Даниел Велинов
Скопје

КИНЕСКА ТЕОРЕМА ЗА ОСТАТОЦИ

Сун Цу Суан- Чинг во четврти век го поставил следниот проблем: “Нека имаме предмети чиј број е непознат. Нивниот број поделен со 3 дава остаток 2; нивниот број поделен со 5 дава остаток 3; поделен со 7 дава остаток 2. Кој е бројот на предметите?” Решението е 23.

Ова е само еден пример каде може да се примени Кинеска теорема за остатоци (подолу ќе бидат дадени и други примери), која е дадена со следната теорема.

Теорема. Нека $m_1, m_2, \ldots, m_k$ се попарно заемно прости природни броеви. Нека $b_1, b_2, \ldots, b_k$ се произволни цели броеви. Тогаш системот

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_k \pmod{m_k} \end{aligned}$$

има единствено решение модул $m_1 m_2 \cdots m_k$.

Доказ. Нека $M = m_1 \cdots m_k$. За $j \in \{1, 2, \ldots, k\}$, дефинираме $M_j = \frac{M}{m_j}$. Ако i и j се од $\{1, 2, \ldots, k\}$ со $i \neq j$, тогаш $(m_i, m_j) = 1$. Следува дека за секој $j \in \{1, 2, \ldots, k\}$, $(M_j, m_j) = 1$, па постои елемент $M'_j \in \mathbb{Z}$ така да $M_j M'_j \equiv 1 \pmod{m_j}$. Нека $x = \sum_{j=1}^{k} b_j M_j M'_j$. Тогаш

$$x \equiv b_j M_j M'_j \equiv b_j \pmod{m_j} \text{ за } j \in \{1, 2, \ldots, k\}.$$

Со ова ние покажавме дека постои решение на системот од конгруенции даден во тврдењето на теоремата.

За да ја покажеме единственоста на решението, нека претпоставиме дека y исто така го исполнува системот од конгруенции $y \equiv b_j \pmod{m_j}$ за секој $j \in \{1, 2, \ldots, k\}$. Тогаш важи $y - x \equiv 0 \pmod{m_j}$ за секој j, па секој m_j го дели $y - x$. Имајќи во предвид дека m_j се попарно прости, заклучуваме дека $M \mid (y - x)$, што значи дека $y \equiv x \pmod{m_1 m_2 \cdots m_k}$.

Забелешка 1. Тврдењето на теоремата може да го преформулираме: Постојат $x_1, x_2, \ldots, x_k \in \mathbb{Z}$ такви што $m_1 x_1 + b_1 = m_2 x_2 + b_2 = \ldots = m_k x_k + b_k$, па горната теорема може да се докаже и со индукција по k.

Забелешка 2. Решението x во горната тоерема е дадено со

$$x \equiv b_1 M_1 y_1 + b_2 M_2 y_2 + \ldots + b_k M_k y_k \pmod{M},$$

каде $M = m_1 m_2 \cdots m_k$, $M_j = \frac{M}{m_j}$ и $y_j \equiv (M_j)^{-1} \pmod{m_j}$, за $j \in \{1, 2, \ldots, k\}$.

Пример 1. Во книгата "Brahma's Correct System" од Брахмагупта се споменува следниот проблем: Кошницата на стара жена, која одела на пазар, била згазната од коњ. Во кошницата имало јајца. Сопственикот на коњот се понудил да ги плати јајцата, кои биле во кошницата. Старата жена не се сеќавала точниот број на јајца, но се сетила дека кога ги редела во кошницата , земајќи по две јајца истовремено, останувало едно јајце. Истото се случувало кога таа земала три, четири, пет и шест истовремено, но кога земала по седум јајца истовремено, не останало ниту едно јајце. Кој е најмалиот број на јајца, кој можело да ги има во кошницата?

Решение. Нека x е бројот на скршени јајца. Тогаш тој мора да задоволува:

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 1 \pmod 3 \\ x &\equiv 1 \pmod 4 \\ x &\equiv 1 \pmod 5 \\ x &\equiv 1 \pmod 6 \\ x &\equiv 0 \pmod 7 \end{aligned}.$$

Од првата конгруенција јасно е дека x е непарен. За да може да ја искористиме Кинеската теорема за остатоци, ќе ја отфрлиме и конгруенцијата модул 6, па модулите на конгруенциите што остануваат $(3, 4, 5, 7)$ се попарно прости. Од Кинеската теорема за остатоци имаме дека постои единствено решение по модул $3 \cdot 4 \cdot 5 \cdot 7 = 420$ кое од Забелешка 2 може да го пресметаме:

$$\begin{aligned} M_3 &= \tfrac{420}{3} = 140 & y_3 &\equiv (140)^{-1} \pmod 3 = 2 \\ M_4 &= \tfrac{420}{4} = 105 & y_4 &\equiv (105)^{-1} \pmod 4 = 1 \\ M_5 &= \tfrac{420}{5} = 84 & y_5 &\equiv (84)^{-1} \pmod 5 = 4 \\ M_7 &= \tfrac{420}{7} = 60 & y_7 &\equiv (60)^{-1} \pmod 7 = 2, \end{aligned}$$

па

$$x \equiv 1 \cdot 140 \cdot 2 + 1 \cdot 105 \cdot 1 + 1 \cdot 84 \cdot 4 + 0 \cdot 60 \cdot 2 = 280 + 105 + 336 = 721 \equiv 301 \pmod{420}.$$

Бидејќи оваа вредност за x е непарна, и уште е задоволено $x \equiv 1 \pmod 6$, најмалиот број на скршени јајца е $x = 301$.

Пример 2. Најди го најмалиот број делив со 10, а при делење со 3 дава остаток 2 и при делење со 7 дава остаток 3.

Решение. Нека x е бараниот број. Тогаш ги имаме следниве конгруенции:

$$x \equiv 2 \pmod 3,\ x \equiv 3 \pmod 7,\ x \equiv 0 \pmod 2 \text{ и } x \equiv 0 \pmod 5.$$

Бидејќи $2,3,5,7$ се попарно прости, користејќи ја Кинеската теорема за остатоци имаме единствено решение по модул $2\cdot 3\cdot 5\cdot 7 = 210$. За да го најдеме, прво пресметуваме

$$M_2 = \frac{210}{2} = 105 \qquad y_2 \equiv (105)^{-1} \pmod 2 = 1$$

$$M_3 = \frac{210}{3} = 70 \qquad y_3 \equiv (70)^{-1} \pmod 3 = 1$$

$$M_5 = \frac{210}{5} = 42 \qquad y_5 \equiv (42)^{-1} \pmod 5 = 3$$

$$M_7 = \frac{210}{7} = 30 \qquad y_7 \equiv (30)^{-1} \pmod 7 = 4.$$

Оттука,

$$x \equiv 0M_2y_2 + 2M_3y_3 + 0M_5y_5 + 3M_7y_7 \equiv 500 \pmod{210} \equiv 80 \pmod{210}.$$

Па, бараниот број е 80.

Задачи за самостојна работа:

1. Реши ја равенката $17x \equiv 3 \pmod{210}$ користејќи ја Кинеската теорема за остатоци.
2. Најди го најмалиот природен број $n > 2$ така да 2 го дели n, 3 го дели $n+1$, 4 го дели $n+2$, 5 го дели $n+3$ и 6 го дели $n+4$. Докажи дека тоа е навистина најмалиот таков n.
3. Докажи дека постои позитивен цел број k за кој $2^n k+1$ е сложен за сите природни броеви n.
4. Најди го остатокот при делењето на бројот $12345678910111213 14...19781979$ со 1980.

Користена литература

1. E. Beklekamp, T. Rodgers, Math Puzzles, Springer-Verlag, New York, Inc., 1992.
2. A. Engel, Problem_solving Strategies, Springer-Verlag, New York, Inc., 1998.
3. G. Rockmaker, 101 Short cuts in math anyone can do, Frederick Fell Publishers, Inc., New York, 1965.
4. E. Lozansky, C. Rouseau, Winning solutions, Springer-Verlag, Inc., New York, 1996.
5. D. Wells, Prime numbers. The most mysterious figures in Math, John Wiley and Sons, Inc., Hoboken, New Jersey, 2005.