

Egész pontokról racionálisan

Tengely Szabolcs

2008. április 16.

Algebrai görbék

❖ Algebrai görbék

- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko–Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell–Weil szita

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:

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

Eszközök

❖ Algebrai görbék

❖ **Eszközök**

❖ Runge módszer

❖ Algoritmus

❖ Példa

❖ Demjanenko–
Manin

❖ Hiperelliptikus
alapozás

❖ Baker módszer +
Mordell–Weil szita

- Elemi, lokális módszerek
- Runge módszer
- Skolem módszer
- Baker módszer
- Chabauty módszer
- Elliptikus Chabauty módszer
- Demjanenko–Manin módszer
- Moduláris módszer
- Mordell–Weil szita

Runge módszer

- ❖ Algebrai görbék
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko–Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell–Weil szita

$$P(X, Y) = \sum_{i=0}^m \sum_{j=0}^n a_{i,j} X^i Y^j, \quad a_{i,j} \in \mathbb{Z}$$

irreducibilis polinom a $\mathbb{Q}[X, Y]$ gyűrűben. Legyen $\lambda > 0$.

- $P_\lambda(X, Y)$: az összes $a_{i,j} X^i Y^j$ összege, ahol $i + \lambda j$ maximális,
- $\tilde{P}(X, Y)$: az összes olyan $a_{i,j} X^i Y^j$ összege, amely előfordul valamely $P_\lambda(X, Y)$ polinomban.

Egy P polinom eleget tesz Runge feltételének, ha nem létezik λ , amelyre $\tilde{P} = P_\lambda$ konstans szorzótól eltekintve egy irreducibilis polinom hatványa.

❖ Algebrai görbék

❖ Eszközök

❖ Runge módszer

❖ Algoritmus

❖ Példa

❖ Demjanenko-
Manin

❖ Hiperelliptikus
alapozás

❖ Baker módszer +
Mordell-Weil szita

Példa:

$$P(X, Y) = X^2 - Y^8 - Y^7 - Y^2 - 3Y + 5,$$

- $P_\lambda(X, Y) = X^2$ ha $\lambda < \frac{1}{4}$,
- $P_\lambda(X, Y) = X^2 - Y^8$ ha $\lambda = \frac{1}{4}$,
- $P_\lambda(X, Y) = Y^8$ ha $\lambda > \frac{1}{4}$,

így $\tilde{P}(X, Y) = X^2 - Y^8 = (X - Y^4)(X + Y^4)$.

Példa:

$$P(X, Y) = X^2 - Y^8 - Y^7 - Y^2 - 3Y + 5,$$

- $P_\lambda(X, Y) = X^2$ ha $\lambda < \frac{1}{4}$,
- $P_\lambda(X, Y) = X^2 - Y^8$ ha $\lambda = \frac{1}{4}$,
- $P_\lambda(X, Y) = Y^8$ ha $\lambda > \frac{1}{4}$,

így $\tilde{P}(X, Y) = X^2 - Y^8 = (X - Y^4)(X + Y^4)$.

Tétel (Runge, 1887). *Ha a P polinom eleget tesz a Runge feltételnek, akkor a $P(x, y) = 0$ diofantikus egyenletnek csak véges sok megoldása van.*

További eredmények: Hilliker és Straus, Walsh, Grytczuk és Schinzel, Laurent és Poulakis.

❖ Algebrai görbék

❖ Eszközök

❖ Runge módszer

❖ Algoritmus

❖ Példa

❖ Demjanenko-
Manin

❖ Hiperelliptikus
alapozás

❖ Baker módszer +
Mordell-Weil szita

Az $F(x) = G(y)$ eset:

$\deg F = n$, $\deg G = m$, $\gcd(m, n) > 1$ és az $F(X) - G(Y)$ polinom irreducibilis a $\mathbb{Q}[X, Y]$ gyűrűben. Legyen $1 < d \mid \gcd(m, n)$. Ekkor Runge feltétele teljesül.

Tétel (T.Sz.,2003). *Ha $(x, y) \in \mathbb{Z}^2$ megoldása az $F(x) = G(y)$ egyenletnek, ahol F és G kielégítik a fenti feltételeket, akkor*

$$\max\{|x|, |y|\} \leq d^{\frac{2m^2}{d}-m} (m+1)^{\frac{3m}{2d}} \left(\frac{m}{d} + 1\right)^{\frac{3m}{2}} (h+1)^{\frac{m^2+mn+m}{d}+2m}.$$

- ❖ Algebrai görbék
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko-Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell-Weil szita

Lemma (Walsh,1992). Az $U^d = F(X)$, $V^d = G(X)$ egyenletek által definiált U, V algebrai függvényekhez léteznek Puiseux kifejtések:

$$u(X) = \sum_{i=-\frac{n}{d}}^{\infty} f_i X^{-i} \text{ és}$$

$$v(X) = \sum_{i=-\frac{m}{d}}^{\infty} g_i X^{-i}$$

úgy, hogy $d^{2(n/d+i)-1} f_i \in \mathbb{Z}$ minden $i > -\frac{n}{d}$ esetén, hasonlóan $d^{2(m/d+i)-1} g_i \in \mathbb{Z}$ minden $i > -\frac{m}{d}$ esetén, és $f_{-\frac{n}{d}} = g_{-\frac{m}{d}} = 1$.

Továbbá $|f_i| \leq (H(F) + 1)^{\frac{n}{d}+i+1}$ ha $i \geq -\frac{n}{d}$ és

$|g_i| \leq (H(G) + 1)^{\frac{m}{d}+i+1}$ ha $i \geq -\frac{m}{d}$.

- ❖ Algebrai görbék
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko-Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell-Weil szita

$$F(X) = \left(\sum_{i=-\frac{n}{d}}^{\infty} f_i X^{-i} \right)^d, \quad G(Y) = \left(\sum_{i=-\frac{m}{d}}^{\infty} g_i Y^{-i} \right)^d,$$

Amennyiben $|t|$ elég nagy:

$$\left| \sum_{i=1}^{\infty} d^{\frac{2m}{d}-1} f_i t^{-i} \right| < \frac{1}{2}$$

és

$$\left| \sum_{i=1}^{\infty} d^{\frac{2m}{d}-1} g_i t^{-i} \right| < \frac{1}{2}.$$

- ❖ Algebrai görbék
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko-Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell-Weil szita

Mivel $F(x) = G(y)$, így $u(x)^d - v(y)^d = 0$, azaz

$$(u(x) - v(y)) (u(x)^{d-1} + u(x)^{d-2}v(y) + \dots + v(y)^{d-1}) = 0,$$

ha d páratlan,

$$(u(x)^2 - v(y)^2) (u(x)^{d-2} + u(x)^{d-4}v(y)^2 + \dots + v(y)^{d-2}) = 0,$$

ha d páros.

A fenti egyenletekből adódik, hogy

$$u(x) = v(y) \text{ ha } d \text{ páratlan, és}$$

$$u(x) = \pm v(y) \text{ ha } d \text{ páros.}$$

❖ Algebrai görbék

❖ Eszközök

❖ Runge módszer

❖ Algoritmus

❖ Példa

❖ Demjanenko-
Manin

❖ Hiperelliptikus
alapozás

❖ Baker módszer +
Mordell-Weil szita

Így

$$0 = |u(x) \pm v(y)| = \left| \sum_{i=-\frac{n}{d}}^{\infty} f_i x^{-i} \pm \sum_{i=-\frac{m}{d}}^{\infty} g_i y^{-i} \right|.$$

Ha $|x|$ és $|y|$ elég nagy, akkor

$$\left| \sum_{i=-\frac{n}{d}}^0 d^{\frac{2m}{d}-1} f_i x^{-i} \pm \sum_{i=-\frac{m}{d}}^0 d^{\frac{2m}{d}-1} g_i y^{-i} \right| < 1.$$

Egész együtthatós polinom!

$$Q(x, y) := \sum_{i=0}^{\frac{n}{d}} d^{\frac{2m}{d}-1} f_{-i} x^i \pm \sum_{i=0}^{\frac{m}{d}} d^{\frac{2m}{d}-1} g_{-i} y^i = 0.$$

Megoldás x -re: $\text{Res}_Y(F(X) - G(Y), Q(X, Y)) = 0$.

Megoldás y -ra: $\text{Res}_X(F(X) - G(Y), Q(X, Y)) = 0$.

Algoritmus

- ❖ Algebrai görbék
- ❖ Eszközök
- ❖ Runge módszer

❖ Algoritmus

- ❖ Példa
- ❖ Demjanenko-Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell-Weil szita

Legyen $u(X) = \sum_{i=-\frac{n}{p}}^0 f_i X^{-i}$ és $v(X) = \sum_{i=-\frac{m}{p}}^0 g_i X^{-i}$, ahol $p \mid \gcd(m, n)$ páratlan. Legyen $t \in \mathbb{R}^+$. Ekkor

$$(u(x) - t)^p < F(x) < (u(x) + t)^p \text{ ahol } x \notin [x_t^-, x_t^+],$$
$$(v(y) - t)^p < G(y) < (v(y) + t)^p \text{ ahol } y \notin [y_t^-, y_t^+].$$

$$x_t^- = \min\{\{0\} \cup \{x \in \mathbb{R} : F(x) - (u(x) - t)^p = 0$$
$$\text{ vagy } F(x) - (u(x) + t)^p = 0\}\},$$

$$x_t^+ = \max\{\{0\} \cup \{x \in \mathbb{R} : F(x) - (u(x) - t)^p = 0$$
$$\text{ vagy } F(x) - (u(x) + t)^p = 0\}\},$$

$$y_t^- = \min\{\{0\} \cup \{x \in \mathbb{R} : G(x) - (v(x) - t)^p = 0$$
$$\text{ vagy } G(x) - (v(x) + t)^p = 0\}\},$$

$$y_t^+ = \max\{\{0\} \cup \{x \in \mathbb{R} : G(x) - (v(x) - t)^p = 0$$
$$\text{ vagy } G(x) - (v(x) + t)^p = 0\}\}.$$

- ❖ Algebrai görbék
- ❖ Eszközök
- ❖ Runge módszer

❖ Algoritmus

- ❖ Példa
- ❖ Demjanenko-Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell-Weil szita

Adódik, hogy

$$u(x) - t < F(x)^{1/p} < u(x) + t \text{ ahol } x \notin [x_t^-, x_t^+],$$

$$v(y) - t < G(y)^{1/p} < v(y) + t \text{ ahol } y \notin [y_t^-, y_t^+].$$

Így

$$-2t < u(x) - v(y) < 2t.$$

A speciális megoldások gyökei a $\text{Res}_Y(F(X) - G(Y), u(X) - v(Y) - T)$ polinomnak. Itt $-2t < T < 2t$ racionális szám, amelynek nevezője osztója $p^{\frac{2m}{p}-1}$ -nek.

- ❖ Algebrai görbék
- ❖ Eszközök
- ❖ Runge módszer

❖ Algoritmus

- ❖ Példa
- ❖ Demjanenko-Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell-Weil szita

Megoldások meghatározása:

$$F(x) = G(k) \text{ valamilyen } k \in [y_t^-, y_t^+],$$

$$G(y) = F(k) \text{ valamilyen } k \in [x_t^-, x_t^+],$$

$$\text{Res}_Y(F(X) - G(Y), u(X) - v(Y) - T) = 0 \text{ ahol } T \in \mathbb{Q}, |T| < 2t$$

a nevezője osztója $p^{\frac{2m}{p}-1}$ számnak.

Adott egyenlet megoldásához tehát t -től függő rendszert kell kezelni. Az rendszerben szereplő egyenletek számát redukáljuk ("baby-step giant-step" effektus).

Példa

- ❖ Algebrai görbék
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko-Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell-Weil szita

$$x^3 - 5x^2 + 45x - 713 =$$

$$y^9 - 3y^8 + 9y^7 - 17y^6 + 38y^5 - 199y^4 - 261y^3 + 789y^2 + 234y.$$

Ekkor

$$u(X) = X - \frac{5}{3},$$

$$v(Y) = Y^3 - Y^2 + 2Y - \frac{4}{3}.$$

t	"rendszer mérete"	$[x_t^-, x_t^+, y_t^-, y_t^+]$
1/6	177	$[-86, 45, -32, 11]$
1/3	95	$[-48, 15, -18, 9]$
2/3	67	$[-27, 13, -10, 8]$
4/3	52	$[-16, 11, -2, 6]$

Megoldás: $(x, y) = (-11, -2)$.

Demjanenko–Manin módszer

- ❖ Algebrai görbék
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko–Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell–Weil szita

$$\mathcal{C}_{u,v} : Y^2 = uX^6 + vX^4 + vX^2 + u =: F(X),$$

Legyen $\mathcal{E}_{u,v} : Y^2 = uX^3 + vX^2 + vX + u$.

Magasság: $h(P) = h(x_1/x_2) = \log(\max\{|x_1|, |x_2|\})$.

Kanonikus magasság: $\hat{h}(P) = \lim_{n \rightarrow \infty} 4^{-n} h([2^n]P)$.

Tulajdonságok: $\hat{h}(P) = h(P) + O(1)$ és $\hat{h}(mP) = m^2 \hat{h}(P)$.

Silverman korlát:

$$\frac{1}{4}h(j) - \frac{1}{6}h(\Delta) - 1.946 \leq \hat{h}(P) - h(P) \leq \frac{1}{6}h(j) + \frac{1}{6}h(\Delta) + 2.14$$

- ❖ Algebrai görbék
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko-Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell-Weil szita

Leképezések:

$$\phi_1(X, Y) = (X^2, Y),$$

$$\phi_2(X, Y) = (1/X^2, Y/X^3).$$

$$(\phi_1 + \phi_2)(X, Y) = (f_+(X), Yg_+(X)) \text{ és}$$

$$(\phi_1 - \phi_2)(X, Y) = (f_-(X), Yg_-(X)), \text{ ahol}$$

$$f_+(X) = \frac{-2uX^3 - 3uX^2 - 2uX + vX^2}{u(X^4 + 2X^3 + 2X^2 + 2X + 1)},$$

$$f_-(X) = \frac{2uX^3 - 3uX^2 + 2uX + vX^2}{u(X^4 - 2X^3 + 2X^2 - 2X + 1)}.$$

- ❖ Algebrai görbék
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa

❖ Demjanenko-Manin

- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell-Weil szita

Tegyük fel, hogy $\mathcal{E}_{u,v}(\mathbb{Q}) = \langle \mathcal{E}_{u,v}(\mathbb{Q})_{tors}, R \rangle$ és $P \in \mathcal{C}_{u,v}(\mathbb{Q})$.
Ekkor

$$\phi_1(P) = [n]R + T_1, \quad \phi_2(P) = [m]R + T_2.$$

Ha N elég nagy, akkor

$$[N]\phi_1(P) = [nN]R, \quad [N]\phi_2(P) = [mN]R.$$

Így $\hat{h}(\phi_1(P)) = n^2 \hat{h}(R)$ és $\hat{h}(\phi_2(P)) = m^2 \hat{h}(R)$.

$$\begin{aligned} |\hat{h}(\phi_1(P)) - \hat{h}(\phi_2(P))| &\leq |\hat{h}(\phi_1(P)) - h(\phi_1(P))| + \\ &|\hat{h}(\phi_2(P)) - h(\phi_2(P))| + |h(\phi_1(P)) - h(\phi_2(P))| \end{aligned}$$

$$\Rightarrow |m^2 - n^2| < konst. \Rightarrow \min\{|m|, |n|\} < konst.$$

Hiperelliptikus alapozás

- ❖ Algebrai görbék
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko-Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell-Weil szita

$$\mathcal{C}: Y^2 = F(X) = X(X-1)(X-2)(X-5)(X-6),$$

Ekkor a megfelelő osztályok:

$$(x, y) + (u, v) - 2\infty \rightarrow \{(x, y), (u, v)\}.$$

Speciális elemek: $\{(x, y), (x, -y)\}, \{\infty, \infty\} \rightarrow \mathcal{O}.$

Megfelelő párok: $(x, y), (u, v) \in C(\mathbb{Q}), C(\mathbb{Q}(\sqrt{d})).$

Példák: $\{(0, 0), (10, -120)\}, \{\infty, (1, 0)\}, \{(\frac{11}{2} + \frac{1}{2}\sqrt{41}, 35 + 5\sqrt{41}), (\frac{11}{2} - \frac{1}{2}\sqrt{41}, 35 - 5\sqrt{41})\}.$

Nem OK: $\{(3, 6), (\frac{11}{2} + \frac{1}{2}\sqrt{41}, 35 + 5\sqrt{41})\}.$

- ❖ Algebrai görbék
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko-Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell-Weil szita

Elemek összeadása: $A = \{(0, 0), (1, 0)\}$, $B = \{(2, 0), (3, 6)\}$.

Az $Y = X(X - 1)(X - 2)$ görbe átmegy a 4 ponton.

Behelyettesítve az $Y^2 = F(X)$ egyenletbe adódik:

$$X(X - 1)(X - 2)(X - 3)(X^2 - X + 10).$$

Legyen

$$C = \{(\frac{1}{2} + \frac{1}{2}\sqrt{-39}, 15 - 5\sqrt{-39}), (\frac{1}{2} - \frac{1}{2}\sqrt{-39}, 15 + 5\sqrt{-39})\}.$$

Ekkor $A + B + C = \mathcal{O}$, azaz $A + B =$

$$\{(\frac{1}{2} + \frac{1}{2}\sqrt{-39}, -15 + 5\sqrt{-39}), (\frac{1}{2} - \frac{1}{2}\sqrt{-39}, -15 - 5\sqrt{-39})\}.$$

Baker módszer + Mordell-Weil szita

- ❖ Algebrai görbék
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko-Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell-Weil szita

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

Fielder, Alford (1998): pozitív megoldások

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

Baker módszer + Mordell-Weil szita

- ❖ Algebrai görbék
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko-Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell-Weil szita

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

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
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko-Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell-Weil szita

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

$k, l, m, n \in \mathbb{N}$ 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
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko–Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell–Weil szita

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

$k, l, m, n \in \mathbb{N}$ 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
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko–Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell–Weil szita

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
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko–Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell–Weil szita

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 $l \geq 3$.

- ❖ Algebrai görbék
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko-Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell-Weil szita

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

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

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
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko–Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell–Weil szita

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

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

összes egész megoldása:

$$(X, Y) = (0, 0), (0, 1), (1, 0), (1, 1), (2, 0), (2, 1), (3, 0), \\ (3, 1), (4, 0), (4, 1), (5, -1), (5, 2), \\ (6, -3), (6, 4), (7, -6), (7, 7), (15, -77), (15, 78), \\ (19, -152), (19, 153).$$

- ❖ Algebrai görbék
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko–Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell–Weil szita

- 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.

- 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.

- 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.

- 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.

- 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.

- 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
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko–Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell–Weil szita

Transzformált alak:

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

- ❖ Algebrai görbék
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko-Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell-Weil szita

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 $\kappa \in \{1, -2\alpha, 4 - 2\alpha, -4 - 2\alpha, -2\alpha + \alpha^2, 2\alpha + \alpha^2, -4 + \alpha^2, 8\alpha - 2\alpha^3\}$.
 Baker korlát $\log x$ -re: 5.1×10^{565} .

- ❖ Algebrai görbék
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko–Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell–Weil szita

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
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko–Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell–Weil szita

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} .

g -gonális számok

- ❖ Algebrai görbék
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko–Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell–Weil szita

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
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko–Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell–Weil szita

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
- ❖ Eszközök
- ❖ Runge módszer
- ❖ Algoritmus
- ❖ Példa
- ❖ Demjanenko-Manin
- ❖ Hiperelliptikus alapozás
- ❖ Baker módszer + Mordell-Weil szita

A következő görbék vizsgálatára vezet:

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

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

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

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

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

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

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

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