Ристо Малчески, Скопје

МУЛТИПЛИКАТИВНИ ФУНКЦИИ И ТЕОРЕМА НА ОЈЛЕР

Како што знаеме броевите кои при делење со еден ист број даваат ист остаток се од посебен интерес во теоријата на броеви. Токму затоа тие биле предмет на разработка на многу знаменити математичари, што довело до поимот конгруенција во множеството цели броеви, т.е. методот на конгруенции во множеството цели броеви. Овој метод е формален аритметички метод заснован на разгледување на својствата на целите броеви кои имаат еднакви остатоци при делење со еден ист број. Методот прв го разработил германскиот математичар Гаус (1777-1855) иако многу резултати биле познати и порано. Во нашите разгледувања ќе препоставиме дека на читателот му се познати основните својства на конгруенциите и подетално ќе се осврнеме на мултипликативните функции и теоремите на Ојлер, Ферма и Вилсон. Притоа, подетално ќе ја разгледаме Ојлеровата функција која има голема примена во криптоанализата (шифрирањето и дешифрирањето).

На почетокот ќе ја дадеме дефиницијата за конгруенција и ќе наведеме неколку соновни својства за конгруенциите кои ни се неопходни за натамошните разгледувања и чии докази можат да се видат, на пример, во [2].

Дефиниција 0.1. Нека $a,b\in\mathbf{Z}$ и $m\in\mathbf{N}$. Ако $m\mid(a-b)$, тогаш ќе велиме дека бројот a *е конгруентен* со бројот b по модул m и ќе пишуваме $a\equiv b\pmod m$.

Ако $m\nmid(a-b)$, тогаш ќе велиме дека бројот a *не е конгруентен* со бројот b по модул m и ќе пишуваме $a\not\equiv b\pmod m$.

Теорема 0.1. а) За секој $a\in\mathbf{Z}$ важи $a\equiv a\pmod m$.

б) Ако $a\equiv b\pmod m$, тогаш $b\equiv a\pmod m$.

в) Ако $a\equiv b\pmod m$ и $b\equiv c\pmod m$, тогаш $a\equiv c\pmod m$. ♦

Теорема 0.2. а) Ако $\text{НЗД}(a,m)=1$ и $ab\equiv ac\pmod m$, тогаш $b\equiv c\pmod m$

б) Ако $\text{НЗД}(a,m)=d$ и $ab\equiv ac\pmod m$, тогаш $b\equiv c\pmod q$ каде што $q=\frac{m}{d}$.

в) Ако $\text{НЗД}(a,m)=d$, $q=\frac{m}{d}$ и $b\equiv c\pmod q$, тогаш $ab\equiv ac\pmod m$. ♦

1. МУЛТИПЛИКАТИВНИ ФУНКЦИИ

Дефиниција 1.1. За функцијата $f:\mathbb{N}\to\mathbb{Z}$ ќе велиме дека е *мултипликативна* ако

1) постои $n_0\in\mathbb{N}$ таков да $f(n_0)\neq 0$ и
2) ако $\text{НЗД}(m,n)=1$, тогаш $f(mn)=f(m)f(n)$.

Ако условот 2) е исполнет за секои $m,n\in\mathbb{N}$, заемно прости или не, тогаш ќе велиме дека функцијата f е *потполно мултипликативна*.

Теорема 1.1. Ако f е мултипликативна функција, тогаш функцијата g дефинирана со $g(n)=\sum_{d|n} f(d)$ е мултипликативна.

Доказ. Нека $m>1, n>1$ и $\text{НЗД}(m,n)=1$. Имаме

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

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

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

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 пзоитивни делители на mn и притоа не се повторува ниту еден делител на mn. Значи,

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

Дефиниција 1.2. Нека $n\in\mathbb{N}$. Со $d(n)$ го означуваме множеството од сите природни делители на n. Со $\sigma(n)$ го означуваме збирот од сите природни делители на n.

Пример 1.1. Во следнава табела се презентирани вредностите на $d(n)$ и $\sigma(n)$, за $n=1,2,3,...,17$.

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

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

Теорема 1.2. Функциите $d(n)$ и $\sigma(n)$ се мултипликативни.

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

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

од теорема 1.1. следува дека функцијата $d(n)$ е мултипликатвна.

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

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

од теорема 1.1. следува дека функцијата $\sigma(n)$ е мултипликатвна. $\blacklozenge$

Теорема 1.3. Ако $n=p_1^{a_1}p_2^{a_2}...p_k^{a_k}$, тогаш

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

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

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

Сега равенствата (1) следуваат од мултипликативноста на функциите $d(n)$ и $\sigma(n)$. $\blacklozenge$

Пример 1.2. Докажи:

а) $\sum_{d|n} d^k = \sum_{d|n} (\frac{n}{d})^k$ и б) $d(n) < 2\sqrt{n}$.

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 полн квадрат, тогаш неговите делители ги групираме во парови од видот $(d, \frac{n}{d})$, $d < \frac{n}{d}$, кои ги има поналку од $\sqrt{n}$. Ако n е полн квадрат, тогаш

$$d(n) \le 2(\sqrt{n}-1)+1 < 2\sqrt{n}. \blacklozenge$$

Пример 1.3. Докажи $\sqrt{n} \le \frac{\sigma(n)}{d(n)}$, $n > 1$.

Решение. Од

$$\sigma(p^a) = \frac{p^{a+1}-1}{p-1} = 1 + p + p^2 + ... + p^a \ge (a+1)p^{\frac{a}{2}} = d(p^a)p^{\frac{a}{2}}$$

добиваме $\frac{\sigma(p^a)}{d(p^a)} \ge \sqrt{p^a}$ и ако ја искористиме мултипликативноста на функциите $d(n)$ и $\sigma(n)$ добиваме $\sqrt{n} \le \frac{\sigma(n)}{d(n)}$. $\blacklozenge$

2. СИСТЕМИ ОСТАТОЦИ

Од теоремата 0.1 непосредно следува дека релацијата "... е конгруентен со ... по модул m ..." е реалција 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 дефинција.

Дефиниција 2.1. 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 да $x \equiv y_i (\mathrm{mod}\, m)$.

Теорема 2.1. Нека $\text{НЗД}(a, m) = 1$ 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 $\text{НЗД}(a, m) = 1$ следува дека постојат $c, k \in \mathbb{Z}$ такви да $ac + mk = 1$, што значи $ac \equiv 1 (\mathrm{mod}\, m)$. Ако $d \in \mathbb{Z}$, тогаш постои единствен $t \in \{1, 2, ..., m\}$ таков да $c(d-b) \equiv a_t (\mathrm{mod}\, m)$. Но, тогаш

$$d - b \equiv ac(d-b) \equiv aa_t (\mathrm{mod}\, m),$$

т.е. $d \equiv (aa_t + b) (\mathrm{mod}\, m)$.

Ако $d \equiv (aa_i + b) (\mathrm{mod}\, m)$, тогаш $(aa_i + b) \equiv (aa_t + b) (\mathrm{mod}\, m)$, па затоа $aa_i \equiv aa_t (\mathrm{mod}\, m)$. Но, $\text{НЗД}(a, m) = 1$ и од последната конгруенција и теорема 0.2

следува $a_i \equiv a_t (\mathrm{mod}\, m)$, што значи $i = t$. Според тоа, T е комплетен систем остатоци по модул m. ♦

Дефиниција 2.2. 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.

Теорема 2.2. Ако $\text{НЗД}(a, m) = 1$ 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 ист број елементи.

Доказ. Од дефиницијата 2.2 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 $a \equiv b (\mathrm{mod}\, m)$. Од $\text{НЗД}(a, m) = 1$ следува дека и $\text{НЗД}(b, m) = 1$, 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' добиваме дека бројот на елементите на S'' е поголем или еднаков на бројот на елементите на S'. Значи, S' и S'' имаат ист број елементи. ♦

Теорема 2.3. 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 еднакво на бројот на елементите на S'.

Доказ. Бидејќи $S = \{1, 2, ..., m\}$ е комплетен систем остатоци по модул m, добиваме дека $S' = \{k \mid k \in S, \text{НЗД}(m, k) = 1\}$ е редуциран систем остатоци по модул m. Сега тврдењето следува од теорема 2.2. ♦

3. ОЈЛЕРОВА ФУНКЦИЈА

Дефиниција 3.1. Функцијата $\varphi : \mathbb{N} \to \mathbb{N}$, каде $\varphi(m)$, $m \in \mathbb{N}$ е еднаков на бројот на елементите на произволен редуциран систем остатоци по модул m ја нарекуваме *Ојлерова функција*.

Пример 3.1. а) Бидејќи за секој прост број p сите елементи на множеството $\{1, 2, ..., p-1, p\}$, освен p, се заемно прости со p добиваме $\varphi(p) = p - 1$.

б) 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	9	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. ♦

Теорема 3.1. Ако $\text{НЗД}(a,m)=1$ 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 дефиниција 2.2 имаме $S'\subseteq S=\{a_1,a_2,...,a_m\}$, каде S е комплетен систем остатоци по модул m. Според теорема 2.1 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, па затоа доволно е да докажеме дека $\text{НЗД}(aa_j,m)=1$, за $j=1,2,...,m$. Последното тврдење следува од равенствата $\text{НЗД}(a,m)=\text{НЗД}(a_j,m)=1$, за $j=1,2,...,m$. ♦

Теорема 3.2. Ако a и p се природни броеви и p е прост број, тогаш

$$\varphi(p^a)=p^a(1-\tfrac{1}{p}).$$

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, $\varphi(p^a)=p^a-p^{a-1}=p^a(1-\tfrac{1}{p})$. ♦

Теорема 3.3. Ојлеровата функција φ е мултипликативна.

Доказ. Јасно $\varphi(1)=1\neq 0$. Нека $\text{НЗД}(m,n)=1$. Во следнава табела ќе го определиме бројот $\varphi(mn)$ на елементите кои се заемно прости со mn. Имаме

1	2	3	$...$	k	$...$	n
$n+1$	$n+2$	$n+3$	$...$	$n+k$	$...$	$2n$
$...$	$...$	$...$	$...$	$...$	$...$	$...$
$(m-1)n+1$	$(m-1)n+2$	$(m-1)n+3$	$...$	$(m-1)n+k$	$...$	mn

Да забележиме дека ако за фиксирано k и за некој $i\in\{0,1,2,...,m-1\}$ бројот $in+k$ е заемно прост со n, тогаш и за секој $j\in\{0,1,2,...,m-1\}$ бројот $jn+k$ е заемно рпост 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 $\varphi(n)$. Бидејќи $\text{НЗД}(m,n)=1$, 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 $\varphi(m)\varphi(n)=\varphi(mn)$. ♦

Пример 3.2. Бидејќи $660=5\bullet 11\bullet 12$, од претходната теорема следува

$$\varphi(660)=\varphi(5)\varphi(11\bullet 12)=\varphi(5)\varphi(11)\varphi(12)=4\bullet 10\bullet 4=160.$$ ♦

Теорема 3.4. Ако $n=p_1^{a_1}p_2^{a_2}...p_k^{a_k}$ е каноничниот запис на број n, тогаш

$$\varphi(n)=p_1^{a_1}p_2^{a_2}...p_k^{a_k}(1-\tfrac{1}{p_1})(1-\tfrac{1}{p_2})...(1-\tfrac{1}{p_k}).$$

Доказ. Непосредно следува од теоремите 3.2 и 3.2. ♦

4. ТЕОРЕМА НА ОЈЛЕР

Теорема 4.1. (Ојлер). Ако $\text{НЗД}(a,m)=1$, тогаш $a^{\varphi(m)} \equiv 1 (\text{mod}\, m)$.

Доказ. Нека $\{a_1, a_2, ..., a_{\varphi(m)}\}$ е редуциран систем остатоци по модул m. Според теоремата 3.1 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 да $a_i \equiv aa_j (\text{mod}\, m)$. Ако ги помножиме сите конгруенции од овој вид, ги има точно $\varphi(m)$, добиваме

$$a^{\varphi(m)} a_1 a_2 ... a_{\varphi(m)} \equiv a_1 a_2 ... a_{\varphi(m)} (\text{mod}\, m).$$

Бидејќи $\text{НЗД}(a_i, m)=1$, за $i=1,2,...,\varphi(m)$, од последната конгруенција добиваме $a^{\varphi(m)} \equiv 1 (\text{mod}\, m)$. ♦

Пример 4.1. Докажи дека $2^{340}-1$ не е прост број.

Решение. Од теоремата на Ојлер следува $2^{10} = 2^{\varphi(11)} \equiv 1 (\text{mod}\, 11)$. Значи,

$$2^{340} = (2^{10})^{34} \equiv 1^{34} (\text{mod}\, 11), \text{ т.е. } 11 \mid (2^{340}-1).$$

Според тоа, $2^{340}-1$ не е прост број. ♦

Пример 4.2. Докажи дека за секој природен број n бројот $N = 1 + 2^{2 \bullet 5^n}$ се дели со 5^{n+1}.

Решение. Од теоремата на Ојлер имаме $2^{4 \bullet 5^n} \equiv 2^{\varphi(5^{n+1})} \equiv 1 (\text{mod}\, 5^{n+1})$. Значи, 5^{n+1} е делител на производот $(2^{2 \bullet 5^n}+1)(2^{2 \bullet 5^n}-1)$. Двата множители во последниот производ се заемно прости и $5 \nmid (2^{2 \bullet 5^n}-1)$ (провери!), па затоа $5^{n+1} \mid (2^{2 \bullet 5^n}+1)$. ♦

Теорема 4.2. (Ферма). Ако p е прост број и $\text{НЗД}(a,p)=1$, тогаш

$$a^{p-1} \equiv 1 (\text{mod}\, p).$$

Доказ. Од $\text{НЗД}(a,p)=1$, според теорема 4.1 добиваме $a^{\varphi(p)} \equiv 1 (\text{mod}\, p)$ и како $\varphi(p) = p-1$ имаме $a^{p-1} \equiv 1 (\text{mod}\, p)$. ♦

Последица 4.1. Ако p е прост број, тогаш за секој цел број a важи

$$a^p \equiv a (\text{mod}\, p). \text{ ♦}$$

Пример 4.3. Ако p и q се различни прости броеви, тогаш

$$p^{q-1} + q^{p-1} \equiv 1 (\text{mod}\, pq).$$

Докажи!

Решение. Од теоремата 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.

$$pq \mid (p^{q-1}q^{p-1} - p^{q-1} - q^{p-1} + 1). \tag{2}$$

Бидејќи p и q се прости броеви имаме

$$pq \mid p^{q-1}q^{p-1}. \tag{3}$$

Од (2) и (3) непосредно следува дека $pq \mid (p^{q-1}+q^{p-1}-1)$, т.е.

$$p^{q-1}+q^{p-1} \equiv 1 (\mathrm{mod}\ pq).$$ ♦

Теорема 4.3. (Вилсон). Ако p е прост број, тогаш

$$(p-1)! \equiv -1 (\mathrm{mod}\ p).$$

Доказ. За $p=2$ и $p=3$ непосредно се проверува дека тврдењето важи. Нека претпоставиме дека $p \geq 5$.

Да забележиме дека $1 \equiv 1 (\mathrm{mod}\ p)$ и $p-1 \equiv -1 (\mathrm{mod}\ p)$. За секој $j, 2 \leq j \leq p-2$ важи $\mathrm{НЗД}(j,p)=1$, па затоа постои еден и само еден i така да $ij \equiv 1 (\mathrm{mod}\ p)$ 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 да $ij \equiv 1 (\mathrm{mod}\ p)$ и $2 \leq i \leq p-2$. Притоа $i \neq j$, бидејќи за секој $j, 2 \leq j \leq p-2$ имаме

$$\mathrm{НЗД}(j-1,p) = \mathrm{НЗД}(j+1,p) = 1$$

и затоа

$$j^2 - 1 = (j-1)(j+1) \not\equiv 0 (\mathrm{mod}\ p).$$

Така, броевите $2,3,\ldots,p-2$ ги поделивме на $\frac{p-3}{2}$ дисјунктни двоелементни множества $\{i,j\}$ за кои важи $ij \equiv 1 (\mathrm{mod}\ p)$. Ако ги помножиме овие конгруенции добиваме $2 \bullet 3 \bullet 4 \bullet \ldots \bullet (p-2) \equiv 1 (\mathrm{mod}\ p)$ и како $1 \equiv 1 (\mathrm{mod}\ p)$ и $p-1 \equiv -1 (\mathrm{mod}\ p)$ од последните три конгруенции следува $(p-1)! \equiv -1 (\mathrm{mod}\ p)$. ♦

Пример 4.4. Докажи дека, ако $(m-1)! \equiv -1 (\mathrm{mod}\ p)$, 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. ♦

5. ЗАДАЧИ ЗА САМОСТОЈНА РАБОТА

1. Најди природен број n така да $n = 2d(n)$.
2. Бројот n е совршен ако $\sigma(n) = 2n$. Докажи дека
   a) Ако $n = 2^{k-1}(2^k - 1), k > 1$ и $p = 2^k - 1$ е прост број, тогаш n е совршен број.
   b) Ако n е парен совршен број, тогаш $n = 2^{k-1}(2^k - 1), k > 1$ и $p = 2^k - 1$ е прост број.
3. Докажи дека постојат бесконечно многу природни броеви n такви да $\sigma(n) = 2n - 1$.
4. Докажи дека броевите $d(m^n)$ и n се заемно прости.
5. Нека m и r се заемно прости цели броеви и $m > 0$. Докажи дека множеството $\{a, a+r, a+2r, \ldots, a+(m-1)r\}, a \in \mathbb{Z}$ е потполн систем остатоци по модул m.
6. Нека $\{a_1, a_2, \ldots, a_m\}$ е потполн систем остатоци по модул m, $\{b_1, b_2, \ldots, b_n\}$ е потполн систем остатоци по модул n и $\mathrm{НЗД}(m,n)=1$. Докажи дека множеството S од сите природни броеви од видот $a_i n + b_j m, i = 1,2,\ldots,m; j = 1,2,\ldots,n$ е потполн систем остатоци по модул mn.

7. Нека $\{a_1, a_2, ..., a_{\varphi(m)}\}$ е редуциран систем остатоци по модул m, $\{b_1, b_2, ..., b_{\varphi(n)}\}$ е потполн систем остатоци по модул n и $\text{НЗД}(m,n)=1$. Докажи дека множеството S од сите природни броеви од видот $a_i n + b_j m, i = 1,2,...,\varphi(m); j = 1,2,...,\varphi(n)$ е редуциран систем остатоци по модул mn.
8. Докажи
   а) $\varphi(p^a) = p^{a-1}\varphi(p)$, $p, a \in \mathbb{N}$ и p е прост број.
   б) $\varphi(m^a) = m^{a-1}\varphi(m)$, $m, a \in \mathbb{N}$.
9. Дадено е $\varphi(m)$. Најди $\varphi(2m)$.
10. Докажи дека $\varphi(4m) = \begin{cases} \varphi(2m), & \text{НЗД}(m,2)=1, \\ 2\varphi(2m), & \text{НЗД}(m,2)=2. \end{cases}$
11. Нека p е прост број. Пресметај го збирот $\varphi(1)+\varphi(p)+\varphi(p^2)+...+\varphi(p^a)$, $a \in \mathbb{N}$.
12. Докажи дека за секој природен број n важи $\sum_{d|n} \varphi(d) = n$.

ЛИТЕРАТУРА

1. Кудреватов, Г. А.: *Сборник задач по теории чисел*, ПросвеЋение, Москва, 1970
2. Малчески, Р.: *Елементарна алгебра*, Просветно дело, Скопје, 2002
3. Mićić, V.; Kadelburg, Z.: *Uvod u teoriju brojeva*, DMS, Beograd, 1989
4. Tošić, R.; Vukoslavčević, V.: *Elementi teorije brojeva*, Alef, Novi Sad, 1995

Статијата прв пат е објавена во списанието Сигма на СММ