Teorija brojeva

Filip Najman

3. predavanje

22.3.2021.

Digresija u algebrarske strukture

Grupa je skup G skupa s binarnom operacijom $+ : G \times G \to G$ takvom da je

1. $+$ asocijativno
2. postoji neutralni element $e \in G$ takav da je

$$e + x = x + e = x, \quad \forall x \in G$$

3. $\forall x \in G$ postoji $y \in G$ takav da je $x + y = y + x = e$.

Primjeri: $(\mathbb{Z}, +)$, svaki vektorski prostoj je s opercaijom zbrajanja grupa.

Klase ekivalencije ostataka modulo m možemo zbrajati na očiti način i tako definirana struktura će biti grupa.

Zadnji put smo radili:

Teorem

Neka su a i m prirodni, te b cijeli broj. Kongruencija $ax \equiv b \pmod{m}$ ima rješenja ako i samo ako $d = (a, m)$ dijeli b. Ako je ovaj uvjet zadovoljen, onda gornja kongruencija ima točno d rješenja modulo m.

Iz prethodnog Teorema slijedi da ako je p prost broj i a nije djeljiv s p, onda kongruencija $ax \equiv b \pmod{p}$ uvijek ima rješenje i to rješenje je jedinstveno.

Kako riješiti jednadžbu $ax \equiv b \pmod{m}$, gdje je $(a, m) = 1$.?
Budući da je $(a, m) = 1$, postoje brojevi $u, v \in \mathbb{Z}$ takvi da je $au + mv = 1$ i u, v se mogu naći pomoću Euklidovog algoritma.

Sada je $au \equiv 1 \pmod{m}$, pa je $a(ub) \equiv b \pmod{m}$, tj. $x \equiv ub \pmod{m}$ je rješenje.

Zadatak: Nađite rješenje od $13x \equiv 8 \pmod{17}$.

Teorem (Kineski teorem o ostatcima)

Neka su $m_1, m_2, \ldots, m_r$ u parovima relativno prosti prirodni brojevi, te neka su $a_1, a_2, \ldots, a_r$ cijeli brojevi. Tada sustav kongruencija

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \ldots, \quad x \equiv a_r \pmod{m_r} \tag{1}$$

ima rješenja. Ako je x_0 jedno rješenje, onda su sva rješenja od (1) dana sa $x \equiv x_0 \pmod{m_1 m_2 \cdots m_r}$.

Dokaz: Neka je $m = m_1 m_2 \cdots m_r$, te neka je $n_j = \frac{m}{m_j}$ za $j = 1, \ldots, r$.

Tada je $(m_j, n_j) = 1$, pa postoji cijeli broj x_j takav da je $n_j x_j \equiv a_j \pmod{m_j}$.

Promotrimo broj

$$x_0 = n_1 x_1 + \cdots + n_r x_r.$$

Za njega vrijedi: $x_0 \equiv 0 + \cdots + 0 + n_j x_j + 0 + \cdots + 0 \equiv a_j \pmod{m_j}$.

Prema tome, x_0 je rješenje od (1).

Ako su sada x, y dva rješenja od (1), onda je $x \equiv y \pmod{m_j}$ tj. m_j dijeli $x - y$, za $j = 1, \ldots, r$, pa jer su m_j u parovima relativno prosti, dobivamo da je $x \equiv y \pmod{m}$. □

Zadatak: Nađite rješenje od

$$x \equiv 3 \pmod{5}, \quad x \equiv 2 \pmod{3}, \quad x \equiv 11 \pmod{14}.$$

Definicija

Reducirani sustav ostataka modulo m je skup cijelih brojeva r_i sa svojstvom da je $(r_i, m) = 1$, $r_i \not\equiv r_j \pmod{m}$ za $i \neq j$, te da za svaki cijeli broj x takav da je $(x, m) = 1$ postoji r_i takav da je $x \equiv r_i \pmod{m}$.

Jedan reducirani sustav ostataka modulo m je skup svih brojeva $a \in \{1, 2, \dots, m\}$ takvih da je $(a, m) = 1$.

Jasno je da svi reducirani sustavi ostataka modulo m imaju isti broj elemenata. Taj broj označavamo s $\varphi(m)$, a funkciju φ zovemo Eulerova funkcija.

Drugim riječima, $\varphi(m)$ je broj brojeva u nizu $1, 2, \dots, m$ koji su relativno prosti sa m.

Zadatak: Reducirani sustav ostataka modulo m s operacijom "množenje modulo m" čini grupu.

Teorem

Neka je $\{r_1, \ldots, r_{\varphi(m)}\}$ *reducirani sustav ostataka modulo* m*, te neka je* $(a, m) = 1$*. Tada je* $\{ar_1, \ldots, ar_{\varphi(m)}\}$ *također reducirani sustav ostataka modulo* m*.*

Dokaz: Primjetimo da ako je $(r_i, m) = 1$ i $(a, m) = 1$, tada je $(ar_i, m) = 1$.

Također imamo da ako je $ar_i \equiv ar_j \pmod{m}$ tada je $r_i \equiv r_j \pmod{m}$.

Dakle $\{ar_1, \ldots, ar_{\varphi(m)}\}$ i $\{r_1, \ldots, r_{\varphi(m)}\}$ imaju isti broje elemenata i svi elementi u prvom skupu su relativno prosti s m.

$\square$

Ovo pak povlači da skup ostataka $\{0, 1, \ldots, p-1\}$ pri dijeljenju sa p, uz zbrajanje i množenje $\pmod{p}$, čini polje, što znači da je osim što je $\{0, 1, \ldots, p-1\}$ s operacijom zbrajanja modulo p grupa, da je $\{1, \ldots p-1\}$ s operacijom množenja modulo p također grupa.

To polje se obično označava sa $\mathbb{Z}/p\mathbb{Z}$ ili $\mathbb{F}_p$.

Teorem (Eulerov teorem)

Ako je $(a, m) = 1$, *onda je* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Dokaz: Neka je $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$ reducirani sustav ostataka modulo m.

Budući da je, po ranije dokazanom, $\{ar_1, ar_2, \ldots, ar_{\varphi(m)}\}$ također reducirani sustav ostataka modulo m, zaključujemo da je

$$\prod_{j=1}^{\varphi(m)} (ar_j) \equiv \prod_{i=1}^{\varphi(m)} r_i \pmod{m},$$

odnosno,

$$a^{\varphi(m)} \prod_{j=1}^{\varphi(m)} r_j \equiv \prod_{i=1}^{\varphi(m)} r_i \pmod{m}.$$

Kako je $(r_i, m) = 1$, možemo "dijeliti" s r_i, dobivamo $a^{\varphi(m)} \equiv 1 \pmod{m}$. $\square$

Teorem (Mali Fermatov teorem)

Neka je p prost broj. Ako $p \nmid a$, onda je $a^{p-1} \equiv 1 \pmod{p}$. Za svaki cijeli broj a vrijedi $a^p \equiv a \pmod{p}$.

Dokaz: Očito je $\varphi(p) = p - 1$, pa tvrdnja teorema slijedi iz prolog teorema. $\square$

Primjer

Odredite ostatak od 7^{6001} pri dijeljenju s 9.

Imamo da je $\phi(9) = 6$

$$7^{6001} = 7^{6000} \cdot 7 = (7^{\phi(9)})^{1000} \cdot 7 \equiv 1^{1000} \cdot 7 \equiv 7 \pmod{9}.$$

Zadatak

Odredite ostatak od $(11^5)^6$ *pri dijeljenju s 21.*

Zadatak

Odredite ostatak od (301^{50053}) *pri dijeljenju s 30.*

Zadatak

Odredite ostatak od 4037^{6002} *pri dijeljenju s 55. Uputa: upotrijebite kineski teorem o ostacima.*

Zadatak

Dokažite da ako je $(x, 6) = 1$ *da je tada* $x^2 \equiv 1 \pmod{24}$*.*

Definicija

Funkciju $\vartheta : \mathbb{N} \to \mathbb{C}$ *za koju vrijedi*
1) $\vartheta(1) = 1$,
2) $\vartheta(mn) = \vartheta(m)\vartheta(n)$ *za sve* m, n *takve da je* $(m, n) = 1$,
zovemo multiplikativna funkcija.

Teorem

Eulerova funkcija φ je multiplikativna.

Dokaz: Neka su m, n relativno prosti prirodni brojevi, te neka a i b prolaze skupom svih reduciranih ostataka modulo m, odnosno modulo n. Naš je cilj pokazati da tada $an + bm$ prolazi skupom svih reduciranih ostataka modulo mn.

Ako to pokažemo, dobit ćemo da je $\varphi(m)\varphi(n) = \varphi(mn)$.

Budući da je $(a, m) = 1$ i $(n, m) = 1$ imamo da $(an + bm, m) = (an, m) = 1$.

Analogno dokažemo da je $(an + bm, n) = 1$, pa je i $(an + bm, mn) = 1$.

Tvrdimo da su svaka dva broja gornjeg oblika su međusobno nekongruentni modulo mn.

Pretpostavimo da je $an + bm \equiv a'n + b'm \pmod{mn}$.

Slijedi da je $(a - a')n \equiv (b' - b)m \pmod{mn}$.

Odavde slijedi da $mn | (a - a')n - (b' - b)m$, pa i $m | (a - a')n - (b' - b)m$, pa zaključujemo da $m | (a - a')n$.

Pošto je $(m, n) = 1$, slijedi $m | (a - a')$, tj. $a \equiv a' \pmod{m}$.

Pošto smo pretpostavili da su a i a' iz reduciranog sustava ostataka, slijedi $a = a'$.

Potpuno analogno dobijemo $b = b'$.

Dakle za različite parove (a, b) gdje a iz RSOM m, b iz RSOM n, vrijednosti $an + bm$ su različiti elementi iz RSOM mn.

Dakle $\phi(m)\phi(n) \leq \phi(mn)$.

Ostaje pokazati da ako je $(c, mn) = 1$, onda je $c \equiv an + bm \pmod{mn}$ za neke a, b, takve da $(a, m) = 1$ i $(b, n) = 1$.

Budući je $(m, n) = 1$, postoje cijeli brojevi x, y takvi da je $mx + ny = 1$.

Imamo da je $(c, mn) = 1$, pa je $(c, m) = 1$. Također imamo $(y, m) = 1$, pa je $(cy, m) = 1$.

Analogno je $(cx, n) = 1$.

Sada brojevi a i b definirani sa $cx \equiv a \pmod{m}$, $cy \equiv b \pmod{n}$ zadovoljavaju

$$ma + nb \equiv m(cx) + n(cy) \equiv c(mx + ny) \equiv c \pmod{mn}$$

imaju tražena svojstva.

Dakle $\phi(m)\phi(n) \geq \phi(mn)$, pa uz prethodno dokazano imamo da je.

Dakle $\phi(m)\phi(n) = \phi(mn)$.

Teorem

Za svaki prirodan broj $n > 1$ vrijedi $\varphi(n) = n\prod_{p|n}(1-\frac{1}{p})$.

Neka je $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$.

Jedini brojevi u nizu $1, 2, \ldots, p_i^{\alpha_i}$ koji nisu relativno prosti s $p_i^{\alpha_i}$ su brojevi $p_i, 2p_i, \ldots, p_i^{\alpha_i-1}\cdot p_i$.

Stoga je $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i-1} = p_i^{\alpha_i}(1-\frac{1}{p_i})$.

Zbog multiplikativnosti od φ, imamo

$$\begin{aligned}
\varphi(n) &= \varphi(\prod_{i=1}^{k} p_i^{\alpha_i}) = \prod_{i=1}^{k}\varphi(p_i^{\alpha_i}) = \prod_{i=1}^{k} p_i^{\alpha_i}\left(1-\frac{1}{p_i}\right) \\
&= n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) = n\prod_{p|n}\left(1-\frac{1}{p}\right).
\end{aligned}$$

$\square$