Néron-Ogg-Safarevics-kritérium

Szőri Vajk

May 2023

1. Bevezetés

A Néron-Ogg-Safarevics-kritérium olyan fontos eredmény a matematikában, amely összekapcsolja a számelmélet és az algebrai geometria két területét. Ez a kritérium arról szól, hogy hogyan lehet kapcsolatot találni egy elliptikus görbe és a hozzá kapcsolódó Galois-csoport között.
Az elliptikus görbék a matematika egyik alapvető tárgya, amelyek sok területen jelentőséggel bírnak, beleértve a kriptográfiát és a számelméletet.
A Néron-Ogg-Safarevics-kritérium azt mondja ki, hogy egy elliptikus görbének jó redukciója van pontosan akkor, amikor a $T_l(E)$ Tate modulus elágazásmentes v-n minden $l \neq char(k)$ prímre. A jó redukció azt jelenti, hogy a görbe képe is egy elliptikus görbe.
Ez a kritérium számos fontos következménnyel jár. Egyrészt lehetővé teszi, hogy a számelméleti tulajdonságokat az elliptikus görbék algebrai geometriájával összekapcsoljuk, ami lehetővé teszi számunkra, hogy gazdagabb és mélyebb megértést nyerjünk ezekről a struktúrákról. Másrészt a kritérium gyakorlati alkalmazásokat is hoz magával, például a prímtesteken való pontszámolás és a kriptográfia területén.
A tételek és állítások bizonyítása megtalálható [1]-ben

2. Szükséges definíciók és állítások

2.1. Definíció. Legyen R egy kommutatív egységelemes gyűrű. Egy (egyparaméteres) kommutatív formális csoport szabálynak nevezünk egy kétváltozós $F(X, Y) \in R[[X, Y]]$ formális hatványsort, ha az alábbi feltételek teljesülnek

1. $F(X,Y) = X + Y$+magasabb fokú tagok;
2. $F(X, F(Y,Z)) = F(F(X,Y), Z)$ (asszociativitás);
3. létezik egy $i_F(X) \in R[[X]]$ hatványsor, melyre $F(X, i_F(X)) = 0$ (inverz);
4. $F(X,Y) = F(Y,X)$(kommutativitás)

2.2. Definíció. Legyen E egy elliptikus görbe, amit meghatároz egy R-beli együtthatójú Weierstrass egyenlet. Ekkor az E-hez asszociált formális csoportot $\hat{E}$-vel jelöljük. Ezt a $F(z_1, z_2)$ hatványsor határozza meg. Ennek a pontos definíciója [1] IV/1-ben található (ez lényegében az elliptikus görbén vett összeadást írja le algebrailag).

2.3. Állítás. *Legyen F egy formális csoport az R gyűrű felett és legyen $m \in \mathbb{Z}$*
(a) $[m](T) = mT+$ (magasabb fokú tagok).
(b) Ha $m \in R^*$, akkor $[m] : F \to F$ egy izomorofizmus

A formális csoportok általában csak egy csoport operátort írnak le hozzátartozó csoport nélkül. Ugyanakkor, ha R egy lokális gyűrű és teljes, valamint az együtthatók M-ből, R maxmiális ideáljából vannak, akkor a formális csoportot meghatározó hatványsorok konvergálnak. Így egy csoport struktúrát adnak M-en.

2.4. Definíció. Jelölje $F(M)$ az F/R-hez asszociált csoportot, ami az M halmaz ellátva az alábbi műveletekkel

$$x \oplus_F y = F(x,y)$$
$$\ominus_F x = i_F(x)$$

, ahol $x, y \in M$. Hasonlóan definiálhatjuk $F(M^n)$-t, ami az M^n halmaz ellátva ugyanezekkel a műveletekkel.

2.5. Állítás. *Legyen F/R egy teljes lokális gyűrűn definiált formális csoport.*
(a) Minden $n \geq 1$-re, az identitás által indukált

$$\frac{F(M^n)}{F(M^{n+1})} \to \frac{M^n}{M^{n+1}}$$

leképezés egy csoport izomorfizmus.
(b) Legyen p a maradék test karakterisztikája. Ekkor minden véges rendű elem $F(M)$-ben p-vel osztható rendű.

A továbbiakban jelölje:
K lokális test, teljes egy v diszkrét értékelésre.
R $= \{x \in K : v(x) \geq 0\}$az egészek gyűrűje
$R^* = \{x \in K : v(x) = 0\}$az egységek gyűrűje
M $= \{x \in K : v(x) > 0\}$ R maximális idálja
π: $M = \pi R$
k $= R/M$ R-hez tartozó maradéktest
Legyen E/K egy elliptikus görbe, és legyen

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

a hozzá tartozó Weierstrass egyenlet. A $(x, y) \mapsto (u^{-2}x, u^{-3}y)$ behelyettesítés egy új egyenlethez vezet, amiben a_i helyett $u^i a_i$ szerepel, tehát ha olyan u-t választunk, ami osztható egy megfelelően nagy hatványával π-nek, akkor olyan Weierstrass egyenletet kapunk aminek minden együtthatója R beli. Ekkor a diszkrimináns $v(\Delta) \geq 0$. Mivel v diszkrét választhatjuk azt az ilyen Weierstrass egyenletet, amelyikre $v(\Delta)$ minimális.

2.6. Definíció. Legyen E/K egy elliptikus görbe. Egy E-hez tartozó Weierstrass egyenlet minimális, ha $v(\Delta)$ minimális azzal a feltétellel, hogy
$a_1, a_2, a_3, a_3, a_4, a_5, a_6 \in R$

3. modulo π redukció

A következőkben a modulo π redukciót vizsgáljuk, amit hullámvonallal jelölünk. Tehát például, a természetes redukció: $R \to k = R/\pi R, t \mapsto \tilde{t}$. Választva E/K-hoz egy minimális Weierstrass egyenletet redukálhatjuk annak együtthatóit és így kapunk egy k beli görbét:

$$\tilde{E} : y^2 + \tilde{a_1}xy + \tilde{a_3}y = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6}$$

Ezt a görbét, $\tilde{E}/k$-t, hívjuk E modulo π redukciójának. Mivel egy minimális egyenletből indultunk ki, így az $\tilde{E}$-hez tartozó egyenlet koordináta csere erejéig egyértelmű k felett.
Most legyen $P \in E(K)$. Meg tudunk adni homogén koordinátákat $P = [x_0, y_0, z_0]$, hogy $x_0, y_0, z_0 \in R$ és legalább az egyik R^* beli. Ekkor a redukált pont

$$\tilde{P} = [\tilde{x_0}, \tilde{y_0}, \tilde{z_0}]$$

$\tilde{E}(k)$-ban van. Ez egy $E(K) \to \tilde{E}(k), P \mapsto \tilde{P}$ redukció.
Általánosabban megadhatunk egy $\mathbb{P}^n(K) \to \mathbb{P}^n(k)$ redukciót. Ekkor az $\tilde{E}/k$ görbe lehet szinguláris, de a nemszinguláris pontok egy $\tilde{E}_{ns}(k)$ részcsoportot alkotnak. Vegyük $E(K)$ két részhalmazát:

$$E_0(K) = \{P \in E(K) : \tilde{P} \in \tilde{E}_{ns}(k)\},$$
$$E_1(K) = \{P \in E(K) : \tilde{P} = \tilde{\mathcal{O}}\}$$

3.1. Állítás. *Létezik Abel csoportok egy egzakt sorozata*

$$0 \to E_1(K) \to E_0(K) \to \tilde{E}_{ns}(k) \to 0$$

ahol a jobboldali leképezés egy π redukció.

3.2. Állítás. *Legyen E/K egy minimális Weierstrass egyenlettel megadva, legyen $\hat{E}/R$ az E-vel asszociált formális csoport, és legyen $w(z) \in R[[x]]$ egy hatványsor ami egy átparaméterezés után az egyik koordinátát fejezi ki a másik függvényében(pontos definícióért [1] IV/1). Ekkor a*

$$\hat{E}(M) \to E_1(K), z \mapsto \left(\frac{z}{w(z)}, \frac{1}{w(z)}\right)$$

leképezés egy csoport izomorfizmus.

3.3. Definíció. Legyen E/K egy elliptikus görbe, és legyen $\tilde{E}$ a redukáltja E egy minimális Weierstrass egyenletének modulo M. E-nek jó redukciója van, ha $\tilde{E}$ nem szinguláris.

Meg lehet még különbőztetni két fajta "rossz" redukciót(multiplikatív,additív), amik egy-egy szingularitás(node, cusp) típushoz tartoznak.

3.4. Állítás. *Legyen E/K egy elliptikus görbe. E-nek pontosan akkor van jó redukciója, ha $v(\Delta) = 0$*

4. Véges rendű pontok

4.1. Definíció. Legyen E/K egy elliptikus görbe. E m-torzió pontjai E-nek, $E[m]$-mel jelölve, azok a pontok amelyek rangja osztja m-et

$$E[m] = \{P \in E : [m]P = 0\} = ker([m]).$$

4.2. Állítás. *Legyen E/K egy elliptikus görbe. Minden $m \in \mathbb{Z}$-re, ami relatív prím $char(K)$-val*

$$E[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$$

4.3. Definíció. Legyen E/K egy elliptikus görbe és legyen $l \in \mathbb{Z}$ egy prím szám. Ekkor E l-adikus Tate modulusa az alábbi csoport:

$$T_l(E) = \varprojlim E[l^n],$$

ahol az inverz limeszt a $E[l^{n+1}] \xrightarrow{[l]} E[l^n]$ természetes leképezésekkel vesszük.

E véges rendű azaz torzió pontjai

$$E_{tors} = \bigcup_{m=1}^{\infty} E[m]$$

4.4. Állítás. *Legyen E/K egy elliptikus görbe és legyen $m \geq 1$ $char(K)$-val relatívprím egész szám. Ekkor $E_1(K)$-nak nincs nem triviális m-ed rendű pontja. Továbbá tegyük fel hogy $\tilde{E}/k$ nem szinguláris, ekkor a*

$$E(K)[m] \to \tilde{E}(k)$$

leképezés injektív.

5. Az inercia hatás

$\overline{K}/K$ inerciarészcsoportja I_v, ami $Gal(\overline{K}/K)$ azon elemei melyek triviálisan hatnak a maradék testen, $\overline{k}$ -n. Továbbá $I_v = Gal(\overline{K}/K^{nr})$, ahol K^{nr} a maximális olyan bővítése K-nak, ami elágazásmentes. Valamint

$$1 \to Gal(\overline{K}/K^{nr}) \to Gal(\overline{K}/K) \to Gal(\overline{k}/k) \to 1$$

egy rövid egzakt sorozat és $Gal(K^{nr}/K) \cong Gal(\overline{k}/k)$.

5.1. Definíció. Ha $Gal(\overline{K}/K)$ hat az Σ halmazon, akkor azt mondjuk Σ elágazásmentes v-n, ha I_v triviálisan hat Σ-n.

5.2. Állítás. *Legyen E/K egy elliptikus görbe jó redukcióval.*

1. *Legyen $m \geq 1$ egy $char(k)$-hoz relatívprím egész szám. Ekkor $E[m]$ elágazásmentes v-n*
2. *Legyen $l \neq char(k)$ egy prím. Ekkor $T_l(E)$ elágazásmentes v-n.*

6. Néron-Ogg-Safarevics-kritérium

6.1. Tétel (Kodira, Néron)**.** *Legyen K egy teljes diszkrét értékelésű test. Ekkor a $E(K)/E_0(K)$ csoport véges.*

6.2. Tétel (Néron-Ogg-Safarevics-kritérium)**.** *Legyen E/K egy elliptikus görbe. Ekkor a következők ekvivalensek:*

1. *E-nek jó redukciója van K-n*
2. *$E[m]$ elágazásmentes v-n minden $m \geq 1$-re ami relatívprím $char(k)$-val*
3. *A $T_l(E)$ Tate modulus elágazásmentes v-n minden $l \neq char(k)$ prímre*
4. *$E[m]$ elágazásmentes v-n végtelensok $m \geq 1$ $char(k)$-val relatívprím egész számra*

Hivatkozások

[1] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2009.