac{p_n}{q_n}| \text{ и } b \leq q_n,$$

т.е.

$$|\alpha b - a| < |\alpha q_n - p_n| \text{ и } b \leq q_n,$$

што е противречност. ■

7.11. Теорема. Нека α е ирационален број. Ако постои рационален број $\frac{a}{b}$, $(a,b)=1$ и $b \geq 1$ таков што $|\alpha - \frac{a}{b}| < \frac{1}{2b^2}$, тогаш $\frac{a}{b}$ е еден од конвергентите на обичната верижна дропка со која е претставен бројот α.

Доказ. Според теоремата 4.4 бројот $\frac{a}{b}$ може да го претставиме како обична верижна дропка, т.е. $\frac{a}{b} = \langle a_0; a_1, a_2, ..., a_n \rangle$. Да ги означиме конвергентите на $\langle a_0; a_1, a_2, ..., a_n \rangle$ со $\frac{p_i}{q_i}$, така што

$$\frac{a}{b} = \langle a_0; a_1, a_2, ..., a_n \rangle = \frac{p_n}{q_n} \text{ и } |\alpha - \frac{p_n}{q_n}| < \frac{1}{2b^2} \tag{8}$$

Непосредно од алгоритамот даден со (2) следува дека постои $\beta > 0$ таков што $\langle a_0; a_1, a_2, \ldots a_n, \beta \rangle = \alpha$ за кој важи

$$\alpha = \langle a_0; a_1, a_2, \ldots a_n, \beta \rangle = \frac{\beta p_n + p_{n-1}}{\beta q_n + q_{n-1}}.$$

Јасно, β е ирационален број и може да се запише во облик

$$\beta = \frac{p_{n-1} - \alpha q_{n-1}}{\alpha q_n - p_n} = \frac{q_{n-1}}{q_n} \cdot \frac{\frac{p_{n-1}}{q_{n-1}} - \alpha}{\alpha - \frac{p_n}{q_n}}. \tag{9}$$

Од друга страна, од забелешката 6.5 и од (8) имаме

$$|\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}| = \frac{1}{q_n q_{n-1}} \geq \frac{1}{q_n^2} > 2|\alpha - \frac{p_n}{q_n}|. \tag{10}$$

Ако $\alpha > \frac{a}{b} = \frac{p_n}{q_n}$, тогаш n е парен број, па така $\frac{p_n}{q_n} < \frac{p_{n-1}}{q_{n-1}}$ и од (10) следува дека α лежи меѓу $\frac{p_n}{q_n}$ и $\frac{p_{n-1}}{q_{n-1}}$. Ако $\alpha < \frac{a}{b} = \frac{p_n}{q_n}$, тогаш n е непарен број, па $\frac{p_n}{q_n} > \frac{p_{n-1}}{q_{n-1}}$ и од (10) следува α лежи меѓу $\frac{p_{n-1}}{q_{n-1}}$ и $\frac{p_n}{q_n}$. И во двата случаи β е позитивен и од (8) следува

$$|\frac{p_{n-1}}{q_{n-1}} - \alpha| = |\frac{p_{n-1}}{q_{n-1}} - \frac{p_n}{q_n}| - |\alpha - \frac{p_n}{q_n}| \geq \frac{1}{q_n q_{n-1}} - \frac{1}{2q_n^2} > \frac{1}{2q_n q_{n-1}} \ .$$

Од последното неравентство, (8) и (9) добиваме

$$\beta > \frac{q_{n-1}}{q_n} \cdot \frac{\frac{1}{2q_{n-1}q_n}}{\frac{1}{2q_n^2}} = 1 .$$

Значи β е ирационален број и $\beta > 1$, па според теоремата 7.5 може да се претстави како обична бесконечна верижна дропка $\beta = \langle b_0; b_1, b_2, ... \rangle$, при што $b_0 = [\beta] \geq 1$. Освен тоа, $\langle a_0; a_1, ..., a_n, b_0, b_1, ... \rangle$ е бесконечна верижна дропка чија вредност ќе ја означиме со ϑ. Притоа важи

$$\vartheta = \langle a_0; a_1, ..., a_n, b_0, b_1, ... \rangle = \langle a_0; a_1, ..., a_n, \vartheta_{n+1} \rangle$$

каде $\vartheta_{n+1} = \langle b_0; b_1, b_2, .. \rangle = \beta$ и затоа $\vartheta = \langle a_0; a_1, ... a_n, \beta \rangle = \alpha$, односно

$$\alpha = \langle a_0; a_1, ... a_n, b_0, b_1, .. \rangle .$$

Бидејќи претставувањето на α е единствено, следува

$$\frac{a}{b} = \langle a_0; a_1, a_2, ..., a_n \rangle$$

е $n-$тиот конвергент на α. ■

7.12. Теорема. Ако $x \in \mathbb{R}$ и $x > 1$, тогаш $n-$тиот конвергент на $\frac{1}{x}$ е еднаков на реципрочната вредност од на $(n-1)-$виот конвергент на x.

Доказ. Имаме

$$x = \langle a_0; a_1, a_2, ... \rangle \text{ и } \frac{1}{x} = \langle 0; a_0, a_1, a_2, ... \rangle .$$

Сега тврдењето следува од последицата 5.3. ■

7.13. Лема. Ако $u \neq 0$, $y \neq 0$, тогаш од равенствата

$$z - x = uy \tag{11}$$

$$ax^2 + by^2 - xy = 0 \tag{12}$$

$$cy^2 + az^2 - yz = 0 \tag{13}$$

следува

$$a^2u^2 + 2a(b+c) = 1 - u^{-2}(b-c)^2 \ .$$

Доказ. Ако ги одземеме равенството (12) од равенството (13), замениме од (11) и скратиме од *y* добиваме

$$au(z+x)=y(b-c+u) \tag{14}$$

Од (11) имаме $au(z-x)=au^2y$. Ако ги квадрираме последното равенство и (14) и ги собереме, добиваме

$$2a^2u^2(z^2+x^2)=a^2u^4y^2+y^2(b-c+u)^2. \tag{15}$$

Ако равенствата (12) и (13) го помножиме со $2au^2$ и за $z+x$ замениме од (14) добиваме

$$a^2u^4+(b-c+u)^2=2u(b-c+u)-2au^2(b+c).$$

Лесно се гледа дека последното равенство е еквивалентно на бараното равенство. ■

7.14. Втор доказ на теорема 3.1 (Хурвиц). а) Бидејќи α се наоѓа меѓу $\frac{p_n}{q_n}$ и $\frac{p_{n-1}}{q_{n-1}}$ имаме

$$|\alpha-\tfrac{p_n}{q_n}|+|\alpha-\tfrac{p_{n-1}}{q_{n-1}}|=|\tfrac{p_n}{q_n}-\tfrac{p_{n-1}}{q_{n-1}}|=\tfrac{1}{q_nq_{n+1}}.$$

Дефинираме $\beta_n=q_n^2|\alpha-\frac{p_n}{q_n}|$ и ако претходното равенство го помножиме со $q_n^2q_{n-1}^2$ добиваме

$$\beta_nq_{n-1}^2+\beta_{n-1}q_n^2-q_nq_{n-1}=0.$$

Ако *n* се замени со $n+1$, тогаш

$$\beta_{n+1}q_n^2+\beta_nq_{n+1}^2-q_{n+1}q_n=0$$

Исто така,

$$q_{n+1}-q_{n-1}=a_{n+1}q_n.$$

Последните три равенства се од облик (12), (13) и (11) па според лемата 7.13 добиваме

$$\beta_n^2a_{n+1}^2+2\beta_n(\beta_{n-1}+\beta_{n+1})=1-a_{n-1}^{-2}(\beta_{n-1}-\beta_{n+1})^2. \tag{16}$$

Десната страна на последното равенство е помала од 1, освен ако $\beta_{n-1}=\beta_{n+1}$. Но, $\beta_{n-1}=\beta_{n+1}$ не е можно бидејќи притоа имаме

$$q_{n-1}^2|\alpha-\tfrac{p_{n-1}}{q_{n-1}}|=q_{n-1}^2|\alpha-\tfrac{p_{n+1}}{q_{n+1}}|,$$

и под апсолутните вредности се еднакви по знак, па затоа

$$q_{n-1}^2(\alpha-\tfrac{p_{n-1}}{q_{n-1}})=q_{n-1}^2(\alpha-\tfrac{p_{n+1}}{q_{n+1}})$$

Како $q_{n+1}\neq q_{n-1}$ од последното равенство следува дека α е рационален број, што е противречност. Значи, $\beta_{n-1}\neq\beta_{n+1}$ и од (16) следува

$$\beta_n^2a_{n+1}^2+2\beta_n(\beta_{n-1}+\beta_{n+1})<1.$$

Ако земеме $\beta = \min\{\beta_{n-1}, \beta_n, \beta_{n+1}\}$ добиваме

$$\beta^2(a_{n+1}^2+4) \le \beta^2 a_{n+1}^2 + 2\beta_n(\beta_{n-1}+\beta_{n+1}) < 1$$

и затоа $5\beta^2 < 1$ односно $\beta = \min\{\beta_{n-1}, \beta_n, \beta_{n+1}\} < \frac{1}{\sqrt{5}}$.

Од досега изнесеното следува дека постојат бесконечно многу рационални броеви $\frac{p}{q}$ такви што $|\alpha - \frac{p}{q}| < \frac{1}{\sqrt{5}q^2}$.

б) Да го разгледаме ирационалниот број α кој е претставен со бесконечната верижна дропка $\langle 1;1,1,1,... \rangle$. Имаме $\alpha = 1 + \frac{1}{\langle 1;1,1,1,... \rangle} = 1 + \frac{1}{\alpha}$ или $\alpha = \frac{\sqrt{5}+1}{2}$. Ако се искористи алгоритамот дефиниран со релацијата (2) со математичка индукција можеме да докажеме дека $\alpha_i = \frac{\sqrt{5}+1}{2}$ за секој $i \ge 0$. Навистина, ако $\alpha_i = \frac{\sqrt{5}+1}{2}$, тогаш

$$\alpha_{i+1} = \frac{1}{\alpha_i - a_i} = \frac{1}{\frac{\sqrt{5}+1}{2} - 1} = \frac{\sqrt{5}+1}{2}.$$

Без тешкотии можеме да докажеме дека $p_0 = q_0 = q_1 = 1, p_1 = q_2 = 2$. Но, како $p_i = p_{i-1} + p_{i-2}$ и $q_i = q_{i-1} + q_{i-2}$ од принципот на математичка индукција следува дека $q_n = p_{n-1}$, за $n \ge 1$. Според тоа

$$\lim_{n\to\infty} \frac{q_{n-1}}{q_n} = \lim_{n\to\infty} \frac{q_{n-1}}{p_{n-1}} = \frac{1}{\alpha} = \frac{\sqrt{5}-1}{2}$$

$$\lim_{n\to\infty} (\alpha_{n+1} + \frac{q_{n-1}}{q_n}) = \frac{\sqrt{5}+1}{2} + \frac{\sqrt{5}-1}{2} = \sqrt{5}.$$

Ако C е произволна константа поголема од $\sqrt{5}$, тогаш неравенството $\alpha_{n+1} + \frac{q_{n-1}}{q_n} > C$ е исполнето за конечно многу вредности на *n*. Така, неравенството

$$|\alpha - \frac{p_n}{q_n}| = \frac{1}{q_n^2(\alpha_{n+1} + \frac{q_{n-1}}{q_n})} < \frac{1}{Cq^2}$$

важи само за конечно многу вредности на *n*. Значи постојат само конечен број рационални броеви $\frac{p}{q}$ за кои важи $|\alpha - \frac{p}{q}| < \frac{1}{Cq^2}$, бидејќи секој таков $\frac{p}{q}$ е еден од конвергентите на α (теорема 7.11). ■

8. ПЕРИОДИЧНИ ВЕРИЖНИ ДРОПКИ

8.1. Во оваа точка покрај стандардните ознаки ќе ги користиме и ознаките

$$A_n = \begin{bmatrix} 0 & 1 \\ 1 & a_n \end{bmatrix},\ M_n = \begin{bmatrix} q_{n-2} & p_{n-2} \\ q_{n-1} & p_{n-1} \end{bmatrix} \text{ и } \gamma_n = q_{n-2} + \alpha_n q_{n-1} \text{ за } n \ge 1.$$

Лема. Нека α е ирационален број. Тогаш за секој $n \geq 1$ важи

$$M_{n+1} = A_n M_n \tag{1}$$

$$\gamma_n\{1,\alpha\} = \{1,\alpha_n\}M_n\ ,\ \gamma_n \neq 0,\ \det M_n = (-1)^n \tag{2}$$

$$M_{n+1} = A_n A_{n-1} \ldots A_1 A_0\ . \tag{3}$$

Освен тоа, M_n^{-1} е целобројна матрица и ако $M_n = M_m$, тогаш $n = m$.

Доказ. Од релациите $p_k = a_k p_{k-1} + p_{k-2}$ и $q_k = a_k q_{k-1} + q_{k-2}$ имаме

$$A_n M_n = \begin{bmatrix} 0 & 1 \\ 1 & a_n \end{bmatrix}\begin{bmatrix} q_{n-2} & p_{n-2} \\ q_{n-1} & p_{n-1} \end{bmatrix} = \begin{bmatrix} q_{n-1} & p_{n-1} \\ a_n q_{n-1} + q_{n-2} & a_n p_{n-1} + p_{n-2} \end{bmatrix}$$
$$= \begin{bmatrix} q_{n-1} & p_{n-1} \\ q_n & p_n \end{bmatrix} = M_{n+1},$$

т.е. важи (1). Од $\alpha = \langle a_0; a_1, a_2, \ldots a_n, \alpha_n \rangle$ имаме $\alpha = \frac{p_{n-2} + \alpha_n p_{n-1}}{q_{n-2} + \alpha_n q_{n-1}}$, односно

$$\{1,\alpha_n\}M_n = \{1,\alpha_n\}\begin{bmatrix} q_{n-2} & p_{n-2} \\ q_{n-1} & p_{n-1} \end{bmatrix} = \{q_{n-2} + \alpha_n q_{n-1},\ p_{n-2} + \alpha_n p_{n-1}\}$$
$$= \{q_{n-2} + \alpha_n q_{n-1},\ \alpha(q_{n-2} + \alpha_n q_{n-1})\}$$
$$= (q_{n-2} + \alpha_n q_{n-1})\{1,\alpha\} = \gamma_n\{1,\alpha\},$$

што значи, дека точно е првото равенство (2). Бројот α_n е ирационален бидејќи α е ирационален број. Бидејќи q_{n-2} и q_{n-1} се цели броеви, ако $\gamma_n = 0$, тогаш $\alpha_n = \frac{-q_{n-2}}{q_{n-1}}$ што е противречност. Значи, $\gamma_n \neq 0$ за секој $n \geq 1$. Од последицата 5.6 следува

$$\det M_n = p_{n-1}q_{n-2} - p_{n-2}q_{n-1} = (-1)^n\ .$$

Бидејќи

$$M_1 = \begin{bmatrix} q_{-1} & p_{-1} \\ q_0 & p_0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & a_0 \end{bmatrix} = A_0$$

Добиваме

$$M_{n+1} = A_n M_n = A_n A_{n-1} M_{n-1} = \ldots = A_n A_{n-1} \ldots A_1 M_1 = A_n A_{n-1} \ldots A_1 A_0\ ,$$

т.е. точно е равенството (3).

Од $\det M_n = (-1)^n$ следува

$$M_n^{-1} = \frac{1}{\det M_n}\begin{bmatrix} p_{n-1} & -p_{n-2} \\ -q_{n-1} & q_{n-2} \end{bmatrix} = (-1)^n \begin{bmatrix} p_{n-1} & -p_{n-2} \\ -q_{n-1} & q_{n-2} \end{bmatrix},$$

т.е. M_n^{-1} е целобројна матрица. На крајот, ако $n \neq m$ и $M_n = M_m$, тогаш

$$\begin{bmatrix} q_{n-2} & p_{n-1} \\ q_{n-1} & p_{n-1} \end{bmatrix} = \begin{bmatrix} q_{m-2} & p_{m-1} \\ q_{m-1} & p_{m-1} \end{bmatrix}.$$

Затоа $q_{n-2} = q_{m-2}$ и $q_{n-1} = q_{m-1}$, што противречи на фактот дека

$$0 = q_{-1} < 1 = q_0 \le q_1 < q_2 < \dots . \blacksquare$$

8.2. Лема. Нека $n \ge 1$ и $j > 0$. Тогаш

$$M_n^{-1} M_{n+j} = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \ne \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} = rI .$$

Доказ. Нека претпоставиме дека $M_n^{-1} M_{n+j} = rI$. Тогаш

$$M_{n+j} = = M_n (M_n^{-1} M_{n+j}) = M_n (rI) = r M_n .$$

Ако ги изедначиме првите редови на M_{n+j} и M_n добиваме

$$q_{n+j-2} = r q_{n-2} \text{ и } p_{n+j-2} = r p_{n-2} .$$

Меѓутоа, r е делител на заемно простите броеви q_{n+j-2} и p_{n+j-2} и затоа $r = \pm 1$. Бидејќи M_{n+j} има ненегативни елементи важи $r = 1$. Значи, $M_n = M_{n+j}$ и од лемата 8.1. следува $n = n + j$, што противречи на $j > 0$. Конечно, од добиената противречност следува $M_n^{-1} M_{n+j} \ne rI$. $\blacksquare$

8.3. Лема. Нека α е ирационален број, r, s, t и u се цели броеви и δ е реален број таков што

$$\delta \{1, \alpha\} = \{1, \alpha\} \begin{bmatrix} r & s \\ t & u \end{bmatrix} .$$

Ако $t = 0$, тогаш

$$\begin{bmatrix} r & s \\ 0 & u \end{bmatrix} = rI .$$

Доказ. Ако $t = 0$, тогаш имаме

$$\{\delta, \delta\alpha\} = \{1, \alpha\} \begin{bmatrix} r & s \\ 0 & u \end{bmatrix} = \{r, s + u\alpha\} .$$

Следува $\delta = r$ и $\delta\alpha = s + u\alpha$. Значи, $r\alpha = s + u\alpha$ или $s + (u - r)\alpha = 0$. Но, тоа значи $s = 0$ и $u - r = 0$. Во спротивно $\alpha = \frac{-s}{u-r}$ е рационален број што е противречност. Според тоа,

$$\begin{bmatrix} r & s \\ t & u \end{bmatrix} = \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} = rI . \blacksquare$$

8.4. Дефиниција. Бесконечната обична верижна дропка ја нарекуваме *периодична* ако постојат $n, r_0 \in \mathbb{N}$ такви што $a_r = a_{n+r}$ за секој $r \ge r_0$. Така периодичната верижна дропка може да се запише во облик

$$\left\langle b_0; b_1, \dots, b_j, a_0, a_1, \dots, a_{n-1}, a_0, a_1, \dots, a_{n-1}, \dots \right\rangle = \left\langle b_0; b_1, b_2, \dots b_j, \overline{a_0, a_1, \dots, a_{n-1}} \right\rangle .$$

8.5. Теорема. Ако α е периодична верижна дропка, тогаш α е ирационален корен од квадратна равенка со ненулти коефициенти пред α^2.

Доказ. Според претпоставката

$$\alpha_{j+n} = \left\langle \overline{a_{n+j}; a_{n+j+1}, ..., a_{j+2n-1}} \right\rangle = \left\langle \overline{a_j; a_{n+1}, ..., a_{j+n-1}} \right\rangle = \alpha_j .$$

Според тоа, α е ирационален број. Според лемата 8.1 имаме

$$\gamma_j \{1, \alpha\} = \{1, \alpha_j\} M_j , \ \gamma_{j+n} \{1, \alpha\} = \{1, \alpha_{j+n}\} M_{n+j} .$$

Од првото од овие две равенства добиваме

$$\{1, \alpha_j\} = (\{1, \alpha_j\} M_j) M_j^{-1} = \gamma_j \{1, \alpha\} M_j^{-1},$$

па од второто равенство имаме

$$\gamma_{n+j} \{1, \alpha\} = \{1, \alpha_{n+j}\} M_{n+j} = \{1, \alpha_j\} M_{n+j} = \gamma_j \{1, \alpha\} M_j^{-1} M_{n+j} ,$$

или ако ставиме $\delta = \frac{\gamma_{n+j}}{\gamma_j}$, што е коректно бидејќи $\gamma_j \neq 0$, добиваме

$$\delta \{1, \alpha\} = \{1, \alpha\} M_j^{-1} M_{n+j} \ . \tag{4}$$

Нека

$$M_j^{-1} M_{n+j} = \begin{bmatrix} r & s \\ t & u \end{bmatrix}, \tag{5}$$

каде r, s, t и u се цели броеви, (M_j^{-1} е целобројна матрица). Бидејќи α е ирационален број од лемата 8.2 и лемата 8.3 добиваме $t \neq 0$.

Равенството (4) го запишуваме во облик

$$\{\delta, \delta\alpha\} = \{1, \alpha\} \begin{bmatrix} r & s \\ t & u \end{bmatrix} = \{r + t\alpha, s + u\alpha\}$$

и затоа $\delta = r + t\alpha$, $\delta\alpha = s + u\alpha$. Така, $(r + t\alpha)\alpha = \delta\alpha = s + u\alpha$ односно

$$t\alpha^2 + (r - u)\alpha - s = 0, \tag{6}$$

т.е. α е ирационален корен од квадратна равенка со ненулти коефициент пред α^2. ■

8.6. Дефиниција. Нека $A = [a_{ij}]_{2\times 2}$, $a_{ij} \in \mathbb{R}, i, j = 1, 2$. Дефинираме норма од A со

$$\| A \| = \max\{ | a_{ij} | : i = 1, 2 ; j = 1, 2 \} .$$

8.7. Лема. Ако A, B и C се 2×2 матрици, тогаш

$$\| A + B \| \leq \| A \| + \| B \| \text{ и } \| ABC \| \leq 4 \| A \| \cdot \| B \| \cdot \| C \| .$$

Доказ. Нека

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} , \ B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}.$$

Тогаш

$$A+B=\begin{bmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{bmatrix} \text{ и } AB=\begin{bmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{bmatrix}.$$

Значи, $|a_{ij}+b_{ij}| \leq |a_{ij}|+|b_{ij}| \leq \|A\|+\|B\|$, за $i=1,2;\ j=1,2$, односно

$$\max\{|a_{ij}+b_{ij}|: i=1,2\ ;\ j=1,2\} \leq \|A\|+\|B\|,$$

па затоа $\|A+B\| \leq \|A\|+\|B\|$. Исто така

$$|a_{i1}b_{1j}+a_{i2}b_{2j}| \leq |a_{i1}|\cdot|b_{1j}|+|a_{i2}|\cdot|b_{2j}| \leq \|A\|\cdot\|B\|+\|A\|\cdot\|B\| = 2\|A\|\cdot\|B\|,$$

односно

$$\max\{|a_{i1}b_{1j}+a_{i2}b_{2j}|: i=1,2;\ j=1,2\} \leq 2\|A\|\cdot\|B\|,$$

па затоа $\|AB\| \leq 2\|A\|\cdot\|B\|$. Според тоа, за матриците A, B и C имаме

$$\|ABC\| = \|(AB)C\| \leq 2\|AB\|\cdot\|C\| \leq 4\|A\|\cdot\|B\|\cdot\|C\|. \blacksquare$$

8.8. Теорема. Нека $a,b,c \in \mathbb{Z}$, $a \neq 0$ и α е позитивен ирационален корен на квадратната равенка $ax^2+bx+c=0$. Тогаш α е периодична верижна дропка.

Доказ. Бидејќи $a\alpha^2 = -b\alpha - c$, добиваме

$$a\alpha\{1,\alpha\} = \{a\alpha, a\alpha^2\} = \{a\alpha, -b\alpha - c\} = \{1,\alpha\}\begin{bmatrix} 0 & -c \\ a & -b \end{bmatrix}.$$

Ако означиме

$$B=\begin{bmatrix} 0 & -c \\ a & -b \end{bmatrix},$$

тогаш

$$a\alpha\{1,\alpha\} = \{1,\alpha\}B. \tag{7}$$

Ќе најдеме квадратна равенка чие решение е α_n, каде $\alpha = \langle a_0; a_1, \ldots a_{n-1}, \alpha_n \rangle$. Според лемата 8.1. имаме $\gamma_n\{1,\alpha\} = \{1,\alpha_n\}M_n$. Од последното равенство и од (7) добиваме

$$\begin{aligned} a\alpha\{1,\alpha_n\} &= a\alpha(\{1,\alpha_n\}M_n)M_n^{-1} = a\alpha(\gamma_n\{1,\alpha\})M_n^{-1} = \gamma_n(\{1,\alpha\}B)M_n^{-1} \\ &= (\gamma_n\{1,\alpha\})BM_n^{-1} = \{1,\alpha_n\}M_nBM_n^{-1}. \end{aligned}$$

Нека

$$M_nBM_n^{-1} = \begin{bmatrix} r_n & s_n \\ t_n & u_n \end{bmatrix}.$$

Последната матрица е целобројна, бидејќи M_n, B и M_n^{-1} се целобројни матрици. Тогаш

$$\{a\alpha, a\alpha\alpha_n\} = \{1,\alpha_n\}\begin{bmatrix} r_n & s_n \\ t_n & u_n \end{bmatrix} = \{r_n + t_n\alpha_n, s_n + u_n\alpha_n\},$$

па затоа

$$a\alpha = r_n + t_n\alpha_n,\ a\alpha\alpha_n = s_n + u_n\alpha_n \tag{8}$$

Ако во равенствата (8) го елиминираме $a\alpha$ добиваме

$$t_n\alpha_n^2 + (r_n - u_n)\alpha_n - s_n = 0\,.$$

Значи, α_n е решение на квадратна равенка со коефициент пред квадратиот член $t_n \neq 0$. Имено, ако $t_n = 0$, тогаш од (8) следува дека $\alpha = \frac{r_n}{a}$ е рационален број, што е противречност.

Според тоа, за секоја матрица $M_nBM_n^{-1}$ постојат само два можни избори за бројот α_n и затоа ако множеството од матрици $M_nBM_n^{-1}$, $n = 0,1,\ldots$ е конечно, тогаш такво е и множеството од броевите $\alpha_n, n = 0,1,\ldots$, па затоа мора да постојат броеви m, n такви што $m \neq n$ и $\alpha_n = \alpha_m$. Тогаш верижната дропка со која го претставуваме бројот α е периодична. Така, доволно е да докажеме дека множеството матрици $M_nBM_n^{-1}$ е конечно. Нека

$$\vartheta = |a\alpha| + 4(1 + |\alpha|)\,\|B - a\alpha\|\,. \tag{9}$$

и да земеме $k = [\vartheta]$. Забележуваме дека бројот ϑ не зависи од бројот *n*. Сакаме да докажеме дека за секој $n \geq 2$ важи $\|M_nBM_n^{-1}\| \leq \vartheta$. Тогаш од дефиниција 8.6 ќе следува дека броевите r_n, s_n, b_n, u_n се меѓу $-\vartheta$ и ϑ, што значи дека за секој број постојат $(2k+1)-$ на можност и затоа имаме $(2k+1)^4$ можности за матриците $M_nBM_n^{-1}$, $n \geq 2$, т.е. ова множество матрици е конечно. Значи, доволно е да докажеме дека за секој $n \geq 2$ важи $\|M_nBM_n^{-1}\| \leq \vartheta$.

Нека

$$F_n = \begin{bmatrix} 0 & p_{n-2} - q_{n-2}\alpha \\ 0 & p_{n-1} - q_{n-1}\alpha \end{bmatrix}.$$

Според последицата 5.11 имаме

$$|q_{n-2}\alpha - p_{n-2}| \leq \frac{1}{q_{n-1}} \text{ за } n \geq 2 \text{ и } |q_{n-1}\alpha - p_{n-1}| \leq \frac{1}{q_n} < \frac{1}{q_{n-1}}\,.$$

Затоа

$$\|F_n\| \leq \frac{1}{q_{n-1}}\ . \tag{10}$$

Понатаму имаме

$$\begin{aligned} M_n &= \begin{bmatrix} q_{n-2} & p_{n-2} \\ q_{n-1} & p_{n-1} \end{bmatrix} = \begin{bmatrix} q_{n-2} & q_{n-2}\alpha \\ q_{n-1} & q_{n-1}\alpha \end{bmatrix} + \begin{bmatrix} 0 & p_{n-2} - q_{n-2}\alpha \\ 0 & p_{n-1} - q_{n-1}\alpha \end{bmatrix} \\ &= \begin{bmatrix} q_{n-2} & 0 \\ 0 & q_{n-1} \end{bmatrix} \begin{bmatrix} 1 & \alpha \\ 1 & \alpha \end{bmatrix} + F_n. \end{aligned} \tag{11}$$

Сега, ако се искористат (7), (10) и (11) добиваме

$$\begin{aligned} M_nB &= \begin{bmatrix} q_{n-2} & 0 \\ 0 & q_{n-1} \end{bmatrix}\begin{bmatrix} 1 & \alpha \\ 1 & \alpha \end{bmatrix}B + F_nB \\ &= \begin{bmatrix} q_{n-2} & 0 \\ 0 & q_{n-1} \end{bmatrix}a\alpha\begin{bmatrix} 1 & \alpha \\ 1 & \alpha \end{bmatrix} + F_nB \\ &= a\alpha\begin{bmatrix} q_{n-2} & 0 \\ 0 & q_{n-1} \end{bmatrix}\begin{bmatrix} 1 & \alpha \\ 1 & \alpha \end{bmatrix} + F_nB \\ &= a\alpha(M_n - F_n) + F_n \\ &= a\alpha M_n + F_n(B - a\alpha E). \end{aligned}$$

Затоа

$$M_nBM_n^{-1} = a\alpha M_nM_n^{-1} + F_n\ (B - a\alpha E)M_n^{-1} = a\alpha E + F_n(B - a\alpha E)M_n^{-1}.$$

Но, тогаш од лемата 8.7 добиваме

$$\begin{aligned} \| M_nBM_n^{-1} \| &\leq \| a\alpha E \| + \| F_n(B - a\alpha E)M_n^{-1} \| \\ &\leq |a\alpha| + 4\| F_n \| \cdot \| B - a\alpha E \| \cdot \| M_n^{-1} \| \end{aligned} \tag{12}$$

Останува да ја определиме $\| M_n^{-1} \|$. Бидејќи

$$M_n^{-1} = (-1)^n\begin{bmatrix} p_{n-1} & -p_{n-2} \\ -q_{n-1} & q_{n-2} \end{bmatrix}$$

и за секој j важи

$$|p_j| \leq \alpha q_j| + |p_j - \alpha q_j| \leq \alpha|q_j + \tfrac{1}{q_{j+1}} \leq \alpha|q_j + q_j = q_j(1+|\alpha|)\ ,$$

добиваме

$$\begin{aligned} &|p_{n-2}| \leq q_{n-2}(1+|\alpha|) < q_{n-1}(1+|\alpha|), \\ &p_{n-1} < q_{n-1}(1+|\alpha|). \end{aligned}$$

Затоа, $\| M_n^{-1} \| \leq q_{n-1}(1+|\alpha|)$, односно од (12) следува

$$\begin{aligned} \| M_nBM_n^{-1} | &\leq |a\alpha| + 4\| F_n \| \cdot \| B - a\alpha E \| \cdot \| M_n^{-1} \| \\ &\leq |a\alpha| + 4 \cdot \tfrac{1}{q_{j+1}} \cdot \| B - a\alpha E \| \cdot q_{n-1}(1+|\alpha|) \\ &= |a\alpha| + 4(1+|\alpha|) \cdot \| B - a\alpha E \| = 9. \ \blacksquare \end{aligned}$$

8.9. Следната теорема се однесува на природните броеви кои не се точни квадрати и истата ќе ја презентираме без доказ.

Теорема. Ако природниот број N не е точен квадрат, тогаш $\sqrt{N}$ може да се претстави како периодична верижна дропка од облик

$\sqrt{N} = \langle a_0; \overline{a_1, a_2, \ldots, a_{n-1}, 2a_0} \rangle$, каде $a_0 = [\sqrt{N}]$.

За секој n важи $a_n \leq 2a_0$, при што $a_n = 2a_0$ ако и само ако

$$p_{n-1}^2 - Nq_{n-1}^2 = (-1)^n\ . \ \blacksquare$$

8.10. Пример. Бројот $\sqrt{69}$ претставете го како периодична верижна дропка.

Решение. Ако се искористи алгоритмот (2) од точка 7 последователно добиваме

$$a_0=[\sqrt{69}]=8 \text{ и } \alpha_1=\frac{1}{\sqrt{69}-8}=\frac{\sqrt{69}+8}{5},$$

$$a_1=[\alpha_1]=3 \text{ и } \alpha_2=\frac{1}{\frac{\sqrt{69}+8}{5}-3}=\frac{5}{\sqrt{69}-7}=\frac{\sqrt{69}+7}{4},$$

$$a_2=[\alpha_2]=3 \text{ и } \alpha_3=\frac{1}{\frac{\sqrt{69}+7}{4}-3}=\frac{\sqrt{69}+5}{11},$$

$$a_3=[\alpha_3]=1 \text{ и } \alpha_4=\frac{1}{\frac{\sqrt{69}+5}{11}-1}=\frac{\sqrt{69}+6}{3},$$

$$a_4=[\alpha_4]=4 \text{ и } \alpha_5=\frac{1}{\frac{\sqrt{69}+6}{3}-4}=\frac{\sqrt{69}+6}{11},$$

$$a_5=[\alpha_5]=1 \text{ и } \alpha_6=\frac{1}{\frac{\sqrt{69}+6}{11}-1}=\frac{\sqrt{69}+5}{4},$$

$$a_6=[\alpha_6]=3 \text{ и } \alpha_7=\frac{1}{\frac{\sqrt{69}+5}{4}-3}=\frac{\sqrt{69}+7}{5},$$

$$a_7=[\alpha_7]=3 \text{ и } \alpha_8=\frac{1}{\frac{\sqrt{69}+7}{5}-3}=\sqrt{69}+8,$$

$$a_8=[\alpha_8]=16 \text{ и } \alpha_9=\frac{1}{\sqrt{69}+8-16}=\frac{\sqrt{69}+8}{5},$$

Бидејќи $\alpha_1=\alpha_9=\frac{\sqrt{69}+8}{5}$, од теоремата 8.9 следува $\sqrt{69}=\langle 8;\overline{3,3,1,4,1,3,3,16}\rangle$. ■

8.11. Теорема. *i*) Ако $N=a^2+1,\ a\in\mathbb{N}$, тогаш $\sqrt{N}=\langle a;\overline{2a}\rangle$,

ii) Ако $N=a^2+2,\ a\in\mathbb{N}$, тогаш $\sqrt{N}=\langle a;\overline{a,2a}\rangle$.

Доказ. Бидејќи претставувањето на $\sqrt{N}$ како верижна дропка $\langle a_0;a_1,a_2,...\rangle$, $a_i\in\mathbb{N}, i\geq 1$ и $a_0\in\mathbb{N}_0$ е еднозначно, доволно е да ги пресметаме вредностите на верижните дропки $\langle a;\overline{2a}\rangle$ и $\sqrt{N}=\langle a;\overline{a,2a}\rangle$ и да докажеме дека нивните вредности се $\sqrt{a^2+1}$ и $\sqrt{a^2+2}$, соодветно.

i) Нека $x=\langle a;\overline{2a}\rangle$. Тогаш $x=a+\frac{1}{a+x}$, т.е. $x^2-a^2=1$ или $x=\pm\sqrt{a^2+1}$. Но, како вредноста на верижната дропка е позитивна, добиваме $x=\sqrt{a^2+1}$.

ii) Нека $x=\langle a;\overline{a,2a}\rangle$. Тогаш $x=a+\frac{a+x}{a^2+ax+1}$, т.е. $x=\pm\sqrt{a^2+2}$. Но, вредноста на верижната дропка $\langle a;\overline{a,2a}\rangle$ е позитивна, па затоа $x=\sqrt{a^2+2}$. ■

8.12. Пример. Броевите $\sqrt{17}$ и $\sqrt{27}$ претстави ги како периодични верижни дропки.

Решение. Бидејќи $17=4^2+1$ имаме $a=4$. Според теорема 8.11 *i*) добиваме $\sqrt{17}=\langle 4;\overline{8}\rangle$.

Од $27=5^2+2$ имаме $a=5$ и од теоремата 8.11 *ii*) следува $\sqrt{27}=\langle 5;\overline{5,10}\rangle$. ■

9. ВЕРИЖНИ ДРОПКИ И КВАДРАТНИ ОСТАТОЦИ

9.1. Да се вратиме на алгоритамот (2) од точката 7. Имено, ако $\alpha_0=\sqrt{N}$ и N не е точен квадрат, тогаш

$$a_0=[\sqrt{N}] \text{ и } \alpha_1=\frac{1}{\sqrt{N}-a_0}=\frac{\sqrt{N}+a_0}{N-a_0^2}=\frac{\sqrt{N}+A_1}{B_1}=a_1+\frac{\sqrt{N}-A_2}{B_1},$$

каде

$$a_1=[\alpha_1],\ A_2=a_1B_1-A_1,\ B_0=1,\ B_1=N-A_1^2 \text{ и } A_1=a_0.$$

Продолжувајќи ја постапката добиваме

$$\alpha_i=\frac{B_{i-1}}{\sqrt{N}-A_i}=\frac{\sqrt{N}+A_i}{B_i}=a_i+\frac{\sqrt{N}-A_{i+1}}{B_i}, \tag{1}$$

каде

$$a_i=[\alpha_i]=[\frac{\sqrt{N}+A_i}{B_i}],\ A_{i+1}=a_iB_i-A_i. \tag{2}$$

9.2. Лема. Ако $A_i,B_i,i=1,2,\ldots$ се зададени со (1) и (2) и N не е точен квадрат, тогаш $A_i<\sqrt{N}$ и $B_i<2\sqrt{N}$, $i=1,2,\ldots$.

Доказ. На почетокот ќе покажеме дека

$$B_i=\frac{N-A_i^2}{B_{i-1}},\ i=1,2,\ldots \tag{3}$$

е цел број. Од $A_1=a_0=[\sqrt{N}],\ B_0=1$ и $B_1=N-A_1^2$ следува дека тврдењето важи за $i=0,1$. Нека претпоставиме дека $B_i=\frac{N-A_i^2}{B_{i-1}}$ е цел број, т.е. $B_i \mid N-A_i^2$. Притоа имаме

$$B_{i+1}=\frac{N-A_{i+1}^2}{B_i}=\frac{N-(a_iB_i-A_i)^2}{B_i}=\frac{N-A_i^2}{B_i}-a_i^2B_i+2a_iA_i$$

т.е. B_{i+1} е цел број.

Бидејќи $a_i=[\frac{\sqrt{N}+A_i}{B_i}]$, лесно се гледа дека $A_i<\sqrt{N}$. Но, тогаш

$$B_i = \frac{A_{i+1}+A_i}{a_i} < \frac{2\sqrt{N}}{a_i} < 2\sqrt{N}\,. \blacksquare$$

9.3. Забелешка. Од теоремата 8.8 непосредно следува, дека ако N не е точен квадрат, тогаш $\sqrt{N}$ е периодична верижна дропка. Овој парцијален резултат на теоремата 8.8 е директна последица и на претходната лема. Имено, вкупниот број на различни дропки од облик $\frac{\sqrt{N}+A_i}{B_i}$ може да биде најмногу $[\sqrt{N}]\cdot[2\sqrt{N}] < 2N$. Тоа значи, дека после најмногу $2N$ чекори ќе имаме повторување на некоја дропка $\frac{\sqrt{N}+A_i}{B_i}$, што според (1) и (2) значи периодичност на верижната дропка со која се претставува $\sqrt{N}$. Последното имплицира дека максимална можна должина на периодот е $2N-1$. Меѓутоа оваа максимална можна должина на периодот никогаш не се достигнува бидејќи бројот на можни комбинации на A_i и B_i е ограничен исто така со условот дека B_{i+1} е делител на $N-A_i^2$.

9.4. Лема. Ако $\frac{p_n}{q_n}$ е $n-$тиот конвергент од претставувањето на $\sqrt{N}$ како обична верижна дропка, а α_n и B_n се дефинирани со (1), (2) и (3), тогаш

$$p_{n-1}^2 - Nq_{n-1}^2 = (-1)^n B_n \text{ , за секој } n \geq 0\,. \tag{4}$$

Доказ. Од $\sqrt{N} = \langle a_0; a_1, a_2, \ldots, a_{n-1}, \alpha_n \rangle$ имаме $\sqrt{N} = \frac{p_{n-2}+\alpha_n p_{n-1}}{q_{n-2}+\alpha_n q_{n-1}}$ и ако заменине $\alpha_n = \frac{\sqrt{N}+A_n}{B_n}$ добиваме

$$\sqrt{N} = \frac{B_n p_{n-2}+A_n p_{n-1}+p_{n-1}\sqrt{N}}{B_n q_{n-2}+A_n q_{n-1}+q_{n-1}\sqrt{N}}$$

односно

$$(B_n q_{n-2} + A_n q_{n-1})\sqrt{N} + Nq_{n-1} = B_n p_{n-2} + A_n p_{n-1} + p_{n-1}\sqrt{N}\,.$$

Но, N не е точен квадрат, па затоа $\sqrt{N}$ е ирационален број, т.е.

$$\begin{cases} B_n q_{n-2} + A_n q_{n-1} = p_{n-1} \\ B_n p_{n-2} + A_n p_{n-1} = Nq_{n-1} \end{cases} \tag{5}$$

Од системот (5) го елиминираме A_n и добиваме

$$(p_{n-1}q_{n-2} - q_{n-1}p_{n-2})B_n = p_{n-1}^2 - Nq_{n-1}^2\,,$$

односно

$$p_{n-1}^2 - Nq_{n-1}^2 = (-1)^n B_n\,. \blacksquare$$

9.5. Од (4) имаме

$$p_{n-1}^2 \equiv (-1)^n B_n (\mathrm{mod}\, N) \tag{6}$$

и затоа $(-1)^n B_n$ е квадратен остаток по модул N. Во лемата 9.2 докажавме дека $B_n < 2\sqrt{N}$. Според тоа, претставувањето на $\sqrt{N}$ како обична верижна дропка ни овозможува брзо да ги пресметаме повеќето од најмалите квадратни остатоци по модул N. Методот е особено брз бидејќи сите B_i се помали од $2\sqrt{N}$, а особено е погоден за доста големи вредности на N.

10. АЛГЕБАРСКИ И ТРАНСЦЕДЕНТНИ БРОЕВИ

10.1. Дефиниција. За комплексниот (специјално, реалниот) број α ќе велиме дека е *алгебарски* ако постои неконстантен полином P со рационални коефициенти таков што $P(\alpha) = 0$. Ако таков полином за бројот α не постои, тогаш за α ќе велиме дека е *трансцендентен број*.

10.2. Бидејќи од $P(\alpha) = 0$ следува $P(\alpha)Q(\alpha) = 0$ за произволен полином $Q(x)$ со рационални коефициенти, јасно е дека за секој алгебарски број α постојат бесконечно многу полиноми со рационални коефициенти чиј корен е α. Од сите овие полиноми најчесто се разгледува полиномот со најмал степен. Така ја имаме следнава дефиниција.

Дефиниција. *Минимален полином* на алгебарскиот број α е полиномот со рационални коефициенти со најмал степен чиј корен е бројот α. Степенот на минималниот полином на алгебарскиот број α го нарекуваме *степен* на α.

10.3. Теорема. а) Минималниот полином P_α на алгебарскиот број α е единствен до производ со константа.

б) Полиномот P_α е неразложлив над $\mathbb{Q}$, што значи дека P_α нема повеќекратни нули.

в) Ако $Q(x)$ е полином со рационални коефициенти таков што $Q(\alpha) = 0$, тогаш полиномот Q е делив со минималниот полином P.

Доказ. а) Ако α има два различни монични (коефициентот пред највисокиот степен е 1) минимални полиноми P_1 и P_2 со степен n, тогаш полиномот $P_1 - P_2$ има степен помал од n и ќе се анулира во α, што противречи на минималноста на n.

б) Ако P_α е разложлив во $\mathbb{Q}$, тогаш некој негов делител ќе се анулира за α, што противречи на фактот дека P_α е минимален полином.

в) Нека R е остатокот при делењето на полиномот P со полиномот Q. Според тоа, полиномот R се анулира во α и има степен помал од степенот на минималниот полином, па затоа мора да е $R \equiv 0$. ■

10.4. Теорема (Луивил). За секој реален алгебарски број α со степен $n \geq 2$ постои позитивна константа c таква што за секој рационален број $\frac{p}{q}$ важи

$$|\alpha - \tfrac{p}{q}| \geq \tfrac{c}{q^n}.$$

Доказ. Нека α е реален алгебарски број со степен $n \geq 2$. Според теоремата 10.3 а) α е корен на полином

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0,$$

со целобројни коефициенти ($a_n \neq 0$, $n \geq 2$). Тогаш $P(x) = (x-\alpha)Q(x)$, каде $Q(x)$ е полином од $(n-1)-$ви степен со реални коефициенти. Нека $\frac{p}{q}$ е произволен рационален број. Овој број не може да се корен на полиномот $P(x)$, бидејќи во спротивно равенката $P(x) = 0$ можеме да ја поделиме со $x - \frac{p}{q}$ и α ќе биде корен на полином со рационални коефициенти со степен помал од n, што противречи на фактот дека степенот на α е n. Затоа важи

$$|P(\tfrac{p}{q})| = \tfrac{|a_n p^n + a_{n-1} p^{n-1} q + \ldots + a_0 q^n|}{q^n} \neq 0. \qquad (1)$$

Броителот на десната страна во (1) е ненегативен цел број различен од 0, па затоа тој е поголем или еднаков на 1. Според тоа,

$$|P(\tfrac{p}{q})| \geq \tfrac{1}{q^n}, \text{ т.е. } |\tfrac{p}{q} - \alpha| \cdot |Q(\tfrac{p}{q})| \geq \tfrac{1}{q^n}.$$

Ќе разгледаме два случаја.

1) $\frac{p}{q} \in [\alpha - 1, \alpha + 1] = A$. Функцијата $|Q(x)|$ е непрекината на затворениот интервал A, што значи дека постои $\max_{x \in A} |Q(x)| = K < +\infty$. Затоа важи

$$\tfrac{1}{q^n} \leq |\tfrac{p}{q} - \alpha| \cdot |Q(\tfrac{p}{q})| \leq K |\tfrac{p}{q} - \alpha|,$$

т.е.

$$|\alpha - \tfrac{p}{q}| \geq \tfrac{\frac{1}{K}}{q^n}.$$

2) $\frac{p}{q} \in A$. Тогаш $|\alpha - \frac{p}{q}| > 1$ и како q е природен број добиваме $|\alpha - \frac{p}{q}| \geq \frac{1}{q^n}$.

Сега очигледно е дека доволно е да земеме $c = \min\{\frac{1}{K}, 1\}$. ■

10.5. Последица. Ако за секој $c>0$ и за секој $n\in\mathbb{N}$ постои рационален број $\frac{p}{q}\neq\alpha$ таков што

$$|\alpha-\frac{p}{q}|<\frac{c}{q^n},$$

тогаш α е трансцендентен број.

Доказ. Непосредно следува од теоремата 10.4. ■

10.6. Пример. Луивиловиот број

$$L=\frac{1}{10^{1!}}+\frac{1}{10^{2!}}+\frac{1}{10^{3!}}+\ldots=0{,}11000100\ldots010\ldots$$

е трансцедентен.

Навистина, нека $n\in\mathbb{N}$ и $c>0$ се произволни. За броевите

$$p=10^{k!}(\frac{1}{10^{1!}}+\frac{1}{10^{2!}}+\ldots+\frac{1}{10^{k!}})\ \text{ и }\ q=10^{k!}$$

важи

$$\begin{aligned}|L-\frac{p}{q}|&=\frac{1}{10^{(k+1)!}}+\frac{1}{10^{(k+2)!}}+\ldots\\&<\frac{1}{10^{(k+1)!}}(1+\frac{1}{2}+\frac{1}{2^2}+\ldots)\\&=\frac{2}{10^{k!}}\cdot\frac{1}{10^{k!k}}.\end{aligned}$$

Избираме k така што важи $k>n$ и $\frac{2}{10^{k!}}<c$. Тогаш

$$|L-\frac{p}{q}|<\frac{c}{(10^{k!})^k}<\frac{c}{q^n},$$

па од последицата 10.5 следува дека L е трансцедентен број. ■

10.7. Коментар. Претходно споменавме дека броевите e и π се ирационални, при што тоа го докажавме за бројот e. Овде ќе спомнеме дека овие два броја се и трансцедентни. Трансцедентноста на бројот e прв ја докажал Ермит во 1873 година, а додека доказот дека бројот π е трансцедентен прв го дал Линдеман во 1882 година. Со докажувањето дека бројот π е транцедентен, конечно се решил повеќевековниот проблем за квадратура на кругот, т.е. е докажано дека не е можно служејќи се само со линијар и шестар да се конструира квадрат чија плоштина е еднаква на плоштината на даден круг.

10.8. Лема. Бројот e е трансцендетен.

Доказ. Нека го претпоставиме спротивното, т.е. дека постојат цели броеви a_0, $a_1,\ldots,a_n$ такви што

$$a_0+a_1e+\ldots+a_ne^n=0. \tag{2}$$

Нека $M=\max\limits_{0\le k\le n}|a_k|$. Да земеме доволно голем прост број p (покасно ќе видиме

што всушност значи доволно голем број, за сега да претпоставиме дека $p > n$ и $p > |a_0|$) и да го разгледаме полиномот

$$f(x) = \frac{x^{p-1}}{(p-1)!}(x-1)^p(x-2)^p...(x-n)^p .$$

За овој полином, со помош на парцијална интеграција наоѓаме

$$\begin{aligned}\int_0^x e^{x-t} f(t)dt &= -f(x) + e^x f(0) + \int_0^x e^{x-t} f'(t)dt \\ &= -[f(x) + f'(x)] + e^x[f(0) + f'(0)] + \int_0^x e^{x-t} f''(t)dt \\ &= ... = -[f(x) + f'(x) + ...] + e^x[f(0) + f'(0) + ...] \\ &= -F(x) + e^x F(0),\end{aligned}$$

каде конечниот збир $f(x) + f'(x) + ...$ е означен со $F(x)$. Во добиената релација последователно ставаме $x = k = 0,1,...,n$ и добиените релации ги множиме последователно со a_k. Ако потоа ги собереме и ја искористиме (2), добиваме

$$\begin{aligned}\sum_{k=0}^{n} a_k \int_0^k e^{k-t} f(t)dt &= -[a_0F(0) + a_1F(1) + ... + a_nF(n)] + F(0)[a_0 + a_1e + ... + a_ne^n] \\ &= -[a_0F(0) + a_1F(1) + ... + a_nF(n)] = R.\end{aligned} \tag{3}$$

Да ги оцениме изразите на двете страни на (3). Ако го развиеме $f(x)$ добиваме

$$f(x) = \frac{1}{(p-1)!}(A_{p-1}x^{p-1} + A_p x^p + A_{p+1}x^{p+1} + ...),\ A_i \in \mathbb{Z}$$

при што $f(0) = f'(0) = ... = f^{(p-2)}(0) = 0,\ f^{(p-1)}(0) = A_{p-1} = (-1)^{np}(n!)^p$ и не е делив со p (бидејќи p е прост број и е поголем од n), а сите натамошни изводи $f^{(p)}(0), f^{(p+1)}(0),...$ се деливи со p (на пример, $f^{(p)}(0) = pA_p$). Затоа $F(0)$ не е делив со p, а како $p > |a_0|$, добиваме дека и $a_0F(0)$ не е делив со p.

Со аналогна постапка се докажува дека $p \mid F(k)$ за секој $k = 1,2,...,n$, па затоа $|R| = |a_0F(0) + a_1F(1) + ... + a_nF(n)|$ не е делив со p. Но, R е цел број, па како не е делив со p тој не е еднаков на нула, т.е. $|R| \geq 1$.

Од друга страна, во секој од интегралите на левата страна на равенството (3) за променливата t важи $t \in [0,n]$, па затоа

$$|f(t)| = \frac{t^{p-1}}{(p-1)!}|(t-1)^p(t-2)^p...(t-n)^p| \leq \frac{n^{p-1}n^{np}}{(p-1)!},$$

од каде следува

$$\left|\int_0^k e^{k-t} f(t)dt\right| < e^n \frac{n^{(n+1)p}}{(p-1)!},$$

што значи

$$|R| \le M(n+1)e^n \frac{n^{(n+1)p}}{(p-1)!}.$$

Но, $\lim_{q\to\infty} M(n+1)e^n \frac{n^{(n+1)q}}{(q-1)!} = 0$, па затоа простиот број p може да се избере така што (покрај досегашните барања) го задоволува и условот $M(n+1)e^n \frac{n^{(n+1)p}}{(p-1)!} < \frac{1}{2}$, односно $|R| < \frac{1}{2}$. Но последното противречи на оценката $|R| \ge 1$ и од добиената противречност следува дека бројот e е трансцедентен. ■

10.9. На крајот од овој дел ќе презентираме уште една теорема, која всушност е подобрување на теоремата на Луивил и чиј доказ излегува од рамките на нашите разгледувања. Всушност следнава теорема е најдобар резултат во теоријата на Диофантовите апроксимации.

Теорема (Рот). Нека α е реален алгебарски број со степен $n \ge 2$. Тогаш за секој $\varepsilon > 0$ неравенката

$$|\alpha - \frac{p}{q}| \ge \frac{1}{q^{2+\varepsilon}}$$

има само конечно многу решенија по $p \in \mathbb{Z}$ и $q \in \mathbb{N}$. □

VIII ГЛАВА
ДИОФАНТОВИ РАВЕНКИ

1. ЛИНЕАРНА ДИОФАНТОВА РАВЕНКА

1.1. Дефиниција. Нека $a,b,c\in\mathbb{Z}$ и $ab\neq 0$. Линеарната равенка од видот

$$ax+by=c, \tag{1}$$

чии решенија (x,y) се подредени парови цели броеви ја нарекуваме *линеарна Диофантова равенка со две непознати*.

Нека $a_1,a_2,...,a_n,c\in\mathbb{Z}$ и $a_1a_2...a_n\neq 0$. Линераната равенка од видот

$$a_1x_1+a_2x_2+...+a_nx_n=c \tag{2}$$

чии решенија $(x_1,x_2,...,x_n)$ се подредени $n-$торки цели броеви ја нарекуваме *линеарна Диофантова равенка со* n *непознати*.

1.2. Секоја линеарна равенка со две променливи и целобројни коефициенти можеме да ја сведиме на равенка од облик (1).

а) Во теоремата I 4.4 (теорема на Безу) докажавме дека ако $c=(a,b)$, тогаш оваа равенка има решение во множеството $\mathbb{Z}$. Притоа за определување на броевите x и y може да се користи, на пример, Евклидовиот алгоритам.

б) Ако бројот c не е делив со $d=(a,b)$ тогаш равенката нема целобројни решенија бидејќи левата страна е делива со d, а десната не е делива со d.

б) Ако $d\mid c$, тогаш равенката $ax+by=c$ има решение $x_1=\frac{c}{d}x_0$, $y_1=\frac{c}{d}y_0$, при што парот (x_0,y_0) е решение на равенката $ax+by=d$. Но, во овој случај дадената равенка има бесконечно многу решенија. Имено, ако претпоставиме дека (t_1,t_2) е произволен подреден пар цели броеви кој е решение на равенката $ax+by=c$, тогаш важи $at_1+bt_2=c$. Од друга страна имаме $ax_1+by_1=c$, па затоа

$$at_1+bt_2=ax_1+by_1, \text{ т.е. } \frac{a}{d}(t_1-x_1)+\frac{b}{d}(t_2-y_1)=0.$$

Бидејќи $(\frac{a}{d},\frac{b}{d})=1$, добиваме $\frac{b}{d}\mid(t_1-x_1)$ и $\frac{a}{d}\mid(t_2-y_1)$, од што непосредно следува

$$t_1=x_1+\frac{b}{d}k,\ t_2=y_1-\frac{a}{d}k,\ k\in\mathbb{Z}.$$

Понатаму, (t_1,t_2), $k\in\mathbb{Z}$ ја задоволува равенката $ax+by=c$. Навистина,

$$\begin{aligned} at_1+bt_2 &= a(x_1+\tfrac{b}{d}k)+b(y_1-\tfrac{a}{d}k)=a(\tfrac{c}{d}x_0+\tfrac{b}{d}k)+b(\tfrac{c}{d}y_0-\tfrac{a}{d}k)\\ &= \tfrac{c}{d}(ax_0+by_0)=\tfrac{c}{d}d=c. \end{aligned}$$

Од досега изнесеното непосредно следува точноста на следната теорема.

Теорема. Линеарната Диофантова равенка (1) има решение ако и само ако $(a,b)=d\mid c$. Притоа, решението на равенката има облик

$$x=\frac{c}{d}x_0+\frac{b}{d}k,\ \ y=\frac{c}{d}y_0-\frac{a}{d}k, k\in\mathbb{Z},$$

при што (x_0,y_0) е решение на равенката (1) и тоа може да се добие со помош на Евклидовиот алгоритам. ■

1.3. Теорема. Линеарната Диофантова равенка (2) има решение ако и само ако и само ако $(a_1,a_2,...,a_n)\mid c$. Притоа, ако равенката (2) има барем едно решение, тогаш таа има бесконечно многу решенија.

Доказ. Јасно, ако равенката (2) има решение, тогаш $(a_1,a_2,...,a_n)\mid c$.

Со математичка индукција ќе докажеме дека ако $(a_1,a_2,...,a_n)\mid c$, тогаш равенката (2) има бесконечно многу решенија. За $n=2$ тврдењето следува од теоремата 1.2. Нека пртпоставиме дека тврдењето важи за равенка со $n-1$ непозната. Нека $d=(a_{n-1},a_n)$. Според претпоставката равенката

$$a_1x_1+...+a_{n-2}x_{n-2}+dy=c$$

има бесконечно многу решенија $(x_1,...,x_{n-2},d)$. За секое решение на оваа равенка ја разгледуваме равенката

$$a_{n-1}x_{n-1}+a_nx_n=dy.$$

Бидејќи $(a_{n-1},a_n)\mid dy$, од теоремата 1.2 следува дека последната равенка има бесконечно многу решенија (x_{n-1},x_n). Јасно, подредената $n-$торка $(x_1,x_2,...,x_n)$ е решение на (2) и нив ги има бесконечно многу. ■

1.4. Пример. Нека a и b се заемно прости броеви. Докажи дека равенката $ax+by=ab$ нема решение во множеството природни броеви.

Решение. Имаме $(a,b)=1$. Нека постојат природни броеви x и y такви што $ax+by=ab$. Јасно, $a\mid by$ и како $(a,b)=1$ добиваме дека $a\mid y$. Според тоа, $y\geq a$. Аналогно се покажува дека $b\mid x$, па затоа $x\geq b$. Значи,

$$ab=ax+by\geq ab+ab=2ab,$$

што е противречност. Конечно, од добиената противречност следува дека дадената равенка нема решение во множеството природни броеви. ■

1.5. Пример. Нека a,b,c се по парови заемно прости природни броеви. Докажи дека $2abc-ab-bc-ca$ е најголем цел број кој не може да се претстави во облик $xbc+yac+zab$, каде x,y,z се ненегативни цели броеви.

Решение. Нека $n > 2abc - ab - bc - ca$ и нека $(x_0, y_0, z_0) \in \mathbb{N}_0 \times \mathbb{N}_0 \times \mathbb{N}_0$ е решение на равенката

$$xbc + yac + zab = n .$$

Според теоремата 1.3 такво решение секогаш постои за секој цел број n, бидејќи $(a,b) = (b,c) = (c,a) = 1$. Ќе докажеме дека можеме да избереме целобројно решение (x, y, z) на оваа равенка за кое $x \geq 0,\ y \geq 0, z \geq 0$. Имаме

$$bc(x - x_0) + ca(y - y_0) + ab(z - z_0) = 0 . \tag{3}$$

Бидејќи $(a,b) = (c,a) = 1$ добиваме $a \mid (x - x_0)$, т.е. $x - x_0 = as,\ s \in \mathbb{Z}$. Со замена во (3) добиваме

$$bcs + c(y - y_0) + b(z - z_0) = 0 . \tag{4}$$

Но, $(b,c) = 1$, па затоа $b \mid (y - y_0)$, т.е. $y - y_0 = bt,\ t \in \mathbb{Z}$. Заменувајќи во (4) наоѓаме $cs + ct + z - z_0 = 0,$ т.е. $z - z_0 = -c(s + t)$. Јасно, секоја тројка $(x_0 + as, y_0 + bt,$ $z_0 - c(s + t))$, s и t се произволни, е решение на дадената равенка.

Во релациите $x = x_0 + as$, $y = y_0 + bt$, $z = z_0 - c(s + t)$ броевите s и t можеме да ги избереме така што $0 \leq x \leq a - 1$ и $0 \leq y \leq b - 1$. Тогаш важи

$$abz = n - bcx - acy > (2abc - ab - bc - ca) - bc(a - 1) - ac(b - 1) = -ab .$$

Значи $z > -1$, т.е. $z \geq 0$.

Ќе докажеме дека $2abc - ab - bc - ca$ не можеме да го претставиме во облик $xbc + yac + zab$ каде x, y, z се ненегативни цели броеви. Да претпоставиме дека

$$2abc - ab - bc - ca = xbc + yac + zab, \text{ зџа } x, y, z \geq 0 .$$

Тогаш,

$$bc(x + 1) + ca(y + 1) + ab(z + 1) = 2abc ,$$

при што $x + 1 \geq 1,\ y + 1 \geq 1,\ z + 1 \geq 1$. Бидејќи $(a,b) = (b,c) = 1$, добиваме $a \mid (x + 1)$, односно $a \leq x + 1$. Слично имаме $b \leq y + 1$ и $c \leq z + 1$. Но, тоа значи

$$3abc \leq bc(x + 1) + ca(y + 1) + ab(z + 1) = 2abc ,$$

што е противречност. ■

2. ПИТАГОРОВИ ТРОЈКИ

2.1. Дефиниција. Решенијата на равенката

$$x^2 + y^2 = z^2 \tag{1}$$

$x, y, z \in \mathbb{N}$, ги нарекуваме *Питагорови тројки*. За Питагоровата тројка (x, y, z) ќе велиме дека е *примитивна* ако $(x, y, z) = 1$.

2.2. Коментар. а) Ако за Питагоровата тројка (x,y,z) важи $d=(x,y,z)>1$, тогаш $(\frac{x}{d},\frac{y}{d},\frac{z}{d})$ е примитивна Питагорова тројка. Според тоа, за да ги определиме решенијата на равенката (1), доволно е да ги определиме само примитивните тројки (x,y,z). Останатите решенија се од облик $(kx,ky,kz), k\in\mathbb{N}$.

б) За секоја Питагорова тројка (x,y,z) броевите x,y се должини на катети, а z е должина на хипотенуза на правоаголен триаголник. Ваквиот триаголник го нарекуваме Питагоров триаголник.

2.3. Теорема. Во множеството природни броеви равенката (1) има бесконечно многу решенија (x,y,z) такви, што $(x,y,z)=1$ и истите се дадени со

$$x=u^2-v^2, y=2uv, z=u^2+v^2, \tag{2}$$

каде што $u,v\in\mathbb{N}$, $(u,v)=1$, $u>v$ и u и v се со различна парност.

Доказ. Од условот следува дека x е непарен, y е парен и z е непарен број. Затоа, $2|(x+z)$ и $2|(z-x)$. Според тоа

$$\tfrac{z+x}{2}\cdot\tfrac{z-x}{2}=(\tfrac{y}{2})^2 \tag{3}$$

каде $\frac{z+x}{2}, \frac{z-x}{2}$ и $\frac{y}{2}$ се природни броеви. Понатаму, $(x,z)=1$, бидејќи ако x и z имаат заеднички прост делител, тој е делител и на y, што противречи на $(x,y,z)=1$. Ако $d=(\frac{z+x}{2},\frac{z-x}{2})$, тогаш $d\mid z=\frac{z+x}{2}+\frac{z-x}{2}$ и $d\mid x=\frac{z+x}{2}-\frac{z-x}{2}$ и како $(x,z)=1$ добиваме дека $d=1$. Од (3) и од теоремата II 2.6 следува дека постојат u и v такви, што $\frac{z+x}{2}=u^2, \frac{z-x}{2}=v^2$. Според тоа, постојат u и v такви што важи (2). Ако $d\mid u$ и $d\mid v$, тогаш $d^2\mid x, d^2\mid y$ и $d^2\mid z$, т.е. $d^2=1$. Значи, $(u,v)=1$. Конечно, од $(x,y,z)=1$ следува дека u и v се со различна парност, а од $x>0$ следува дека $u>v$.

Обратно, нека u и v се такви што важи (2), каде што $u,v\in\mathbb{N}$, $(u,v)=1$, $u>v$ и u и v се со различна парност. Тогаш

$$.(u^2-v^2)^2+(2uv)^2=(u^2+v^2)^2.,$$

т.е. со (2) е дадено решение на (1). Сега, од $u>v$ следува дека $x>0, y>0, z>0$. Понатаму, ако p е прост број таков што $p\mid d_1=(u^2-v^2,2uv,u^2+v^2)$, тогаш $p\mid(u^2+v^2+2uv)$ и $p\mid(u^2+v^2-2uv)$. Според тоа, $p\mid(u+v)^2$ и $p\mid(u-v)^2$, па од теоремата II 2.2 следува дека $p\mid u+v$ и $p\mid u-v$. Тоа значи $p\mid 2u$ и $p\mid 2v$ и како $(u,v)=1$ добиваме дека $p=2$. Сега, u и v се со различна парност, па затоа u^2+v^2 е непарен број, што противречи на $2\mid(u^2+v^2)$. Од добиената противреч-

ност следува $d_1 = 1$, т.е. $(x, y, z) = 1$, што значи дека со (2) е дадено примитивно решение на (1). ■

2.4. Лема. Не постои Питагоров триаголник во кој хипотенузата и една катета се квадрати на природни броеви.

Доказ. Нека (x, y, z) е Питагорова тројка со најмала хипотенуза која го има бараното својство. Јасно, тројката (x, y, z) е примитивна. Нека $x = a^2$, $z = c^2$.

Ако y е парен, тогаш постојат $m, n \in \mathbb{N}$ такви што

$$a^2 = x = m^2 - n^2,\ y = 2mn,\ c^2 = z = m^2 + n^2.$$

Оттука следува $(ac)^2 = m^4 - n^4$, па во Питагоровата тројка (n^2, ac, m^2) хипотенузата е $m^2 < z$, што е противречност со минималноста на z.

Според тоа, y мора да е непарен што значи дека a е парен. Од

$$y^2 = c^4 - a^4 = (c^2 - a^2)(c^2 + a^2)$$

следува дека постојат природни броеви r, s такви што

$$c^2 - a^2 = r^2,\ c^2 + a^2 = s^2.$$

Оттука $2c^2 = r^2 + s^2$, т.е. $c^2 = (\frac{s+r}{2})^2 + (\frac{s-r}{2})^2$. Според тоа, постојат $m, n \in \mathbb{N}$ такви што

$$\tfrac{s \pm r}{2} = m^2 - n^2,\ \tfrac{s \mp r}{2} = 2mn,\ c = m^2 + n^2,$$

па затоа

$$2a^2 = s^2 - r^2 = 8mn(m-n)(m+n).$$

Бидејќи m и n се заемно прости броеви со различна парност, броевите $m, n, m+n$ и $m-n$ се по парови заемно прости. Затоа постојат $k, l, p, q \in \mathbb{N}$ такви што

$$m = k^2,\ \ n = l^2,\ \ m - n = p^2,\ \ m + n = q^2.$$

Оттука следува $k^4 - l^4 = (pq)^2$, па добивме Питагорова тројка (l^2, pq, k^2) со хипотенуза $k^2 = m < m^2 + n^2 = c < c^2 = z$, што повторно е противречност. ■

2.5. Последица. Не постои Питагоров триаголник чија плоштина е точен квадрат.

Доказ. Нека претпоставиме дека таков триаголник (x, y, z) постои. Тогаш $x^2 + y^2 = z^2$ и $xy = 2P$. Според претпоставката постои $u \in \mathbb{N}$ таков што $P = u^2$, односно $2xy = (2u)^2$. Затоа важи

$$z^2 + (2u)^2 = (x+y)^2,\ \ z^2 - (2u)^2 = (x-y)^2,$$

од каде добиваме

$$z^4 = (2u)^4 + (x^2 - y^2)^2,$$

т.е. добивме Питагоров триаголник во кој хипотенузата z^2 и катетата $(2u)^2$ се точни квадрати. Последното противречи на лемата 2.4. ■

2.6. Пример. Определи ги сите Питагорови тројки кои формираат:
а) аритметичка прогресија
б) геометриска прогресија

Решение. а) Нека $a = m^2 - n^2, b = 2mn, c = m^2 + n^2$ е примитивна Питагорова тројка. За истата да формира аритметичка прогресија потребно и доволно е да $2b = a + c$, односно $4mn = 2m^2$, од каде следува $m = 2n$. Значи, $a = 3n^2, b = 4n^2$ и $c = 5n^2$, односно $n^2 = 1$, од каде следува $n = 1$. Значи, тројката (3,4,5) е единствена примитивна тројка чии елементи формираат аритметичка прогресија, т.е. сите Питагорови тројки кои формираат аритметичка прогресија се дадени со $(3k, 4k, 5k), k \in \mathbb{N}$.

б) Ако примитивната тројка $a = m^2 - n^2, b = 2mn, c = m^2 + n^2$ формира геометриска прогресија, тогаш $b^2 = ac$, односно

$$4m^2n^2 = m^4 - n^4. \tag{4}$$

Во множеството природни броеви ќе ја решиме равенката (4). Јасно, m и n мора да се со иста парност. Ако $m = 2m_1, n = 2n_1$, тогаш со замена во (4) добиваме $4m_1^2n_1^2 = m_1^4 - n_1^4$, т.е. треба m_1 и n_1 да се со иста парност. Ако тие се парни во секој следен чекор, тогаш добиваме дека m и n треба бесконечно многу пати да се деливи со 2, а тоа е можно ако и само ако $m = n = 0$, што не е можно. Затоа, за некој k ќе важи $m_{k+1} = 2m_k + 1$ и $n_{k+1} = 2n_k + 1$, што значи

$$(2m_k + 1)^2(2n_k + 1)^2 = 2(m_k - n_k)(m_k + n_k + 1)(2m_k^2 + 2n_k^2 + 2m_k + 2n_k + 1),$$

што е противречност. Според тоа, не постои Питагорова тројка која формира геометриска прогресија. ■

2.7. Пример. Докажи дека ако радиусот на кружницата е непарен прост број, тогаш околу неа можат да се опишат точно два нескладни примитивни Питагорови триаголници.

Решение. Ако $a = m^2 - n^2, b = 2mn, c = m^2 + n^2$ е примитивна Питагорова тројка, тогаш радиусот на опишаната кружница на соодветниот триаголник е

$$r = n(m - n).$$

Ако r е непарен прост број p, тогаш можни се само следниве случаи

$$n = 1, m = p + 1, a = p(p + 2), b = 2(p + 1), c = p^2 + 2p + 1,$$

$$n = p,\ m = p+1,\ a = 2p+1,\ b = 2p(p+1),\ c = 2p^2+2p+2,$$

што значи дека околу кружницата може да се опишат точно два нескладни примитивни Питагорови триаголници. ■

2.8. Пример. Нека p,q и r се прости броеви и нека n е природен број таков што

$$p^n + q^n = r^2. \tag{5}$$

Докажи, дека $n=1$.

Решение. Јасно, еден трите броеви p,q и r е парен. Ако $r=2$, тогаш од равенството $p^n+q^n=4$ следува $p=q=2$ и $n=1$.

Нека $p>q=2$. Нека претпоставиме дека $n>1$ е непарен број. Сега равенството (5) можеме да го запишеме во обликот

$$(p+2)(p^{n-1}-2p^{n-2}+2^2p^{n-3}+\ldots-2^{n-2}p+2^{n-1}) = r^2.$$

Понатаму,

$$p^{n-1}-2p^{n-2}+\ldots-2^{n-2}p+2^{n-1} = 2^{n-1}+(p-2)(p^{n-2}+2^2p^{n-4}+\ldots+2^{n-3}p) > 1$$

и $p+2>1$, па затоа мора двата множители да се еднакви на r. Сега од (1) следува $p^n+2^n=(p+2)^2=p^2+4p+4$, што не е можно за $n\geq 3$.

Нека претпоставиме дека $n>1$ е парен број и нека $n=2m$. Сега равенството (5) можеме да го запишеме во обликот

$$(p^m)^2+(2^m)^2=r^2,$$

па од теоремата 2.3 следува дека

$$p^m = a^2-b^2,\ 2^m = 2ab \text{ и } r = a^2+b^2,$$

за некои природни броеви a и b такви што $(a,b)=1$. Затоа a и b се степени на бројот 2, т.е. $b=1$ и $a=2^{m-1}$. Значи, $p^m = 4^{m-1}-1<4^m$ и бидејќи p е прост број добиваме дека единствена можност е $p=3$. Но, тогаш $3^m=4^{m-1}-1$, што очигледно не е точно за $m=1,2,3,4$, а за $m\geq 5$ со индукција се докажува дека $4^{m-1}>3^m+1$.

Конечно, од претходните разгледувања следува дека $n=1$. Примери на тројки прости броеви кои го задоволуваат условот на задачата се

$$p=7,\ q=2,\ r=3;$$
$$p=23, q=2, r=5,$$
$$p=47, q=2, r=7\ .\ \blacksquare$$

3. МЕТОД НА ФЕРМА

3.1. При решавањето на Диофантовите равенки често пати се користиме со следниот метод на Ферма. Ако претпоставиме дека равенката има решение во множеството $\mathbb{N}$, тогаш докажуваме дека истата има „помало“ решение во множеството природни броеви. На тој начин конструираме строго монотоно опаѓачка бесконечна низа од природни броеви кои се решенија на дадената равенка, што противречи на фактот дека во $\mathbb{N}$ не постои строга монотона опаѓачка бесконечна низа. Последната противречност значи дека разгледуваната равенка нема решение. Да забележиме дека оваа постапка веќе ја применивме при решавање на пример 2.4 б).

3.2. Теорема. Равенката

$$x^4 + y^4 = z^2 \tag{1}$$

во множеството $\mathbb{Z}$ нема решение (x, y, z) такво што $x \neq 0,\ y \neq 0,\ z \neq 0$.

Доказ. Ако $x = x_0,\ y = y_0,\ z = z_0$ е решение на (1), тогаш и $x = |x_0|,\ y = |y_0|,\ z = |z_0|$ е решение на (1). Затоа доволно е тврдењето да го докажеме за природните броеви. Понатаму, можеме да претпоставиме дека $(x, y) = 1$. Навистина, ако $(x, y) = d$, тогаш $x = dx_1,\ y = dy_1$, т.е.

$$x_1^4 + y_1^4 = \left(\frac{z}{d^2}\right)^2,$$

што значи дека $z_1 = \frac{z}{d^2}$ е природен број. Но, тогаш

$$x_1^4 + y_1^4 = z_1^2,\ (x_1, y_1) = 1,\ x_1, y_1, z_1 \in \mathbb{N}.$$

Според тоа, повторно можеме да разгледуваме само примитивни решенија на равенката (1). Нека (x_1, y_1, z_1) е такво решение. Ќе докажеме дека постои решение (x_2, y_2, z_2) такво, што $(x_2, y_2) = 1,\ x_2, y_2, z_2 \in \mathbb{N}$ и $0 < z_2 < z_1$.

Од $(x_1^2)^2 + (y_1^2)^2 = z_1^2$ следува дека x_1^2, y_1^2, z_1 е примитивна Питагорова тројка. Според теоремата 2.3 постојат $u, v \in \mathbb{N}$, $u > v$ $(u, v) = 1$ такви, што

$$x_1^2 = u^2 - v^2,\ y_1^2 = 2uv,\ z_1 = u^2 + v^2. \tag{2}$$

Од (2) следува дека $x_1^2 + v^2 = u^2$ каде $(x_1, v, u) = 1$, па затоа (x_1, v, u) е примитивна Питагорова тројка. Можеме да претпоставиме, дека x_1 е непарен и затоа v е парен. Според тоа, u е непарен, па затоа постојат $a, b \in \mathbb{N}$ такви што

$$a^2 + b^2 = u,\ 2ab = v,\ (a, b) = 1. \tag{3}$$

Бидејќи u е непарен, v е парен и $(u, v) = 1$, добиваме $(u, 2v) = 1$. Според тоа, $y_1^2 = u \cdot 2v$ па затоа постојат $z_2, c \in \mathbb{N}$ такви што $u = z_2^2$, $2v = c^2$. Бидејќи c е парен број, имаме $c = 2d$, односно $v = 2d^2$. Така

$$ab = \frac{v}{2} = d^2.$$

Но, $(a,b)=1$, што значи дека постојат x_2 и y_2 такви, што

$$a = x_2^2, b = y_2^2 \text{ и } (x_2, y_2) = 1.$$

Со замена за a,b и u во (3) добиваме

$$x_2^4 + y_2^4 = z_2^2.$$

Значи, постојат $x_2, y_2, z_2 \in \mathbb{N}$, $(x_2, y_2)=1$ и

$$0 < z_2 \le z_2^4 = u^2 < u^2 + v^2 = z_1,$$

такви што подредената тројка (x_2, y_2, z_2) е решение на равенката (1).

Продолжувајќи ја постапката, во множеството шриродни броеви наоѓаме ново решение (x_3, y_3, z_3) на (1), за кое $(x_3, y_3)=1$ и $0 < z_3 < z_2$ итн. Според тоа, ако $\mathbb{N}$ равенката (1) има решение (x_1, y_1, z_1), тогаш таа има во $\mathbb{N}$ има бесконечно многу решенија $(x_i, y_i, z_i), i = 1,2,...$ за кои важи $z_1 > z_2 > z_3 > z_4 > z_5 > ...$, што не е можно. Од добиената противречност следува, дека не постојат решенија на (1), за кои $x \neq 0,\ y \neq 0,\ z \neq 0$. ■

3.3. Последица. Равенката $x^4 + y^4 = z^4$ нема решение во множеството на целите броеви, при што $x \neq 0,\ y \neq 0,\ z \neq 0$.

Доказ. Нека претпоставиме дека x_0, y_0, z_0 е решение на $x^4 + y^4 = z^4$ во множеството на целите броеви за кое $x_0 \neq 0, y_0 \neq 0, z_0 \neq 0$. Тогаш во множеството на целите броеви равенката (1) има решение $x_0 \neq 0, y_0 \neq 0,\ z_0^2 \neq 0$, што противречи на теоремата 3.2. ■

3.4. Равенката $x^4 + y^4 = z^4$ е специјален случај на таканаречената Голема теорема на Ферма која гласи: *Равенката $x^n + y^n = z^n$, каде $n \ge 3$ е природен број, нема решенија во множеството* $\mathbb{N}$.

Формулаијата на теоремата Ферма ја запишал на маргините на една Диофантова книга и допишал: „Најдов навистина извонреден доказ на ова тврдење, но оваа маргина е премногу тесна за да можам да го запишам доказот.“ На ова тврдење, запишано во средината на XVII век, многу големи научници потрошиле многу време и вложиле многу труд за да го докажат. Обидите да се докаже дале многу корисни резултати, особено во теоријата на алгебарските броеви. Самата теорема е докажана за многу посебни вредности на степенот n. За $n=3$ теоремата ја докажал Ојлер и доказот е многу потежок отколку доказот за $n=4$. Големата теорема на Ферма конечно во 1995 година ја докажал англискиот математичар Ендру Вајлс.

Интересно е да се напомене дека Ојлер, при обидите да ја докаже Големата теорема на Ферма, поставил хипотеза дека равенката

$$x^4 + y^4 + z^4 = w^4$$

нема решенија во множеството природни броеви. За ова тврдење долго време не се знаело дали е точно или не, сè додека Нам Елкис во 1988 година не нашол контрапример:

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4,$$

а покасно е најдено и помало решение

$$95800^4 + 217519^4 + 414560^4 = 422481^4.$$

Тоа значи дека и равенката

$$x^2 + y^2 + z^2 = w^2. \tag{4}$$

има решение. Логично се поставува прашањето дали последната равенка има конечно или бесконечно многу решение. Одгворот на ова прашање го дава следната теорема.

3.5. Нека претпоставиме дека $(x, y, z, w) = 1$ и дека $x, y, z, w \in \mathbb{N}$. Ако $w = 0$, тогаш $x = y = z = 0$. Ако еден од x, y, z е нула, тогаш останатите три броја формираат Питагорова тројка. Нека претпоставиме дека

$$w = x + y. \tag{5}$$

Тогаш (4) го добива обликот $z^2 = 2xy$. Според тоа, z е парен и имаме $z = 2u$, па затоа $2u^2 = xy$. Но, ова значи дека еден од броевите x или y е парен. Земаме x да е парен, т.е. $x = 2v$ и добиваме $u^2 = vy$. Според тоа, постојат $a, b \in \mathbb{N}$ такви, што $(a, v) = 1$ и

$$v = a^2, \ y = b^2. \tag{6}$$

Од (6) дека наоѓаме решение на равенката (4) се

$$x = 2a^2, y = b^2, z = 2ab, w = 2a^2 + b^2, \ a, b \in \mathbb{N}. \tag{7}$$

Значи, постојат бесконечно многу решенија на равенката (4) за кои $x \neq 0$, $y \neq 0$, $z \neq 0$ и $w \neq 0$. Што се однесува до определувањето на решенијата на равенката (4), може да се определи и друга класа на решенија за која $w \neq x + y$. Имено, нека претпоставиме дека две променливи од x, y, z се првиот пар на Питагорови тројки. Тогаш

$$t^2 + z^2 = x^2 + y^2 + z^2 = w^2,$$

па затоа x, y, t и t, z, w се Питагорови тројки. Според теоремата 3.2 можеме да претпоставиме дека тројките x, y, t и t, z, w се примитивни. Така имаме

$$x^2 + y^2 = t^2, t^2 + z^2 = w^2, \ (x, y, t) = (t, z, w) = 1, \ x, y, z, t, w \in \mathbb{N}. \tag{8}$$

Бидејќи x, y, t е примитивна Питагорова тројка t е непарен и без ограничување на општоста можеме да претпоставиме дека x е непарен, а y е парен број. Но, како t, z, w е примитивна Питагорова тројка и t е непарен број, па затоа z е парен и w е непарен број. Според теоремата 2.3 постојат $r, s, u, v \in \mathbb{N}$ такви што $(r,s) = (u,v) = 1$, $r > s, u > v$, при што r и s се со различна парност и u и v се со различна парност и

$$x = r^2 - s^2,\ y = 2rs,\ t = r^2 + s^2,$$
$$t = u^2 - v^2,\ z = 2uv,\ w = u^2 + v^2.$$

Притоа $t = r^2 + s^2 = u^2 - v^2$, односно $r^2 + s^2 + v^2 = u^2$, каде $r, s, u, v \in \mathbb{N}$. Исто така од $(r,s) = 1$ следува $(r,s,v,u) = 1$. Освен тоа,

$$u \le u^2 < u^2 + v^2 = w.$$

Така за секое решение на (4), кое е и решение на (8), имаме решение на (4) со помала последна променлива. Притоа да забележиме дека r и s не мора да се два члена на Питагорова тројка (r,s,α) и u и v не мора да се два члена на Питагорова тројка (α,v,u). Во спротивно добиваме дека равенката (4) нема решение (следува од методот на Ферма), а ние веќе докажавме дека (4) има бесконечно многу решенија.

Последната дискусија со Питагоровите тројки овозможува исто така да се определат бесконечно многу решенија на равенката (4). Имено, едно решение на (4) е

$$u = 3, v = 2, r = 2, s = 1, \text{ т.е. } 1^2 + 2^2 + 2^2 = 3^2.$$

Сега добиваме

$$x = 3, y = 4, t = 5,\ z = 12 \text{ и } w = 13,$$

дека е решение на (8). Земаме $u = 13$. Бидејќи v е парен број и $(u,v) = 1$ имаме $v = 12$ и како $r > s$ имаме $r = 4$ и $s = 3$. Но тогаш

$$x = 7, y = 24, t = 25, z = 312, w = 313,$$

е решение на (11). Земаме $u = 313$. Бидејќи v е парен број, имаме $v = 24$ и како $r > s$ имаме $r = 312$ и $s = 7$. Но, тогаш добиваме

$$x = 312^2 - 7^2,\ y = 2 \cdot 312 \cdot 7,\ t = 312^2 + 7^2,$$
$$z = 2 \cdot 312 \cdot 24,\ w = 313^2 + 24^2$$

што претставува ново решение на (8), т.е. на (4). Значи, (4) и (8) имаат бесконечно многу решенија. Со тоа ја докажавме следнава теорема.

Теорема. Равенката (4) и системот равенки (8) имаат бесконечно многу решенија, за кои сите променливи се различни од нула. ■

4. ЗБИР НА ЧЕТИРИ КВАДРАТИ

4.1. Во овој параграф ќе ја разгледаме Диофантовата равенка

$$x^2+y^2+z^2+v^2=n,\ \ n\in\mathbb{N}. \tag{1}$$

Со непосредни пресметувања се докажува точноста на следната лема.

Лема. За секои $x,y,z,v,x_1,y_1,z_1,v_1\in\mathbb{Z}$ важи

$$\begin{aligned}(x^2+y^2+z^2+v^2)(x_1^2+y_1^2+z_1^2+v_1^2) &= (xx_1+yy_1+zz_1+vv_1)^2\\ &+(xy_1-yz_1+zv_1-vz_1)^2\\ &+(xz_1-zx_1+vy_1-yv_1)^2\\ &+(xv_1-vx_1+yz_1-zy_1)^2.\ \blacksquare\end{aligned} \tag{2}$$

4.2. Забелешка. Идентитетот во претходната лема покажува дека, ако A и B можат да се претстават како збир од четири квадрати, тогаш и производот AB може да се претстави како збир од четири квадрати.

4.3. Теорема. Ако p е непарен прост број, тогаш постои n таков што $1\le n<p$ и $np=x^2+y^2+z^2+v^2$ за некои $x,y,z,v\in\mathbb{Z}$.

Доказ. Нека

$$S_1=\{0^2,1^2,\ldots,(\tfrac{p-1}{2})^2\}\ \text{ и }\ S_2=\{-0^2-1,-1^2-1,\ldots,-(\tfrac{p-1}{2})^2-1\}.$$

Јасно два елемента од S_1 и два елементи од S_2 не се конгруетни по модул p. Но, бидејќи S_1 и S_2 имаат $p+1$ елементи, а постојат p различни класи на остатоци по модул p, од принципот на Дирихле следува дека

$$x^2\equiv -y^2-1(\mathrm{mod}\,p),\ x^2\in S_1,\ -y^2-1\in S_2,$$

Односно

$$x^2+y^2+1\equiv 0(\mathrm{mod}\,p),\ 1\le x\le\tfrac{p-1}{2},\ 0\le y\le\tfrac{p-1}{2}.$$

Значи, $x^2+y^2+1^2+0^2=np$ и

$$1\le n=\tfrac{1}{p}(x^2+y^2+1)\le\tfrac{1}{p}(2(\tfrac{p-1}{2})^2+1)<p.\ \blacksquare$$

4.4. Теорема. Ако n е најмалиот природен број од теоремата 4.3, тогаш $n=1$.

Доказ. Меѓу броевите n од теорема 4.3 сигурно постои најмал елемент n. Ако n е парен, тогаш и бројот $np=x^2+y^2+z^2+v^2$ е парен, па затоа или сите x,y,z,v се парни, или два од нив се парни, или ниту еден не е парен број. Ако барем два од броевите x,y,z,v се парни, тогаш можеме да земеме дека x и y се парни, а z и v се или двата парни или двата непарни. Но, во тој случај $x\pm y$ и $z\pm v$ се парни

и важи $(\frac{x+y}{2})^2+(\frac{x-y}{2})^2+(\frac{z+v}{2})^2+(\frac{z-v}{2})^2=\frac{n}{2}p$, односно n не е најмал број. Значи, n е непарен број.

Нека претпоставиме дека $n>1$ е најмалиот непарен број од теорема 4.3, односно $3\le n<p$. За x,y,z,v дефинираме броеви x_1,y_1,z_1,v_1 со

$$x\equiv x_1(\mathrm{mod}\,n), y\equiv y_1(\mathrm{mod}\,n), z\equiv z_1(\mathrm{mod}\,n), v\equiv v_1(\mathrm{mod}\,n), \quad (3)$$

$-\frac{n-1}{2}\le x_1,y_1,z_1,v_1\le\frac{n-1}{2}$. Тогаш

$$x_1^2+y_1^2+z_1^2+v_1^2\equiv x^2+y^2+z^2+v^2\equiv 0(\mathrm{mod}\,n),$$

бидејќи

$$x^2+y^2+z^2+v^2=np,$$

па затоа имаме

$$x_1^2+y_1^2+z_1^2+v_1^2=nk,\ 0\le k\le\frac{1}{n}4(\frac{n-1}{2})^2<n. \quad (4)$$

Ако $k=0$, тогаш од (4) имаме $x_1=y_1=z_1=v_1=0$, па од (3) следува

$$x\equiv y\equiv z\equiv v\equiv 0(\mathrm{mod}\,n).$$

Според тоа, добиваме дека

$$np=x^2+y^2+z^2+v^2(\mathrm{mod}\,n^2),$$

односно $p\equiv n(\mathrm{mod}\,n)$, што противречи на фактот дека p е прост број и $3\le n<p$. Затоа $k>0$.

Од лемата 4.1 следува

$$n^2kp=(x^2+y^2+z^2+v^2)(x_1^2+y_1^2+z_1^2+v_1^2)=X^2+Y^2+Z^2+V^2, \quad (5)$$

при што X,Y,Z,V се определени со (2). Ако се земат во предвид (3) и (2), лесно се гледа дека $n\mid X, n\mid Y, n\mid Z, n\mid V$. Сега во (5) делиме со n^2 и добиваме

$$kp=(\frac{X}{n})^2+(\frac{Y}{n})^2+(\frac{Z}{n})^2+(\frac{V}{n})^2,\ 0<k<n.$$

Последното равенство докажува дека ако $n>1$, тогаш n не е најмалиот број во теоремата 4.3. Затоа $n=1$. ■

4.3. Бидејќи $2=1^2+1^2+0^2+0^2$, во претходната теорема докажавме дека секој прост број можеме да го претставиме како збир од четири квадрати. Ако природниот број n го разложиме на прости множители $n=p_1p_2\ldots p_j$, тогаш со последователна примена на лемата 4.1 ја добиваме следнава теорема.

Теорема (Лагранж). Секој природен број n може да се претстави како збир на квадрати на четири природни броеви, т.е. Диофантова равенка (1) има рашение. ■

4.4. Лежандр и Гаус докажале дека природен број n може да се претстави како збир на три квадрати ако и само ако n е од видот $4^m(8k+7), k,m\ge 0$. Во следната

лема ќе докажеме дека ако n е од дадениот вид, тогаш тој не може да се претстави како збир на три квадрати. Доказот на обратното тврдење ја користи теоријата на таканаречените тернарни квадратни форми, па затоа истиот нема да го презентираме.

Лема. Ако $n=4^m(8k+7), k,m\geq 0$, тогаш n не може да се претстави во видот $x^2+y^2+z^2$, за $x,y,z\in\mathbb{Z}$.

Доказ. Нека претпоставиме дека тврдењето не е точно и нека n е најмалиот природен број кој може да се претстави како збир на три квадрати. Според тоа,

$$n=4^m(8k+7)=x^2+y^2+z^2$$

за некои $x,y,z\in\mathbb{Z}$. Квадрат на непарен број

$$(2a+1)^2=8\cdot\frac{a(a+1)}{2}+1$$

дава остаток 1 при делење со 8. Ако меѓу броевите x,y,z има еден, два или три непарни броја, тогаш $x^2+y^2+z^2$ е од видот $4l+1, 4l+2$ или $8l+3$. Меѓутоа, n не е од ниту еден од наведените видови. Затоа сите броеви x,y,z се парни, на пример: $x=2u$, $y=2v$ и $z=2w$. Сега имаме $\frac{n}{4}=4^{m-1}(8k+7)=u^2+v^2+w^2$, што противречи на минималноста на n. ■

5. ЗБИР ОД ДВА КВАДРАТИ

5.1. Нека $n\in\mathbb{N}$. Во овој параграф ќе ја разгледаме равенката

$$x^2+y^2=n\ , \tag{1}$$

$x,y\in\mathbb{Z}$. Оваа равенка нема секогаш решение, т.е. не може секој природен број да се претстави како збир од два квадрати на два цели броја.

Решението x,y на равенката (1) ќе го нарекуваме *примитивно* ако $(x,y)=1$. Во натамошните разгледувања ќе ги користиме следниве функции:

$N(n)$ – број на решенија на равенката (1),

$P(n)$ – број на ненегативни примитивни решенија на равенката (1), и

$Q(n)$ – број на примитивни решенија на равенката (1).

Притоа, решенијата x_1,y_1 и x_2,y_2 ќе ги сметаме дека различни ако $x_1\neq x_2$ или $y_1\neq y_2$.

5.2. Теорема. За функциите $N(n), P(n)$ и $Q(n)$ важи $N(1)=Q(1)=4,\ P(1)=2$. Ако $n>1$, тогаш

$$Q(n)=4P(n) \text{ и } N(n)=\sum_{d^2|n} Q(\tfrac{n}{d^2}).$$

Доказ. Бидејќи $1=(\pm1)^2+0^2=0^2+(\pm1)^2$ и не постојат други решенија добиваме $N(1)=Q(1)=4,\ P(1)=2$.

Ако $n>1$ и x,y е ненегативно примитивно решение, тогаш $x\geq1,\ y\geq1$ па затоа $\pm x,\pm y$ е примитивно решение за секоја промена на знакот. Од тоа следува $Q(n)=4P(n)$.

Ако x,y е произволно решение на равенката (1) и ако $(x,y)=d$, тогаш $d^2\mid n$, $(\frac{x}{d},\frac{y}{d})=1$ и $(\frac{x}{d})^2+(\frac{y}{d})^2=\frac{n}{d^2}$. Според тоа, $N(n)=\sum_{d^2|n} Q(\frac{n}{d^2})$. ■

5.3. Теорема. Нека $n>1$. За секое ненегативно примитивно решение на равенката (1) постои единствен број s по модул n таков што $sy\equiv x(\mathrm{mod}\,n)$. Освен тоа $s^2\equiv-1(\mathrm{mod}\,n)$ и за различните ненегативни решенија постојат различни s_1,s_2 по модул n кои ги исполнуваат горните услови

Доказ. Ако x,y е ненегативно решение, тогаш $(y,n)=1$ и затоа конгруенцијата $sy\equiv x(\mathrm{mod}\,n)$ има единствено решение s по модул n. Освен тоа ако y' е решение на $yy'\equiv1(\mathrm{mod}\,n)$, тогаш $s\equiv xy'(\mathrm{mod}\,n)$ и добиваме

$$s^2\equiv x^2y'^2\equiv-y^2y'^2\equiv-1(\mathrm{mod}\,n).$$

Останува да докажеме дека различните решенија определуваат различни s по модул n. Нека x,y и u,v се различни ненегативни решенија такви што $sy\equiv x\ (\mathrm{mod}\,n)$ и $sv\equiv u(\mathrm{mod}\,n)$. Тогаш $xv\equiv syv\equiv yu(\mathrm{mod}\,n)$. Но, $1\leq x<\sqrt{n}$ и $1\leq v<\sqrt{n}$, па така имаме $1\leq xv<n$ и слично $1\leq yv<n$. Затоа $xv=yu$, од каде $x=u$ и $y=v$, бидејќи $(x,y)=(u,v)=1$ и сите четири броја се позитивни. ■

5.4. Теорема. Нека $n>1$ и $s^2\equiv-1(\mathrm{mod}\,n)$. Постои ненегативно примитивно решение x,y на равенката (1) за кое $sy\equiv x(\mathrm{mod}\,n)$.

Доказ. Да го разгледаме множеството од цели броеви $u-sv$, за u и v такви што $0\leq u\leq\sqrt{n},\ 0\leq v\leq\sqrt{n}$. Постојат $(1+[\sqrt{n}])^2>n$ различни парови u,v, па од принципот на Дирихле следува дека постојат два пара u_1,v_1 и u_2,v_2 такви што

$$u_1-sv_1\equiv u_2-s_2v_2(\mathrm{mod}\,n).$$

ИЗбираме $v_2-v_1=v_0$ и $u_2-u_1=u_0$. Тогаш $sv_0\equiv u_0(\mathrm{mod}\,n)$ и $|u_0|\leq\sqrt{n},|v_0|\leq\sqrt{n}$. Освен тоа, бидејќи u_1,v_1 и u_2,v_2 се различни решенија, броевите u_0,v_0 не можат

да бидат и двата еднакви на нула, а од $sv_0 \equiv u_0 (\mathrm{mod}\, n)$ следува дека ниту еден од нив не е еднаков на нула. Исто така, може да се докаже дека најмалку еден од $|u_0|$ и $|v_0|$ е помал од $\sqrt{n}$. Ова е точно ако n не е точен квадрат. Ако n е точен квадрат и $|u_0| \neq |v_0| \neq \sqrt{n}$ имаме $s\sqrt{n} \equiv \pm\sqrt{n} (\mathrm{mod}\, n)$ и затоа $s \equiv \pm 1 (\mathrm{mod}\, \sqrt{n})$, т.е. $s^2 \equiv 1 (\mathrm{mod}\, \sqrt{n})$. Но, $s^2 \equiv -1 (\mathrm{mod}\, n)$, така што имаме $s^2 \equiv -1 (\mathrm{mod}\, \sqrt{n})$ и затоа $1 \equiv -1 (\mathrm{mod}\, \sqrt{n})$. Според тоа, $\sqrt{n} = 2$, т.е. $n = 4$, што не е можно бидејќи не постои цел број s таков што $s^2 \equiv -1 (\mathrm{mod}\, 4)$.

Од ограниченоста на u_0 и v_0 следува $1 < u_0^2 + v_0^2 < 2n$. Понатаму, од конгруенцијата $sv_0 \equiv u_0 (\mathrm{mod}\, n)$ следува

$$u_0^2 + v_0^2 \equiv sv_0^2 + v_0^2 \equiv v_0^2 (s^2 + 1) \equiv 0 (\mathrm{mod}\, n).$$

Последното значи дека $u_0^2 + v_0^2 = n$.

Сега нека $d = (u_0, v_0)$. Тогаш $d^2 \mid n$ и $s\frac{v_0}{d} \equiv \frac{u_0}{d} (\mathrm{mod}\, \frac{n}{d})$ и затоа

$$\frac{n}{d^2} \equiv \frac{u_0^2 + v_0^2}{d^2} \equiv (\frac{sv_0}{d})^2 + (\frac{v_0}{d})^2 \equiv -(\frac{v_0}{d})^2 + (\frac{v_0}{d})^2 \equiv 0 (\mathrm{mod}\, \frac{n}{d}).$$

Ова е можно само ако $d = 1$ и затоа $(u_0, v_0) = 1$. Ако u_0 и v_0 имаат ист знак, тогаш $x = |v_0|$ и $y = |u_0|$. И во двата случаја x, y е ненегативно примитивно решение. Во првиот случај имаме $sy \equiv s(\pm v_0) \equiv \pm u_0 \equiv x (\mathrm{mod}\, n)$, а во вториот случај $sy \equiv s(\pm u_0) \equiv \pm s(sv_0) \equiv \mp v_0 \equiv x (\mathrm{mod}\, n)$. ■

5.5. Последица. Нека $R(n)$ го означува бројот на решенијата на конгруенцијата $s^2 \equiv -1 (\mathrm{mod}\, n)$. Тогаш $P(1) = 2$, $R(1) = 1$, $Q(1) = 4$, $P(n) = R(n)$ за $n > 1$, $Q(n) = 4R(n)$ за $n \geq 1$ и

$$N(n) = 4 \sum_{d^2 \mid n} R(\frac{n}{d^2}).$$

Доказ. Следува непосредно од последните три теореми. ■

5.6. Теорема. Функциите $R(n)$ и $\frac{N(n)}{4}$ се мултипликативни.

Доказ. Очигледно $R(n)$ е мултипликативна функција. Нека n_1 и n_2 се заемно прости броеви. Тогаш

$$\frac{1}{4} N(n_1 n_2) = \sum_{d^2 \mid n_1 n_2} R(\frac{n_1 n_2}{d^2}) = \sum_{d_1^2 \mid n_1} \sum_{d_2^2 \mid n_2} R(\frac{n_1}{d_1^2} \cdot \frac{n_2}{d_2^2}) = \sum_{d_1^2 \mid n_1} \sum_{d_2^2 \mid n_2} R(\frac{n_1}{d_1^2}) R(\frac{n_2}{d_2^2})$$

$$= \sum_{d_1^2 \mid n_1} R(\frac{n_1}{d_1^2}) \sum_{d_2^2 \mid n_2} R(\frac{n_2}{d_2^2}) = \frac{1}{4} N(n_1) \frac{1}{4} N(n_2). \blacksquare$$

5.7. Теорема. Нека p е непарен прост број и $e \geq 1$. Дефинираме

$$h(1)=1, h(2^e)=0,\ h(p^e)=(-1)^{\frac{p-1}{2}e},$$

Нека $h(n)$ е определено така што

$$h(p_1^{e_1}p_2^{e_2})=h(p_1^{e_1})h(p_2^{e_2}),$$

за прости броеви p_1 и p_2, $p_1 \neq p_2$ и $e_1, e_2 \geq 1$. Тогаш

$$N(n)=4\sum_{d|n}h(d).$$

Доказ. Забележуваме дека $h(n)$ е мултипликативна функција, па затоа функцијата сума $\sum_{d|n}h(d)$ е мултипликативна. Бидејќи $\frac{1}{4}N(n)$ исто така е мултипликативна функција доволно е да докажеме $N(n)=4\sum_{d|n}h(d)$ ако n е степен на прост број.

Заради теоремата IV 5.1 конгуренцијата $s^2 \equiv -1 (\mathrm{mod}\, 2)$ има едно решение $s \equiv 1 (\mathrm{mod}\, 2)$. За $e>1$ конгруенцијата $s^2 \equiv -1 (\mathrm{mod}\, 2^e)$ нема решение бидејќи конгруенцијата $s^2 \equiv -1 (\mathrm{mod}\, 4)$ нема решение. Затоа, според последицата 5.5 важи

$$N(2^e)=4\sum_{f=0}^{[\frac{e}{2}]}R(2^{e-2f})=4\ .$$

Исто така имаме

$$4\sum_{d|2^e}h(d)=4\sum_{f=o}^{e}h(2^f)=4.$$

Да го разгледаме случајот кога p е непарен прост број. Повторно според теоремата IV 5.1 конгуруенцијата $s^2 \equiv -1 (\mathrm{mod}\, p)$ има две решенија ако $p \equiv 1 (\mathrm{mod}\, 4)$ и нема решение ако $p \equiv 3 (\mathrm{mod}\, 4)$. Добиваме дека $s^2 \equiv -1 (\mathrm{mod}\, p^e)$ го има истиот број на решенија за секој $e \geq 1$. Според тоа

$$R(p^e)=R(p)=\begin{cases}2, & \text{ако } p \equiv 1 (\mathrm{mod}\, 4)\\ 0, & \text{ако } p \equiv 3 (\mathrm{mod}\, 4),\end{cases} \qquad e \geq 1.$$

Тогаш, според последицата 5.5, ако e е парен број, имаме

$$N(p^e)=4\sum_{f=0}^{e/2}R(p^{e-2f})=4\tfrac{e}{2}R(p)+4R(1)=\begin{cases}4e+4, & \text{ако } p \equiv 1 (\mathrm{mod}4)\\ 4, & \text{ако } p \equiv 3 (\mathrm{mod}4)\end{cases} \tag{2}$$

и ако e е непарен број, тогаш

$$N(p^e)=4\sum_{f=0}^{(e-1)/2}R(p^{e-2f})=4\tfrac{e+1}{2}R(p)=\begin{cases}4e+4, & \text{ако } p \equiv 1 (\mathrm{mod}4)\\ 0, & \text{ако } p \equiv 3 (\mathrm{mod}4)\end{cases} \tag{3}$$

Соодветно на ова имаме:

$$4\sum_{d|p^e} h(d) = 4\sum_{f=0}^{e} h(p^f) = 4h(1) + 4\sum_{f=1}^{e} (-1)^{\frac{(p-1)f}{2}}$$
$$= \begin{cases} 4+4e & \text{ако } p \equiv 1 \pmod 4 \\ 4 & \text{ако } p \equiv 3 \pmod 4, e \text{ е парен број} \\ 0 & \text{ако } p \equiv 3 \pmod 4, e \text{ е непарен број.} \end{cases} \quad (4)$$

Сега тврдењето следува од (2), (3) и (4). ■

5.8. Последица. Равенката (1) има решение ако и само ако каноничната факторизација на n не содржи фактор од облик p^e, каде p е од облик $4j+3$ и e е непарен број.

Доказ. Непосредно следува од (2), (3) и теорема 5.6. ■

5.9. Теорема. Целиот број n може да се претстави во облик $n = x^2 - y^2$ ако и само ако $n \not\equiv 2 (\mathrm{mod}\, 4)$.

Доказ. Нека $n \equiv 2 (\mathrm{mod}\, 4)$ и $n = x^2 - y^2 = (x-y)(x+y)$. Бидејќи n е парен број, барем еден од броевите $x-y$ и $x+y$ е парен. Но, $x-y$ и $x+y$ се со иста парност, па затоа $n \equiv 0 (\mathrm{mod}\, 4)$, што е противречност.

Обратно, нека $n \not\equiv 2 (\mathrm{mod}\, 4)$. Разликуваме двца случаја и тоа:

- ако $n = 2k+1$, тогаш $n = (k+1)^2 - k^2$, и
- ако $n = 4k$, тогаш $n = (k+1)^2 - (k-1)^2$. ■

*
* *

5.10. Општата теорија на Диофантовите равенки содржи голем број отворени прашања. Меѓутоа, теоријата на квадратните Диофантови равенки скоро целосно е изградена. Еден од позначајните резултат во оваа теорија е теоремата на Хасе-Минковски, која нема да ја разгледуваме, бидејќи истата излегува надвор од рамките на нашите разгледувања. Меѓутоа, подолу ќе презентирам,е еден метод за наоѓање на општото решение на Диофантовата равенка

$$p(x,y,z) = ax^2 + by^2 + cz^2 + dyz + ezx + fxy = 0, \quad (5)$$

каде $a,b,c,d,e,f \in \mathbb{Z}$, ако ни е познато едно нетривијално решение (x_0, y_0, z_0) во кое, на пример, $z_0 \neq 0$.

Методот се базира на следново: ако тројката (x,y,z) е рационално решение на равенката (5), тогаш и тројката $(kx, ky, kz), k \in \mathbb{Q}$ е рационално решение на равен-

ката (5). Ако $z \neq 0$, тогаш за погодно k важи $kz = 1$, па затоа без ограничување на општоста можеме да претпоставиме дека $z = 1$. Сега равенката (5) го добива видот

$$P(x,y) = p(x,y,1) = ax^2 + by^2 + fxy + ex + dy + c = 0. \qquad (6)$$

Множеството решенија на $P(x,y) = 0$ е некоја крива која ја содржи точката со рационални координати $M(x_1, y_1) = (\frac{x_0}{z_0}, \frac{y_0}{z_0}, z_0)$. Навистина,

$$P(x_1, y_1) = p(x_1, y_1, 1) = \frac{1}{z_0^2} p(x_0, y_0, z_0) = 0.$$

Понатаму, секоја права (l) која минува низ точката M, ако целосно не лежи на кривата, ја сече кривата во уште една точка N (ако (l) е тангента, тогаш сметаме дека $M = N$). Ако правата (l) се менува во множеството прави кои минуваат низ точката M и имаат рационален коефициент на правец, тогаш множеството од добиените пресечни точки N е всушност множеството рационални решенија на равенката (6).

5.11. Пример. Во множеството $\mathbb{Q}$ реши ја равенката

$$2x^2 + 1 = y^2. \qquad (7)$$

Решение. Едно решение на равенката (7) е $(x_1, y_1) = (0,1)$. Според алгоритамот даден во 5.10 сите решенија на равнеката (7) се дадени со $(pt, 1+qt)$, каде $p, q \in \mathbb{Z}$ и $t \in \mathbb{Q}$. Ако ги фиксираме p и q, тогаш од равенката (7) ја добиваме следната равенка по t: $2p^2t^2 = 2qt + q^2t^2$, од каде наоѓаме $t = 0$ или $t = \frac{2q}{2p^2 - q^2}$. Според тоа, сите решенија на равенката (7) во множеството $\mathbb{Q}$ се дадени со

$$x = \frac{2pq}{2p^2 - q^2},\ y = \frac{2p^2 + q^2}{2p^2 - q^2},\ \ p, q \in \mathbb{Z},\ p^2 + q^2 \neq 0. \blacksquare$$

5.12. Пример. Равенката $2a^2 + 7b^2 = c^2$ реши ја во множеството:
а) рационални,
б) цели броеви.

Решение. Едно нетривијално решение на дадената равенка ее $(1,1,3)$.

Ако $c = 0$, тогаш единствено решение е $(0,0,0)$. Затоа нека $c \neq 0$. Ако ставиме $x = \frac{a}{c}$ и $y = \frac{b}{c}$, во множеството рационални броеви равенката ја сведуваме на $2x^2 + 7y^2 = 1$. Тројката $(a,b,c) = (1,1,3)$ го дава решението $(x_1, y_1) = (\frac{1}{3}, \frac{1}{3})$. Нека (x,y) е некое решение на равенката и нека $t \in \mathbb{Q}$ и $p, q \in \mathbb{Z}$, $p^2 + q^2 \neq 0$, се такви што $x = \frac{1}{3} + pt,\ y = \frac{1}{3} + qt$. Ако овие вредности ги замениме во $2x^2 + 7y^2 = 1$, добиваме

$$2(\tfrac{1}{3}+pt)^2+7(\tfrac{1}{3}+qt)^2=1,$$

од каде наоѓаме

$$\frac{4pt}{3}+\frac{14qt}{3}+(2p^2+7q^2)t^2=0,$$

односно $t=\frac{2(2p+7q)}{3(2p^2+7q^2)}$ и затоа рационалните решенија на дадената равенка се дадени со формулите:

$$x=\frac{-2p^2-14pq+7q^2}{3(2p^2+7q^2)},\ y=\frac{2p^2+4pq-7q^2}{3(2p^2+7q^2)}. \tag{8}$$

Што се однесува до целобројните решенија, бидејќи $x=\frac{a}{c}$ и $y=\frac{b}{c}$, можеме да земеме

$$x=k(-2p^2-14pq+7q^2),\ y=k(2p^2+4pq-7q^2),\ z=3k(2p^2+7q^2), \tag{9}$$

при што p,q се цели броеви и k е рационален број за кој вредностите на a,b,c зададени со (9) се целобројни. Да споменеме дека не може да се ограничиме само на целобројни вредности на k, бидејќи тогаш решението $(a,b,c)=(3,1,5)$ не може да се добие. Сепак, може да се докаже дека во овој случај доволно е да $42k$ да биде цел број. Докажи! ■

5.13. Пример. Во множеството цели броеви реши ја равенката

$$a^2+b^2+c^2=3(a+2b)c. \tag{10}$$

Решение. Лесно се гледа дека $(a,b,c)=(4,5,1)$ е едно нетривијално решение на (10). За $c=0$ равенката нема решенија освен тривијалното решение $(0,0,0)$. Нека $c\neq 0$ и $x=\frac{a}{c}$, $y=\frac{b}{c}$. Со оваа смена равенката (10) се сведува на равенката

$$x^2+y^2+1=3x+6y$$

и едно нејзино решение е $(x_1,y_1)=(4,5)$. Ставаме $x=5+pt$, $y=5+qt$, каде $t\in\mathbb{Q}$ и $p,q\in\mathbb{Z}$, $p^2+q^2\neq 0$ и добиваме

$$5pt+4qt+p^2t^2+q^2t^2=0,$$

односно $t=-\frac{5p+4q}{p^2+q^2}$ и $t=0$. Сега

$$x=\frac{-p^2-4pq+4q^2}{p^2+q^2},\ y=\frac{5p^2-5pq+q^2}{p^2+q^2}. \tag{11}$$

Оттука лесно ги добиваме решенијата на (10):

$$a=k(-p^2-4pq+4q^2),\ b=k(5p^2-5pq+q^2),\ c=k(p^2+q^2)$$

при што p,q се цели броеви и k е рационален број за кој вредностите на a,b,c зададени со последната равенка се целобројни. ■

6. МЕТОДИ ЗА РЕШАВАЊЕ НА ПОЛИНОМНИ ДИОФАНТОВИ РАВЕНКИ

6.1. Како што рековме општата теорија на Диофантови равенки содржи голем број отворени прашања, а додека теоријата на квадратните Диофантови равенки скоро целосно е изградена. Во претходните разгледувања се задржавме на некои карактеристични равенки и го разгледавме методот на Ферма, кој го применивме во решавање на некои полиномни диофантови равенки. Во продолжение ќе се задржиме на три основни методи за решавање на Диофантови равенки од видот

$$f(x,y,...)=0,$$

каде f е полином со целобројни коефициенти.

а) *Модуларна аритметика* (*разгледување на равенката по погодни модули*). Бидејќи од секое решение на дадената равенка се добива точно бројно равенство, ова равенство треба да е точно по секој модул. Најчесто се користат мали модули, (на пример, 3, 4, 5, 7, 8, 9) или модули кои произлегуваат од задавањето на самата равенка.

б) *Наоѓање на разложување и користење на основната теорема на аритметиката*. Разгледуваната равенка се претставува во облик $AB=n$, каде A и B се изрази кои ги содржат непознатите од равенката, а n е даден цел број. Потоа се применува основната теорема на аритметиката, што значи дека решенијата треба да се такви што добиените бројни вредности за A и B треба да се делители на n. Последното доведува до разгледување на неколку подслучаи во кои се решаваат погодни системи равенки.

Во други случаи дадената равенка се претставува во видот $AB=x^2+y^2$, по што најчесто се применува Малата теорема на Ферма или некое друго познато тврдење.

в) *Користење на оценки*. Фактот дека $|d|\leqq n|$ кога $d|n$ и $n\neq 0$ често пати се користи при добивање на оценки кои може да се искористат за решавање на дадена Диофантова равенка. Освен тоа, природата на непознатите во дадена равенка овозможува равенката да се запише во погоден вид, а потоа да се добијат погодни оценки кои водат кон решенијата на равенката. Класичен пример за ваква примена е користењето на ненегативноста на дискриминантата на равенката, која е квадратна по една од променливите. Друг стандарден пристап е ограничување на даден израз меѓу точни степени и дискусија на вредностите на изразот.

6.2. Пример. Во множеството цели броеви реши ја равенката

$$a^2+b^2+c^2=a^2b^2. \tag{1}$$

Решение. Очигледно, $a=b=c=0$ е решение на равенката (1). Затоа да претпоставиме дека барем еден од броевите a,b,c е различен од 0. Нека $d=(a,b,c)$. Тогаш $a=dx, b=dy, c=dz$ за некои броеви $x,y,z\in\mathbb{Z}$ такви што $(x,y,z)=1$. Ако

замениме во (1) добиваме

$$x^2+y^2+z^2=x^2y^2d^2.$$

Десната страна на последната равенка е точен квадрат, па затоа при делење со 4 дава остаток 0 или 1. Притоа, овој остаток може да е 1 ако и само ако x,y и d се непарни броеви. Но, тогаш остатокот кој при делење со 4 го дава бројот $x^2+y^2+z^2$ е еднаков на 2 или 3, што е противречност. Од друга страна, ако разгледуваниот остаток е 0, тогаш

$$x^2+y^2+z^2\equiv 0(\mathrm{mod}\,4),$$

што е можно ако и само ако броевите x,y,z се парни, што противречни на $(x,y,z)=1$.

Конечно, од горните разгледувања следува дека единствено решение на (1) е $a=b=c=0$. ■

6.3. Пример. Докажи дека равенката

$$x^2+5=y^3$$

нема решенија во множеството цели броеви.

Решение. Нека го претпоставиме спротивното. Прво да ја разгледаме парноста на броевите x и y. Ако x е непарен, тогаш $x^2\equiv 1(\mathrm{mod}\,4)$, па затоа $y^3\equiv 2(\mathrm{mod}\,4)$, што не е можно бидејќи y е парен, па затоа $y^3\equiv 0(\mathrm{mod}\,4)$. Значи, x е парен број, па важи $y^3\equiv 1(\mathrm{mod}\,4)$, т.е. $y\equiv 1(\mathrm{mod}\,4)$. Ако сега ставиме $x=2u$ и $y=4v+1$, добиваме

$$4u^2+5=(4v+1)^3=64v^3+48v^2+12v+1,$$

односно

$$u^2+1=v(16v^2+12v+3).$$

Јасно, $16v^2+12v+3=4v(4v+3)+3$, па затоа овој број мора да има прост делител од видот $4t+3$. Овој прост број е делител на u^2+1. Според тоа, од $u^2\equiv -1(\mathrm{mod}\,p)$, па затоа

$$u^{p-1}\equiv u^{4t+2}=(u^2)^{2t+1}\equiv(-1)^{2t-1}=-1(\mathrm{mod}\,p),$$

па како $p>2$ последното противречи на малата теорема на Ферма.

Коментар. Равенката дадена во задачата е специјален случај на таканаречената Башетова равенка $x^2+k=y^3$, каде $k\in\mathbb{Z}$. Оваа равенка прв ја разгледувал францускиот математичар Клод Гаспар Башет де Мезириак, според кој и го добила името. Општата Башетова равенка и денес е предмет на активно изучување во теоријата на броеви. ■

6.4. Пример. Во множеството цели броеви реши ја равенката

$$x^5 - x^3 - x^2 + 1 = y^2.$$

Решение. Дадената равенка е еквивалентна на равенката

$$(x-1)^2(x+1)(x^2+x+1) = y^2.$$

Ако $x=1$, тогаш $y=0$. Ако $x\neq 1$, горната равенка можеме да ја запишеме во видот

$$(x+1)(x^2+x+1) = (\tfrac{y}{x-1})^2.$$

Значи, $x-1 \mid y$. Да ставиме $A=x+1, B=x^2+x+1$. Бидејќи $B-xA=1$, заклучуваме дека $(A,B)=1$. Но, од $B=(x+\frac{1}{2})^2+\frac{3}{4}>0$ заклучуваме дека A и B се точни квадрати. За $x>1$ имаме

$$x^2 < x^2+x+1 < (x+1)^2,$$

а за $x\leq -2$ имаме

$$x^2 > x^2+x+1 > (x+1)^2,$$

па затоа B не може да биде квадрат на цел број. Преостануваат случаите $x=-1$ и $x=0$ од кои соодветно добиваме $y=0$ и $y=\pm 1$. ■

6.5. Пример. Во множеството цели броеви реши ја равенката

$$x^3 + x^2y + xy^2 + y^3 = 8(x^2+xy+y^2+1).$$

Решение. Дадената равенка е еквивалентна на равенката

$$(x+y)(x^2+y^2) = 4(x^2+y^2) + 4(x+y)^2 + 8. \qquad (2)$$

Бидејќи $x=y=0$ не е решение на разгледуваната равенка, истата може да се запише во видот

$$x+y = 4 + 4\frac{(x+y)^2}{x^2+y^2} + \frac{8}{x^2+y^2}, \qquad (3)$$

од каде следува дека $x+y>4$, т.е. $x+y\geq 5$. Од друга страна од неравенството меѓу аритметичката и квадратната средина следува

$$x^2+y^2 \geq \tfrac{1}{2}(|x|+|y|)^2 \geq \tfrac{1}{2}(x+y)^2,$$

па затоа $x^2+y^2 \geq \frac{25}{2} > 8$ и $0 \leq \frac{(x+y)^2}{x^2+y^2} \leq 2$. Ако ги земеме во предвид овие неравенства, од (3) следува дека $x+y<13$, т.е. $x+y\leq 12$. Освен тоа, бидејќи броевите $x+y$ и x^2+y^2 се со иста парност, од (2) следува дека $x+y$ е парен број. Значи, $x+y\in\{6,8,10,12\}$. Воведуваме смена $x+y=2a$ и $xy=b$. Тогаш разгледуваната равенка го добива видот

$$2a(4a^2-2b) = 8(4a^2-b+1),$$

од каде

$$b=\frac{2a^3-8a^2-2}{a-2}=2a^2-4a-8-\frac{18}{a-2}.$$

Значи, $(a-2)\mid 18$, па како $3\le a\le 6$ за a можни се три случаи, т.е. $a\in\{3,4,5\}$. За овие случаи за вредностите на b соодветно добиваме $-20,-1$ и 16. Според тоа, (x,y) се добива како пар решенија на три квадратни равенки

$$t^2-6t-20=0,\quad t^2-8t-1=0,\quad t^2-10t+6=0.$$

Лесно се гледа дека само третата од овие равенки има целобројни решенија. Овие решенија се 2 и 8, па ни преостанува само да провериме дека паровите (2,8) и (8,2) навистна се решенија на дадената равенка. ■

6.6. Пример. Определи ги сите природни броеви x,y за кои важи

$$x+y^2+z^3=xyz, \tag{4}$$

каде $z=(x,y)$.

Решение. Нека $x=az,\ y=bz$ и $(a,b)=1$. Тогаш равенката (4) го добива видот

$$a+b^2z+z^2=abz^2.$$

Од последната равенка следува дека $a=cz$ за некој природен број c, па така ја добиваме равенката

$$c+b^2+z=cbz^2.$$

Сега, бидејќи $bz^2\neq 1$, во спротивно би добиле $y=b=z=1$, т.е. $x=x+2$, добиваме

$$c=\frac{b^2+z}{bz^2-1}. \tag{5}$$

Ако (5) ја помножиме со z^2 добиваме

$$cz^2=\frac{b^2z^2+z^3}{bz^2-1}=b+\frac{b+z^3}{bz^2-1}. \tag{6}$$

Вториот собирок во (6) мора да е природен број, па тој е поголем или еднаков на 1. Според тоа, $b+z^3\ge bz^2-1$, т.е. $b(z^2-1)\le z^3+1$, од каде добиваме

$$b(z-1)\le z^2-z+1.$$

Ако $z=1$, тогаш од (6) добиваме

$$c=b+1+\frac{2}{b-1},$$

па затоа $b=2$ или $b=3$, а соодветните решенија се $(x,y)\in\{(5,2),(5,3)\}$. Во спротивно добиваме

$$b\le\frac{z^2-z+1}{z-1}=z+\frac{1}{z-1}.$$

За $z=2$ равенката (6) го добива обликот

$$16c=\frac{16b^2+32}{4b-1}=4b+1+\frac{33}{4b-1},$$

од каде ги добиваме решенијата $b=1$ и $b=3$, т.е. $(x,y)\in\{(4,2),(4,6)\}$. Од друга страна, за $z\geq 3$ важи $\frac{1}{z-1}<1$, па заклучуваме $b<z+1$, т.е. $b\leq z$. Сега од (5), ако се искористи дека $b\geq 1$, следува

$$c<\frac{z^2+z}{z^2-1}=\frac{z}{z-1}=1+\frac{1}{z-1}<2.$$

Значи, $c=1$. Според тоа, b е решение на квадратната равенка

$$b^2-z^2b+z+1=0,$$

од што следува дека дискриминантата на оваа равенка z^4-4z-4 е точен квадрат на природен број. Но, бидејќи $z\geq 3$, важи

$$(z^2-1)^2<z^4-4z-4<(z^2)^2,$$

што е противречност. Конечно, множеството решенија на равенката е

$$(x,y)\in\{(4,2),(4,6),(5,2),(5,3)\}.\ \blacksquare$$

7. МЕТОДИ ЗА РЕШАВАЊЕ ЕКСПОНЕНЦИЈАЛНИ ДИОФАНТОВИ РАВЕНКИ

7.1. Експоненцијална Диофантова равенка ја нарекуваме равенката во која една или повеќе непознати се појавуваат и во степенов показател на еден или повеќе степени. Може да се каже дека теоријата на Диофантовите равенки содржи најмалку резултати токму за решавање на експоненцијалните Диофантови равенки. Во продолжение ќе наведеме три основни методи за решавање на овие равенки и ќе дадеме повеќе решени примери.

а) *Разгледување на равенката по модули на простите броеви кои учествуваат во степените кои се појавуваат во равенката*. Бидејќи од секое решение на дадената равенка се добива точно бројно равенство, ова равенство треба да е точно по секој модул. Простите делители (и нивните степени) на основите на степените кои се појавуваат во равенката најчесто се земаат за модули по кои се разгледува равенката.

б) *Наоѓање на разложување и користење на основната теорема на аритметиката*. Примената на а) дава информација за својствата на степените кои се појавуваат во равенката. Често пати оваа информација овозможува да се најде разложување на множители, по што е можно едноставна анализа и користење на основната теорема на аритметиката.

в) *Разгледување на равенката по други модули*. Добиениките информации од а) и б) ни озвозможуваат равенката да ја разгледуваме по модули кои се појавуваат или се блиски до степените добиени во разложувањето.

7.2. Пример. Во множеството ненегативни цели броеви реши ја равенката

$$4^a + 5^b + 6^c = 7^d .$$

Решение. За $c > 0$ равенката по модул 3 се сведува на $1 + 2^b + 0 \equiv 1 (\mathrm{mod}\, 3)$, т.е. на $2^b + 0 \equiv 0 (\mathrm{mod}\, 3)$, што не е можно. Затоа $c = 0$. Ако сега $a > 0$, тогаш левата страна на равенката е парна, а десната непарна, што е противречност, па затоа мора да е $a = 0$. Според тоа, равенката се сведува на равенката $5^b + 2 = 7^d$.

Ако $b > 1$, тогаш $7^d \equiv 2 (\mathrm{mod}\, 25)$. Меѓутоа, можни остатоци на 7^d при делење со 25 се само ± 7 и ± 1, па затоа во овој случај равенката нема решение. Остануваат случаите $b \leq 1$. Сега, лесно се проверува дека единствено решение на дадената равенка е $(a, b, c, d) = (0, 1, 0, 1)$. ■

7.3. Пример. Во множеството природни броеви реши ја равенката

$$3^x + 4^y = 5^z .$$

Решение. *Прв начин*. Дадената равенка ја разгледуваме по модул 3. Имаме

$$2^z \equiv 5^z \equiv 1 (\mathrm{mod}\, 3),$$

па z мора да е парен број, т.е. $z = 2t$. Затоа важи

$$3^x = 5^{2t} - 4^y = (5^t - 2^y)(5^t + 2^y),$$

од каде следува дека $5^t + 2^y$ е степен на бројот 3, додека $5^t - 2^y$ е еднаков на бројот 1 или е степен на бројот 3. Но, вториот случај не е можен, бидејќи тогаш бројот $(5^t + 2^y) + (5^t - 2^y) = 2 \cdot 5^t$ би бил делив со 3. Според тоа,

$$5^t - 2^y = 1 \text{ и } 5^t + 2^y = 3^x .$$

Последните равенки ги разгледуваме по модул 3 и добиваме

$$(-1)^t - (-1)^y \equiv 1 (\mathrm{mod}\, 3) \text{ и } (-1)^t + (-1)^y \equiv 0 (\mathrm{mod}\, 3),$$

од каде следува дека t е непарен, додека y е парен. Ставаме $y = 2v$, $v \in \mathbb{N}$. Добиваме $5^t - 4^v = 1$ и $5^t + 4^v = 3^x$. Од првата равенка следува $5^t = 4^v + 1$ од каде следува $v = 1$, бидејќи ако $v \geq 2$ ќе важи $5^t \equiv 1 (\mathrm{mod}\, 8)$, што не е можно бидејќи t е непарен, а $5^{2s+1} = 5 \cdot 25^s \equiv 5 (\mathrm{mod}\, 8)$. Сега, од $v = 1$ следува $t = 1$, па од втората од двете наведени равенки следува $x = 2$. Значи, $x = y = z = 2$ е единствено решение на задачата.

Втор начин. Равенката ќе ја запишпеме во вид

$$3^m + 4^n = 5^k .$$

Ако земеме предвид дека $5^k \equiv (-1)^k (\mathrm{mod}\, 3)$ и $4^n \equiv 1 (\mathrm{mod}\, 3)$, од дадената равенка добиваме $(-1)^k \equiv 1 (\mathrm{mod}\, 3)$, па затоа k е парен број, т.е. $k = 2K$. Слично добиваме $5^k \equiv 1 (\mathrm{mod}\, 4)$ и $3^m \equiv (-1)^m (\mathrm{mod}\, 4)$, па затоа $(-1)^m \equiv 1 (\mathrm{mod}\, 4)$, од каде следува m

е парен број, т.е. $m=2M$. Добиваме

$$2^{2n}=4^n=5^k-3^m=5^{2K}-3^{2M}=(5^K-3^M)(5^K+3^M). \qquad (1)$$

Од (1) следува дека $5^K-3^M=2^a$ и $5^K+3^M=2^b$, за некои природни броеви a и b. Ако ги одземеме последните две равенки добиваме $2^a(2^{b-a}-1)=2\cdot 3^M$, па затоа $a=1$ и $2^{b-1}-1=3^M$. Понатаму, од $3^M\equiv 1$ или $3 (\mathrm{mod} 8)$ следува

$$2^{b-1}\equiv 2(\mathrm{mod}8) \text{ или } 2^{b-1}\equiv 4(\mathrm{mod}8).$$

Тоа значи, $b=2$ или $b=3$. Сега, од (1) имаме $2n=a+b$, па затоа $b=3$ и $n=2$. Оттука добиваме $M=1, K=1$, односно $m=2, k=2$, што значи дека дадената равенка има единствено решение $m=n=k=2$. ■

7.4. Пример. Во множеството природни броеви реши ја равенката

$$7^x-3\cdot 2^y=1.$$

Решение. Дадената равенка е еквивалентна на равенката

$$2^{y-1}=\tfrac{7^x-1}{7-1}=7^{x-1}+7^{x-2}+\ldots+1.$$

Оттука добиваме дека $x=1, y=1$ е едно решение на равенката. Нека сега претпоставиме дека $y\geq 2$. Тогаш левата страна на последната равенка е парен број, а десната страна е збир на x непарни броеви, па затоа x мора да е парен број. Според тоа, дадената равенка може да се запише во видот

$$2^{y-1}=(7+1)(7^{x-2}+7^{x-4}+\ldots+1),$$

односно

$$2^{y-4}=7^{x-2}+7^{x-4}+\ldots+1,$$

па затоа мора да е $y\geq 4$. Лесно се добива дека $x=2, y=4$ е второ решение. Затоа нека претпоставиме дека $y\geq 5$. Тогаш збир на $\frac{x}{2}$ непарни броеви е парен број, па затоа x еделив со 4. Сега можеме да запишеме

$$2^{y-4}=(7^2+1)(7^{x-4}+7^{x-8}+\ldots+1),$$

па како $7^2+1=2\cdot 25$ последното не е можно, бидејќи левата страна е степен на бројот 2 и не е делива со 25.

Конечно, единствени решенија се $x=1, y=1$ и $x=2, y=4$. ■

7.5. Пример. Во множеството цели броеви реши ја равенката

$$12^x+y^4=2008^z.$$

Решение. *Прв начин*. За $z\leq 0$ равенката има тривијално решение $(0,0,0)$. Понатаму, нека $z>0$. Бидејќи $2008=2^3\cdot 251$, двете страни на равенката се деливи со 251. Ако $x=2a$, тогаш

$$(12^a)^2 \equiv -(y^2)^2 \pmod{251},$$

па ако степенуваме на степен 125 од малата теорема на Ферма следува

$$1 \equiv (12^a)^{250} \equiv -(y^2)^{250} \equiv -1 \pmod{251},$$

што не е можно. Значи, x мора да е непарен број. Очигледно, y е парен број и нека $y = 2^u b$ каде b е непарен број. Тогаш

$$2^{2x}3^x + 2^{4u}b^4 = 2^{3z}251^z.$$

Но, x е непарен број, па затоа $2x \neq 4u$, што значи дека најголемиот степен на бројот 2 кој е делител на левата страна е 2^{2x} или 2^{4u}, додека најголемиот степен на бројот 2 кој е делител на десната страна е 2^{3z}. Ќе покажеме дека во ниту еден од двата случаја дадената равенка нема решение.

1) Ако $3z = 2x < 4u$, тогаш $2 \mid z$. Ако скратиме со 2^{2x}, ја добиваме равенката $3^x + 2^{4u-2x}b^4 = 251^z$, што не е можно бидејќи од $2 \nmid x$ следува дека левата страна е од видот $4k+3$, а од $2 \mid z$ следува дека десната страна е од видот $4k+1$.
2) Ако $3z = 4u < 2x$, тогаш $2 \mid z$. Ако скратиме со 2^{4u}, ја добиваме равенката $2^{2x-4u}3^x + b^4 = 251^z$. Десната страна на последната равенка е од видот $5k+1$, па ако $5 \nmid b$ имаме $b^4 \equiv 1 \pmod{5}$ и добиваме $2^{2x-4u}3^x \equiv 0 \pmod{5}$, што не е можно, а ако $5 \mid b$, тогаш заради $2 \nmid x$ добиваме

$$1 \equiv 2^{2x-4u}3^x \equiv \pm 3^x \equiv \pm 3 \pmod{5},$$

што не е можно.

Втор начин. Ако x е парен број, тогаш левата страна на равенката има облик $a^2 + b^2$, а за непарен x левата страна на равенката има облик $a^2 + 3b^2$. Но, бидејќи -1 и -3 се квадратни неостатоци по модул 251, ниту $a^2 + b^2$ ниту $a^2 + 3b^2$ не може да се дели со 251 ако $251 \nmid a$. Според тоа, дадената равенка нема целобројни решенија за $z > 0$. За $z \leq 0$ равенката има тривијално решение $(0,0,0)$. ■

7.6. Пример. Во множеството ненегативни цели броеви реши ја равенката

$$(14y)^x + y^{x+y} = 2007.$$

Решение. Ако $x = 0$, тогаш $y^y = 2006$, што не е можно за ниту еден ненегативен цел број y. За $y = 0$ задачата нема смисла. Затоа $x, y \geq 1$. Ако $x \geq 3$, тогаш

$$(14y)^x + y^{x+y} > (14y)^x \geq 14^x \geq 14^3 > 2007.$$

Останува $x = 1$ или $x = 2$. Ако $x = 1$ ја добиваме равенката

$$y(14 + y^y) = 2007 = 3^2 \cdot 223.$$

Лесно се проверува дека равенката нема решение во $\mathbb{N}$. Ако $x=2$ имаме

$$y^2(196+y^y)=2007,$$

од каде се добива $y=3$. Значи, $x=2, y=3$ е единствено решение на дадената равенка. ■

7.7. Пример. Во множеството природни броеви реши ја равенката

$$a^n-1=(a^p-1)(a^q-1)(a^r-1).$$

Решение. Во примерот V 4.5 оваа равенка ја решивме со помош на теоремата на Жигимонди. Овде ќе дадеме втор начин на решавање на дадената равенка.

Ако $a=1$, тогаш сите петорки $(1,n,p,q,r)$ ја задоволуваат дадената равенка. Нека $a>1$. Без ограничување на општоста можеме да земеме дека $p\geq q\geq r$. Имаме:

$$a^n-1\leq(a^p-1)(a^p-1)(a^p-1)=(a^p-1)^3=a^{3p}-3a^p(a^p-1)-1<a^{3p}-1,$$

од каде следува $n<3p$. Сега од $a^p-1\mid a^n-1$ и

$$a^{(p,n)}-1=(a^n-1,a^p-1)=a^p-1$$

следува $p=(p,n)$, т.е. $p\mid n$. Значи, $n=p$ или $n=2p$.

Ако $n=p$, тогаш $(a^q-1)(a^r-1)=1$, од каде се добива $a=2, q=r=1$. Според тоа, за (a,n,p,q,r) ги добивме решенијата

$$(2,n,n,1,1),(2,n,1,n,1),(2,n,1,1,n).$$

Ако $n=2p$, тогаш $a^{2p}-1=(a^p-1)(a^q-1)(a^r-1)$, па затоа

$$a^p+1=(a^q-1)(a^r-1), \text{ т.е. } a^p+1=a^{q+r}-a^q-a^r+1,$$

од каде следува

$$a^{p-r}+a^{q-r}=a^q-1. \tag{1}$$

Ако $q-r>0$, тогаш и $p-r>0$, па затоа левата страна е делива со a, а десната страна не е делива со a. Затоа $q=r$ и (1) го добива обликот

$$a^{p-q}=a^q-2. \tag{2}$$

Ако $a=2$, тогаш $p-q=1$ и $q=2$. Значи, $p=3, n=6, r=q=2$, т.е. петорката $(a,n,p,q,r)=(2,6,3,2,2)$ е решение како и сите други пермутации на p,q,r, т.е. $(2,6,2,3,2)$ и $(2,6,2,2,3)$ се решение на равенката.

Ако $a>2$ и $p-q>0$, тогаш од (2) следува $a\mid 2$, што не е можно. Значи, $p=q$. Добиваме $a^q=3$, па затоа $a=3$ и $q=1$. Оттука $p=q=r=1$, $n=2$, $(a,n,p,q,r)=(3,2,1,1,1)$ е решение на равенката. ■

7.8. Пример. Во множеството природни броеви реши ја равенката

$$x^3+2x+1=2^n.$$

Решение. Ако $n=1$, тогаш ја добиваме равенката $x^3+2x=1$ која нема решение во множеството природни броеви. За $n=2$ добиваме $x=1$, т.е. $(1,2)$ е едно решение на равенката. Ќе докажеме дека за $n\geq 3$ равенката нема решение.

Бројот $x(x^2+2)=2^n-1$ е непарен, па затоа x е непарен број. Оттука $x^2\equiv 1(\mathrm{mod}8)$, т.е. $x^2+2\equiv 3(\mathrm{mod}8)$. Понатаму, за $n\geq 3$ важи $2^n-1\equiv -1(\mathrm{mod}8)$, па затоа $3x\equiv -1(\mathrm{mod}8)$, т.е. $x\equiv 5(\mathrm{mod}8)$.

Од друга страна, ако $x\equiv 0(\mathrm{mod}3)$, тогаш $2^n\equiv 1(\mathrm{mod}3)$, а ако $x\equiv 1,2(\mathrm{mod}3)$, тогаш $x^2\equiv 1(\mathrm{mod}3)$, од каде следува дека $3\mid x^2+2$. Оттука $2^n\equiv 1(\mathrm{mod}3)$, односно во секој случај n е парен број.

Дадената равенка е еквивалентна со равенката $(x+1)(x^2-x+3)=2^n+2$. Но, n е парен број, па затоа 2^n е точен квадрат.

Ако p е непарен прост делител на бројот $(x+1)(x^2-x+3)$, тогаш конгруенцијата $x^2\equiv -2(\mathrm{mod}\,p)$ има решение $x=2^k$, за $k=\frac{n}{2}$. Според тоа -2 е квадратен остаток на секој непарен прост делител p на $(x+1)(x^2-x+3)$, т.е. $(\frac{-2}{p})=1$. Добиваме

$$1=(\frac{-2}{p})=(\frac{-1}{p})(\frac{2}{p})=(-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}=(-1)^{\frac{p^2+4p-5}{8}},$$

од каде следува дека $p^2+4p-5=16s$. Лесно се проверува дека $p\equiv 1(\mathrm{mod}8)$ или $p\equiv 3(\mathrm{mod}8)$. Значи,

$$(x+1)(x^2-x+3)\equiv 1(\mathrm{mod}8) \text{ или } (x+1)(x^2-x+3)\equiv 3(\mathrm{mod}8). \qquad (3)$$

Од друга страна, бидејќи $x\equiv 5(\mathrm{mod}8)$ добиваме $(x+1)(x^2-x+3)\equiv 7(\mathrm{mod}8)$ што противречи на (3).

Конечно, во множеството природни броеви парот $(1,2)$ е единствено решение на дадената равенка. ■

8. РАВЕНКА НА ТУЕ

8.1. Дефиниција. Полиномот од две или повеќе променливи во кој сите мономи имаат еднаков степен го нарекуваме *хомоген полином*.

На пример, $x^3+xyz+y^2z+z^3$ е хомоген полином со три променливи и е од

трет степен.

8.2. Во нашите разгледувања ќе се задржиме на бинарните форми од вид

$$F(x,y)=a_0x^n+a_1x^{n-1}y+a_2x^{n-2}y^2+\ldots+a_ny^n, \qquad (1)$$

каде $a_0,a_1,\ldots,a_n\in\mathbb{Z}$, т.е. на хомогените полиноми со две променливи од $n-$ти степен и целобројни коефициенти.

Нека (1) е бинарна форма со целобројни коефициенти, иредуцибилна над $\mathbb{Q}$ и со степен $n\geq 3$. Да забележиме дека бинарната форма (1) не може да биде иредуцибилна над $\mathbb{C}$. Имено,

$$F(x,1)=a_0(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n),$$

каде $\alpha_1,\alpha_2,\ldots,\alpha_n$ се алгебарски броеви од степен n, па затоа

$$F(x,y)=y^nF(\tfrac{x}{y},1)=a_0(x-\alpha_1y)(x-\alpha_2y)\ldots(x-\alpha_ny).$$

Но, иредуцибилноста над $\mathbb{Q}$ повлекува дека $F(x,1)$ нема повеќекратни корени, т.е. дека броевите $\alpha_1,\alpha_2,\ldots,\alpha_n$ се по парови различни.

8.3. Дефиниција. Нека $n\geq 3$ и $m\neq 0$ е цел број. Диофантовата равенка од видот

$$F(x,y)=m \qquad (2)$$

ја нарекуваме *равенка на Туе*.

8.4. Во 1909 година, користејќи свои резултати од Диофантовите апроксимации, Туе докажал дека равенката (2) има само конечно многу решенија.

Прво ќе докажеме едноставен специјален случај на овој резултат.

Теорема. Ако равенката $F(x,1)=0$ нема реални решенија, тогаш равенката (2) има само конечно многу целобројни решенија. Попрецизно, сите решенија го задоволуваат неравенството

$$|y|\leq\frac{|m|}{\min\limits_{1\leq i\leq n}|\mathrm{Im}\,\alpha_i|},$$

каде $\alpha_1,\alpha_2,\ldots,\alpha_n$ се корените на полиномот $F(x,1)$.

Доказ. Нека претпоставиме дека (x,y) е решение на равенката (2) и нека α_k е таков што $|x-\alpha_ky|=\min\limits_{1\leq i\leq n}|x-\alpha_iy|$. Тогаш

$$|y|\cdot|\mathrm{Im}\,\alpha_k|=|\mathrm{Im}(\alpha_ky)|\leq|x-\alpha_ky|\leq|m|,$$

од каде што следува тврдењето на теоремата. ■

8.5. Теорема (Туе). Равенката на Туе има само конечно многу целобројни решенија.

Доказ. Нека $F(x,y)=m$. При претходно воведените ознаки имаме

$$a_0(x-\alpha_1 y)(x-\alpha_2 y)...(x-\alpha_n y)=m. \tag{3}$$

Понатаму, можеме да претпоставиме дека $y\neq 0$, бидејќи за $y=0$ имаме најмногу две решенија. Ја делиме (3) со y^n, земаме апсолутни вредности и добиваме

$$|a_0|\cdot|\alpha_1-\tfrac{x}{y}|\cdot|\alpha_2-\tfrac{x}{y}|\cdot...\cdot|\alpha_n-\tfrac{x}{y}|=|\tfrac{m}{y^n}|. \tag{4}$$

Како и во доказот на теоремата 8.4, нека α_k е таков што

$$|x-\alpha_k y|=\min_{1\le i\le n}|x-\alpha_i y|, \text{ т.е. } |\alpha_k-\tfrac{x}{y}|=\min_{1\le i\le n}|\alpha_i-\tfrac{x}{y}|.$$

Нека $\gamma=\frac{1}{2}\min_{i\neq j}|\alpha_i-\alpha_j|>0$. За доволно големо y двете страни на (4) може да се направат произвоно мали. Ова посебно важи и за најмалиот множител на левата страна, односно за $|\alpha_k-\tfrac{x}{y}|$. Според тоа, постои $y_0>0$ таков што за $y\ge y_0$ важи $|\alpha_k-\tfrac{x}{y}|<\gamma$. За $i\neq k$ имаме

$$|\alpha_i-\tfrac{x}{y}|\ge|\alpha_i-\alpha_k|-|\alpha_k-\tfrac{x}{y}|\ge 2\gamma-\gamma=\gamma.$$

Затоа од (4) следува

$$|\alpha_k-\tfrac{x}{y}|\le|\frac{m}{a_0y^n\gamma^{n-1}}|=\frac{c}{|y|^n}. \tag{5}$$

Бидејќи $n\ge 3$, од теоремата на Рот следува дека неравенката (5) има само конечно многу решенија, што и требаше да се докаже. ■

9. РАВЕНКА НА ПЕЛ

9.1. Дефиниција. Нека d е природен број кој не е точен квадрат. Диофантовата равенка

$$x^2-dy^2=1 \tag{1}$$

ја нарекуваме *равенка на Пел*.

9.2. Лема. Нека d е природен број кој не е точен квадрат. Тогаш постои цел број $k, |k|<1+2\sqrt{d}$, таков што равенката

$$x^2-dy^2=k \tag{2}$$

има бесконечно многу решенија во множеството природни броеви.

Доказ. Според последицата VII 2.2 за ирационалниот број $\sqrt{d}$ постојат бесконечно многу подредени парови природни броеви (x,y) такви што

$$|\sqrt{d}-\tfrac{x}{y}|<\tfrac{1}{y^2}\text{, т.е. } |x-y\sqrt{d}|<\tfrac{1}{y}.$$

За секој таков пар (x,y) важи

$$|x+y\sqrt{d}|=|x-y\sqrt{d}+2y\sqrt{d}|<\tfrac{1}{y}+2y\sqrt{d}\le(1+2\sqrt{d})y,$$

па затоа

$$|x^2-dy^2|=|x-y\sqrt{d}|\cdot|x+y\sqrt{d}|<1+2\sqrt{d}.$$

Бидејќи парови (x,y) со наведеното својство има бесконечно многу, а целите броеви кои по апсолутна вредност помали од $1+2\sqrt{d}$ се конечно многу, заклучуваме дека постои цел број k таков што $|k|<1+2\sqrt{d}$ и за кој равенката (2) има бесконечно многу решенија. ■

9.3. Теорема. Во множеството природни броеви равенката (1) има барем едно решение.

Доказ. Според лемата 9.2 постои цел број $k,|k|<1+2\sqrt{d}$ таков што равенката (2) има бесконечно многу решенија во множеството природни броеви. Овие решенија ги делиме во k^2 класи, при што решенијата (x_1,y_1) и (x_2,y_2) припаѓаат на иста класа ако и само ако $x_1\equiv x_2(\mathrm{mod}\,k)$ и $y_1\equiv y_2(\mathrm{mod}\,k)$. Тогаш некоја класа ќе содржи најмалку две (всушност бесконечно многу) различни решенија (x_1,y_1) и (x_2,y_2) во кои x_1 и x_2 се различни природни броеви. Земаме

$$x=\tfrac{x_1x_2-dy_1y_2}{k},\ y=\tfrac{x_1y_2-y_1x_2}{k}. \tag{3}$$

Тогаш

$$x_1x_2-dy_1y_2\equiv x_1^2-dy_1^2=k\equiv 0(\mathrm{mod}\,k),$$
$$x_1y_2-y_1x_2\equiv x_1y_1-y_1x_1=0(\mathrm{mod}\,k),$$

па затоа $x,y\in\mathbb{Z}$. Нека претпоставиме дека $y=0$, односно $x_1y_2=y_1x_2$. Тогаш

$$k=x_2^2-dy_2^2=x_2^2-d\tfrac{x_2^2y_1^2}{x_1^2}=\tfrac{x_2^2}{x_1^2}(x_1^2-dy_1^2)=k\tfrac{x_2^2}{x_1^2},$$

т.е. $x_1^2=x_2^2$, што противречи на претпоставката дека x_1 и x_2 се различни природни броеви. Конечно,

$$\begin{aligned}x^2-dy^2&=\tfrac{1}{k^2}((x_1x_2-dy_1y_2)^2-d(x_1y_2-y_1x_2)^2)\\&=\tfrac{1}{k^2}(x_1^2x_2^2+d^2y_1^2y_2^2-dx_1^2y_2^2-dx_2^2y_1^2)\\&=\tfrac{1}{k^2}(x_1^2-dy_1^2)(x_2^2-dy_2^2)=\tfrac{1}{k^2}\cdot k\cdot k=1,\end{aligned}$$

т.е. (3) се решенија на (1). ■

9.4. Ако (x_1, y_1) и (x_2, y_2) се две различни решенија на (1), тогаш лесно се гледа $x_1 < x_2$ ако и само ако $y_1 < y_2$, што значи дека постои најмало решение на (1), т.е. решение во кое природните броеви x_1 и y_1 се најмали. Најмалото решение на равенката (1) во множеството природни броеви ќе го нарекуваме *фундаментално решение* и за истото ќе ги користиме ознаките (x_1, y_1) или $x_1 + y_1\sqrt{d}$.

9.5. Теорема. Равенката на Пел (1) има бесконечно многу решенија. Ако (x_1, y_1) е фундаменталното решение, тогаш во множеството природни броеви сите решенија на (1) се дадени со формулата

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n, n \in \mathbb{N}, \tag{4}$$

т.е.

$$x_n = x_1^n + \binom{n}{2} d x_1^{n-2} y_1^2 + \binom{n}{4} d^2 x_1^{n-4} y_1^4 + ...,$$
$$y_n = n x_1^{n-1} y_1 + \binom{n}{3} d x_1^{n-3} y_1^3 + \binom{n}{5} d^2 x_1^{n-5} y_1^5 + ...$$

Доказ. Од (4) и Њутновата биномна формула следува

$$x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$$

и ако последното равенство се помножи со равенството (4) добиваме

$$x_n^2 - d y_n^2 = (x_1^2 - d y_1^2)^n = 1,$$

што значи дека (x_n, y_n), $n \in \mathbb{N}$ навистина се решенија на (1).

Нека претпоставиме дека (s,t) е решение на (1) кое не е од видот (x_n, y_n), $n \in \mathbb{N}$. Бидејќи (x_1, y_1) е фундаменталното решение и $x_1 + y_1\sqrt{d} > 1$ и $s + t\sqrt{d} > 1$, постои природен број m таков што

$$(x_1 + y_1\sqrt{d})^m < s + t\sqrt{d} < (x_1 + y_1\sqrt{d})^{m+1}. \tag{5}$$

Ако (5) ја помножиме со $(x_1 + y_1\sqrt{d})^{-m} = (x_1 - y_1\sqrt{d})^m$, добиваме

$$1 < (s + t\sqrt{d})(x_1 - y_1\sqrt{d})^m < x_1 + y_1\sqrt{d}.$$

Нека $a, b \in \mathbb{Z}$ се такви што

$$a + b\sqrt{d} = (s + t\sqrt{d})(x_1 - y_1\sqrt{d})^m = (s + t\sqrt{d})(x_1 + y_1\sqrt{d})^{-m}.$$

Јасно, $a + b\sqrt{d} > 0$ и лесно се гледа дека

$$a - b\sqrt{d} = (s - t\sqrt{d})(x_1 + y_1\sqrt{d})^m,$$

па затоа

$$a^2 - d b^2 = (s^2 - d t^2)(x_1^2 - d y_1^2)^m = 1.$$

Но, $a + b\sqrt{d} > 0$, па затоа $a - b\sqrt{d} > 0$, и како $a + b\sqrt{d} > a - b\sqrt{d} > 0$, добиваме дека $a + b\sqrt{d} > 1$ и $0 < a - b\sqrt{d} < 1$. Сега од последните три неравенства следува

$$2a = a + b\sqrt{d} + (a - b\sqrt{d}) > 0 \text{ и } 2b\sqrt{d} = a + b\sqrt{d} - (a - b\sqrt{d}) > 0,$$

т.е. $a>0$ и $b>0$. Според тоа (a,b) е решение на равенката (1) во множеството природни броеви и

$$a+b\sqrt{d}<x_1+y_1\sqrt{d}\ ,$$

што е противречност. Конечно, од добиената противречност следува дека сите решенија на (1) се дадени со (4). ■

9.6. Теорема. Нека $(x_n,y_n), n\in\mathbb{N}$ е низата решенија во множеството природни броеви на равенката (1) запишани во растечки ресолед. Нека $(x_0,y_0)=(1,0)$. Тогаш

$$x_{n+2}=2x_1x_{n+1}-x_n,\quad y_{n+2}=2x_1y_{n+1}-y_n,\ n\geq 0. \tag{6}$$

Доказ. Од (4) следува

$$x_{n+2}+y_{n+2}\sqrt{d}=(x_{n+1}+y_{n+1}\sqrt{d})(x_1+y_1\sqrt{d}),$$
$$x_n+y_n\sqrt{d}=(x_{n+1}+y_{n+1}\sqrt{d})(x_1-y_1\sqrt{d}),$$

од каде добиваме

$$x_{n+2}=x_1x_{n+1}+dy_1y_{n+1},$$
$$x_n=x_1x_{n+1}-dy_1y_{n+1}.$$

Ако ги собереме последните две равенства добиваме

$$x_{n+2}=2x_1x_{n+1}-x_n.$$

Аналогно се добиваат равенствата

$$y_{n+2}=x_1y_{n+1}+y_1x_{n+1},$$
$$y_n=x_1y_{n+1}-y_1x_{n+1},$$

со чие собирање го добиваме равенството

$$y_{n+2}=2x_1y_{n+1}-y_n.\ ■$$

9.7. За методите за наоѓање на фундаменталнопто решение ќе говориме покасно и како што ќе видиме тоа не е лесен проблем. Но, за некои вредности на d фундаменталното решение може лесно да се определи.

Лема. Ако $a+b\sqrt{d}$ е решение на равенката (1) за кое важи $a>\frac{1}{2}b^2-1$, тогаш тоа е фундаменталното решение на (1). Специјално, ако u и v се природни броеви и $d=u(uv^2+2)$, тогаш $1+uv^2+v\sqrt{d}$ е фундаменталното решение на (1).

Доказ. Ако $b=1$, тогаш тврдењето е очигледно точно. Нека $b>1$ и $x_1+y_1\sqrt{d}$ е фундаменталното решение на (1). Нека претпоставиме дека $b>y_1$. Тогаш од

$$d=\frac{a^2-1}{b^2}=\frac{x_1^2-1}{y_1^2}$$

следува $x_1^2b^2-y_1^2a^2=b^2-y_1^2=\delta$, за некој $\delta\in\mathbb{N}$. Според тоа, $x_1b+y_1a=\delta_1$ и $x_1b-y_1a=\delta_2$, каде $\delta_1\delta_2=\delta$. Сега, имаме

$$a=\frac{\delta_1-\delta_2}{2y_1}\le\frac{\delta-1}{2y_1}=\frac{b^2-y_1^2-1}{2y_1}\le\frac{b^2}{2}-1,$$

што е противречност.

Специјалнот случај следува од $(1+uv^2)^2-u(uv^2+2)v^2=1$ и $1+uv^2>\frac{v^2}{2}-1$. ■

9.8. Пример. Во множеството природни броеви реши ја равенката

$$x^2-2y^2=1. \tag{7}$$

Решение. Лесно се гледа дека фундаменталното решение на равенката (7) е $(x_1,y_1)=(3,2)$. Според теоремата 9.6 сите решенија на (7) се дадени со формулите (6), каде $(x_0,y_0)=(1,0)$. За првите четири нетривијални решенија имаме:

$$x_1=3, y_1=2,$$
$$x_2=2\cdot3\cdot3-1=17,\ y_2=2\cdot3\cdot2-0=12,$$
$$x_3=2\cdot3\cdot17-3=99,\ y_3=2\cdot3\cdot12-2=70 \text{ и}$$
$$x_4=2\cdot3\cdot99-17=577,\ y_3=2\cdot3\cdot70-12=408. \blacksquare$$

9.9. Коментар. Во претходните разгледувања видовме дека за да ја решиме равенката (1) ни преостанува уште да го определиме нејзиното фундаментално решение. Во пример 9.8 тоа го направивме со проба, но последното не е секогаш лесно да се направи. Така на пример, фундаменталното решение на равенката $x^2-61y^2=1$ е $(x_1,y_1)=(1766319049,226153980)$, па е бесмислено истото да се определува со проба. Затоа во следните разгледувања ќе дадеме два метода за ределување на фундаменталното решение на равенката (1).

9.10. Метод на Чакравала. Овој метод го открил средновековниот индиски математичар Чакравала и истиот се базира на идентитетот

$$(x_1^2-dy_1^2)(x_2^2-dy_2^2)=(x_1x_2+dy_1y_2)^2-d(x_1y_2+y_1x_2)^2. \tag{8}$$

Нека (x_1,y_1) е произволен пар таков што $(x_1,y_1)=1$ и да ставиме $x_1^2-dy_1^2=k_1$. Ако во (8) на местото (x_2,y_2) ставиме $(m,1)$ го добиваме равенството

$$(mx_1+dy_1)^2-d(x_1+my_1)^2=(m^2-d)k_1.$$

Сега m ќе го избереме така што $k_1\mid x_1+my_1$ и $|m^2-d|$ прима најмала можна вредност. Тогаш од

$$(m^2-d)y_1^2=(-my_1)^2-dy_1^2\equiv x_1^2-dy_1^2\equiv0(\mathrm{mod}\,k_1)$$

следува $k_1\mid m^2-d$, а оттука следува дека

$$mx_1+dy_1\equiv mx_1+m^2y_1=m(x_1+my_1)\equiv0(\mathrm{mod}\,k_1),$$

т.е. $k_1\mid mx_1+dy_1$. Според тоа, сите собирци во равенството

$$(\frac{mx_1+dy_1}{|k_1|})^2-d(\frac{x_1+my_1}{|k_1|})^2=\frac{m^2-d}{k_1}$$

се цели броеви. Така, од тројката (x_1,y_1,k_1) ја добивме тројката $(x_2,y_2,k_2)=(\frac{mx_1+dy_1}{|k_1|},\frac{x_1+my_1}{|k_1|},\frac{m^2-d}{k_1})$. Постапката ја продолжуваме се додека не добиеме тројка $(x_n,y_n,1)$, односно решение на равенката (1). Лагранж докажал дека оваа постапка е конечна.

Пример. Ќе го определиме фундаменталното решение на равенката

$$x^2-67y^2=1. \tag{9}$$

Чекор 1. Избираме $(x_1,y_1)=(8,1)$ и $k=8^2-67\cdot 1^2=-3$.

Чекор 2. Избираме m така што $k=-3\mid x_1+my_1=8+m$ и $|m^2-67|$ е најмал можен број. Тоа е $m=7$. Добиваме $(x_2,y_2,k_2)=(\frac{7\cdot 8+67\cdot 1}{3},\frac{8+7\cdot 1}{3},\frac{7^2-67}{-3})=(41,5,6)$.

Чекор 3. Избираме m така што $k=6\mid 41+5m$ и $|m^2-67|$ е најмал можен број. Тоа е $m=5$. Добиваме $(x_3,y_3,k_3)=(\frac{5\cdot 41+67\cdot 5}{6},\frac{41+5\cdot 5}{6},\frac{5^2-67}{6})=(90,11,-7)$.

Чекор 4. Изборот на $m=9$ дава $(x_4,y_4,k_4)=(221,27,-2)$.

Чекор 5. Изборот на $m=9$ дава $(x_4,y_4,k_4)=(1899,232,-7)$ итн.

Чекор 8. $(x_8,y_8,k_8)=(48842,5967,1)$ и тоа е фундаменталното решение на равенката (9). ■

9.11. Метод на верижни дропки. Во теоремата VII 8.9 видовме дека ако природниот број d не е точен квадрат, тогаш $\sqrt{d}$ може да се претстави како периодична верижна дропка од облик

$$\sqrt{d}=\langle a_0;\overline{a_1,a_2,\ldots,a_{n-1},2a_0}\rangle, \text{ каде } a_0=[\sqrt{d}].$$

Понатаму, конечната верижна дропка

$$\langle a_0;a_1,a_2,\ldots,a_{n-1}\rangle$$

сооодветствува на рационален број $\frac{x}{y},(x,y)=1$ за кој важи $x^2-dy^2=(-1)^n$. Ако n е парен број, тогаш парот (x,y) е фундаменталното решение на равенката (1), а ако n е непарен број, тогаш фундаментално решение на равенката (1) е парот (x,y) кој соодветствува на дропката $\frac{x}{y}$ која е вредноста на верижната дропка

$$\langle a_0;a_1,a_2,\ldots,a_{n-1},2a_0,a_1,a_2,\ldots,a_{n-1}\rangle.$$

Пример. Ќе го определиме фундаменталното решение на равенката

$$x^2-61y^2=1. \tag{10}$$

Имаме,

$$\sqrt{61}=\langle 7;\overline{1,4,3,1,2,2,1,3,4,1,14}\rangle .$$

Периодот на верижната дропка е 11, т.е. тој е непарен број, па затоа ја пресметуваме вредноста $\frac{x}{y}$ на конечната верижна дропка

$$\langle 7;1,4,3,1,2,2,1,3,4,1,14,1,4,3,1,2,2,1,3,4,1\rangle .$$

Имаме, $\frac{x}{y}=\frac{1766319049}{226153980}$, па затоа $(x_1,y_1)=(1766319049,226153980)$ е фундаментално решение на равенката (10). ■

9.12. Пример. Докажи дека постојат бесконечно многу триаголници кои не се складни и чии должини на страни се три последователни природни броја, а плоштината исто така е природен број.

Решение. Ако должините на страните на триаголникот се $n-1,n,n+1$, тогаш неговата плоштина е $P=\frac{n}{4}\sqrt{3(n^2-4)}$. Ако n е непарен, тогаш P не е природен број. Нека $n=2m$. Тогаш $P=m\sqrt{3(m^2-1)}$, па затоа е потребно и доволно да докажеме дека постојат бесконечно многу броеви m за кои $m^2-1=3k^2$. Но, според теоремата 9.5 равенката на Пел $m^2-3k^2=1$ во множеството природни броеви има бесконечно многу решенија. Нејзино фундаментално решение е $(m_1,k_1)=(2,1)$, па ако ставиме $(m_0,k_0)=(1,0)$, тогаш според теоремата 9.6 сите нејзини решенија се дадени со

$$m_{n+2}=2m_1m_{n+1}-m_n,\quad k_{n+2}=2m_1k_{n+1}-k_n,\ n\geq 0 .\ \blacksquare$$

9.13. Пример. Определи ги сите природни броеви d за кои равенката на Пел $x^2-dy^2=1$ има решение за кое важи $x-y=d$.

Решение. Во множеството природни броеви треба да ја решиме равенката $(x+d)^2-dx^2=1$. Последната равенка е еквивалентна со равенката

$$2dx+(d^2-1)=(d-1)x^2,$$

од каде следува дека $d-1\mid 2dx$, односно $d-1\mid 2x$. Ставаме $2x=(d-1)t$, $t\in\mathbb{N}$ и равенката ја сведуваме на равенката

$$4dt+4(d+1)=(d-1)^2t^2.$$

Но, $4(d+1)t\geq 4(d+1)$, па затоа $4dt+4(d+1)t\geq 4dt+4(d+1)$, што значи

$$(8d+4)t\geq 4dt+4(d+1)=(d-1)^2t^2\geq (d-1)^2t,$$

т.е. $8d+4 \geq (d-1)^2$. Но, d е природен број, па од последната неравенка добиваме $d \leq 10$. Со испитување на вредностите за d наоѓаме дека единствено решение е $d=5$ и тогаш $(x,y)=(9,5)$. ■

9.14. Пример. Докажи дека ако разликата на третите степени на два последователни приуродни броја е n^2, тогаш $2n-1$ е точен квадрат.

Решение. Условот на задачата последователно е еквивалентен на

$$(m+1)^3 - m^3 = n^2,$$
$$3m^2+3m+1 = n^2,$$
$$(2n)^2 - 3(2m+1)^2 = 1.$$

Бидејќи фундаменталното решение на равенката на Пел $x^2-3y^2=1$ е $(2,1)$, заклучуваме дека

$$2n+(2m+1)\sqrt{3} = (2+\sqrt{3})^k$$

за некој природен број k. Со споредување на коефициентите пред $\sqrt{3}$ добиваме дека k е непарен природен број. Нека $k=2t+1$. Тогаш ако се искористи дека за решенијата (4) на равенката (1) важи

$$x_n = \frac{(x_1+y_1\sqrt{d})^n+(x_1-y_1\sqrt{d})^n}{2},\ y_n = \frac{(x_1+y_1\sqrt{d})^n-(x_1-y_1\sqrt{d})^n}{2\sqrt{d}},\ n \in \mathbb{N}$$

и дека $(1+\sqrt{3})^2 = 2(2+\sqrt{3})$ и $(1-\sqrt{3})^2 = 2(2-\sqrt{3})$, добиваме:

$$\begin{aligned} 4(2n-1) &= 4\left(\frac{(2+\sqrt{3})^{2t+1}+(2-\sqrt{3})^{2t+1}}{2}-1\right) \\ &= (1+\sqrt{3})^2(2+\sqrt{3})^{2t} + (1-\sqrt{3})^2(2-\sqrt{3})^{2t} - 4 \\ &= ((1+\sqrt{3})(2+\sqrt{3})^t + (1-\sqrt{3})(2-\sqrt{3})^t)^2. \end{aligned}$$

Конечно, од последното равенство следува дека $2n-1$ е точен квадрат. ■

IX ГЛАВА
КВАДРАТНИ ПОЛИЊА

1. ПОИМ ЗА КВАДРАТНО ПОЛЕ. ОСНОВНИ СВОЈСТВА

1.1. Лема. Нека $d \neq 1$ е цел број кој не е делив со квадрат на цел број. Множеството $\mathbb{Q}[\sqrt{d}] = \{x + y\sqrt{d} \mid x, y \in \mathbb{Q}\}$ со вообичаените операции собирање и множење е поле.

Доказ. Нека $\alpha = a_1 + a_2\sqrt{d}, \beta = b_1 + b_2\sqrt{d}$, $a_1, a_2, b_1, b_2 \in \mathbb{Q}$.

а) Имаме

$$\alpha + \beta = (a_1 + b_1) + (a_2 + b_2)\sqrt{d} \text{ и } \alpha\beta = (a_1b_1 + a_2b_2d) + (a_1b_2 + a_2b_1)\sqrt{d},$$

што значи дека множеството $\mathbb{Q}[\sqrt{d}]$ е затворено во однос на операциите собирање и множење.

б) За секои $\alpha, \beta, \gamma \in \mathbb{Q}[\sqrt{d}]$ важи $\alpha, \beta, \gamma \in \mathbb{C}$, па затоа

$$\alpha + \beta = \beta + \alpha, (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma), \ \alpha\beta = \beta\alpha, \ (\alpha\beta)\gamma = \alpha(\beta\gamma) \text{ и } (\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma.$$

в) Јасно, $0, 1 \in \mathbb{Q}[\sqrt{d}]$ и важи $1 = 1 \cdot \alpha = \alpha + 0 = a$, за секој $\alpha \in \mathbb{Q}[\sqrt{d}]$.

г) Ако $\alpha = a_1 + a_2\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, тогаш $-\alpha = -a_1 - a_2\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ и $\alpha + (-\alpha) = 0$.

д) Ако $\alpha = a_1 + a_2\sqrt{d} \in \mathbb{Q}[\sqrt{d}] \setminus \{0\}$, тогаш $a_1 \neq 0$ или $a_2 \neq 0$, па затоа важи $a_1 - a_2\sqrt{d} \neq 0$. Значи, $a_1^2 - da_2^2 \neq 0$ и затоа $\alpha^{-1} = \frac{a_1 - a_2\sqrt{d}}{a_1^2 - da_2^2} \in \mathbb{Q}[\sqrt{d}]$ и $\alpha\alpha^{-1} = 1$.

Конечно, од а) – д) следува дека алгебарската структура $(\mathbb{Q}[\sqrt{d}], +, \cdot)$ е поле. ■

1.2. Дефиниција. Нека $d \neq 1$ е цел број кој не е делив со квадрат на цел број поголем од 1. Тогаш полето $(\mathbb{Q}[\sqrt{d}], +, \cdot)$ го нарекуваме *квадратно поле* или *квадратно проширување* на полето $\mathbb{Q}$.

Квадратнои поле $\mathbb{Q}[\sqrt{d}]$ ќе велиме дека е *реално* ако $d > 0$, а ако $d < 0$, тогаш за $\mathbb{Q}[\sqrt{d}]$ ќе велиме дека е *имагинарно*.

Јасно, за секој рационален број a важи $a = a + 0 \cdot \sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, т.е. $\mathbb{Q} \subset \mathbb{Q}[\sqrt{d}]$.

1.3. Дефиниција. Нека $\alpha = u + v\sqrt{d}$ е елемент на квадратното поле $\mathbb{Q}[\sqrt{d}]$. *Коњугат* на елементот α е $\overline{\alpha} = u - v\sqrt{d}$, а негова *норма* е $N(\alpha) = \alpha\overline{\alpha} = u^2 - dv^2$.

1.4. Теорема. а) $\alpha=\bar{\alpha}$ ако и само ако $\alpha\in\mathbb{Q}$.

б) Ако $\alpha,\beta\in\mathbb{Q}[\sqrt{d}]$, тогаш $\overline{(\bar{\alpha})}=\alpha$, $\overline{\alpha+\beta}=\bar{\alpha}+\bar{\beta}$, $\overline{\alpha-\beta}=\bar{\alpha}-\bar{\beta}$ и $\overline{\alpha\beta}=\bar{\alpha}\cdot\bar{\beta}$.

в) Ако $\alpha,\beta\in\mathbb{Q}[\sqrt{d}]$ и $z\neq 0$, тогаш $\overline{(\frac{\beta}{\alpha})}=\frac{\bar{\beta}}{\bar{\alpha}}$.

Доказ. а) Ако $\alpha=a+0\cdot\sqrt{d}$ е рационален број, тогаш $\bar{\alpha}=a-0\cdot\sqrt{d}=\alpha$.

Обратно, нека $\alpha=a+b\sqrt{d}$. Ако $\alpha=\bar{\alpha}$, тогаш $a+b\sqrt{d}=a-b\sqrt{d}$, па затоа $b=-b$, т.е. $b=0$. Според тоа, $\alpha=a+b\sqrt{d}=a+0\cdot\sqrt{d}=a\in\mathbb{Q}$.

б) Нека $\alpha=u+v\sqrt{d}$ и $\beta=s+t\sqrt{d}$. Тогаш

$$\overline{(\bar{\alpha})}=\overline{a-b\sqrt{d}}=a-(-b)\sqrt{d}=a+b\sqrt{d}=\alpha,$$

$$\overline{\alpha+\beta}=\overline{u+s+(v+t)\sqrt{d}}=u+s-(v+t)\sqrt{d}=(u-v\sqrt{d})+(s-t\sqrt{d})=\bar{\alpha}+\bar{\beta},$$

$$\overline{\alpha-\beta}=\overline{u-s+(v-t)\sqrt{d}}=u-s-(v-t)\sqrt{d}=(u-v\sqrt{d})-(s-t\sqrt{d})=\bar{\alpha}-\bar{\beta}\text{ и}$$

$$\overline{\alpha\beta}=\overline{us+vtd+(ut+vs)\sqrt{d}}=us+vtd-(ut+vs)\sqrt{d}=(u-v\sqrt{d})(s-t\sqrt{d})=\bar{\alpha}\cdot\bar{\beta}.$$

в) Нека Нека $\alpha=u+v\sqrt{d}$ и $\beta=s+t\sqrt{d}$. Ако $\alpha\neq 0$, тогаш $u\neq 0$ или $v\neq 0$, па затоа $\bar{\alpha}=u-v\sqrt{d}$. Освен тоа, $\frac{1}{\alpha\bar{\alpha}}=\frac{1}{u^2-dv^2}\in\mathbb{Q}$, па од б) следува

$$\overline{(\frac{\beta}{\alpha})}=\overline{(\frac{1}{\alpha\bar{\alpha}}\beta\bar{\alpha})}=\frac{1}{\bar{\alpha}\bar{\alpha}}\bar{\beta}\bar{\bar{\alpha}}=\frac{1}{\alpha\bar{\alpha}}\bar{\beta}\bar{\bar{\alpha}}=\frac{1}{\alpha\bar{\alpha}}\bar{\beta}\alpha=\frac{\bar{\beta}}{\bar{\alpha}}.\ \blacksquare$$

1.5. Теорема. Нека $\mathbb{Q}[\sqrt{d}]$ е квадратно поле. Тогаш

а) ако $\alpha\in\mathbb{Q}$, тогаш $N(\alpha)=\alpha^2$,

б) Ако $\alpha\in\mathbb{Q}[\sqrt{d}]$, тогаш $N(\alpha)\in\mathbb{Q}$,

в) $N(\alpha)=0$ ако и само ако $\alpha=0$,

г) ако $d<0$, тогаш $N(\alpha)\geq 0$,

д) $N(\alpha\beta)=N(\alpha)N(\beta)$ за секои $\alpha,\beta\in\mathbb{Q}[\sqrt{d}]$, а ако $\beta\neq 0$, тогаш $N(\frac{\alpha}{\beta})=\frac{N(\alpha)}{N(\beta)}$.

Доказ. а) Ако $\alpha\in\mathbb{Q}$, тогаш $\alpha=\bar{\alpha}$, па затоа $N(\alpha)=\alpha\bar{\alpha}=\alpha^2$.

б) Нека $\alpha=u+v\sqrt{d}$. Тогаш $N(\alpha)=\alpha\bar{\alpha}=(u+v\sqrt{d})(u-v\sqrt{d})=u^2-dv^2\in\mathbb{Q}$.

в) Ако $\alpha=0$, тогаш $\bar{\alpha}=0$, па затоа $N(\alpha)=0$. Ако $N(\alpha)=0$, тогаш $\alpha\bar{\alpha}=0$, па затоа $\alpha=0$ или $\bar{\alpha}=0$. Но од $\bar{\alpha}=0$ следува $\alpha=0$.

г) Нека $\alpha=u+v\sqrt{d}$. Ако $d<0$, тогаш $-d>0$, па како $u^2\geq 0$ и $v^2\geq 0$, добиваме $N(\alpha)=u^2-dv^2\geq 0$.

д) Нека $\alpha=u+v\sqrt{d}$ и $\beta=s+t\sqrt{d}$. Тогаш

$$N(\alpha\beta)=\alpha\beta\overline{\alpha\beta}=\alpha\bar{\alpha}\cdot\beta\bar{\beta}=N(\alpha)N(\beta).$$

Ако $\beta \neq 0$, тогаш

$$N(\tfrac{\alpha}{\beta}) = \tfrac{\alpha}{\beta} \cdot \overline{(\tfrac{\alpha}{\beta})} = \tfrac{\alpha}{\beta} \cdot \tfrac{\bar{\alpha}}{\bar{\beta}} = \tfrac{\alpha\bar{\alpha}}{\beta\bar{\beta}} = \tfrac{N(\alpha)}{N(\beta)} . \blacksquare$$

1.6. Лема. Ако α е ирационален број таков што $\alpha \in \mathbb{Q}[\sqrt{d}] \cap \mathbb{Q}[\sqrt{d_1}]$, тогаш $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}[\sqrt{d_1}]$.

Доказ. Нека претпоставиме дека $\alpha \in \mathbb{Q}[\sqrt{d}] \cap \mathbb{Q}[\sqrt{d_1}]$, т.е. дека $\alpha = a + b\sqrt{d} = a_1 + b_1\sqrt{d_1}$. Тоа значи, $\bar{\alpha} \in \mathbb{Q}[\sqrt{d}]$ и $\bar{\alpha} \in \mathbb{Q}[\sqrt{d_1}]$, односно

$$\bar{\alpha} = a - b\sqrt{d} = a_1 - b_1\sqrt{d_1} .$$

Затоа

$$b\sqrt{d} = \tfrac{\alpha - \bar{\alpha}}{2} = b_1\sqrt{d_1}$$

и како $b \neq 0$ добиваме $\sqrt{dd_1} = \tfrac{b_1 d_1}{b}$, од каде $\sqrt{dd_1} \in \mathbb{Q}$. Значи дека постојат $r, s \in \mathbb{N}$ такви што $(r,s) = 1$ и $\sqrt{dd_1} = \tfrac{r}{s}$, т.е. $s^2 dd_1 = r^2$. Ќе докажеме дека $s = 1$. Ако $s > 1$, тогаш постои прост делител p на s и од равенството $s^2 dd_1 = r^2$ следува $p \mid r$, што противречи на $(r,s) = 1$.

Според тоа, $\sqrt{dd_1}$ е природен број, што значи дека секој прост фактор во каноничното претставување на dd_1 се јавува на парен степен. Но, d и d_1 не се деливи со квадрати на природни броеви, па затоа $d = d_1$, односно $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}[\sqrt{d_1}]$. $\blacksquare$

1.7. Пример. а) Докажи дека не постојат $m, n \in \mathbb{Z}$ такви што $(3+i)^m = (7+i)^n$.

б) Докажи дека не постојат природни броеви m и n такви што

$$(5 + 3\sqrt{2})^m = (7 + 4\sqrt{2})^n .$$

Решение. а) Ако такви m и n постојат, тогаш

$$10^m = N((3+\sqrt{-1})^m) = N((7+\sqrt{-1})^n) = 50^n ,$$

што не е можно.

б) Ако го конјугираме даденото равенство добиваме

$$(5 - 3\sqrt{2})^m = (7 - 4\sqrt{2})^n .$$

Но,

$$0 < 5 - 3\sqrt{2} < 1 < 7 - 4\sqrt{2} ,$$

па затоа десната страна во последното равенство е поголема од 1, а левата е помала од 1, што е противречност. $\blacksquare$

2. КВАДРАТНО ЦЕЛИ БРОЕВИ

2.1. Да забележиме дека бројот $\alpha = a + b\sqrt{d}$ е корен на полиномот

$$P(x) = x^2 - 2ax + (a^2 - b^2 d). \tag{1}$$

Исто така и $\bar{\alpha} = a - b\sqrt{d}$ е корен на полиномот (1).

Нека $\alpha \in \mathbb{Q}[\sqrt{d}]$ е корен на полиномот

$$P(x) = ax^2 + bx + c,\ a,b,c \in \mathbb{Z}. \tag{2}$$

Бидејќи $a,b,c \in \mathbb{Z} \subset \mathbb{Q}$ и $P(\alpha) = 0$ добиваме

$$P(\bar{\alpha}) = a\bar{\alpha}^2 + b\bar{\alpha} + c = \bar{a}\overline{\alpha^2} + \bar{b}\bar{\alpha} + \bar{c} = \overline{a\alpha^2} + \overline{b\alpha} + \bar{c} = \overline{a\alpha^2 + b\alpha + c} = \bar{0} = 0.$$

Значи, α е корен на (2) ако и само ако $\bar{\alpha}$ е корен на (2). Ако α е ирационален број, тогаш $\alpha \neq \bar{\alpha}$, па затоа

$$P(x) = ax^2 + bx + c = a(x - \alpha)(x - \bar{\alpha}).$$

Според тоа, ако α е ирационален број, тогаш постојат бесконечно многу квадратни полиноми со целобројни коефициенти чиј корен е α, но сите тие се добиваат од еден полином кој го множиме со цели броеви. Ако полиномот (2) го поделиме со (a,b,c) и го помножиме со -1, ако тоа е потребно, добиваме единствен квадратен полином со позитивен водечки коефициент. Од претходната дискусија следува дека следнава дефиниција е коректна.

2.2. Дефиниција. Ако α е ирационален број во $\mathbb{Q}[\sqrt{d}]$, тогаш полиномот (2) го нарекуваме *определувачки* за α ако α е корен на (2), $a,b,c \in \mathbb{Z}$, $(a,b,c) = 1$ и $a > 0$.

Бројот $\alpha \in \mathbb{Q}[\sqrt{d}]$ го нарекуваме *квадратно цел број* ако $\alpha \in \mathbb{Z}$ или ако α е ирационален и определувачкиот полином на α е моничен.

2.3. Забелешка. Во квадратното поле $\mathbb{Q}[\sqrt{d}]$ секој елемент $\alpha = a + b\sqrt{d}$, каде $a,b \in \mathbb{Z}$ е квадратно цел, бидејќи $\alpha \in \mathbb{Z}$ или α е ирационален број кој е нула на моничниот полином (1) за чии коефициенти важи $(1, -2a, a^2 - b^2 d) = 1$.

Меѓутоа, тоа не мора да се единствените квадратно цели броеви во $\mathbb{Q}[\sqrt{d}]$. Навистина, во квадратното поле $\mathbb{Q}[\sqrt{-3}]$ елементот $\alpha = \frac{-1+\sqrt{-3}}{2}$ е квадратно цел бидејќи неговиот определувачки полином е $P(x) = x^2 + x + 1$.

2.4. Теорема. Ако $d \equiv 2$ или $3 \pmod 4$, тогаш квадратно цели броеви во $\mathbb{Q}[\sqrt{d}]$ се сите броеви од облик $u + v\sqrt{d}$, $u,v \in \mathbb{Z}$.

Ако $d \equiv 1 (\mathrm{mod}\, 4)$, тогаш квадратно цели броеви во $\mathbb{Q}[\sqrt{d}]$ се сите броеви од облик $s + \frac{1+\sqrt{d}}{2} t$, $s,t \in \mathbb{Z}$.

Доказ. Нека $\alpha = u + v\sqrt{d}$ е квадратно цел број во $\mathbb{Q}[\sqrt{d}]$. Тоа значи, $\alpha \in \mathbb{Z}$ или α е ирационален број. Ако α е ирационален број, тогаш земаме $a = 2u$, $b = 2v$ и $c = u^2 - dv^2$ и притоа α е нула на полиномот $P(x) = x^2 - ax + c$. Тоа значи дека определувачкиот полином на α е полином од видот $kP(x)$, каде k е најмалиот заеднички именител на рационалните броеви броеви a и c. Но, α е квадратно цел број, па затоа полиномот $kP(x)$ е моничен, што значи дека $k = 1$, т.е. a и c се цели броеви. Понатаму, $db^2 = a^2 - 4c$ и како d не е делив со квадрат на цел број поголем од 1, заклучуваме дека $b \in \mathbb{Z}$.

Нека $d \equiv 2$ или $3 (\mathrm{mod}\, 4)$. Тогаш

$$a^2 \equiv 0 \text{ или } 1 (\mathrm{mod}\, 4) \text{ и } db^2 \equiv 0, 2 \text{ или } 3 (\mathrm{mod}\, 4),$$

па како $db^2 \equiv a^2 (\mathrm{mod}\, 4)$, добиваме дека броевите a и b се парни, што значи дека $u, v \in \mathbb{Z}$.

Ако $d \equiv 1 (\mathrm{mod}\, 4)$, тогаш $b^2 \equiv a^2 (\mathrm{mod}\, 4)$, па затоа a и b се со иста парност. Затоа $u - v = \frac{1}{2}(a - b)$ е цел број. Ставаме $s = u - v, t = 2v$. Тогаш $s,t \in \mathbb{Z}$ и притоа важи $u + v\sqrt{d} = s + \frac{1+\sqrt{d}}{2} t$. ■

2.5. Последица. Ако $d \equiv 1 (\mathrm{mod}\, 4)$, тогаш $\alpha \in \mathbb{Q}[\sqrt{d}]$ е квадратно цел број ако и само ако $\alpha = \frac{a+b\sqrt{d}}{2}$, каде $a,b \in \mathbb{Z}$ се броеви со иста парност.

Доказ. Нека $d \equiv 1 (\mathrm{mod}\, 4)$.

Ако α е квадратно цел број во $\mathbb{Q}[\sqrt{d}]$, тогаш од теоремата 2.4 следува

$$\alpha = s + \frac{1+\sqrt{d}}{2} t = \frac{2s+t+t\sqrt{d}}{2}, \; s,t \in \mathbb{Z}$$

и притоа $2s + t \equiv t (\mathrm{mod}\, 2)$, односно $2s + t$ и t се броеви со иста парност.

Обратно, нека $\alpha = \frac{a+b\sqrt{d}}{2}$, каде $a,b \in \mathbb{Z}$ се броеви со иста парност. Тогаш

$$\alpha = \frac{a+b\sqrt{d}}{2} = \frac{a-b}{2} + \frac{1+\sqrt{d}}{2} b,$$

каде $\frac{a-b}{2}, b \in \mathbb{Z}$, па од теоремата 2.4 следува дека α е квадратно цел број. ■

2.6. Последица. Ако α е квадратно цел број во $\mathbb{Q}[\sqrt{d}]$, тогаш $N(\alpha) \in \mathbb{Z}$.

Доказ. Нека α е квадратно цел број во $\mathbb{Q}[\sqrt{d}]$.

Ако $d \equiv 2$ или $3 (\mathrm{mod}\, 4)$, тогаш $\alpha = u + v\sqrt{d}$, $u, v \in \mathbb{Z}$, па затоа

$$N(\alpha) = u^2 - dv^2 \in \mathbb{Z}.$$

Ако $d \equiv 1 (\mathrm{mod}\, 4)$, тогаш $\alpha = u + v\frac{1+\sqrt{d}}{2}$, $u, v \in \mathbb{Z}$, па затоа

$$N(\alpha) = (u + v\tfrac{1+\sqrt{d}}{2})(u + v\tfrac{1-\sqrt{d}}{2}) = u^2 + uv - \tfrac{d-1}{4}v^2 \in \mathbb{Z}. \blacksquare$$

2.7. Коментар. Според теоремата 2.4 ако $d \equiv 2$ или $3 (\mathrm{mod}\, 4)$, тогаш множеството квадратно цели броеви е

$$\mathbb{Z}[\sqrt{d}] = \{u + v\sqrt{d} \mid u, v \in \mathbb{Z}\},$$

а ако $d \equiv 1 (\mathrm{mod}\, 4)$, тогаш множеството квадратно цели броеви е

$$\mathbb{Z}[\tfrac{1+\sqrt{d}}{2}] = \{u + v\tfrac{1+\sqrt{d}}{2} \mid u, v \in \mathbb{Z}\} = \{u + v\tfrac{-1+\sqrt{d}}{2} \mid u, v \in \mathbb{Z}\} = \mathbb{Z}[\tfrac{-1+\sqrt{d}}{2}].$$

б) Квадратно целите броеви во полето $\mathbb{Q}[\sqrt{-1}]$ се таканаречените *Гаусови цели броеви* $u + iv$, $u, v \in \mathbb{Z}$, а квадратно целите броеви во полето $\mathbb{Q}[\sqrt{-3}]$ се таканаречените *Ајзенштајнови цели броеви* $u + v\alpha$, $u, v \in \mathbb{Z}$, каде $\alpha = \frac{-1+i\sqrt{3}}{2}$ е примитивен трети корен на единицата.

2.8. Лема. Ако α и β се квадратно цели броеви во $\mathbb{Q}[\sqrt{d}]$, тогаш $\alpha + \beta, \alpha - \beta$ и $\alpha\beta$ се квадратно цели броеви во $\mathbb{Q}[\sqrt{d}]$.

Доказ. Ќе ги разгледаме случаите $d \equiv 1 (\mathrm{mod}\, 4)$ и $d \not\equiv 1 (\mathrm{mod}\, 4)$. За поедноставно означување ставаме

$$w = \begin{cases} \sqrt{d}, & d \not\equiv 1 (\mathrm{mod}\, 4) \\ \frac{1+\sqrt{d}}{2}, & d \equiv 1 (\mathrm{mod}\, 4). \end{cases}$$

Според теоремата 2.4 бројот $\gamma \in \mathbb{Q}[\sqrt{d}]$ е квадратно цел ако и само ако може да се запише во видот

$$\gamma = m + nw \text{ каде } m, n \in \mathbb{Z}. \qquad (3)$$

Броевите α и β се квадратно цели во $\mathbb{Q}[\sqrt{d}]$, па затоа

$$\alpha = a + bw, \beta = c + ew \text{ каде } a, b, c, e \in \mathbb{Z}.$$

Според тоа,

$$\alpha + \beta = (a + c) + (b + e)w, \quad a + c, b + e \in \mathbb{Z}$$
$$\alpha - \beta = (a - c) + (b - e)w, \quad a - c, b - e \in \mathbb{Z}$$

што значи дека броевите $\alpha + \beta$ и $\alpha - \beta$ може да се запишат во обликот (3), па затоа тие се квадратни цели броеви.

Имаме, $w^2 = sw+t$, каде $s=0, t=d$ ако $d \not\equiv 1 \pmod 4$ и $s=1$, $t=\frac{d-1}{4}$ ако $d \equiv 1 \pmod 4$. Затоа,

$$\alpha\beta = ac+(ae+bc)w+bew^2 = ac+(ae+bc)w+be(sw+t)$$
$$= (ac+bet)+(ae+bc+bes)w,$$

што значи дека $\alpha\beta$ може да се запишпе во обликот (3), па затоа тој е квадратно цел број. ■

2.9. Пример. Нека x, y се квадратно цели броеви во некое квадратно поле $\mathbb{Q}[\sqrt{d}]$, такви што $N(x)=1$ и $N(y)=2$. Ако $N(x+y)>0$, определи ја најмалата можна вредност на $N(x+y)$.

Решение. Нека $x=a+b\sqrt{d}$ и $y=u+v\sqrt{d}$. Имаме

$$N(x+y) = (a+u)^2 - d(b+v)^2 = N(x)+N(y)+2(au-dbv).$$

Бидејќи

$$(au-dbv)^2 = N(x)N(y)+d(av-bu)^2 \geq N(x)N(y),$$

следува дека

$$N(x+y) \geq (N(x)^{\frac{1}{2}}+N(y)^{\frac{1}{2}})^2 = (\sqrt{2}+1)^2 > 5$$

или

$$N(x+y) \leq (N(x)^{\frac{1}{2}}-N(y)^{\frac{1}{2}})^2 = (\sqrt{2}-1)^2 < 1.$$

Втората можност отпаѓа, па мора да важи $N(x+y) \geq 6$. Ако $N(x+y)=6$, од горните равенства следува $au-dbv=\frac{3}{2}$ и $(av-bu)^2=\frac{1}{4d}$, што не е можно бидејќи d не е делив со квадрат на природен број различен од 1. Според тоа, $N(x+y) \geq 7$. Најмалата вредност $N(x+y)=7$ се достигнува во $\mathbb{Q}[\sqrt{2}]$ за $x=1$ и $y=2-\sqrt{2}$. ■

3. ДЕЛИВОСТ ВО $\mathbb{Q}[\sqrt{d}]$

3.1. Дефиниција. Ако α и β се квадратно цели броеви во $\mathbb{Q}[\sqrt{d}]$, $\alpha \neq 0$, ќе велиме дека α е *делител* на β, во ознака $\alpha \mid \beta$, ако постои квадратно цел број $\gamma \in \mathbb{Q}[\sqrt{d}]$ таков што $\beta = \alpha\gamma$.

Секогаш кога ќе пишуваме $\alpha \mid \beta$ претпоставуваме дека α и β се квадратно цели броеви во $\mathbb{Q}[\sqrt{d}]$ и $\alpha \neq 0$.

3.2. Теорема. а) Ако $\alpha \mid \beta$ и $\alpha \mid \gamma$, тогаш $\bar{\alpha} \mid \bar{\beta}$ и за секои квадратно цели броеви $a,b \in \mathbb{Q}[\sqrt{d}]$ важи $\alpha \mid (a\beta + b\gamma)$.

б) Ако $\alpha \mid \beta$ и $\beta \mid \gamma$, тогаш $\alpha \mid \gamma$.

в) Ако α,β,γ се квадратно цели броеви во $\mathbb{Q}[\sqrt{d}]$ такви што $\alpha \mid \gamma$, $\beta \mid \gamma$ и $(N(\alpha), N(\beta)) = 1$, тогаш $\alpha\beta \mid \gamma$.

Доказ. а) Според дефиницијата 3.1 постојат квадратно цели броеви δ и η такви што $\beta = \alpha\delta$ и $\gamma = \alpha\eta$. Тогаш $\bar{\beta} = \bar{\alpha}\bar{\delta}$ и $a\beta + b\gamma = a\alpha\delta + b\alpha\eta = \alpha(a\delta + b\eta)$. Понатаму, според 2.1 броевите $\bar{\beta}, \bar{\alpha}$ и $\bar{\delta}$ се квадратно цели и како $\bar{\beta} = \bar{\alpha}\bar{\delta}$, $\bar{\alpha} \neq 0$, од дефиницијата 3.1 следува дека $\bar{\alpha} \mid \bar{\beta}$. Од лемата 2.8 следува дека броевите $a\beta + b\gamma$ и $a\delta + b\eta$ се квадратно цели, па како $a\beta + b\gamma = \alpha(a\delta + b\eta)$, од дефиницијата 3.1 следува дека $\alpha \mid (a\beta + b\gamma)$.

б) $\alpha \mid \beta$ и $\beta \mid \gamma$, тогаш постојат квадратно цели броеви δ и η такви што $\beta = \alpha\delta$ и $\gamma = \beta\eta$. Затоа $\gamma = \beta\eta = \alpha(\delta\eta)$ и како $\delta\eta$ е квадратно цел број заклучуваме дека $\alpha \mid \gamma$.

в) Бројот $\delta = \frac{\bar{\beta}\gamma}{\alpha} = m + n\sqrt{d}$ е квадратно цел. Од условот следува $N(\beta) = b \mid \alpha\delta$ и треба да докажеме дека $b \mid \delta$. Ако ставиме $\alpha = p + q\sqrt{d}$, добиваме

$$b \mid \alpha\delta = (pm + qnd) + (pn + qm)\sqrt{d},$$

што значи дека $b \mid pm + qnd$ и $b \mid pn + qm$. Според тоа, b е делител на

$$p(pn + qm) - q(pm + qnd) = n(p^2 - dq^2) = nN(\alpha).$$

Но, $(N(\alpha), b) = (N(\alpha), N(\beta)) = 1$, па затоа $b \mid n$. Слично, b е делител на

$$p(pm + qnd) - dq(pn + qm) = m(p^2 - dq^2) = mN(\alpha),$$

па затоа $b \mid m$. Според тоа, $b \mid \delta$.■

3.3. Дефиниција. Нека α,β,γ се квадратно цели броеви во $\mathbb{Q}[\sqrt{d}]$. Ако $\gamma \mid (\alpha - \beta)$, тогаш ќе велиме дека бројот α е конгруентен со бројот β по модул γ и ќе пишуваме $\alpha \equiv \beta (\mathrm{mod}\, \gamma)$.

3.4. Коментар. Аритметиката со конгруенции по даден модул ν во полето $\mathbb{Q}[\sqrt{d}]$ е доста слична со аритметиката со конгруенциите во множеството $\mathbb{Z}$. Тоа се должи на фактот дека секој цел број ν е квадратно цел во $\mathbb{Q}[\sqrt{d}]$ со норма $N(\nu) = \nu^2$. Така, на пример, тврдењето:

Ако $xy \equiv xz(\mathrm{mod}\, xn)$, *тогаш* $y \equiv z(\mathrm{mod}\, n)$.

е точно и во квадратното поле $\mathbb{Q}[\sqrt{d}]$. Јасно, при кратењето треба да се внимава, бидејќи заедничкиот фактор во конгруенцијата $\alpha\beta \equiv \alpha\delta(\mathrm{mod}\,\gamma)$ може да биде делител на γ, како што е случај во следниов пример.

3.5. Пример. Во конгруенцијата

$$(1+\sqrt{3})x \equiv (1+\sqrt{3})^2(\mathrm{mod}10), \qquad (1)$$

иако бројот $1+\sqrt{3}$ е делител на двете страни, не можеме да скратиме со $1+\sqrt{3}$ бидејќи $(1+\sqrt{3})\,|\,10$, односно

$$10 = 5(\sqrt{3}-1)(1+\sqrt{3})$$

и $5(\sqrt{3}-1)$ е квадреатно цел број во $\mathbb{Q}[\sqrt{3}]$. Според тоа, од конгруенцијата (1) следува конгруенцијата

$$x \equiv 1+\sqrt{3}(\mathrm{mod}\,\tfrac{10}{\sqrt{3}+1}),$$

т.е. конгруенцијата

$$x \equiv 1+\sqrt{3}(\mathrm{mod}\,5(\sqrt{3}-1)). \blacksquare$$

3.6. Дефиниција. За квадратно целиот број ε ќе велиме дека е *единица* во $\mathbb{Q}[\sqrt{d}]$ ако $\varepsilon\,|\,1$.

3.7. Теорема. Квадратно целиот број во $\varepsilon \in \mathbb{Q}[\sqrt{d}]$ е ε е единица ако и само ако $N(\varepsilon) = \pm 1$.

Доказ. Нека ε е единица. Тогаш постои квадратно цел број ε' во $\mathbb{Q}[\sqrt{d}]$ таков што $\varepsilon\varepsilon' = 1$. Значи,

$$N(\varepsilon)N(\varepsilon') = N(\varepsilon\varepsilon') = N(1) = 1.$$

Според последицата 2.6 $N(\varepsilon)$ и $N(\varepsilon')$ се цели броеви, па од последното равенство следува $N(\varepsilon) = \pm 1$.

Обратно, ако $N(\varepsilon) = \pm 1$, тогаш $\varepsilon\bar{\varepsilon} = \pm 1$. Според тоа, за квадратно целите броеви $\varepsilon' = \pm\bar{\varepsilon}$ важи

$$\varepsilon\varepsilon' = \varepsilon(\pm\bar{\varepsilon}) = \pm(\varepsilon\bar{\varepsilon}) = \pm(\pm 1) = 1,$$

што значи дека ε е единица во $\mathbb{Q}[\sqrt{d}]$. $\blacksquare$

3.8. Теорема. Ако ε_1 и ε_2 се единици во $\mathbb{Q}[\sqrt{d}]$, тогаш $\overline{\varepsilon_1}, \varepsilon_1\varepsilon_2, \frac{\varepsilon_1}{\varepsilon_2}$ се единици во $\mathbb{Q}[\sqrt{d}]$.

Доказ. Бидејќи ε_1 и ε_2 се единици во $\mathbb{Q}[\sqrt{d}]$, тие се квадратно цели броеви и постојат квадратно цели броеви δ_1 и δ_2 такви што $\varepsilon_1\delta_1=\varepsilon_2\delta_2=1$. Тогаш $\overline{\varepsilon_1}$, $\varepsilon_1\varepsilon_2$ и $\overline{\delta_1}$ се квадратно цели броеви и важи

$$\overline{\varepsilon_1}\,\overline{\delta_1}=\overline{\varepsilon_1\delta_1}=\overline{1}=1 \text{ и } (\varepsilon_1\varepsilon_2)(\delta_1\delta_2)=(\varepsilon_1\delta_1)(\varepsilon_2\delta_2)=1,$$

па затоа $\overline{\varepsilon_1}$ и $\varepsilon_1\varepsilon_2$ се единици во $\mathbb{Q}[\sqrt{d}]$. Освен тоа, $\frac{\varepsilon_1}{\varepsilon_2}=\frac{\varepsilon_1\delta_2}{\varepsilon_2\delta_2}=\varepsilon_1\delta_2$ е квадратно цел број и важи $\frac{\varepsilon_1}{\varepsilon_2}\varepsilon_2\delta_1=1$, каде $\varepsilon_2\delta_1$ е квадратно цел број, што значи дека $\frac{\varepsilon_1}{\varepsilon_2}$ е единица во $\mathbb{Q}[\sqrt{d}]$. ■

3.9. Теорема. Нека $d<0$ е цел број кој не е делив со квадрат на цел број поголем од 1. Квадратното поле $\mathbb{Q}[\sqrt{d}]$ има единици ±1 и тоа се единствените единици освен во случаите $d=-1$ и $d=-3$. Единиците во $\mathbb{Q}[\sqrt{-1}]$ се $\pm1,\pm i$, а единиците во $\mathbb{Q}[\sqrt{-3}]$ се $\pm1,\frac{1\pm\sqrt{-3}}{2},\frac{-1\pm\sqrt{-3}}{2}$.

Доказ. Според теоремата 3.8 треба да ги определиме сите квадратно цели броеви ε такви што $N(\varepsilon)=\pm1$.

Ако $d\equiv 2 \text{ или } 3 \pmod 4$, тогаш ε има облик $\varepsilon=x+y\sqrt{d}$, $x,y\in\mathbb{Z}$. Следува дека треба да се реши равенката $x^2-dy^2=\pm1$. Бидејќи d е негативен, случајот $x^2-dy^2=-1$ отпаѓа. Ако $d\le -1$, тогаш $x^2-dy^2\ge 2y^2$, па затоа единствено решение е $y=0$ $x=\pm1$, па затоа $\varepsilon=\pm1$. Ако $d=-1$, тогаш ја добиваме равенката $x^2+y^2=1$ чии решенија се $x=\pm1, y=0$ и $x=0, y=\pm1$, т.е. $\varepsilon=\pm1,\pm i$.

Ако $d\equiv 1 \pmod 4$, тогаш ε има облик $x+\frac{1+\sqrt{d}}{2}y$, $x,y\in\mathbb{Z}$, па затоа

$$N(\varepsilon)=(x+\tfrac{y}{2})^2-\tfrac{1}{4}dy^2.$$

Повторно за $d<0$ равенката $N(\varepsilon)=-1$ нема решенија. Ако $d\le -7$, тогаш $(x+\frac{y}{2})^2-\frac{1}{4}dy^2\ge\frac{7}{4}y^2$, па од $N(\varepsilon)=1$ следува $y=0, x=\pm1$, па затоа $\varepsilon=\pm1$. Ако $d=-3$, тогаш ја добиваме равенката

$$(x+\tfrac{y}{2})^2+\tfrac{3}{4}y^2=1, \tag{11}$$

односно $x^2+xy+y^2=1$. Од (11) следува $|y|\le 1$. Ако $y=0$, тогаш $x=\pm1$, т.е. $\varepsilon=\pm1$. Ако $y=1$, тогаш $x=0$ или $x=-1$, т.е. $\varepsilon=\frac{1+\sqrt{-3}}{2}$ или $\varepsilon=\frac{-1+\sqrt{-3}}{2}$. Ако $y=-1$, тогаш $x=0$ или $x=-1$, т.е. $\varepsilon=\frac{-1-\sqrt{-3}}{2}$ или $\varepsilon=\frac{1-\sqrt{-3}}{2}$. ■

3.10. Теорема. Ако $d>0$, тогаш $\mathbb{Q}[\sqrt{d}]$ има бесконечно многу единици.

Доказ. Броевите $\alpha=a+b\sqrt{d}, a,b\in\mathbb{Z}$ се квадратно цели во $\mathbb{Q}[\sqrt{d}]$ со норма $N(\alpha)=a^2-db^2$. Ако $x^2-dy^2=1$, тогаш квадратно целиот број $\varepsilon=x+y\sqrt{d}$ е единица. Но, $x^2-dy^2=1$ е равенка на Пел која, бидејќи $d>1$ е природен број кој не е точен квадрат, според теоремата VIII 9.5 има бесконечно многу решенија. ■

4. КВАДРАТНО ПРОСТИ БРОЕВИ И ФАКТОРИЗАЦИЈА ВО $\mathbb{Q}[\sqrt{d}]$

4.1. Дефиниција. Квадратно целиот број $\pi\in\mathbb{Q}[\sqrt{d}]$, различен од нула и единица, го нарекуваме *прост број* во $\mathbb{Q}[\sqrt{d}]$ ако за секоја декомпозиција на π како производ на два квадратно цели броеви $\pi=\alpha\beta$ или α или β е единица. Ако $\alpha\in\mathbb{Q}[\sqrt{d}]$ не е прост број, ниту е нула или единица, тогаш ќе велиме дека α е сложен број во $\mathbb{Q}[\sqrt{d}]$.

За да ги разликуваме од простите броеви во $\mathbb{Q}$, простите броеви во $\mathbb{Q}[\sqrt{d}]$ ќе ги наречеме *квадратно прости броеви*.

4.2. Пример. Имаме $5=(1+\sqrt{6})(-1+\sqrt{6})$ и $N(1+\sqrt{6})=N(-1+\sqrt{6})=-5$. Бидејќи $1+\sqrt{6}$ и $-1+\sqrt{6}$ не се единици во $\mathbb{Q}[\sqrt{6}]$ заклучуваме дека 5 е прост број, но не е квадратно прост во $\mathbb{Q}[\sqrt{6}]$. ■

4.3. Теорема. Ако α е квадратно цел број во $\mathbb{Q}[\sqrt{d}]$ и $N(\alpha)$ е прост број, тогаш α е квадратно прост број.

Доказ. Бидејќи $N(\alpha)$ е прост број, α не е нула или единица. Да претпоставиме дека $\alpha=\beta\gamma$, каде β и γ се квадратно цели во $\mathbb{Q}[\sqrt{d}]$. Според тоа, важи $N(\alpha)=N(\beta)N(\gamma)$, каде $N(\beta)$ и $N(\gamma)$ се цели броеви. Бидејќи $N(\alpha)$ е прост број, добиваме дека или $N(\beta)=\pm1$ или $N(\gamma)=\pm1$, шт значи дека или β или γ е единица во $\mathbb{Q}[\sqrt{d}]$, т.е. α е квадратно цел број. ■

4.4. Пример. Бидејќи $N(\frac{3+\sqrt{-163}}{2})=43$ и 43 е прост број од претходната теорема следува дека $\frac{3+\sqrt{-163}}{2}$ е квадратно прост број во $\mathbb{Q}[\sqrt{-163}]$.

Од $N(-1+\sqrt{6})=-5$ следува дека $-1+\sqrt{6}$ е квадратно прост во $\mathbb{Q}[\sqrt{6}]$.

Имаме $N(\frac{11+2\sqrt{-1}}{5})=5$ и 5 е прост број, но бројот $\frac{11+2\sqrt{-1}}{5}$ не е квадратно цел број $\mathbb{Q}[\sqrt{-1}]$, па затоа не е квадратно прост. ■

4.5. Дефиниција. Ако α и β се ненулти квадратно цели броеви во $\mathbb{Q}[\sqrt{d}]$ такви што $\alpha=\beta\varepsilon$, каде ε е единица во $\mathbb{Q}[\sqrt{d}]$, тогаш за α ќе велиме дека е *еквивалентен* (*асоцијација*) на β.

Според тоа, α е еквивалентен на β ако и само ако $\frac{\alpha}{\beta}$ е единица.

4.6. Теорема. а) Ако α и β се ненулти квадратно цели броеви во $\mathbb{Q}[\sqrt{d}]$, тогаш α е еквивалентен на β ако и само ако β е еквивалентен на α.

б) Броевите α и β се еквивалентни еден на друг ако и само ако $\alpha|\beta$ и $\beta|\alpha$.

в) Нека α и β се еквивалентни еден на друг. Ако $\gamma|\alpha$, тогаш $\gamma|\beta$. Ако $\alpha|\delta$, тогаш $\beta|\delta$.

г) Ако α е квадратно прост број, тогаш секој елементен еквивалентен на α е квадратно прост број. Ако α е сложен број во $\mathbb{Q}[\sqrt{d}]$, тогаш секој елемент еквивалентен на α во $\mathbb{Q}[\sqrt{d}]$ е сложен број.

Доказ. а) Нека α е еквивалентен на β. Ако ε е единица таква што $\alpha=\beta\varepsilon$, тогаш $\frac{1}{\varepsilon}$ е единица таква што $\beta=\alpha\frac{1}{\varepsilon}$, т.е. β е еквивалентен на α и обратно.

б) Броевите α и β се еквивалентни еден на друг, па затоа постои единица ε таква што $\alpha=\beta\varepsilon$ и $\beta=\alpha\frac{1}{\varepsilon}$. Но, ε и $\frac{1}{\varepsilon}$ се единици, што значи дека се квадратно цели, па затоа $\alpha|\beta$ и $\beta|\alpha$.

Обратно, ако $\alpha|\beta$ и $\beta|\alpha$, тогаш $\alpha=\beta\varepsilon$ и $\beta=\alpha\delta$ за некои квадратно цели броеви ε и δ. Затоа, $\varepsilon\delta=\frac{\alpha}{\beta}\cdot\frac{\beta}{\alpha}=1$, т.е. $N(\varepsilon)N(\delta)=1$, од што следува дека ε и δ се единици во $\mathbb{Q}[\sqrt{d}]$. Сега од дефиницијата 4.5 следува дека α и β се еквивалентни еден на друг.

в) Нека α и β се еквивалентни еден на друг. Тогаш $\alpha|\beta$ и ако $\gamma|\alpha$, од теоремата 3.2 следува дека $\gamma|\beta$. Слично, ако $\alpha|\delta$, бидејќи $\beta|\alpha$ повторно од теоремата 3.2 следува дека $\beta|\delta$.

г) Нека претпоставиме дека α и β се ненулти и неединечни елементи еквивалентни еден на друг во $\mathbb{Q}[\sqrt{d}]$. Ќе докажеме дека двата или се сложени или се квадратно прости. Нека претпоставиме дека α е квадратно прост, а β е сложен.

Тогаш имаме $\beta=\gamma\delta$ каде γ и δ не се единици. Но, α и β се еквивалентни еден на друг, па затоа постои единица ε таква што $\alpha=\beta\varepsilon$. Така $\alpha=\gamma(\delta\varepsilon)$ Но, γ не е единица, а исто така и $\delta\varepsilon$ не е единица, бидејќи во спротивно $\delta=\delta\varepsilon\cdot\frac{1}{\varepsilon}$ ќе биде единица. Според тоа, α е производ на два неединечни елементи, што е противречност бидејќи тој е квадратно прост број. Од добиената противречност следува дека α и β или се сложени или се квадратно прости. ■

4.7. Теорема. Ако $\alpha\in\mathbb{Q}[\sqrt{d}]$ е квадратно цел број кој не е ниту нула ниту единица, тогаш α може да се запише како производ на конечен број квадратно прости броеви во $\mathbb{Q}[\sqrt{d}]$.

Доказ. Нека $\alpha\in\mathbb{Q}[\sqrt{d}]$ е квадратно цел број кој не е ниту нула ниту единица. Ако α не е квадратно прост, тогаш $\alpha=\alpha_1\alpha_2$, каде α_1 и α_2 не се единици во $\mathbb{Q}[\sqrt{d}]$. Постапката ја продолжуваме со факторизирање на α_1 и α_2 ако некој од нив не е квадратно прост итн. Оваа постапка мора да заврши по конечен број чекори, бидејќи во спротивно α ќе има облик

$$\alpha=\alpha_1\alpha_2...\alpha_n, \tag{1}$$

каде n е произволен природен број, а ниту еден од броевите $\alpha_1,\alpha_2,...,\alpha_n$ не е единица. Последното значи дека

$$|N(\alpha)|=\prod_{j=1}^{n}|N(\alpha_j)|\geq 2^n,$$

бидејќи $|N(\alpha_j)|$ е природен број поголем од 2. Ова противречи на фактот дека $|N(\alpha)|$ е конечен природен број. ■

5. ЕДИНСТВЕНОСТ НА ФАКТОРИЗАЦИЈАТА ВО $\mathbb{Q}[\sqrt{d}]$

5.1. Во теорема 4.7 докажавме дека секој кавдратно цел број во $\mathbb{Q}[\sqrt{d}]$ може да се фактризира на квадратно прости броеви во $\mathbb{Q}[\sqrt{d}]$.

Да го разгледаме бројот 10 и неговите две факторизации во $\mathbb{Q}[\sqrt{-6}]$:

$$10=2\cdot 5=(2+\sqrt{-6})(2-\sqrt{-6}).$$

Броевите $2,5,2+\sqrt{-6},2-\sqrt{-6}$ се квадратно прости во $\mathbb{Q}[\sqrt{-6}]$. Навистина, прво да забележиме дека ако квадратно целиот број α во $\mathbb{Q}[\sqrt{-6}]$ не е 0 или единица, тогаш $N(\alpha)=N(a+b\sqrt{-6})=a^2+6b^2\geq 4$ и $N(\alpha)\neq 5$. Сега, ако $2=\alpha\beta$, тогаш од

$N(\alpha)N(\beta)=4$ следува $N(\alpha)=\pm 1$ или $N(\beta)=\pm 1$. Аналогно, ако $5=\alpha\beta$, тогаш од $N(\alpha)N(\beta)=25$ следува $N(\alpha)=\pm 1$ или $N(\beta)=\pm 1$. Конечно, ако $2\pm\sqrt{-6}=\alpha\beta$, тогаш од $N(\alpha)N(\beta)=10$ повторно следува $N(\alpha)=\pm 1$ или $N(\beta)=\pm 1$. Според тоа, бројот 10 во $\mathbb{Q}[\sqrt{-6}]$ може да се запише на два начина како производ на квадратно прости множители, што значи дека има две факторизации.

5.2. Дефиниција. Ќе велиме дека квадратното поле $\mathbb{Q}[\sqrt{d}]$ има *својство на единствена факторизација* ако секој квадратно цел број во $\mathbb{Q}[\sqrt{d}]$, кој не е 0 ниту единица, може да се факторизира на квадратно прости множители на единствен начин, до редослед на множителите и замена на множител со нему еквивалентен број.

5.3. Теорема. Квадратното поле $\mathbb{Q}[\sqrt{d}]$ има својство на единствена факторизација ако и само ако $\mathbb{Q}[\sqrt{d}]$ го има својството:

ако $\pi\mid\alpha\beta$, каде π е квадратно прост број и α и β се квадратно цели броеви во $\mathbb{Q}[\sqrt{d}]$, тогаш $\pi\mid\alpha$ или $\pi\mid\beta$.

Доказ. Нека претпоставиме дека квадратното поле $\mathbb{Q}[\sqrt{d}]$ има својство на единствена факторизација. Нека $\pi\mid\alpha\beta$, каде π е квадратно прост број и α и β се квадратно цели броеви во $\mathbb{Q}[\sqrt{d}]$. Од $\pi\mid\alpha\beta$ следува дека постои квадратно цел број γ таков што $\alpha\beta=\pi\gamma$. Според теоремата 4.7 постојат квадратно прости броеви $\pi_1,\pi_2,...,\pi_n$ и единица ε во $\mathbb{Q}[\sqrt{d}]$ такви што $\gamma=\varepsilon\pi_1\pi_2...\pi_n$ и тогаш

$$\alpha\beta=\varepsilon\pi\pi_1\pi_2...\pi_n$$

е факторизација на $\alpha\beta$ на квадратно прости броеви. Исто така постојат квадратно прости броеви $\pi_1',\pi_2',...,\pi_r',\pi_1'',\pi_2'',...,\pi_s''$ и единици $\varepsilon_1,\varepsilon_2$ такви што

$$\alpha=\varepsilon_1\pi_1'\pi_2'...\pi_r' \text{ и } \beta=\varepsilon_2\pi_1''\pi_2''...\pi_s'',$$

па затоа

$$\varepsilon\pi\pi_1\pi_2...\pi_n=\alpha\beta=(\varepsilon_1\varepsilon_2)\pi_1'\pi_2'...\pi_r'\pi_1''\pi_2''...\pi_s''. \quad (1)$$

Бројот $\alpha\beta$ не е единица, бидејќи е делив со квадратно прост број π и имаме две негови факторизации на квадратно прости броеви. Но, според условот $\mathbb{Q}[\sqrt{d}]$ има својство на единствена факторизација, па затоа некој од квадратно простите броеви на десната страна на (1) е еквивалентен со π и затоа е делив со π. Ако некој од $\pi_1',\pi_2',...,\pi_r'$ е делив со π, тогаш $\pi\mid\alpha$, а ако некој од квадратно простите броеви $\pi_1'',\pi_2'',...,\pi_s''$ е делив со π, тогаш $\pi\mid\beta$. Значи, $\pi\mid\alpha$ или $\pi\mid\beta$.

Обратно, нека претпоставиме дека $\mathbb{Q}[\sqrt{d}]$ го има својството:

ако $\pi \mid \alpha\beta$, каде π е квадратно прост број и α и β се квадратно цели броеви во $\mathbb{Q}[\sqrt{d}]$, тогаш $\pi \mid \alpha$ или $\pi \mid \beta$.

Нека квадратно целиот број α не е единица во $\mathbb{Q}[\sqrt{d}]$ и

$$\alpha = \varepsilon\pi_1\pi_2...\pi_r = \varepsilon_1'\pi_1'\pi_2'...\pi_s', \tag{2}$$

каде ε и ε_1' се единици, а $\pi_1, \pi_2, ..., \pi_r, \pi_1', \pi_2', ..., \pi_s'$ се квадратно прости броеви. Без ограничување на општоста можеме да претпоставиме дека $r \le s$. Ќе докажеме дека π_1 е еквивалентен со некој од квадратно простите броеви $\pi_1', \pi_2', ..., \pi_s'$. Бидејќи $\pi_1 \mid \alpha$, важи $\pi_1 \mid (\pi_1'\pi_2'...\pi_{s-1}')\pi_s'$. Сега од претпоставката следува $\pi_1 \mid \pi_s'$ или $\pi_1 \mid \pi_1'\pi_2'...\pi_{s-1}'$. Ако $\pi_1 \mid \pi_s'$, тогаш $\frac{\pi_s'}{\pi_1}$ е единица, бидејќи во спротивно π_s' ќе биде квадратно сложен број. Затоа π_1 е еквивалентен на π_s'. Ако π_1 не е делител на π_s', тогаш $\pi_1 \mid \pi_1'\pi_2'...\pi_{s-1}'$. Постапката ја повторуваме конечен број пати и добиваме дека π_1 е еквивалентен најмалку на еден од броевите $\pi_1', \pi_2', ..., \pi_s'$. Без ограничување на општоста можеме да земеме дека π_1 е еквивалентен на π_1'. Така $\pi_1' = \varepsilon_1\pi_1$, каде ε_1 е единица и затоа од (2) следува

$$\varepsilon\pi_2...\pi_r = (\varepsilon_1'\varepsilon_1)\pi_2'...\pi_s', \tag{3}$$

каде $\varepsilon_1'\varepsilon_1$ е единица. Продолжувајќи ја постапката добиваме

$$\varepsilon\pi_r = (\varepsilon_1'\varepsilon_1\varepsilon_2...\varepsilon_{r-1})\pi_r'...\pi_s', \tag{4}$$

каде $\varepsilon_1'\varepsilon_1\varepsilon_2...\varepsilon_{r-1}$ е единица во $\mathbb{Q}[\sqrt{d}]$. Бројот на левата страна на (4) е квадратно прост, па затоа и бројот на десната страна на (4) мора да е квадратно прост, а тоа е можно ако и само ако $s = r$ и $\varepsilon\pi_r = (\varepsilon_1'\varepsilon_1\varepsilon_2...\varepsilon_{r-1})\pi_r'$, т.е. π_r и π_r' се еквивалентни еден на друг, што значи дека $\mathbb{Q}[\sqrt{d}]$ има својство на единствена факторизација. ■

5.4. Теорема. а) Нека $a, b \in \mathbb{Z}$, $a \neq 0, b \neq 0$ и $(a,b) = d$. Ако α е квадратно цел број во $\mathbb{Q}[\sqrt{d}]$ таков што $\alpha \mid a$ и $\alpha \mid b$, тогаш $\alpha \mid d$.

б) Ако $(a,b) = 1$, тогаш заеднички делители на a и b во $\mathbb{Q}[\sqrt{d}]$ се само единиците.

Доказ. а) Ако $(a,b) = d$, тогаш постојат $x, y \in \mathbb{Z}$ такви што $ax + by = d$. Затоа, ако $\alpha \mid a$ и $\alpha \mid b$, тогаш $\alpha \mid d$.

б) Ако $(a,b) = 1$, тогаш од а) следува дека $\alpha \mid 1$, т.е. α е единица во $\mathbb{Q}[\sqrt{d}]$. ■

5.5. Теорема. Нека $\mathbb{Q}[\sqrt{d}]$ има својство на единствена факторизација. Тогаш за секој квадратно прост број $\pi \in \mathbb{Q}[\sqrt{d}]$ постои еден и само еден прост број p таков што $\pi \mid p$.

Доказ. Квадратно простиот број π е делител на целиот број $N(\pi)$ и затоа постои природен број кој е делив со π. Нека n е најмалиот природен број кој е делив со π. Тогаш n е прост број. Навистина, ако $n = n_1 n_2$, тогаш од теоремата 5.3 следува дека $\pi \mid n_1$ или $\pi \mid n_2$, што противречи на изборот на n, бидејќи $0 < n_1, n_2 < n$.

Конечно, ако π е делител на некој друг прост број q различен од p, тогаш бидејќи $(p,q) = 1$ од теоремата 5.4 следува дека $\pi \mid 1$, што е противречност. ■

5.6. Теорема. Нека $\mathbb{Q}[\sqrt{d}]$ има својство на единствена факторизација. Тогаш

а) Секој прост број p или е квадратно прост во $\mathbb{Q}[\sqrt{d}]$ или е производ $\pi_1\pi_2$ на два, не задолжително различни, квадратно прости броеви во $\mathbb{Q}[\sqrt{d}]$.

б) Сите квадратно прости броеви π, π_1, π_2 добиени во а), над сите прости броеви во $\mathbb{Z}$, заедно со нивните асоцијации, го формираат множеството квадратно прости броеви во $\mathbb{Q}[\sqrt{d}]$.

в) Во $\mathbb{Q}[\sqrt{d}]$ непарен прост број p таков што $(p,d) = 1$ е производ $\pi_1\pi_2$ на два квадратно прости броеви ако и само ако $(\frac{d}{p}) = 1$.

Доказ. а) Нека $p = \pi\beta$ за некој квадратно прост број π и некој квадратно цел број β во $\mathbb{Q}[\sqrt{d}]$. Тогаш

$$N(\pi)N(\beta) = N(p) = p^2.$$

Бидејќи $N(\pi) \neq \pm 1$, последното равенство е можно ако и само ако $N(\beta) = \pm 1$ или $N(\beta) = \pm p$. Ако $N(\beta) = \pm 1$, тогаш β е единица во $\mathbb{Q}[\sqrt{d}]$ и π е асоцијација на p, што значи дека p е квадратно прост во $\mathbb{Q}[\sqrt{d}]$. Ако $N(\beta) = \pm p$, ќе докажеме дека β е квадратно прост во $\mathbb{Q}[\sqrt{d}]$. Ако $\beta = \beta_1\beta_2$, тогаш $N(\beta_1)N(\beta_2) = \pm p$, па затоа или $N(\beta_1) = \pm 1$ или $N(\beta_2) = \pm 1$, што значи дека или β_1 или β_2 е единица. Тоа значи дека β е квадратно прост број и p е производ на два квадратно прости броја во $\mathbb{Q}[\sqrt{d}]$.

б) Непосредно следува од а) и теоремата 5.5.

в) Нека p е непарен прост број таков што $(p,d) = 1$ и $(\frac{d}{p}) = 1$. Значи, постои цел број x таков што

$$x^2 \equiv d \pmod{p},$$

т.е. $p \mid x^2 - d$, односно $p \mid (x-\sqrt{d})(x+\sqrt{d})$. Ако p е квадратно прост во $\mathbb{Q}[\sqrt{d}]$, тогаш тој е делител на еден од факторите $x-\sqrt{d}$ и $x+\sqrt{d}$. Тоа значи дека еден од броевите $\frac{x}{p}-\frac{\sqrt{d}}{p}$ и $\frac{x}{p}+\frac{\sqrt{d}}{p}$ е квадратно цел, што противречи на теоремата 2.4 (Докажи!). Значи, p не е квадратно прост во $\mathbb{Q}[\sqrt{d}]$, па од а) следува дека $p=\pi_1\pi_2$, каде π_1, π_2 се квадратно прости броеви.

Обратно, нека p е непарен прост број таков што $(p,d)=1$ и $p=\pi\beta$, каде π и β се квадратно прости броеви во $\mathbb{Q}[\sqrt{d}]$. Тоа значи $N(\pi)N(\beta)=p^2$, па затоа $N(\pi)=\pm p$ и $N(\beta)=\pm p$. Бидејќи π е квадратно прост број, од теоремата 2.4 и последицата 2.5 имаме $\pi=a+b\sqrt{d}$, каде $a,b\in\mathbb{Z}$ или ако $d\equiv 1 (\mathrm{mod}\, 4)$ имаме и $\pi=\frac{a+b\sqrt{d}}{2}$ каде a,b се непарни цели броеви. Според тоа, $a^2-db^2=N(\pi)=\pm p$ или ако $d\equiv 1(\mathrm{mod}\, 4)$ имаме и $\frac{a^2-db^2}{4}=N(\pi)=\pm p$. Значи, во секој случај важи $a^2\equiv db^2 (\mathrm{mod}\, p)$, односно $(2a)^2\equiv d(2b)^2 (\mathrm{mod}\, p)$. Притоа, $2a$ и $2b$ се цели броеви и ниту еден од нив не е делив со p. Навистина, ако едниот е делив со p, тогаш и другиот е делив со p, па затоа $p^2 \mid 4a^2$ и $p^2 \mid 4b^2$, т.е. $p^2 \mid (4a^2-4db^2)$ од каде ќе следува $p^2 \mid 4p$, што е противречност. Затоа $(2b,p)=1$ и постои цел број k таков што $2kb\equiv 1(\mathrm{mod}\, p)$, од каде добиваме

$$(2ak)^2\equiv d(2bk)^2\equiv d(\mathrm{mod}\, p),$$

што значи $(\frac{d}{p})=1$. ■

5.7. Нека $\mathbb{Q}[\sqrt{d}]$ има својство на единствена факторизација и да ги разгледаме простите броеви. Од претходните разгледувања следува дека простиот број p за кој $(p,2d)=1$ и $(\frac{d}{p})=-1$, заедно со неговите асоцијации во $\mathbb{Q}[\sqrt{d}]$ е квадратно прост во $\mathbb{Q}[\sqrt{d}]$. Понатаму, ако за простиот број p важи $(p,2d)=1$ и $(\frac{d}{p})=1$, тогаш $p=\pi_1\pi_2$, каде π_1 и π_2 се квадратно прости броеви во $\mathbb{Q}[\sqrt{d}]$ такви што $N(\pi_1)=N(\pi_2)=\pm p$. Јасно, секој квадратно прост фактор на p е асоцијација на π_1 или на π_2. Конечно, простите броеви p за кои $(p,2d)=1$ или се квадратно прости или се производ на два квадратно прости броја во $\mathbb{Q}[\sqrt{d}]$.

Нека претпоставиме дека α е квадратно цел во $\mathbb{Q}[\sqrt{d}]$ и $N(\alpha)=\pm p$, p е прост број. Тогаш $\bar{\alpha}$ е квадратно цел во $\mathbb{Q}[\sqrt{d}]$ и $\alpha\bar{\alpha}=N(\alpha)=\pm p$, што значи де-

ка α е квадратно прост во $\mathbb{Q}[\sqrt{d}]$. Ако $d \not\equiv 1 (\mathrm{mod}\, 4)$, тогаш $\alpha = x + y\sqrt{d}$ и $N(\alpha) = x^2 - dy^2$ за некои цели броеви x и y, а ако $d \equiv 1 (\mathrm{mod}\, 4)$, тогаш $\alpha = \frac{x+y\sqrt{d}}{2}$ и $4N(\alpha) = x^2 - dy^2$ за некои цели броеви x и y со иста парност.

Од досега изнесеното имаме: ако $\mathbb{Q}[\sqrt{d}]$ има својство на единствена факторизација и p е прост број таков што $(p, 2d) = 1$ и $(\frac{d}{p}) = 1$, тогаш за $d \not\equiv 1 (\mathrm{mod}\, 4)$ барем една од равенките $x^2 - dy^2 = \pm p$ има решение. Нека $x = a, y = b$ е такво решение. Тогаш броевите $\alpha = x + y\sqrt{d}$, $\bar{\alpha} = x - y\sqrt{d}$ и нивните асоцијации се квадратно прости во $\mathbb{Q}[\sqrt{d}]$ и тие се единствените квадратно прости броеви во $\mathbb{Q}[\sqrt{d}]$ кои се делители на p. Понатаму, ако $d \equiv 1 (\mathrm{mod}\, 4)$, тогаш барем една од равенките $x^2 - dy^2 = \pm 4p$ има решение при што x и y се со иста парност. Нека $x = a, y = b$ е такво решение. Тогаш броевите

$$\alpha = \frac{x+y\sqrt{d}}{2},\ \bar{\alpha} = \frac{x-y\sqrt{d}}{2}$$

и нивните асоцијации се квадратно прости во $\mathbb{Q}[\sqrt{d}]$ и тие се единствените квадратно прости броеви во $\mathbb{Q}[\sqrt{d}]$ кои се делители на p.

Простите броеви p кои се делители на $2d$ можеме да ги разгледуваме одделно. Ако $d \not\equiv 1 (\mathrm{mod}\, 4)$, тогаш ја разгледувамне равенката $x^2 - dy^2 = \pm p$. Ако оваа равенка нема решение, тогаш p и неговите асоцијации се квадратно прости во $\mathbb{Q}[\sqrt{d}]$. Ако оваа равенка има решение $x = a$ и $y = b$, тогаш $\alpha = x + y\sqrt{d}$, $\bar{\alpha} = x - y\sqrt{d}$ и нивните асоцијации се квадратно прости во $\mathbb{Q}[\sqrt{d}]$. Во случај кога $d \equiv 1 (\mathrm{mod}\, 4)$ ги разгледуваме равенката $x^2 - dy^2 = \pm 4p$ и $\alpha = \frac{x+y\sqrt{d}}{2}$, $\bar{\alpha} = \frac{x-y\sqrt{d}}{2}$.

5.8. Пример (Гаусови прости броеви). Нека $d = -1$ и да го разгледаме квадратното поле $\mathbb{Q}[\sqrt{-1}]$. Имаме,

$$2d = -2,\ 1^2 + 1^2 = 2,\ \overline{1+\sqrt{-1}} = 1 - \sqrt{-1} \text{ и } (\tfrac{d}{p}) = \begin{cases} 1, & p = 4k+1, \\ -1, & p = 4k+3. \end{cases}$$

За секој прост број p од облик $4k+1$ равенката $x^2 + y^2 = p$ има решение $x = a_p$ и $y = b_p$, а равенката $x^2 + y^2 = -p$ нема решение.

Квадратно прости броеви во $\mathbb{Q}[\sqrt{-1}]$ се $1 + \sqrt{-1}$, сите прости броеви p од облик $4k+3$, сите броеви $a_p + b_p\sqrt{-1}$, $a_p - b_p\sqrt{-1}$ каде p од облик $4k+1$ и нивните асоцијации. Притоа, да забележиме дека

$$1-\sqrt{-1}=-\sqrt{-1}(1+\sqrt{-1}),$$

односно $1-\sqrt{-1}$ е асоцијација на $1+\sqrt{-1}$. ■

5.9. Пример. Нека $d=-3$ и да го разгледаме квадратното поле $\mathbb{Q}[\sqrt{-3}]$. Имаме, $2d=-6$, $x^2+3y^2=\pm 4\cdot 2$ нема решение, но

$$3^2+3\cdot 1^2=4\cdot 3,\ \ \overline{\frac{3+\sqrt{-3}}{2}}=\frac{3-\sqrt{-3}}{2}\ \text{ и }\ \left(\frac{d}{p}\right)=\begin{cases}1, & p=3k+1,\ (p,6)=1\\ -1, & p=3k+2,\ (p,6)=1.\end{cases}$$

За секој непарен p од облик $3k+1$ постојат a_p,b_p такви што $a_p^2+3b_p^2=4p$.

Квадратно прости броеви во $\mathbb{Q}[\sqrt{-3}]$ се $2, \frac{3+\sqrt{-3}}{2}$, сите непарни прости броеви од облик $3k+2$, сите броеви од облик $\frac{a_p+b_p\sqrt{-3}}{2}$, $\frac{a_p-b_p\sqrt{-3}}{2}$ каде p е прост број од облик $3k+1$ и нивните асоцијации. Притоа, бројот $\frac{3-\sqrt{-3}}{2}$ не генерира нови квадратно пртости броеви, бидејќи тој е асоцијација на бројот $\frac{3+\sqrt{-3}}{2}$. Докажи! ■

5.9. Теорема. Нека $\mathbb{Q}[\sqrt{d}]$ има својство на единствена факторизација. Ако ε е единица во $\mathbb{Q}[\sqrt{d}]$ и α, β, γ се квадратно цели броеви такви што α и β немаат заеднички делители освен единиците и $\alpha\beta=\varepsilon\gamma^n$ за некој $n\in\mathbb{N}$, тогаш постојат единици ε' и ε'' и квадратно цели броеви δ и ξ во $\mathbb{Q}[\sqrt{d}]$ такви што

$$\alpha=\varepsilon'\delta^n \text{ и } \beta=\varepsilon''\xi^n.$$

Доказ. Ако γ е единица во $\mathbb{Q}[\sqrt{d}]$, тогаш α и β се единиоци во $\mathbb{Q}[\sqrt{d}]$. Ставаме $\varepsilon'=\alpha$, $\varepsilon''=\beta$ и $\delta=\xi=1$ и добиваме $\alpha=\varepsilon'\delta^n$ и $\beta=\varepsilon''\xi^n$. Ако $\gamma=0$, тогаш α или β е 0, па како $\alpha\beta=\varepsilon\cdot 0^n$, добиваме дека β или α е единица. Според тоа, теоремата повторно важи при што едниот од δ и ξ е 0, а другиот е единица.

Нека претпоставиме дека $\gamma\neq 0$ и не е единица. Тогаш $\gamma=\pi_1\pi_2...\pi_r$, каде $\pi_1,\pi_2,...,\pi_r$ се квадратно прости броеви, при што некои од нив може да се асоцијации едни на други. Ако α е единица, тогаш ставаме $\varepsilon'=\alpha$, $\delta=1$, $\xi=\gamma$ и $\varepsilon''=\frac{\varepsilon}{\varepsilon'}$ и добиваме $\alpha=\varepsilon'\delta^n$ и $\beta=\varepsilon''\xi^n$. Нека претпоставиме дека α не е единица, а исто така $\alpha\neq 0$ бидејќи $\gamma\neq 0$. Според тоа, $\alpha=\pi_1'\pi_2'...\pi_s'$, каде $\pi_1',\pi_2',...,\pi_s'$ се квадратно прости броеви. Тогаш

$$\pi_1'\pi_2'...\pi_s'\beta=\varepsilon\pi_1^n\pi_2^n...\pi_r^n. \qquad (5)$$

Од својството на единствена факторизација следува дека π_1' е асоцијација на некој од квадратно простите броеви $\pi_1, \pi_2, ..., \pi_r$, на пример π_1. Сега, ако некоја асоцијација на π_1 е делител на β, тогаш $\pi_1 | \beta$, па затоа $\pi_1' | \beta$ и како $\pi_1' | \alpha$, добиваме противречност. Според тоа, π_1 и неговите асоцијации мора да се n пати меѓу квадратно простите броеви $\pi_1', \pi_2', ..., \pi_s'$. Да земеме дека $\pi_1', \pi_2', ..., \pi_n'$ се $n-$те асоцијации на π_1. Ова подразбира дека $s \geq n$ и постојат единици $\varepsilon_1, \varepsilon_2, ..., \varepsilon_n$ такви што $\pi_i' = \varepsilon_i \pi_1$, за $i = 1, 2, ..., n$, т.е.

$$\pi_1' \pi_2' ... \pi_n' = (\varepsilon_1 \varepsilon_2 ... \varepsilon_n) \pi_1^n .$$

Ако $s = n$, доказот е завршен, а ако $s > n$ тогаш (5) ја делиме со π_1^n и добиваме

$$(\varepsilon_1 \varepsilon_2 ... \varepsilon_n) \pi_{n+1}' \pi_{n+2}' ... \pi_s' \beta = \varepsilon \pi_2^n ... \pi_r^n . \qquad (6)$$

Повторувајќи ги претходните размислувања добиваме дека (ако е потребно ќе извршиме преиндексирање) π_2 е асоцијација на $\pi_{n+1}', \pi_{n+2}', ..., \pi_{2n}'$. Тоа значи дека $s \geq 2n$ и дека постојат единици $\varepsilon_{n+1}, \varepsilon_{n+2}, ..., \varepsilon_{2n}$ такви што $\pi_i' = \varepsilon_i \pi_2$, за $i = n+1, n+2, ..., 2n$, и затоа

$$\pi_{n+1}' \pi_{n+2}' ... \pi_{2n}' = (\varepsilon_{n+1} \varepsilon_{n+2} ... \varepsilon_{2n}) \pi_2^n .$$

Ако $s = 2n$, тогаш

$$\alpha = (\varepsilon_1 \varepsilon_2 ... \varepsilon_{2n}) (\pi_1 \pi_2)^n ,$$

па затоа $\varepsilon' = \varepsilon_1 \varepsilon_2 ... \varepsilon_{2n}$ и $\delta = \pi_1 \pi_2$, со што доказот е завршен. Ако $s > 2n$, тогаш (6) ја делиме со π_2^n и постапката ја повторуваме. Бидејќи постојат конечен број квадратно прости броеви во факторизацијата на α, по конечен број повторувања оваа постапка мора да заврши. Значи, $s = kn$ и

$$\alpha = (\varepsilon_1 \varepsilon_2 ... \varepsilon_{kn}) (\pi_1 \pi_2 ... \pi_k)^n ,$$

па затоа $\varepsilon' = \varepsilon_1 \varepsilon_2 ... \varepsilon_{kn}$ и $\delta = \pi_1 \pi_2 ... \pi_k$. Ако сега (5) ја поделиме со $(\pi_1 \pi_2 ... \pi_k)^n$ добиваме

$$(\varepsilon_1 \varepsilon_2 ... \varepsilon_{kn}) \beta = \varepsilon \pi_{k+1}^n \pi_{k+2}^n ... \pi_r^n ,$$

т.е.

$$\beta = \frac{\varepsilon}{\varepsilon_1 \varepsilon_2 ... \varepsilon_{kn}} (\pi_{k+1} \pi_{k+2} ... \pi_r)^n .$$

Ставаме, $\varepsilon'' = \frac{\varepsilon}{\varepsilon_1 \varepsilon_2 ... \varepsilon_{kn}}$ и $\xi = \pi_{k+1} \pi_{k+2} ... \pi_r$, со што доказот е завршен. ■

6. ЕВКЛИДСКИ ПОЛИЊА

6.1. Дефиниција. Квадратното поле $\mathbb{Q}[\sqrt{d}]$ го нарекуваме Евклидско ако за секои квадратно цели броеви α и β во $\mathbb{Q}[\sqrt{d}]$, $\beta \neq 0$, во $\mathbb{Q}[\sqrt{d}]$ постојат квадратно цели броеви γ и δ такви што $\alpha = \gamma\beta + \delta$, $|N(\delta)| \lhd |N(\beta)|$.

6.2. Теорема. Ако $\mathbb{Q}[\sqrt{d}]$ е Евклидско поле и α и β се квадратно цели броеви во $\mathbb{Q}[\sqrt{d}]$, од кои барем еден е различен од 0, тогаш во $\mathbb{Q}[\sqrt{d}]$ постои квадратно цел број δ таков што

1) $\delta | \alpha$ и $\delta | \beta$,

2) ако $\gamma | \alpha$ и $\gamma | \beta$, тогаш $\gamma | \delta$.

Секој квадратно цел број δ' кој ги има својствата 1) и 2) е асоцијација на δ. Освен тоа, ако δ ги има својствата 1) и 2), тогаш тој е линеарна комбинација на α и β, т.е. постојат квадратно цели броеви ξ и η такви што

$$\delta = \alpha\xi + \beta\eta. \tag{1}$$

Доказ. Бидејќи α и β не се и двата еднакви на 0, може да земеме дека $\beta \neq 0$.

Според дефиницијата 6.1 постојат квадратно цели броеви γ_1 и β_1 такви што $\alpha = \gamma_1\beta + \beta_1$, $|N(\beta_1)| \lhd |N(\beta)|$. Ако $\beta_1 = 0$, тогаш постапката завршува. Ако $\beta_1 \neq 0$, тогаш постојат квадратно цели броеви γ_2 и β_2 такви што е исполнето

$$\beta = \gamma_2\beta_1 + \beta_2, \; |N(\beta_2)| \lhd |N(\beta_1)|.$$

Ако $\beta_2 = 0$, тогаш постапката завршува. Ако $\beta_2 \neq 0$, тогаш постојат квадратно цели броеви γ_3 и β_3 такви што

$$\beta_1 = \gamma_3\beta_2 + \beta_3, \; |N(\beta_3)| \lhd |N(\beta_2)|.$$

Продолжувајќи ја постапката наоѓаме низа квадратно цели броеви $\beta, \beta_1, \beta_2, \ldots$ такви што

$$|N(\beta)| \rhd |N(\beta_1)| \rhd |N(\beta_2)| \rhd \ldots \rhd |N(\beta_k)| \rhd \ldots$$

и $N(\beta_i)$ се цели броеви, поголеми или еднакви на 0, па затоа $N(\beta_n) = 0$ за некој $n \in \mathbb{N}$. Но, тоа значи дека $\beta_n = 0$, па затоа

$$\begin{aligned}
&\alpha = \gamma_1\beta + \beta_1 \\
&\beta = \gamma_2\beta_1 + \beta_2 \\
&\beta_1 = \gamma_3\beta_2 + \beta_3 \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
&\beta_{n-3} = \gamma_{n-1}\beta_{n-2} + \beta_{n-1} \\
&\beta_{n-2} = \gamma_n\beta_{n-1}.
\end{aligned} \tag{2}$$

Земаме, $\delta = \beta_{n-1}$ и од (2) последователно добиваме $\delta \mid \beta_{n-2}, \delta \mid \beta_{n-3}, ..., \delta \mid \beta_1, \delta \mid \beta$ и $\delta \mid \alpha$, т.е. точно е 1).

Имаме,

$$\begin{aligned}\beta_{n-1} &= \beta_{n-3} - \gamma_{n-1}\beta_{n-2} \\ &= \beta_{n-3} - \gamma_{n-1}(\beta_{n-4} - \gamma_{n-2}\beta_{n-3}) \\ &= -\gamma_{n-1}\beta_{n-4} + (1 + \gamma_{n-1}\gamma_{n-2})\beta_{n-3},\end{aligned}$$

т.е. β_{n-1} е линеарна комбинација од β_{n-3} и β_{n-4}. Продолжувајќи ја постапката од равенствата (2) добиваме $\beta_{n-1} = \alpha\xi + \beta\eta$, со што е докажано 2).

Очигледно дека секоја асоцијација на $\delta = \beta_{n-1}$ ги има својствата 1) и 2). Освен тоа, ако δ' ги има својствата 1) и 2), тогаш од 2) следува $\delta' \mid \delta$ и како $\delta \mid \delta'$, добиваме дека δ и δ' се асоцијации еден на друг.

Ако ε е единица, тогаш

$$\varepsilon\delta = \alpha(\varepsilon\xi) + \beta(\varepsilon\eta),$$

па затоа секој асоцијација на δ може да се запише во обликот (3). Добиваме дека секој δ кој ги има својствата 1) и 2) го има својството (3). ■

6.3. Коментар. Според дефиницијата 6.1 кавдартното поле е Евклидско ако и само ако во него постои аналогија на делењето со остаток кај целите броеви. Притоа, равенствата (2) всушност се идентични со равенствата од Евклидовиот алгоритам за определување на најголем заеднички делител (НЗД) на два цели броја. Притоа во Евклидското поле $\mathbb{Q}[\sqrt{d}]$ можеме да зборуваме за НЗД на два квадратно цели броја и според претходната теорема НЗД на два квадратни броја е еднозначно определен до еквиваленција. Меѓутоа, ако квадратното поле не е Евклидско, т.е. ако операцијата делење со остаток не е изводлива, тогаш може да зборуваме само за максимален заеднички делител (МЗД) на два броја.

На пример, полето $\mathbb{Q}[\sqrt{-10}]$ не е Евклидско. Навистина, ако $\alpha = 1 + \sqrt{-10}$ и $\beta = 3$, тогаш за секој $\gamma = a + b\sqrt{-10}, a, b \in \mathbb{Z}$ добиваме

$$N(\delta) = N(\alpha - \gamma\beta) = (1 - 3a)^2 + 10(1 - 3b)^2 \geq 11 > N(\beta).$$

Подоцна ќе докажеме дека полето $\mathbb{Q}[\sqrt{-2}]$ е Евклидско. Со Евклидовиот алгоритам ќе определиме (α, β), каде $\alpha = 7 + 10\sqrt{-2}$ и $\beta = 8 + 5\sqrt{-2}$. Имаме, $N(\alpha) = 249$ и $N(\beta) = 114$. Понатаму,

$$\begin{aligned}&\alpha = 1 \cdot \beta + \beta_1, && \beta_1 = -1 + 5\sqrt{-2}, && N(\beta_1) = 51, \\ &\beta = (1 - \sqrt{-2})\beta_1 + \beta_2, && \beta_2 = -1 - \sqrt{-2}, && N(\beta_2) = 3, \\ &\beta_1 = (-3 - 2\sqrt{-2})\beta_2, && \beta_3 = 0,\end{aligned}$$

па затоа $(\alpha, \beta) = -1 - \sqrt{-2}$.

6.4. Пример. Квадратното поле $\mathbb{Q}[\sqrt{-5}]$ нема својство на единствена факторизација. На пример, $9=3\cdot 3=(2+\sqrt{-5})(2-\sqrt{-5})$ и квадратно простите броеви 3 и $2+\sqrt{-5}$ не се еквивалентни. Јасно, $\alpha=9$ и $\beta=6+3\sqrt{-5}$ припаѓаат на $\mathbb{Q}[\sqrt{-5}]$. Понатаму, $N(\alpha)=N(\beta)=81$ и броевите α и β не се еквивалентни, па затоа нивниот МЗД има норма 1, 3, 9 или 27. Но, во $\mathbb{Q}[\sqrt{-5}]$ не постои квадратно цел број со норма 27. Од друга страна броевите 3 и $2+\sqrt{-5}$ не се еквивалентни, имаат норма 9 и се делители на α и β, па затоа секој од нив е МЗД на α и β. ■

6.5. Теорема. Секое Евклидско поле има својство на единствена факторизација.

Доказ. Нека $\mathbb{Q}[\sqrt{d}]$ е Евклидско поле и $\pi\mid\alpha\beta$, каде π е квадратно прост и α и β се квадратно цели во $\mathbb{Q}[\sqrt{d}]$. Доволно е да докажеме дека $\pi\mid\alpha$ или $\pi\mid\beta$. Нека $\pi\nmid\alpha$. Тогаш секоја асоцијација на π не е делител на α. Исто така, секој делител на π е асоцијација на π или е единица. Според тоа, секој заеднички делител на α и π може да биде само единица. Бидејќи сите единици се делители на 1, заклучуваме дека за бројот 1 важат својствата 1) и 2) од теоремата 6.2. Имено, $1\mid\alpha$ и $1\mid\pi$ и ако $\gamma\mid\alpha$ и $\gamma\mid\pi$, тогаш $\gamma\mid 1$. Сега, од теоремата 6.2 следува дека постојат ξ и η такви што $\alpha\xi+\pi\eta=1$. Затоа,

$$(\alpha\beta)\xi+(\pi\beta)\eta=\beta.$$

Сега, бидејќи $\pi\mid\alpha\beta$, добиваме $\pi\mid\alpha\beta\xi+\pi\beta\eta$, па затоа $\pi\mid\beta$.

Значи, ако $\pi\mid\alpha\beta$, тогаш $\pi\mid\alpha$ или $\pi\mid\beta$, па според теоремата 5.3 $\mathbb{Q}[\sqrt{d}]$ има својство на единствена факторизација. ■

6.6. Коментар. Познато е дека постојат точно 21 Евклидско поле $\mathbb{Q}[\sqrt{d}]$ и тоа за

$$d=-11,-7,-3,-2,-1,2,3,5,6,7,11,13,17,19,21,29,33,41,57,73.$$

Тоа не се сите квадратни полиња со единствена факторизација. Имено, Бекер и Старк во 1966 година докажале дека ако $d<0$ тогаш $\mathbb{Q}[\sqrt{d}]$ има својство на единствена факторизација ако и само ако

$$d=-163,-67,-43,-19,-11,-7,-3,-2,-1.$$

Понатаму, ако $2\le d<100$ постојат 60 квадратни полиња $\mathbb{Q}[\sqrt{d}]$ од кои точно 38 имаат својство на единствена факторизација и тоа:

$$d=2,3,5,6,7,11,13,14,17,19,21,22,23,29,31,33,37,38,41,43,$$
$$46,47,53,57,59,61,62,67,69,71,73,77,83,86,89,93,94,97.$$

Постои хипотеза дека за $d>0$ има бесконечно многу квадратни полиња со својство на единствена факторизација.

6.7. Теорема. Квадратните полиња $\mathbb{Q}[\sqrt{d}]$ за $d=-11,-7,-3,-2,-1,2,3,5$ се Евклидски.

Доказ. Нека α,β се квадратно цели броеви во $\mathbb{Q}[\sqrt{d}]$ и нека $\beta\neq 0$. Тогаш $\frac{\alpha}{\beta}=u+v\sqrt{d}$, $u,v\in\mathbb{Q}$ Нека $x,y\in\mathbb{Z}$ се такви што

$$0\leq|u-x|\leq\tfrac{1}{2},\quad 0\leq|v-y|\leq\tfrac{1}{2}.$$

Нека $x+y\sqrt{d}=\gamma$, $\alpha-\beta\gamma=\delta$. Броевите γ и δ се квадратно цели во $\mathbb{Q}[\sqrt{d}]$ и важи

$$\begin{aligned}N(\delta)&=N(\alpha-\beta\gamma)=N(\beta)N(\tfrac{\alpha}{\beta}-\gamma)\\&=N(\beta)N((u-x)+(v-y)\sqrt{d})\\&=N(\beta)((u-x)^2-d(v-y)^2),\end{aligned}$$

па затоа

$$|N(\delta)|\leq|N(\beta)|\cdot|(u-x)^2-d(v-y)^2|. \tag{3}$$

Ако $d>0$, тогаш

$$-\tfrac{d}{4}\leq(u-v)^2-d(v-y)^2\leq\tfrac{1}{4},$$

а ако $d<0$, тогаш

$$0\leq(u-v)^2-d(v-y)^2\leq\tfrac{1}{4}+\tfrac{1}{4}(-d),$$

Според тоа, ако $d=2,3,-1,-2$, тогаш од (3) добиваме $|N(\delta)|<|N(\beta)|$, па за овие вредности на d квадратното поле $\mathbb{Q}[\sqrt{d}]$ е Евклидско.

За $d=-11,-7,-3,5$ постапуваме малку поинаку. Да забележиме дека во сите овие случаи $d\equiv 1(\mathrm{mod}\,4)$. Нека u и v се дефинирани како претходно. Избираме $y\in\mathbb{Z}$ да е најблизок до бројот $2v$ и ставаме $s=v-\frac{1}{2}y$. Тогаш $|s|\leq\frac{1}{4}$. Понатаму, избираме $x\in\mathbb{Z}$ најблизок до бројот $u-\frac{1}{2}y$ и ставаме $r=u-x-\frac{1}{2}y$. Тогаш $|r|\leq\frac{1}{2}$. Нека $x+y\frac{1+\sqrt{d}}{2}=\gamma$ и $\alpha-\beta\gamma=\delta$. Сега

$$N(\delta)=N(\beta)(r^2-ds^2).$$

Од $|d|\leq 11$ следува

$$|r^2-ds^2|\leq\tfrac{1}{4}+11\cdot\tfrac{1}{16}<1,$$

па затоа $|N(\delta)|<|N(\beta)|$, што и требаше да се докаже. ■

6.8. Пример. Во множеството цели броеви реши ја равенката

$$y^2=x^3-11.$$

Решение. Според теоремата 6.7 полето $\mathbb{Q}[\sqrt{-11}]$ е Евклидско, па од теоремата 6.5 следува дека тоа има својство на единствена факторизација. Единиците во $\mathbb{Q}[\sqrt{-11}]$ се ± 1. Затоа, согласно теоремата 5.9, од

$$(y+\sqrt{-11})(y-\sqrt{-11}) = x^3$$

следува дека постои квадратно цел број број $\alpha \in \mathbb{Q}[\sqrt{-11}]$ таков што

$$y+\sqrt{-11} = \pm\alpha^3.$$

Бидејќи $-\alpha^3 = (-\alpha)^3$, предзнакот $-$ може да го испуштиме. Значи,

$$y+\sqrt{-11} = \alpha^3,\ \alpha = a+\tfrac{1+\sqrt{-11}}{2}b = (a+\tfrac{b}{2})+\tfrac{b}{2}\sqrt{-11}\,.$$

Ако ги изедначиме коефициентите пред $\sqrt{-11}$, добиваме

$$1 = 3(a+\tfrac{b}{2})^2\,\tfrac{b}{2} - 11(\tfrac{b}{2})^3,$$

односно

$$b(3a^2+3ab-2b^2) = 2.$$

Оттука $b = \pm 1$ или $b = \pm 2$, па затоа $(a,b) = (0,-1),(1,-1),(1,2),(1,-3)$. Сега, од

$$y = (a+\tfrac{b}{2})^3 + 3(a+\tfrac{b}{2})(\tfrac{b}{2})^2 \cdot (-11),$$

следува $y = \pm 4, \pm 58$. Решенијата на дадената равенка се $(x,y) = (3,\pm 4),(15,\pm 58)$. ■

7. МНОЖЕСТВОТО $\mathbb{Z}[\sqrt{d}]$

7.1. Нека d е цел број кој не е делив со квадрат на природен број поголем од 1. Во претходните разгледувања со $\mathbb{Z}[\sqrt{d}]$ го означивме множеството квадратни броеви од видот $a+b\sqrt{d}$, $a,b \in \mathbb{Z}$, т.е. $\mathbb{Z}[\sqrt{d}] = \{a+b\sqrt{d} \mid a,b \in \mathbb{Z}\}$.

За броевите на множеството $\mathbb{Z}[\sqrt{d}]$ важи дека збирот,разликата и производот на два броја од $\mathbb{Z}[\sqrt{d}]$ припаѓа на $\mathbb{Z}[\sqrt{d}]$. Понатаму, ако $\alpha,\beta \in \mathbb{Z}[\sqrt{d}]$ и $\alpha,\beta \neq 0$, тогаш ќе велиме дека во $\alpha \mid \beta$ $\mathbb{Z}[\sqrt{d}]$, ако $\frac{\beta}{\alpha} \in \mathbb{Z}[\sqrt{d}]$. На пример, во $\mathbb{Q}[\sqrt{5}]$ важи $2 \mid (1+\sqrt{5})$, но тоа не важи во $\mathbb{Z}[\sqrt{5}]$.

Нормата на броевите во $\mathbb{Z}[\sqrt{d}]$ се дефинира на потполно ист начин како и нормата во $\mathbb{Q}[\sqrt{d}]$. Јасно, ако $\alpha \in \mathbb{Z}[\sqrt{d}]$, тогаш $N(\alpha) \in \mathbb{Z}$. Дефинираме единица во $\mathbb{Z}[\sqrt{d}]$ како број кој е делител на 1 во $\mathbb{Z}[\sqrt{d}]$. На потполно идентичен начин се докажува дека α е единица во $\mathbb{Z}[\sqrt{d}]$ ако и само ако $N(\alpha) = \pm 1$. Јасно, ако $d > 0$,

тогаш во $\mathbb{Z}[\sqrt{d}]$ постојат бесконечно многу единици. Слично, како во случајот на претходно воведените поими, можеме да дефинираме прости броеви и еквивалентни броеви (асоцијации) во $\mathbb{Z}[\sqrt{d}]$. Понатаму, секој ненулти број во $\mathbb{Z}[\sqrt{d}]$ кој не е единица може да се претстави како производ од прости броеви во $\mathbb{Z}[\sqrt{d}]$. Доказот на ова тврдење е идентичен со доказот на тврдењето за квадратното поле $\mathbb{Q}[\sqrt{d}]$.

За $\mathbb{Z}[\sqrt{d}]$ ќе велиме дека има својство на единствена факторизација ако претставувањето на елементите на $\mathbb{Z}[\sqrt{d}]$ како производ на прости броеви во $\mathbb{Z}[\sqrt{d}]$ единствено со точност редослед и еквивалентност на броевите. Теоремата 5.3 и нејзиниот доказ се точни во $\mathbb{Z}[\sqrt{d}]$.

7.2. Теорема. Ако $\mathbb{Z}[\sqrt{d}]$ има својство на единствена факторизација, тогаш 2 не е прост број во $\mathbb{Z}[\sqrt{d}]$.

Доказ. Еден од броевите d и $d-1$ е парен, па затоа $2 \mid d(d-1)$. Понатаму, од

$$(d-\sqrt{d})(d+\sqrt{d}) = d^2 - d = d(d-1)$$

следува $2 \mid (d-\sqrt{d})(d+\sqrt{d})$. Меѓутоа, $\frac{d}{2}+\frac{\sqrt{d}}{2} \notin \mathbb{Z}[\sqrt{d}]$ и $\frac{d}{2}-\frac{\sqrt{d}}{2} \notin \mathbb{Z}[\sqrt{d}]$, па затоа во $\mathbb{Z}[\sqrt{d}]$ имаме $2 \nmid d-\sqrt{d}$ и $2 \nmid d+\sqrt{d}$. Значи, 2 е делител на производ на два броја од $\mathbb{Z}[\sqrt{d}]$, а не е делител на ниту еден од овие броеви и како $\mathbb{Z}[\sqrt{d}]$ има својство на единствена факторизација заклучуваме дека 2 не е прост број во $\mathbb{Z}[\sqrt{d}]$. ■

7.3. Теорема. а) Ако $d \le -3$, тогаш $\mathbb{Z}[\sqrt{d}]$ нема својство на единствена факторизација, т.е. за $d<0$ само $\mathbb{Z}[\sqrt{-1}]$ и $\mathbb{Z}[\sqrt{-2}]$ имаат својство на единствена факторизација.

б) Ако $d>0$ и $d \equiv 1 \pmod 4$, тогаш $\mathbb{Z}[\sqrt{d}]$ нема својство на единствена факторизација.

Доказ. а) Јасно, $\mathbb{Z}[\sqrt{-1}]$ и $\mathbb{Z}[\sqrt{-2}]$ имаат својство на единствена факторизација. Нека $d \le -3$ и $\mathbb{Z}[\sqrt{d}]$ има својство на единствена факторизација. Според теоремата 7.2 бројот 2 не е прост во $\mathbb{Z}[\sqrt{d}]$. Значи, постојат $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$ такви што

$$2 = \alpha\beta, \ |N(\alpha)| > 1, |N(\beta)| > 1.$$

Според тоа,

$$N(\alpha)N(\beta) = N(\alpha\beta) = 4,$$

па затоа важи

$$|N(\alpha)| \nmid |N(\beta)| = 2.$$

Значи, постои $\alpha = a + b\sqrt{d}$, $a,b \in \mathbb{Z}$ таков што

$$a^2 - db^2 = N(\alpha) = \pm 2. \tag{1}$$

Сега, бидејќи $d \le -3$, ако $b \neq 0$, тогаш

$$\pm 2 = a^2 - db^2 \ge 0 + 3 \cdot 1^2 = 4,$$

што е противречност, а ако $b = 0$, тогаш

$$\pm 2 = a^2 - db^2 = a^2,$$

што повторно е противречност. Конечно, од добиените противречности $\mathbb{Z}[\sqrt{d}]$ нема својство на единствена факторизација, кога $d \le -3$.

б) Нека $d > 0$, $d \equiv 1 (\mathrm{mod}\, 4)$ и $\mathbb{Z}[\sqrt{d}]$ има својство на единствена факторизација. Според теорема 7.2 бројот 2 не е прост во $\mathbb{Z}[\sqrt{d}]$. Сега, повторно како во доказот под а) постои $\alpha = a + b\sqrt{d}$, $a,b \in \mathbb{Z}$ таков што важи (1). Сега од (1) следува

$$a^2 - b^2 \equiv a^2 - db^2 \equiv \pm 2 \equiv 2 (\mathrm{mod}\, 4),$$

што е противречност бидејќи за секој цел број m важи $m^2 \equiv 0$ или $1 (\mathrm{mod}\, 4)$. Конечно, од добиената противречност следува дека $\mathbb{Z}[\sqrt{d}]$ нема својство на единствена факторизација, кога $d > 0$ и $d \equiv 1 (\mathrm{mod}\, 4)$. ■

8. КИНЕСКА ТЕОРЕМА ЗА ОСТАТОЦИ

8.1. Теорема. За даден ненулти квадратно цел број $z \in \mathbb{Q}[\sqrt{d}]$ бројот на класите на еквиваленција во $\mathbb{Q}[\sqrt{d}]$ по модул z е еднаков на $|N(z)|$.

Доказ. Нека α е ненулти квадратно цел број во $\mathbb{Q}[\sqrt{d}]$, т.е. $\alpha^2 = p\alpha + q$, за некои $p,q \in \mathbb{Z}$. Нека $z = a + b\alpha$, $a,b \in \mathbb{Z}$. Ако $b = 0$, тогаш

$$a_1 + b_1\alpha \equiv a_2 + b_2\alpha (\mathrm{mod}\, z),$$

ако и само ако $a_1 \equiv a_2 (\mathrm{mod}\, z)$ и $b_1 \equiv b_2 (\mathrm{mod}\, z)$, па затоа бројот на класите на еквиваленција е еднаков на $z^2 \nmid |N(z)|$.

Нека претпоставиме дека $b \neq 0$ и нека $(a,b) = m$. Тогаш $\alpha z = (a + bp)\alpha + bq$. Бидејќи $(a + bp, b) = m$, коефициентот пред α во γz, γ е квадратно цел број, може да биде произволен цел број делив со m и ниту еден друг број. Понатаму, најмалиот природен број делив со z е

$$\frac{|(a+b\alpha)(\overline{a+b\alpha})|}{m} = \frac{|N(\beta)|}{m}.$$

Затоа за секој квадратно цел број γ во $\mathbb{Q}[\sqrt{d}]$ постои единствен квадратно цел број $\delta = A + B\alpha$ во $\mathbb{Q}[\sqrt{d}]$, каде $A, B \in \mathbb{Z}$, $0 \le A < \frac{|N(z)|}{m}$ и $0 \le B < m$, таков што $\gamma \equiv \delta (\mathrm{mod}\, z)$. Оттука следува дека бараниот број класи на еквиваленција е еднаков на $|N(z)|$. ■

8.2. Дефиниција. За квадратно целите броеви $\alpha, \beta \in \mathbb{Q}[\sqrt{d}]$ ќе велиме дека се *заемно прости* ако немаат други заеднички делители освен единиците во $\mathbb{Q}[\sqrt{d}]$.

8.3. Теорема (Кинеска теорема за остатоци). Нека $\mathbb{Q}[\sqrt{d}]$ е квадратно поле со својство на единствена факторизација, $\alpha_1, \alpha_2, ..., \alpha_k$ се по парови заемно прости квадратно цели броеви и $\beta_1, \beta_2, ..., \beta_k$ се произволни квадратно цели броеви во $\mathbb{Q}[\sqrt{d}]$. Тогаш постои квадратно цел број γ во $\mathbb{Q}[\sqrt{d}]$ таков што $\gamma \equiv \beta_i (\mathrm{mod}\, \alpha_i)$ за $i = 1, 2, ..., k$ кој е единствен по модул $\alpha_1 \alpha_2 ... \alpha_k$.

Доказ. Доволно е тврдењето да го докажеме за $k = 2$. За произволен k тврдењето следува од принципот на математичка индукција.

Да означиме $\gamma_i = \beta_1 + i\alpha_1$. Доволно е да докажеме дека $\gamma_i \equiv \beta_2 (\mathrm{mod}\, \alpha_2)$ за барем еден $i \in \{0, 1, ..., |N(\alpha_2)| - 1\}$. Нека го претпоставиме спротивното. Бидејќи има $|N(\alpha_2)|$ класи на еквиваленција по модул α_2, постојат различни $i, j \in \{0, 1, ..., |N(\alpha_2)| - 1\}$, $i > j$, такви што $\gamma_i \equiv \gamma_j (\mathrm{mod}\, \alpha_2)$. Значи, $\alpha_2 \mid \gamma_i - \gamma_j = (i - j)\alpha_1$ и како $\mathbb{Q}[\sqrt{d}]$ е квадратно поле со својство на единствена фактоириазија, а α_1 и α_2 се заемно прости, добиваме дека $\alpha_2 \mid i - j$, што е противречност. ■

8.4. Пример. Ќе покажеме дека Кинеската теорема за остатоци не мора да важи во квадратно поле $\mathbb{Q}[\sqrt{d}]$ кое нема својство на единствена факторизација.

Во примерот 6.4 видовме дека квадратното поле $\mathbb{Q}[\sqrt{-5}]$ нема својство на единствена факторизација, бидејќи $9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$ и квадратно простите броеви 3 и $\pi = 2 + \sqrt{-5}$ не се еквивалентни.

Ќе покажеме дека не постои квадратно цел број $\alpha \in \mathbb{Q}[\sqrt{-5}]$ таков што $\alpha \equiv 0 (\mathrm{mod}\, \pi)$ и $\alpha \equiv 1 (\mathrm{mod}\, 3)$. Нека претпоставиме дека таков α постои. Тогаш $\alpha = (3m + 1) + 3n\sqrt{-5}$ за некои $m, n \in \mathbb{Z}$. Ако $\pi \mid \alpha$, тогаш $\pi \mid \alpha - 3n\pi = 3(m - 2n) + 1$. Но, $\pi \mid 9$, па затоа $\pi \mid (3(m - 2n) + 1, 9) = 1$, што е противречност. ■

9. МАЛА ТЕОРЕМА НА ФЕРМА

9.1. Во овој дел ќе дадеме генерализација на малата теорема на Ферма

$$a^p \equiv a(\mathrm{mod}\, p) \tag{1}$$

за квадратно цели броеви во $\mathbb{Q}[\sqrt{d}]$. Прво ќе ги разгледаме случаите кога $d \equiv 2$ или $3(\mathrm{mod}\, 4)$. Нека претпоставиме дека p е непарен прост број кој не е делител на d. Тогаш од Њутновата биномна формула за $\alpha = r + s\sqrt{d}$, следува

$$\alpha^p = (r + s\sqrt{d})^p = r^p + \sum_{i=1}^{p-1} \binom{p}{i} r^{p-i} s^i d^{\frac{i}{2}} + s^p d^{\frac{p}{2}} \tag{2}$$

и како за $i = 1, 2, ..., p-1$ важи $\binom{p}{i} \equiv 0(\mathrm{mod}\, p)$ од (2) добиваме

$$\alpha^p \equiv r^p + s^p d^{\frac{p}{2}} (\mathrm{mod}\, p), \tag{3}$$

па од (2) следува

$$\alpha^p \equiv r + s d^{\frac{p-1}{2}} \sqrt{d} (\mathrm{mod}\, p). \tag{4}$$

Сега од критериумот на Ојлер (теоремата VI 1.5) следува

$$\alpha^p \equiv r + s\sqrt{d}\left(\frac{d}{p}\right)(\mathrm{mod}\, p) = \begin{cases} \alpha(\mathrm{mod}\, p), & \text{ако } \left(\frac{d}{p}\right) = 1, \\ \bar{\alpha}(\mathrm{mod}\, p), & \text{ако } \left(\frac{d}{p}\right) = -1. \end{cases}$$

Во случај кога $d \equiv 1(\mathrm{mod}\, 4)$ со аналогни пресметувања добиваме

$$\begin{aligned} \alpha^p &= \left(r + s\frac{-1+\sqrt{d}}{2}\right)^p \\ &= 2^{-p}((2r-s) + s\sqrt{d})^p \\ &\equiv 2^{-p}((2r-s)^p + s^p d^{\frac{p-1}{2}} \sqrt{d}) \\ &\equiv \tfrac{1}{2}(2r - s + s\sqrt{d}\left(\tfrac{d}{p}\right)) \\ &\equiv r + s\frac{-1+\sqrt{d}\left(\frac{d}{p}\right)}{2} \\ &\equiv \begin{cases} \alpha(\mathrm{mod}\, p), & \text{ако } \left(\frac{d}{p}\right) = 1, \\ \bar{\alpha}(\mathrm{mod}\, p), & \text{ако } \left(\frac{d}{p}\right) = -1. \end{cases} \end{aligned}$$

Со тоа ја докажавме следнава теорема.

Теорема (Ферма во $\mathbb{Q}[\sqrt{d}]$). Ако α е квадратно цел број во $\mathbb{Q}[\sqrt{d}]$ и p е непарен прост број, тогаш

$$\alpha^p \equiv \alpha(\mathrm{mod}\, p), \text{ ако } \left(\frac{d}{p}\right) = 1, \tag{5}$$

$$\alpha^p \equiv \bar{\alpha}(\mathrm{mod}\, p), \text{ ако } \left(\frac{d}{p}\right) = -1. \blacksquare \tag{6}$$

9.2. Пример. а) Нека $\alpha = 1+2\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$ и $p = 13$. Од теоремите VI 1.6 и VI 2.3 (Гаусовиот закон за реципроцитет) следува $(\frac{3}{13})(\frac{13}{3}) = 1$ и $(\frac{13}{3}) = (\frac{1}{3}) = 1$, т.е. $(\frac{3}{13}) = 1$, па затоа $\alpha^{13} \equiv \alpha (\mathrm{mod} 13)$.

б) Нека $\alpha = 1+2\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ и $p = 13$. Од теоремата VI 1.11 (правилото на двојката) следува $(\frac{2}{13}) = (-1)^{\frac{13^2-1}{8}} = -1$, па затоа $\alpha^{13} \equiv \bar{\alpha} (\mathrm{mod} 13)$. ■

9.3. Последица. Ако α е квадратно цел број во $\mathbb{Q}[\sqrt{d}]$, p е непарен прост број и $(\frac{d}{p}) = -1$, тогаш

$$\alpha^{p+1} \equiv N(\alpha) (\mathrm{mod}\, p).$$

Доказ. Бидејќи $\alpha \equiv \alpha (\mathrm{mod}\, p)$ за секој квадратно цел број α и $(\frac{d}{p}) = -1$, ако оваа конгруенција ја помножиме со конгруенцијата (6) добиваме

$$\alpha^{p+1} \equiv \alpha\bar{\alpha} = N(\alpha) (\mathrm{mod}\, p). \blacksquare$$

9.4. Теоремата 9.1 ја има следнава примена. Ако (6) ја помножиме со α добиваме

$$\alpha^{p+1} \equiv \alpha\bar{\alpha} = N(\alpha) (\mathrm{mod}\, p), \tag{7}$$

ако $(\frac{d}{p}) = -1$. Понатаму, од (5) следува дека при $n > 2$ важи

$$\alpha^{p^n} \equiv (\alpha^p)^{p^{n-1}} \equiv (\alpha + kp)^{p^{n-1}} \equiv \alpha^{p^{n-1}} (\mathrm{mod}\, p^n),$$

бидејќи сите членови во Њутновиот биномен развој $(\alpha + kp)^{p^{n-1}}$, различни од $\alpha^{p^{n-1}}$, се деливи со p^n. Сега, ако α и p немаат заеднички квадратно цел делител во $\mathbb{Q}[\sqrt{d}]$, кој не е единица, тогаш

$$\alpha^{p^{n-1}(p-1)} \equiv 1 (\mathrm{mod}\, p^n), \tag{8}$$

ако $(\frac{d}{p}) = 1$. Аналогно

$$\alpha^{p^{n-1}(p+1)} \equiv (\alpha^{p+1})^{p^{n-1}} = (N(\alpha) + kp)^{p^{n-1}} \equiv (N(\alpha))^{p^{n-1}} (\mathrm{mod}\, p^n), \tag{9}$$

ако $(\frac{d}{p}) = -1$. Конгруенциите (9) и (10) се генерализации на теоремата на Ојлер во $\mathbb{Q}[\sqrt{d}]$ кога модулот е од видот p^n.

10. РАВЕНКИ ОД ПЕЛОВ ТИП

10.1. Равенката од видот $x^2 - dy^2 = a$, $a \in \mathbb{Z}$ и d не е точен квадрат ја нарекуваме равенка од Пелов тип. Во равенката од Пелов тип условот d не е точен квадрат е еквивалентен со условот d не е делив со квадрат на природен број поголем од 1. Навистина, ако $d = ck^2, c, k \in \mathbb{N}$, тогаш со смената $z = ky$ добиваме еквивалентна равенка од Пелов тип $x^2 - cz^2 = a$ во која c не е делив со квадрат на природен број поголем од 1.

За $a = 1$ равенката од Пелов тип се сведува на равенката на Пел

$$x^2 - dy^2 = 1 \tag{1}$$

Во теоремата VIII 9.5 докажавме дека ако (x_1, y_1) е фундаменталното решение на (1), тогаш сите решенија (x_n, y_n) на (1) се дадени со

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n, n \in \mathbb{N}.$$

Сега, ако земеме $\alpha = x_1 + y_1\sqrt{d}$, добиваме дека сите решенија на (1) се дадени со $x_n + y_n\sqrt{d} = \alpha^n, n \in \mathbb{N}$. Понатаму, ако се има предвид дека $x_n - y_n\sqrt{d} = \bar{\alpha}^n, n \in \mathbb{N}$, добиваме дека решенијата на (1) се дадени со

$$x_n = \frac{\alpha^n + \bar{\alpha}^n}{2}, \; y_n = \frac{\alpha^n - \bar{\alpha}^n}{2\sqrt{d}}, n \in \mathbb{N}. \tag{2}$$

Решенијата (2) на равенката (1) се запишани во нотацијата на квадратните полиња. Притоа, самата равенка на Пел може да се запише како $N(\alpha) = 1$, каде $\alpha = x + y\sqrt{d}$ е квадратно цел број во $\mathbb{Q}[d]$. Бидејќи $\alpha, \bar{\alpha}$ и $-\alpha, -\bar{\alpha}$ се решенија на равенката на Пел, ние истата ја решаваме во множеството $\mathbb{N}$, т.е. зедовме $x, y > 0$.

10.2. Равенка од Пелов тип која е во најдиректна врска со равенката на Пел е равенката

$$x^2 - dy^2 = -1, \tag{3}$$

односно равенката $N(\alpha) = -1$, каде $\alpha = x + y\sqrt{d}$ е квадратно цел број во $\mathbb{Q}[d]$. Оваа равенка нема решение за секој d. На пример, равенката $x^2 - 3y^2 = -1$ нема решение, бидејќи левата страна е конгруентна со 1 по модул 3, а десната страна е конгруентна со -1 по модул 3. Понатаму, за да (3) има решение, бројот d мора да е делител на $x^2 + 1$ за некој природен број x, а знаеме дека таков x постои ако и само ако сите непарни прости делители на d се од видот $4k + 1$ и $4 \nmid d$, види теорема IV 5.1. Покасно ќе видиме дека и ова не е доволен услов за постоење на решенија на равенката (3). Ако равенката (3) има решение, тогаш најмалото

нејзино решение во множеството природни броеви ќе го нарекуваме *фундаментално решение*.

10.3. Теорема. Нека равенката (3) има решение и нека $x_1+y_1\sqrt{d}$ е нејзино фундаментално решение. Тогаш $(x_1+y_1\sqrt{d})^2$ е фундаментално решение на равенката (1). Ако $x_n+y_n\sqrt{d}=(x_1+y_1\sqrt{d})^n, n\in\mathbb{N}$, тогаш во множеството $\mathbb{N}$ сите решенија на равенката (1) се дадени со

$$x_{2n}+y_{2n}\sqrt{d}=(x_1+y_1\sqrt{d})^{2n}, n\in\mathbb{N},$$

а сите решенија во множеството природни броеви на равенката (3) се дадени со

$$x_{2n+1}+y_{2n+1}\sqrt{d}=(x_1+y_1\sqrt{d})^{2n+1}, n\in\mathbb{N},$$

Доказ. Имаме $x_n-y_n\sqrt{d}=(x_1-y_1\sqrt{d})^n, n\in\mathbb{N}$, па затоа

$$x_n^2-dy_n^2=(x_n^2-dy_n^2)^n=(-1)^n.$$

Значи, навистина $x_{2n}+y_{2n}\sqrt{d}$ е решение на (1), а $x_{2n+1}+y_{2n+1}\sqrt{d}$ е решение на (3). Нека претпоставиме дека за решението $a+b\sqrt{d}$ на равенката (1) важи

$$1<a+b\sqrt{d}<(x_1+y_1\sqrt{d})^2.$$

Од $(-x_1+y_1\sqrt{d})(x_1+y_1\sqrt{d})=1$ следува $0<-x_1+y_1\sqrt{d}<1$, па затоа

$$-x_1+y_1\sqrt{d}<(-x_1+y_1\sqrt{d})(a+b\sqrt{d})=s+t\sqrt{d}<x_1+y_1\sqrt{d},$$

каде

$$s=-ax_1+dby_1,\ t=ay_1-bx_1$$

и важи $s^2-dt^2=-1$. Сега, од $s+t\sqrt{d}>0$ и $s+t\sqrt{d}>0$, следува $t>0$. Ако $s<0$, тогаш од $-x_1+y_1\sqrt{d}<s+t\sqrt{d}$ следува $-s+t\sqrt{d}<x_1+y_1\sqrt{d}$. Значи, $|s|+t\sqrt{d}$ е решение на (3) кое е помало од фундаменталното, што е противречност.

Нека претпоставиме дека $u+v\sqrt{d}$ е решение на (3) кое не е содржано во низата $x_{2n+1}+y_{2n+1}\sqrt{d}$. Тогаш постои $m\in\mathbb{N}$ таков што

$$(x_1+y_1\sqrt{d})^{2m-1}<u+v\sqrt{d}<(x_1+y_1\sqrt{d})^{2m+1}.$$

Ако горнитре неравенства ги помножиме со $(x_1-y_1\sqrt{d})^{2m}$, добиваме

$$-x_1+y_1\sqrt{d}<w+z\sqrt{d}<x_1+y_1\sqrt{d},$$

каде $w^2-dz^2=-1$. Но, веќе докажавме дека такви w и z не може да постојат. ■

10.4. Пример. Определи ги сите парови квадратно цели броеви (x,y) во полето $\mathbb{Q}[\sqrt{2}]$ такви што $\frac{1}{x}+\frac{1}{y}=2$.

Решение. Дадената равенка е еквивалентна со равенката

$$(2x-1)(2y-1)=1.$$

Значи, елементот $2x-1$ е единица во $\mathbb{Q}[\sqrt{2}]$. Понатаму, сите единици во $\mathbb{Q}[\sqrt{2}]$ се решенијата на равенките

$$u^2-2v^2=\pm 1. \tag{4}$$

Фундаменталното решение на равенката $u^2-2v^2=-1$ е $u_1+v_1\sqrt{2}=1+\sqrt{2}$, па од теоремата 10.3 следува дека сите решенија на равенките (4) се дадени со $\pm(1+\sqrt{2})^n$, $n\in\mathbb{Z}$ (Зошто?). Според тоа,

$$2x-1=\pm(1+\sqrt{2})^n \text{ и } 2y-1=\pm(1+\sqrt{2})^{-n}, \text{ за некој } n\in\mathbb{Z}.$$

Понатаму, x и y треба да се квадратно цели броеви во $\mathbb{Q}[\sqrt{2}]$, па затоа треба да биде уште $u+v\sqrt{2}=(1+\sqrt{2})^n\equiv 1(\mathrm{mod}\,2)$, односно $u\equiv 1(\mathrm{mod}\,2)$ и $v\equiv 0(\mathrm{mod}\,2)$, што е исполнето ако и само ако $n=2k$ за $k\in\mathbb{Z}$. ■

10.5. Пример. Докажи дека равенката од Пелов тип

$$x^2-34y^2=-1 \tag{5}$$

нема целобројни решенија.

Решение. Со методот на Чакравала или со методот на верижни дропки лесно се наоѓа фундаменталното решение на соодветната равенка на Пел: $35+6\sqrt{34}$. Сега, ако $x_1+y_1\sqrt{34}$ е фундаменталното решение на (5), тогаш од претходната теорема следува дека

$$(x_1+y_1\sqrt{34})^2=35+6\sqrt{34},$$

од каде го добиваме системот равенки

$$\begin{cases} x_1^2+34y_1^2=35, \\ x_1y_1=3, \end{cases}$$

кој нема целобројни решенија. Затоа равенката (5) нема целобројни решенија. ■

10.5. Лема. Ако p е прост број и $p\equiv 1(\mathrm{mod}\,4)$, тогаш равенката $x^2-py^2=-1$ има целобројни решенија.

Доказ. Нека $x_1+y_1\sqrt{d}$ е фундаментално решение на равенката $x^2-py^2=1$. Тогаш $x_1^2-y_1^2\equiv 1(\mathrm{mod}\,4)$, па затоа x_1 е непарен, а y_1 е парен. Од $(\frac{x_1-1}{2},\frac{x_1+1}{2})=1$ и $\frac{x_1-1}{2}\cdot\frac{x_1+1}{2}=p(\frac{y_1}{2})^2$ следува дека постојат $a,b\in\mathbb{N}$, $(a,b)=1$ такви што

$$\frac{x_1\pm 1}{2}=pa^2,\ \frac{x_1\mp 1}{2}=b^2,\ \frac{y_1}{2}=ab.$$

Оттука следува $b^2 - pa^2 = \mp 1$. Но, $u < y_1$, па како $x_1 + y_1\sqrt{d}$ е фундаментално решение на равенката $x^2 - py^2 = 1$ знакот + отпаѓа, односно важи $b^2 - pa^2 = -1$, што значи дека равенката $x^2 - py^2 = -1$ има целобројно решение. ■

10.6. Нека d е природен број кој не е точен квадрат. Да ја разгледаме равенката од Пелов тип

$$x^2 - dy^2 = 4 \tag{6}$$

Како што знаеме, равенката (1) има бесконечно многу целобројни решенија и ако (a,b) е нејзино решение, тогаш $x = 2a, y = 2b$ е решение на равенката (6). Според тоа, равенката (6) има бесконечно многу целобројни решенија. Точна е следнава теорема.

Теорема. Ако (x_1, y_1) е фундаменталното решение на равенката (6), тогаш сите нејзини решенија во множеството природни броеви се дадени со формулата

$$\frac{x_n + y_n\sqrt{d}}{2} = \left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^n,\ n \in \mathbb{N}.$$

Доказ. Доказот е потполно аналоген на доказот на теоремата VIII 9.5. Деталите ги оставаме на читателот за вежба. ■

10.7. Сега да ги разгледаме случаите кои може да се појават во зависност од парноста на броевите x_1 и y_1. Јасно, случајот кога y_1 е непарен, а x_1 е парен не е можен, па затоа можни се следниве три случаи:

- Ако x_1 и y_1 се парни, тогаш за секој $n \in \mathbb{N}$ броевите x_n и y_n се парни и $\frac{x_1}{2} + \frac{y_1}{2}\sqrt{d}$ е фундаментално решение на равенката (1).
- Ако x_1 е парен, а y_1 е непарен, тогаш $4 \mid d$, т.е. $d = 4d'$ и $\frac{x_1}{2} + y_1\sqrt{d'}$ е фундаментално решение на равенката $x^2 - d'y^2 = 1$.
- Ако x_1 и y_1 се непарни, тогаш $d \equiv dy_1^2 \equiv x_1^2 - 4 \equiv 5 (\mathrm{mod}\, 8)$. Според тоа, потребе услов равенката (6) да има решение во множеството непарни броеви е $d \equiv 5 (\mathrm{mod}\, 8)$. На пример, за $d = 5, 13, 21, 29$ равенката (6) има решенија во множеството непарни броеви. Така, за $d = 5$ нејзиното фундаментално решение е $(x_1, y_1) = (3,1)$. Но, условот $d \equiv 5 (\mathrm{mod}\, 8)$ не е и доволен, бидејќи, на пример, за $d = 37$ фундаменталното решение на (6) е $(x_1, y_1) = (146, 24)$, па затоа сите нејзини решенија се парни.

10.8. Лема. Ако равенката (6) има решение во множеството непарни броеви и ако $x_1 + y_1\sqrt{d}$ е нејзиното фундаментално решение, тогаш

$$(\tfrac{x_1+y_1\sqrt{d}}{2})^3=\tfrac{1}{8}(x_1^3+3dx_1y_1^2)+\tfrac{1}{8}(3x_1^2y_1+dy_1^3)\sqrt{d}$$

е фундаментално решение на равенката (1).

Доказ. Броевите x_1, y_1 се непарни и $d\equiv 5(\mathrm{mod}8)$, па затоа

$$x_1^2+3dy_1^2\equiv 1+15\equiv 0(\mathrm{mod}8),\quad 3x_1^2+dy_1^2\equiv 3+5\equiv 0(\mathrm{mod}8),$$

што значи дека броевите $u_1=\tfrac{1}{8}(x_1^3+3dx_1y_1^2)$ и $v_1=(3x_1^2y_1+dy_1^3)$ се цели. Понатаму $u_1^2-dv_1^2=(\tfrac{x_1^2-dy_1^2}{4})^3=1$, т.е. $u_1+v_1\sqrt{d}$ е решение на (1).

Да претпоставиме дека $u_1+v_1\sqrt{d}$ не е фундаментално решение на (1) и нека $s_1+t_1\sqrt{d}$ е фундаменталното решение на (1). Тоа значи дека

$$1<s_1+t_1\sqrt{d}<(\tfrac{x_1+y_1\sqrt{d}}{2})^3.$$

Притоа не може да биде $s_1+t_1\sqrt{d}<\tfrac{x_1+y_1\sqrt{d}}{2}$, бидејќи тогаш $2s_1+2t_1\sqrt{d}$ ќе биде решение на (6) кое е помало од $x_1+y_1\sqrt{d}$, што е противречност. Исто така, не може да биде $s_1+t_1\sqrt{d}=(\tfrac{x_1+y_1\sqrt{d}}{2})^2$, бидејќи бројот $\tfrac{x_1^2+dy_1^2}{4}$ не е природен број. Затоа

$$(\tfrac{x_1+y_1\sqrt{d}}{2})^i<s_1+t_1\sqrt{d}<(\tfrac{x_1+y_1\sqrt{d}}{2})^{i+1} \tag{7}$$

за $i=1$ или $i=2$. Ако неравенствата (7) ги помножиме со $(\tfrac{x_1-y_1\sqrt{d}}{2})^i$ добиваме

$$1<\tfrac{a+b\sqrt{d}}{2}<\tfrac{x_1+y_1\sqrt{d}}{2},$$

каде $a^2-db^2=4$, што противречи на претпоставката дека $x_1+y_1\sqrt{d}$ е фундаментално решение на равенката (6). ■

10.9. Да ја разгледаме равенката

$$x^2-dy^2=-4 \tag{8}$$

Оваа равенка не мора да има решенија. Меѓутоа, ако равенката (3) има решение, тогаш и равенката (8) има решение, и тоа во множеството парни броеви. Но, равенката (8) може да има решенија и во множеството непарни броеви. Така, на пример за $d=5$ решение е $x=y=1$, а има непарни решенија и за $d=13,29,53$. Повторно потребен услов за постоење непарни решенија е $d\equiv 5(\mathrm{mod}8)$. Точна е следнава теорема.

Теорема. Нека претпоставиме дека равенката (8) има решение и $x_1+y_1\sqrt{d}$ е нејзиното фундаментално решение. Тогаш сите решенија на оваа равенка се дадени со формулата

$\frac{x_n+y_n\sqrt{d}}{2}=(\frac{x_1+y_1\sqrt{d}}{2})^n$ n е непарен број,

а $(\frac{x_1+y_1\sqrt{d}}{2})^2$ е фундаменталното решение на равенката (6).

Доказ. Доказот е потполно аналоген на доказот на теоремата 10.3. Деталите ги оставаме на читателот за вежба. ■

10.10. Пример. Во множеството природни броеви реши ја равенката

$$x^2-5y^2=4. \tag{9}$$

Решение. Соодветната равенка на Пел е $x^2-5y^2=1$ и нејзиното фундаментално решение е $9+4\sqrt{5}$. Понатаму, од лемата 10.8 следува дека ако $x_1+y_1\sqrt{5}$ е фундаменталното решение на равенката (9), тогаш

$$\begin{cases}72=x_1^3+15x_1y_1^2,\\32=3x_1^2y_1+9y_1^3.\end{cases} \tag{10}$$

Понатаму, бидејќи x_1 и y_1 се природни броеви, од втората равенка на системот добиваме дека единствена можност е $y_1=1$ и сега лесно се добива дека $x_1=3$ и тоа е решение на системоts (10). Според тоа, фундаменталното решение на равенката (9) е $3+\sqrt{5}$. Сега, од теорема 10,6 следува дека во множеството природни броеви сите решенија на равенката (9) се дадени со

$$x_n+y_n\sqrt{5}=2(\tfrac{3+\sqrt{5}}{2})^n,\ n\in\mathbb{N}.$$

Според тоа: $(x_1,y_1)=(3,1)$, $(x_2,y_2)=(7,3)$, $(x_3,y_3)=(18,8)$, $(x_4,y_4)=(47,21)$, ...
Забележуваме дека за првите четири решенија на равенката (9) важи

$$x_n=l_{2n}\ \text{и}\ y_n=f_{2n}, \tag{11}$$

каде f_n се Фибоначиевите броеви, а l_n се Лукасовите броеви определени со

$$l_1=1, l_2=3\ \text{и}\ l_{n+2}=l_{n+1}+l_n, \text{за}\ n\geq 1.$$

Постапувајќи аналогно како во доказот на теоремата VIII 9.6, може да се докаже дека формулите (11) се точни за секој $n\in\mathbb{N}$. Деталите ги оставаме на читателот за вежба. ■

10.11. Сега да ја разгледаме општата равенка од Пелов тип

$$x^2-dy^2=a,\ a\in\mathbb{Z}, \tag{12}$$

која ја запишуваме во видот $N(\alpha)=a$, каде $\alpha=x+y\sqrt{d}$. Ако $\alpha_0=x_0+y_0\sqrt{d}$ е едно нејзино решение, а $\xi=u+v\sqrt{d}$ е фундаменталното решение на равенката на Пел $x^2-dy^2=1$, тогаш за

$$\alpha\xi^n=(u+v\sqrt{d})^n(x+y\sqrt{d})\ \text{за}\ n\in\mathbb{N} \tag{13}$$

од својствата на нормата следува $N(\alpha\xi^n)=N(\alpha)N(\xi)^n=a\cdot 1^n=a$, т.е. броевите (13) се решенија на равенката (12). Според тоа, за да ја решиме равенката од Пелов тип (12), прво треба да ја решиме соодветната равенка на Пел $x^2-dy^2=1$. Во следната теорема ќе покажеме дека сите решенија на равенката (12) се генерирани со конечниот број нејзини таканаречени мали решенија.

10.12. Теорема. Нека a е цел број, $\alpha_1=x_1+y_1\sqrt{d}$ е решение на равенката (12) и $\xi=u+v\sqrt{d}$ е фундаменталното решение на соодветната равенка на Пел. Тогаш постојат решение $\alpha_0=x_0+y_0\sqrt{d}$ на равенката (12) и цел број m такви што

$$\alpha_1=\alpha_0\xi^m \text{ и } 2x_0^2\le|a|(u+1).$$

Доказ. Постои $m\in\mathbb{Z}$ таков што

$$\sqrt{|\tfrac{a}{\xi}|}\le\xi^m\alpha_1<\sqrt{|a\xi|}.$$

Тогаш и $\alpha_0=\xi^m\alpha_1=x_0+y_0\sqrt{d}$ е решение на (12) и важи

$$2|x_0|=|\alpha_0+\overline{\alpha_0}|=|\alpha_0+\tfrac{a}{\alpha_0}|\le\max_{[\sqrt{|\frac{a}{\xi}|},\sqrt{|a\xi|})}|t+\tfrac{a}{t}|\le\tfrac{\xi+1}{\sqrt{\xi}}\sqrt{|a|}.$$

Ако го квадрираме последното неравенство и земеме предвид дека $\xi+\frac{1}{\xi}=2u$, ја добиваме саканата оценка. ■

10.13. Пример. Во множеството цели броеви реши ја равенката:

а) $x^2-7y^2=2$,

б) $x^2-6y^2=-29$.

Решение. а) Фундаменталното решение на соодветната равенка на Пел е $u+v\sqrt{7}=8+3\sqrt{7}$. Ќе ги определиме сите решенија на равенката $x^2-7y^2=2$ за кои важи $2x^2\le|a|(u+1)=18$. Значи, $|x|\le 3$ и $|y|=\sqrt{\frac{x^2-2}{7}}\le\sqrt{\frac{3^2-2}{7}}=1$. Единствено такво решение до еквивалентност во $\mathbb{Q}[\sqrt{7}]$ е $3+\sqrt{7}$.

Според тоа, сите решенија (x,y) на дадената равенка се определени со:

$$x_n+y_n\sqrt{7}=\pm(3+\sqrt{7})(8+3\sqrt{7})^n,\ n\in\mathbb{Z}.$$

б) Фундаменталното решение на соодветната равенка на Пел е $u+v\sqrt{6}=5+2\sqrt{6}$. Ќе ги определиме сите решенија на равенката $x^2-6y^2=-29$ за кои е важи $2x^2\le|a|(u+1)=174$. Значи, $|x|<10$ и $|y|=\sqrt{\frac{x^2+29}{6}}\le\sqrt{\frac{87+29}{6}}<5$. Единствено такво решение до еквивалентност во $\mathbb{Q}[\sqrt{6}]$ е $5+3\sqrt{6}$.

Според тоа, сите решенија (x,y) на дадената равенка се определени со:

$$x_n + y_n\sqrt{6} = \pm(5+3\sqrt{6})(5+2\sqrt{6})^n,\ n\in\mathbb{Z}.\ \blacksquare$$

10.14. Пример. Во множеството цели броеви реши ја равенката

$$3x^2 - 2y^2 = 1. \tag{14}$$

Решение. Дадената равенка е еквивалентна на равенката $9x^2 - 6y^2 = 3$. Воведуваме смена $3x = z$ и ја добиваме равенката

$$z^2 - 6y^2 = 3. \tag{15}$$

Фундаменталното решение на соодветната равенка на Пел е $u+v\sqrt{6} = 5+2\sqrt{6}$. Ќе ги определиме сите решенија на равенката $z^2 - 6y^2 = 3$ за кои е исполнетао $2z^2 \le |a|(u+1) = 18$. Значи, $|z| \le 3$ и $|y| = \sqrt{\frac{x^2-3}{6}} \le \sqrt{\frac{9-3}{6}} = 1$. Единствено такво решение до еквивалентност во $\mathbb{Q}[\sqrt{6}]$ е $3+\sqrt{6}$. Според тоа, сите решенија (z,y) на равенката (15) се определени со:

$$z_n + y_n\sqrt{6} = \pm(3+\sqrt{6})(5+2\sqrt{6})^n,\ n\in\mathbb{Z}. \tag{16}$$

Сега, за да ги определиме решенијата на равенката (14) потребно е да најдеме за кои решенија на равенката (15) важи $3 \mid z_n$.

Ако $z_n + y_n\sqrt{6}$ е решение на равенката (15), тогаш од (16) следува дека

$$z_n + y_n\sqrt{6} = (5+2\sqrt{6})(z_{n-1} + y_{n-1}\sqrt{6}),$$

од каде го добиваме рекурентните формули

$$z_n = 5z_{n-1} + 12y_{n-1} \text{ и } y_n = 2z_{n-1} + 5y_{n-1},$$

од каде следува рекурентната формула

$$z_{n+1} = 10z_n - z_{n-1}. \tag{17}$$

Сега, од (16) можеме директно да пресметаме дека $z_0 = 3$ и $z_1 = 27$, односно $z_0 = -3$ и $z_1 = -27$, па од рекурентната формула (17) следува дека и во двата случаја секој z_n е делив со 3, односно определува по едно решение $x_n = \frac{z_n}{3}$. $\blacksquare$

ИНДЕКС НА ПОИМИ

А

Ајзенштајнови цели броеви, 252
Алгебарски број, 202
Аритметичка функција, 58

Б

Бескоенчна верижна дропка, 175
Бинарен систем, 16
Број на решенија на
конгруентна равенка, 101

В

Верижна (непрекината) дропка, 174
Вистински делител, 9
Вредност на верижна дропка, 181

Г

Гаусов закон за реципроцитет, 154
Гаусови прости броеви, 164
Гаусови цели броеви, 252

Д

Деленик, 14
Делител, 9, 14, 253

Е

Евклидов алгоритам, 21
Евклидско поле, 267
Единица, 255
Еквивалентен (асоцијација)
на број, 258
Еквивалентни полиномни
конгруентни равенки, 109
Експоненцијална Диофантова
равенка, 232

З

Заеднички делител, 18
Заеднички содржател, 26
Заемно прости броеви, 18, 273
Заемно прости во целина, 19
Заемно прости по парови, 19
Закон за реципроцитет, 159

К

Каноничен запис, 35
Кармајклов број, 94
Квадратно поле, 247
- -, имагинарно, 247
- -, реално, 247
Квадратно прост број, 257
Квадратно цел број, 249
k – ти парцијален количник, 176
Квадратен неостаток, 147
- остаток, 147
Кинеска теорема за
остатоци, 104, 274
Класа на конгруенции по модул, 86
Количник, 14
Комплетен систем остатоци, 85
Коневергентна верижна дропка, 181
Конволуциска инверзија, 69
Конволуциски производ (производ
на Дирихле), 67
Конгруентен, 79, 254
Конечна верижна дропка, 175
Коњугат, 247
Корен на комплексен број, 129
Критериум на Ојлер, 148

Л

Лема на Гаус, 150
Лема на Ермит, 47
Лема на Хенсел, 115
Лема на Шур, 114
Линеарна Диофантова равенка

со две непознати, 208
Линеарна Диофантова равенка со n непознати, 208
Линеарна конгруентна равенка, 101
Луивилов број, 205
Лукас-Лемеров тест, 42

М

Мебиусова инверзна формула, 71
Медијанта, 170
Мерсенов број, 41
- прост број, 41
Метод на верижни дропки, 244
Метод на Чакравала, 243
Минимален полином на алгебраски број, 203
Множество остатоци на број, 14
Мултипликативна функција, 58

Н

Најголем заеднички делител, 18
Најдобра апроксимација, 171
Најмал заеднички содржател, 26, 28
Непрекината (верижна) дропка, 174
Низа на Фарej, 169
Низа на Фибоначи, 24
Норма, 247
$n-$та конвергента на верижна дропка, 185
$n-$ти цикломатоичен полином, 132

О

Обична (стандардна) верижна дропка, 175
Ојлерова функција, 73
Определувачкиу полином, 249
Основа (база) на броен систем, 16
Основна теорема на аритметикате, 34
Остаток, 14

П

Периодична верижна дропка, 195
Питагороб триаголник, 211
Питагорова тројка, 210
Поле на остатоци по модул прост број, 124
Полиномна конгруентна равенка од $n-$ ред, 101
Постулат на Бертран, 55
Потполно мултипликативна функција, 58
Правило на двојката, 151
Примитивен корен по модул, 124
- $n-$ти корен на единицата, 130
Примитивна Питагорова тројка, 210
Примитивно решение на равенка, 221
Производ на Дирихле (конволуциски производ), 67
Прост број, 29

Р

Равенка од Пелов тип, 277
Равенка на Пел, 239
Равенка на Туе, 238
Равенство на Гаус, 48
Ред на број, 130
Ред на број по модул, 117
Редуциран систем остатоци, 87

С

Својство на единствена факторизација, 160
Симбол на Јакоби, 156
Симбол на Лежандр, 148
Систем со основа b, 16
Сложен број, 29
Совршен бро, 61
Содржател, 9

Стандардна (обична) верижна дропка, 175
Степен на алгебарски број, 203

Т

Теорема за делење со остаток, 13
- голема на Ферма, 216
- мала на Ферма, 93, 275
- на Безу, 21
- на Вилсон, 96
- на Гаус, 73
- на Дирихле, 56, 139, 168
- на Жигимонди, 143, 145
- на Кармајкл, 95
- на Лагранж, 80, 111, 113, 220
- на Лажендр, 46
- на Луивил, 66, 204
- на Лукас, 119
- на Ојлер, 61, 93, 101
- на Принсгејм, 184
- на Рот, 207
- на Туе, 238
- на Хурвиц, 171
- на Чебишев, 55

Трансацедентен број, 203

Ф

Ферматов број, 39
Фундаментално решение, 241, 278
Функција дробен дел, 44
- на Кармајкл, 95
- на Мебиус, 69
- сума, 58
- $\pi(x)$, 54
- $\sigma(n)$, збир на делители, 60
- $\tau(n)$, број на делители, 60
- цел дел, 44

Х

Хексадецимален систем, 16
Хомоген полином, 237

ЛИТЕРАТУРА

1. Adleman, L. M., Pomerance, C. Runely, R. S.: On distinguishing Prime Numbers from Composite Numbers, Ann. Of Math. 117 (1983), 173-206
2. Andreescu, T., Andrica, D.: Number Theory – Structures, Examples and Problems, Birkhauser, 2009
3. Bingulac, S., Matić, I.: Kineski teorem o ostatcima za polinome, Osječki matematički list, 12, 2012
4. Bugeaud, Y.: Approximation by Algebraic Numbers, Cambridge University Press, Cambridge, 2004.
5. Burazin, K.: Nelinearne diofantske jednadžbe, Osječki matematički list, 7, 2007
6. Burton, D. M.: Elementary Number Theory, Wm. C. Brown, Dubuque, Iowa, 1994
7. Cassels, J. W. S.: An Introduction to Diophantine Approximation, Cambridge University Press, Cambridge, 1965.
8. Damianou, P. A.: On Prime Values of Cyclotomic Polynomials, http://arxiv.org/pdf/1101.1152.pdf
9. Djukić, D., Janković, V., Matić, I., Petrović, N.: The IMO Compendium - A Collection of Problems Suggested for The International Mathematical Olympiads: 1959-2009 (Second Edition), Springer New York Dordrecht Heidelberg London, 2011
10. Dolinka, I.: Teorija brojeva: moji omiljeni zadaci, DMS, Beograd, 2007
11. Duverney, D.: Number Theory: An Elementary Introduction Through Diophantine Problems, World Scientific, 2010
12. Dye R. H., Nickakalls R. W. D.: A new algorithm for generating Pythagorean triples, Mathematical Gazette; 1998
13. Friendlander, J. B., Heath-Brown, D. R., Iwaniec, H., Kaczorowski, J.: Analytic Number Theory, Springer, Berlin, 2006
14. Gallot, Y.: Cyclotomic Polynomials and Prime Numbers, http://perso.orange.fr/yves.gallot/papers/cyclotomic.pdf
15. Ge, Y.: Elementary Properties of Cyclotomic Polynomials, http://www.yimin-ge.com/doc/cyclotomic polynomials.pdf
16. Grozdev, S., Kolev, E., Mushkarov, O., Nikolov, N.: Bulgarian Mathematical Competitions 1997-2002, SMB, Sofia, 2002
17. Hardy, G. H., Wright, E. M.: An Introduction to the Theory of Numbers, Fifth edition, Oxford, 1979
18. Hatch G.: Pythagorean triples and triangular square numbers, Mathematical Gazette; 1995
19. Hensley, D.: Continued Fractions, World Scientific, Singapore, 2006
20. Hong - Bing, Y.: Problems od Number Theory in Mathematical Competitions (Mathematical Olympiad Series), World Scientific Publishing Company, 2009
21. Ilišević, I.: Wilsonov teorem, Osječki matematički list, 4, 2004
22. Khinchin, A. Y.: Continued Fractions, Dover, New York, 1997

23. Khintchie, A. Y.: Continued Fractions, Noordhoff, Groningen, 1963
24. Landau, E.: Elementary number theory, Chelsea Publishing Company, New York, 1966
25. Lang, S.: Introduction to Diophantine Approximations, Springer-Verlag, New York, 1995
26. Loo, A.: Zsigmondys Theorem, Mathematical excalibur, Vol. 16, No. 4, 2012
27. Mandić, I., Soldo, I.: Pellova jednadžba, Osječki matematički list, 8, 2008
28. Mićić, V., Kadelburg, Z.: Uvod u teoriji brojeva, DMS, Beograd, 1989
29. Nakić, I.: Diskretna matematika, https://web.math.pmf.unizg.hr/ nastava/ komb/predavanja/predavanja.pdf
30. Nathanson, M. B.: Elementary Methods in Number Theory, Springer, 1993
31. Neville, R.: Beginning Number Theory, 2nd ed. Sudbury, Mass.: Jones and Bartlett, 2006.
32. Newman, D. J.: Simple Analytic Proof of the Prime Number Theorem, Am. Math. Montly, 87, 1980
33. Niven, I., Zuckerman, H. S.: An introduction to the Theory of Numbers, John Wiley & Sons, Inc., New Yor, 1980
34. Niven, I.: Diophantine Approximations, John Wiley & Sons, New York, 1963.
35. Parvardi, A. H.: Lifting The Exponent Lemma, 2011, http://www.artofproblemsolving.com/Resources/Papers/LTE.pdf
36. Santos, D. A.: Number Theory for Mathematical Contests, http://docplayer.net/217662-Number-theory-for-mathematical-contests-david-asantos-dsantos-ccp-edu.html
37. Schmidt, W. M.: Diophantine Approximation and Diophantine Equations, Springer-Verlag, Berlin, 1996
38. Schmidt, W. M.: Diophantine Approximation, Springer-Verlag, Berlin, 1996
39. Shockley, J. E.: Introduction to Number Theory, Holt, Rinehart and Winston, Inc., New York, 1967
40. Shoup, V.: A Compuaitional to Number Theory and Algebra, Cambridge University Press, 2005
41. Sierpinski, W.: Elementary theory of numbers, PWN, Warszawa, 1964
42. Sitaramachandrarao, R., Suryanarayana, D.: On $\sum_{n\le x}\sigma^*(n)$ and $\sum_{n\le x}\varphi^*(n)$, Proc. Of the Amer. Math. Soc., Vol. 41, 1973
43. Stark, H. M.: An introduction to Number Theory, Markh. Publis. Comp., Chicago, 1970
44. Sun, L.: Cyclotomic Polynomials in Olympiad Number Theory, http://lessol.w.staszic.waw.pl/pdfy/h.pdf
45. Tafro, A.: Kongruencije, Playmath, 1, 2003
46. Thompson, L.: Zsigmondy's Theorem, 2009, www.artofproblemsolving.com/Forum/download/file.php?id=25872

47. Tonov, I., Bankov, K., Vitanov, T., Rakovska, D.: Bulgarian Mathematics Competitions, Selected Problems, Regalia, Sofia, 2001
48. Vandendriessche, P., Lee, H.: Problems in elementary number theory, http://www.problem-solving.be/pen/published/pen-20070711.pdf
49. Varošanec, S.: Diofantske jednadžbe, https://web.math.pmf.unizg.hr/nastava/metodika/materijali/diofant.pdf
50. Vehka, T.: Explicit Construction of a Admissible Set the Conjecture that sometimes $\pi(x+y) > \pi(x)+\pi(y)$, Notices Am. Math. Soc. 26, 1979
51. Xiong Bin, Lee Peng Yee: Mathematical Olympiad in China (Problem and Solutions), East China Normal University Press & World Scientific, 2007
52. Алексиев, К., Бангачев, К., Бойваленков, П.: 640 задачи или Теория на числата за олимпиади, УНИМАТ СМБ, София, 2017
53. Арноль, И. В.: Теория чиесл, Учиедгиз, Москва, 1939
54. Ашић, М., Божић, М., Чукић, Љ., Јанковић, В., Каделбург, З., Мићић, В., Милин, Л., Вукмировић: Међународне математичке олимпијаде, ДМС, Београд, 1986
55. Бухштаб, А. А.: Теория чисел, Москва, 1966
56. Виноградов, И. М.: Основы теории чисел, Наука, Москва, 1972
57. Гаврилов, М, Давидов, Л. Делимост на числата, Народна просвета, София, 1976
58. Дирихле, П. Г. Л.: Лекции по теория на числата, Наука и изкуство, София, 1980
59. Дуденков, С., Чакърян, К.: Задачи по теория на числата, Регалия 6, София, 1999
60. Ђукић, Д., Радовановић, М.: Математичке олимпијаде средњошколаца од 2012 до 2019 године, ДМ Србије, Београд, 2012
61. Ђукић, Д.: Апроксимације ирационалних бројева рационалним, Београд, 2015
62. Ђукић, Д.: Аритметичка својства биномних коефицијената, Београд, 2017
63. Ђукић, Д.: Верижни разломци, Београд, 2011
64. Ђукић, Д.: Дељивост и канонска факторизација, Београд, 2014
65. Ђукић, Д.: Квадратна раширења поља рационалних бројева, Београд, 2012
66. Ђукић, Д.: Конгруенције вишег степена, Београд, 2012
67. Ђукић, Д.: Пелова једначина, Београд, 2015
68. Јанковић, В., Каделбург, З., Младеновић, П.: Међународне и балканске математичке олимпијаде 1984-1995, ДМС; Београд, 1996
69. Јанковић, З., Каделбург, З., Младеновић, П.: Међународне и балканске математичке олимпијаде 1984-1995, ДМС, Београд, 1995
70. Каделбург, З., Младеновић, П.: Савезна такмичења из математике, ДМС, Београд, 1990
71. Кендеров, П., Табов, Й.: Български олимпиади по математика, Народна просвета, София, 1990

72. Кртинић, Ђ.: Математичке олимпијаде средњошколаца 2007-2011 године, ДМ Србије, Београд, 2012
73. Кудреватов, Г. А.: Сборник задач по теории чисел, Просвещение, Москва, 1970
74. Лукић, М.: Експоненцијалне конгруенције, Београд, 2006
75. Малешевић, Б.: Рационалне апроксимације реалних бројева и неке примене, Настава математике XLIII, 3, 1998
76. Малчески, Р., Малчески, А., Аневска, К.: Вовед во елементарна теорија на броеви, СММ, Скопје, 2015
77. Малчески, А., Малчески, Р.: Функционални равенки во множествата природни и цели броеви, Математички талент, Скопје, 2021
78. Малчески, Р., Малческа, В.: Математика 1 – алгебарски структури (трето издание), Армаганка, Скопје, 2020
79. Малчески, Р., Малческа, В.: Математика 5 – дискретна математика (второ издание), Армаганка, Скопје, 2020
80. Малчески, Р., Малчески, А., Малчески, С.: Балкански математички олимпијади 1984-2020, Скопје, 2021
81. Малчески, Р., Малчески, А., Малчески, С.: Маѓународни математички олимпијади 1959-2019, Скопје, 2021
82. Малчески, Р., Малчески, С.: Белешка за распределбата на простите броеви, Сигма, Скопје, 2018
83. Малчески, Р., Малчески, С.: Диофантови апроксимации, Математика, София, 2021
84. Малчески, Р., Малчески, С.: Ред на број по модул и примитивни корени, Сигма, Скопје, 2018
85. Малчески, Р.: Мултипликативни функции и теорема на Ојлер, Сигма, Скопје, 2004
86. Малчески, Р.: Основи на математичка анализа (трето издание), Армаганка, Скопје, 2019
87. Малчески, Р.: Теорема на Луивил, Скопје, 2020,
88. Малчески, Р.: Функциите [x] и {x}, Сигма, Скопје, 2015
89. Малчески, С.: Математички талент 26 – збирка задачи по елементарна теорија на броеви, Скопје, 2021
90. Марчевский, М. Н.: Теория чисел, Издательство Харьковского Университета, Харьков, 1958
91. Мићић, В., Каделбург, З.: Увод у теорији бројева, ДМС, Београд, 2001
92. Михелович, Ш. Х.: Теория чисел, Высшая школа, Москва, 1967
93. Морозова, Е. А., Петраков, А. С., Скворцов, В. А.: Международные математические олимпиады, Просвещение, Москва, 1976
94. Нагел, Т.: Увод в теорията на числата, Наука и изкуство, София, 1971
95. Серпинский, В.: 250 задач по елементарной теории чисел, Просвещение, Москва, 1976

96. Серпинский, В.: Что мы знаем и чего мы не знаем о Простиых числа, Физматгиз, Москва, 1963
97. Тошић, Р., Вукосавчевић, В.: Елементи теорије бројева, Алеф, Нови сад, 1995
98. Тренчевски, К., Урумов, В.: Меѓународни олимпијади по математика, Природно – математички факултет, Скопје, 2000
99. Трост, Э.: Простые числа, Гусадарственное издатечьство физико-математической литературы, Моска, 1959
100. Филиповски, С.: 200 –теорија на броеви (подготвителни задачи), Скопје, 2013
101. Хинчин, А. Я.: Три бисера од теорията на числата, Наука и изкуство, София, 1971
102. Хинчин, А. Я.: Цепные дроби, Физматгиз, Москва, 1961
103. Хинчин, А. Я.: Элементи теории чиесл, Гостехиздат, Москва-Ленинград, 1951
104. Цветковски, З., Малчески, Р.: Алгоритам за генерирање на една класа Питагорини тројки, Сигма, Скопје, 2006
105. Чупона, Ѓ., Трпеновски, Б.: Алгебра, Просветно дело, Скопје
106. Шидловский, А. Б.: Диофантовы приближения и трансцедентные числа, Изд. Московского универзитета, Москва, 1982
107. Шнилерман, Л. Г.: Простые числа, Гостехиздат, Москва-Ленинград, 1940