Катерина Аневска, Скопје
Ристо Малчески, Скопје

КОНГРУЕНЦИ ВО МНОЖЕСТВОТО НА ЦЕЛИТЕ БРОЕВИ II

3. ПРИМЕНА НА КОНГРУЕНЦИИТЕ

Во оваа точка со помош на конгруенциите ќе најдеме неколку посебните признаци за деливост. За таа цел прво ќе разгледаме еден пример.

Пример 9. Нека $P = p_1^{2012} + p_2^{2012} + ... + p_{2011}^{2012}$, каде $p_1, p_2, ..., p_{2013}$ се првите 2011 прости броеви. Докажете дека $10 \mid P$.

Решение. Во низата прости броеви 2, 3, 5, 7, 11, 13, ...само бројот $p_1 = 2$ е парен, а останатите се непарни броеви. Понатаму,

$$p_1^{2012} \equiv 2^{2012} \equiv (2^4)^{503} \equiv 6^{503} \equiv 6 (\text{mod} 10) \text{ и } p_3^{2012} \equiv 5^{2012} \equiv 5 (\text{mod} 10).$$

Останатите прости броеви завршуваат на една од цифрите 1, 3, 7 или 9 и како

$1^4 \equiv 1 (\text{mod} 10)$, $3^4 \equiv 81 \equiv 1 (\text{mod} 10)$, $7^4 \equiv 2401 \equiv 1 (\text{mod} 10)$ и $9^4 \equiv 6561 \equiv 1 (\text{mod} 10)$,

добиваме дека за секој прост број $p \neq 2, 5$ важи

$$p^{2012} \equiv (p^4)^{512} \equiv 1^{512} \equiv 1 (\text{mod} 10).$$

Според тоа,

$$P = p_1^{2012} + p_2^{2012} + ... + p_{2011}^{2012} \equiv 6 + 5 + 2009 \cdot 1 \equiv 0 \left(\text{mod} 10\right)\text{)}, \text{ т.е. } 10 \mid P. \blacksquare$$

Теорема 6. Нека $f(x) = a_k x^k + a_{k-1} x^{k-1} + ... + a_1 x + a_0$, каде што $a_0, a_1, ..., a_{k-1}$, a_k, $a_k \neq 0$ се цели броеви. Ако $a \equiv b \, (\text{mod } m)$, тогаш

$$f(a) \equiv f(b) \, (\text{mod } m).$$

Доказ. Од последица 1 б) следува $a^t \equiv b^t \, (\text{mod } m)$ за $t = 0, 1, ..., k$. Сега од последица 1 а) следствено добиваме

$$a_t a^t \equiv a_t b^t \, (\text{mod } m) \text{ за } t = 0, 1, ..., k$$

$$a_k a^k + a_{k-1} a^{k-1} + ... + a_1 a + a_0 \equiv a_k b^k + a_{k-1} b^{k-1} + ... + a_1 b + a_0 \, (\text{mod } m)$$

односно $f(a) \equiv f(b) \, (\text{mod } m)$. $\blacksquare$

Ќе покажеме како претходната теорема може да се искористи за добивање на некои посебни признаци за деливост.

Последица 2. Секој природен број е конгруентен со збирот на своите цифри по модул 9.

Доказ. Нека n е природен број чиј декаден запис е

$$n = a_k 10^k + a_{k-1} 10^{k-1} + ... + a_1 10 + a_0,$$

каде што $a_0, a_1, ..., a_{k-1}, a_k \in \{0, 1, 2, ..., 9\}$. Ставаме

$$f(x)=a_kx^k+a_{k-1}x^{k-1}+\ldots+a_1x+a_0.$$

Тогаш, бидејќи $10\equiv 1 \pmod 9$ од теоремата 6 следува

$f(10)\equiv f(1) \pmod 9$, т.е. $n=a_k+a_{k-1}+\ldots+a_1+a_0 \pmod 9$. ■

Последица 3. Ако природниот број n има декаден запис

$$n=a_k10^k+a_{k-1}10^{k-1}+\ldots+a_110+a_0$$

тогаш

$$n\equiv(-1)^k a_k+(-1)^{k-1}a_{k-1}+\ldots+a_4-a_3+a_2-a_1+a_0 \pmod{11}.$$

Доказ. Нека n е природен број чиј декаден запис е

$$n=a_k10^k+a_{k-1}10^{k-1}+\ldots+a_110+a_0,$$

каде што $a_0,a_1,\ldots,a_{k-1},a_k\in\{0,1,2,\ldots,9\}$. Ставаме

$$f(x)=a_kx^k+a_{k-1}x^{k-1}+\ldots+a_1x+a_0.$$

Тогаш, бидејќи $10\equiv -1 \pmod{11}$, од теорема 6 следува

$$f(10)\equiv f(-1) \pmod{11},$$

т.е.

$$n\equiv(-1)^k a_k+(-1)^{k-1}a_{k-1}+\ldots+a_4-a_3+a_2-a_1+a_0 \pmod{11}.$$ ■

Последица 4. Ако природниот број n има декаден запис

$$n=a_k10^k+a_{k-1}10^{k-1}+\ldots+a_110+a_0,$$

тогаш n е делив со 7 ако и само ако збирот

$$\{(a_0+3a_1+2a_2)+(a_6+3a_7+2a_8)+\ldots\}-\{(a_3+3a_4+2a_5)+(a_9+3a_{10}+2a_{11})+\ldots\}$$

е делив со 7.

Доказ. Нека n е природен број чиј декаден запис е

$$n=a_k10^k+\ldots+a_610^6+a_510^5+a_410^4+a_310^3+a_210^2+a_110+a_0,$$

каде што $a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7,\ldots,a_{k-1},a_k\in\{0,1,2,\ldots,9\}$. Бидејќи

$$10^0\equiv 1 \pmod 7,\ 10^1\equiv 3 \pmod 7,\ 10^2\equiv 2 \pmod 7,$$

$$10^3\equiv 6\equiv(-1) \pmod 7,\ 10^4\equiv 4\equiv(-3) \pmod 7,$$

$$10^5\equiv 5\equiv(-2) \pmod 7,\ 10^6\equiv 1 \pmod 7 \text{ итн.}$$

следува дека

$$10^{6k}\equiv 1 \pmod 7,\ 10^{6k+1}\equiv 3 \pmod 7,\ 10^{6k+2}\equiv 2 \pmod 7,$$

$$10^{6k+3}\equiv(-1) \pmod 7,\ 10^{6k+4}\equiv(-3) \pmod 7,\ 10^{6k+5}\equiv(-2) \pmod 7.$$

Според тоа,

$$\begin{aligned} n&=a_k10^k+\ldots+a_610^6+a_510^5+a_410^4+a_310^3+a_210^2+a_110+a_0\\ &=a_0+10a_1+a_210^2+a_310^3+a_410^4+a_510^5+a_610^6+a_710^7+\ldots\\ &\equiv a_0+3a_1+2a_2+(-1)a_3+(-3)a_4+(-2)a_5+a_6+3a_7+2a_8+\ldots \pmod 7 \end{aligned}$$

што и требаше да се докаже. ■

Пример 10. Докажи дека ако бројот n е делив со 99, тогаш збирот на неговите цифри не е помал од 18.

Решение. Нека $99 \mid n$. Тогаш $9 \mid n$, па затоа и збирот на цифрите A на n е делив со 9. Бидејќи n е природен број, $A > 0$, па единствен број кој е делив со 9 и е помал од 18 е 9. Ако $A = 9$, тогаш од

$$n = a_k 10^k + a_{k-1} 10^{k-1} + ... + a_1 10 + a_0$$

следува $A = a_k + a_{k-1} + ... + a_1 + a_0$. Од друга страна, бидејќи $11 \mid n$ следува

$$11 \mid \{(-1)^k a_k + (-1)^{k-1} a_{k-1} + ... - a_1 + a_0\}$$

и бидејќи

$$-9 \le (-1)^k a_k + (-1)^{k-1} a_{k-1} + ... - a_1 + a_0 \le 9$$

добиваме дека

$$(-1)^k a_k + (-1)^{k-1} a_{k-1} + ... - a_1 + a_0 = 0,$$

т.е. $a_0 + a_2 + ... = a_1 + a_3 + ...$. Според тоа $9 = 2(a_0 + a_2 + ...)$, што е противречност. ■

4. КЛАСИ НА КОНГРУЕНЦИИ

Како што веќе кажавме, за цел број a и природен број m постојат цели броеви q и r, $0 \le r < m$ такви што

$$a = qm + r.$$

Од последното равенство следува дека $a = qm + r \equiv r \pmod m$, што значи дека секој цел број е конгруентен по модул m со барем еден од броевите $0, 1, ..., m-1$. Следната теорема покажува дека секој цел број е конгруентен по модул m точно со еден од броевите $0, 1, ..., m-1$.

Теорема 7. 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 $a \equiv r \pmod m$, $a \equiv s \pmod m$, за $0 \le r, s < m$. Тогаш, $s \equiv r \pmod m$, т.е. $m \mid (s - r)$ и бидејќи $-m < s - r < m$, добиваме дека $s - r = 0$, т.е. $s = r$, што и требаше да се докаже. ■

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, т.е.

$$C_m(r) = \{a \mid a \in \mathbf{Z}, a \equiv r (\mathrm{mod}\, m)\}.$$

Од претходната теорема непосредно следува точноста на следново тврдење.

Последица 5. а) Ако $m > 0$, $0 \le r, s < m-1$ и $r \ne s$, тогаш

$$C_m(r) \cap C_m(s) = \varnothing.$$

б) $C_m(0) \cup C_m(1) \cup ... \cup C_m(m-1) = \mathbf{Z}$. ■

Дефиниција 2. Множеството $C_m(r)$ го нарекуваме *класа на конгруенции* по модул m.

За множеството $\{a_0, a_1, ..., a_{m-1}\}$ ќе велиме дека е *комплетен систем на остатоци* по модул m ако $a_r \in C_m(r)$ за $r = 0, 1, ..., m-1$.

Теорема 8. Секое множество од m последователни цели броеви е комплетен систем на остатоци по модул m.

Доказ. Нека $\{a, a+1, a+2, ..., a+m-1\}$ е множество од m последователни цели броеви. Од теорема 8 следува дека $a \equiv r (\mathrm{mod}\, m)$ за некој $r \in \{0, 1, ..., m-1\}$, т.е. $a \in C_m(r)$. Тогаш, за секој $t \in \{0, 1, 2, ..., m-1\}$ важи

$$a + t \equiv r + t (\mathrm{mod}\, m),$$

од каде што следува дека за $t \in \{0, 1, ..., m-r-1\}$ важи $a + t \in C_m(r+t)$, а за $t \in \{m-r, ..., m-1\}$ важи $a + t \in C_m(r+t-m)$, бидејќи во овој случај имаме

$$a + t \equiv r + t \equiv r + t - m (\mathrm{mod}\, m),$$

а и во двата случаја важи $r + t \in \{0, 1, 2, ..., m-1\}$. Според тоа,

$$a \in C_m(r),\ a+1 \in C_m(r+1), ...,\ a+m-r-1 \in C_m(m-1),$$
$$a+m-r \in C_m(0),\ a+m-r+1 \in C_m(1),\ ...,\ a+m-1 \in C_m(r-1),$$

што значи дека $\{a, a+1, a+2, ..., a+m-1\}$ е комплетен систем на остатоци по модул m. ■

Најчесто користени комплетни системи на остатоци по модул m се:

$$\{0, 1, ..., m-1\} \text{ и } \{1, 2, ..., m\},$$

а кога m е непарен број, се користи и комплетниот истем на остатоци по модул m

$$\{-\tfrac{m-1}{2}, -\tfrac{m-1}{2}+1, ..., -1, 0, 1, ..., \tfrac{m-1}{2}\}.$$

Пример 11. Докажи дека за секој природен број n, бројот $n^3 + 5n$ е делив со 6.

Решение. Комплетен систем на остатоци по модул 6 е 0, 1, 2, 3, 4 и 5. Според тоа, доволно е да испитаме дали $n^3 + 5n$ е делив со 6 за $n = 0, 1, 2, 3, 4, 5$. При множење со модул 6 имаме

$$0^3 = 0,\quad 1^3 = 1,\quad 2^3 = 2,\quad 3^3 = 3,\quad 4^3 = 4,\quad 5^3 = 5.$$

Според тоа, $n^3 + 5n \equiv n + 5n \equiv 6n \equiv 0 \pmod 6$. ■

5. МАЛА ТЕОРЕМА НА ФЕРМА

На крајот од нашите разгледувања ќе се задржиме на таканаречената мала теорема на Ферма, која има широка примена во теоријата на броеви. За таа цел прво ќе ја докажеме следнава теорема.

Теорема 9. Ако p е прост број и $p \nmid a$, тогаш броевите $a, 2a, 3a, ..., (p-1)a$ имаат различни остатоци при делење со p.

Доказ. Ако постојат $k, m \in \{1, 2, ..., p-1\}$ такви што ka и ma имаат исти остатоци при делење со p, тогаш $(k-m)a \equiv ka - ma \equiv 0 (\mathrm{mod}\, p)$, што не е можно бидејќи p е прост број, но $p \nmid (k-m)$ и $p \nmid a$. ■

Теорема10. (мала теорема на Ферма). Ако p е прост број и $\mathrm{NZD}(a, p) = 1$, тогаш $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.

Доказ. Броевите $a, 2a, 3a, ..., (p-1)a$ не се делат со и имаат различни остатоци при делење со p, што значи дека во некој редослед овие остатоци се броевите $1, 2, ..., p-1$. Значи имаме конгруенции од видот $ka \equiv m (\mathrm{mod}\, p)$, $k, m = 1, 2, ..., p-1$. Од последица 1 а) следува $a \cdot 2a \cdot ... \cdot (p-1) \equiv 1 \cdot 2 \cdot ... \cdot (p-1) (\mathrm{mod}\, p)$, па како $NZD(1 \cdot 2 \cdot ... \cdot (p-1), p) = 1$ од теорема 4 б следува дека во последната конгруенција можеме да скратиме со $1 \cdot 2 \cdot ... \cdot (p-1)$ и добиваме $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$. ■

Последица 5. Ако p е прост број, тогаш за секој цел број a важи

$$a^p \equiv a (\mathrm{mod}\, p). \blacksquare$$

Пример 12. Ако p и q се различни прости броеви, тогаш

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

Докажи!

Решение. 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. $pq \mid (p^{q-1}q^{p-1} - p^{q-1} - q^{p-1} + 1)$. Бидејќи p и q се прости броеви имаме $pq \mid p^{q-1}q^{p-1}$. Конечно, од досега изнесеното следува дека $pq \mid (p^{q-1} + q^{p-1} - 1)$, т.е. $p^{q-1} + q^{p-1} \equiv 1 (\mathrm{mod}\, pq)$. ■

Пример 13. Ако $x \in \mathbf{N}$, тогаш $x^2 + 1$ има непарни прости делители само од видот $4k + 1$.

Доказ. Нека p е непарен прост број и $p \mid x^2 + 1$. Тогаш последователно имаме

$$x^2 + 1 \equiv 0 (\mathrm{mod}\ p), \qquad x^2 \equiv -1 (\mathrm{mod}\ p)$$

$$(x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} (\mathrm{mod}\ p), \qquad x^{p-1} \equiv (-1)^{\frac{p-1}{2}} (\mathrm{mod}\ p)$$

Од друга страна, од $p \mid x^2 + 1$ следува $\mathrm{NZD}(x, p) = \mathrm{NZD}(x^2, p) = 1$, па од малата теорема на Ферма добиваме $x^{p-1} \equiv 1 (\mathrm{mod}\, p)$. Конечно, од последните две

конгруенции следува $(-1)^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$, од каде добиваме дека бројот $\frac{p-1}{2}$ мора да е парен, т.е. $\frac{p-1}{2} = 2k$, односно $p = 4k+1$, што и требаше да се докаже. ■

На крајот од овој дел ви предлагаме самостојно да ги решите следниве задачи:

1. Докажи дека за секој природен број n, бројот $4^n + 15n - 1$ е делив со 9.
2. Докажи дека за секој природен број n, бројот $2^{2n+1}3^{2n-2} + 5^5 2^{n-1}$ е делив со 13.
3. Најди ги сите природни броеви n за кои бројот $7^n + 99$ е квадрат на природен број.
4. Ако $p > 5$ е прост број поголем од 5, докажете дека бројот кој е запишан со $(p-1)$ – единица е делив со p.
5. Ако $p > 3$ е прост број, докажете дека $1 + 2 + 2^2 + 2^3 + ... + 2^{p-1}$ е сложен број.
6. Докажи дека простиот број p е делител на бесконечно многу броеви од видот $2^n - n$.

Статијата прв пат е објавена во списанието НУМЕРУС на СММ