Ристо Малчески, Скопје
Самоил Малчески, Скопје

РЕД НА БРОЈ ПО МОДУЛ И ПРИМИТИВНИ КОРЕНИ

1. ВОВЕД

Познатата мала теорема Ферма, која гласи: *Ако* p *е прост број и* $\mathrm{NZD}(a,p)=1$, *тогаш* $a^{p-1}\equiv 1 \pmod p$, е непосредна последица од теоремата на Ојлер, која гласи: *Ако* $\mathrm{NZD}(a,m)=1$, *тогаш* $a^{\ddot{}(m)}\equiv 1 \pmod m$.

Меѓутоа, обратното тврдење на теоремата на Ферма не важи. Така, на пример, $3^{90}\equiv 1 \pmod{91}$, но $91=7\cdot 13$ е сложен број. Од друга страна ако p е природен број и $0<p<a$ е таков што $a^{p-1}\not\equiv 1 \pmod p$, 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.

Претходно кажаното е непосредна причина за продлабочени разгледувања на конгруенцијата $a^k\equiv 1 \pmod n$, на кои ќе се осврнеме во оваа статија.

2. РЕД НА БРОЈ ПО МОДУЛ

Дефиниција 1. Нека n е природен број и a е цел број таков што $\mathrm{NZD}(a,n)=1$.

Ред на бројот a *по модул* n, го нарекуваме најмалиот природен број $¢=¢(a,n)$ таков што $a^{¢}\equiv 1 \pmod n$.

Пример 1. Имаме $¢(3,11)=5$, бидејќи $3^5\equiv 1 \pmod{11}$, а $3^i\not\equiv 1 \pmod{11}$, за $i\in\{1,2,3,4\}$. ■

Теорема 1. Нека n е природен број, $\mathrm{NZD}(a,n)=1$ и нека $¢=¢(a,n)$. Тогаш

а) $a^m\equiv 1 \pmod n$, $m\in\mathbb{N}$ ако и само ако $¢\mid m$

б) $¢ \mid \ddot{}(n)$

в) за природните броеви r и s важи $a^r\equiv a^s \pmod n$ ако и само ако $r\equiv s \pmod ¢$,

г) $a^i\not\equiv a^j \pmod ¢$ за $i,j\in\{1,2,...,¢\}$, $i\neq j$

д) ако m е природен број, тогаш редот на a^m по модул n е еднаков на $\frac{¢}{\mathrm{NZD}(¢,m)}$

ѓ) редот за a^m по модул n е $¢$ ако и само ако m и $¢$ се заемно прости броеви.

е) низата $1,a,a^2,a^3,...$ е периодична по модул n со минимален период $¢$.

Доказ. а) Ако $a^m \equiv 1(\mathrm{mod}\, n)$ за некој природен број m, тогаш од $m = ¢q + r$, $0 \le r < ¢$, добиваме $a^m = a^{¢q+r} = a^{¢q}a^r$, 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 $¢$, па затоа $r = 0$. Значи, $m = ¢q$, т.е. $¢ \mid m$.

Обратно, ако $m = ¢q$, тогаш

$$a^m \equiv a^{q¢} \equiv (a^{¢})^q \equiv 1(\mathrm{mod}\, n).$$

б) Според теоремата на Ојлер имаме $a^{¨(n)} \equiv 1(\mathrm{mod}\, n)$ па од тврдењето под а) следува $¢ \mid ¨(n)$.

в) Нека $r > s$. Бидејќи a и n се заемно прости броеви важи $a^r \equiv a^s \,(\mathrm{mod}\, n)$ ако и само ако $a^{r-s} \equiv 1(\mathrm{mod}\, n)$, па од а) следува $¢ \mid (r-s)$ т.е. $r \equiv s\,(\mathrm{mod}\, ¢)$.

г) Непосредно следува од тврдењето под в)

д) Нека $d = \mathrm{NZD}(¢, m)$. Тогаш $¢ = ud$ и $m = vd$, па затоа

$$(a^m)^{\frac{¢}{\mathrm{NZD}(¢,m)}} = (a^m)^{\frac{ud}{d}} = a^{mu} = a^{uvd} = a^{(ud)v} = a^{¢v} \equiv 1(\mathrm{mod}\, n)$$

Нека претпоставиме дека t е таков што $(a^m)^t \equiv 1(\mathrm{mod}\, n)$. Тогаш

$$a^{mt} \equiv 1(\mathrm{mod}\, n)$$

па од $¢ = ¢(a,n)$ и тврдењето под а) следува $¢ \mid mt$. Затоа, $ud \mid vdt$ и како u и v се заемно прости добиваме $u \mid t$. Бидејќи

$$¢ = ud, u = \frac{¢}{d} = \frac{¢}{\mathrm{NZD}(¢,m)}$$

го дели произволниот број t со својство $(a^m)^t \equiv 1(\mathrm{mod}\, n)$ од дефиницијата на ред по модул следува дека $\frac{¢}{\mathrm{NZD}(¢,m)}$ е ред за a^m по модул n.

ѓ) Непосредно следува од тврдењето под д).

е) Непосредно следува од в) и г). ■

Последица 1. Ако $p > 2$ е прост број и $a \in \mathbb{Z}$, тогаш за секој прост делител q на бројот $\frac{a^p - 1}{a-1} = a^{p-1} + a^{p-2} + \ldots + a + 1$ важи $p \mid q-1$ или $p = q$.

Доказ. Ако $q \mid a-1$, тогаш $q \mid a^{p-1} + \ldots + a + 1 \equiv 1 + \ldots + 1 + 1 = p\,(\mathrm{mod}\, q)$, па затоа $q = p$.

Од друга страна, ако $q \nmid a-1$, 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 $p \mid q-1$. ■

Теорема 2. Ако $\mathrm{NZD}(a,n) = \mathrm{NZD}(b,n) = 1$ и $¢(a,n)$ е заемно прост со $¢(b,n)$, тогаш

$$¢(ab,n) = ¢(a,n) \cdot ¢(b,n).$$

Доказ. Нека $¢(a,n) = R$ и $¢(b,n) = S$. Тогаш

$$(ab)^{RS} = a^{RS}b^{RS} = (a^R)^S (b^S)^R \equiv 1 \cdot 1 \equiv 1(\mathrm{mod}\, n)$$

Според теорема 1. а) имаме $¢(ab,n) \mid RS$. Бидејќи R и S се заемно прости, постојат цели броеви r и s за кои $¢(ab,n) = rs, rw = R$ и $sx = S$. Ќе докажеме дека $r = R$ и $s = S$. Од дефиницијата на r и s имаме

$$(ab)^{rs} = a^{rs}b^{rs} \equiv 1 (\mathrm{mod}\, n), \qquad (a^{rs}b^{rs})^{w} \equiv 1 (\mathrm{mod}\, n)$$
$$(a^{rw})^{s}(b^{rw})^{s} \equiv 1 (\mathrm{mod}\, n)$$

Меѓутоа, бидејќи $a^{rw} \equiv 1 (\mathrm{mod}\, n)$ и $rw = R$ имаме $b^{Rs} \equiv 1 (\mathrm{mod}\, n)$. Од теорема 1 а) имаме $S = ¢(b,n) \mid Rs$ и како $\mathrm{NZD}(R,S) = 1$ следува $S \mid s.$ Но, $s \mid S$, па затоа $S = s$. Аналогно се докажува дека $r = R$, па затоа

$$¢(ab,n) = RS = ¢(a,n) \cdot ¢(b,n). \blacksquare$$

Теорема 3 (Лукас). Ако n е природен број и ако постои цел број a таков што

$$a^{n-1} \equiv 1 (\mathrm{mod}\, n) \text{ и } a^{\frac{n-1}{p}} \not\equiv 1 (\mathrm{mod}\, n)$$

за секој прост делител p на $n-1$, тогаш n е прост број.

Доказ. Од $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ следува $\mathrm{NZD}(a,n) = 1$ и од теорема 1 а) имаме $¢(a,n) \mid (n-1)$. 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 $¢(a,n) \nmid \frac{n-1}{p}$. Навистина, ако $¢(a,n) \mid \frac{n-1}{p}$, тогаш $a^{\frac{n-1}{p}} \equiv 1 (\mathrm{mod}\, n)$, што е противречност. Меѓутоа, $¢(a,n) \mid (n-1)$ и $¢(a,n) \nmid \frac{n-1}{p}$, за секој p кој е делител на $n-1$ повлекува $¢(a,n) = n-1$. Според теорема 1 б) имаме $¨(n) = n-1$, што значи дека бројот n е прост. $\blacksquare$

Дефиниција 2. Нека p е прост број, $k \in \mathbb{N}$ и $m \in \mathbb{Z}$. Ќе велиме дека p^k *точно го дели* m ако $p^k \mid m$ и $p^{k+1} \nmid m$. Притоа ќе пишуваме $p^k \parallel m$.

Теорема 4. Нека $p > 2$ е прост број, $a \neq 1$ е цел број и $n \in \mathbb{N}$. Ако $p^k \parallel a-1$ и $p^l \parallel n$, тогаш $p^{k+l} \parallel a^n - 1$.

Доказ. Имаме $a = p^k B + 1$, за некој цел број B кој не е делив со p. Тогаш

$$a^n - 1 = (1 + p^k B)^n - 1 = np^k B + \binom{n}{2} p^{2k} B^2 + \binom{n}{3} p^{3k} B^3 + \ldots + p^{nk} B^n \ . \qquad (1)$$

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 додека првиот собирок е дели 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 $p^{t-1} \parallel N = \frac{n}{p}$, тогаш од индуктивната претпоставка применета на $A = a^p$ и N следува дека $p^{k+t} = p^{(k+1)+(t-1)} \parallel A^N - 1 = (a^p)^{\frac{n}{p}} - 1 = a^n - 1$. Конечно, од принципот на математичка индукција следува дека тврдењето важи за секој природен број l. $\blacksquare$

Пример 2. 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 4 следува дека $3^{n+1} \| (-2)^{3^n}-1 = -(2^{3^n}+1)$. ■

Последица 2. Ако $¢ = ¢(p,a)$ и $p^k \| a^{¢}-1$, тогаш $¢(p^{k+l},a) = p^l ¢$.

Доказ. Непосредно следува од теорема 4, применета на $a^{¢}$. ■

Последица 3. Нека $p>2$ е прост број, $p^k \| a-b$ и $p^l \| n$. Тогаш

$$p^{k+l} \| a^n - b^n .$$

Доказ. За секој $b \in \mathbb{Z}$, $p \nmid b$, постои цел број c таков што $bc \equiv 1 (\mathrm{mod}\, p^{k+l})$. Во теорема 4 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. ■

За $p=2$ теорема 4 не е точна. На пример, $2 \| 3-1$ и $2 \| 2$, меѓутоа $2^3 \mid 3^2 -1$. Но, за $p=2$ точна е следнава теорема.

Теорема 5. Нека $a \neq 1$ е непарен цел број и нека $2^k \| a^2 -1$. Тогаш за секој цел број $l \geq 0$ важи $2^{k+l} \mid a^n -1$ ако и само ако $2^{l+1} \mid n$.

Доказ. Постапете аналогно како во доказот на теорема 4. ■

3. ПРИМИТИВНИ КОРЕНИ

Во теорема 1 докажавме дека $¢(a,n) \mid ¨(n)$. Логично е да се запрашаме дали за даден природен број n може да се избере a таков што $¢(a,n) = ¨(n)$? Во врска со ова прашање ја имаме следнава дефиниција.

Дефиниција 3. Нека $n \in \mathbb{N}$ и $\mathrm{NZD}(a,n)=1$. Ако $¢(a,n) = ¨(n)$, тогаш ќе велиме дека a е *примитивен корен по модул* n .

Теорема 6. Ако a е примитивен корен од n, тогаш $\{a, a^2, ..., a^{¨(n)}\}$ е редуциран систем на остатоци по модул n .

Доказ. Според дефиниција 4 имаме $\mathrm{NZD}(a,n)=1$. Оттука следува дека $\mathrm{NZD}(a^i,n)=1$, за секој $1 \leq i \leq ¨(n)$. Понатаму, броевите a^i , $i \in \{1,2,...,¨(n)\}$ не се меѓусебно конгруентни по модул n (зошто?). Бидејќи имаме само $¨(n)$ природни броеви помали од n кои се заемно прости со n , заклучуваме дека елементите на множеството $\{a, a^2, ..., a^{¨(n)}\}$ мора да се конгруентни со нив. Според тоа, $\{a, a^2, ..., a^{¨(n)}\}$ е редуциран систем на остатоци по модул n . ■

Во натамошните разгледувања ќе ја користиме следната лема, која ќе ја прифатиме без доказ.

Лема 1. Нека p е прост број. Ако $n \mid p-1$, тогаш конгруентната равенка $x^n \equiv 1 (\mathrm{mod}\, p)$ има n решенија. □

Лема 2. Ако $n \in \mathbb{N}$, тогаш $\sum_{d|n} \ddot{\varphi}(d) = n$.

Доказ. Ќе докажеме дека за секој $d, d \mid n$, бројот на елементите $x \in \{1,2,...,n\}$ за кои $\mathrm{NZD}(x,n) = \frac{n}{d}$ е еднаков на $\ddot{\varphi}(d)$. Навистина, $\mathrm{NZD}(x,n) = \frac{n}{d}$ ако и само ако $x = \frac{n}{d} \cdot k$, $k \in \{1,2,...,d\}$ и $\mathrm{NZD}(k,d) = 1$, а вакви броеви k има точно $\ddot{\varphi}(d)$. Според тоа, збирот на сите $\ddot{\varphi}(d)$, кога $d \mid n$ е еднаков на бројот на сите елементи $x \in \{1,2,...,n\}$, па затоа $\sum_{d|n} \ddot{\varphi}(d) = n$. ■

Теорема 7. 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 $\ddot{\varphi}(d)$ елементи на множеството $\mathbb{Z}_p$ (остатоци по модул p) со ред по модул еднаков на d. Тврдењето е тривијално за $d = 1$. Нека претпоставиме дека тврдењето е точно за сите делители на бројот $p-1$ помали од d. Од лема 1 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 $\ddot{\varphi}(m)$ имаат ред m, каде m е произволен делител на d помал од d. Преостанатите $d - \sum_{d>m|d} \ddot{\varphi}(m)$ имаат ред d, а од лема 2 следува дека $d - \sum_{d>m|d} \ddot{\varphi}(m) = \ddot{\varphi}(d)$. ■

Последица 4. Постојат точно $\ddot{\varphi}(p-1)$ примитивни корени на p.

Доказ. Непосредно следува од теорема 7. ■

Последица 5. Нека p е прост број и $n \in \mathbb{N}$. Ако за секој a таков што $\mathrm{NZD}(a,p) = 1$ 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. ■

Теорема 8. 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 теорема 6 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 $\ddot{\varphi}(p^2) = p(p-1)$ 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

$$(u+p)^{p-1} - u^{p-1} \equiv (p-1)pu^{p-2} \not\equiv 0 (\mathrm{mod}\, p^2),$$

што е противречност.

Нека u е примитивен корен по p^2. Ќе докажеме дека u е примитивен корен по модул p^n. Бидејќи p точно го дели $u^{p-1} - 1$, од теорема 4 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 $\ddot{}(p^n)$, што значи дека u е примитивен корен по модул p^n.

Конечно, бидејќи $\ddot{}(2p^n) = \ddot{}(p^n)$, 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 $2p^n$. ■

На крајот од овој дел, без доказ ќе наведеме уште едно тврдење за примитивните корени по модул $n, n \in \mathbb{N}$.

Теорема 9. 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 $n \in \{2,4\}$. □

4. ДОПОЛНИТЕЛНИ РЕШЕНИ ЗАДАЧИ

Во претходните разгледувања се осврнавме на редот на број по даден модул и на примитивните корени по даден модул, при што теориските разгледувања ги илустриравме со неколку елементарни примери. На крајот од нашите разгледувања ќе разгледаме неколку задачи кои се задавани на различни математички натпревари и во чии решенија се користат претходно разгледаните поими и својства.

Задача 1. Докажи, дека ако $\mathrm{NZD}(a,n) = 1$ и $n = p_1^{a_1} p_2^{a_2} \ldots p_t^{a_t}$ 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 $p_i^{a_i}$, $i = 1,2,\ldots,t$. ■

Решение. Нека редот на a по модул $p_i^{a_i}$ е k_i, k е ред на a по модул n и $m = \mathrm{NZS}(k_1, k_2, \ldots, k_t)$. Тогаш, од конгруенцијата $a^k \equiv 1 (\mathrm{mod}\ n)$ следуваат конгруенциите

$$a^k \equiv 1 (\mathrm{mod}\ p_i^{a_i}),\ i = 1,2,\ldots,t,$$

па затоа $k_i \mid k$, за секој $i = 1,2,\ldots,t$, т.е. $m \le k$. Но, од друга страна од

$$a^{k_i} \equiv 1 (\mathrm{mod}\ p_i^{a_i}),\ i = 1,2,\ldots,t$$

следува

$$a^m \equiv 1 (\mathrm{mod}\ p_i^{a_i}),\ i = 1,2,\ldots,t,$$

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.

Задача 2. Нека $n, a > 1$ се природни броеви. Докажи, дека $n \mid \ddot{}(a^n - 1)$.

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 $n \mid \ddot{}(a^n - 1)$. ■

Задача 3. Нека $a, b \in \mathbb{N}$ и $d = \mathrm{NZD}(a,b)$. Докажи, дека ако n е произволен природен број и $\frac{b}{d}$ е непарен број, тогаш $\mathrm{NZD}(n^a + 1, n^b - 1) \le 2$.

Решение. Да ставиме $m=n^d$, $a=dx, b=dy$. 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 $\text{NZD}(m^x+1,m^y-1)=l$. Ако $l>1$ и k е ред на m по модул l (јасно $\text{NZD}(m,l)=1$), тогаш од конгруенцијата $m^y\equiv 1(\text{mod}\, l)$ следува дека $k\mid y$, па значи k е непарен број. Понатаму, од конгруенцијата $m^x\equiv -1(\text{mod}\ l)$ следува $m^{2x}\equiv 1(\text{mod}\, l)$, па значи $k\mid 2x$ и како k е непарен број добиваме дека $k\mid x$. Но, $\text{NZD}(x,y)=1$ и k е заеднички делител на x и y, па затоа $k=1$. Но, $k=1$ е ред на m по модул l и затоа $m\equiv 1(\text{mod}\, l)$, па затоа $m^x\equiv 1(\text{mod}\, l)$. Но, $m^x\equiv -1(\text{mod}\, l)$ па затоа $2\equiv 0(\text{mod}\, l)$, т.е. $l\le 2$. ■

Задача 4. Нека $a\in\mathbb{N}$ и p и q се непарни прости броеви такви да $a^p\equiv 1(\text{mod}\ q)$. Докажи, дека или q е делител на $a-1$ или $q=1+2np$.

Решение. Јасно, $\text{NZD}(a,q)=1$. Нека k е редот на a по модул q. Според теорема 3.4 а) имаме $k\mid p$ и како p е прост број, можни се два случаја:

1) $k=1$ и тогаш $a\equiv 1(\text{mod}\ q)$, т.е. $q\mid(a-1)$,
2) $k=p$ и тогаш $k\mid\ddot{}(q)=q-1$, т.е. $p\mid q-1$. Но, броевите p и q се непарни, па затоа $q-1$ се дели со $2p$, што значи $q=1+2np$. ■

Задача 5. Нека p и q се прости броеви и $2^p\equiv -1(\text{mod}\, q)$. Докажи, дека или $q=3$ или $q=1+2np$.

Решение. Ако $p=2$, тогаш $q=5$, т.е. q е од облик $1+2np$. Нека $p>2$. Јасно, $q\ne 2$. Ако $q=3$, $2^p\equiv(-1)^p=-1(\text{mod}\, 3)$ и условот е исполнет. Нека $q>3$. Тогаш од конгруенцијата $2^p\equiv -1(\text{mod}\ q)$ следува $2^{2p}\equiv 1(\text{mod}\ q)$. Но, редот k на 2 по модул q е делител на $2p$, па затоа можни се следниве случаи:

1) $k=1$ и тогаш $2\equiv 1(\text{mod}\ q)$, т.е. $q=1$, што е противречност.
2) $k=2$ и тогаш $2^2\equiv 1(\text{mod}\ q)$, т.е. $q=3$, што е противречност.
3) $k=p$ и тогаш $2^p\equiv 1(\text{mod}\, q)$, па заедно со $2^p\equiv -1(\text{mod}\, q)$ добиваме $q=2$, што е противречност.
4) $k=2p$ и како $k\mid\ddot{}(q)=q-1$, добиваме $2p\mid q-1$, што значи дека $q=1+2np$. ■

Задача 6. Докажи, дека ако $\text{NZD}(x,y)=1$, тогаш секој непарен прост делител на бројот $x^{2^n}+y^{2^n}$ е од облик $2^{n+1}m+1$.

Решение. Нека p е непарен прост делител на бројот $x^{2^n}+y^{2^n}$, каде $\text{NZD}(x,y)=1$. Јасно, $p\nmid y$, бидејќи во спротивно од $p\mid(x^{2^n}+y^{2^n})$ ќе следува $p\mid x$, што противречи на $\text{NZD}(x,y)=1$. Ставаме $z=xy^{p-2}$. Од конгруенцијата

$$x^{2^n} + y^{2^n} \equiv 0 (\mathrm{mod}\, p),$$

после множењето со $(y^{p-2})^{2^n}$ добиваме

$$z^{2^n} + (y^{p-1})^{2^n} \equiv 0 (\mathrm{mod}\, p) \ .$$

Од малата теорема на Ферма имаме $y^{p-1} \equiv 1 (\mathrm{mod}\, p)$, па затоа од последната конгруенција следува

$$z^{2^n} \equiv -1 (\mathrm{mod}\, p),$$

од каде наоѓаме

$$z^{2^{n+1}} \equiv 1 (\mathrm{mod}\, p)$$

Нека k е редот на бројот z по модул p. Тогаш $k \mid 2^{n+1}$, па затоа $k = 2^m$, $m \le n+1$ Но, ако $m \le n$, тогаш $z^{2^m} \equiv 1 (\mathrm{mod}\, p)$, од каде после степенување на 2^{n-m} добиваме $z^{2^n} \equiv 1 (\mathrm{mod}\, p)$, што противречи на $z^{2^n} \equiv -1 (\mathrm{mod}\, p)$, бидејќи $p \neq 2$. Значи, $m = n+1$ и $k = 2^{n+1}$. Конечно,

$$k = 2^{n+1} \mid \ddot{\varphi}(p) = p-1, \text{ т.е. } p = 2^{n+1}m + 1 . \blacksquare$$

Задача 7. Докажи, дека броевите 1, 2, ..., 100 можат да се распоредат во полињата на таблица 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

$$k \equiv 10^{10(2i+1)+(2j+1)} (\mathrm{mod} 101) . \blacksquare$$

ЛИТЕРАТУРА

1. Andreescu, T., Andrica, D. Number Theory – Structures, Examples and Problems, Birkhauser, 2009
2. Burton, D. M. Elementary Number Theory, Wm. C. Brown, Dubuque, Iowa, 1994
3. Niven, I., Zuckerman, H. S. An introduction to the Theory of Numbers, John Wiley & Sons, Inc., New Yor, 1980
4. Малчески, Р. (2004). Мултипликативни функции и теорема на Ојлер, Сигма, Скопје
5. Малчески, Р., Аневска, К. (2016). Мала теорема на Ферма, Нумерус, Скопје
6. Малчески, Р., Малческа, В. Математика 1 – алгебарски структури, ФОН универзитет, Скопје, 2011
7. Малчески, Р., Малчески, А., Аневска, К. Вовед во елементарна теорија на броеви, СММ, Скопје, 2015

Статијата прв пат е објавена во списанието СИГМА на Сојузот на математичарите на Македонија