

TÖRTénet EGÉSZ pontokról

Tengely Szabolcs

2008. március 21.

Algebrai görbék

❖ Algebrai görbék

- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Legyen $f \in \mathbb{Q}[X, Y]$, $C(R) = \{(x, y) \in R^2 : f(x, y) = 0\}$.

- génusz legalább 1: Siegel (1929) igazolta, hogy $C(\mathbb{Z})$ véges.
- génusz legalább 2: Faltings (1983) bebizonyította, hogy $C(\mathbb{Q})$ véges.

1 génuszú görbék:

$$Y^2 = X^3 + a_1X + a_2.$$

2 génuszú görbék:

$$Y^2 = b_6X^6 + b_5X^5 + b_4X^4 + b_3X^3 + b_2X^2 + b_1X + b_0.$$

Elliptikus görbék

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Véges sok megoldás létezik: Mordell (1922).

Korlát a megoldásokra: Baker (1968)

$$\max(|x|, |y|) < \exp((10^6 H)^{10^6}).$$

Algoritmusok az egész pontok meghatározására:
Stroeker, Tzanakis (1994),
Gebel, Pethő, Zimmer (1998).

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Nehezen meghatározható generátorok:

$$Y^2 = X(X - 157)(X + 157).$$

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Nehezen meghatározható generátorok:

$$Y^2 = X(X - 157)(X + 157).$$

Végtelen rendű pont $P = (x, y)$, ahol:

$$x = \frac{-166136231668185267540804}{2825630694251145858025},$$

$$y = \frac{-167661624456834335404812111469782006}{150201095200135518108761470235125}.$$

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Lokálisan minden p esetén létezik megoldás, de nincs globális megoldás.

$$3X^3 + 4Y^3 + 5Z^3 = 0.$$

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Lokálisan minden p esetén létezik megoldás, de nincs globális megoldás.

$$3X^3 + 4Y^3 + 5Z^3 = 0.$$

Rang, konduktor és egész pontok.

$$Y^2 + Y = X^3 + X^2 - 2X,$$

a görbe rangja 2 és 20 egész pont van rajta.

- ❖ Algebrai görbék
- ❖ **Elliptikus görbék**
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Lokálisan minden p esetén létezik megoldás, de nincs globális megoldás.

$$3X^3 + 4Y^3 + 5Z^3 = 0.$$

Rang, konduktor és egész pontok.

$$Y^2 + Y = X^3 + X^2 - 2X,$$

a görbe rangja 2 és 20 egész pont van rajta.

$$Y^2 + Y = X^3 - 7X + 6,$$

a görbe rangja 3 és 36 egész pont van rajta.

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Egész pontok elliptikus görbe családokon. Legyen

$$E_m : Y^2 = X^3 + mX^2 - (m+3)X + 1.$$

Duquesne (2001): ha E_m rangja 1, akkor E_m egész pontjai a következők

$(0, 1)$ ha m páros,

$(0, 1)$ és $2(0, 1)$ ha m páratlan.

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Egész pontok elliptikus görbe családokon. Legyen

$$E_m : Y^2 = X^3 + mX^2 - (m+3)X + 1.$$

Duquesne (2001): ha E_m rangja 1, akkor E_m egész pontjai a következők

$(0, 1)$ ha m páros,

$(0, 1)$ és $2(0, 1)$ ha m páratlan.

Legyen

$$Q_m : Y^2 = X^4 - mX^3 - 6X^2 + mX + 1,$$

ahol $m^2 + 16$ nem osztható páratlan négyzetszámmal. Duquesne (2007): ha Q_m rangja 1, akkor Q_m egész pontjai $(0, \pm 1)$.

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Speciális elliptikus görbék esetében az általános korlát élesítése:

Draiotis (2006):
Legyen

$$E : Y^2 = (X - k)f(X)$$

elliptikus görbe $\mathbb{Q}$ felett, ahol $k \in \mathbb{Z}$ és $f(k) = \pm 1$.

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Speciális elliptikus görbék esetében az általános korlát élesítése:

Draiotis (2006):
Legyen

$$E : Y^2 = (X - k)f(X)$$

elliptikus görbe $\mathbb{Q}$ felett, ahol $k \in \mathbb{Z}$ és $f(k) = \pm 1$. Ekkor bármely $(x, y) \in E(\mathbb{Z})$ pontra

$$|x| < 11H^2 + 5,$$

ahol H az $(X - k)f(X)$ polinom magassága.

g -gonális számok

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Definíció:

$$\mathcal{G}_{m,g} = \frac{m\{(g-2)m - (g-4)\}}{2}.$$

Rekurzív sorozatokban található g -gonális számok vizsgálata
 $g \in \{3, 4, 5, 7\}$ esetében: J.H.E Cohn, Katayama, Ljunggren,
Luo, Prasad, Rao.

g -gonális számok

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Definíció:

$$\mathcal{G}_{m,g} = \frac{m\{(g-2)m - (g-4)\}}{2}.$$

Rekurzív sorozatokban található g -gonális számok vizsgálata $g \in \{3, 4, 5, 7\}$ esetében: J.H.E Cohn, Katayama, Ljunggren, Luo, Prasad, Rao.

Tengely (2008): $g \in \{6, 8, 9, 10, \dots, 20\}$ esetében

$$F_n = \mathcal{G}_{m,g}, \quad L_n = \mathcal{G}_{m,g},$$

$$P_n = \mathcal{G}_{m,g}, \quad Q_n = \mathcal{G}_{m,g}$$

egyenletek megoldásainak meghatározása.

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ **g -gonális számok**
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

A következő görbék vizsgálatára vezet:

$$C_{F_n}^{even} : Y^2 = 5((g-2)X^2 - (g-4)X)^2 + 16,$$

$$C_{F_n}^{odd} : Y^2 = 5((g-2)X^2 - (g-4)X)^2 - 16,$$

$$C_{L_n}^{even} : Y^2 = 5((g-2)X^2 - (g-4)X)^2 - 80,$$

$$C_{L_n}^{odd} : Y^2 = 5((g-2)X^2 - (g-4)X)^2 + 80,$$

$$C_{P_n}^{even} : Y^2 = 2((g-2)X^2 - (g-4)X)^2 + 4,$$

$$C_{P_n}^{odd} : Y^2 = 2((g-2)X^2 - (g-4)X)^2 - 4,$$

$$C_{Q_n}^{even} : Y^2 = 2((g-2)X^2 - (g-4)X)^2 - 8,$$

$$C_{Q_n}^{odd} : Y^2 = 2((g-2)X^2 - (g-4)X)^2 + 8.$$

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

További tervek.

Görbe családok vizsgálata:

például $(0, 4) \in C_{F_n}^{even}(\mathbb{Q})$, $(1, 2) \in C_{F_n}^{even}(\mathbb{Q})$.

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ **g -gonális számok**
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

További tervek.

Görbe családok vizsgálata:

például $(0, 4) \in C_{F_n}^{even}(\mathbb{Q})$, $(1, 2) \in C_{F_n}^{even}(\mathbb{Q})$.

"Pontatlan" görbék esete:

$$C_{L_n}^{even} : Y^2 = 5((g - 2)X^2 - (g - 4)X)^2 - 80,$$

ha $g \in \{8, 9, 11, 13, 14, 16, 19\}$, akkor nincs megoldás $\mathbb{Q}_5$ -ben.

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ **g -gonális számok**
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

További tervek.

Görbe családok vizsgálata:

például $(0, 4) \in C_{F_n}^{even}(\mathbb{Q})$, $(1, 2) \in C_{F_n}^{even}(\mathbb{Q})$.

"Pontatlan" görbék esete:

$$C_{L_n}^{even} : Y^2 = 5((g-2)X^2 - (g-4)X)^2 - 80,$$

ha $g \in \{8, 9, 11, 13, 14, 16, 19\}$, akkor nincs megoldás $\mathbb{Q}_5$ -ben.

A $g = 12$ eset:

$$Y^2 = 500X^4 - 800X^3 + 320X^2 - 80.$$

Egy kimaradó eset elliptikus görbéi

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Bennett (2008):

Az $(x^k - 1)(y^k - 1) = (z^k - 1)$, $|z| \geq 2$, $k \geq 3$ egyenlet megoldásai a következők: $(x, y, z, k) = (-1, 4, -5, 3)$ és $(4, -1, -5, 3)$.

Egy kimaradó eset elliptikus görbéi

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Bennett (2008):

Az $(x^k - 1)(y^k - 1) = (z^k - 1)$, $|z| \geq 2$, $k \geq 3$ egyenlet megoldásai a következők: $(x, y, z, k) = (-1, 4, -5, 3)$ és $(4, -1, -5, 3)$.

Az $(x^k - 1)(y^k - 1) = (z^k - 1)^2$ egyenletnek nincs megoldása, ha $|z| \geq 2$, $k \geq 4$ és $x \neq \pm y$.

Egy kimaradó eset elliptikus görbéi

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok

❖ Egy kimaradó eset elliptikus görbéi

- ❖ Hiperelliptikus görbék

Bennett (2008):

Az $(x^k - 1)(y^k - 1) = (z^k - 1)$, $|z| \geq 2$, $k \geq 3$ egyenlet megoldásai a következők: $(x, y, z, k) = (-1, 4, -5, 3)$ és $(4, -1, -5, 3)$.

Az $(x^k - 1)(y^k - 1) = (z^k - 1)^2$ egyenletnek nincs megoldása, ha $|z| \geq 2$, $k \geq 4$ és $x \neq \pm y$.

Az $(x^3 - 1)(y^3 - 1) = u^2$ egyenlet esetében Elkies a következő megoldásokat határozta meg:

$$(x, y, u) = (-20, -362, 616077), (-6, -26, 1953), \\ (-1, -23, 156), (0, -2, 3), (2, 4, 21), \\ (2, 22, 273), (3, 313, 28236), (4, 22, 819).$$

Véges sok megoldása létezik csak az egyenletnek?

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

$$\begin{aligned}x^3 - 1 &= dy_1^2, \\y^3 - 1 &= dy_2^2.\end{aligned}$$

Elegendő az

$$E_d : Y^2 = X^3 - d^3$$

görbékét vizsgálni ("quadratic twists"). Amennyiben a görbén található 3 "megfelelő" egész pont, akkor az eredeti probléma egy megoldásához jutunk. Az egyik egész pont mindig adott: $T = (d, 0)$.

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

$$\begin{aligned}x^3 - 1 &= dy_1^2, \\ y^3 - 1 &= dy_2^2.\end{aligned}$$

Elegendő az

$$E_d : Y^2 = X^3 - d^3$$

görbéket vizsgálni ("quadratic twists"). Amennyiben a görbén található 3 "megfelelő" egész pont, akkor az eredeti probléma egy megoldásához jutunk. Az egyik egész pont mindig adott: $T = (d, 0)$. Ismert megoldásoknál $d \in \{-889, -217, -2, -1, 7, 26\}$.

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Legyen $P = (dx, d^2y)$. Ekkor $P + T$ esetében

$$x(P + T) = d \left(1 + \frac{3}{x-1} \right).$$

Ez akkor lesz "megfelelő" egész pont x -koordinátája, ha $x \in \{-2, 0, 2, 4\}$.

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok

❖ Egy kimaradó eset
elliptikus görbéi

- ❖ Hiperelliptikus görbék

Legyen $P = (dx, d^2y)$. Ekkor $P + T$ esetében

$$x(P + T) = d \left(1 + \frac{3}{x-1} \right).$$

Ez akkor lesz "megfelelő" egész pont x -koordinátája, ha $x \in \{-2, 0, 2, 4\}$.

A $2P$ pont esetében

$$x(2P) = d \frac{x^4 + 8x}{4(x^3 - 1)}.$$

Ez akkor lesz "megfelelő" egész pont x -koordinátája, ha $x \in \{-2, 0\}$.

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Legyen $P = (dx, d^2y)$. Ekkor $P + T$ esetében

$$x(P + T) = d \left(1 + \frac{3}{x-1} \right).$$

Ez akkor lesz "megfelelő" egész pont x -koordinátája, ha $x \in \{-2, 0, 2, 4\}$.

A $2P$ pont esetében

$$x(2P) = d \frac{x^4 + 8x}{4(x^3 - 1)}.$$

Ez akkor lesz "megfelelő" egész pont x -koordinátája, ha $x \in \{-2, 0\}$.

Stratégia: megmutatni, hogy $(dx, d^2y) = mR + nT$ csak kis m értékekre lehetséges. Az ismert megoldások esetében $m \leq 2$.

Hiperelliptikus görbék

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

$$Y^p - Y = X^q - X, \quad 2 \leq p < q.$$

Fielder, Alford (1998): pozitív megoldások

$(3, 2, 2, 3), (6, 2, 2, 5), (15, 2, 6, 3), (16, 2, 3, 5),$
 $(13, 3, 3, 7), (91, 2, 2, 13), (280, 2, 5, 7), (4930, 2, 30, 5).$

Hiperelliptikus görbék

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

$$Y^p - Y = X^q - X, \quad 2 \leq p < q.$$

Fielder, Alford (1998): pozitív megoldások

$$(3, 2, 2, 3), (6, 2, 2, 5), (15, 2, 6, 3), (16, 2, 3, 5), \\ (13, 3, 3, 7), (91, 2, 2, 13), (280, 2, 5, 7), (4930, 2, 30, 5).$$

További eredmények:

Mordell (1963): $p = 2, q = 3$ eset,

Mignotte és Pethő (1999): végességi eredmények, teljes megoldás $p = 2, q > 2$ esetben, feltéve, hogy y teljes hatványa valamilyen prímnek.

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

$$\binom{n}{k} = \binom{m}{l},$$

$k, l, m, n \in \mathbb{N}$ és $2 \leq k \leq \frac{n}{2}, 2 \leq l \leq \frac{m}{2}$.

Ismert megoldások:

$$\binom{16}{2} = \binom{10}{3}, \quad \binom{56}{2} = \binom{22}{3}, \quad \binom{120}{2} = \binom{36}{3},$$

$$\binom{21}{2} = \binom{10}{4}, \quad \binom{153}{2} = \binom{19}{5}, \quad \binom{78}{2} = \binom{15}{5} = \binom{14}{6},$$

$$\binom{221}{2} = \binom{17}{8}, \quad \binom{F_{2i+2}F_{2i+3}}{F_{2i}F_{2i+3}} = \binom{F_{2i+2}F_{2i+3}-1}{F_{2i}F_{2i+3}+1} \text{ ahol } i = 1, 2, \dots,$$

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

$$\binom{n}{k} = \binom{m}{l},$$

$k, l, m, n \in \mathbb{N}$ és $2 \leq k \leq \frac{n}{2}, 2 \leq l \leq \frac{m}{2}$.

Ismert megoldások:

$$\binom{16}{2} = \binom{10}{3}, \quad \binom{56}{2} = \binom{22}{3}, \quad \binom{120}{2} = \binom{36}{3},$$

$$\binom{21}{2} = \binom{10}{4}, \quad \binom{153}{2} = \binom{19}{5}, \quad \binom{78}{2} = \binom{15}{5} = \binom{14}{6},$$

$$\binom{221}{2} = \binom{17}{8}, \quad \binom{F_{2i+2}F_{2i+3}}{F_{2i}F_{2i+3}} = \binom{F_{2i+2}F_{2i+3}-1}{F_{2i}F_{2i+3}+1} \text{ ahol } i = 1, 2, \dots,$$

Lind (1968), Singmaster (1975): Fibonacci sorozattal megadott megoldás családok. De Weger (1997): $\binom{n}{k} \leq 10^{30}$ vagy $n \leq 1000$ esetében nincs több nem triviális megoldás.

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Mordell (1963), Avanesov (1966/1967), Pintér (1995), De Weger (1996), Stroeker és De Weger (1999): teljes megoldások

$$(k, l) \in \{(2, 3), (2, 4), (2, 6), (2, 8), (3, 4), (3, 6), (4, 6)\}$$

esetében. Ezek a problémák Thue egyenletekre vagy elliptikus görbékre vezetnek.

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Mordell (1963), Avanesov (1966/1967), Pintér (1995), De Weger (1996), Stroeker és De Weger (1999): teljes megoldások

$$(k, l) \in \{(2, 3), (2, 4), (2, 6), (2, 8), (3, 4), (3, 6), (4, 6)\}$$

esetében. Ezek a problémák Thue egyenletekre vagy elliptikus görbékre vezetnek.

Általános végességi eredmények:

Kiss (1988): $k = 2$ és l adott páratlan prím.

Brindza (1991): $k = 2$ és $l \geq 3$.

Egy kis kihívás:

$$\begin{pmatrix} y \\ 2 \end{pmatrix} = \begin{pmatrix} x \\ 5 \end{pmatrix}.$$

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Bugeaud, Mignotte, Siksek, Stoll, Tengely (2008):

$$C: Y^2 - Y = X^5 - X$$

összes egész megoldása:

$$(X, Y) = (-1, 0), (-1, 1), (0, 0), (0, 1), (1, 0), (1, 1), (2, -5), \\ (2, 6), (3, -15), (3, 16), (30, -4929), (30, 4930).$$

$J(\mathbb{Q})$ Mordell-Weil csoportjának a rangja 3.

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

- Mivel $F(X, Y) = Y^2 - Y - X^5 + X$ esetében $F(0, 0) = 0$, Runge-módszerrel meghatározhatók az adott legnagyobb közös osztóval rendelkező megoldások.

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

- Mivel $F(X, Y) = Y^2 - Y - X^5 + X$ esetében $F(0, 0) = 0$, Runge-módszerrel meghatározhatók az adott legnagyobb közös osztóval rendelkező megoldások.
- Chabauty módszere nem alkalmazható, mert $J(\mathbb{Q})$ Mordell-Weil csoportjának a rangja nagyobb, mint a görbe génusza.

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

- Mivel $F(X, Y) = Y^2 - Y - X^5 + X$ esetében $F(0, 0) = 0$, Runge-módszerrel meghatározhatók az adott legnagyobb közös osztóval rendelkező megoldások.
- Chabauty módszere nem alkalmazható, mert $J(\mathbb{Q})$ Mordell-Weil csoportjának a rangja nagyobb, mint a görbe génusza.
- Elliptikus Chabauty módszer esetében számtest felett kell a Mordell-Weil csoport rangját meghatározni.

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

- Mivel $F(X, Y) = Y^2 - Y - X^5 + X$ esetében $F(0, 0) = 0$, Runge-módszerrel meghatározhatók az adott legnagyobb közös osztóval rendelkező megoldások.
- Chabauty módszere nem alkalmazható, mert $J(\mathbb{Q})$ Mordell-Weil csoportjának a rangja nagyobb, mint a görbe génusza.
- Elliptikus Chabauty módszer esetében számtest felett kell a Mordell-Weil csoport rangját meghatározni.
- S -egység egyenletek, Baker módszer + LLL algoritmus: a fellépő számtestek foka nagy.

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

- Mivel $F(X, Y) = Y^2 - Y - X^5 + X$ esetében $F(0, 0) = 0$, Runge-módszerrel meghatározhatók az adott legnagyobb közös osztóval rendelkező megoldások.
- Chabauty módszere nem alkalmazható, mert $J(\mathbb{Q})$ Mordell-Weil csoportjának a rangja nagyobb, mint a görbe génusza.
- Elliptikus Chabauty módszer esetében számtest felett kell a Mordell-Weil csoport rangját meghatározni.
- S -egység egyenletek, Baker módszer + LLL algoritmus: a fellépő számtestek foka nagy.
- S -egység egyenletek + Skolem módszere: a fellépő számtestek foka nagy.

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

- Mivel $F(X, Y) = Y^2 - Y - X^5 + X$ esetében $F(0, 0) = 0$, Runge-módszerrel meghatározhatók az adott legnagyobb közös osztóval rendelkező megoldások.
- Chabauty módszere nem alkalmazható, mert $J(\mathbb{Q})$ Mordell-Weil csoportjának a rangja nagyobb, mint a görbe génusza.
- Elliptikus Chabauty módszer esetében számtest felett kell a Mordell-Weil csoport rangját meghatározni.
- S -egység egyenletek, Baker módszer + LLL algoritmus: a fellépő számtestek foka nagy.
- S -egység egyenletek + Skolem módszere: a fellépő számtestek foka nagy.
- Demjanenko-Manin módszer: független leképezések kellenek elliptikus görbére.

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Transzformált alak:

$$C : 2y^2 = x^5 - 16x + 8,$$

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Transzformált alak:

$$C : 2y^2 = x^5 - 16x + 8,$$

Mordell-Weil bázis $J(\mathbb{Q})$ -ban:

$$D_1 = (0, 2) - \infty, \quad D_2 = (2, 2) - \infty, \quad D_3 = (-2, 2) - \infty.$$

Ekkor $x - \alpha = \kappa \xi^2$, ahol $\kappa \in \{1, -2\alpha, 4 - 2\alpha, -4 - 2\alpha, -2\alpha + \alpha^2, 2\alpha + \alpha^2, -4 + \alpha^2, 8\alpha - 2\alpha^3\}$.

- ❖ Algebrái görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Bruin, Stoll: Mordell–Weil szita

$$J(C(\mathbb{Q})) \subseteq W + BJ(\mathbb{Q}),$$

ahol W az ismert racionális pontok képe és

$$B = 2^8 \cdot 3^4 \cdot 5^3 \cdot 7^3 \cdot 11^2 \cdot 13^2 \cdot 17^2 \cdot 19 \cdot 23 \cdot 29 \cdot 31^2 \cdot \prod_{\substack{37 \leq p \leq 149 \\ p \neq 107}} p$$

Legyen $L_0 = B\mathbb{Z}^3$ és

$$\phi : \mathbb{Z}^3 \rightarrow J(\mathbb{Q}), \quad \phi(a_1, \dots, a_r) = \sum a_i D_i,$$

- ❖ Algebrai görbék
- ❖ Elliptikus görbék
- ❖ g -gonális számok
- ❖ Egy kimaradó eset elliptikus görbéi
- ❖ Hiperelliptikus görbék

Ekkor

$$J(C(\mathbb{Q})) \subset W + \phi(B\mathbb{Z}^3).$$

Rácsok csökkenő lánc:

$$B\mathbb{Z}^3 = L_0 \supsetneq L_1 \supsetneq L_2 \supsetneq \cdots \supsetneq L_k,$$

úgy, hogy

$$J(C(\mathbb{Q})) \subset W + \phi(L_j).$$

Az így meghatározott rács indexe: 3.32×10^{3240} ,
az ebben a rácsban található legrövidebb vektor hossza:
 1.156×10^{1080} .

Amennyiben létezne $P \in C(\mathbb{Q})$ ismeretlen pont, akkor

$$\log x(P) \geq 0.95 \times 10^{2159},$$

ellentmondás, mert a felső korlát 5.1×10^{565} .