Eötvös Loránd Tudományegyetem

Természettudományi Kar

Mogyorósi Bálint

Elliptikus görbék aritmetikája

Egyéni kutatómunka
Matematika MSc
matematikus szakirány

Témavezető:

dr. Zábrádi Gergely

Algebra és Számelmélet Tanszék

Budapest, 2022

Tartalomjegyzék

Bevezetés

Az egyéni kutatómunkám fő célja elliptikus görbék vizsgálata a racionális számok teste fölött. Az aritmetikai geometriában ezek nagyon fontos objektumok, melyekhez rengeteg sejtés kapcsolódik. Ennek fő oka, hogy a racionális pontok halmaza egy Abel-csoportot alkot egy, a pontokon geometriai módon értelmezett műveletre. Nagell és Lutz tétele effektív módszert ad a görbén a véges rendű pontok megtalálására, egyben speciális esetként az is következik, hogy csak véges sok ilyen pont lehet. A másik fontos tétel, melynek a bizonyítását szeretném megérteni, Mordell és Weil tétele, mely szerint a racionális pontok csoportja végesen generált.

1. fejezet

Geometria és Aritmetika

1.1. Racionális pontok

A síkunkon egy pontot racionálisnak nezevünk ha minkét koordinátája racionális szám. Egy egyenest racionális egyenesnek hívunk ha az egyenes egyenletét feltudjuk írni racionális számokkal, azaz:

$$ax + by + c = 0$$

$a, b, c \in \mathbb{Q}$. Azt a tényt könnyen láthatjuk hogyha van két racionális pontunk akkor a rajtuk átmenő egyenes racionális egyenes lesz, egyszerűen csak fel kell írni az egyenes egyenletét. Ha van két racionális egyenesünk és ha van közös pontjuk akkor ez a pont racionális lesz, ezt abból láthatjuk, hogy egy egyenletrendszert oldunk meg aminek racionális együtthatói vannak így csak racionális eredményt kaphatunk.

Minket a görbéken lévő racionális pontok fognak érdekelni, az előzőekhez hasonlóan definiáljuk a racionális kúpot, legyen

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

a kúpunk egyenlete, akkor hívjuk racionálisnak ha minden együtthatója racionális. Ha ennek szeretnénk nézni a metszetét egy racionális egyenessel akkor az egyenletek megoldása során egy másodfokú egyneletet kapnánk aminek két megoldása lesz, de nem szükségszerűen lennének a megoldásai racionálisak, viszont ha tudjuk, hogy az egyik az akkor a másik is, ez a Viét formulák miatt van.

1.2. Harmadfokú görbék geometriája

Harmadfokú görbének hívjuk a következőt

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + jx + iy + j = 0$$

Azt mondjuk, hogy a harmadfokú görbe racionális ha az egyűttthatói racionálisak.
Egy egyenes a görbénket 3 pontban fogja metszeni, ezt kihasználva ha tudunk két racionális pontot a görbénken akkor az őket összekötő egyenesen lesz még egy harmadik racionális pont ami a görbénken is rajta van. Ez azért lesz mert ha felírjuk az egyenleteket egy harmadfokú polinomunk lesz aminek két gyökéről tudjuk, hogy racionális így a harmadik is az kell, hogy legyen.
Ezzel egy műveletet kapunk a görbénk racionális pontjainak halmazán ami két ponthoz rendel egy harmadikat amit $P*Q$ jelölünk, de ez még önmagában nem lesz csoportművelet mert nem szükségszerűen lesz egységelemünk.

Ahhoz, hogy ebből csoportműveletet csináljunk kicsit módosítanunk kell illetve kelleni fog találni egy racionális pontot a görbénken amit rögzítünk. A rögzített racionális pontunkat jelölje $\mathfrak{O}$. Ekkor P és Q pontunkhoz rendeljük hozzá $P * Q$ pontot, ezután nézzük a $(P * Q) * \mathfrak{O}$ pontot, ezt definiáljuk $P + Q$-nak. Ezzel már egy csoportműveletet definiáltunk aminek egységeleme $\mathfrak{O}$, valamint kommutatív is. Az inverzet a következő képpen kapjuk meg, vegyük $\mathfrak{O} * \mathfrak{O}$ pontot legyen S. Q inverze a $-Q = Q * S$ pont lesz, hiszen $-Q + Q = (-Q * Q) * \mathfrak{O} = (S) * \mathfrak{O} = \mathfrak{O}$, első lépésben a $-Q$ Q egyenesen a 3.pont S lesz a kontrukció miatt, de S és a kitüntetett pontunk egyenesén megint a kitüntetett pont lesz a 3. hisz S-et így definiáltuk.
Az asszociviatás is hasonló geometriai okoskodással kijön.

1.3. Weierstrass Normalizált alak

1.3.1. Definíció. *A projektív síkot az* $[a : b : c]$ *hármasok halmazának definiáljuk azokkal a kitételekkel, hogy*
(1) két pont ekvivalens $[a : b : c] \sim [a' : b' : c']$*, ha* $\exists t : a' = at$*,* $c' = ct$*,* $c' = ct$
(2) a $[0 : 0 : 0]$ *pontot nem vesszükbe a projektív síkunkba.*

Tegyük fel, hogy van egy harmadfokú görbénk a projektív síkon valamint a kitüntett $\mathfrak{O}$

pont, azt fogjuk megvalósítani, hogy úgy választjuk meg a tengelyeinket, hogy a görbénk egyenlete minél egyszerűbb legyen.
A $Z = 0$ tengelyt válasszuk a görbe $\mathfrak{O}$-beli érintőjének ez az egyenes még egy pontban metszi a görbénket, az itt lévő érintő lesz az $X = 0$ tengely, végül $Y = 0$ egy tetszőleges $\mathfrak{O}$-en átmenő egyenes ami nem a $Z = 0$.
Ezután ha áttérünk affin koordinátákra az $x = X/Z$ és $y = Y/Z$ megfeleltetésekkel, az egyenletünk a következő alakot ölti:

$$xy^2 + (ax + b)y = cx^2 + dx + e$$

eztán végigszorozva x-szel valamint az $y = xy$ helyetesítéssel élve:

$$y^2 + (ax + b)y = f(x)$$

ahol, $deg(f(x)) = 3$, ha $f(x)$ főegyütthatója nem 1 akkor helyetesítsük x-et és y-ot λx illetve $\lambda^2 y$-nal, így az egyenletünk Weierstrass alakja:

$$y^2 = x^3 + ax^2 + bx + c$$

Ha az $x^3 + ax^2 + bx + c$ nincs többszörös gyöke akkor a fenti görbét elliptikus görbének nevezzük.

1.4. Explicit képletek elliptikus görbén a csoport szabályra

$$y^2 = x^3 + ax^2 + bx + c$$

A fenti egyenletet szeretnénk homogenizálni, $x = X/Z$ és $y = Y/Z$:

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$$

Keressük a görbénk és a $Z = 0$ (végtelen beli) egyenes metszetét, vagyis a $X^3 = 0$ egyenlet megoldásait. Vagyis a görbénknek pontosan egy pontja lesz a végtelenben, az a pont ahol a függőleges egyenesek metszik egymást, ezt a pontot fogjuk mi $\mathfrak{O}$-nak választani.
Össze szeretnénk adni $P_1 = (x_1, y_1)$ illetve $P_2 = (x_2, y_2)$ pontokat. Első lépésben húzunk rajta egy egyenest és megkeressük a 3. metszéspontot, ez lesz $P_1 * P_2 = (x_3, y_3)$. Az $\mathfrak{O}$ választása miatt $P_1 + P_2$ a $P_1 * P_2$-nak az $x = 0$ egyenesre vett tükörképe lesz, mert $\mathfrak{O}$-ban

a függőleges egyenesek találkoznak vagyis 3.metszépont az $\mathfrak{O}$ *és* $P_1 * P_2 = (x_3, y_3)$ *által feszített egyenesen és a görbe metszete lesz de a görbénk szimmetrikus* $x = 0$*-ra így valóban a tükörképe lesz, koordinátákkal kifejezve* $P_1 + P_2 = (x_3, -y_3)$*. Tehát, hogy tudjuk számolni* $P_1 + P_2$ *elég* $P_1 * P_2$ *koordinátájit tudni.*
A P_1 *és* P_2 *pontok által feszített egyenes egyenlete:*
$y = \lambda x + \nu$*, ahol* $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ *és* $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$ *A konstrukció miatt tudjuk, hogy a görbénk* P_1*-ben és* P_2*-ben metszi az egyenesünket, a harmadik pontot ugy kaphatjuk meg, hogy az egyenes egyenletét behelyettesítjuk a görbénk egyenletébe:*

$$y^2 = (\lambda x + \nu)^2 = x^3 + ax^2 + bx + c$$

Tudjuk, hogy van két racionális gyöke így a harmadik is az kell legyen vagyis van gyöktényezős alakja, rendezve az egyenletet kajuk:

$$0 = x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = (x - x_1)(x - x_2)(x - x_3)$$

Nézzük meg mindkét oldalt x^2 *eggyütthatóját, ebből kapjuk, hogy:*

$$a - \lambda^2 = -x_1 - x_2 - x_3$$

ezt rendezve valamint felhasználva az egyenes egyenletét:

$$x_3 = \lambda^2 - a - x_1 - x_2 \qquad y_3 = \lambda x_3 + \nu$$

Ezzel a $P_1 + P_2$ *koordinátái:*

$$(\lambda^2 - a - x_1 - x_2, -\lambda(\lambda^2 - a - x_1 - x_2) - \nu)$$

2. fejezet

Véges rendű pontok

2.1. Diszkrimináns

Legyen egy racionális elliptikus görbénk:

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

Ha $x = d^2X$ és $y = d^3Y$ helyettesítésekkel élünk megfelelő d választással akkor eltüntethetjuk a, b, c nevezőit így kapva egy egész együthatós görbét, ezért szűkítsük le a vizsgálódásunkat egész együtthatós görbékre.
A görbénkhez rendelt diszkriminánst az alábbi egyenlettel defniálljuk:

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

2.1.1. Lemma. *Legyen $P = (x, y)$ egy pont az elliptikus görbénken, úgy hogy mind P és $2P$ is egészkoordinátájú. Ekkor $y = 0$ vagy $y|D$*

Bizonyítás. *Tegyük fel, hogy $y \neq 0$. Mivel $y \neq 0$ így $2P \neq \mathfrak{O}$, vagyis felírhatjuk $2P = (X, Y)$. Feltételünk miatt x, y, X, Y mind egészek. Alkalmazzuk rájuk az összeadó formulánkat:*

$$2x + X = \lambda^2 - a \qquad \lambda = \frac{f^{'}(x)}{2y}$$

Lambda egy racionális szám valamint x, X, a egészek és az egészek gyűrűt alkotnak így λ is muszáj egész legyen. Mivel $2y$ és $f(x)egszek, gy2y \mid f(x)$ speciálisan $y|f^{'}(x)$. Valamint $y|f(x)$. A diszkrinimáns kifejezhető $f(x)$ és $f^{'}(x)$ lineáris kombinációjaként:

$$D = r(x)f(x) + s(x)f^{'}(x)$$

ahol $r(x), s(x)$ egész együtthatós polinomok vagyis $y|D$. □

2.2. Véges rendű pontok egész koordinátájúak

2.2.1. Állítás. *Legyen p egy prím, és legyen R azon racionális számok gyűrűje ahol a nevező relatív prím p-hez, és $C(p^\nu)$ azon racionális (x, y) pontok halmaza a görbénkről ahol x nevezője osztható $p^{2\nu}$-vel, valmint tartalmazza $\mathfrak{O}$ pontot.*
(a) $C(p)$ tartalmazza az össze olyan racionális pontot amire vagy x vagy y nevezője osztható p-vel.
(b) Minden $\nu \geq 1$ esetén a $C(p^\nu)$ egy részcsoport $C(Q)$-ban.
(c) A leképezés

$$\frac{C(p^\nu)}{C(p^{3\nu})} \to \frac{p^\nu R}{p^{3\nu} R}, \qquad P = (x, y) \mapsto t(P) = \frac{x}{y}$$

egy injektív homomorfizmus.

2.2.2. Következmény. *(a) Minden p prímre, az egyetlen véges rendő pont a $C(p)$-ben az egység elem lesz, azaz $\mathfrak{O}$.*
(b) Legyen $P = (x, y) \in C(Q)$ egy racionális pont véges renddel, ekkor x és y is egészek.

2.3. Nagell-Lutz tétel

2.3.1. Tétel (Nagell-Lutz).

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

Egy nemszinguláris harmadrendű görbe egész együtthatókkal, és

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

diszkriminánssal. Legyen $P = (x, y)$ egy véges rendű racionális pont. Ekkor x és y egészek és vagy $y = 0$ ekkor P másodrendű vagy $y|D$.
Bizonyítás. *Az előző következmény miatt a P pontunk koordinátái egész számok, ha P rendje kettő akkor $y = 0$ ezzel az esettel kész vagyunk. Most tegyük fel, hogy a rend nem kettő. Ekkor $2P$ is egy véges rendű pont lesz, emiatt a koordinátái egészek lesznek és erre alkalmazva az előző alfejezetben a diszkriminánsra kimondott lemmát kapjuk, hogy y osztja D-t.* □

3. fejezet

A Mordell-Weil tétel

3.1. A magasság függvény

3.1.1. Definíció. *Legyen x egy racionális szám $x = m/n$ m és n relatív prímek. Ekkor x magasságán a következő pozitív egész számot értjük:*

$$H(x) = max(|m|, |n|)$$

3.1.2. Megjegyzés. *Azon racionális pontok halmaza mellyek kisebbek egy fix magasságnál egy véges halmaz.*

Mi esetünkben pontjaink vannak de itt úgy fogjuk értelmezni a magasságfüggvényt,hogy a P pontunk x koordinátájára fogjuk alkalmazni.
Azért, hogy a magasságfüggvényünknek ne multiplikatív hanem additív tulajdonsága legyen vesszük a logaritmusát $h(P) = logH(P)$.

$$\{P \in C(Q) : h(p) \leq M\}$$

egy véges halmaz lesz, meggondolható az előző megjegyzésből.

Az alábbi lemmákat nem bizonyítom csak kimondom, a bizonyításuk inkább technikai jellegű az összeadó képlettel való számoláson alapszik.

3.1.3. Lemma. *Minden valós M-re, a*

$$\{P \in C(Q) : h(p) \leq M\}$$

véges.

3.1.4. Lemma. *Legyen P_0 egy rögzített racionális pont C-n. Ekkor létezik egy κ_0 konstans ami csak P_0, a, b, c-től függ, amire:*

$$h(P + P_0) \leq 2h(P) + \kappa_0$$

minden $p \in C(Q)$.

3.1.5. Lemma. *Létezik egy konstans κ, ami csak a, b, c-től függ,amire:*

$$h(2P) \leq 4h(P) - \kappa$$

minden $p \in C(Q)$.

3.1.6. Lemma. *Az index $(C(Q) : 2C(Q))$ véges. Ahol a $2C(Q)$ részcsoport a $C(Q)$ képe a kettővel való szorzás homomorfizmusnál.*

3.1.7. Tétel (Leszállási Tétel). *Legyen Γ egy kommutatív csoport, és tegyük fel, hogy létezik egy függvény*

$$h : \Gamma \to [0, \infty)$$

a következő tulajdonságokkal:
(a) Minden valós M-re, a halmaz $\{P \in \Gamma : h(p) \leq M\}$ véges.
(b) Minden $P_0 \in \Gamma$-ra létezik egy κ_0 konstans, amire

$$h(P + P_0) \leq 2h(P) + \kappa_0$$

(c) Létezik egy κ konstans,hogy minden $P \in \Gamma$ esetén

$$h(2P) \leq 4h(P) - \kappa$$

Valamint
(d) A 2Γ részcsoport indexe véges Γ-ban.
Ekkor Γ egy végesen generált csoport lesz.

Bizonyítás. *Első lépésben válasszunk minden 2Γ mellékosztálynak egy Γ-beli reprezentánst. Tudjuk, hogy csak véges sok mellékosztály van legyen ezek száma n, és $Q_1, ..., Q_n$ pedig legyenek ezek reprezentásai.Ez azt jelenti, hogy minden $P \in \Gamma$, létezik egy i_1 P-től függő index amire*

$$P - Q_{i_1} \in 2\Gamma.$$

Ez azért van így mert P-t valamelyik mellékosztálynak tartalmaznia kell. Ezt átírhatjuk a következő formában

$$P - Q_{i_1} = 2P_1$$

valamilyen $P_1 \in \Gamma$. *Ezt ezután elvégezzük a* P_1*-re is. Folytatva ezt a folyamatot kapjuk*

$$P_1 - Q_{i_2} = 2P_2$$

$$P_2 - Q_{i_3} = 2P_3$$

.

.

.

$$P_{m-1} - Q_{i_m} = 2P_m$$

Iterálva behelyettesítve az első egyeneltünkbe kapjuk, hogy

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + ... + 2^{m-1}Q_{i_m} + 2^m P_m.$$

Vegyünk egy pontot a $P, P_1, P_2, ..$ *sorozatból mondjuk* P_j*-t és hasonlítsuk össze* P_{j-1}*-gyel magasság szempontjából. Alkalmazzuk a (b)-t* $-Q_i$*-re, kapunk egy* κ_i *konstanst, amire*

$$h(P - Q_i) \leq 2h(P) + \kappa_i$$

minden $P \in \Gamma$.
Ezt csináljuk meg minden Q_i *reprezentánsra. Legyen* $\kappa^{'} = max_i\{\kappa_i\}$, *ekkor*

$$h(P - Q_i) \leq 2h(P) + \kappa^{'}$$

minden $P \in \Gamma$ *és minden* $1 \leq i \leq n$. *Legyen* κ *(c)-beli konstans, ekkor*

$$4h(P_j) \leq h(2P_j) + \kappa = h(P_{j-1} - Q_{i_j}) + \kappa$$

$$\leq 2h(P_{j-1}) + \kappa^{'} + \kappa$$

Írjuk át a következő alakra:

$$h(P_j) \leq \frac{1}{2}h(P_{j-1}) + \frac{\kappa + \kappa^{'}}{4}$$

$$= \frac{3}{4}h(P_{j-1}) - \frac{h(P_{j-1}) - (\kappa + \kappa^{'})}{4}$$

Ez alapján ha feltesszük, hogy $h(P_{j-1}) \geq \kappa + \kappa^{'}$ *akkor:*

$$h(P_j) \leq \frac{3}{4} h(P_{j-1})$$

Vagyis amíg a pontjaink magassága egy adott kolát fölött van akkor a sorozatunkban lévő pont magassága 3/4 lesz az előzőnek vagyis egy monoton csökkenő 0-ba tartó sorozatunk lesz, azaz találunk majd egy m indexet amitől kezdve már $h(P_m) \leq \kappa + \kappa^{'}$. *És ezzel már készen is vagyunk hiszen minden* $P \in \Gamma$ *felírható az alábbi formában:*

$$P = a_1 Q_1 + a_2 Q_2 + ... + a_n Q_n + 2^m R$$

ahol a_i *egészek valamint* $R \in \Gamma$ *amire igaz* $h(R) \leq \kappa + \kappa^{'}$. *Tehát a*

$$\{Q_1, Q_2, ..., Q_n\} \cup \{R \in \Gamma : (R) \leq \kappa + \kappa^{'}\}$$

halmaz generálja a Γ *csoportot, az (a) és (d) feltételek miatt tudjuk hogy ezekek végesek, azaz* Γ *egy végesen generált csoport lesz.*

□

3.2. Mordell Weil tétel

3.2.1. Tétel. *Legyen C egy nem-szinguláris harmadfokú görbe*

$$C : y^2 = x^3 + ax^2 + bx,$$

ahol a és b egészek. Ekkor a racionális pontok csoportja $C(Q)$ *végesen generált.*

Bizonyítás. *Az előző alfejezetben kimondtuk a magasság függvényre a lemmákat amik miatt a magasság függvény teljesítni az Leszállási Tétel feltételeit, azaz a* $C(Q)$ *csoport egy végesen generált csoport lesz.* □

Irodalomjegyzék

[1] Joseph H. Silverman, Jhon T. Tate, Rational Points on Elliptic Curves*, Springer, 2015*

[2] Joseph H. Silverman, The Arithmetic of Elliptic Curves*, Springer, 1985*