Uvod u aritmetiku eliptičkih krivulja

Eliptičke krivulje nad konačnim poljem - 14. lekcija

Konačna polja. Za svaki prost p, postoji polje od p elemenata, a može se realizirati kao

$$\mathbf{F}_p := \{0, 1, ..., p-1\}$$

uz zbrajanje i množenje modulo p. Analogna je realizacija kao kvocijentnog prstena $\mathbf{F}_p :\cong \mathbf{Z}/p\mathbf{Z}$.
Za svaki prirodan broj n postoji i konačno polje $\mathbf{F}_{p^n}$ od p^n elemenata, koje je proširnje stupnja n polja $\mathbf{F}_p$. To su sva, do na izomorfizam, konačna polja. Uobičajeno je pisati $q := p^n$ i $\mathbf{F}_q$ za pripadno polje.
Ako fiksiramo jedno algebarsko zatvorenje $\bar{\mathbf{F}}_p$ polja $\mathbf{F}_p$, onda su polja $\mathbf{F}_q$ jedina (kao skupovi) polja koja sadrže $\mathbf{F}_p$ i vrijedi

$$\mathbf{F}_q = \{x \in \bar{\mathbf{F}}_p : \ x^q = x\}.$$

Konkretna realizacija polja $\mathbf{F}_q$ ostvaruje se biranjem ireducibilnog polinoma f nad $\mathbf{F}_p$ i biranjem nekog njegovog korijena η. Tada je

$$\mathbf{F}_q = \{a_0 + a_1\eta + ... + a_{n-1}\eta^{n-1} : \ a_j \in \mathbf{F}_p\}$$

uz pokomponentno zbrajanje i množenje polinoma uz uvjet $f(\eta) = 0$.

Primjer 1. Polinom $f(x) := x^2 + 1$ ireducibilan je nad $\mathbf{F}_3$ pa je

$$\mathbf{F}_{3^2} = \{a + b\eta : \ a, b \in \mathbf{F}_3\},$$

uz uvjet $\eta^2 = -1$ i ima 9 elemenata.

Eliptičke krivulje nad $\mathbf{F}_p$.

Ograničujemo se na krivulje E s jednadžbama oblika

$$y^2 = x^3 + ax^2 + bx + c \tag{1}$$

gdje su $a, b, c \in \mathbf{F}_p$, a točke (x, y) gledamo da x, y budu u algebarskom zatvorenju $\bar{\mathbf{F}}_p$. Vidi se da je $O[0, 1, 0]$, kao i u karakteristici 0, jedina beskonačno

daleka točka. Tu točku i afine točke s koordinatama u $\mathbf{F}_p$ zovemo racionalnima. Zanimaju nas samo nesingularne krivulje. Zato odmah odbacujemo $p = 2$, jer je tada E singularna, tj. ima singularnu točku. Naime, ako stavimo $F(x, y) := y^2 - x^3 - ax^2 - bx - c$, onda je $\frac{\partial F}{\partial y} = 2y = 0$ za sve (x, y). Dalje, $\frac{\partial F}{\partial x} = -3x^2 - 2ax - b = x^2 + b$ (jer je karakteristika $p = 2$). Jednadžba $x^2 + b = 0$ ima jedinstveno rješenje $x = b$, takodjer, postoji jedinstvena točka na E s prvom koordinatom b, i ta je točka singularna.
Od sad je $p \neq 2$ i E je nesingularna ako i samo ako je $D \neq 0$, gdje je D, kao i prije, diskriminanta kubnog polinoma u varijabli x, tj.

$$D := -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

. Tada kažemo da je E **eliptička krivulja** nad $\mathbf{F}_p$.
Grupni zakon na eliptičkoj krivulji E definira se analogno kao i u karakteristici nula, kao:
$P_1 + P_2 + P_3 = O$ ako su P_1, P_2, P_3 na jednom pravcu.
Podsjetimo, ako je $y = \lambda x + \mu$ jednadžba pravca kroz $P_1(x_1, y_1),\ P_2(x_2, y_2)$, onda je
$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ za $x_2 \neq x_1$, i $\lambda = \frac{3x_1^2 + 2ax_1 + b}{2y_1}$ za $x_2 = x_1$.
Vidimo da da formula nema smisla za $p = 2$. Dalje, ako je $P_3(x_3, y_3$ onda je $x_3 = \lambda^2 - a - x_1 - x_2;\ y_3 = \lambda x_3 + \mu$ dok $P_1 + P_2$ ima koordinate $(x_3, -y_3)$.
Jasno je da je E abelova grupa s neutralnim elementom elementom O, nadalje skup racionalnih točaka $E(\mathbf{F}_p)$ je **konačna abelova grupa**. Evo nekoliko primjera.
Primjer 2. (i) $E : y^2 = x^3 + x + 1$ nad $\mathbf{F}_5$. Tu je $D = 4$ pa je E eliptička krivulja. Kvadrati u $\mathbf{F}_5$ su $0, 1, 4$ pa se lako dobije da je
$E(\mathbf{F}_5) = \{O, (0, \pm 1), (2, \pm 1), (3, \pm 1), (4, \pm 2)\}$, dakle $|E(\mathbf{F}_5)| = 9$. Lako se provjeri da je riječ o cikličkoj grupi reda 9 (a ne o produktu grupa reda 3).
(ii) $E : y^2 = x^3 - x$ nad $\mathbf{F}_5$. Tu je, opet, $D = 4$ pa je E eliptička krivulja. Dobije se $|E(\mathbf{F}_5)| = 8$.
(iii) $E : y^2 = x^3 + x$ nad $\mathbf{F}_5$. Dobije se $|E(\mathbf{F}_5)| = 4$.

Općenito, stavimo $N_p := |E(\mathbf{F}_p)|$ za eliptičku krivulju E nad konačnim poljem $\mathbf{F}_p$. Kako u $\mathbf{F}_p$ ima pola kvadrata i pola nekvadrata (ne računajući nulu), a E ima jednadžbu oblika $y^2 = f(x)$ za kubni polinom f, intuitivno je jasno da će f (u prosjeku) jednako mnogo puta postizati kvadrate kao i nekvadrate. Dakle, možemo očekivati $2\frac{p-1}{2} = p - 1$ takvih racionalnih točaka. Tome treba dodati beskonačno daleku točku i još jednu (f prosječno postiže

jednom vrijednost nulu) i to je $p+1$ točaka. Kako je to tek u prosjeku, očekujemo da bude

$$p+1-\epsilon \leq N_p \leq p+1+\epsilon$$

za neku grješku ϵ, što se može zapisati i kao

$$|p+1-N_p| \leq \epsilon.$$

Pokazuje se da je zaista tako i da je $\epsilon = 2\sqrt{p}$, što je "zanemarivo" u usporedbi s p (za velike p). Ta je činjenica poznata kao **Hasseova ocjena** ili **Hasse-Weilova ocjena** i može se pokazati da je analogna (još ne dokazanoj **Riemannovoj slutnji**). Dakle vrijedi:

$$|p+1-N_p| \leq 2\sqrt{p}.$$

Naravno da tu jednakost nikad ne nastupa, ali taj se obliki tradicionalno piše jer vrijedi i za svako konačno polje s $q := p^n$ elemenata

$$|q+1-N_q| \leq 2\sqrt{q}.$$

To je specijalni slučaj tvrdnje za krivulje genusa g:

$$|q+1-N_q| \leq 2g\sqrt{q}.$$

(tu je tvrdnju prvi dokazao A.Weil).

Redukcija modulo p.
Vratimo se na eliptičke krivulje nad $\mathbf{Q}$, tj. na krivulje

$$E : y^2 = x^3 + ax^2 + bx + c$$

gdje možemo izabrati da a, bc budu cijeli brojevi. Neka je, kao i prije, D diskriminanta od E.
Podsjetimo da postoji homomorfizam redukcije modulo p sa $\mathbf{Z}$ na $\mathbf{F}_p$, zadan kao $m \mapsto m$ modulo p, što kraće pišemo kao $m \mapsto \bar{m}$ (to vrijedi i za $p=2$, ali taj slučaj tu ne razmatramo).
Redukcijom modulo p koeficijenata, od E nastaje krivulja nad $\mathbf{F}_p$

$$\bar{E} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x + \bar{c}.$$

To općenito nije eliptička krivulja (jer ne mora biti nesingularna), ali ako je $\bar{D} \neq 0$ u $\mathbf{F}_p$, onda jest. Kako uvjet $\bar{D} \neq 0$ znači da D nije djeljiv s p vidimo

da vrijedi:
Ako p ne dijeli D, onda je $\bar{E}$ eliptička krivulja.
Posebno, $\bar{E}$ je eliptička krivulja za gotovo sve p.
Ne možemo govoriti općenito o redukciji točaka eliptičke krivulje, ali ako su točke s cjelobrojnim koordinatama, onda je to vrlo prirodan postupak (čak ako su i racionalne, ali sad nas to ne zanima). Naime, ako je $(x, y) \in E(\mathbf{Q})$ i $x, y \in \mathbf{Z}$, onda je $(\bar{x}, \bar{y}) \in E(\mathbf{F}_p)$ (bez obzira je li reducirana krivulja nesingularna, naravno uz uvjet da su a, b, c cijeli brojevi).
Kako su racionalne torzijske točke na E nužno s cjelobrojnim koordinatama (opet uz uvjet da su a, b, c cijeli), one se mogu reducirati na $\bar{E}$. Nije teško vidjeti da je preslikavanje redukcije s $E(\mathbf{Q})_{tors}$ u $\bar{E}(\mathbf{F}_p)$ homomorfizam (naravno uz uvjet da je reducirana krivulja $\bar{E}$ nesingularna, tj. eliptička). Razlog je jednostavan: ako su tri točke od E (s cjelobrojnim koordinatama) na jednom pravcu, onda su njihove redukcije takodjer na jednom pravcu (za detalje vidite [S-T]). Zato vrijedi:

Teorem. Preslikavanje redukcije $E(\mathbf{Q})_{tors} \to \bar{E}(\mathbf{F}_p)$ definirano kao

$$(x, y) \mapsto (\bar{x}, \bar{y}),\ i\ O \mapsto \bar{O},$$

je injektivni homomorfizam grupa (uz uvjet da p ne dijeli $2D$).
Dokaz. Sve smo komentirali osim injektivnosti, a ona izravno slijedi iz toga što je preslikavanje redukcije homomorfizam (naime, jezgra je očito samo O).

Teorem govori da za sve osim konačno mnogo prostih p (djelitelja od D) grupu $E(\mathbf{Q})_{tors}$ možemo smatrati podgrupom grupe $E(\mathbf{F}_p)$. Kako je ovu drugu grupu relativno lako računati, tako često dobijemo korisne informacije o torzijskoj grupi. To je naročito korisno kod razmatranja familija eliptičkih krivulja (o čemu će više riječi biti poslije). Sad razmotrimo dva konkretna primjera.

Primjer 3. Za $E : y^2 = x^3 + 3$ je $D = -3^5$ pa je $E(\mathbf{Q})_{tors} \hookrightarrow \bar{E}(\mathbf{F}_p)$ za $p \geq 5$. Nije teško vidjeti da je $|\bar{E}(\mathbf{F}_5)| = 6$ i $|\bar{E}(\mathbf{F}_7)| = 13$. Zato je racionalna torzijska grupa od E trivijalna (Lutz-Nagellovom metodom postupak bi bio složeniji).

Primjer 4. Za $E : y^2 = x^3/43x + 166$ je $D = -2^{15} \cdot 13$ pa je Lutz-Nagellov postupak dosta složen. Nije teško vidjeti da je $|\bar{E}(\mathbf{F}_3)| = 7$, a

kako točka $(3, 8)$ ima red 7 (provjerite), zaključujemo da je $E(\mathbf{Q})_{tors} = \{O, (3, \pm 8), (-5, \pm 16), (11, \pm 32)\}$.