Predavanje 6

LINEARNE KONGRUENCIJE, KINESKA TEOREMA O OSTACIMA

Neka je $f(x)$ polinomska funkcija sa celim koeficijentima, $f(x) \in \mathbb{Z}[x]$, i neka je $m \in \mathbb{Z}^+$. Tada izraz

$$f(x) \equiv 0 \pmod{m} \tag{6.1}$$

zovemo *(polinomska) kongruencijska jednačina.* Njeno rešenje je svaki broj $s \in \mathbb{Z}$ koji (uvršten umesto x) zadovoljava gornji uslov. Međutim, primetimo sledeće: ako je s rešenje jednačine (6.1) i $t \equiv s \pmod{m}$, tada je i t rešenje. Prema tome, skup rešenja jednačine (6.1) je unija klasa ostataka po modulu m, pa tako možemo reći, malo slobodnije govoreći, da su rešenja te jednačine pojedine klase ostataka. U skladu sa tim, rećićemo da je *broj rešenja* jednačine (6.1) ukupan broj klasa ostataka po modulu m koje čine skup rešenja te jednačine. Ekvivalentno, u pitanju je broj elemenata maksimalnog skupa celih brojeva koji se sastoji od međusobno nekongruentnih rešenja za (6.1).

Ključna pitanja koja se postavljaju u vezi kongruencijskih jednačina jesu sledeća: Koji su potrebni i dovoljni uslovi da bi (6.1) bila rešiva? Koliki je broj rešenja (u gornjem smislu)? Na koji način se ta rešenja mogu odrediti?

Ako je $f(x)$ linearna funkcija (sa celim koeficijentima), tada jednačinu (6.1) zovemo *linearna kongruencijska jednačina*, ili samo *linearna kongruencija.* Linearnu kongruenciju je zgodno pisati u obliku

$$ax \equiv b \pmod{m}, \tag{6.2}$$

gde je $a, b \in \mathbb{Z}$. Sledeće tvrđenje daje kriterijum rešivosti jednačine (6.2).

Tvrđenje 6.1. *Jednačina* (6.2) *ima rešenja ako i samo ako* $(a, m) \mid b$.

Dokaz. Neka je $s \in \mathbb{Z}$ tako da je $as \equiv b \pmod{m}$. Tada postoji $c \in \mathbb{Z}$ tako da je $as - b = mc$, odnosno $as + m(-c) = as - mc = b$. Prema tome, diofantska jednačina $ax + my = b$ ima rešenja, što je po Tvrđenju 2.4 ekvivalentno uslovu $(a, m) \mid b$. Obratno, ako važi ovaj uslov, tada i jednačina $ax+my = b$ ima rešenje (x_0, y_0). Ali, tada je $ax_0 \equiv b \pmod{m}$, pa posmatrana linearna kongruencija ima rešenje. □

Pitanje broja i oblika svih rešenja za (6.2) raspravljeno je u narednom tvrđenju.

Teorema 6.2. *Pretpostavimo da jednačina* (6.2) *ima rešenja, i neka je* $s \in \mathbb{Z}$ *jedno njeno rešenje. Tada su elementi niza*

$$s, \quad s + \frac{m}{(a,m)}, \quad \ldots, \quad s + ((a,m)-1)\frac{m}{(a,m)}$$

međusobno nekongruentna rešenja jednačine (6.2)*, i pri tome je svako njeno rešenje kongruentno nekom od navedenih. Prema tome, broj rešenja* (6.2) *jednak je* (a, m).

Dokaz. Po datim uslovima, $as \equiv b \pmod m$. Neka je sada t bilo koje rešenje jednačine (6.2); tada je $at \equiv b \pmod m$. Otuda je $at \equiv as \pmod m$, pa po Tvrđenju 4.3 sledi

$$t \equiv s \pmod{\frac{m}{(a,m)}}.$$

Drugim rečima,

$$t = s + k\frac{m}{(a,m)}$$

za neko $k \in \mathbb{Z}$. Lako se proverava da se zapravo za svako $k \in \mathbb{Z}$ dobija po jedno rešenje za (6.2), tako da navedena ("dvostrano" beskonačna) aritmetička progresija predstavlja traženi skup rešenja.

Preostaje da se utvrdi koja su od ovih rešenja međusobno nekongruentna po modulu m. Zaista, ako je

$$t_1 = s + k_1\frac{m}{(a,m)}, \quad t_2 = s + k_2\frac{m}{(a,m)},$$

tada je $t_1 \equiv t_2 \pmod m$ ako i samo ako je $k_1 m' \equiv k_2 m' \pmod m$ (gde je $m' = m/(a,m)$), a što je dalje ekvivalentno sa $k_1 \equiv k_2 \pmod{(a,m)}$ (ponovo po Tvrđenju 4.3). Prema tome, dobićemo maksimalni skup nekongruentnih rešenja ako i samo ako pustimo k da uzima vrednosti u nekom potpunom sistemu ostataka po modulu (a,m). U formulaciji teoreme figuriše upravo standardni potpuni sistem ostataka po modulu (a,m), pa je dokaz time okončan. □

Posledica 6.3. *Ako je* $(a,m) = 1$*, tada kongruencija* (6.2) *ima jedinstveno rešenje za svako* $b \in \mathbb{Z}$*.*

Naravno, preostaje pitanje kako odrediti to jedno partikularno rešenje s iz Teoreme 6.2 (odnosno, jedinstveno rešenje u slučaju $(a,m) = 1$). Navešćemo tri pristupa.

1. *Pretraživanje grubom silom.* Ovaj metod je pogodan za "ručnu" primenu samo u slučaju malih modula. Na primer, kongruencija $23x \equiv 11 \pmod 5$ se može pojednostaviti do $3x \equiv 1 \pmod 5$, kada nije teško neposredno utvrditi da je sa $x \equiv 2 \pmod 5$ dato jedinsveno rešenje posmatrane kongruencije.
2. *Diofantske jednačine.* Ranije smo već videli da je $ax \equiv b \pmod m$ ekvivalentno linearnoj diofantskoj jednačini $ax + my = b$ u smislu da za svako x koje rešava linearnu kongruenciju postoji $y \in \mathbb{Z}$ tako da je (x,y) rešenje odgovarajuće diofantske jednačine; obratno, prva komponenta svakog rešenja (x,y) potonje jednačine rešava i linearnu kongruenciju. U načelu, (celobrojna) rešenja jednačine $ax + my = b$ (gde $(a,m) \mid b$) dobijaju se na osnovu Euklidovog algoritma za izračunavanje (a,m). O ovom će još biti reči kasnije.
3. *Ojlerova teorema.* U načelu, traženje partikularnog rešenja kongruencije $ax \equiv b \pmod m$ može se svesti na slučaj kada je $(a,m) = 1$; u suprotnom, ako je $a = (a,m)a_1$, $b = (a,m)b_1$ i $m = (a,m)m_1$, tada je po Tvrđenju 4.3 svako rešenje jednačine $a_1 x \equiv b_1 \pmod{m_1}$ ujedno i rešenje za polaznu kongruenciju. Primetimo da je tada $(a_1, m_1) = 1$; zbog toga je, po

Ojlerovoj teoremi $a_1^{\varphi(m_1)} \equiv 1 \pmod{m_1}$, pa $s = a_1^{\varphi(m_1)-1} b_1$ predstavlja jedno traženo rešenje, s obzirom na

$$a_1 \cdot a_1^{\varphi(m_1)-1} b_1 = a_1^{\varphi(m_1)} b_1 \equiv b_1 \pmod{m_1}.$$

Posmatrajmo sada *sistem* kongruencijskih jednačina

$$f_1(x) \equiv 0 \pmod{m_1}, \quad f_2(x) \equiv 0 \pmod{m_2}, \quad \ldots, \quad f_k(x) \equiv 0 \pmod{m_k}, \tag{6.3}$$

gde je $f_1(x), f_2(x), \ldots, f_k(x) \in \mathbb{Z}[x]$. Kako bi ovaj sistem uopšte imao rešenja, potrebno je da svaka od navedenih jednačina ponaosob bude rešiva. Kao što smo ranije raspravili, rešenje jednačine $f_i(x) \equiv 0 \pmod{m_i}$ dobićemo u obliku $x \equiv c_i \pmod{m_i}$ (pri čemu u opštem slučaju u obzir dolazi nekoliko različitih vrednosti c_i). Zbog toga, posebnu ulogu u rešavanju opštih sistema polinomnih kongruencijskih jednačina igraju sistemi *linearnih* kongruencija oblika

$$x \equiv c_1 \pmod{m_1}, \quad x \equiv c_2 \pmod{m_2}, \quad \ldots, \quad x \equiv c_k \pmod{m_k}. \tag{6.4}$$

Najpre ćemo razmotriti slučaj $k = 2$, kada se sistem sastoji od dve jednačine.

Tvrđenje 6.4. *Sistem linearnih kongruencija*

$$x \equiv c_1 \pmod{m_1}, \quad x \equiv c_2 \pmod{m_2}$$

ima rešenje ako i samo ako $(m_1, m_2) \mid c_1 - c_2$. *U tom slučaju, skup svih rešenja gornjeg sistema čini jednu klasu ostatka po modulu* $[m_1, m_2]$. *Drugim rečima, ako je* $s \in \mathbb{Z}$ *jedno rešenje gornjeg sistema, tada je sa*

$$t = s + k[m_1, m_2], \quad k \in \mathbb{Z},$$

dat skup svih rešenja tog sistema.

Dokaz. Dati sistem linearnih kongruencija ima rešenje (po x) ako i samo ako sistem linearnih diofantskih jednačina

$$x = c_1 + m_1 y, \quad x = c_2 + m_2 z$$

ima celobrojno rešenje (x, y, z). Međutim, egzistencija rešenja gornjeg sistema ekvivalentna je egzistenciji rešenja jednačine $c_1 + m_1 y = c_2 + m_2 z$, odnosno

$$m_2 z - m_1 y = c_1 - c_2.$$

Međutim, po Tvrđenju 2.4, gornja diofantska jednačina je rešiva ako i samo ako $(m_2, -m_1) = (m_1, m_2) \mid c_1 - c_2$, što se i tražilo.

Neka je sada $s \in \mathbb{Z}$ jedno (fiksirano) rešenje datog sistema; uočimo proizvoljno rešenje t. U tom slučaju je $t \equiv s \pmod{m_1}$ i $t \equiv s \pmod{m_2}$, tj. $t - s$ je deljivo sa m_1 i m_2. Po definiciji najmanjeg zajedničkog sadržaoca, poslednji uslov je ekvivalentan sa $[m_1, m_2] \mid t - s$. Dakle, $t = s + k[m_1, m_2]$ za neko $k \in \mathbb{Z}$; s druge strane, lako se verifikuje da se za svako $k \in \mathbb{Z}$ dobija rešenje datog sistema, pa tvrđenje sledi. □

Posledica 6.5. *Ako je* $(m_1, m_2) = 1$*, tada sistem*

$$x \equiv c_1 \pmod{m_1}, \quad x \equiv c_2 \pmod{m_2}$$

ima rešenje za svako $c_1, c_2 \in \mathbb{Z}$*, i pri tome skup svih rešenja čini jednu klasu ostatka po modulu* $m_1 m_2$*.*

Prethodna posledica predstavlja zapravo samo jedan specijalni slučaj opštijeg poznatog rezultata u vezi sa linearnim sistemima kongruencija tipa (6.4). U pitanju je *kineska teorema o ostacima*, verovatno najstarija zapisana matematička teorema, koja u potpunosti daje odgovor na pitanje o rešivosti sistema (6.4) kada su moduli u tom sistemu po parovima uzajamno prosti.

Teorema 6.6 (Kineska teorema o ostacima)**.** *Neka su* $m_1, m_2 \ldots, m_k$ *po parovima uzajamno prosti pozitivni celi brojevi. Tada sistem linearnih kongruencija*

$$x \equiv c_1 \pmod{m_1}, \quad x \equiv c_2 \pmod{m_2}, \quad \ldots, \quad x \equiv c_k \pmod{m_k}$$

ima rešenje za sve $c_1, c_2, \ldots, c_k \in \mathbb{Z}$*, i pri tome skup svih rešenja čini jednu klasu ostatka po modulu* $m_1 m_2 \cdots m_k$*.*

Prvi dokaz. Dokaz izvodimo indukcijom po k, broju jednačina koje čine sistem. Za $k = 2$ imamo prethodnu posledicu; zato pretpostavimo da je $k > 2$ i da svaki sistem tipa (6.4) koji se sastoji od $k - 1$ jednačine ima rešenje, pri čemu skup svih rešenja čini jednu klasu ostatka po modulu proizvoda datih modula. Zbog toga je sistem

$$x \equiv c_1 \pmod{m_1}, \quad x \equiv c_2 \pmod{m_2}, \quad \ldots, \quad x \equiv c_{k-1} \pmod{m_{k-1}}$$

ekvivalentan uslovu $x \equiv c \pmod{m_1 m_2 \cdots m_{k-1}}$ za pogodno odabrano $c \in \mathbb{Z}$. Prema tome, posmatrani sistem ekvivalentan je sistemu koji se sastoji od samo dve linearne kongruencije:

$$x \equiv c \pmod{m_1 m_2 \cdots m_{k-1}}, \quad x \equiv c_k \pmod{m_k}.$$

Budući da je po datim uslovima $(m_1 m_2 \cdots m_{k-1}, m_k) = 1$, Posledica 6.5 povlači egzistenciju rešenja gornjeg, pa tako i polaznog sistema. Pri tome sva rešenja formiraju jednu klasu ostatka po modulu $m_1 m_2 \cdots m_k$. □

Drugi dokaz. Drugi dokaz se odnosi samo na egzistenciju rešenja. Naime, neka je $M = m_1 m_2 \cdots m_k$ i definišimo $M_i = M/m_i$ (što je proizvod svih modula osim i-tog). Po datim uslovima, važi $(M_i, m_i) = 1$ za sve $1 \leqslant i \leqslant k$. Zbog toga, po Tvrđenju 6.1 (odnosno, po Posledici 6.3), linearna kongruencija

$$M_i y \equiv c_i \pmod{m_i}$$

ima rešenje; neka je, na primer, $y = \xi_i$ jedno od rešenja. Tvrdimo da je tada

$$x = M_1 \xi_1 + M_2 \xi_2 + \cdots + M_k \xi_k$$

rešenje sistema (6.4). Zaista, primetimo da $m_i \mid M_j$ ako i samo ako $i \neq j$. Prema tome, za sve $1 \leqslant i \leqslant k$ imamo

$$x \equiv M_i \xi_i \equiv c_i \pmod{m_i},$$

što je upravo ono što se i tražilo. □

Dakle, rešavanje sistema (6.4) u slučaju kada je $(m_i, m_j) = 1$ za sve $i \neq j$ svodi se na pojedinačno rešavanje linearnih kongruencija oblika $M_i y \equiv c_i \pmod{m_i}$; ukoliko uspemo da nađemo partikularna rešenja (označena sa ξ_i u prethodnom dokazu) ovih jednačina, tada opšte rešenje sistema (6.4) u posmatranom slučaju glasi:

$$x = kM + \sum_{i=1}^{k} \xi_i M_i,$$

gde je $k \in \mathbb{Z}$.