# Elliptikus görbék aritmetikája

Mogyorosi Bálint

Konzulens: dr.Zábrádi Gergely

# Alapok

## Definíció

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

A fenti egyenlet által leírt görbéket nevezzük elliptikus görbéknek, és azon $(x, y)$ párokat amik megoldások és $x, y \in \mathbb{Q}$ a görbe racionális pontjainak hívjuk.

## Definíció

Bézout-tételének köszönhetően tudjuk, az elliptikus görbéknek és egy egyenesnek 3 metszéspontja lesz (algebrailag zárt testfelett, multiplicitással számolva). Így ha veszünk két racionális potot a görbénken amiket összekötünk egy egyenessel kapunk egy harmadik racionális pontot a görbénken. Jelölés a műveletre $*$.

# Alapok

## Definíció

Az előbb definiált $*$ művelet nem lesz még csoport művelet. De ha lefixálunk egy $\mathfrak{O}$ racionális pontot és a racionális pontok összeadását a következő képpen definiáljuk $P_1 + P_2 = (P_1 * P_2) * \mathfrak{O}$. Akkor a racionális pontok halmazán egy Abel csoportműveletet definiálunk.

## Állítás

A fenti összeadás valóban Abel-csoport művelet:
$P_1$ és $P_2$ sorrendjétől nem függ, hogy hol fogja metszeni a görbét, így felcserélhetőek, vagyis kommutatív.
Az egységelemünk az $\mathfrak{O}$ pont lesz. Ezt könnyen láthatjuk a definícióból.
Egy elem inverzét úgy kapjuk meg, hogy:
$S := \mathfrak{O} * \mathfrak{O}$ ekkor $-Q := Q * S$.

# Alapok

## Explicit képlet csoportműveletre

$P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ és $P_1 * P_2 = (x_3, y_3)$ valamint, ha ügyesen választjuk meg a koordinátarendszert akkor $P_1 + P_2 = (x_3, -y_3)$.
$\lambda := \frac{y_2 - y_1}{x_2 - x_1}$ és $\nu := y_1 - \lambda x_1 = y_2 - \lambda x_2$
Ekkor, ha felírjuk az egyenes egyenletét és rendezzük, kapjuk:

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

Ezzel a $P_1 + P_2$ koordinátái:

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

## Definíció

A görbénkhez rendelt diszkriminánst az alábbi képlettel definiáljuk:

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

## 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 $\mathbb{Z}$ egészre zárt, így $\lambda$ is muszáj egész legyen. Mivel $2y$ és $f^{'}(x)$ egészek, így $2y|f^{'}(x)$, speciálisan $y|f^{'}(x)$. Valamint $y|f(x)$. A diszkrimináns 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 $y|D$. $\square$

## Definíció

$C(p^\nu)$ azon racionális $(x, y)$ pontok halmaza a görbénkről ahol $x$ nevezője osztható $p^{2\nu}$-vel.

## Lemma

(a) Minden $p$ prímre, az egyetlen véges rendű pont a $C(p)$-ben az egység elem lesz, azaz $\mathfrak{O}$.

(b) Legyen $P = (x, y) \in C(\mathbb{Q})$ egy racionális pont véges renddel, ekkor $x$ és $y$ is egészek.

## Nagell-Lutz tétel

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

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 dián a diszkriminánsra kimondott lemmát kapjuk, hogy $y$ osztja $D$-t. □

## Definíció

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

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

## Megjegyzés

Azon racionális pontok halmaza melyek kisebbek egy fix magasságnál egy véges halmaz.

## Megjegyzés

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

# Lemmák

## Lemma1

Minden valós $M$-re, a

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

véges.

## Lemma2

Legyen $P_0$ egy rögzített racionális pont $C$-n. Ekkor létezik egy $\kappa_0$ konstans ami csak $P_0, a, b, c$-től függ, amire:

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

minden $P \in C(\mathbb{Q})$.

## Lemma3

Létezik egy konstans $\kappa$, ami csak $a, b, c$-től függ, amire:

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

minden $P \in C(\mathbb{Q})$.

## Lemma4

Az index $(C(\mathbb{Q}) : 2C(\mathbb{Q}))$ véges. Ahol a $2C(\mathbb{Q})$ részcsoport a $C(\mathbb{Q})$ képe a kettővel való szorzás homomorfizmusnál.

# Leszállási Tétel

Legyen $\Gamma$ egy kommutatív csoport, és tegyük fel, hogy létezik egy függvény

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

a következő tulajdonságokkal:

(a) Minden valós $M$-re, a $\{P \in \Gamma : h(P) \leq M\}$ halmaz véges.

(b) Minden $P_0 \in \Gamma$-ra létezik egy $\kappa_0$ konstans, amire

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

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

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

Valamint

(d) A $2\Gamma$ részcsoport indexe véges $\Gamma$-ban.

Ekkor $\Gamma$ egy végesen generált csoport lesz.

## Bizonyítás

Első lépésben válasszunk minden $2\Gamma$ mellékosztálynak egy $\Gamma$-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 $P_1 \in \Gamma$.

## Bizonyítás

Ezt ezután elvégezzük a $P_1$-re is. Folytatva ezt a folyamatot kapjuk:

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

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

$$\vdots$$

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

## Bizonyítás

Iterálva behelyettesítve az első egyenletünkbe 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 $\kappa_i$ 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 $1 \leq i \leq n$.

## Bizonyítás

Legyen $\kappa$ (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:

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

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

## Bizonyítás

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 korlát 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 $h(R) \leq \kappa + \kappa'$.

## Bizonyítás

Tehát a

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

halmaz generálja a $\Gamma$ csoportot, az (a) és (d) feltételek miatt tudjuk, hogy ezek végesek, azaz $\Gamma$ egy végesen generált csoport lesz.

## Mordell-Weil tétel

Legyen C egy nem-szinguláris harmadfokú görbe

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

ahol $a$ és $a$ egészek. Ekkor a racionális pontok csoportja $C(\mathbb{Q})$ végesen generált.

**Bizonyítás.** Az előző alfejezetben kimondtuk a magasság függvényre a lemmákat amik miatt a magasság függvény teljesíteni az Leszállási Tétel feltételeit, azaz a $C(\mathbb{Q})$ csoport egy végesen generált csoport lesz. $\square$

Köszönöm a figyelmet!