Uvod u aritmetiku eliptičkih krivulja

Grupni zakon na eliptičkoj krivulji II - 6. lekcija

Analitički zapis grupnog zakona.
Od sad nadalje, ako drukčije ne kažemo, eliptička krivulja E je zadana afinom Weierstrassovom jednadžbom

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

gdje je $f(x) := x^3 + ax^2 + bx + c = (x - e_1)(x - e_2)(x - e_3)$ kubni polinom s različitim korijenima (ili, u skraćenom obliku $y^2 = x^3 + Ax + B$). U oba slučaja $O = [0, 1, 0]$ je jedina točka u beskonačnosti i nju smatramo istaknutom. Zato pod grupnim zakonom mislimo na onaj u kojemu je O neutralni element. Napominjemo da se u O sijeku afini pravci usporedni s y-osi. Naime, pravac

$$\alpha X + \beta Y + \gamma Z = 0$$

sadrži O ako i samo ako je $\beta = 0$, pa to može biti beskonačno daleki pravac $Z = 0$ ili pravci $X = -\frac{\gamma}{\alpha} Z$, tj. $x = -\frac{\gamma}{\alpha}$.
Zato za grupni zakon vrijedi:
(I) Ako je $P(x, y)$ afina točka, onda je $-P(x, -y)$ suprotna točka.
(I) Ako su P, Q afine točke onda se $P \oplus Q$ dobije kao točka presjeka krivulje i usporednice s y-osi kroz $P * Q$. Rezultat je afina točka, osim ako je $Q = -P$, posebno ako je $P = Q = (e_i, 0)$ za neki $i = 1, 2, 3$.
Uočite, takodjer, da su točke $O, (e_1, 0), (e_2, 0), (e_3, 0)$ rješenja jednadžbe $2P = 0$.

Teorem 1. (i) Neka su $P(x_1, y_1), Q(x_2, y_2)$ afine točke i $Q \neq -P$. Tada je i $(P \oplus Q)(x_3, y_3)$ afina i vrijedi:

$$x_3 = -x_1 - x_2 + \lambda^2 - a, \; y_3 = \lambda(x_1 - x_3) - y_1$$

gdje je $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ ako je $P \neq Q$, i $\lambda = \frac{f'(x_1)}{2y_1}$ ako je $P = Q$.
(ii) Ako je krivulja E definirana nad $\mathbf{Q}$ i ako su P, Q definirane nad $\mathbf{Q}$, onda je i $P \oplus Q$ definirana nad $\mathbf{Q}$, odnosno $2P$ je definirana nad $\mathbf{Q}$..
Dokaz. (i) Riješimo sustav jednadžba

$$y^2 = x^3 + ax^2 + bx + c, \; y = \lambda x + \nu$$

gdje je druga jednadžba jednadžba pravca kroz P, Q. Kako taj pravac siječe krivulju u točkama s prvim koordinatama x_1, x_2, x_3, nakon eliminiranja varijable y iz Vieteovih formula dobijemo

$$x_1 + x_2 + x_3 = \lambda^2 - a$$

, sto smo i trebali. Sad samo treba primijeniti činjenicu da za $P \neq Q$ vrijedi $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, a ako je $P = Q$, pravac je tangenta u (x_1, y_1) pa je $\lambda = \frac{f'(x_1)}{2y_1}$.
(ii) vidi se iz formula.

Napomena Ako označimo koordinate afine točke T kao $x(T), y(T)$ onda je

$$x(2P) = \frac{1}{4}\frac{x^4 - 2bx^2 - 8cx + (b^2 - 4ac}{x^3 + ax^2 + bx + c}$$

To se dobije izravnim računanjem.

Važnost grupnog zakona na eliptičkoj krivulji prvenstveno je u tomu što se iz dviju točaka može dobiti nova točka, odnosno iz zadane točke nova (dvostruka) točka. To je, na neki način, u dalekoj prošlosti otkrio i primijenio Diofant.
Primjer 1. Neka je E zadana afinom jednadžbom $y^2 = x^3 + 17$. Očite točke su $P(-1, 4)$ i $Q(2, 5)$. Neka je $(P \oplus Q)(x_3, y_3)$. Tada je, prema teoremu 1 $(x_3, y_3) = (-\frac{8}{9}, \frac{109}{27}$. Takodjer je $2P(\frac{137}{64}, -\frac{2651}{51})$. Postavlja se pitanje možemo li pomoću P, Q povlačenjem sekanata i tangenata dobiti svaku točku krivulje E se racionalnim koordinatama ($\mathbf{Q}$-racionalne točke).

Dokaz zakona asocijativnosti.
Definicija 1. Neka su C_1, C_2 dvije (ne nužno ravninske) algebarske krivulje. Kažemo da je $\phi : C_1 \to C_2$ racionalno preslikavanje, ako se lokalno može zadati racionalnim funkcijama. Kažemo da je ϕ morfizam ako definirana na cijelom C_1 (ili ako se može proširiti).

Primjer 2. Ako je E eliptička krivulja onda je $\phi : E \to E$, $\phi(P) = 2P$ racionalno preslikavanje. Naime, na afinom dijelu je ϕ, ako je $2P \neq O$, prema teoremu 1, zadano kao $\phi(x, y) = (\phi_1(x, y), \phi_2(x, y)$ gdje su ϕ_1, ϕ_2 racionalne funkcije od x, y, tj. one su racionalne funkcije na E.

Za dokaz asocijativnosti potrebna nam je standardna (iako ne elementarna) lema o preslikavanjima algebarskih krivulja.

Lema 1. Neka su C_1, C_2 nesingularne projektivne krivulje. Tada:
(i) Svako racionalno preslikavanje $\phi : C_1 \to C_2$ proširuje se do morfizma.
(ii) Morfizam ϕ je konstanta ili surjekcija.
(iii) Ako je ψ drugi morfizam i $\psi \neq \phi$, onda je skup svih P tako da je $\phi(P) = \psi(P)$ konačan.
Ovu lemu nećemo dokazivati.

Prije dokaza napominjemo opet već poznatu činjenicu da je asocijativnost

$$P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$$

evidentna ako je neka od točaka fleks O ili u posebnom slučaju

$$-P \oplus (P \oplus R) = R = (-P \oplus P) \oplus R, \tag{1}$$

odakle, kao poseban slučaj vidimo da je $P \oplus (-Q) = O$ akko $P = Q$.

Dokaz asocijativnosti. Iz (1) slijedi da možemo predpostaviti da je $Q, R \neq O$ i $Q \oplus R \neq O$. Definirajmo (za sad skupovno) preslikavanje

$$h : E \to E,\ h(P) := [P \oplus (Q \oplus R)] \oplus [-(P \oplus Q) \oplus R] \tag{2}$$

Iz (1) izlazi da je dovoljno dokazati da je $h(P) = O$ za sve P. Očito je $h(O) = O$. Takodjer, h ne postiže $-R$. Naime iz jednakosti $h(P) = -R$ i (1) slijedi

$$P \oplus (Q \oplus R) = ((P \oplus Q) \oplus R) \oplus (-R) = P \oplus Q$$

a odavde, $Q \oplus R = Q$, tj. $R = O$, što je kontradikcija.
Iz Leme (i) i (ii), vidi se da je za dokazivanje zakona, dovoljno dokazati da je h racionalno preslikavanje. Prvo uočite da je $\phi : E \to E$ definirano kao $P \mapsto P \oplus (Q \oplus R)$ morfizam algebarskih krivulja. Naime, iz (4)-(5), ϕ je racionalno preslikavanje regularno za $P \neq O, \pm(Q \oplus R)$, pa je po Lemi (i), ϕ definirano na cijelom E. Slično, preslikavanje $\psi : E \to E$ definirano kao $P \mapsto (P \oplus Q) \oplus R$ je morfizam algebarskih krivulja.
Sad, ako je $\phi = \psi$ sve je u redu.
Ako je pak $\phi = -\psi$, onda je, prema (6)-(7) h racionalno preslikavanje .
Predpostavimo konačno da je $\phi \neq \psi$ i $\phi \neq -\psi$. Onda iz Leme (iii) slijedi da je $\phi(P) \neq \pm\psi(P)$ za gotovo sve P. Sad iz (4)-(5) vidimo da je h racionalno preslikavanje.