Даниел Велинов
Скопје

РЕД НА ПРОСТ БРОЈ

Овде ќе го воведеме поимот ред на број по модул n. Користејќи ја дефиницијата ќе докажеме дека од $p \mid n^2+1$ следува $p \equiv 1 (\mathrm{mod}\, 4)$. Потоа ќе биде воведен терминот примитивен корен. Користејќи го примитивниот корен ќе ја докажеме и обратната насока.

Дополнително ќе бидат дадени примери, кои лесно може да се решат користејќи го терминот ред на прост број и примитивен корен.

Ќе биде разгледана и лемата за кревање на експонент (Lifting The Exponent Lemma), која скратено ќе ја означуваме како LTE. Многу проблеми од експоненцијалните равенки или теоријата на броеви, со помош на оваа лема може многу едноставно да се решат. Со помош на оваа лема, можеме да го најдеме најголемиот степен на прост број $p \geq 3$, кој ги дели $a^n \pm b^n$, за некои природни броеви.

Нека p е прост број и нека $a \not\equiv 0 (\mathrm{mod}\, p)$. Под ред на $a \pmod p$ се подразбира најмалиот природен број m така што $a^m \equiv 1 \pmod p$. Често се означува и со $ord\, a \pmod p$ или $ord_p a$.

Ред на $a \pmod p$ е секогаш конечен број заради теоремата на Ферма бидејќи $a^{p-1} \equiv 1 \pmod p$, т.е. редот на $a \pmod p$ е најмногу $p-1$.

Јасно, може да забележиме дека сите редови се делители на $p-1$. Навистина, ако $m \mid p-1$, тогаш $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.

Теорема 1. (Фундаментална теорема за ред на прост број) Нека $a^n \equiv 1 (\mathrm{mod}\, p)$. Тогаш редот на $a \pmod p$ го дели n.

Да забележиме дека Теорема 1 е точна и во ситуација кога простиот број p ќе го замениме со било кој природен број n за кој важи $Н.З.Д(a,n)=1$. Во овој случај $m \mid \varphi(n)$, каде $\varphi(n)$ е Ојлеровата функција.

Теорема 2. Нека $p \geq 3$ е прост број. Ако $n^2 \equiv -1 (\mathrm{mod}\, p)$, тогаш $p \equiv 1 (\mathrm{mod}\, 4)$.

Доказ. Ако ги квадрираме двете страни на $n^2 \equiv -1 (\mathrm{mod}\, p)$ добиваме $n^4 \equiv 1 (\mathrm{mod}\, p)$. Сега тврдиме дека редот на n по модул p е точно 4. Ако ова не е точно, тогаш редот мора да биде 2 или 1, од каде $n^2 \equiv 1 (\mathrm{mod}\, p)$. Но, ова е контрадикција со условот $n^2 \equiv -1 (\mathrm{mod}\, p)$. Значи редот на n по модул p е 4.

Бидејќи сите редови по модул p се делители на $p-1$, добиваме дека $4 \mid p-1$, односно $p \equiv 1 (\mathrm{mod}\, 4)$.

Идејата на наредната теорема која ќе ја дадеме без доказ е дека секој ненулти остаток по модул p може да се запише на единствен начин со g^{α}, каде $\alpha = 1, 2, 3, ..., p-1$.

Теорема 3. Нека p е прост број. Тогаш постои цел број g, кој го нарекуваме примитивен корен, така што редот на q модул p е еднаков на $p-1$.

Сега ќе ја дадеме обратната теорема на Теорема 2.

Теорема 4. Ако $p \equiv 1 (\mathrm{mod}\, p)$ е прост број, тогаш постои n така што $n^2 \equiv -1 (\mathrm{mod}\, p)$.

Доказ. Нека g е примитивен корен по модул p. Тогаш бараното n го дефинираме како $n = g^{\frac{p-1}{4}}$. Јасно е дека $n^2 \equiv -1 (\mathrm{mod}\, p)$.

Теорема 5. Примитивен корен по модул n е цел број g за кој важи $Н.З.Д(g, n) = 1$ така што g има ред по модул n, $\varphi(n)$, каде $\varphi(n)$ е Ојлеровата функција. Примитивен корен по модул n постои ако и само ако $n = 2$, $n = 4$, $n = p^k$ или $n = 2p^k$, каде $p \geq 3$ е прост број.

Пример 1. (МОР, 2011) Нека p е прост број и нека n е природен број. Нека p целосно го дели $2^n - 1$ (тоа значи дека $p \mid 2^n - 1$, но p^2 не го дели $2^n - 1$. Докажи дека p целосно го дели $2^{p-1} - 1$.

Решение. Јасно $p \neq 2$, па претпоставуваме дека p е непарен. Нека со m го означиме редот на 2 по модул p. Па, $p \mid 2^m - 1$. Јасно е и дека m е делител и на n и на $p-1$. Од $m \mid n$, можеме да заклучиме дека $p \mid 2^m - 1 \mid 2^n - 1$.

Да забележиме дека бројот $2^n - 1$ има точно еден степен на p во неговата канонична репрезентација, па оттука $2^m - 1$ има точно еден степен на p (има најмалку еден бидејќи $p \mid 2^m - 1$ и има најмногу еден бидејќи $p \mid 2^n - 1$). Останува да покажеме дека ако $p \mid 2^m - 1$, тогаш $2^{p-1} - 1$ не се здобива со дополнителен степен на p. Нека го разгледаме количникот

$$\frac{2^{p-1}-1}{2^m-1} = 1 + 2^m + (2^m)^2 + ... + (2^m)^{\frac{p-1}{m}-1}.$$

Ако докажеме дека количникот не е делив со p, сме го докажале тврдењето на задачата. Ако гледаме по модул p, добиваме

$$\frac{2^{p-1}-1}{2^m-1} \equiv \underbrace{1+1+\ldots+1}_{\frac{p-1}{m}} = \frac{p-1}{m} \pmod{p}.$$

Бидејќи, $0 < \frac{p-1}{m} < p$, па докажавме дека количникот не е делив со p, од каде добиваме дека p целосно го дели $2^{p-1}-1$.

Пример 2. Најди ги сите природни броеви n, за кои $n \mid 2^n - 1$.

Решение. Единствената вредност за кој важи барањето на задачата е $n=1$. Јасно, мора n да биде непарен, бидејќи $2^n - 1$ е непарен. Нека p е прост број кој е делител на n. Имаме, $p \mid 2^n - 1$, односно $2^n \equiv 1 \pmod{p}$. Па можеме да го реформулираме проблемот, како: За било кој прост број $p \mid n$, редот на 2 по модул p исто така го дели n.

Сега нека го земеме најмалиот прост број кој го дели n ($p > 2$). Нека $m = ord_p 2$ и $p \neq 2$. Тогаш редот на m мора да го дели n, но исто така мора да го дели $p-1$. Но, ова е можно само кога $m=1$, што не е можно. Значи $n=1$ е единствениот природен број за кој важи $n \mid 2^n - 1$.

Пред да ја дадеме LTE, ќе дадеме две важни и корисни леми.

Нека $p \mid n$. Со $v_p(n)$ ќе го означуваме степенот на p во каноничната репрезентација на n.

Лема 1. Нека x и y се цели броеви и n е природен број. За произволен прост број p за кој $Н.З.Д(n, p) = 1$, $n \mid x - y$ и ниту x ниту y се деливи со p. Тогаш $v_p(x^n - y^n) = v_p(x - y)$.

Доказ. Ќе користиме дека

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \ldots + y^{n-1}).$$

Сега ако покажеме дека p не е делител на

$$x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \ldots + y^{n-1},$$

тогаш сме ја докажале лемата. Бидејќи $x - y \equiv 0 \pmod{p}$ или $x \equiv y \pmod{p}$, па следува

$$\begin{aligned} x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \ldots + y^{n-1} &\equiv x^{n-1} + x^{n-2}x + x^{n-3}x^2 + \ldots + xx^{n-2} + x^n \\ &\equiv nx^{n-1} \pmod{p} \end{aligned}$$

од каде добиваме дека изразот $x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \ldots + y^{n-1}$ не е делив со p, бидејќи $НЗД(n, p) = 1$ и p не е делител на x.

Лема 2. Нека x и y се цели броеви и n е непарен природен број. За произволен прост број p за кој $НЗД(n,p)=1$, $n \mid x+y$ и ниту x ниту y се деливи со p. Тогаш $v_p(x^n+y^n)=v_p(x+y)$.

Доказ. Доказот е сличен како во Лема 1. Од

$$x^n+y^n=(x+y)(x^{n-1}-x^{n-2}y+x^{n-3}y^2-...+y^{n-1})$$

и од $x\equiv -y \pmod p$ имаме

$$x^{n-1}-x^{n-2}y+x^{n-3}y^2-...+y^{n-1}\equiv x^{n-1}-x^{n-2}(-x)+x^{n-3}(-x)^2+...-(-x)x^{n-2}+x^{n-1}$$
$$\equiv nx^{n-1} \pmod p$$

што значи дека изразот $x^{n-1}-x^{n-2}y+x^{n-3}y^2-...+y^{n-1}$ не е делив со p.

Теорема 6. (прв облик на LTE) Нека x и y се цели броеви и $p\geq 3$ е прост таков што $p \mid x-y$ и ниту x ниту y се деливи со p. Тогаш

$$v_p(x^n+y^n)=v_p(x+y)+v_p(n)\ .$$

Доказ. Ќе користиме индукција по бројот на прости делители на n. Прво, нека го докажеме следново тврдење:

$$v_p(x^p-y^p)=v_p(x-y)+1.$$

За да го докажеме ова, ќе докажеме дека

$$p \parallel x^{p-1}+x^{p-2}y+...+xy^{p-2}+y^{p-1}\ .$$

Ќе докажеме дека $p \mid x^{p-1}+x^{p-2}y+...+xy^{p-2}+y^{p-1}$. Да забележиме дека

$$x^{p-1}+x^{p-2}y+...+xy^{p-2}+y^{p-1}\equiv px^{p-1}\equiv 0 \pmod p.$$

Нека сега $y=x+kp$, каде k е цел број. За цел број $1<t<p$ имаме

$$y^t x^{p-1-t}\equiv (x+kp)^t x^{p-1-t}\equiv x^{p-1-t}(x^t+t(kp)(x^{t-1})+\frac{t(t-1)}{2}(kp)^2(x^{t-2})+...)$$
$$\equiv x^{p-1-t}(x^t+t(kp)(x^{t-1}))\equiv x^{p-1}+tkpx^{p-2} \pmod{p^2}.$$

Ова значи дека

$$y^t x^{p-1-t}\equiv x^{p-1}+tkpx^{p-2} \pmod{p^2},\ t=2,3,4,...,p-1.$$

Од овде имаме,

$$x^{p-1}+x^{p-2}y+...+xy^{p-2}+y^{p-1}\equiv x^{p-1}+(x^{p-1}+kpx^{p-2})+(x^{p-1}+2kpx^{p-2})+$$
$$+...+(x^{p-1}+(p-1)kpx^{p-2})$$
$$\equiv px^{p-1}+(1+2+3+...+p-1)kpx^{p-2}$$
$$\equiv px^{p-1}+\frac{p(p-1)}{2}kpx^{p-2}\equiv px^{p-1}+\frac{p-1}{2}kp^2x^{p-1}$$
$$\equiv px^{p-1} \pmod{p^2}$$

Значи $v_p(x^p-y^p)=v_p(x-y)+1$ е точно. Сега го докажуваме

$$v_p(x^n + y^n) = v_p(x+y) + v_p(n) \ .$$

Со $\| x \|_p$ го означуваме најголемиот степен на простиот број p кој е делител на x, односно ако $\| x \|_p = \alpha$, тогаш $p^\alpha \mid x$, но $p^{\alpha+1}$ не е делител на x. Нека сега $n = p^\alpha b$, каде $H.З.Д(p,b) = 1$. Па,

$$\begin{aligned} \| x^n - y^n \|_p &= \| (x^{p^\alpha})^b - (y^{p^\alpha})^b \|_p = \| x^{p^\alpha} - y^{p^\alpha} \|_p = \| (x^{p^{\alpha-1}})^p - (y^{p^{\alpha-1}})^p \|_p \\ &= \| x^{p^{\alpha-1}} - y^{p^{\alpha-1}} \|_p + 1 = \| (x^{p^{\alpha-2}})^p - (y^{p^{\alpha-2}})^p \|_p + 1 \\ &= \| x^{p^{\alpha-2}} - y^{p^{\alpha-2}} \|_p + 2 = \ldots = \| (x^{p^1})^1 - (y^{p^1})^1 \|_p + \alpha - 1 \\ &= \| x - y \|_p + \alpha = \| x - y \|_p + \| n \|_p \end{aligned}$$

Овде беше користено дека ако $p \mid x - y$ тогаш $p \mid x^k - y^k$.

Теорема 7. (втор облик на LTE) Нека x и y се цели броеви и n е непарен природен број и p е прост број за кој $p \mid x + y$ и ниту x ниту y се деливи со p. Тогаш $v_p(x^n + y^n) = v_p(x+y) + v_p(n)$.

Доказ. Доказот на оваа теорема е сосема аналоген како на претходната теорема, па заради тоа ќе го оставиме за вежба на читателот.

Теорема 8. (LTE за $p = 2$) Нека x и y се два непарни цели броеви така што $4 \mid x - y$. Тогаш $v_2(x^n - y^n) = v_2(x-y) + v_2(n)$.

Доказ. Во Лема 1, докажавме дека за било кој прост број p, таков што $НЗД(p,n) = 1$, $p \mid x - y$ и ниту еден од x и y не делив со p имаме

$$v_p(x^n - y^n) = v_p(x-y) \ .$$

Доволно е да докажеме дека

$$v_2(x^{2^n} - y^{2^n}) = v_2(x-y) + n \ .$$

Разложувањето на множители ни дава

$$x^{2^n} - y^{2^n} = (x^{2^{n-1}} + y^{2^{n-1}})(x^{2^{n-2}} + y^{2^{n-2}}) \cdot \ldots \cdot (x^2 + y^2)(x-y) \ .$$

Сега, бидејќи $x \equiv y \equiv \pm 1 \pmod 4$ тогаш имаме $x^{2^k} \equiv y^{2^k} \equiv 1 \pmod 4$ за сите природни броеви k, па $x^{2^k} + y^{2^k} \equiv 2 \pmod 4$, $k = 1, 2, 3, \ldots$. Ова значи дека степенот на 2 во сите множители, освен во $x - y$ е 1. Со ова е докажана теоремата.

Теорема 9. Нека x и y се два непарни цели броеви и нека n е парен природен број. Тогаш

$$v_2(x^n - y^n) = v_2(x-y) + v_2(x+y) + v_2(n) - 1 \ .$$

Доказ. Знаеме дека квадрат на непарен природен број е од облик $4k+1$. Па, за непарни x и y имаме $4 \mid x^2 - y^2$. Сега, нека m е непарен цел број и нека k е природен број така што $n = m \cdot 2^k$. Па,

$$\begin{aligned} v_2(x^n - y^n) &= v_2(x^{m\cdot 2^k} - y^{m\cdot 2^k}) = v_2((x^2)^{2^k} - (y^2)^{2^k}) = \ldots \\ &= v_2(x^2 - y^2) + k - 1 \\ &= v_2(x-y) + v_2(x+y) + v_2(n) - 1. \end{aligned}$$

Задачи за вежбање

1. (Iran TST 2, 2008) Докажи дека единствениот природен број a за кој $4(a^n+1)$ е куб на некој број, за сите природни броеви n е 1.
2. (Ireland, 1996) Нека p е прост број и a и n се природни броеви. Докажи дека ако $2^p + 3^p = a^n$, тогаш $n = 1$.
3. (Russia, 1996) Најди ги сите природни броеви n за кој постојат природни броеви x, y и k така што $Н.З.Д(x,y) = 1, k > 1$ и $3^n = x^k + y^k$.
4. (Russia, 1996) Нека x, y, p, n, k се природни броеви така што n е непарен и p е прост непарен број. Докажи дека ако $x^n + y^n = p^k$, тогаш $n = p^s$, за некој $s \in \mathbb{N}$.
5. (Bulgaria, 1997) За некој природен број n, бројот $3^n - 2^n$ е степен на некој прост број. Докажи дека n е прост број.
6. (IMO Shortlist, 1991) Најди го најголемиот степен k на 1991 за кој 1991^k го дели бројот $1990^{1991^{1992}} + 1992^{1991^{1990}}$.
7. (Czech-Slovakia, 1996) Најди ги сите природни броеви x, y така што $p^x - y^p = 1$, каде p е прост број.
8. (Romania TST, 1993) Нека n е број кој не е полн квадрат. Докажи дека не постои природни броеви x и y така што $(x+y)^3 \mid x^n + y^n$.
9. (IMO, 2000) Дали постои природен број n, така што n има точно 2000 прости делители и $n \mid 2^n + 1$?
10. (China TST, 2009) Нека $a > b > 1$ се природни броеви и нека b е непарен број и нека n е природен број. Ако $b^n \mid a^n - 1$, тогаш $a^b > \frac{3^n}{n}$. Докажи!
11. (Romania TST, 2008) Нека p е прост број, $p \neq 3$ и a и b цели броеви така што $p \mid a+b$ и $p^2 \mid a^3 + b^3$. Докажи дека $p^2 \mid a+b$ или $p^3 \mid a^3 + b^3$.

12. (IMO, 1990) Најди ги сите цели броеви $n>1$ така што $\frac{2^n+1}{n^2}$ е цел број.
13. (IMO Shortlist, 2007) Најди ги сите сурјекции $f:\mathbb{N}\to\mathbb{N}$ така што за секои $m,n\in\mathbb{N}$ и секој прост број p, бројот $f(m+n)$ е делив со p ако и само ако $f(m)+f(n)$ е делив со p.
14. (Romania TST, 1994) Нека n е непарен природен број. Докажи дека $((n-1)^n+1)^2$ е делител на $n(n-1)^{(n-1)^n+1}+n$.
15. (Romania TST, 2009) Нека $a,n\geq 2$ се два цели броја со следново својство: постои цел број $k\geq 2$, така што n е делител на $(a-1)^k$. Докажи дека n го дели $a^{n-1}+a^{n-2}+...+a+1$.

Користена литература

1. E. Chen, Orders modulo a prime, Electronic edition, 2015.
2. E. Chen, Exponents in Number Theory, Winter math Camp., 2014.
3. S. Cuellar, J. A. Samper, A nice and tricky lemma (lifting the exponent), Mathematical Reflections 3, 2007.
4. A. Hossein, Lifting the Exponent, Electronic Edition, 2011.
5. Малчески, Р., Малческа, В. (2020). Математика 1 – алгебарски структури (трето издание), Армаганка, Скопје