Diskretne strukture 1

11. čas: Aritmetika.

Prosti brojevi

Definicija. Broj $p \in \mathbb{N}$ je *prost* ako $p \neq 1$ i važi:

$$(\forall a, b \in \mathbb{N})(p \mid ab \rightarrow p \mid a \wedge p \mid b).$$

Lema. Neka $p, d \in \mathbb{N}$, p je prost i $d \mid p$, onda $d = 1$ ili $d = p$.

Teorema. Postoji beskonačno mnogo prostih brojeva.

Osnovna teorema aritmetike. Svaki broj $n > 1$ se na jedinstven način može zapisati kao proizvod prostih.

NZD i NZS

Definicija. Broj $d \in \mathbb{N}$ je NZD brojeva a i b, $d = (a, b)$, ako:

- $d \mid a$ i $d \mid b$;
- ako $e \mid a$ i $e \mid b$, onda i $e \mid d$.

Broj $s \in \mathbb{N}$ je NZS brojeva a i b, $d = [a, b]$, ako:

- $a \mid s$ i $b \mid s$;
- ako $a \mid t$ i $b \mid t$, onda i $s \mid t$.

Osobine. Neka $a, b \in \mathbb{N}$.

- $(a, b) = a$ akko $a \mid b$ akko $[a, b] = b$;
- $(a, 0) = a$ i $[a, 0] = 0$;
- $(1, b) = 1$ i $[1, b] = b$;
- $ab = (a, b)[a, b]$.

Bezuova lema

Tvrđenje. Ako $a = qb + r$, onda $(a, b) = (b, r)$.

Teorema. Neka $a, b \in \mathbb{N}$. Postoje $p, q \in \mathbb{Z}$ tako da $pa + qb = (a, b)$.

Dokaz. Euklidov algoritam...

Uzajamno prosti brojevi

Definicija. Brojevi m i n su *uzajamno prosti* ako $(m, n) = 1$.

Lema. Brojevi m i n su uzajamno prosti akko postoje $p, q \in \mathbb{Z}$ takvi da $pa + bq = 1$.

Tvrđenje.

- Ako $(m_1, n) = (m_2, n) = 1$, onda i $(m_1 m_2, n) = 1$;
- ako $(m_1, n) = (m_2, n) = \cdots = (m_k, n) = 1$, onda i $(m_1 m_2 \ldots m_k, n) = 1$;
- ako $(m_1, m_2) = 1$, $m_1 \mid s$ i $m_2 \mid s$, onda i $m_1 m_2 \mid s$;
- ako su $m_1, m_2, \ldots, m_k$ međusobno uzajamno prosti, $m_i \mid s$ za sve i, $1 \leqslant i \leqslant k$, onda i $m_1 m_2 \ldots m_k \mid s$.

Kongruencija modulo m

Definicija. a i b su jednaki modulo $m \geqslant 2$, $a \equiv_m b$, ako $m \mid a - b$.
Znamo da je $\equiv_m$ ekvivalencija na $\mathbb{Z}$ sa m klasa.

Tvrđenje. $\equiv_m$ je *kongruencija*, tj. ako $a \equiv_m a'$ i $b \equiv_m b'$, onda:

- $a + b \equiv_m a' + b'$;
- $ab \equiv_m a'b'$;
- $a^n \equiv_m a'^n$ za sve $n \geqslant 1$.

Inverz modulo m

Definicija. Broj b je *inverz* broja a modulo m ako je $ab \equiv_m 1$.

Tvrđenje. Broj a ima inverz modulo m akko $(a, m) = 1$.

Ako je b inverz od a modulo m, onda je b' inverz od a modulo m akko $b' \equiv_m b$.

Kineska teorema o ostacima

Teorema. Neka su $m_1, m_2, \ldots, m_k \geqslant 2$ međusobno uzajamno prosti brojevi i $a_1, a_2, \ldots, a_k \in \mathbb{Z}$. Sistem kongruencija:

$$\begin{aligned} x &\equiv_{m_1} a_1 \\ x &\equiv_{m_2} a_2 \\ &\vdots \\ x &\equiv_{m_k} a_k \end{aligned}$$

ima rešenje. Ako je x_0 jedno rešenje, onda je x rešenje datog sistema akko $x \equiv_M x_0$, gde je $M = m_1 m_2 \ldots m_k$.

Primer. Rešiti sistem kongruencija:

$$\begin{aligned} x &\equiv_3 2 \\ x &\equiv_4 1 \\ x &\equiv_{11} 7. \end{aligned}$$

Ojlerova funkcija

Definicija. Za $n \geqslant 1$, sa U_n označavamo skup:

$$U_n = \{i \mid 1 \leqslant i \leqslant n, \, (i, n) = 1\},$$

dakle skup brojeva manjih od n koji su uzajamno prosti sa n. Broj elemenata skupa U_n obeležavamo sa $\varphi(n)$:

$$\varphi(n) := |U_n|,$$

dakle $\varphi(n)$ je broj elemenata koji su manji od n i uzajamno prosti sa n. Funkciju φ zovemo *Ojlerova funkcija*.

Primer. Izračunati $\varphi(1)$, $\varphi(p)$ i $\varphi(p^n)$, gde je p prost i $n \geqslant 1$.

Teorema. Ako $(m, n) = 1$, onda je $\varphi(mn) = \varphi(m)\varphi(n)$.

Posledica. Generalna formula...

Teorema (Ojler). Neka su $n \geqslant 1$ i $a \in \mathbb{Z}$ takvi da $(n, a) = 1$. Tada:

$$a^{\varphi(n)} \equiv_n 1.$$

Posledica (Mala Fermaova teorema). Ako $p \nmid a$, gde je p prost broj, onda $a^{p-1} \equiv_p 1$.

Posledica. Neka su $n \geqslant 1$ i $a \in \mathbb{Z}$ takvi da $(n, a) = 1$, i neka su $m, k \in \mathbb{N}$ takvi da $m \equiv_{\varphi(n)} k$. Tada $a^m \equiv_n a^k$.

Primer. Odrediti dve poslednje cifre brojeva 3^{1234} i 2^{1234}.