# Moduláris formák Hida családjainak nemkommutatív Iwasawa-elmélete

Zábrádi Gergely

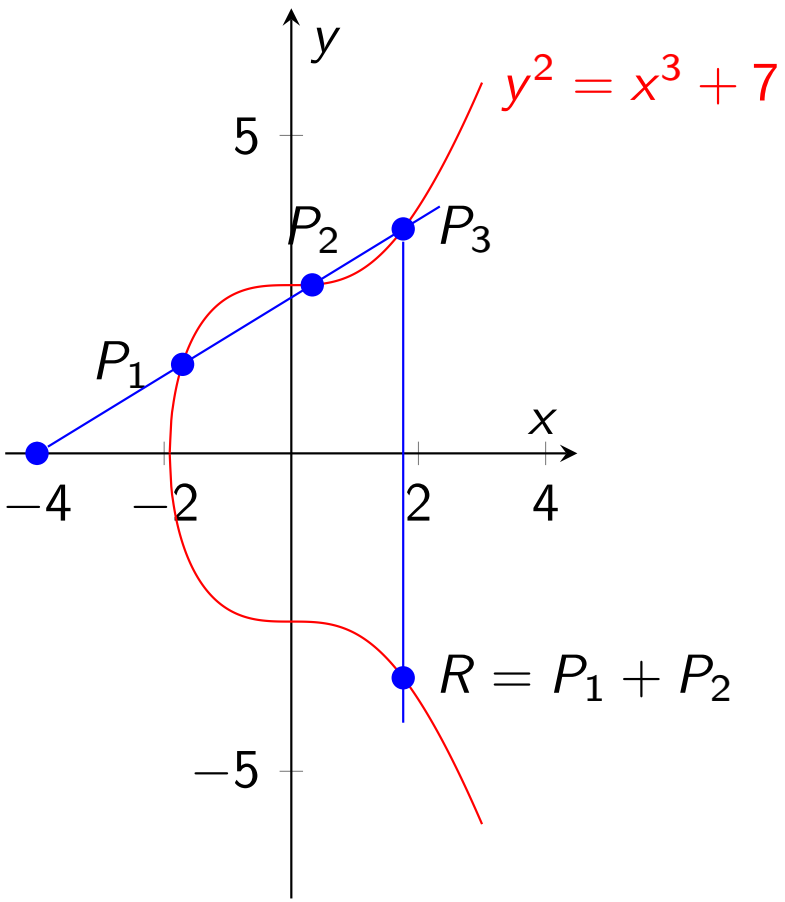
2022. január 13.

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE
HUNGARY

PROGRAM FINANCED FROM THE NRDI FUND

# Elliptikus görbék

$E\colon y^2 = x^3 + ax + b$ egy $\mathbb{Q}$ fölötti elliptikus görbe, $\mathbb{Q} \leq K (\leq \mathbb{C})$ egy testbővítés. Ekkor a $K$-racionális pontok $E(K)$ halmaza egy Abel-csoport:



# Elliptikus görbék

**Tétel (Mordell-Weil)**

Ha $K/\mathbb{Q}$ egy véges bővítés, akkor $E(K)$ egy végesen generált Abel-csoport.

Végesen generált Abel-csoportok alaptétele:

$$E(K) \cong \mathbb{Z}^{r_{E,K}} \oplus E(K)_{tors} \ .$$

Konkrét $E$ és $K$ esetén $E(K)_{tors}$ viszonylag könnyen kiszámolható: $E(K)_{tors} \leq E(\mathbb{C})_{tors} \cong (\mathbb{Q}/\mathbb{Z})^2$, sőt

**Tétel (Mazur, 1978)**

$$E(\mathbb{Q})_{tors} \cong \begin{cases} C_n, \text{ ahol } 1 \leq n \leq 10 \\ C_{12} \\ C_{2n} \oplus C_2, \text{ ahol } 1 \leq n \leq 4 \ . \end{cases}$$

# A Mordell–Weil rang

Fő kérdés: mennyi $r_{E,K}$?

- Bhargava–Shankar (2015): Az $r_{E,\mathbb{Q}}$ rang „átlaga" az összes $E$ görbére legfeljebb $7/6$
- Legnagyobb ismert rangú görbe (Elkies, 2006):

$$y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x + 3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$$

  rangja $\geq 28$
- megoldatlan, hogy $r_{E,\mathbb{Q}}$ korlátos-e
- $r_{E,\mathbb{Q}}$ kiszámítása $\rightsquigarrow$ Birch–Swinnerton-Dyer sejtés

# Elliptikus görbék $L$-függvénye

**Tétel (Hasse, 1933)**

Ha $E$ sima modulo $p$, akkor

$$|(p+1) - \#E(\mathbb{F}_p)| \leq 2\sqrt{p}$$

Birch és Swinnerton-Dyer (Cambridge, 196x) számításai konkrét görbékre $\rightsquigarrow$ sejtés:

$$\prod_{p \leq x} \frac{\#E(\mathbb{F}_p)}{p} \sim C \log(x)^{r_{E,\mathbb{Q}}} \qquad (x \to \infty) \ .$$

Legyen $a_p := p + 1 - \#E(\mathbb{F}_p)$ és $p$ „rossz", ha $E$ nem sima modulo $p$, továbbá

$$L(E/\mathbb{Q}, s) := \prod_{\text{rossz } p} \frac{1}{1 - a_p p^{-s}} \prod_{\text{jó } p} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

# A Birch–Swinnerton-Dyer sejtés

Ugyan a fenti szorzat csak $\mathrm{Re}(s) > 3/2$ esetén konvergál, de heurisztikusan:

$$L(E/\mathbb{Q},1) \approx \prod_{\text{jó } p}(1 - a_p p^{-1} + p^{-1})^{-1} = \prod_{\text{jó } p} \frac{p}{p - a_p + 1} = \prod_{\text{jó } p} \frac{p}{\#E(\mathbb{F}_p)}$$

**Tétel (Wiles, Taylor–Wiles, Breuil–Conrad–Diamond–Taylor, 2001)**

$\mathbb{Q}$ fölött minden elliptikus görbe moduláris, azaz $L(E/\mathbb{Q},s)$ folytatható holomorf módon az egész komplex síkra.

**Sejtés (Birch és Swinnerton-Dyer)**

Az $L(E/\mathbb{Q},s)$ függvénynek pontosan $r_{E,\mathbb{Q}}$-szoros gyöke van $s = 1$-ben.

# Mit tudunk a BSD-sejtésről?

**Tétel (Coates–Wiles, 1977)**

Tegyük fel, hogy $E$-n van komplex szorzás (azaz $E$ endomorfizmusgyűrűje szigorúan nagyobb, mint $\mathbb{Z}$). Ekkor ha $L(E/\mathbb{Q}, 1) \neq 0$, akkor $E(\mathbb{Q})$ véges, azaz $r_{E,\mathbb{Q}} = 0$.

**Tétel (Gross–Zagier, 1986)**

Tegyük fel, hogy $E$ moduláris (2001 óta ezt tudjunk minden $E$-re). Ekkor ha $L(E/\mathbb{Q}, s)$-nek elsőrendű nullhelye van $s = 1$-ben, akkor $E(\mathbb{Q})$ végtelen, azaz $r_{E,\mathbb{Q}} > 0$.

**Tétel (Kolyvagin, 1989)**

Ha $E$ moduláris és $L(E/\mathbb{Q}, s)$-nek legfeljebb elsőrendű nullhelye van $s = 1$-ben, akkor igaz a BSD sejtés.

# Mit tudunk a BSD-sejtésről?

**Tétel (Nekovář 2009, Dokchitser–Dokchitser 2010)**

Amennyiben a $Ш(E/\mathbb{Q})$ $p$-hatványrendű torziórésze véges valamely $p$ prímre, akkor az analitikus és algebrai rang azonos paritású.

**Tétel (Bharghava–Shankar 2015)**

Az elliptikus görbék nagy részének (legalább $83,75\%$-ának) a rangja legfeljebb 1, tehát igaz rá a BSD-sejtés. Az átlagos rang legfeljebb $7/6$.

A fenti tételek közül Coates–Wiles, Kolyvagin, Dokchitser–Dokchitser módszere: Iwasawa-elmélet!

# Iwasawa-elmélet – analitikus oldal

Rögzítsünk egy $p$ prímet és legyen $\chi\colon (\mathbb{Z}/p^n\mathbb{Z})^\times \to \mathbb{C}^\times$ egy mod $p^n$ multiplikatív karakter ($n \geq 1$). A ($\chi$-vel) csavart $L$-függvénye $E$-nek:

$$L(E,\chi,s) := \prod_{\text{rossz } q} \frac{1}{1-\chi(q)a_q q^{-s}} \prod_{\text{jó } q} \frac{1}{1-\chi(q)a_q q^{-s}+\chi(q)^2 q^{1-2s}}$$

Kicsit általánosabban, ha $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\overline{\mathbb{Q}})$ egy Galois-reprezentáció, akkor van egy $L(E,\rho,s)$ csavart $L$-függvény.

**Deligne periódus-sejtése (1979)**

$L^*(E,\rho) := \frac{L(E,\rho,1)}{\Omega_+(E)^{\dim \rho_+}\Omega_-(E)^{\dim \rho_-}} \in \overline{\mathbb{Q}}$, ahol $\Omega_\pm(E)$ az $E$ görbének egy periódusa: az $E(\mathbb{C})$ tóruszon értelmezett $\omega_E$ kanonikus differenciál integrálja egy zárt görbén.

# Iwasawa-elmélet – algebrai oldal

Selmer és Tate-Safarevics csoportok:

$$0 \to \mathbb{Q}_p/\mathbb{Z}_p \otimes E(K) \to \mathrm{Sel}_{p^\infty}(E/K) \to Ш(E/K)[p^\infty] \to 0$$

**Tate-Safarevics sejtés**

$Ш(E/K)$ véges.

Másrészt $\mathbb{Q}_p/\mathbb{Z}_p \otimes E(K) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{r_{E,K}}$, tehát ha igaz a T-S-sejtés, akkor $\mathrm{Sel}_{p^\infty}(E/K) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{r_{E,K}} \oplus$véges.
Legyen $K_\infty/\mathbb{Q}$ egy végtelen Galois bővítés, pl. $K_\infty = \mathbb{Q}(\mu_{p^\infty})$ (körosztási), $\mathbb{Q}(\mu_{p^\infty}, \sqrt[p^\infty]{m})$ („hamis Tate-görbe bővítés") vagy $K_\infty = \mathbb{Q}(E[p^\infty])$ („$\mathrm{GL}_2$-bővítés") és

$$\mathrm{Sel}_{p^\infty}(E/K_\infty) := \varinjlim_{\mathbb{Q} \leq \textbf{véges} K \leq K_\infty} \mathrm{Sel}_{p^\infty}(E/K) \ .$$

# Iwasawa-elmélet – algebrai oldal

Legyen $G := \mathrm{Gal}(K_\infty/K)$ és $X(E/K_\infty) := \mathrm{Hom}(\mathrm{Sel}_{p^\infty}(E/K_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$. Ekkor $X(E/K_\infty)$ egy végesen generált $\mathbb{Z}_p[[G]]$-modulus (Iwasawa-algebra).

**Sejtés (Coates–Sujatha, 200x)**

Ha $\mu_{p^\infty} \subset K_\infty$ és $E$-nek jó közönséges redukciója van modulo $p$, akkor $X(E/K_\infty)/X(E/K_\infty)(p)$ végesen generált a $\mathbb{Z}_p[[H]]$ Iwasawa algebra fölött is, ahol $H = \mathrm{Gal}(K_\infty/\mathbb{Q}(\mu_{p^\infty}))$.

Létezik egy $S \subset \mathbb{Z}_p[[G]]$ multiplikatív részhalmaz, hogy $\mathbb{Z}_p[[G]]_S \otimes_{\mathbb{Z}_p[[G]]} M = 0 \Leftrightarrow M$ végesen generált $/\mathbb{Z}_p[[H]]$. Algebrai $K$-elmélet lokalizálás hosszú egzakt sorozata:

$$K_1(\mathbb{Z}_p[[G]]) \to K_1(\mathbb{Z}_p[[G]]_S) \xrightarrow{\partial} K_0(\mathfrak{M}_H(G)) \to 0 \ .$$

Ha $\rho\colon G \to \mathrm{GL}_n(\overline{\mathbb{Q}})$ egy reprezentáció, $f \in K_1(\mathbb{Z}_p[[G]]_S)$, akkor $f(\rho) \in \overline{\mathbb{Q}_p} \cup \{\infty\}$.

# Az Iwasawa-elmélet fősejtése

**Nemkommutatív Iwasawa-elmélet fősejtése (Coates–Fukaya–Kato–Sujatha–Venjakob, 2006)**

Létezik egy $\mathcal{L}_{E,p} \in K_1(\mathbb{Z}_p[[G]]_S)$ „$p$-adikus $L$-függvény", melyre

(1) $\partial(\mathcal{L}_{E,p}) = [X(E/K_\infty)]$, azaz $\mathcal{L}_{E,p}$ egy karakterisztikus eleme a duális Selmernek

(2) minden $\rho\colon G \to \mathrm{GL}_n(\overline{\mathbb{Q}})$ reprezentációra $\mathcal{L}_{E,p}(\rho) = L^*(E, \rho, 1)$, azaz $\mathcal{L}_{E,p}$ interpolálja a (módosított) komplex $L$-értékeket.

Korábban: kommutatív fősejtések (Mazur, Coates, Greenberg, 1970-), hasonló fősejtések elliptikus görbék helyett más *motívum*okra, mint pl. az osztálycsoport. Kommutatív példa: $K_\infty = \mathbb{Q}(\mu_{p^\infty})$, $\mathbb{Z}_p[[G]] \cong \mathbb{Z}_p[[T]]$ hatványsorgyűrű, $f(T) = T(T+p)$,
$\partial(f(T)) = [\mathbb{Z}_p[[T]]/(T) \oplus \mathbb{Z}_p[[T]]/(T+p)]$,
$f(\chi) = f(\chi(1+p)-1) = (\chi(1+p)-1)(\chi(1+p)-1+p)$.

# Hida-családok

Legyen $\mathbb{Z}_p \subseteq R$ (tipikusan $R = \mathbb{Z}_p[[X]]$) egy lokális noether-gyűrű, ami „paraméterezi" moduláris formáknak egy $\mathcal{F}$ családját, azaz minden $\mathfrak{m} \lhd R$ maximális ideálhoz tartozik egy 2 súlyú $f_{\mathfrak{m}} \in \mathcal{F}$ ($p$-adikus) moduláris forma, $f_{\mathfrak{m}} \rightsquigarrow E_{\mathfrak{m}}$ elliptikus görbe.

**Projekt (Somnath Jha–Z)**

*a*) Tegyük fel, hogy adott $\mathfrak{m}_1, \ldots, \mathfrak{m}_k, \cdots \lhd R$ ideálokra ismerjük $X(E_{\mathfrak{m}_k}/K_\infty)$-t minden $k \geq 1$-re. Meghatározza ez $X(\mathcal{F}/K_\infty)$-t?

*b*) Ha igaz az Iwasawa-elmélet fősejtése az $\mathcal{F}$ család végtelen sok speciális elemére, következik-e ebből a fősejtés a többire?

# Cikkek és projektek

- A. Carter, K.S. Kedlaya, Z: Drinfeld's lemma for perfectoid spaces and overconvergence of multivariate $(\varphi, \Gamma)$-modules, *Documenta Mathematica* **26** (2021), 1329–1393. (Q1)
- J. Ray, F. Wei, Z: Multivariable $(\varphi, \Gamma)$-modules and Representations of Products of Galois Groups: The Case of Imperfect Residue Field, *Bull. Soc. Math. France* **149**(3) (2021), 521–546. (Q2)
- G. Cherubini, H. Wu, Z: On Kuznetsov–Bykovskii's formula of counting prime geodesics, *Math. Zeitschrift* **300** (2022), 881–928. (Q1)
- T. Csahók, P. Kutas, Z: Algorithmic applications of the corestriction of central simple algebras, kéziratban: arXiv:2007.06981
- M. Erdélyi, Á. Tóth, Z: Bounds for matrix Kloosterman sums, hamarosan beküldjük
- P. Maga, Z: Subconvexity bounds for Maass forms on general groups, kb. fél év még
- S. Jha, Z: Noncommutative Iwasawa theory for Hida families of modular forms, hosszútávú projekt