Predavanje 9

BINOMNE KONGRUENCIJE, KVADRATNI OSTACI

Neka je $k \geqslant 2$, p prost broj i $a \in \mathbb{Z}$ tako da je $(a, p) = 1$ (tj. $p \nmid a$). U narednom ćemo razmatrati pitanje rešivosti kongruencije

$$x^k \equiv a \pmod{p}.$$

Kongruencijske jednačine ovog tipa zovemo *binomne kongruencije*. Primetimo da se naoko opštija dvočlana ("binomna") kongruencija $bx^k \equiv c \pmod{p}$ (gde $p \nmid b$) lako svodi na posmatrani oblik uvođenjem smene $y = x^k$ i nalaženjem rešenja linearne kongruencije $by \equiv c \pmod{p}$ u obliku $y \equiv a \pmod{p}$. Osim toga, jednostavnosti radi razmatramo slučaj *prostog* modula, sa napomenom da se veći deo pojmova i rezultata koji slede mogu lako adaptirati i na slučaj složenih modula u odnosu na koje postoji primitivan koren.

Problem rešivosti binomnih kongruencija po prostom modulu $p \neq 2$ se na prilično elegantan način može rešiti primenom pojma diskretnog logaritma, odnosno indeksa broja a koji pripada redukovanoj klasi ostataka $\bmod p$. Naime, neka je g neki primitivni koren po modulu p (u Teoremi 8.5 smo videli ne samo da takav koren postoji, nego da ih ima $\varphi(p-1)$ međusobno nekongruentnih). Tada po Tvrđenju 8.2 brojevi

$$1, g, \ldots, g^{p-2}$$

čine redukovan sistem ostataka $\bmod p$, pa kako je po pretpostavci $(a, p) = 1$, postoji tačno jedan eksponent k, $0 \leqslant k \leqslant p-2$, tako da je $a \equiv g^k \pmod{p}$. Ovaj broj k zovemo *indeks* ili *diskretni logaritam* broja a, u oznaci $k = \operatorname{ind}_{p,g} a$ (p se izostavlja ako je modul jasan iz konteksta). Naravno, indeks broja zavisi od izbora g, pa tako o indeksu ima smisla govoriti samo kada je prethodno fiksiran primitivni koren u odnosu na koji se on posmatra. Takođe, jasno je da $a \equiv b \pmod{p}$ povlači $\operatorname{ind}_g a = \operatorname{ind}_g b$, tako da je indeks zapravo karakteristika redukovane klase, a ne samog broja.

Podsetimo se Tvrđenja 8.1 (2) u slučaju kada je modul prost, a osnova stepena primitivni koren. Tada imamo:

$$g^u \equiv g^v \pmod{p} \text{ ako i samo ako } u \equiv v \pmod{p-1}.$$

Iz ove osobine se lako dokazuje da, posmatrano po modulu $\varphi(p) = p-1$, indeks ima nekoliko svojstava koje veoma liče na poznate osobine realne funkcije $f(x) = \log_b x$ za pozitivnu bazu $b \neq 1$ i $x \in \mathbb{R}^+$. Naime, imamo (za bilo koje primitivne korene g, h po modulu p):

(1) $\operatorname{ind}_g 1 = 0$; $\operatorname{ind}_g g = 1$;
(2) $\operatorname{ind}_g(ab) \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{p-1}$;
(3) $\operatorname{ind}_g(a^k) \equiv k \operatorname{ind}_g a \pmod{p-1}$;
(4) $\operatorname{ind}_h a \equiv \operatorname{ind}_h g \cdot \operatorname{ind}_g a \pmod{p-1}$.

Vratimo se sada pitanju rešavanja opšte binomne kongruencije.

Teorema 9.1. *Neka je p prost broj i $(a,p)=1$. Tada binomna kongruencija $x^k \equiv a \pmod p$ ima rešenje ako i samo ako je*

$$a^{\frac{p-1}{(k,p-1)}} \equiv 1 \pmod p.$$

U slučaju rešivosti, broj po parovima nekongruentnih rešenja je $(k,p-1)$. Osim toga uslov rešivosti je ekvivalentan i sa

$$(k,p-1) \mid \operatorname{ind}_g a,$$

gde je g proizvoljan primitivni koren po modulu p.

Dokaz. Po definiciji indeksa, za svaki ceo broj x važi $x \equiv g^{\operatorname{ind}_g x} \pmod p$, pa ćemo rešenje tražiti u obliku kao na desnoj strani poslednje kongruencije. Primenjujući ovo i na a, dobijamo sledeću kongruencijsku jednačinu po $\operatorname{ind}_g x$:

$$g^{k \operatorname{ind}_g x} \equiv g^{\operatorname{ind}_g a} \pmod p.$$

Po već razmotrenom specijalnom slučaju Tvrđenja 8.1, tačka (2), ta jednačina je ekvivalentna sa

$$k \operatorname{ind}_g x \equiv \operatorname{ind}_g a \pmod{p-1}.$$

Ovo je sada *linearna* kongruencija po $\operatorname{ind}_g x$ koja je po Tvrđenju 6.1 rešiva ako i samo ako $(k,p-1) \mid \operatorname{ind}_g a$; potonji uslov je, dakle, ekvivalentan rešivosti kongruencije $x^k \equiv a \pmod p$. S druge strane, važi

$$a^{\frac{p-1}{(k,p-1)}} \equiv \left(g^{\operatorname{ind}_g a}\right)^{\frac{p-1}{(k,p-1)}} = g^{\frac{(p-1)\operatorname{ind}_g a}{(k,p-1)}} \pmod p,$$

pa važi $a^{(p-1)/(k,p-1)} \equiv 1 \pmod p$ ako i samo ako je eksponent na desnoj strani, $((p-1)\operatorname{ind}_g a)/(k,p-1)$, deljiv sa $p-1$, tj. ako i samo ako $(k,p-1) \mid \operatorname{ind}_g a$.

Najzad, iz prethodnih razmatranja je jasno da je broj po parovima nekongruentnih rešenja rešive kongruencije $x^k \equiv a \pmod p$ jednak broju međusobno nekongruentnih rešenja jednačine $k \operatorname{ind}_g x \equiv \operatorname{ind}_g a \pmod{p-1}$, što je po Teoremi 6.2 upravo $(k,p-1)$. □

Za ceo broj a, $(a,p)=1$, kažemo da je *ostatak k-tog stepena po modulu p* ukoliko kongruencija $x^k \equiv a \pmod p$ ima rešenja. Prema tome, prethodna teorema daje kriterijum kada je neki broj ostatak k-tog stepena.

Posledica 9.2. *Broj po parovima nekongruentnih ostataka k-tog stepena po modulu p jednak je*

$$\frac{p-1}{(k,p-1)}.$$

Dokaz. Po prethodnoj teoremi, ostaci k-tog stepena po modulu p su upravo rešenja binomne kongruencije

$$x^{\frac{p-1}{(k,p-1)}} \equiv 1 \pmod p.$$

Po istoj teoremi, broj njenih po parovima nekongruentnih rešenja je

$$\left(\frac{p-1}{(k,p-1)}, p-1\right) = \frac{p-1}{(k,p-1)},$$

što je i trebalo dokazati. □

Specijalno, kada je $k = 2$, ostatke k-tog stepena zovemo *kvadratni ostaci* (po modulu p). Kada je $p = 2$, kvadratni ostaci su zapravo neparni brojevi, tj. klasa $(1)_2$, pa pretpostavimo da je $p > 2$. Sada imamo da je $a \in \mathbb{Z}$ kvadratni ostatak ako i samo ako važi

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

odnosno ako je indeks broja a (u odnosu na bilo koji primitivan koren $\bmod p$) paran. S druge strane, brojeve koji *nisu* kvadratni ostaci prepoznaćemo po tome što za njih važi

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

budući da za $y = a^{(p-1)/2}$ mora biti $y^2 \equiv 1 \pmod{p}$, tj. $p \mid y^2 - 1 = (y-1)(y+1)$, pa je $y \equiv -1 \pmod{p}$ jedina preostala mogućnost. (Primetimo da brojeve iz klase $(0)_p$ ne svrstavamo ni u jednu od ove dve kategorije.) Dalje, broj po parovima nekongruentnih kvadratnih ostataka je $(p-1)/2$; ukoliko je a kvadratni ostatak, tada kongruencija $x^2 \equiv a \pmod{p}$ ima tačno dva nekongruentna rešenja.

Kako bismo kompaktnije i lakše izražavali svojstvo "biti kvadratni ostatak", uvodimo tzv. *Ležandrov simbol*:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{ako je } a \text{ kvadratni ostatak } \bmod p, \\ -1 & \text{ako } a \text{ nije kvadratni ostatak } \bmod p. \end{cases}$$

U nekim slučajevima je zgodno proširiti Ležandrov simbol i na brojeve a deljive sa p, kada definišemo $(a/p) = 0$. Međutim, ukoliko to nije drugačije naglašeno, sama pojava Ležandrovog simbola podrazumeva da $p \nmid a$ (kao i to da je $p > 2$).

Po prethodnim razmatranjima, imamo:

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Osnovna svojstva Ležandrovog simbola rezimirana su u sledećem tvrđenju.

Tvrđenje 9.3.

(i) *Ako je* $a \equiv b \pmod{p}$, *tada je* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(iii) $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \textit{ako je } p \equiv 1 \pmod{4}, \\ -1 & \textit{ako je } p \equiv -1 \pmod{4}. \end{cases}$

Dokaz. (i) Ako je $a \equiv b \pmod{p}$, tada je i $a^{(p-1)/2} \equiv b^{(p-1)/2} \pmod{p}$, odakle je $(a/p) \equiv (b/p) \pmod{p}$; drugim rečima, $p \mid (a/p) - (b/p)$. Međutim, primetimo da važi $|(a/p) - (b/p)| \leqslant 2$, pa iz $p > 2$ sledi da je $(a/p) = (b/p)$.

(ii) Leva i desna strana jednakosti koju dokazujemo su kongruentne po modulu p, budući da su, po definiciji Ležandrovog simbola, obe kongruentne sa $(ab)^{(p-1)/2} = a^{(p-1)/2}b^{(p-1)/2}$. Sada zaključak o jednakosti sledi isto kao i u prethodnoj tački.

(iii) Ova tačka sledi direktno iz

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

i kriterijuma za kvadratne ostatke: desna strana kongruencije je jednaka 1 ako i samo ako je broj $(p-1)/2$ paran, tj. ako i samo ako je $p \equiv 1 \pmod 4$. □

Na osnovu ovog tvrđenja zaključujemo da se vrednost *svakog* Ležandrovog simbola (a/p), $a > 1$, može izraziti preko vrednosti $(2/p)$ i (q/p), gde je q neparan prost broj različit od p; naime, ako je $a = q_1^{\alpha_1} \cdots q_k^{\alpha_k}$ kanonički oblik broja a (pri čemu se uslov $p \nmid a$ reflektuje u tome da su svi prosti brojevi q_i različiti od p), tada imamo

$$\left(\frac{a}{p}\right) = \left(\frac{q_1}{p}\right)^{\alpha_1} \cdots \left(\frac{q_k}{p}\right)^{\alpha_k}.$$

Izračunavanje vrednosti ovih "elementarnih" Ležandrovih simbola omogućiće nam Gausova omiljena *Theorema Aureum* — zakon kvadratne recipročnosti.