Ристо Малчески, Скопје
Катерина Аневска, Скопје

КОНГРУЕНЦИ ВО МНОЖЕСТВОТО НА ЦЕЛИТЕ БРОЕВИ I

1. ПОИМ ЗА КОНГРУЕНЦИЈА

Нека се $a,q\in\mathbf{Z}$, $b\in\mathbf{N}$, $b\neq 0$ се такви да $a=bq$. Тогаш за бројот a велиме дека е делив со бројот b и $b\,|\,a$. Ако, пак a не е делив со b, тогаш може да се докаже дека постојат единствени цели броеви q и r такви што

$$a=bq+r,\quad 0\le r<b\,.$$

Бројот r го нарекуваме *остаток* од делењето на бројот a со бројот b. Според тоа, при делење на произволем цел број a со бројот $b\in\mathbf{N}$ можни остатоци се $0,1,2,...,b-1$, па затоа целите броеви можеме да ги поделиме во *класи*, при што во секоја класа се содржат броевите кои при делење со бројот b даваат еднакви остатоци. Овие класи броеви, со еднакци остатоци прид елење со даден број b, се основата на нашите натамошни разгледувања.

Дефиниција 1. Нека $a,b\in\mathbf{Z}$ и $m\in\mathbf{N}$. Ако $m\,|\,(a-b)$, тогаш ќе велиме дека бројот a *е конгруентен* со бројот b по модул m и ќе пишуваме

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

Ако $m\nmid(a-b)$, тогаш ќе велиме дека бројот a *не е конгруентен* со бројот b по модул m и ќе пишуваме

$$a\not\equiv b\ (\text{mod}\ m)\,.$$

Пример 1. а) Да ги разгледаме броевите $a=75, b=89$ и $m=7$. Бидејќи $a-b=75-89=-14=-7\cdot 2$, од дефиниција 1 добиваме

$$78\equiv 85\ (\text{mod}\ 7)\,.$$

б) За броевите $a=121, b=95$ важи $a-b=121-95=26$ и бидејќи $3\nmid 26$ заклучуваме дека $123\not\equiv 97\ (\text{mod}\ 3)$. ■

Теорема 1. Нека $a,b\in\mathbf{Z}$ и $m\in\mathbf{N}$. Тогаш:

а) $a\equiv b\ (\text{mod}\ m)$ ако и само ако постои цел број k таков, што $a=b+km$.

б) $a\equiv b\ (\text{mod}\ m)$ ако и само ако при делење со m, броевите a и b имаат еднакви остатоци.

Доказ. а) Од дефиницијата 1 следува дека $a\equiv b\ (\text{mod}\ m)$ 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 $a = mp + r$, $b = mq + s$, $p, q, r, s \in \mathbf{Z}$ и $0 \leq r, s < m$. Тогаш $a \equiv b \pmod m$ ако и само ако $m \mid (a - b)$, што значи ако и само ако $m \mid [(mp + r) - (mq + s)]$. Според тоа, $a \equiv b \pmod m$ ако и само ако

$$m \mid [m(p - q) + (r - s)],$$

па затоа $a \equiv b \pmod m$ ако и само ако $m \mid (r - s)$. Но, $-m < r - s < m$, односно $a \equiv b \pmod m$ ако и само ако $r - s = 0$, т.е. ако и само ако $r = s$. ■

Пример 2. а) При делење на броевите 56, 57, 58, 59, 60, 61 и 62 со бројот 7 се добива количник 8 и остатоци 0, 1, 2, 3, 4, 5 и 6, соодветно. Од теоремата 1 б) следува дека

$$56 \equiv 0 \pmod 7;\ 57 \equiv 1 \pmod 7,\ 58 \equiv 2 \pmod 7,\ 59 \equiv 3 \pmod 7,$$
$$60 \equiv 4 \pmod 7;\ 61 \equiv 5 \pmod 7 \text{ и } 62 \equiv 6 \pmod 7.$$

б) Од теоремата 1 б) имаме дека $38 \equiv 26 \pmod{12}$. Навистина, при делењето на 37 и 25 со 12 се добива остаток 2. ■

2. ОСНОВНИ СВОЈСТВА НА КОНГРУЕНЦИИТЕ

Во следните теореми ќе докажеме неколку важни својства на конгруенциите. Притоа ќе сметаме дека бројот m е природен број.

Теорема 2. 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 $a \equiv c \pmod m$

Доказ. а) Од $a - a = 0$, за секој $a \in \mathbf{Z}$ следува $a \equiv a \pmod m$, за секој $a \in \mathbf{Z}$.

б) Ако $a \equiv b \pmod m$, тогаш $m \mid (a - b)$. Од $b - a = (-1)(a - b)$ следува $m \mid (b - a)$, па од дефиницијата 7 заклучуваме дека $b \equiv a \pmod m$.

в) Ако $a \equiv b \pmod m$ и $b \equiv c \pmod m$, тогаш $m \mid (a - b)$ и $m \mid (b - c)$. Според тоа, $m \mid [(a - b) + (b - c)] = a - c$, па затоа $a \equiv c \pmod m$. ■

Теорема 3. Ако $a \equiv b \pmod m$ и $c \equiv d \pmod m$, тогаш

$$a + c \equiv b + d \pmod m,\ a - c \equiv b - d \pmod m \text{ и } ac \equiv bd \pmod m.$$

Доказ. Нека $a \equiv b \pmod m$ и $c \equiv d \pmod m$. Од дефиницијата 7 имаме дека $m \mid (a - b)$ и $m \mid (c - d)$. Според тоа

$$m \mid (a - b) + (c - d) = (a + c) - (b + d),$$
$$m \mid (a - b) - (c - d) = (a - c) - (b - d),$$
$$m \mid [c(a - b) + b(c - d)] = ac - bd$$

што значи дека

$$a + c \equiv b + d \pmod m,\ a - c \equiv b - d \pmod m \text{ и } ac \equiv bd \pmod m. \ ■$$

Последица 1. а) Ако $a \equiv b \pmod{m}$, тогаш

$$a + c \equiv b + c \pmod{m},\ \ a - c \equiv b - c \pmod{m}\ \text{ и }\ ac \equiv bc \pmod{m},$$

за секој $c \in \mathbf{Z}$.

б) Ако $a \equiv b \pmod{m}$, тогаш $a^n \equiv b^n \pmod{m}$, за секој $n \in \mathbf{N}$.

Доказ. Непосредно следува од теоремите 1 и 2. ■

Пример 3. Колкав е остатокот од делењето на бројот

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13$$

со 7.

Решение. Имаме

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720 \equiv -1 \pmod{7}. \qquad (1)$$

Понатаму

$8 \equiv 1 \pmod{7}$, $9 \equiv 2 \pmod{7}$, $10 \equiv 3 \pmod{7}$, $11 \equiv 4 \pmod{7}$, $12 \equiv 5 \pmod{7}$ и $13 \equiv 6 \pmod{7}$,

па од теорема 3 следува

$$8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \pmod{7}. \qquad (2)$$

Конечно, од (1), (2) и последица 1 б) добиваме

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \equiv\sim (1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6)^2 \equiv (-1)^2 \equiv 1 \pmod{7}.\ ■$$

Пример 4. а) Докажи дека $10 \mid 3^{1988} - 1$.

б) Најди го остатокот од делењето на бројот 4^{56} со 9.

Решение. а) Од $3^4 = 81$ следува $3^4 \equiv 1 \pmod{10}$. Сега од последица б) добиваме

$$(3^4)^{497} \equiv 1^{497} \pmod{10},\ \text{т.е.}\ 3^{1998} \equiv 1 \pmod{10},$$

што значи $10 \mid 3^{1988} - 1$.

б) Ќе го побараме оној степен на бројот 4 кој е конгруентен со 1 по модул 9.

Имаме

$4 \equiv 4 \pmod{9}$,

$4^2 \equiv 7 \pmod{9}$, бидејќи $16 = 9 \cdot 1 + 7$,

$4^3 \equiv 1 \pmod{9}$, бидејќи $64 = 9 \cdot 7 + 1$.

Бидејќи $56 = 18 \cdot 3 + 2$, последната конгруенција ја степенуваме на 18 и добиваме $4^{54} \equiv 1 \pmod{9}$. Понатаму, ако ги помножиме конгруенциите

$$4^2 \equiv 7 \pmod{9}\ \text{ и }\ 4^{54} \equiv 1 \pmod{9}$$

добиваме $4^{54} \cdot 4^2 \equiv 1 \cdot 7 \pmod{9}$, т.е. $4^{56} \equiv 1 \pmod{9}$.

Значи, остатокот од делењето на бројот 4^{56} со 9 е 7. ■

Пример 5. Ако $n \in \mathbf{N}$, тогаш $n^2 \equiv 0$ или $1 \pmod 3$.

Решение. Нека $n \in \mathbf{N}$. Тогаш $n = 3k$, $n = 3k+1$ или $n = 3k+2$, па затоа

$$n^2 = 9k^2 \equiv 0 \pmod 3,$$
$$n^2 = 9k^2 + 6k + 1 \equiv 1 \pmod 3,$$
$$n^2 = 9k^2 + 12k + 4 \equiv 1 \pmod 3,$$

соодветно. Конечно, $n^2 \equiv 0$ или $1 \pmod 3$, за секој $n \in \mathbf{N}$. ■

Пример 6. Во множеството природни броеви реши ја равенката

$$x_1^4 + x_2^4 + \ldots + x_{10}^4 = 2011. \qquad (3)$$

Решение. Ако некој x_i е парен број, $x_i = 2k$, тогаш $x_i^4 = 16k^4 \equiv 0 \pmod{16}$. Ако x_i е непарен број, тогаш $x_i - 1$ и $x_i + 1$ се последователни парни броеви, што значи едниот е делив со 2, а другиот со 4 и бројот $x_i^2 + 1$ е парен, т.е. делив со 2, па затоа

$$x_i^4 - 1 = (x_i - 1)(x_i + 1)(x_i^2 + 1) \equiv 0 \pmod{16}$$

од каде следува дека $x_i^4 \equiv 1 \pmod{16}$. Според тоа,

$$x_1^4 + x_2^4 + \ldots + x_{10}^4 \equiv k \pmod{16},\ k \le 10.$$

Од друга страна, $2011 \equiv 11 \pmod{16}$, што значи дека десната страна на равенката (3) при делење со 16 дава остаток 11, а левата страна остаток кој е помал или еднаков на 10, што не е можно. Конечно, равенка (3) нема решение во множеството природни броеви. ■

Пример 7. Докажи дека за секои прости броеви p и q, $p, q > 3$, важи или

$$p \equiv q \pmod 6 \text{ или } p + q \equiv 0 \pmod 6.$$

Решение. Како што знаеме, секој прост број поголем од 3 е од видот $6k+1$ или $6t-1$. Ќе разгледаме три случаи:

а) ако $p = 6k+1$ и $q = 6t+1$, тогаш од теорема 1 б) следува дека $p \equiv q \pmod 6$,

б) ако $p = 6k-1$ и $q = 6t-1$, тогаш од теоремата 1 б) следува дека $p \equiv q \pmod 6$ и

в) ако $p = 6k+1$ и $q = 6t-1$, тогаш $p \equiv 1 \pmod 6$ и $q \equiv -1 \pmod 6$ и од теорема 3 следува дека

$$p + q \equiv 1 + (-1) \pmod 6, \text{ т.е. } p + q \equiv 0 \pmod 6. \ ■$$

Пример 8. Најди ги сите прости броеви p за кои $p^6 - 6p^2 + 1$ е квадрат на природен број.

Решение. Ако $p=3$, тогаш $p^6-6p^2+1=3^6-6\cdot 3^2+1=729-54+1=676=26^2$. Нека $p\neq 3$, тогаш $p\equiv \pm 1 (\mathrm{mod}\, 3)$, па затоа $p^2\equiv 1(\mathrm{mod}\, 3)$. Според тоа,

$$p^6-6p^2+1=(p^2)^3-6p^2+1\equiv 1^3-6\cdot 1+1\equiv -4\equiv 2(\mathrm{mod}\, 3). \qquad (4)$$

Но, според пример 5 имаме $n^2\equiv 0$ или $1\,(\mathrm{mod}\, 3)$, за секој $n\in\mathbf{N}$, па од (4) следува дека не постои прост број $p\neq 3$ таков што p^6-6p^2+1 е квадрат на природен број.

Конечно, единствено решение е $p=3$. ■

Да забележиме дека теорема 3 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 $8\equiv -4\,(\mathrm{mod}\, 12)$ броевите 8 и -4 се деливи со 2 и со 4, меѓутоа ако поделиме со 2, односно со 4 добиваме $4\equiv -2\,(\mathrm{mod}\, 12)$ односно $2\equiv -1\,(\mathrm{mod}\, 12)$, што не е точно. Во следната теорема ќе докажеме кога двете страни во една конгруенција може да се поделат со некој број.

Теорема 4. а) Ако НЗД$(a,m)=1$ и $ab\equiv ac\,(\mathrm{mod}\, m)$, тогаш $b\equiv c\,(\mathrm{mod}\, m)$.

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

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

Доказ. б) Нека НЗД$(a,m)=d$ и $ab\equiv ac\,(\mathrm{mod}\, m)$. Постојат цели броеви p и q такви, што $m=dq$ и $a=dp$ и важи НЗД$(p,q)=1$. Од $ab\equiv ac\,(\mathrm{mod}\, m)$ следува дека постои $k\in\mathbf{Z}$ 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, НЗД$(p,q)=1$, па затоа од последното равенство следува $q\,|\,(b-c)$, т.е. $b\equiv c\,(\mathrm{mod}\, q)$, каде што $q=\frac{m}{d}$.

а) Следува од тврдењето под б) за $d=1$.

в) Бидејќи НЗД$(a,m)=d$, добиваме $a=dp$ и $m=dq$, за некои цели броеви p и q. Понатаму, од $b\equiv c\,(\mathrm{mod}\, q)$ следува дека постои $k\in\mathbf{Z}$ 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 $ab-ac=m(pk)$. Според тоа, $m\,|\,(ab-ac)$, т.е. $ab\equiv ac\,(\mathrm{mod}\, m)$. ■

Теорема 5. Ако $a \equiv b \pmod{m}$ и $a \equiv b \pmod{n}$ и НЗС$(m,n) = k$, тогаш $a \equiv b \pmod{k}$.

Доказ. Нека НЗД$(m,n) = t$. Тогаш $n = pt$ и $m = qt$, каде што НЗД$(p,q) = 1$ и НЗС$(m,n) = pqt$. 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 НЗД$(p,q) = 1$ 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, НЗС$(m,n) = pqt = k$, па затоа $a \equiv b \pmod{k}$. ■

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

1. Ако $m \equiv 1 \pmod{2}$ или $m \equiv -1 \pmod{2}$, докажете дека $m^2 \equiv 1 \pmod{8}$.
2. Ако $a \in \mathbf{Z}$, докажете дека $a^2 \equiv 0 \pmod{2}$ или $a^2 \equiv 1 \pmod{2}$.
3. Докажи дека квадратот на секој цел број е конгруентен со 0 или 1 по модул 4.
4. Ако $a \in \mathbf{Z}$, докажете дека $a^2 \equiv 0 \pmod{8}$ или $a^2 \equiv 1 \pmod{8}$ или $a^2 \equiv 4 \pmod{8}$.
5. Ако a е цел број кој не е делив со 7, докажете дека

а) $a^3 \equiv 1 \pmod{7}$ или $a^3 \equiv -1 \pmod{7}$.

б) $a^4 \equiv 1 \pmod{7}$ или $a^4 \equiv 2 \pmod{7}$ или $a^4 \equiv 4 \pmod{7}$.

6. Ако a е цел број кој не е делив со 8, докажете дека $a^4 \equiv 0 \pmod{8}$ или $a^4 \equiv 1 \pmod{0}$.
7. Докажете дека збирот на квадратите на два цели броја е делив со 7 ако и само ако и двата броја се деливи со 7.
8. Докажете дека за секој природен број n бројот $n^3 - n$ е делив со 6.
9. Најди го остатокот од делењето на бројот 2^{200} со бројот 13.
10. На која цифра завршува бројот:

    а) 6^{811};   б) 2^{1000};   в) 3^{333}

11. Најди го остатокот при делењето на:

    а) $(5^{100} + 55)^{100}$ со 24;   б) $(17^{17} + 116)^{21}$ со 8.

(Продолжува во следниот број)

Su{tinata na matematikata e vo nejzinata sloboda.

G. Kantor

Vo glavata na Arhimed imalo pove}e fantazija otkolku vo Homerovata.

F. Volter