Alacsony rangú elliptikus görbék

Csahók Tímea

Témavezető:
Zábrádi Gergely

2021. június 9.

Áttekintés

- Elliptikus görbék

Áttekintés

- Elliptikus görbék
- A sejtés ismertetése

Áttekintés

- Elliptikus görbék
- A sejtés ismertetése
- Számítások

Áttekintés

- Elliptikus görbék
- A sejtés ismertetése
- Számítások
- Kitekintés

Elliptikus görbék

Definíció

Egy **elliptikus görbe** a k tökéletes test felett egy 1 génuszú görbe, amelyen ki van jelölve egy $O \in E(k)$ pont.

Elliptikus görbék

Definíció

Egy **elliptikus görbe** a k tökéletes test felett egy 1 génuszú görbe, amelyen ki van jelölve egy $O \in E(k)$ pont.

Általános egyenlet:

$$y^2z = x^3 + axz^2 + bz^3$$

Elliptikus görbék

Definíció

Egy **elliptikus görbe** a k tökéletes test felett egy 1 génuszú görbe, amelyen ki van jelölve egy $O \in E(k)$ pont.

Általános egyenlet:

$$y^2z = x^3 + axz^2 + bz^3$$

Definíció

Az $y^2z = x^3 + axz^2 + bz^3$ egyenletű görbe diszkriminánsa $\Delta = 4a^3 + 27b^2$.

A görbe pontosan akkor nemszinguláris, ha a diszkriminánsa nemnulla.

Elliptikus görbék

A görbét tekinthetjük $\mathbb{F}_p$ felett is (az együtthatókat modulo p redukálva).

Elliptikus görbék

A görbét tekinthetjük $\mathbb{F}_p$ felett is (az együtthatókat modulo p redukálva).

Definíció

A redukció p-nél **jó**, ha a görbe $\mathbb{F}_p$ felett is nemszinguláris.

Elliptikus görbék

A görbét tekinthetjük $\mathbb{F}_p$ felett is (az együtthatókat modulo p redukálva).

Definíció

A redukció p-nél **jó**, ha a görbe $\mathbb{F}_p$ felett is nemszinguláris.

Állítás

Ha $p \neq 2$, akkor pontosan akkor jó a redukció p-nél, ha $p \nmid \Delta$.

A görbét tekinthetjük $\mathbb{F}_p$ felett is (az együtthatókat modulo p redukálva).

Definíció

A redukció p-nél **jó**, ha a görbe $\mathbb{F}_p$ felett is nemszinguláris.

Állítás

Ha $p \neq 2$, akkor pontosan akkor jó a redukció p-nél, ha $p \nmid \Delta$.

Definíció

Az E elliptikus görbe **konduktora** $\Pi_{p \text{ rossz}} p^{f_p}$, ahol

$$f_p = \begin{cases} 1, & \text{ha } p\text{-nél multiplikatív a redukció} \\ \geq 2 & \text{különben} \end{cases}$$

Elliptikus görbék

Legyen E egy elliptikus görbe $\mathbb{Q}$ felett, amelyen nincs komplex szorzás, p pedig egy olyan prím, amelyre E-nek van jó közönséges redukciója modulo p.

Elliptikus görbék

Legyen E egy elliptikus görbe $\mathbb{Q}$ felett, amelyen nincs komplex szorzás, p pedig egy olyan prím, amelyre E-nek van jó közönséges redukciója modulo p.
Jelölje $F_\infty = \mathbb{Q}(E[p^\infty])$ a p-hatványrendű osztópontok által generált testet.

Elliptikus görbék

Legyen E egy elliptikus görbe $\mathbb{Q}$ felett, amelyen nincs komplex szorzás, p pedig egy olyan prím, amelyre E-nek van jó közönséges redukciója modulo p.
Jelölje $F_\infty = \mathbb{Q}(E[p^\infty])$ a p-hatványrendű osztópontok által generált testet.

Tétel (Serre nyílt leképezés)

Ebben az esetben $G = \mathrm{Gal}(F_\infty/\mathbb{Q})$ véges indexű részcsoportja $GL_2(\mathbb{Z}_p)$-nek.

Legyen E egy elliptikus görbe $\mathbb{Q}$ felett, amelyen nincs komplex szorzás, p pedig egy olyan prím, amelyre E-nek van jó közönséges redukciója modulo p.
Jelölje $F_\infty = \mathbb{Q}(E[p^\infty])$ a p-hatványrendű osztópontok által generált testet.

Tétel (Serre nyílt leképezés)

Ebben az esetben $G = \mathrm{Gal}(F_\infty/\mathbb{Q})$ véges indexű részcsoportja $GL_2(\mathbb{Z}_p)$-nek.

Legyen

$$\mathrm{Sel}_{p^\infty}(E/F_\infty) = \varinjlim_{\substack{\mathbb{Q}<F<F_\infty \\ F \text{ véges} \\ n\to\infty}} \mathrm{Sel}_{p^n}(E/F).$$

Definíció

Ha G kompakt p-adikus Lie-csoport, akkor a hozzá tartozó Iwasawa-algebra

$$\mathbb{Z}_p[[G]] = \varprojlim_{\substack{N \lhd G \\ \text{véges indexű,} \\ \text{nyílt}}} \mathbb{Z}_p[G/N].$$

Definíció

Ha G kompakt p-adikus Lie-csoport, akkor a hozzá tartozó Iwasawa-algebra

$$\mathbb{Z}_p[[G]] = \varprojlim_{\substack{N \lhd G \\ \text{véges indexű,} \\ \text{nyílt}}} \mathbb{Z}_p[G/N].$$

Legyen X a $\mathrm{Sel}_{p^\infty}(E/F_\infty)$ Pontryagin-duálisa, vagyis

$$X = \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Sel}_{p^\infty}(E/F_\infty), \mathbb{Q}/\mathbb{Z}),$$

Definíció

Ha G kompakt p-adikus Lie-csoport, akkor a hozzá tartozó Iwasawa-algebra

$$\mathbb{Z}_p[[G]] = \varprojlim_{\substack{N \lhd G \\ \text{véges indexű,} \\ \text{nyílt}}} \mathbb{Z}_p[G/N].$$

Legyen X a $\mathrm{Sel}_{p^\infty}(E/F_\infty)$ Pontryagin-duálisa, vagyis

$$X = \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Sel}_{p^\infty}(E/F_\infty), \mathbb{Q}/\mathbb{Z}),$$

ez egy modulus a $\mathbb{Z}_p[[G]]$ Iwasawa-algebra fölött.

Definíció

Ha G kompakt p-adikus Lie-csoport, akkor a hozzá tartozó Iwasawa-algebra

$$\mathbb{Z}_p[[G]] = \varprojlim_{\substack{N \lhd G \\ \text{véges indexű,} \\ \text{nyílt}}} \mathbb{Z}_p[G/N].$$

Legyen X a $\mathrm{Sel}_{p^\infty}(E/F_\infty)$ Pontryagin-duálisa, vagyis

$$X = \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Sel}_{p^\infty}(E/F_\infty), \mathbb{Q}/\mathbb{Z}),$$

ez egy modulus a $\mathbb{Z}_p[[G]]$ Iwasawa-algebra fölött.

Sejtés

Semely nemnulla $x \in X$ elem annullátorában sincs p-vel nem osztható centrumeleme $\mathbb{Z}_p[[G]]$-nek.

Eddigi eredmények

Coates (2003) foglalkozott először a témával, a konkrét $E = X_1(11)$ görbét vizsgálva.

Eddigi eredmények

Coates (2003) foglalkozott először a témával, a konkrét $E = X_1(11)$ görbét vizsgálva.

Állítás (Backhausz, Zábrádi)

Elég olyan E görbét találni, amelyre a körosztási test fölött még triviális a p^∞-Selmer, valamint a P_1 prímhalmaz 1 elemű, ahol

$$P_1 = \{l \text{ prím} \mid \text{elágazási indexe } \infty \text{ az } F_\infty \text{ bővítésben}$$

$$\text{és a redukció hasadó multiplikatív}\}.$$

Eddigi eredmények

Coates (2003) foglalkozott először a témával, a konkrét $E = X_1(11)$ görbét vizsgálva.

Állítás (Backhausz, Zábrádi)

Elég olyan E görbét találni, amelyre a körosztási test fölött még triviális a p^∞-Selmer, valamint a P_1 prímhalmaz 1 elemű, ahol

$$P_1 = \{l \text{ prím} \mid \text{elágazási indexe } \infty \text{ az } F_\infty \text{ bővítésben}$$

$$\text{és a redukció hasadó multiplikatív}\}.$$

Állítás (Backhausz)

Ha $p \geq 5$, akkor nem létezik a feltételeket teljesítő görbe.

Számítások

$$E : y^2 + (a+1)\,xy + y = x^3 + x^2$$

$\mathbb{Q}(\sqrt{-3})$ felett, ahol a az első primitív hatodik egységgyök.

Számítások

$$E : y^2 + (a+1)\,xy + y = x^3 + x^2$$

$\mathbb{Q}(\sqrt{-3})$ felett, ahol a az első primitív hatodik egységgyök.

$$G = \mathrm{Gal}\left(\mathbb{Q}(\sqrt{-3})(E[3^\infty]) \big/ \mathbb{Q}(\sqrt{-3})\right) \subset GL_2(\mathbb{Z}_3)$$

Számítások

$$E : y^2 + (a+1)\,xy + y = x^3 + x^2$$

$\mathbb{Q}(\sqrt{-3})$ felett, ahol a az első primitív hatodik egységgyök.

$$G = \mathrm{Gal}\left(\mathbb{Q}(\sqrt{-3})(E[3^\infty]) \big/ \mathbb{Q}(\sqrt{-3})\right) \subset GL_2(\mathbb{Z}_3)$$

Kérdés: G-ben van-e harmadrendű elem?

Kitekintés, további teendők

- E kilencedrendű pontjainak kiszámítása

Kitekintés, további teendők

- E kilencedrendű pontjainak kiszámítása
- Ellenőrizni, hogy E teljesíti-e a feltételeket

Kitekintés, további teendők

- E kilencedrendű pontjainak kiszámítása
- Ellenőrizni, hogy E teljesíti-e a feltételeket
- Az eddigi tétel kiterjesztése $p = 3$-ra

Kitekintés, további teendők

- E kilencedrendű pontjainak kiszámítása
- Ellenőrizni, hogy E teljesíti-e a feltételeket
- Az eddigi tétel kiterjesztése $p = 3$-ra
- $\mathbb{Q}$ felett valóban nem létezik ilyen görbe?

Kitekintés, további teendők

- E kilencedrendű pontjainak kiszámítása
- Ellenőrizni, hogy E teljesíti-e a feltételeket
- Az eddigi tétel kiterjesztése $p = 3$-ra
- $\mathbb{Q}$ felett valóban nem létezik ilyen görbe? Ha nem, miért nem?

Köszönöm a figyelmet!