# Uvod u aritmetiku eliptičkih krivulja

## Grupni zakon na eliptičkoj krivulji - 5. lekcija

**Kubične krivulje (kubike).** To su krivulje zadane jednadžbom oblika

$$F(X, Y, Z) = 0$$

gdje je $F$ homogeni polinom trećeg stupnja (kubična forma). Napominjemo da rješenja gledamo u projektivnoj ravnini (prvenstveno s kompleksnim koordinatama, ali i iz bilo kojega algebarski zatvorenog polja), tj. izbacujemo trivijalno rješenje $(0, 0, 0)$, a netrivijalna proporcionalna rješenja poistovjećujemo. Pripadna afina krivulja zadana je afinom jednadžbom $f(x, y) = 0$.

**Primjer 1.** Evo nekoliko projektivnih kubika i njihovih pridruženih afinih:
(i) $X^3 + Y^3 - \alpha Z^3 = 0,\ (i)'\ x^3 + y^3 - \alpha = 0$
(ii) $X^3 - X^2 Z - Y^2 Z = 0,\ (ii)'\ x^3 - x^2 - y^2 = 0,\ tj.\ y^2 = x^3 - x^2$
(iii) $X^3 + AXZ^2 + BZ^3 - Y^2 Z = 0,\ (iii)'\ x^3 + Ax + B - y^2 = 0,\ tj.\ y^2 = x^3 + Ax + B$.

Skupovna razlika izmedju projektivne i afine krivulje najviše je u 3 točke. Postoji jednostavna korespodencija izmedju svojstava forme $F$ (odnosno polinoma $f$) i geometrije pripadne krivulje $C$:
(I) $F = L^3$, za linearnu formu $L$ —- $C$ je trostruki pravac.
(II) $F = L_1^2 L_2$ —- $C$ je unija dvostrukog pravca i pravca.
(III) $F = L_1 L_2 L_3$ —- $C$ je unija triju pravaca.
(IV) $F = KL$, gdje je $K$ kvadratna forma —- $C$ je unija konike i pravca.
To su bili slučajevi **reducibilnih** krivulja, u nastavku su **ireducibilne**.
(V) $F$ je ireducibilan polinom, ali pripadna krivulja $C : F(X, Y, Z) = 0$ ima singularnu točku. Vidjet ćemo da se taj slučaj svodi na konike; tu je genus (rod) jednak 0.
(VI) $F$ je ireducibilan polinom, a $C$ je nesingularna. U nastavku će nas u pravilu zanimati samo takve krivulje. Tu je genus jednak 1, a pripadne krivulje eliptičke (nakon izbora jedne točke).

**Geometrija i aritmetika**. Kažemo da je kubika $C : F(X, Y, Z) = 0$ definirana nad $\mathbf{Q}$ (ili nad nekim drugim poljem) ako postoji $\lambda \neq 0$, tako da svi koeficijenti od $\lambda F$ budu iz $\mathbf{Q}$, a onda je moguće i da budu iz $\mathbf{Z}$ (ili tog drugog polja). Ako je $C$ definirana nad $\mathbf{Q}$, onda je pripadni aritmetički (diofantski) problem, problem odredjivanja $\mathbf{Q}$-racionalnih točaka, tj. rješenja jednadžbe $F(X,Y,Z) = 0$ za koje postoji reprezentant $(a,b,c)$ gdje su svi $a,b,c$ racionalni brojevi (a onda je moguće i da budu cijeli). Za pripadnu afinu krivulju $C_0 : f(x,y) = 0$ s cjelobrojnim koeficijentima ima smisla i problem odredjivanja cjelobrojnih točaka.

**Primjer 2.** Kubika $Y^2Z = X^3 + 17Z^3$ definirana je nad $\mathbf{Q}$. Lako se vidi da je nesingularna. Točka $O$ u beskonačnosti očito je definirana nad $\mathbf{Q}$, jer je $O = [0,1,0]$. Kako su ostale točke afine, gledamo jednadžbu $y^2 = x^3 + 17$. Vidimo da su $(-1,\pm 4)$ i $(2,\pm 5)$ definirane nad $\mathbf{Q}$ (ujedno i nad $\mathbf{Z}$). Pokušajte odgovoriti na pitanja:
(1.) Je su li ove četiri točke jedine cjelobrojne?
(2.) Postoji li neka druga $\mathbf{Q}$-racionalna točka različite od ovih 5 navedenih?

**Zašto singularna točka pojednostavljuje krivulju?** Neka je $C : F(X,Y,Z) = 0$ ireducibilna kubika i neka je $P$ neka njena točka. Nakon jednostavne projektivne zamjene koordinata, možemo smatrati da je to točka $[0,0,1]$ (objasnite). Zato možemo preći na afinu jednadžbu $f(x,y) = 0$ i njenu točku $P(0,0)$. Razvoj $f = f_3 + f_2 + f_1 + f_0$ oko $P$ ima $f_0 = 0$ (jer krivulja prolazi ishodištem). Zato možemo pisati:

$$f(x,y) = (a_0x^3 + a_1x^2y + a_2xy^2 + a_3y^3) + (b_0x^2 + b_1xy + b_2y^2) + (c_0x + c_1y).$$

Stavimo zamjenu $y = tx$ i dobit ćemo jednadžbu:

$$x^3g_3(t) + x^2g_2(t) + xg_1(t) = 0$$

Ako je $P(0,0)$ singularna, onda je $g_1 = 0$, pa nakon dijeljenja s $x^2$ dobijemo $xg_3(t) + g_2(t) = 0$, odakle dobijemo parametrizaciju

$$x = -\frac{g_2(t)}{g_3(t)},\ y = -\frac{g_2(t)}{g_3(t)} \cdot t$$

što izravno pokazuje da je krivulja $C$ racionalna (ima genus 1).

**Ireducibilne nesingularne kubike - grupni zakon**. Na svaku takvu krivulju $C$ možemo uvesti tzv. grupni "sekantno-tangentni" zakon koji se

zasniva na:
(I) Činjenici da svaki pravac siječe kubiku u tri točke (ako pravilno brojimo kratnosti). Preciznije, pravac općenito cijeće $C$ u trima različitim točkama. Iznimno, ako je pravac tangenta u nekoj točki krivulje, tu brojimo dvostruko, a pravac siječe $C$ u još jednoj točki. Konačno, može se dogoditi da tangenta ne siječe krivulju ni u jednoj drugoj točki. Tada tu točku brojimo trostruko, zovemo je infleksijskom točkom (fleksom). Pokazuje se da svaka kubika ima točno 9 fleksova. Primjer fleksa je beskonačno daleka točka $O[0,1,0]$ na kubici $C: X^3 + AXZ^2 + BZ^3 - Y^2Z = 0$, gdje tangenta $Z = 0$ u toj točki dira krivulju trostruko.
(II) Činjenici (jedinstvena tangenta - nesingularnost) da pri fiksiranoj točki krivulje, svi pravci koji njome prolaze sijeku krivulju u dvjema novim točkama (ili u dvostrukoj točki), a samo je jedan tangenta.
Za grupni zakon najprije biramo po volji točku $O$ krivulje. Time će zakon biti jednoznačno odredjen.
Sad zbroj $P \oplus Q$ točaka $P, Q$ definiramo ovako (za slike pogledajte [Silverman-Tate, str. 16-21]):
**1. korak.** Neka je $R$ treća točka presjeka pravca kroz $P$ i $Q$ s krivuljom. Tu točku označavat ćemo kao $P * Q$.
**2. korak.** $P \oplus Q$ definiramo kao treću točku presjeka pravca kroz $R$ i $O$ s krivuljom.
Tom načelnom zakonu treba dodati sljedeće posebne slučajeve:
(i) ako je $P = Q$, onda $P \oplus Q$ postaje $P \oplus P = 2P$ tako da u 1. koraku povlačimo tangentu u $P$; iznimno, ako je $P$ fleks, definiramo $P * P = P$ (treća točka presjeka opet je $P$).
(ii) ako bude $P * Q = O$, onda u 2. koraku povlačimo tangentu kroz $O$.
Sad je lako pokazati sljedeće:
($G_0$) $(P, Q) \mapsto P \oplus Q$ dobro je definirano.
($G_1$) $\oplus$ je komutativna operacija.
($G_2$) $O$ je neutralni element: $P \oplus O = P$.
($G_3$) Za svaki $P$ jednoznačno je definiran suprotni element ovako: neka je $S$ treća točka presjeka tangente u $O$ s krivuljom; $-P$ je treća točka presjeka pravca kroz $P$ i $S$ s krivuljom. Iznimno, ako je $O$ fleks, onda je $S = O$ pa su $P, O$ i $-P$ na istom pravcu.
Jedino je netrivijalan zakon asocijativnosti
($G_4$) $P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$ za sve $P, Q, R$,
i izgleda da se ne može elementarno geometrijski dokazati.
**Lagani dio zakona asocijativnosti.** Zakon asocijativnosti očit je u poseb-

nim slučajevima:

$$P \oplus (Q \oplus R) = (P \oplus Q) \oplus R \text{ ako je } P, Q, \text{ ili } R \text{ jednako } O \tag{1}$$

$$-P \oplus (P \oplus R) = R = (-P \oplus P) \oplus R \tag{2}$$

Radi jednostavnosti, (2) ćemo obrazložiti ako je $O$ fleks. Uočimo sljedeće: Ako je $P \oplus R = T$ onda su $P, R$ i $-T$ na istom pravcu. Zato su $-P, -R$ i $-(-T) = T$ na istom pravcu, pa je $-P \oplus T = -(-R) = R$. Dakle, $-P \oplus (P \oplus R) = R$.
Tipičan geometrijski dokaz zakona asocijativnosti je pomoću tzv. "teorema o devet točaka", koji se izvodi iz Bezout-ova teorema, a za koji je potrebno razviti teoriju presjeka ravninskih krivulja (vidi [Silverman-Tate, Appendix]). Taj dokaz je revizija dobrog dijela klasične projektivne geometrije u ravnini 17. i 18. stoljeća. Moderniji dokaz koristi se teorijom divizora na algebarskim krivuljama i teoremom Riemanna-Rocha (vidi [Silverman, III, Prop.3.4.]). Mi ćemo dati jedan drugi dokaz nakon uvodjenja Weierstrassova modela.

**Weierstrassov model.**
Neka je $C : F(X, Y, Z) = 0$ ireducibilna nesingularna kubika s istaknutom točkom $O$. Tada se pokazuje:
(I) Ako je $O$ fleks onda se $C$ projektivnim transformacijama ravnine može dovesti u oblik

$$E : Y^2Z = X^3 + AXZ^2 + BZ^3, \text{ uz } 4A^3 + 27B^2 \neq 0 \tag{3}$$

Pri tom flex $O$ prelazi u beskonačno daleku točku $O[0, 1, 0]$.
Pripadna afina jednadžba je

$$E_0 : y^2 = x^3 + Ax + B \tag{4}$$

(II) Ako $O$ nije fleks, opet se $C$ dovodi u oblik (3) samo što nisu dovoljne projektivne transformacije, već tzv. "biracionalne transformacije" (kvocijenti polinoma).
(3) se naziva Weierstrassova jednadžba eliptičke krivulje (ili Weierstrassov model) i postoji u svakoj karakteristici različitoj od 2 i 3; uvjet $4A^3+27B^2 \neq 0$ je uvjet nesingularnosti (to znači da se i ostale ireducibilne kubike svode na ovaj oblik, ali su nesingularne akko zadovoljavaju taj uvjet).

(I) ćemo ilustrirati primjerom.
**Primjer 3. [Silverman-Tate, str. 24]** Neka je $C: X^3 + Y^3 - \alpha Z^3 = 0$. Uz (projektivnu) zamjenu koordinata

$$X = W + V,\ Y = W - V,\ Z = U$$

dobijemo jednadžbu

$$4V^2W = \frac{\alpha}{6}U^3 + \frac{1}{3}W^3$$

ili, nakon dijeljenja s $W^3$, afinu jednadžbu

$$v^2 = \frac{\alpha}{6}u^3 - \frac{1}{3}.$$

Sad, množenjem s $6^4\alpha^2$ (za $\alpha \neq 0$) dobijemo $(6^2\alpha v)^2 = (6\alpha)^3 - 432\alpha^2$, odnosno afinu jednadžbu eliptičke krivulje

$$y^2 = x^3 - 432\alpha^2.$$

Pripadna homogena jednadžba je:

$$E: Y^2Z = X^3 - 432\alpha^2Z^3.$$

Krivulje $C$ i $E$ su projektivno ekvivalentne (izomorfne). Pri tom je flex $[-1, 1, 0]$ na $C$ prešao u flex $[0, 1, 0]$ na $E$.
Uočite da je za $\alpha = 0$ početna krivulja reducibilna, a ova završna je ireducibilna. To se dogodilo zbog množenja nulom; lako je vidjeti da je $C$ tada ekvivalentna krivulji, $C': V^2W = \frac{1}{3}W^3$ (takodjer reducibilnoj).

**Napomena.** Lako je vidjeti da je $E$ iz (3) nesingularna akko je polinom $f(x) := x^3 + Ax + B$ iz (4) bez višestrukih nultočaka. Naime, već znamo da je $O[0, 1, 0]$ nesingularna pa treba gledati samo afine točke. Dalje, za polinom $g(x, y) := y^2 - f(x)$ vrijedi: sustav $\frac{\partial g}{\partial x} = \frac{\partial g}{\partial y} = 0$ akko sustav $f(x) = f'(x) = 0$ ima rješenje, a to je akko $f$ ima višestruku nultočku.

**Zadatak.** Dokažite da je uvjet nesingularnosti krivulje $E$ (iz (3)), odnosno $E_0$ (iz (4)) upravo $4A^3 + 27B^2 \neq 0$.

**Aritmetički slučaj.**
Ako je $C: F(X, Y, Z) = 0$ definirana nad $\mathbf{Q}$, onda imamo dva slučaja:
**1. slučaj.** Postoji bar jedna $\mathbf{Q}$ racionalna točka na $C$. Tada $C$ ima Weierstrassov model i riječ je o **eliptičkoj krivulji nad Q**. Postoje dva slučaja

tehnički različita:
(i) ako je bar jedan od fleksova $O$ definiran nad $\mathbf{Q}$, onda se do Weiersstrasova modela nad $\mathbf{Q}$ dolazi projektivnim transformacijama ravnine s koeficijentima iz $\mathbf{Q}$ i pri tom se može izabrati da taj flex prelazi u beskonačno daleku W. modela $[0, 1, 0]$ (tako je bilo u primjeru 3. uz racionalan $\alpha \neq 0$).
(ii) ako ni jedan od fleksova nije definiran nad $\mathbf{Q}$, onda se do W. modela dolazi biracionalnim transformacijama ravnine s koeficijentima iz $\mathbf{Q}$.
(II) $C$ nema ni jednu $\mathbf{Q}$-racionalnu točku. Tada $C$ nema Weierstrassov model nad $\mathbf{Q}$, i nije eliptička krivulja nad $\mathbf{Q}$ (već samo nad $\mathbf{C}$, odnosno nad nekim algebarskim proširenjem od $\mathbf{Q}$), iako je $C$ krivulja genusa 1 nad $\mathbf{Q}$.

**Primjer 4. (Selmer)** Neka je $C : 3X^3 + 4Y^3 + 5Z^3 = 0$. Tada $C$ nema $\mathbf{Q}$-racionalnu točku i nije eliptička krivulja nad $\mathbf{Q}$ (već samo nad nekim proširenjem nad kojim ima $\mathbf{Q}$-racionalnu točku, pa i W. model, na primjer nad $\mathbf{Q}(\sqrt[3]{6})$).