Poglavlje 2

Kongruencije

Neka su $a, b \in \mathbb{Z}$ i $m \in \mathbb{N}$. Kažemo da je a kongruentan b mod m i pišemo $a \equiv b \pmod{m}$ ako $m \mid a - b$. Nije teško provjeriti da je $\equiv$ relacija ekvivalencije, a vrijede i sljedeća svojstva:

- $a \equiv b \pmod{m},\ c \equiv d \pmod{m} \implies a \pm c \equiv b \pm d \pmod{m},\ ac \equiv bd \pmod{m}$
- $a \equiv b \pmod{m} \implies ac \equiv bc \pmod{mc}$
- $ac \equiv bc \pmod{m} \implies a \equiv b \pmod{\frac{m}{(m.c)}}$

Kineski teorem o ostacima

Teorem (**Kineski teorem o ostacima, CRT**): *Neka su $m_1, \ldots, m_r$ u parovima relativno prosti prirodni brojevi, te neka su $a_1, \ldots, a_r \in \mathbb{Z}$. Tada sustav kongruencija*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

ima jedinstveno rješenje mod $m_1 \ldots m_r$. To rješenje dano je formulom

$$x \equiv \sum_{i=1}^{r} a_i \cdot \frac{m_1 \ldots m_r}{m_i} \cdot \left(\frac{m_1 \ldots m_r}{m_i} \right)^{-1} \pmod{m_1 \ldots m_r}.$$

Ovdje je $\left(\frac{m_1 \ldots m_r}{m_i} \right)^{-1}$ multiplikativni inverz broja $\frac{m_1 \ldots m_r}{m_i}$ mod m_i, tj. vrijedi

$$\left(\frac{m_1 \ldots m_r}{m_i} \right)^{-1} \cdot \frac{m_1 \ldots m_r}{m_i} \equiv 1 \pmod{m_i}.$$

Takav broj postoji jer su brojevi $m_1, \ldots, m_r$ u parovima relativno prosti.

Zadatak 2.1. Odredite $13^{-1} \pmod{29}$.

Rješenje. Tražimo $x \in \mathbb{Z}$ takav da je $13x \equiv 1 \pmod{29}$. Drugim riječima. tražimo $x, y \in \mathbb{Z}$ takve da je $13x - 29y = 1$. Koristeći Euklidov algoritam možemo dobiti da je $x = 9, y = 4$. Stoga je $9 \equiv 13^{-1} \pmod{29}$.

Zadatak 2.2. Riješite sustav kongruencija

$$\begin{aligned} x &\equiv -2 \pmod{7} \\ x &\equiv -3 \pmod{11} \\ x &\equiv 3 \pmod{17} \end{aligned}$$

Rješenje. Po CRT-u znamo da je rješenje oblika

$$x \equiv (-2)\cdot(11\cdot 17)\cdot(11\cdot 17)^{-1} + (-3)\cdot(7\cdot 17)\cdot(7\cdot 17)^{-1} + 3\cdot(7\cdot 11)\cdot(7\cdot 11)^{-1} \pmod{7\cdot 11\cdot 17}.$$

U formuli imamo multiplikativne inverze pa prvo izračunajmo njih. Moduli su dovoljno mali da nam ne treba Euklidov algoritam za računanje inverza:

$$\begin{aligned} (11 \cdot 17)^{-1} \pmod 7 &= 187^{-1} \pmod 7 = 5^{-1} \pmod 7 = 3, \\ (7 \cdot 17)^{-1} \pmod{11} &= 119^{-1} \pmod{11} = 9^{-1} \pmod{11} = 5, \\ (7 \cdot 11)^{-1} \pmod{17} &= 77^{-1} \pmod{17} = 9^{-1} \pmod{17} = 2. \end{aligned}$$

Stoga je $x \equiv (-2) \cdot 187 \cdot 3 + (-3) \cdot 119 \cdot 5 + 3 \cdot 77 \cdot 2 = -2445 \equiv 173 \pmod{1309}$.

Zadatak 2.3. Riješite sustav kongruencija

$$\begin{aligned} x &\equiv 15 \pmod{28} \\ x &\equiv 9 \pmod{24} \\ x &\equiv 6 \pmod{15} \end{aligned}$$

Rješenje. Brojevi $28, 24, 15$ nisu u parovima relativno prosti. Njihovim rastavljanjem na proste potencije dobivamo sustav

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 1 \pmod 7 \end{aligned}$$

$$\begin{aligned} x &\equiv 1 \pmod 8 \\ x &\equiv 0 \pmod 3 \end{aligned}$$

$$\begin{aligned} x &\equiv 0 \pmod 3 \\ x &\equiv 1 \pmod 5 \end{aligned}$$

Kako ne može istovremeno biti $x \equiv 3 \pmod 4$ i $x \equiv 1 \pmod 8$. ovaj sustav nema rješenja.

Zadatak 2.4. Riješite sustav kongruencija

$$\begin{aligned} x &\equiv 1 \pmod{28} \\ x &\equiv -7 \pmod{24} \\ x &\equiv -4 \pmod{15} \end{aligned}$$

Rješenje. Brojevi $28, 24, 15$ nisu u parovima relativno prosti. Njihovim rastavljanjem na proste potencije dobivamo sustav

$$\begin{aligned} x &\equiv 1 \pmod 4 \\ x &\equiv 1 \pmod 7 \end{aligned}$$

$$\begin{aligned} x &\equiv 1 \pmod 8 \\ x &\equiv 2 \pmod 3 \end{aligned}$$

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 1 \pmod 5 \end{aligned}$$

Ovdje su ostaci kompatibilni. Stoga početni sustav postaje

$$\begin{aligned} x &\equiv 1 \pmod 8 \\ x &\equiv 1 \pmod 7 \\ x &\equiv 0 \pmod 3 \\ x &\equiv 1 \pmod 5 \end{aligned}$$

Njegovim rješavanjem dobivamo rješenje $x \equiv 281 \pmod{840}$.

Zadatak 2.5. Dokažite da postoji 100 uzastopnih prirodnih brojeva od kojih nijedan nije potencija prostog broja.

Rješenje. Neka su $p_1, q_1, p_2, q_2, \ldots, p_{100}, q_{100}$ međusobno različiti prosti brojevi. Po CRT-u postoji rješenje sustava kongruencija

$$\begin{aligned} n &\equiv 0 \pmod{p_1 q_1} \\ n &\equiv -1 \pmod{p_2 q_2} \\ &\ldots \\ n &\equiv -99 \pmod{p_{100} q_{100}}. \end{aligned}$$

Sada brojevi $n, n+1, \ldots, n+100$ nisu potencije prostog broja.

Zadatak 2.6. Dokažite da postoji 100 uzastopnih prirodnih brojeva od kojih nijedan nije kvadratno slobodan.

Rješenje. Neka su $p_1, p_2, \ldots, p_{100}$ međusobno različiti prosti brojevi. Po CRT-u postoji rješenje sustava kongruencija

$$\begin{aligned} n &\equiv 0 \pmod{p_1^2} \\ n &\equiv -1 \pmod{p_2^2} \\ &\ldots \\ n &\equiv -99 \pmod{p_{100}^2}. \end{aligned}$$

Sada brojevi $n, n+1, \ldots, n+100$ nisu kvadratno slobodni.

Zadatak 2.7. Dokažite da postoji beskonačno mnogo parnih $k \in \mathbb{N}$ takvih da je $p^2 + k$ složen za sve proste brojeve p.

Rješenje. Primijetimo da je $p^2 \equiv 1 \pmod 3$ za sve $p \neq 3$. Stoga, ako uzmemo $k \equiv 2 \pmod 3$, riješit ćemo sve $p \neq 3$. Još jedino broj $9 + k$ mora biti složen. Sustav kongruencija

$$\begin{aligned} k &\equiv 0 \pmod 2 \\ k &\equiv 2 \pmod 3 \\ k &\equiv -9 \pmod{35} \end{aligned}$$

ima beskonačno mnogo rješenja u $\mathbb{N}$ po CRT-u.

Zadatak 2.8 (Hrvatska matematička olimpijada 2014, IMO test *)**.** Neka je n neparan prirodni broj veći od 3. Označimo s k najmanji prirodni broj takav da je $kn + 1$ potpun kvadrat i l najmanji prirodni broj takav da je ln potpun kvadrat. Dokažite da je broj n prost ako i samo ako vrijedi $k > \frac{n}{4}$ i $l > \frac{n}{4}$.

Rješenje. Pretpostavimo da je n prost. Tada je očito $l = n$. Nadalje, ako je $kn + 1 = x^2$, tada je $x \equiv \pm 1 \pmod n$ pa je $x \geq n - 1$ i $k \geq n - 2 > \frac{n}{4}$.

Pretpostavimo sada da je $k, l > \frac{n}{4}$. Ako n nije kvadratno slobodan, tada postoji prost broj p takav da $p^2 \mid n$. Stoga je $n \cdot \frac{n}{p^2}$ potpun kvadrat i vrijedi $l \leq \frac{n}{p^2} \leq \frac{n}{4}$, kontradikcija. Dakle, n je kvadratno slobodan.

Neka je $kn + 1 = x^2$. Primijetimo da je $k > \frac{n}{4}$ ako i samo ako $x > \frac{n}{2}$. Međutim, sada je

$$(n - x)^2 = n^2 - 2nx + kn + 1 = (n - 2x + k)n + 1.$$

Kako je $n - x < \frac{n}{2}$, vrijedi da je $n - 2x + k < \frac{n}{4}$ pa smo dobili kontradiciju.