Predavanje 8
RED I PRIMITIVNI KORENI

Neka je $(a, m) = 1$. Iz Ojlerove teoreme neposredno sledi postojanje pozitivnog celog broja t takvog da je $a^t \equiv 1 \pmod m$: takav je, na primer, $t = k\varphi(m)$ za bilo koje $k \geqslant 1$ (s druge strane, ako $(a, m) \neq 1$, takav broj t očito ne može da postoji). Najmanji broj t koji zadovoljava posmatrani uslov jeste *red* celog broja a po modulu m — u pitanju je zapravo red elementa $(a)_m$ u grupi $\mathcal{U}_m$ (zbog čega brojevi kongruentni po modulu m imaju isti red). Red broja a označavamo sa $o_m(a)$.

Iz definicije odmah sledi da je $o_m(a) \leqslant \varphi(m)$. Još neke osnovne osobine reda rezimirane su u narednom tvrđenju.

Tvrđenje 8.1. *Neka je $(a, m) = 1$ i neka su $t, u, v \in \mathbb{Z}^+$.*

(1) $a^t \equiv 1 \pmod m$ *ako i samo ako* $o_m(a) \mid t$.
(2) $a^u \equiv a^v \pmod m$ *ako i samo ako* $u \equiv v \pmod{o_m(a)}$.
(3) *Broj a ima tačno $o_m(a)$ stepeni koji su po parovima nekongruentni po modulu m.*
(4) $o_m(a) \mid \varphi(m)$.

Dokaz. (1) Ako je $t = qo_m(a)$, tada je

$$a^t = (a^{o_m(a)})^q \equiv 1 \pmod m.$$

S druge strane, pretpostavimo da je $t = qo_m(a) + r$, gde je $0 \leqslant r < o_m(a)$. Važi:

$$a^t = (a^{o_m(a)})^q a^r \equiv a^r \pmod m,$$

pa će biti $a^t \equiv 1 \pmod m$ ako i samo ako je $r = 0$, tj. $o_m(a) \mid t$.

(2) Bez ograničenja opštosti, neka je $u \geqslant v$. Budući da je $(a, m) = 1$, kongruencija $a^u \equiv a^v \pmod m$ se može skratiti sa a^i za sve $1 \leqslant i \leqslant v$, tako da se dobija ekvivalentna kongruencija $a^{u-v} \equiv 1 \pmod m$. Po tački (1), poslednja kongruencija je dalje ekvivalentna sa uslovom $o_m(a) \mid u - v$, tj. $u \equiv v \pmod{o_m(a)}$.

(3) Ovo je direktna posledica tačke (2).

(4) Sledi iz Ojlerove teoreme i tačke (1). □

Ceo broj g je *primitivni koren* po modulu m ako je $o_m(g) = \varphi(m)$. Na primer, $o_{10}(3) = 4 = \varphi(10)$, pa je 3 primitivni koren po modulu 10. S druge strane, ako a nije primitivni koren po modulu m tada po tački (4) prethodnog tvrđenja postoji neki pravi delitelj $d \mid \varphi(m)$ tako da je $a^d \equiv 1 \pmod m$; stoga postoji neki prost delitelj $p \mid \varphi(m)$ tako da d deli $\varphi(m)/p$. Prema tome, da bismo proverili da li je a primitivni koren po modulu m potrebno je i dovoljno ustanoviti da li je $a^{\varphi(m)/p} \equiv 1 \pmod m$ za neki prost broj $p \mid \varphi(m)$.

U narednom tvrđenju dajemo nekoliko ekvivalentnih formulacija pojma primitivnog korena.

Tvrđenje 8.2. *Sledeći uslovi su ekvivalentni:*

(1) *Broj $g \in \mathbb{Z}$ je primitivni koren po modulu m.*
(2) *$1, g, g^2, \ldots, g^{\varphi(m)-1}$ je redukovan sistem ostataka po modulu m.*
(3) *$\mathcal{U}_m$ je ciklična grupa generisana klasom $(g)_m$.*

Dokaz. (1)⇒(2): Neka je $o_m(g) = \varphi(g)$. Tada su po tački (3) prethodnog tvrđenja svi brojevi $1, g, g^2, \ldots, g^{\varphi(m)-1}$ po parovima nekongruentni po modulu m; osim toga, zbog $(g, m) = 1$, oni su svi uzajamno prosti sa m. Pošto navedenih brojeva ima tačno $\varphi(m)$, po Tvrđenju 4.8 sledi da oni čine redukovan sistem ostataka po modulu m.

(2)⇒(3): Očigledno.

(3)⇒(1): Po definiciji reda elementa sledi da je $o_m(g) = \varphi(m)$. Osim toga, $(g)_m \in \mathcal{U}_m$ povlači da je $(g, m) = 1$. □

Naravno, postavlja se pitanje u odnosu na koje module uopšte postoji (bar jedan) primitivan koren. Iz prethodnog tvrđenja je jasno da je pitanje egistencije takvog korena po modulu m ekvivalentno pitanju da li je grupa $\mathcal{U}_m$ ciklična. Na primer, ako je $m = 12$, tada je jedan redukovani sistem ostataka $\{\pm 1, \pm 5\}$, pa se lako proverava da nijedan od njih nije reda $\varphi(12) = 4$ (tako grupa $\mathcal{U}_{12}$ nije ciklična grupa reda 4, već Klajnova grupa — direktan proizvod dve ciklične grupe reda 2). U narednom ćemo dokazati da primitivan koren postoji za svaki *prost* modul. (Ovo je opet specijalan slučaj opštijeg algebarskog rezultata: multiplikativna grupa nenula elemenata svakog konačnog polja je ciklična.) Najpre su nam potrebna dva pomoćna rezultata.

Lema 8.3. *Neka je $a \in \mathbb{Z}^+$ i $(a, m) = 1$. Tada je $o_m(a^k) = o_m(a) = d$ ako i samo ako je $(k, d) = 1$.*

Dokaz. Po tački (1) Tvrđenja 8.1 važi da je

$$(a^k)^t = a^{kt} \equiv 1 \pmod{m}$$

ako i samo ako $o_m(a) = d \mid kt$. Prema tome, ako je $(k, d) = 1$, tada mora biti $d \mid t$. S druge strane, $a^{kd} = (a^d)^k \equiv 1 \pmod{m}$, pa je $o_m(a^k) = d$.

Obratno, ako je $(k, d) = d' > 1$, tada za $t = d/d'$ imamo da $d \mid kt$, pa je $(a^k)^t \equiv 1 \pmod{m}$, što znači da je $o_m(a^k) \leqslant d/d' < d = o_m(a)$. Specijalno, $o_m(a^k) \neq o_m(a)$. □

Lema 8.4. *Za svako $n \geqslant 1$ važi*

$$\sum_{d \mid n} \varphi(d) = n.$$

Dokaz. Ako je $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ kanonički oblik broja n, tada se proizvoljan delilac $d \mid n$ prikazuje u obliku $d = p_1^{\beta_1} \cdots p_k^{\beta_k}$, gde je $\beta_i \leqslant \alpha_i$ za sve $1 \leqslant i \leqslant k$. Zbog multiplikativnosti Ojlerove funkcije (Lema 5.3) imamo $\varphi(d) = \varphi(p_1^{\beta_1}) \cdots \varphi(p_k^{\beta_k})$, odakle nije teško videti da važi jednakost

$$\sum_{d \mid n} \varphi(d) = \prod_{i=1}^{k} (1 + \varphi(p_i) + \cdots + \varphi(p_i^{\alpha_i})).$$

Međutim, opšti član proizvoda na desnoj strani je jednak

$$1 + (p_i - 1) + \cdots + (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = p_i^{\alpha_i},$$

što znači da je desna strana jednaka n. □

Teorema 8.5. *Za svaki prost broj p postoji tačno $\varphi(p-1)$ po parovima nekongruentnih primitivnih korena po modulu p.*

Dokaz. Za $d \geqslant 1$ definišimo $h(d)$ kao broj nenula ostataka pri deljenju sa p koji su reda d,

$$h(d) = |\{a \in \{1, \ldots, p-1\} : o_p(a) = d\}|.$$

Jasno, za svaki broj a važi $o_p(a) \mid \varphi(p) = p - 1$, pa je $h(d) = 0$ za sve d takve da $d \nmid p - 1$. Zbog toga je $\sum_{d \mid p-1} h(d) = p - 1$. Tvrdimo da važi $h(d) \leqslant \varphi(d)$; tačnije, dokazaćemo da je $h(d) = \varphi(d)$ kad god postoji bar jedan element grupe $\mathcal{U}_p$ reda d.

Pretpostavimo, dakle, da je $o_p(a) = d$. Tada su brojevi $1, a, \ldots, a^{d-1}$ po parovima nekongruentni po modulu p. Osim toga, svi ovi brojevi su rešenja konguencijske jednačine $x^d \equiv 1 \pmod p$, pošto za sve $0 \leqslant i \leqslant d - 1$ važi $(a^i)^d = (a^d)^i \equiv 1 \pmod p$. Ovo poslednje tvrđenje se drugim rečima može izraziti na sledeći način: $(1)_p, (a)_p, \ldots, (a^{d-1})_p$ su različiti elementi polja $\mathbb{Z}_p$ i svaki od njih je koren polinoma

$$q(x) = (1)_p x^d + (-1)_p \in \mathbb{Z}_p[x].$$

Kako svaki polinom stepena d nad nekim poljem $\mathbb{F}$ može imati najviše d korena u $\mathbb{F}$ (što je posledica Bezuovog stava), sledi da su nabrojanim klasama iscrpljeni *svi* koreni polinoma $q(x)$ u $\mathbb{Z}_p$. Prema tome, svako rešenje kongruencije $x^d \equiv 1 \pmod p$ kongruentno je po modulu p sa nekim od brojeva $1, a, \ldots, a^{d-1}$.

Kako je svaki broj reda d takođe rešenje jednačine $x^d \equiv 1 \pmod p$, sledi da je svaki broj reda d kongruentan po modulu p sa nekim od $1, a, \ldots, a^{d-1}$. Međutim, po Lemi 8.3 imamo da je $o_p(a^k) = d$ ako i samo ako je $(k, d) = 1$. Otuda sledi da među brojevima $1, a, \ldots, a^{d-1}$ ima tačno $\varphi(d)$ onih koji su reda d. Dakle, dokazali smo da $h(d) > 0$ za neko $d \mid p - 1$ povlači da je $h(d) = \varphi(d)$.

Najzad, iz prethodnog tvrđenja i Leme 8.4 imamo sledeći niz jednakosti i nejednakosti:

$$p - 1 = \sum_{d \mid p-1} h(d) \leqslant \sum_{d \mid p-1} \varphi(d) = p - 1.$$

Ova nejednakost postaje jednakost samo ukoliko je $h(d) = \varphi(d)$ za *sve* delioce $d \mid p - 1$. Specijalno, za $d = p - 1$ dobijamo da u skupu $\{1, 2, \ldots, p-1\}$ ima tačno $\varphi(p-1)$ primitivnih korena po modulu p. □

Opšti rezultat koji opisuje sve module m u odnosu na koje primitivni koreni postoje (odnosno, za koje je $\mathcal{U}_m$ ciklična grupa) dajemo bez dokaza.

Teorema 8.6. *Neka je $m \geqslant 2$ prirodan broj. Postoji primitivni koren po modulu m ako i samo ako je $m \in \{2, 4\}$ ili $m = p^\alpha$ ili $m = 2p^\alpha$ za neki prost broj $p \geqslant 3$ i prirodan broj $\alpha \geqslant 1$.*