Alacsony rangú elliptikus görbék

Csahók Tímea

Témavezető: Zábrádi Gergely

1 Bevezetés

Az előző félévben kezdtem el az algebrai görbék témakörével foglalkozni, az egyéni kutatómunka 1 tárgy keretében, akkor főleg a témával ismerkedve, egy jegyzetet feldolgozva. Ebben a félévben témavezetőm, Zábrádi Gergely egyik kutatási témájába tudtam bekapcsolódni, amely által még tovább tudtam mélyíteni a tudásomat az elliptikus görbék, az algebrai számelmélet, valamint az algebrai geometria témakörében.

2 A probléma ismertetése

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. Ekkor a Serre-féle nyílt leképezés tétel a következőt mondja:

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

A p^n-edik Selmer-csoportok alapján értelmezhetjük E p^∞-Selmer csoportját is, legyen

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

2.2. 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.

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

Ez a sejtés minden E görbére vonatkozik, azonban egyetlen E sem ismert, amelyre igazoltan teljesül, így az első célunk az, hogy találjunk egy ilyen E görbét. Ennek a sejtésnek az igazolása vagy cáfolása esetén is következtetéseket lehet levonni E Mordell-Weil rangjának aszimptotikus viselkedéséről az F_∞ toronyban.

Coates [3] cikkében a konkrét $E = X_1(11)$ görbével foglalkozik, itt a 7.10-es állítás a legfontosabb. A [2] cikkben sikerült ezt az állítást általánosabban kimondani, amelynek a 6.3-as következménye szerint elég olyan E görbét találni, amelyre a körosztási test fölött még triviális a p^∞-Selmer, valamint a P_1 prímhalmaz 1 elemű, ahol

$$P_1 = \{l \text{ prím} \mid \text{elágazási indexe } \infty \text{ az } F_\infty \text{ bővítésben és a redukció hasadó multiplikatív}\}.$$

Az [1] cikk szerint viszont ezeket a feltételeket teljesítő görbe nem létezik $p \geq 5$ esetén, tehát érdemes a $p = 3$ esettel foglalkozni. Itt ugyan nincs igazolva a [2] cikk 6.2-as tétele, de valószínű, hogy ebben az esetben is igaz.

3 Weil-párosítás

Ez a rész a [4] könyv 8. fejezetén alapszik. Legyen $n \geq 2$ egész, $p = \mathrm{char}\, K$. Egy $X \in E$ pont képét a divizor-osztálycsoportban (X)-szel fogjuk jelölni. Ha $T \in E[m]$ m-edrendű elem, akkor létezik egy T' pont, amelyre $mT' = T$. Legyen g egy olyan függvény, aminek a divizorja

$$\mathrm{div}\, g = \sum_{R \in E[m]} (T' + R) - (R).$$

Ha τ_S-sel jelöljük az $S \in E[m]$ elemmel való eltolást, akkor

$$\mathrm{div}(g \circ \tau_S) = \sum_{R \in E[m]} (T' + R + S) - (R + S) = \mathrm{div}\, g,$$

vagyis g és $g \circ \tau_S$ divizorjai megegyeznek, vagyis $e_m(S,T) = (g \circ \tau_S)/g = \mu$ konstans. Innen indukcióval adódik, hogy $g \circ \tau_S^i = \mu^i g$, és mivel $\tau_S^m = 1$, így azt kaptuk, hogy μ m-edik egységgyök, vagyis

$$e_m : E[m] \times E[m] \to \mu_m$$

Weil-párosítás.

3.1. Állítás. *A Weil-párosítás bilineáris, alternáló, nemelfajuló, Galois-invariáns, kompatibilis bilineáris forma.*

3.2. Tétel (Néron-Ogg-Safarevics-kritérium)**.** *Legyen K lokális test, $p = \operatorname{char} K$. Ekkor egy $l \neq p$ prím pontosan akkor ágazik el a $K(E[P^n])/K$ bővítés felett, ha E modulo l redukciója nem jó.*

3.3. Megjegyzés. A Weil-párosításból kapjuk, hogy p mindig elágazik.

4 Az a bizonyos görbe

Most tehát a $p = 3$ esettel foglalkozunk és a $\mathbb{Q}(\sqrt{-3})$ test feletti görbék körében vizsgálódunk. Tehát a keresett görbére mindenképp igaz, hogy pontosan egy prím van, ahol a redukciója hasadó multiplikatív, ez azzal ekvivalens, hogy a görbe konduktora prímhatvány (és ez a prím nem a 3). Az LMFDB adatbázis (The L-functions and Modular Forms Database) segítségével 73 konduktorral találtam 8 darab ilyen görbét, a legfeljebb 400 konduktorúak között nincs is több az adatbázis szerint. Ezt mindenképp fontos megjegyezni, még később vissza fogunk rá térni.

Így vizsgálódásunk fő tárgya ezentúl az $E : y^2 + (a+1)\,xy + y = x^3 + x^2$ görbe a $\mathbb{Q}(\sqrt{-3})$ test felett, ahol a az első primitív hatodik egységgyök.

A fő kérdésünk az, hogy ha $G = \operatorname{Gal}\left(\mathbb{Q}(\sqrt{-3})(E[3^\infty])/\mathbb{Q}(\sqrt{-3})\right) \subset GL_2(\mathbb{Z}_3)$, akkor G =-ben van-e harmadrendű elem?

Legyen $G_9 = \operatorname{Gal}\left(\mathbb{Q}(\sqrt{-3})(E[9])/\mathbb{Q}(\sqrt{-3})\right)$. Ha G_9-ben van olyan elem, amely modulo 9 kongruens egy harmadrendű elemmel $GL_2(\mathbb{Z}_3)$-ben, akkor G-ben mindenképp van harmadrendű elem, így az a célunk, hogy ezt a kérdést megválaszoljuk. Ehhez legyen K_9 $\mathbb{Q}(\sqrt{-3})$-nak $E[9]$-cel való bővítése, E_9 pedig az E görbe K_9 felett, ekkor E_9 torziócsoportja szolgáltat nekünk majd információt.

A $GL_2(\mathbb{Z}_3)$-beli harmadrendű elemekről tudjuk, hogy a determinánsuk 1 (a Weil-párosítás miatt), valamint hogy a nyomuk -1 (hiszen a két sajátérték pont a primitív harmadik egységgyökök), ilyen például a $\begin{pmatrix} -2 & -1 \\ 3 & 1 \end{pmatrix}$ mátrix és konjugáltjai.

5 Számítások

A konkrét görbére vonatkozó számításokat a Magma rendszerben végeztem. A végső cél a görbe kilencendrendű (komplex) pontjainak meghatározása, először azonban a harmadrendűeket határoztam meg.

5.1. Állítás. *[5] A $y^2 = x^3 + Ax^2 + Bx + C$ egyenletű görbe harmadrendű pontjai pontosan azok, amelyek x-koordinátája teljesíti az $3x^4 + 4x^3 + 6Bx^2 + 12Cx + 4AC - B^2 = 0$ egyenletet, valamint az origó.*

5.2. Állítás. *Az $E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ görbét a következőképpen tudjuk $y^2 = x^3 + Ax^2 + Bx + C$ alakra hozni:*

$$A = a_2 + \frac{a_1^2}{4}, \quad B = a_4 + \frac{a_1a_3}{2} \quad C = a_6 + \frac{a_3^2}{4}.$$

Az átalakítást visszafelé a koordináták között pedig $X = x$ és $Y = y - \frac{a_3}{2} - \frac{a_1}{2}x$ adja meg.

Ennek az állításnak a második fele megmutatja nekünk, hogy valóban nem számít, hogy melyik paraméterezésbeli koordinátákkal bővítünk. Először kiszámítottam az 5.1 állításban szereplő polinom felbontási testét, ez a racionálisak felett hatodfokúnak adódott. Ezen test felett tekintve a görbét, már 9 darab harmadfokú pontja volt, ami azt jelenti, hogy az y-koordinátákat is belevettük. Kilencedrendű pontból is csak 9 van (amik pont a harmadrendűek), így ahhoz, hogy mind a 81-et megkapjuk, még a kilencedrendű pontok koordinátáival is bővítenünk. Ehhez először az 5.1 állításhoz hasonló polinomiális feltételt kell adnunk a kilencedrendű pontok koordinátáira, amelyet az addíciós formulák segítségével lehet megtenni.

```
_<x> := PolynomialRing(Rationals());
K<a> := NumberField(x^2-x+1);
E<X,Y,Z> := EllipticCurve([a+1,1,1,0, 0]);
A := 1+(a+1)^2/4;
B := (a+1)/2;
```

```
C := 1/4;
R<y> := PolynomialRing(K);
f := 3*y^4+4*A*y^3+6*B*y^2+12*C*y+4*A*C-B^2;
L := SplittingField(f);
L;
_<z> := PolynomialRing(Rationals());
K1<alfa> := NumberField(9*z^6 + 15*z^5 + 25*z^4 + 16*z^3 + 9*z^2 + 4*z + 1);
R<y> := PolynomialRing(K1);
f := y^2-y+1;
Roots(f);
a := 1/3*(-18*alfa^5 - 21*alfa^4 - 35*alfa^3 - 7*alfa^2 - 5*alfa);
A := 1+(a+1)^2/4;
B := (a+1)/2;
C := 1/4;
g := 3*y^4+4*A*y^3+6*B*y^2+12*C*y+4*A*C-B^2;
Roots(g);
E1<X,Y,Z> := EllipticCurve([1/3*(-18*alfa^5 - 21*alfa^4 - 35*alfa^3 -
                        - 35*alfa^3 - 7*alfa^2 - 5*alfa) + 1 , 1 , 1 , 0 , 0]);
DivisionPoints(E1!0, 3);
TorsionSubgroup(E1);
```

6 További teendők

Az első és legfontosabb dolog, hogy az E görbének a kilencedrangú pontjait is kiszámítsuk. Ha ez a görbe teljesíti a kívánt feltételeket, akkor át kell dolgozni a [2] cikk 6.2-as tételét, hogy E-re valóban igaz legyen a sejtés. A másik érdekes kérdés, ami a vizsgálódások során felmerült, hogy az LMFDB adatbázis szerint $\mathbb{Q}$ felett nem találtunk megfelelő görbét. Meg lehetne vizsgálni, hogy valóban nem léteznek-e ilyen görbék, és ennek a kérdésnek a megválaszolása is közelebb vihet bennünket a sejtés igazolásához vagy cáfolásához.

Hivatkozások

[1] Backhausz, T. et al. (2015). Ranks of gl_2 Iwasawa modules of elliptic curves. *Functiones et Approximatio Commentarii Mathematici*, 52(2):283–298.

[2] Backhausz, T. and Zábrádi, G. (2015). Algebraic functional equations and completely faithful Selmer groups. *International Journal of Number Theory*, 11(04):1233–1257.

[3] Coates, J., Schneider, P., and Sujatha, R. (2003). Modules over Iwasawa algebras. *Journal of the Institute of Mathematics of Jussieu*, 2(1):73–108.

[4] Silverman, J. H. (2009). *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media.

[5] Tao, A. (2008). Points of finite order.