

A leideni hozomány (részlet)

Tengely Szabolcs
tengely@math.klte.hu

Debreceni Egyetem

Alapfogalmak

$$\mathcal{C} : Y^2 = F(X),$$

ahol

$$F(X) = f_0 + f_1X + \dots + f_6X^6 \in \mathbb{Q}[X]$$

Divizor:

$$\sum_{P \in \mathcal{C}(\overline{\mathbb{Q}})} n_P P$$

$Pic_{\mathbb{Q}}^0(\mathcal{C})$: azon divizorok csoportja (lineáris ekvivalencia erejéig), amelyeknek a foka 0, azaz $\sum_P n_P = 0$.

Reprezentáció: $\{(x_1, y_1), (x_2, y_2)\} = (x_1, y_1) + (x_2, y_2) - \infty^+ - \infty^-$.

$Pic_{\mathbb{Q}}^0(\mathcal{C})$: azon részcsoportja $Pic_{\mathbb{Q}}^0(\mathcal{C})$ -nak, amelyben a pontpár $\mathbb{Q}$ felett definiált vagy $\mathbb{Q}$ másodfokú bővítéséből való.

$$\mathcal{O} = \{(x, y), (x, -y)\}.$$

Példa

$$\mathcal{C}: Y^2 = -X^6 + 2X^3 + 3.$$

$J(\mathbb{Q})$ néhány eleme:

$$\mathcal{O} = \{(1, 2), (1, -2)\}, D = \{(-1, 0), (1, -2)\}, T = \{(\frac{1-\sqrt{-3}}{2}, 0), (\frac{1+\sqrt{-3}}{2}, 0)\}.$$

FONTOS! $\{(\frac{1-\sqrt{-3}}{2}, 0), (1, 2)\} \notin J(\mathbb{Q})$.

$$\begin{aligned} \text{Összeadás: } T + T &= \{(\frac{1-\sqrt{-3}}{2}, 0), (\frac{1+\sqrt{-3}}{2}, 0)\} + \{(\frac{1-\sqrt{-3}}{2}, 0), (\frac{1+\sqrt{-3}}{2}, 0)\} = \\ &= \{(\frac{1-\sqrt{-3}}{2}, 0), (\frac{1-\sqrt{-3}}{2}, 0)\} + \{(\frac{1+\sqrt{-3}}{2}, 0), (\frac{1+\sqrt{-3}}{2}, 0)\} = \mathcal{O} + \mathcal{O} = \mathcal{O}. \end{aligned}$$

$T + D$ kiszámítása: $Y = -X^3 - 1$ metszi $\mathcal{C}$ -t a D és T pontjaiban, ezt behelyettesítve az $Y^2 = F(X)$ polinomba kapjuk, hogy

$$(X - 1)(X + 1)(X - \alpha)(X - \bar{\alpha})(2X^2 + 2X + 2) = 0,$$

így megkapjuk a keresett x -koordinátákat: $\beta_1 = \frac{-1-\sqrt{-3}}{2}, \beta_2 = \frac{-1+\sqrt{-3}}{2}$.

Azaz $T + D = \{(\beta_1, 2), (\beta_2, 2)\}$.

Torziós részcsoporth

Legyen p egy prím, amelyre $p \nmid 2\Delta(F)$, ekkor $\mathcal{C} \bmod p$ egy görbe, $\tilde{\mathcal{C}}$, amelynek a génusza 2.

$$\sim: J(\mathbb{Q}) \longrightarrow \tilde{J}(\mathbb{F}_p),$$

a redukció injektív a torziós csoporton, azaz $\#J(\mathbb{Q})_{tors} \mid \#\tilde{J}(\mathbb{F}_p)$.

Az utóbbit a következő képlet alapján könnyen kiszámíthatjuk:

$$\#\tilde{J}(\mathbb{F}_p) = \frac{1}{2}\#\tilde{\mathcal{C}}(\mathbb{F}_{p^2}) + \frac{1}{2}\left(\#\tilde{\mathcal{C}}(\mathbb{F}_p)\right)^2 - p.$$

A Mordell-Weil csoport rangja

Legyen

$$\mathcal{C} : Y^2 = \prod_{i=1}^{2g+1} (X - e_i) \quad e_i \in \mathbb{Z},$$

ahol g a génusz.

$$S = \{2\} \cup \{p : p \mid \prod_{i \neq j} (e_i - e_j)\} = \{p_1, \dots, p_r\},$$

$$\mathbb{Q}(S) = \{\pm p_1^{k_1} \cdots p_r^{k_r} : k_i = 0, 1\}.$$

A következő injektív leképezés segítségével korlátot kapunk a rangra:

$$\begin{aligned} \mu : J(\mathbb{Q})/2J(\mathbb{Q}) &\longrightarrow (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{2g}, \\ (x, y) - \infty &\longmapsto [x - e_1, \dots, x - e_{2g}]. \end{aligned}$$

Példa

$$Y^2 = X(X - 2)(X + 2),$$

léteznek racionális számok a, b, c :

$$x = au^2$$

$$x - 2 = bv^2$$

$$x + 2 = cw^2$$

és $abc = \square$.

$$a, b, c \in \{\pm 1, \pm 2\}.$$

Az $(a, b, c) = (-1, 1, -1)$ eset:

$$x = -u^2$$

$$x - 2 = v^2$$

$$x + 2 = -w^2,$$

azaz

$$C_{-1,1,-1} : -u^2 - v^2 = 2, -u^2 + w^2 = -2$$

nincs megoldás $\mathbb{Q}_\infty$ -ben.

Az $(a, b, c) = (1, 2, 2)$ eset:

$$C_{1,2,2} : u^2 - 2v^2 = 2, u^2 - 2w^2 = -2$$

nincs megoldás $\mathbb{Q}_2$ -ben.

Hogy kerül a μ az asztalra?

$$\mu : (x, y) \longrightarrow [x, x - 2]$$

$$(0, 0) \longrightarrow [(-2)(2), -2] = [-1, -2]$$

$$(2, 0) \longrightarrow [(2, (2)(4))] = [2, 2]$$

$$(-2, 0) \longrightarrow [-2, (-2)(-4)] = [-2, 2]$$

$$H = \langle [-1, -2], [2, 2], [-2, 2] \rangle \leq \text{im} \mu \leq \{\pm 1, \pm 2\}^{\times 2}$$

Így a $(\mathbb{Q}(S))^{\times 2} \setminus H$ elemekről kell megmutatni, hogy nem léphetnek fel.

$$Y^2 = X(X-1)(X-2)(X-5)(X-6)$$

$$\mu : (x, y) \longrightarrow [x, x-1, x-2, x-5]$$

$$\{(0, 0), \infty\} \longrightarrow [(-1)(-2)(-5)(-6), -1, -2, -5] = [15, -1, -2, -5]$$

$$\{(1, 0), \infty\} \longrightarrow [1, (1)(-1)(-4)(-5), -1, -4] = [1, -5, -1, -1]$$

$$\{(2, 0), \infty\} \longrightarrow [2, 1, 6, -3]$$

$$\{(5, 0), \infty\} \longrightarrow [5, 1, 3, -15]$$

$$\{(3, 6), \infty\} \longrightarrow [3, 2, 1, -2]$$

$$H \leq \text{im}\mu \leq \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 5, \pm 10, \pm 15, \pm 30\}^{\times 4}$$

Chabauty-módszer

Fontos megjegyzés:

$$P \in \mathcal{C}(\mathbb{Q}) \longleftrightarrow \{P, P\} \in J(\mathbb{Q})$$

Tegyük fel, hogy sikeresen meghatároztuk a Mordell-Weil csoportot, azaz adott, hogy $J(\mathbb{Q}) = \langle J(\mathbb{Q})_{tors}, D \rangle$.

Legyen $p \nmid 2\Delta(F)$ egy rögzített prím, $J(\mathbb{F}_p) \ni \tilde{D} = D \pmod{p}$ és $\text{ord}(\tilde{D}) = m$.
 $J(\mathbb{Q})$ elemei felírhatóak $A + nE, n \in \mathbb{Z}$ alakban, ahol $E = mD$ és

$$A \in U = \{T + iD : T \in J(\mathbb{Q})_{tors}, 1 \leq i \leq m-1\}.$$

Projektív koordináták:

$$a = (a_i) = (z_i(A)) \in \mathbb{P}^{15}(\mathbb{Q})$$

$$s = \begin{pmatrix} z_1(E)/z_0(E) \\ z_2(E)/z_0(E) \end{pmatrix}$$

Kummer-koordináták: $(\xi_j(A + nE)) = (\Phi_{4j}(a, \sigma(t)))$,
ha $\{(x, y), (u, v)\} = A + nE$, akkor

$$(1, x + u, xu) = (\xi_1(A + nE), \xi_2(A + nE), \xi_3(A + nE)) \\ (\Phi_{41}(a, \sigma(t)), \Phi_{42}(a, \sigma(t)), \Phi_{43}(a, \sigma(t))).$$

$$\{(x, y), (u, v)\} = \{P, P\} \implies \mathbb{Z}_p[[n]] \ni \Theta_{A,E}(n) = \\ \Phi_{42}(a, \sigma(t))^2 - 4\Phi_{41}(a, \sigma(t))\Phi_{43}(a, \sigma(t)) = 0$$

$$\Theta_{A,E}(n) = c_0 + c_1n + c_2n^2 + \dots, c_i \in \mathbb{Z}_p.$$

Tétel (Strassman). *Legyen*

$\Theta(X) = c_0 + c_1X + c_2X^2 + \dots \in \mathbb{Z}_p[[X]]$ *olyan, hogy*
 $c_j \rightarrow 0 \quad \mathbb{Z}_p$ -*ben. Jelölje* k *azt az indexet, amelyre*
 $|c_k|_p \geq |c_j|_p \forall j \geq 0$ *és* $|c_k|_p > |c_j|_p \forall j > k$. *Ekkor*
legfeljebb k *olyan* $x \in \mathbb{Z}_p$ *létezik, hogy* $\Theta(x) = 0$ *és*
 $|x|_p \leq 1$.