Predavanje 7

VILSONOVA TEOREMA, PRSTEN OSTATAKA

Teorema 7.1 (Vilsonova teorema)**.** *Neka je p prost broj. Tada je*

$$(p-1)! \equiv -1 \pmod{p}.$$

Dokaz. Tvrđenje teoreme je očito tačno za $p = 2, 3$, pa pretpostavimo da je $p \geqslant 5$. Dokazaćemo da se skup $\{2, 3 \ldots, p-2\}$ može razbiti u $(p-3)/2$ parova tako da proizvod svakog para daje ostatak 1 pri deljenju sa p.

Naime, za svako $2 \leqslant a \leqslant p-2$, po Posledici 6.3, postoji tačno jedno rešenje linearne kongruencije

$$ax \equiv 1 \pmod{p}$$

u skupu $\{0, 1, \ldots, p-1\}$. Međutim, to rešenje očito nije $x = 0$, kao ni $x \in \{1, p-1\}$ (jer bi u suprotnom bilo $a \equiv \pm 1 \pmod{p}$, što nije slučaj). Prema tome, to rešenje, koje ćemo označiti sa $f(a)$, takođe leži u skupu $\{2, 3, \ldots, p-2\}$. Ovim smo definisali jednu transformaciju posmatranog skupa, tj. funkciju $f : \{2, 3, \ldots, p-2\} \to \{2, 3, \ldots, p-2\}$. Ova funkcija ima sledeća svojstva:

(1) $af(a) \equiv 1 \pmod{p}$;
(2) $f(f(a)) = a$, tj. ako je $f(a) = b$, tada je $f(b) = a$ (ovo je posledica prethodne tačke i jedinstvenosti rešenja kongruencije $f(a)x \equiv 1 \pmod{p}$ u skupu $\{2, 3, \ldots, p-2\}$);
(3) $f(a) \neq a$ za sve $a \in \{2, 3, \ldots, p-2\}$ (u suprotnom bi bilo $a^2 \equiv 1 \pmod{p}$, tj. $p \mid a^2 - 1 = (a-1)(a+1)$, što je moguće samo ako je $a \equiv \pm 1 \pmod{p}$).

Drugim rečima $\{\{a, f(a)\} : a \in \{2, 3, \ldots, p-2\}\}$ predstavlja upravo traženo sparivanje.

Otuda odmah sledi da je

$$(p-1)! = 1 \cdot [(2 \cdot f(2)) \cdots] \cdot (p-1) \equiv 1 \cdot (p-1) \equiv -1 \pmod{p},$$

što se i tražilo. □

Pri tome važi i obrat ove teoreme: ako za neki prirodan broj $n \geqslant 2$ važi

$$(n-1)! \equiv -1 \pmod{n},$$

tada n mora biti prost; naime, ako je n složen, tada $n \mid (n-1)!$.

Prethodni dokaz Vilsonove teoreme predstavlja jedan od motiva da se na skupu svih klasa ostataka $(a)_m$ po modulu m definiše algebarska struktura uvođenjem operacija $+$ i $\cdot$ definisanih sa

$$(a)_m + (b)_m = (a+b)_m,$$
$$(a)_m (b)_m = (ab)_m.$$

Ove definicije su logički dobre, tj. ne zavise od izbora predstavnika a, b, budući da smo još u Tvrđenju 4.1 pokazali da je $\cdot \equiv \cdot \pmod{m}$ zaista kongruencija prstena

$\mathbb{Z}$. Na taj način, skup svih klasa ostataka $\{(a)_m : 0 \leqslant a \leqslant n-1\}$ zajedno sa opisanim operacijama takođe čini prsten, koji zovemo *prsten ostataka po modulu* m i označavamo sa $\mathbb{Z}_m$. Naime, ako je $m\mathbb{Z}$ ideal od $\mathbb{Z}$ koji se sastoji od svih celih brojeva deljivih sa m, tada je $\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z}$. Drugim rečima, preslikavanje koje svakom celom broju dodeljuje njegovu klasu ostatka po modulu m je sirjektivni homomorfizam prstena $\mathbb{Z} \to \mathbb{Z}_m$, i jezgro tog homomorfizma je baš $m\mathbb{Z}$. Prsten $\mathbb{Z}_m$ je, baš kao i $\mathbb{Z}$, komutativan i ima jedinicu — u pitanju je klasa $(1)_m$.

Aditivna grupa $(\mathbb{Z}_m, +)$ prstena ostataka je uvek ciklična: ona je očito generisana klasom $(1)_m$, pošto je

$$(a)_m = \underbrace{(1)_m + \cdots + (1)_m}_{a \text{ sabiraka}}$$

i $(0)_m = (m)_m$. S druge strane, u odnosu na množenje imamo komutativni monoid sa nulom $(\mathbb{Z}_m, \cdot)$ koji u opšem slučaju nije grupa, budući da ne moraju svi njegovi (nenula) elementi biti invertibilni u odnosu na jedinicu $(1)_m$.

Tvrđenje 7.2. *$(a)_m$ je invertibilan element prstena $\mathbb{Z}_m$ ako i samo ako je $(a)_m$ redukovana klasa, tj. ako je $(a, m) = 1$.*

Dokaz. Dokaz tvrđenja sledi iz činjenice da je egzistencija klase $(x)_m$ takve da je $(a)_m(x)_m = (1)_m$ ekvivalentna egzistenciji rešenja kongruencije $ax \equiv 1 \pmod{m}$. Sada je dovoljno pozvati se na Tvrđenje 6.1. □

Primetimo da je skup svih redukovanih klasa zatvoren na množenje: ako je $(a, m) = (b, m) = 1$, tada je i $(ab, m) = 1$, tj. $(ab)_m$ je takođe redukovana klasa. Prema tome, redukovane klase u odnosu na množenje čine podmonoid od $(\mathbb{Z}_m, \cdot)$ u kojem svaki element ima inverz; dakle, u pitanju je grupa, koju označavamo sa $\mathcal{U}_m$ (oznaka potiče od toga što se u engleskoj terminologiji invertibilni elementi prstena zovu 'units' — 'jedinice'). Budući da su sve nenula klase po modulu m redukovane ako i samo ako je m prost broj, odmah imamo sledeći zaključak.

Posledica 7.3. *$\mathbb{Z}_m$ je polje ako i samo ako je m prost broj.*

Sada imamo da je Vilsonova teorema specijalan slučaj sledećeg poznatog tvrđenja: *proizvod svih nenula elemenata bilo kog konačnog polja je -1.* Ono se dokazuje na isti način kao i Vilsonova teorema (koja tvrdi ovo isto u polju $\mathbb{Z}_p$): svi elementi koji su sami sebi inverzni su koreni polinoma $x^2 - 1 = 0$ (dakle, 1 i -1), dok se svi preostali elementi mogu podeliti u parove koji se sastoje iz nekog elementa i njegovog inverza.

Takođe, pošto je $|\mathcal{U}_m| = \varphi(m)$, imamo da je Ojlerova teorema direktna posledica Lagranžove teoreme iz elementarne teorije grupa. Pošto red svake podgrupe deli red konačne grupe G, sledi da *red elementa* $a \in G$, najmanji $n \in \mathbb{Z}^+$ tako da u G važi $a^n = 1$, deli $|G|$. Zbog toga mora biti $a^{|G|} = 1$. Primenjujući ovo na grupu $\mathcal{U}_m$, dobijamo da za svaku redukovanu klasu $(a)_m$ važi

$$(a)_m^{\varphi(m)} = (1)_m.$$

Drugim rečima, ako je $(a, m) = 1$, tada je $a^{\varphi(m)} \equiv 1 \pmod{m}$.