Aritmetika : Geometria : 1-1

Tengely Szabolcs

tengely@math.klte.hu

Debreceni Egyetem

Stellingen

- Let $q > 1$ be an integer and $f : \mathbb{N} \longrightarrow \overline{\mathbb{Q}}$ a periodic function $\bmod q$, i.e. $f(n+q) = f(n)$ for all $n \in \mathbb{N}$. Denote by $\varphi(q)$ the Euler totient function and by $\nu_p(n)$ the exponent to which p divides n. Put

$$P(d) = \{p \text{ prime } \mid p \text{ divides } q, \nu_p(d) \geq \nu_p(q)\},$$

$$\varepsilon(r,p) = \nu_p(q) + \frac{1}{p-1} \text{ if } p \in P(r) \text{ and } \nu_p(r) \text{ otherwise.}$$

  Let $f(m) = f(n)$ for all m, n with $\nu_p(m) = \nu_p(n)$ for all prime divisors p of q. Then $\sum_{n=1}^{\infty} \frac{f(n)}{n} = 0$ if and only if

$$\sum_{v \mid q} \varphi\left(\frac{q}{v}\right) f(v) = 0$$

  and

$$\sum_{r=1}^{q} f(r)\varepsilon(r,p) = 0 \qquad \text{for all prime divisors } p \text{ of } q.$$

- Erdős conjectured that if $f : \mathbb{N} \longrightarrow \mathbb{Z}$ is periodic $\mod q$ such that $f(n) \in \{-1, 1\}$ when $n = 1, \ldots, q-1$ and $f(q) = 0$, then $\sum_{n=1}^{\infty} \frac{f(n)}{n} \neq 0$. However, there exists a function $f : \mathbb{N} \longrightarrow \{\pm 1\}$ with period 36 such that

$$\sum_{n=1}^{\infty} \frac{f(n)}{n} = 0.$$

- Erdős conjectured that if $f : \mathbb{N} \longrightarrow \mathbb{Z}$ is periodic $\bmod q$ such that $f(n) \in \{-1, 1\}$ when $n = 1, \ldots, q-1$ and $f(q) = 0$, then $\sum_{n=1}^{\infty} \frac{f(n)}{n} \neq 0$. However, there exists a function $f : \mathbb{N} \longrightarrow \{\pm 1\}$ with period 36 such that

$$\sum_{n=1}^{\infty} \frac{f(n)}{n} = 0.$$

- If $f : \mathbb{N} \longrightarrow \mathbb{Z}$ is a function with period $q = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ such that $f(n) \in \{-1, 1\}$ when $n = 1, \ldots, q-1$ and $f(q) = 0$ and $f(m) = f(n)$ for all m, n with $\nu_p(m) = \nu_p(n)$ for all primes $p \mid q$ and $\sum_{n=1}^{\infty} \frac{f(n)}{n} = 0$. Then $\alpha_i \geq 2$ for $i = 1, 2, \ldots, r$.

- Let $U = \{u_1, \dots, u_k\}$ be a set of distinct positive integers and $s = \sum_{i=1}^{k} u_i$. The set U is said to be a unique-sum set if the equation $\sum_{i=1}^{k} c_i u_i = s$ with $c_i \in \mathbb{N} \cup \{0\}$ has only the solution $c_i = 1$ for $i = 1, 2, \dots, n$. Let u be an element of a unique-sum set U. Then

$$\#U \leq \frac{u}{2} + 1.$$

- Let $U = \{u_1, \ldots, u_k\}$ be a set of distinct positive integers and $s = \sum_{i=1}^k u_i$. The set U is said to be a unique-sum set if the equation $\sum_{i=1}^k c_i u_i = s$ with $c_i \in \mathbb{N} \cup \{0\}$ has only the solution $c_i = 1$ for $i = 1, 2, \ldots, n$. Let u be an element of a unique-sum set U. Then

$$\#U \leq \frac{u}{2} + 1.$$

- For every positive integer n the set

$$G_n = \bigcup_{k=0}^{n-1} \{2^n - 2^k\}$$

is a unique-sum set.

- Let $U = \{u_1, \ldots, u_k\}$ be a set of distinct positive integers and $s = \sum_{i=1}^{k} u_i$. The set U is said to be a unique-sum set if the equation $\sum_{i=1}^{k} c_i u_i = s$ with $c_i \in \mathbb{N} \cup \{0\}$ has only the solution $c_i = 1$ for $i = 1, 2, \ldots, n$. Let u be an element of a unique-sum set U. Then

$$\#U \leq \frac{u}{2} + 1.$$

- For every positive integer n the set

$$G_n = \bigcup_{k=0}^{n-1} \{2^n - 2^k\}$$

  is a unique-sum set.
- All the solutions of the Diophantine equation $x^4 + 2x^3 - 9x^2y^2 + 2xy - 15y - 7 = 0$ in rational integers are given by

$$(x, y) \in \{(-4, -1), (-1, -1), (1, -1), (2, -1)\}.$$

- There exists a solution of the Diophantine equation $x^2 + q^4 = 2y^p$ in positive integers x, y, p, q, with p and q odd primes.

- There exists a solution of the Diophantine equation $x^2 + q^4 = 2y^p$ in positive integers x, y, p, q, with p and q odd primes.
- The Diophantine equation $x^2 + q^{2m} = 2 \cdot 2005^p$ does not admit a solution in integers x, m, p, q, with p and q odd primes.

- There exists a solution of the Diophantine equation $x^2 + q^4 = 2y^p$ in positive integers x, y, p, q, with p and q odd primes.
- The Diophantine equation $x^2 + q^{2m} = 2 \cdot 2005^p$ does not admit a solution in integers x, m, p, q, with p and q odd primes.
- Let C be the curve given by

$$Y^2 = X^6 - 17X^4 - 20X^2 + 36.$$

Then $C(\mathbb{Q}) = \{\infty^-, \infty^+, (\pm 1, 0), (0, \pm 6)\}$.

- There exists a solution of the Diophantine equation $x^2 + q^4 = 2y^p$ in positive integers x, y, p, q, with p and q odd primes.
- The Diophantine equation $x^2 + q^{2m} = 2 \cdot 2005^p$ does not admit a solution in integers x, m, p, q, with p and q odd primes.
- Let C be the curve given by

$$Y^2 = X^6 - 17X^4 - 20X^2 + 36.$$

  Then $C(\mathbb{Q}) = \{\infty^-, \infty^+, (\pm 1, 0), (0, \pm 6)\}$.
- One can use TEX not only for typesetting but also for resolving Diophantine equations.

- There exists a solution of the Diophantine equation $x^2 + q^4 = 2y^p$ in positive integers x, y, p, q, with p and q odd primes.
- The Diophantine equation $x^2 + q^{2m} = 2 \cdot 2005^p$ does not admit a solution in integers x, m, p, q, with p and q odd primes.
- Let C be the curve given by

  $$Y^2 = X^6 - 17X^4 - 20X^2 + 36.$$

  Then $C(\mathbb{Q}) = \{\infty^-, \infty^+, (\pm 1, 0), (0, \pm 6)\}$.
- One can use TEX not only for typesetting but also for resolving Diophantine equations.
- Klaar is kész.

$C(\mathbb{Q}) \longleftrightarrow E(\mathbb{Q}(\alpha))$

Tekintsük a következő görbét:

$$\mathcal{C}: \quad Y^2 = f_3X^6 + f_2X^4 + f_1X^2 + f_0 =: F(X),$$

ahol $f_i \in \mathbb{Z}$ és F diszkriminánsa nem nulla.

$\mathcal{C}(\mathbb{Q}) \longleftrightarrow E(\mathbb{Q}(\alpha))$

Tekintsük a következő görbét:

$$\mathcal{C}: \quad Y^2 = f_3X^6 + f_2X^4 + f_1X^2 + f_0 =: F(X),$$

ahol $f_i \in \mathbb{Z}$ és F diszkriminánsa nem nulla.

- $\mathcal{C}$ génusza 2

$C(\mathbb{Q}) \longleftrightarrow E(\mathbb{Q}(\alpha))$

Tekintsük a következő görbét:

$$\mathcal{C}: \quad Y^2 = f_3X^6 + f_2X^4 + f_1X^2 + f_0 =: F(X),$$

ahol $f_i \in \mathbb{Z}$ és F diszkriminánsa nem nulla.

- $\mathcal{C}$ génusza 2
- ha $\mathcal{J}_{\mathcal{C}}$ rangja < 2

$C(\mathbb{Q}) \longleftrightarrow E(\mathbb{Q}(\alpha))$

Tekintsük a következő görbét:

$$\mathcal{C}: \quad Y^2 = f_3X^6 + f_2X^4 + f_1X^2 + f_0 =: F(X),$$

ahol $f_i \in \mathbb{Z}$ és F diszkriminánsa nem nulla.

- $\mathcal{C}$ génusza 2
- ha $\mathcal{J}_{\mathcal{C}}$ rangja < 2
- Chabauty-módszer alkalmazható

$C(\mathbb{Q}) \longleftrightarrow E(\mathbb{Q}(\alpha))$

Tekintsük a következő görbét:

$$\mathcal{C}: \quad Y^2 = f_3X^6 + f_2X^4 + f_1X^2 + f_0 =: F(X),$$

ahol $f_i \in \mathbb{Z}$ és F diszkriminánsa nem nulla.

- $\mathcal{C}$ génusza 2
- ha $\mathcal{J}_{\mathcal{C}}$ rangja < 2
- Chabauty-módszer alkalmazható
- ha $\mathcal{J}_{\mathcal{C}}$ rangja > 1

$C(\mathbb{Q}) \longleftrightarrow E(\mathbb{Q}(\alpha))$

Tekintsük a következő görbét:

$$\mathcal{C}: \quad Y^2 = f_3X^6 + f_2X^4 + f_1X^2 + f_0 =: F(X),$$

ahol $f_i \in \mathbb{Z}$ és F diszkriminánsa nem nulla.

- $\mathcal{C}$ génusza 2
- ha $\mathcal{J}_{\mathcal{C}}$ rangja < 2
- Chabauty-módszer alkalmazható
- ha $\mathcal{J}_{\mathcal{C}}$ rangja > 1
- ?

Elliptikus Chabauty

- $\phi_1 : (X, Y) \longrightarrow (X^2, Y)$

Elliptikus Chabauty

- $\phi_1 : (X, Y) \longrightarrow (X^2, Y)$
- $\mathcal{E}^a : \quad Y^2 = F^a(x) = f_3x^3 + f_2x^2 + f_1x + f_0$

Elliptikus Chabauty

- $\phi_1 : (X,Y) \longrightarrow (X^2, Y)$
- $\mathcal{E}^a : \quad Y^2 = F^a(x) = f_3x^3 + f_2x^2 + f_1x + f_0$
- $\phi_2 : (X,Y) \longrightarrow (1/X^2, Y/X^3)$

Elliptikus Chabauty

- $\phi_1 : (X, Y) \longrightarrow (X^2, Y)$
- $\mathcal{E}^a : \quad Y^2 = F^a(x) = f_3x^3 + f_2x^2 + f_1x + f_0$
- $\phi_2 : (X, Y) \longrightarrow (1/X^2, Y/X^3)$
- $\mathcal{E}^b : \quad Y^2 = F^b(x) = f_0x^3 + f_1x^2 + f_2x + f_3$

Elliptikus Chabauty

- $\phi_1 : (X, Y) \longrightarrow (X^2, Y)$
- $\mathcal{E}^a : \quad Y^2 = F^a(x) = f_3x^3 + f_2x^2 + f_1x + f_0$
- $\phi_2 : (X, Y) \longrightarrow (1/X^2, Y/X^3)$
- $\mathcal{E}^b : \quad Y^2 = F^b(x) = f_0x^3 + f_1x^2 + f_2x + f_3$
- Tegyük fel, hogy F^a irreducibilis és

$$\{(x_1, Y_1), \ldots, (x_m, Y_m)\}$$

egy reprezentációja $\mathcal{E}^a(\mathbb{Q})/2\mathcal{E}^a(\mathbb{Q})-$nak.

A μködő leképezés

Legyen α gyöke $F^a(x)-$nek.

$$\mu : \mathcal{E}^a(\mathbb{Q}) \longrightarrow \mathbb{Q}(\alpha)^*/(\mathbb{Q}(\alpha)^*)^2$$

$$(x, Y) \mapsto f_3(x-\alpha), \quad \mu(\infty) = 1$$

$(x, Y)-$hoz létezik (x_i, Y_i) úgy, hogy $(x, Y) + (x_i, Y_i) \in 2\mathcal{E}^a(\mathbb{Q})$
ker $\mu = 2\mathcal{E}^a(\mathbb{Q})$ így $(x-\alpha)(x_i-\alpha) \in \mathbb{Q}(\alpha)^2$
$F^a(x) = (x-\alpha)(f_3x^2 + (f_2+\alpha f_3)x + (f_1+\alpha f_2+\alpha^2 f_3)) = Y^2 \in \mathbb{Q}(\alpha)^2$
$x = X^2 \in \mathbb{Q}(\alpha)^2$

$$(x_i-\alpha)x(f_3x^2 + (f_2+\alpha f_3)x + (f_1+\alpha f_2+\alpha^2 f_3)) = y^2$$

Tétel (Flynn,Wetherell). *Legyen* $F^a(x) = f_3(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ *(nem feltétlenül irreducibilis), tegyük fel, hogy* $(X,Y) \in \mathcal{C}(\mathbb{Q})$ *és* $x = X^2$*. Ekkor van olyan* $1 \le i \le m$*, hogy* x *kielégíti a következő egyenleteket:*

$$\mathcal{E}^a_{i,k}: \quad y_k^2 = (x_i - \alpha_k)xF^a(x)/(x-\alpha_k), \quad k = 1,2,3,$$

ahol $y_k \in \mathbb{Q}(\alpha_k)$ *és* $(x_i - \alpha_k) = f_3$*, ha* $(x_i, Y_i) = \infty$ *és* $(x_i - \alpha_k) = f_3 \prod_{k \neq i}(x_i - \alpha_k)$*, ha* $x_i = \alpha_k$*.*

A F-W tétel alkalmazása

$$Y^2 = X^6 - 17X^4 - 20X^2 + 36 = (X-1)(X+1)(X^2-18)(X^2+2)$$

$$F^a(x) = (x-18)(x-1)(x+2)$$

∞	$E_{\infty,1} : y^2 = x(x-1)(x+2)$
$T_1 = (-2:0:1)$	$E_{1,1} : y^2 = -20x(x-1)(x+2)$
$T_2 = (1:0:1)$	$E_{2,3} : y^2 = 3x(x-18)(x-1)$
$G = (0:-6:1)$	$E_{3,1} : y^2 = -18x(x-1)(x+2)$
$T_1 + T_2$	$E_{4,3} : y^2 = 20x(x-18)(x-1)$
$T_1 + G$	$E_{5,1} : y^2 = 10x(x-1)(x+2)$
$T_2 + G$	$E_{6,1} : y^2 = 34x(x-1)(x+2)$

$$C(\mathbb{Q}) = \{\infty^-, \infty^+, (\pm 1, 0), (0, \pm 6)\}$$

$(x, y) \in \mathcal{E}(\mathbb{Q}(\alpha)), x \in \mathbb{Q}$

Legyen $\mathcal{E}: \ y^2 = g_3x^3 + g_2x^2 + g_1x + g_0$ elliptikus görbe $\mathbb{Q}(\alpha)$ felett.

$$z = -x/y, \quad w = -1/y, \quad w = g_3z^3 + g_2z^2w + g_1zw^2 + g_0w^3$$

Rekurzív helyettesítéssel:

$$w = w(z) \in \mathbb{Z}[g_0, g_1, g_2, g_3][[z]].$$

Szintén hatványsort kapunk $1/x-$re:

$$1/x = 1/x(z) \in \mathbb{Z}[g_0, g_1, g_2, g_3][[z]].$$

Két pont összegének $x-$koordinátája:

$$((x_0, y_0)+(x, y))_x = \frac{w(1 + y_0w)^2 - (g_2w + g_3z + g_3x_0w)(z - x_0w)^2}{g_3w(z - x_0w)^2} \in \mathbb{Z}[g_0, g_1, g_2, g_3, x_0, y_0][[z]]$$

Redukált görbe: $\tilde{\mathcal{E}}: \quad y^2 = \tilde{g}_3 x^3 + \tilde{g}_2 x^2 + \tilde{g}_1 x + \tilde{g}_0.$

$$\mathcal{E}(\mathbb{Q}(\alpha)) = \langle \mathcal{E}(\mathbb{Q}(\alpha))_{tors}, P_1, \ldots, P_r \rangle$$

Az $\tilde{\mathcal{E}}$ görbén P_i már torzió,

$$Q_i = m_i P_i.$$

$$\mathcal{S} = \{T + k_1 P_1 + \ldots + k_r P_r\}.$$

Bármely P pontra

$$P = S + n_1 Q_1 + \ldots + n_r Q_r.$$

A megoldásszámot korlátozó hatványsorok:

$$\theta_\infty(n_1, \ldots, n_r) = (n_1 Q_1 + \ldots + n_r Q_r)_x^{-1} \in \mathbb{Z}_p[\alpha][[n_1, \ldots, n_r]],$$

$$\theta_S(n_1, \ldots, n_r) = (S + n_1 Q_1 + \ldots + n_r Q_r)_x \in \mathbb{Z}_p[\alpha][[n_1, \ldots, n_r]],$$

θ_S felbontása

$$\theta_S = \theta_S^{(0)} + \theta_S^{(1)}\alpha + \ldots + \theta_S^{(d-1)}\alpha^{d-1},$$

ahol $\theta_S^{(i)} = \theta_S^{(i)}(n_1, \ldots, n_r) \in \mathbb{Z}_p[[n_1, \ldots, n_r]]$
A P pont $x-$koordinátája racionális, ezért

$$\theta_S^{(1)} = \ldots = \theta_S^{(d-1)} = 0,$$

a szereplő hatványsorok megoldásszamára Strassman-tételével nyerhetünk korlátot, ha ez megegyezik az ismert pontok számával készen vagyunk.

Dem´janenko-Manin-módszer

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

Ekkor $\mathcal{E}^a = \mathcal{E}^b$.

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

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

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

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

$(\phi_1 + \phi_2)(X, Y) = (f_+(X), Yg_+(X))$ és $(\phi_1 - \phi_2)(X, Y) = (f_-(X), Yg_-(X))$, ahol

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

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

Tegyük fel, hogy $\mathcal{E}^a(\mathbb{Q}) = \langle \mathcal{E}^a(\mathbb{Q})_{tors}, R\rangle$ 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 $\hat{h}(\phi_2(P)) = m^2\hat{h}(R)$.

$$|\hat{h}(\phi_1(P))-\hat{h}(\phi_2(P))| \leq |\hat{h}(\phi_1(P))-h(\phi_1(P))|+|\hat{h}(\phi_2(P))-h(\phi_2(P))|+|h(\phi_1(P))-h(\phi_2(P))|$$

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