Visine

$x = \frac{m}{n} \in \mathbb{Q}, \quad (m,n) = 1$

$H(x) = H\left(\frac{m}{n}\right) = \max\{|m|, |n|\} \in \mathbb{Z}_{>0}$

- visina racionalnog broja x

Ako je

$E: y^2 = f(x) = x^3 + ax^2 + bx + c, \quad a,b,c \in \mathbb{Z}$

eliptička krivа i $P = (x,y) \in E(\mathbb{Q})$ onda definišimo visinu racionalne tačke P sa

$$H(P) := H(x) \qquad (H(\mathcal{O}) = 1)$$

- Ova visina se 'ponaša multiplikativno': $H(P+Q)$ je uporedivo sa $H(P) \cdot H(Q)$

Zato se koristi i visina koja se 'ponaša aditivno':

$$h(P) := \log H(P) \in \mathbb{R}_{\geq 0}$$

(L.1) Za svako $M \in \mathbb{R}_{>0}$ skup

$$\{P \in E(\mathbb{Q}) : h(P) \leq M\}$$ je konačan.

▽ Važi $\Leftrightarrow$ $H(P) \leq e^M$; konačan broj mogućnosti za x-koordinatu; za svaku x-koordinatu, najviše 2 mogućnosti za y-koordinatu △

Visine — alat kojim geometrijske informacije prebacujemo u aritmetičke informacije

(što je veća visina, veća je 'aritmetička kompleksnost')

- Racionalna tačka na E mora biti oblika

$$P = \left(\frac{m}{e^2}, \frac{n}{e^3} \right)$$

Specijalno imamo $\boxed{|m|, e^2 \leq H(P)}$

Zamenom u j-nu za E; množenjem sa e^6 dobijamo:

$$n^2 = m^3 + ae^2m^2 + be^4m + ce^6$$

odakle je

$$|n^2| \leq |m^3| + |ae^2m^2| + |be^4m| + |ce^6|$$

$$\leq H(P)^3 + |a| H(P)^3 + |b| H(P)^3 + |c| H(P)^3$$

$$= (1 + |a| + |b| + |c|) H(P)^3$$

tj. za svaku racionalnu tačku P na $E(\mathbb{Q})$ važi:

$$\boxed{|n| \leq K \cdot H(P)^{\frac{3}{2}}}$$

za apsolutnu konstantu $K = \sqrt{1 + |a| + |b| + |c|}$.

L.2 Neka je P_0 fiksirana racionalna tačka na $E(\mathbb{Q})$

Onda postoji konstanta $\kappa_0 = \kappa_0(P_0, a, b, c)$ takva da je

$$h(P+P_0) \leq 2\,h(P) + \kappa_0, \qquad \forall P \in E(\mathbb{Q}) \tag{1}$$

▼ Trivijalno ako $P_0 = \mathcal{O}$. Zato neka je $P_0 = (x_0, y_0) \neq \mathcal{O}$

Dovoljno je dokazati (1) za tačke $P \notin \{P_0, -P_0, \mathcal{O}\}$

(Konačno mnogo izuzetaka je o.k:

$$\kappa_0 = \max\{\kappa_0(\text{sa izuzecima}),\ h(P+P_0) - 2h(P)\}$$
P - prolazi sa svim konačno mnogo izuzetaka)

- $P = (x, y)$, $x \neq x_0$ (zbog $P \neq \pm P_0$)

$P + P_0 = (\xi, \eta)$

$$\xi + x + x_0 = \lambda^2 - a, \qquad \lambda = \frac{y - y_0}{x - x_0}$$

$$\xi = \frac{(y-y_0)^2}{(x-x_0)^2} - a - x - x_0 = \frac{(y-y_0)^2 - (x-x_0)^2(x+x_0+a)}{(x-x_0)^2}$$

$y^2 - x^3$ u brojiocu zamenimo sa $ax^2 + bx + c$ (jer je $P \in E$)

Dakle

$$\xi = \frac{A y + B x^2 + C x + D}{E x^2 + F x + G}$$

gdje su A, B, C, D, E, F, G – racionalni brojevi koji ovise samo o a, b, c, x_0, y_0

Množenjem NZS-ominitelja, možemo da pretpostavimo da su svi $A, B, \ldots, G \in \mathbb{Z}$.

$$P = (x, y) = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$$

$$\xi = \frac{A n e + B m^2 + C m e^2 + D e^4}{E m^2 + F m e^2 + G e^4}$$

— ne mora biti u pobraćenom obliku, ali pobraćivanje samo smanji $H(P)$

$$H(\xi) \leq \max\left\{\left|A n e + B m^2 + C m e^2 + D e^4\right|, \left|E m^2 + F m e^2 + G e^4\right|\right\}$$

$$e \leq H(P)^{\frac{1}{2}}, \quad |n| \leq K \cdot H(P)^{\frac{3}{2}}, \quad |m| \leq H(P)$$

pa

$$H(P + P_0) = H(\xi) \leq \underbrace{\max\left\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\right\}}_{K_0 = \log(\text{ove konstante})} H(P)^2$$

zavisi samo od $a, b, c : (x_0, y_0)$

L.3 Postoji konstanta $\kappa = \kappa(a, b, c)$ takva da je

$$\boxed{h(2P) \geq 4h(P) - \kappa, \quad \forall P \in E(\mathbb{Q})}$$

- U dokazu možemo izuzeti ponovo bilo kojih konačno mnogo tačaka (eventualnim povećavanjem konstante κ da bude $> h(2P)$, za sve izuzetke P).

Izuzećemo konačno mnogo tačaka P koje zadovoljavaju $2P = \mathcal{O}$.

- $P = (x, y)$, $\quad 2P = (\xi, \eta)$

Iz formule za duplirane tačke znamo da je

$$\xi + 2x = \lambda^2 - a, \qquad \lambda = \frac{f'(x)}{2y} \quad \left(\begin{array}{l} f(x) \neq 0 \\ y \neq 0 \text{ jer} \\ 2P \neq \mathcal{O} \end{array}\right)$$

$$\xi = \frac{f'(x)^2}{4y^2} - 2x - a = \frac{f'(x)^2 - (8x + 4a) f(x)}{4 f(x)}$$

$$f'(x) = 3x^2 + 2ax + b$$

$$\xi = \frac{x^4 + \dots}{4x^3 + 4ax^2 + 4bx} \quad \text{– količnik dva polinoma iz } \mathbb{Z}[x]$$

Ovi polinomi nemaju zajednički (kompleksni) koren, jer su f i f' uzajamno prosti (E je glatka, f nema višestruke korene!)

Sada, $h(P) = h(x)$, $h(2P) = h(\xi)$

tj. za sve racionalne brojeve $x = \frac{m}{n}$ treba dokazati da važi $(m,n)=1$

$$h\left(\frac{x^4+\dots}{4x^3+\dots}\right) \geq 4h(x) - \kappa$$

Ideja: Brojilac raste $\sim x^4$, pa je za očekivati da je

$$H\left(\frac{x^4+\dots}{4x^3+\dots}\right) = \max\{|\text{brojioc}|, |\text{imenioc}|\} \sim |x|^4 \pm \text{malo}$$

odakle je $h\left(\frac{x^4+\dots}{4x^3+\dots}\right) \sim 4h(x) \pm \text{malo}$.

Ali ova strategija bi radila samo ako u razlomku $\frac{x^4+\dots}{4x^3+\dots}$ ne bi bilo preveliko poklapanja

(inače bi veličina i brojioca i imenioca, pa time i H mogla da bolapsira). Naravno generički ne očekujemo da se to desi. Ideja je da to formalizujemo.

- Neka su zato (opštije)

$$\phi(X), \psi(X) \in \mathbb{Z}[X]$$ bez zajedničkih korena u $\mathbb{C}$

$$d = \max\{\deg\phi, \deg\psi\}$$

Zbog definicije H, možemo pretp. da je

$$\deg(\phi) = d, \quad \deg(\psi) = e \leq d$$

Označićemo:

$$\Phi(m,n) := n^d \phi\left(\frac{m}{n}\right) = a_0 m^d + a_1 m^{d-1} n + \ldots + a_d n^d$$

$$\Psi(m,n) := n^d \psi\left(\frac{m}{n}\right) = b_0 m^e n^{d-e} + b_1 m^{e-1} n^{d-e+1} + \ldots + b_e n^d$$

gdje su $a_i, b_j \in \mathbb{Z}$.

Interesuje nas potpadanje razlomka

$$\frac{\phi\left(\frac{m}{n}\right)}{\psi\left(\frac{m}{n}\right)} = \frac{n^d \phi\left(\frac{m}{n}\right)}{n^d \psi\left(\frac{m}{n}\right)} = \frac{\Phi(m,n)}{\Psi(m,n)}$$

- Kako $\phi(X), \psi(X)$ nemaju zajedničke korijene u $\mathbb{C}$, ovi polinomi su stojamo prosti u $\mathbb{Q}[X]$, pa postoje $F(X), G(X) \in \mathbb{Q}[X]$ takvi da je

$$F(X)\,\phi(X) + G(X)\,\psi(X) = 1 \qquad \left(\text{Euklidov algoritam}\right) \quad (*)$$

- Neka je još $A \in \mathbb{Z}_{>0}$ takvo da su

$$A \cdot F(X),\ A \cdot G(X) \in \mathbb{Z}[X]$$

$$D = \max\{\deg F, \deg G\}$$

(A: D zavisi samo od polinoma ϕ, ψ, ne od m, n)

Stavimo u $(*)$ $X = \frac{m}{n}$: (i pomnožimo sa $A \cdot n^{D+d}$)

$$n^D A\cdot F\left(\frac{m}{n}\right)\cdot \underbrace{n^d \Phi\left(\frac{m}{n}\right)}_{\overline{\Phi}(m,n)} + n^D A\cdot G\left(\frac{m}{n}\right)\cdot \underbrace{n^d \Psi\left(\frac{m}{n}\right)}_{\overline{\Psi}(m,n)} = A\, n^{D+d}$$

$$\gamma = \gamma(m,n) = NZD\left(\overline{\Phi}(m,n),\ \overline{\Psi}(m,n)\right)$$

↑ to je ono što smo dobili 'pobratimo'

Sledi: $\boxed{\gamma \mid A\, n^{D+d}}$

Ali:

$$\gamma \mid A\, n^{D+d-1}\overline{\Phi}(m,n) = A\, n^{D+d-1}\cdot a_0 m^d + A\, n^{D+d}\cdot a_1 m^{d-1} + A\, n^{D+d+1}\cdot a_2 \cdot m^{d-2} + \dots + A\, n^{D+2d-1}\cdot a_d$$

} sve deljivo sa γ

$$\longrightarrow \gamma \mid NZD\left(A n^{D+d},\ A a_0 m^d n^{D+d-1}\right) =$$

$$= A\, n^{D+d-1}\ NZD\left(n,\ a_0 m^d\right)$$

Ali $(m,n)=1$ pa sledi $\boxed{\gamma \mid A a_0 n^{D+d-1}}$

Ponovimo isti trik: iz

$$\gamma \mid A a_0 n^{D+d-2} \Phi(m,n),$$

istim argumentom nalazimo da:

$$\boxed{\gamma \mid A a_0^2 n^{D+d-2}}$$

Ponavljajem ovog argumenta, nalazimo da ipak

$$\boxed{\gamma \mid A \cdot a_0^{D+d} =: R}$$ – pritom broj koji ne zavisi od m,n (samo od polinoma ϕ, ψ koji su fiksirani)

Dakle dokazali smo:

(L4) Pod navedenim pretpostavkama, za sve $(m,n)=1$ vrijedi

$$\boxed{NZD\left(\Phi(m,n), \Psi(m,n)\right) \mid R}$$

(L.3') Neka su $\phi(x), \psi(x) \in \mathbb{Z}[x]$, bez zajedničkog korijena u $\mathbb{C}$; $d = \max\{\deg\phi, \deg\psi\}$.
Onda $\exists$ konstanta κ koja zavisi samo od polinoma ϕ, ψ takva da je za sve racionalne brojeve $\frac{m}{n} \in \mathbb{Q}$, (koji nisu korijeni $\psi(x)$) istinito

$$\boxed{h\left(\frac{\phi\left(\frac{m}{n}\right)}{\psi\left(\frac{m}{n}\right)}\right) \geq d \cdot h\left(\frac{m}{n}\right) - \kappa}$$

(L.3) je dable specijalni slučaj (L.3')

- dovoljno je dokazati za sve osim konačno mnogo izuzetaka $\frac{m}{n}$, pa neka $\frac{m}{n}$ nije koren od ϕ
- zbog simetrije visina, možemo pretp. da je $\deg \phi = d$, $\deg \psi = e \leq d$
- želimo da ocenimo visinu

$$\Xi := \frac{\phi\left(\frac{m}{n}\right)}{\psi\left(\frac{m}{n}\right)} = \frac{\Phi(m,n)}{\Psi(m,n)}$$

Zbog (L.4), ovde je 'skraćivanje' najviše R pa je

$$H(\Xi) \geq \frac{1}{R} \max\left\{ |\Phi(m,n)|, |\Psi(m,n)| \right\}$$

$$\geq \frac{1}{2R} \left(\left| n^d \phi\left(\frac{m}{n}\right) \right| + \left| n^d \psi\left(\frac{m}{n}\right) \right| \right)$$

- Ovo hoćemo da uporedimo sa

$$H\left(\frac{m}{n}\right)^d = \max\left\{ |m|^d, |n|^d \right\}$$

Posmatramo količnik

$$\frac{H(\Xi)}{H\left(\frac{m}{n}\right)^d} \geq \frac{1}{2R} \cdot \frac{\left|\phi\left(\frac{m}{n}\right)\right| + \left|\psi\left(\frac{m}{n}\right)\right|}{\max\left\{ \left|\frac{m}{n}\right|^d, 1 \right\}}$$

- $$p(t) := \frac{|\phi(t)| + |\psi(t)|}{\max\left\{ |t|^d, 1 \right\}}$$

$$\lim_{|t|\to\infty} p(t) = \begin{cases} |a_0|+|b_0|, & \text{ako je } \deg\psi = \deg\phi = d \\ |a_0|, & \text{ako je } \deg\psi < d \end{cases}$$

U svakom slučaju $\exists$ kompaktan (zatvoren) interval I takav da je $p(t) \neq 0$ (npr. $> \frac{1}{2}|a_0|$) van I.

Na I, $p(t)$ je neprekidna i nikad nije $=0$ (jer ϕ, ψ nemaju zajedničku nulu), pa dostiže minimum koji je > 0.

Sve zajedno: $p(t) \geq c_1 > 0$, $\forall t \in \mathbb{R}$, pa je

$$\frac{H\left(\frac{m}{n}\right)}{H\left(\frac{m}{n}\right)^d} \geq \frac{1}{2R}\, p\left(\frac{m}{n}\right) \geq \frac{c_1}{2R}$$

Uzmemo log, $K_1 = \log \frac{2R}{c_1}$. ◢

T. 5 [Teorema spusta] Neka je A komutativna grupa i neka postoji funkcija $h : A \to [0, +\infty)$ koja zadovoljava:

(a) Za svako $M \in \mathbb{R}_{\geq 0}$, skup $\{P \in A \mid h(P) \leq M\}$ je konačan

(b) Za svako $P_0 \in A$, $\exists$ konstanta K_0 takva da je

$$h(P+P_0) \leq 2h(P) + K_0, \quad \forall P \in A$$

(c) $\exists$ konstanta K takva da je

$$h(2P) \geq 4h(P) - K, \quad \forall P \in A.$$

Neka još dodatno vrijedi

(d) $[A : 2A] < \infty$

Onda je A konačno generirana.

Posljedica [Mordell-ova teorema] Grupa $E(\mathbb{Q})$ je konačno - generirana.

Neka je $[A : 2A] = n$ i neka su $Q_1, Q_2, \ldots, Q_n$ predstavnici svih različitih koseta

- Dakle, za proizvoljno $P \in A$, $\exists i_1$ t.d.

$$P - Q_{i_1} \in 2A, \qquad P - Q_{i_1} = 2P_1, \text{ za neke } P_1 \in A$$

- Za P_1, $\exists i_2$ t.d.

$$P_1 - Q_{i_2} = 2P_2, \text{ za neke } P_2 \in A$$

- $P_2 - Q_{i_3} = 2P_3, \quad P_3 \in A$

$$\vdots$$

$$P_{m-1} - Q_{i_m} = 2P_m, \quad P_m \in A$$

Kad zamenimo natrag:

$$P = Q_{i_1} + 2P_1 = Q_{i_1} + 2Q_{i_2} + 4P_2 = \ldots$$

$$= Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \ldots + 2^{m-1}Q_{i_m} + 2^m P_m$$

Specijalno

$$P \in \langle Q_1, Q_2, \dots, Q_n, P_m \rangle \qquad (*)$$

- Primenom (c) za $P_0 = -Q_i$ dobijamo da postoje konstante κ_i, $1 \le i \le n$ takve da je:

$$h(P - Q_i) \le 2\, h(P) + \kappa_i, \qquad \forall P \in A$$

$$\kappa' := \max\{\kappa_1, \kappa_2, \dots, \kappa_n\}$$

- Primenom (c) na $P = P_j$:

$$4\, h(P_j) \le h(2P_j) + \kappa$$

$$= h(P_{j-1} - Q_{i_j}) + \kappa$$

$$\le 2\, h(P_{j-1}) + \kappa' + \kappa$$

$\Leftrightarrow$

$$h(P_j) \le \frac{1}{2} h(P_{j-1}) + \frac{\kappa' + \kappa}{4}$$

$$= \frac{3}{4} h(P_{j-1}) - \frac{1}{4}\left(h(P_{j-1}) - (\kappa' + \kappa)\right)$$

pa ako je $h(P_{j-1}) \ge \kappa' + \kappa$, onda je $h(P_j) \le \frac{3}{4} h(P_{j-1})$

- Dakle u niz $P_1, P_{1_1}, P_{2_1}, P_{3_1}, \dots$ mora da se pojavi tačka P_m za koju je $h(P_m) \le \kappa' + \kappa$. $(**)$

Ali onda $(*)$ + $(**)$ tvrdi da

$$\{Q_1, Q_2, \dots, Q_n\} \cup \underbrace{\{R \in A \mid h(R) \le \kappa' + \kappa\}}_{\text{konačan, pa (L.1)}}$$

generišu A.