Predavanje 4
KONGRUENCIJE I SISTEMI OSTATAKA

Imajući u vidu postupak deljenja sa ostatkom, prirodno je izvršiti klasifikaciju skupa $\mathbb{Z}$ celih brojeva na klase brojeva koji daju isti ostatak pri deljenju sa nekim fiksnim deliteljem m. Ovo se realizuje binarnom relacijom *kongruencije po modulu* m. Naime, definišemo da je

$$a \equiv b \pmod{m} \quad \text{ako i samo ako} \quad m \mid a - b.$$

Pri tome ne predstavlja nikakvo ograničenje opštosti ako pretpostavimo da je $m > 0$, budući da $m \mid a - b$ ako i samo ako $-m \mid a - b$.

Termin 'kongruencija' ovde nije odabran slučajno; sledeće tvrđenje pokazuje da je $\cdot \equiv \cdot \pmod{m}$ zaista kongruencija prstena $\mathbb{Z}$.

Tvrđenje 4.1. *Za sve $a, b, c, d \in \mathbb{Z}$ i $m > 0$ važi:*

(i) $a \equiv a \pmod{m}$.
(ii) $a \equiv b \pmod{m} \;\Rightarrow\; b \equiv a \pmod{m}$.
(iii) $a \equiv b \pmod{m},\ b \equiv c \pmod{m} \;\Rightarrow\; a \equiv c \pmod{m}$.
(iv) $a \equiv b \pmod{m},\ c \equiv d \pmod{m} \;\Rightarrow$
$$a + c \equiv b + d \pmod{m},\ a - c \equiv b - d \pmod{m}.$$
(v) $a \equiv b \pmod{m},\ c \equiv d \pmod{m} \;\Rightarrow\; ac \equiv bd \pmod{m}$.

Dokaz. Ilustracije radi, pokazaćemo samo (v). Po datim uslovima, imamo da $m \mid a - b$ i $m \mid c - d$. Zbog toga,

$$m \mid c(a - b) + b(c - d) = ac - bd,$$

tj. $ac \equiv bd \pmod{m}$. □

Višestrukom primenom tačke (v) dobijamo da $a \equiv b \pmod{m}$ povlači da važi $a^n \equiv b^n \pmod{m}$ za sve $n \geqslant 1$. Zato važi i sledeće.

Posledica 4.2. *Neka je $a, b \in \mathbb{Z}$, $m > 0$, dok je $f(x)$ polinom sa celim koeficijentima. Tada je*

$$f(a) \equiv f(b) \pmod{m}.$$

Prema tome, relacija kongruencije po modulu je invarijantna na tri od četiri osnovne računske operacije: sabiranje, oduzimanje, množenje. Međutim, to nije slučaj sa deljenjem; na primer $6 \equiv 2 \pmod{4}$, ali to ne znači da možemo kongruenciju skratiti sa 2, jer nije tačno da je $3 \equiv 1 \pmod{4}$. Skraćivanje kongruencija je moguće samo uz istovremenu *promenu modula* u odnosu na kojeg se kongruencija posmatra; o tome govori naredni rezultat.

Tvrđenje 4.3. *Neka $a, b, c \in \mathbb{Z}$, $m > 0$ i neka je $d = (c, m)$. Tada važi*

$$ac \equiv bc \pmod{m} \quad \textit{ako i samo ako} \quad a \equiv b \pmod{\frac{m}{d}}.$$

Dokaz. Kongruencija $ac \equiv bc \pmod{m}$ ekvivalentna je uslovu $m \mid (a-b)c$. On je, dalje, ekvivalentan sa

$$\frac{m}{d} \mid (a-b)\frac{c}{d}.$$

Pošto je $(m/d, c/d) = 1$, gornja deljivost važi ako i samo ako $\frac{m}{d} \mid a-b$, odnosno $a \equiv b \pmod{m/d}$. □

Kada su modul i broj kojim se skraćuje uzajamno prosti, imamo specijalan slučaj u kojem skraćivanje kongruencije *jeste* korektno.

Posledica 4.4. *Ako su $a, b, c \in \mathbb{Z}$ i $m > 0$ takvi da $ac \equiv bc \pmod{m}$ i $(c, m) = 1$, tada je $a \equiv b \pmod{m}$.*

Za $a \in \mathbb{Z}$ i fiksan modul m, klasu ekvivalencije elementa a u odnosu na relaciju $\cdot \equiv \cdot \pmod{m}$ označavamo sa $(a)_m$ i zovemo je *klasa ostatka*. Na taj način, imamo particiju skupa $\mathbb{Z}$ na m klasa, od kojih je svaka (dvostrano) beskonačna aritmetička progresija. Proizvoljna transverzala ove particije (skup brojeva takav da svakoj klasi pripada tačno jedan odabrani broj) je *potpun sistem ostataka*. Očigledno, $0, 1, \ldots, m-1$ jeste jedan potpun sistem ostataka; njega ćemo zvati *standardnim*. Sledeći kriterijum je očigledan, pa izostavljamo dokaz.

Tvrđenje 4.5. *Niz celih brojeva $r_1, \ldots, r_k$ čini potpun sistem ostataka po modulu $m > 0$ ako i samo ako važi:*

(1) *$k = m$;*
(2) *dati brojevi su po parovima nekongruentni po modulu m, tj.*

$$i \neq j \Rightarrow r_i \not\equiv r_j \pmod{m}.$$

Tvrđenje 4.6. *Neka je $r_1, \ldots, r_m$ proizvoljni potpun sistem ostataka po modulu $m > 0$ i neka je $a, b \in \mathbb{Z}$ tako da je $(a, m) = 1$. Tada je i*

$$ar_1 + b, \ldots, ar_m + b$$

potpun sistem ostataka po modulu m.

Dokaz. Očigledno, $ar_1 + b, \ldots, ar_m + b$ jeste niz koji se sastoji od m različitih brojeva. Štaviše, $ar_i + b \equiv ar_j + b \pmod{m}$ povlači da je $ar_i \equiv ar_j \pmod{m}$, odakle po Posledici 4.4 sledi $r_i \equiv r_j \pmod{m}$, budući da je $(a, m) = 1$. Dakle, mora biti $i = j$, pa po prethodnom tvrđenju zaključujemo da je posmatrani niz potpun sistem ostatak po modulu m. □

Uslov $(a, m) = 1$ je ovde neophodan, jer u suprotnom nisu sve klase ostataka zastupljene u nizu $ar_1 + b, \ldots, ar_m + b$: na primer, nije moguće da je $ar_i \equiv 1 \pmod{m}$ (jer $d = (a, m) > 1$ deli i a i m), pa tako klasa $(b+1)_m$ ne bi imala svog predstavnika.

Sada ćemo ispitati kako su brojevi koji su uzajamno prosti sa m raspoređeni u odnosu na klase ostataka. U narednom tvrđenju će se ispostaviti da je taj raspored izuzetno pravilan: ako za neko $b \in (a)_m$ važi $(b, m) = 1$, tada su *svi* elementi klase $(a)_m$ uzajamno prosti sa m. Prema tome, "biti uzajamno prost sa" (nekim fiksnim brojem m) nije toliko svojstvo individualnih celih brojeva koliko klasa ostataka po modulu m.

Tvrđenje 4.7. *Neka su $a, b \in \mathbb{Z}$ i $m > 0$ takvi da je $a \equiv b \pmod m$. Tada je $(a, m) = (b, m)$. Specijalno, važi $(a, m) = 1$ ako i samo ako $(b, m) = 1$.*

Dokaz. Pretpostavka da $m \mid a - b$ znači da je $b = cm + a$ za neko $c \in \mathbb{Z}$. Odavde je očito da $(a, m) \mid b$, jer $(a, m) \mid a$ i $(a, m) \mid m$; stoga $(a, m) \mid (b, m)$. S druge strane, izražavajući $a = b - cm$, analogno dobijamo da $(b, m) \mid (a, m)$, pa sledi $(a, m) = (b, m)$. □

Klasa ostatka $(a)_m$ je *redukovana* ako je $(a, m) = 1$; drugim rečima redukovane klase ostataka su one koje se sastoje iz brojeva uzajamno prostih sa m. Za $m \geqslant 1$, označimo sa $\varphi(m)$ broj svih elemenata standardnog potpunog sistema ostataka po modulu m (tj. niza $0, 1, \ldots, m - 1$) koji su uzajamno prosti sa m. Na ovaj način se dobija *Ojlerova funkcija* $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$. Možemo uočiti da je $\varphi(m)$ zapravo ukupan broj redukovanih klasa ostataka po modulu m.

Redukovani sistem ostataka po modulu m je bilo koja transverzala (sistem predstavnika) redukovanih klasa. Prva zapažanja u vezi sa redukovanim sistemima ostataka možemo sumirati na sledeći način.

Tvrđenje 4.8. *Niz celih brojeva $r_1, \ldots, r_k$ čini redukovan sistem ostataka po modulu $m > 0$ ako i samo ako važi:*

(1) *$k = \varphi(m)$;*
(2) *dati brojevi su po parovima nekongruentni po modulu m;*
(3) *$(r_i, m) = 1$ za sve $1 \leqslant i \leqslant \varphi(m)$.*

Tvrđenje 4.9. *Neka je $r_1, \ldots, r_{\varphi(m)}$ proizvoljni redukovan sistem ostataka po modulu $m > 0$ i neka je $a \in \mathbb{Z}$ tako da je $(a, m) = 1$. Tada je i*

$$ar_1, \ldots, ar_{\varphi(m)}$$

redukovan sistem ostataka po modulu m.

Dokaz. Proverićemo uslove iz prethodnog kriterijuma. Zaista, niz $ar_1, \ldots, ar_{\varphi(m)}$ sadrži $\varphi(m)$ različitih brojeva. Oni su po parovima nekongruentni po modulu m, jer $ar_i \equiv ar_j \pmod m$ povlači $r_i \equiv r_j \pmod m$ (i stoga $i = j$) po Posledici 4.4. Najzad, za svako i važi $(ar_i, m) = 1$, budući da je $(a, m) = 1$ i $(r_i, m) = 1$ (Lema 3.6). □