SZEGEDI TUDOMÁNYEGYETEM

Természettudományi Kar Bolyai Intézet

Geometria Tanszék

Matematika BSc

SZAKDOLGOZAT

# Véges testek feletti elliptikus görbék

Vörös Anett

Témavezető: Dr. Nagy Gábor Péter

2011.

# Előszó

Jelen dolgozatom a Matematika alapszakon készült, Szegeden. Ezúton is köszönetemet szeretném kifejezni Dr. Nagy Gábor Péter tanár úrnak hasznos tanácsaiért, türelméért és segítőkészségéért. Hálás vagyok továbbá családomnak a sok támogatásért és bátorításért.

Szeged, 2011. 05. 13.

Vörös Anett

# Összefoglalás

Véges testek feletti elliptikus görbék bevezető vizsgálatát tűztem ki célul az algebrai geometria területén belül, természetesen a teljesség igénye nélkül. Mivel a BSc-s tanulmányaim zárásaként írtam ezt a szakdolgozatot, sok helyen az alapokfogalmaktól kezdtem az építkezést, viszont sokszor az ok-okozati kapcsolatok feltárása érdekében magasabb matematikai tételeket is belevettem.

A Bevezetésben tisztázok néhány - a dolgozat későbbi tételeinek megértése szempontjából fontos - algebrai definíciót, úgymint félcsoport, csoport, Abel-csoport, részhalmaz által generált részcsoport, ciklikus csoport, gyűrű, test, test karakterisztikája, test rendje, résztest, testbővítés, algebrailag zárt test, algebrai elem test felett, test algebrai lezártja, test prímteste.

A második részben a véges testekkel kapcsolatban ismertetek néhány fontos tételt: a véges testek rendjéről, multiplikatív csoportjáról.

Harmadikként az elliptikus görbék tulajdonságaira térek ki, tisztázva a görbe, az érintő, a sima és szinguláris görbepont fogalmát. Említem a technikailag fontos Bézout-tételt és az Algebra Alaptételét. Ezután rátérek a dolgozat fő témájára, az elliptikus görbékre. Levezetem az általános alakból a Weierstrass-egyenleteket a test karakterisztikájának függvényében, definiálom többek között azok diszkriminánsát. A görbe pontjainak halmazán értelmezem az összeadás műveletét, amivel együtt azok Abel-csoportot alkotnak. Definiálom az elliptikus görbe feletti endomorfizmust, annak fokát és az izogéniát. A Cauchy-Schwarz-egyenlőtlenség felhasználásával vázlatosan „bizonyítom” a Hasse-tételt, megfogalmazom a Weil-sejtést is.

Az utolsó fejezetben az elliptikus görbék kriptográfiában betöltött fontos szerepére világítok rá, ezen belül kitérek Lenstra prímfaktorizációjára, Pollard algoritmusára, Diffie és Hellman, ElGamal és Schoof algoritmusaira.

# Tartalomjegyzék

# 1. Bevezetés

**1.1. Definíció.** *Legyen* $\mathbf{G} \neq \emptyset$*, rajta* $\cdot$ *egy kétváltozós asszociatív művelet. Ekkor a* $(\mathbf{G}, \cdot)$ *algebrai struktúrát félcsoportnak nevezzük.*

**1.2. Definíció.** *Legyen* $\mathbf{G} \neq \emptyset$*, rajta* $\cdot$ *egy kétváltozós művelet, amely asszociatív, egységelemes, és minden elemnek van inverze* $\mathbf{G}$*-ben. Ekkor a* $(\mathbf{G}, \cdot)$ *algebrai struktúrát csoportnak nevezzük.*

**1.3. Definíció.** *Legyen* $(\mathbf{G}, \cdot)$ *csoport, és* $\cdot$ *kommutatív* $\mathbf{G}$*-n. Ekkor a* $(\mathbf{G}, \cdot)$ *struktúrát Abel-csoportnak nevezzük.*

**1.4. Definíció.** *Legyen* $\mathbf{G}$ *csoport,* $\mathbf{A} \subseteq \mathbf{G}$*. Ekkor a* $\cap\{\mathbf{H} \leq \mathbf{G} : \mathbf{A} \subseteq \mathbf{H}\}$ *részcsoportot az* $\mathbf{A}$ *részhalmaz által generált részcsoport* $\mathbf{G}$*-ben (*$\mathbf{A}$ *generátuma* $\mathbf{G}$*-ben). Jele:* $[\mathbf{A}]$*. Ha* $\mathbf{A}$*-ra teljesül, hogy* $[\mathbf{A}] = \mathbf{G}$*, akkor az* $\mathbf{A}$ *halmaz a* $\mathbf{G}$ *generátorrendszere (*$\mathbf{A}$ *generálja* $\mathbf{G}$*-t).*

**1.5. Definíció.** *Legyen* $\mathbf{G}$ *csoport. Azt mondjuk, hogy* $\mathbf{G}$ *ciklikus, ha van olyan eleme a csoportnak, amely generálja a* $\mathbf{G}$*-t:*

$$\exists g \in \mathbf{G} : \quad [g] = \mathbf{G}$$

**1.6. Definíció.** *Legyen* $\mathbf{R}$ *nemüres halmaz,* $\mathbf{R} = \{a, b, ...\}$*. Ekkor gyűrűnek nevezzük az* $\{\mathbf{R}, +, \cdot\}$ *struktúrát, ha* $\mathbf{R}$ *az* $+$*-ra nézve Abel-csoportot, a* $\cdot$*-ra nézve félcsoportot alkot, és* $\cdot$ *disztributív az* $+$*-ra nézve, vagyis*

$$\forall a, b, c \in \mathbf{R} : \qquad a(b + c) = ab + ac \text{ és}$$
$$(b + c)a = ba + ca.$$

Ez részletesen azt jelenti, hogy egy $\mathbf{R}$ halmazt gyűrűnek nevezünk, ha definiálva van benne két asszociatív művelet, az $a + b$ összeadás és az $ab$ szorzás, az összeadás kommutatív és invetálható, továbbá teljesül a disztributivitás.

**1.7. Definíció.** *Az* $\{\mathbf{R}, +, \cdot\}$ *gyűrűt kommutatívnak nevezzük, ha* $\cdot$ *kommutatív. Az* $\{\mathbf{R}, +, \cdot\}$ *gyűrűt egységelemesnek nevezzük, ha a* $\cdot$*-ra nézve létezik az* $1 \in \mathbf{R}$ *egységelem.*

**1.8. Definíció.** *Egy* $\{\mathbf{R}, +, \cdot\}$ *gyűrűt testnek nevezünk, ha egységelemes, kommutatív, és* $\mathbf{R}\backslash\{0\}$ *a szorzásra nézve csoportot alkot.*

**1.9. Definíció.** *Legyen* $\{\mathbf{K}, +, \cdot\}$ *test. Ekkor* $\mathbf{K}$ *karakterisztikája* $\operatorname{char}\mathbf{K} = 0$*, ha* $\forall a \neq 0, a \in \mathbf{K}$ *és* $\varnothing(a) = 0$*. Ha* $\exists n \in \mathbb{N}$ *úgy, hogy* $\forall a \in \mathbf{K}$ *esetén* $na = 0$*, akkor a legkisebb ilyen* $n$ *számot nevezzük* $\mathbf{K}$ *karakterisztikájának. Minden más esetben* $\operatorname{char}\mathbf{K} = \infty$*.*

$\mathbb{Q}$, $\mathbb{R}$ és $\mathbb{C}$ mind 0 karakterisztikájú testek.

**1.10. Definíció.** *Test rendjén a test elemszámát értjük:* $|\mathbf{K}|$.

**1.11. Definíció.** *Legyen* $\mathbf{K}$, $\mathbf{L}$ *test. Azt mondjuk, hogy* $\mathbf{K}$ *az* $\mathbf{L}$ *részteste, ha* $\mathbf{K} \subseteq \mathbf{L}$ *és a* $\mathbf{K}$*-beli műveletek az* $\mathbf{L}$*-beli műveletek* $\mathbf{K}$*-ra vonatkozó megszorításai. Ekkor azt is mondjuk, hogy* $\mathbf{L}$ *a* $\mathbf{K}$ *bővítése. Jelölés:* $\mathbf{L}|\mathbf{K}$.

**1.12. Definíció.** *Legyen* $\mathbf{K}$ *test.* $\mathbf{K}$*-et algebrailag zártnak nevezzük, ha minden* $f \in \mathbf{K}[x], f \neq 0$ *polinom előáll* $\mathbf{K}$ *felett elsőfokú polinomok szorzataként.*

**1.13. Definíció.** *Legyenek* $\mathbf{L}$, $\mathbf{K}$ *testek,* $\mathbf{L}|\mathbf{K}, a \in \mathbf{L}$. *Ekkor azt mondjuk, hogy a algebrai elem* $\mathbf{K}$ *fölött, ha*

$$\exists f \in \mathbf{K}[x]: \quad f \neq 0 \text{ és } f(a) = 0,$$

*különben a transzcendens elem* $\mathbf{K}$ *fölött.*

**1.1. Tétel.** *Minden testhez létezik olyan nála bővebb algebrailag zárt test, amelynek minden eleme algebrai az eredeti test felett, továbbá az ilyen test izomorfiától eltekintve egyértelműen meghatározott.*

**1.14. Definíció.** *Ezt a testet az eredeti test algebrai lezártjának nevezzük.*

**1.2. Tétel.** *Legyenek* $\mathbf{L}, \mathbf{K}$ *testek,* $\mathbf{L}|\mathbf{K}$ *testbővítés,* $a \in \mathbf{L}$. *Tegyük fel, hogy a algebrai elem* $\mathbf{K}$ *felett, azaz* $f \neq 0, f \in \mathbf{K}[x] : f(a) = 0$. *Ekkor létezik egyetlen olyan* $m \in \mathbf{K}[x]$ *főpolinom, amelyre*

$$m(a) = 0$$

*és*

$$\forall g \in \mathbf{K}[x]$$

*esetén ha* $g(a) = 0$, *akkor* $m|g$. *Ekkor* $m$*-et az a elem minimálpolinomjának nevezzük.*

Adott $\mathbf{L}$, $\mathbf{A} \subseteq \mathbf{L}$ esetén $\cap\{\mathbf{K} : \mathbf{L}|\mathbf{K}, \mathbf{A} \subseteq \mathbf{K}\}$ a legszűkebb, $\mathbf{A}$-t tartalmazó résztest $\mathbf{L}$-ben. Ez a test az $\mathbf{A}$ halmaz által generált résztest $\mathbf{L}$-ben. Minden esetben létezik legszűkebb résztest egy testen belül, mégpedig a $\emptyset$ által generált résztest.

**1.15. Definíció.** *Ezt a generált résztestet nevezzük a test prímtestének.*

# 2. Véges testek

**2.1. Definíció.** *Egy testet végesnek nevezünk, ha véges számú elemet tartalmaz.*

**2.2. Definíció.** *Legyen $p$ prím, $\mathbf{F}_p := \{0, 1, \ldots, p-1\}$ és legyen $\phi : \mathbb{Z}/(p) \to \mathbf{F}_p$ leképezés, melyre $\phi([a]) = 0$ minden $a = 0, 1, \ldots, p-1$ esetén. Ekkor $\mathbf{F}_p$ a $\phi$ által indukált teststruktúrával véges testet alkot, egészen pontosan a $p$ rendű Galois testet.*

**2.1. Lemma.** *Ha egy test karakterisztikája $p$ prím, akkor prímteste $\cong \mathbb{Z}_p$. Ha egy test karakterisztikája $0$, akkor prímteste $\cong \mathbb{Q}$.*

**2.1. Tétel.** *Minden véges test prímhatvány rendű.*

**Bizonyítás.** Legyen $\mathbf{K}$ véges test. Ekkor a lemma szerint $\mathbf{K}$ prímteste $\mathbb{Z}_p$. Ekkor $\mathbf{K}|\mathbb{Z}_p$ véges fokú testbővítés. Ha $[\mathbf{K} : \mathbb{Z}_p] = n$, akkor $\mathbf{K}$ mint $\mathbb{Z}_p$ fölötti vektortér izomorf a $\mathbb{Z}_p$ vektrotérrel. Ezért elemszámuk megegyezik: $|\mathbf{K}| = |\mathbb{Z}_p| = p^n$.

**2.2. Tétel.** *Legyen $\mathbf{L}$ véges test, $\mathbf{K}$ résztest $\mathbf{L}$-ben, $|\mathbf{L}| = p^l$, $|\mathbf{K}| = p^k$. Ekkor $k$ osztója $l$-nek, azaz $k|l$.*

**Bizonyítás.** $\mathbf{L}|\mathbf{K}$ testbővítés, foka: $[\mathbf{L} : \mathbf{K}] = d$. Ekkor $\mathbf{L}$ $\mathbf{K}$ feletti vektortér, így izomorf $\mathbf{K}^d$ vektortérrel, ezáltal rendjük megegyezik:

$$p^l = |\mathbf{L}| = |\mathbf{K}^d| = |\mathbf{K}|^d = p^{k^d} = p^{kd} \Rightarrow l = kd \Rightarrow k|l.$$

**2.3. Tétel.** *Véges test multiplikatív csoportja ciklikus.*

**Bizonyítás.** Legyen $\mathbf{K}$ véges test, $|\mathbf{K}| = p^n$. Legyen $\mathbf{K}^* = (\mathbf{K}\backslash 0, \cdot)$ véges Abel-csoport, $|\mathbf{K}^*| = p^n - 1$. Legyen $s$ a legkisebb olyan kitevő, amelyre $a^s = 1$ az összes $a \in \mathbf{K}^*$-ra. Ekkor minden $a \in \mathbf{K}^*$ esetén teljesül, hogy o(a)$|s$. Ekkor

$$\begin{aligned} & \mathrm{lkkt}(o(a) : a \in \mathbf{K}^*)|s \\ \Longrightarrow \quad & a^{\mathrm{lkkt}(o(a):a\in\mathbf{K}^*)} = 1 \text{ az összes } a \in \mathbf{K}^*\text{-ra} \\ \Longrightarrow \quad & s = \mathrm{lkkt}(o(a) : a \in \mathbf{K}^*) \end{aligned}$$

Ekkor

$$\begin{aligned} & \forall a \in \mathbf{K}^* : a^s - 1 = 0 \\ \Longrightarrow \quad & \mathbb{Z}_\mathrm{l}[x] \ni (x^s - 1)\text{-nek } \forall a \in \mathbf{K}^* \text{ gyöke} \\ \Longrightarrow \quad & \mathbb{Z}_\mathrm{l}[x] \ni (x^{s+1} - x)\text{-nek } \forall a \in \mathbf{K} \text{ gyöke} \end{aligned}$$

Tudjuk, hogy test feletti polinomnak legfeljebb annyi páronként különböző gyöke van, mint a fokszám: $p^n \leq s + 1$, ami átrendezve $s \geq p^n - 1$.

A Lagrange-tétel szerint viszont $\forall a \in \mathbf{K}^*$-ra ha $a^{p^n-1} = 1$, akkor $o(a)|p^n - 1$, amiből az következik, hogy $s|p^n - 1$, tehát $s \leq p^n - 1$. Előbbi eredményünkkel ezt egyeztetve kapjuk, hogy $s = \mathrm{lkkt}(o(a) : a \in \mathbf{K}^*) = p^n - 1$.

Most meg fogjuk mutatni, hogy $\mathbf{K}^*$-ban van olyan elem, amelynek a rendje lkkt$(o(a) : a \in \mathbf{K}^*)$. Írjuk fel most $s$-t a következő prímhatványszorzat alakban: $s = q_1^{j_1} \dots q_r^{j_r}$. Ekkor minden $i$, $i = 1, \dots, r$ esetén létezik olyan $a_i$ $\mathbf{K}^*$-beli elem, hogy $q_i^{j_i} | o(a_i)$, amiből $o(a_i) = u_i q_i^{j_i}$, vagyis $o(a_i^{u_i}) = q_i^{j_i}$, amelyben jelöljük $a_i^{u_i}$-t $b_i$-vel. Definiáljuk $b = b_1 \dots b_r$-et, amelynek rendje így $o(b) = o(b_1) \dots o(b_r) = q_1^{j_1} \cdot \dots \cdot q_r^{j_r} = s = p^n - 1$. Tehát $[b] = \mathbf{K}^*$.

**2.4. Tétel.** *Minden prímhatványhoz létezik – izomorfiától eltekintve – egyetlen ilyen rendű test, mégpedig a $p^n$ rendű test. Ez a test a $x^{p^n} - x \in \mathbb{Z}_{p[x]}$ polinom felbontási teste. Ekkor $\mathbf{K}$ $n$-edfokú algebrai test.*

**Megjegyzés.** A fenti $p^n$ elemű test jelölése: $\mathbf{GF}(p^n)$ (Galois field).

**2.1. Következmény.** *Minden véges test egyszerű algebrai bővítése a saját prímtestének, és izomorf egy $\mathbb{Z}_p[x]/<f>$ által generált faktortesttel, ahol $f \in \mathbb{Z}_p[x]$ irreducibilis. Továbbá minden $p$ prímre és minden $n \in \mathbb{N}$-re létezik $\mathbb{Z}_p$ feletti $n$-edfokú irreducibilis főpolinom.*

**Bizonyítás.** Legyen adott $p$ prím és $n \in \mathbb{N}$, továbbá legyen $\mathbf{K} = \mathbf{GF}(p^n)$. Tudjuk, hogy ekkor $\mathbf{K}^*$ ciklikus, tegyük fel, hogy $a$ generálja: $\mathbf{K}^* = [a]$, $\mathbb{Z}_p(a) = \mathbf{K}$. Ekkor a $\mathbf{K}|\mathbb{Z}_p$ testbővítés foka $[\mathbf{K} : \mathbb{Z}_p] = n$ megegyezik $a$ minimálpolinomjának fokszámával, tehát $a$ minimálpolinomja $\mathbb{Z}_p$ feletti n-edfokú irreducibilis polinom.
**Példa.** Legyen $f \in \mathbb{Z}_p[x]$ irreducibilis $n$-edfokú polinom. A $\mathbb{Z}_p[x]/<f>$ véges test elemszáma $p^n$, mivel $\mathbb{Z}_p[x]/<f>$ elemei az alábbi alakban írhatók fel:

$$\overline{r} = a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$$

, ahol $a_0, \dots, a_{n-1} \in \mathbb{Z}_p$.

Négy elemű testre példa a $\mathbb{Z}_2[x]/ < x^2 + x + 1 >$. Nyilvánvalóan $x^2 + x + 1$ irreducibilis, mert másodfokú, és 0 és 1 nem gyökei. A faktortest elemei tehát $\overline{0}$, $\overline{1}$, $\overline{x}$, $\overline{x+1}$. A rajtuk végzett műveletekhez tartozó táblázatok:

| $+$ | $\overline{0}$ | $\overline{1}$ | $\overline{x}$ | $\overline{x+1}$ |
|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{1}$ | $\overline{x}$ | $\overline{x+1}$ |
| $\overline{1}$ | $\overline{1}$ | $\overline{0}$ | $\overline{x+1}$ | $\overline{x}$ |
| $\overline{x}$ | $\overline{x}$ | $\overline{x+1}$ | $\overline{0}$ | $\overline{1}$ |
| $\overline{x+1}$ | $\overline{x+1}$ | $\overline{x}$ | $\overline{1}$ | $\overline{0}$ |

| $\cdot$ | $\overline{0}$ | $\overline{1}$ | $\overline{x}$ | $\overline{x+1}$ |
|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ |
| $\overline{1}$ | $\overline{0}$ | $\overline{1}$ | $\overline{x}$ | $\overline{x+1}$ |
| $\overline{x}$ | $\overline{0}$ | $\overline{x}$ | $\overline{x+1}$ | $\overline{1}$ |
| $\overline{x+1}$ | $\overline{0}$ | $\overline{x+1}$ | $\overline{1}$ | $\overline{x}$ |

# 3. Elliptikus görbék

**3.1. Definíció.** *Egy* $\Gamma = \{(x,y) \in \mathbb{R}^2 \,|\, f(x,y) = 0\} \subseteq \mathbb{R}^2$ *injektív leképezést görbének nevezünk.*

**3.2. Definíció.** *Az érintő a szelő határhelyzete.*

**3.1. Tétel.** *Legyen* $P(a,b)$ *a* $\Gamma = \{(x,y) \in \mathbb{R}^2 \,|\, f(x,y) = 0\}$ *görbe pontja. A* $P$*-beli érintő egyenlete:* $\frac{\mathrm{d}f}{\mathrm{d}x}(a,b)(x-a) + \frac{\mathrm{d}f}{\mathrm{d}y}(a,b)(y-b) = 0$

**3.3. Definíció.** *A* $\Gamma : f(x,y) = 0$ *görbe* $P(a,b)$ *pontját sima vagy egyszeres görbepontnak nevezzük, ha valamelyik parciális deriváltja nem* $0$ $(a,b)$*-ben. Ellenkező esetben szinguláris pontról beszélünk.*

**3.1. Állítás.** *A* $\Gamma : f(x,y) = 0$ *görbének akkor és csak akkor van érintője a* $P(a,b)$ *pontban, ha* $P$ *egyszeres pont, azaz* $\left(\frac{\mathrm{d}f}{\mathrm{d}x}(a,b), \frac{\mathrm{d}f}{\mathrm{d}y}(a,b)\right) \neq (0,0)$

**3.2. Állítás.** *Az általános másodfokú görbének nincs szinguláris pontja, ha az egyensúlyi helyzeteiből képzett mátrix determinánsa nem* $0$*.*

Legyen adott $\Gamma : (x,y) = 0$, ahol

$$f(x,y) = a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + \ldots + a_{mn}x^m y^n = \sum_{i,j=0}^{m,n} a_{ij}x^i y^j$$

a két változós polinom általános alakja. Továbbá paraméteresen adott egy egyenes, tehát a valós számok halmaza bijektíven van leképezve egy egyenesre:

$$r(t) = (u_1 + tv_1, u_2 + tv_2) = (u_1, u_2) + t(v_1, v_2),$$

ahol $(u_1, u_2)$ az $e$ egyenes egy pontja, $(v_1, v_2)$ pedig az irányvektora. Behelyettesítve kapjuk, hogy

$$g(t) = f(u_1 + tv_1, u_2 + tv_2) \in R[t].$$

Ekkor a görbe és az egyenes metszéspontjait megkaphatjuk így: $g(t) = 0, g$ gyökei $t_1, \ldots, t_k$, ebből $e \cap \Gamma = \{P_1 = r(t_1), \ldots, P_k = r(t_k)\}$.

Adott $\mathbf{D}$ integritástartomány és $f(x) \in d[x]$ esetén $f$ $\mathbf{D}$-beli gyökeinek keresése ekvivalens $f$ $\mathbf{D}$ feletti szorzattá alakításával.

**3.2. Tétel (Bézout).** $f(a) = 0 \Leftrightarrow x - a | f \Leftrightarrow f(x) = (x-a)h(x) \Rightarrow deg(h) = deg(f) - 1$.

**3.3. Tétel (Algebra alaptétele).** *A komplex számok teste algebrailag zárt, azaz minden legalább elsőfokú* $\mathbb{C}$ *feletti polinomnak van gyöke* $\mathbb{C}$*-ben.*

Eszerint ha $f(x)$ $\mathbb{C}$ feletti polinom, $deg(f) = n$, akkor $f(x) = (x - a_1)h_1(x) = (x-a_1)(x-a_2)h_2(x) = \ldots = (x-a_1)\cdot\ldots\cdot(x-a_n)h_n(x)$, ahol $h_n(x) = c \neq 0$ nulladfokú polinom. Így $f(x) = c\prod_{i=1}^{k}(x - a_i)^{m_i}$, ahol $a_1, \ldots, a_k$ páronként különböző gyökök és $m_i$ az $a_i$ gyök multiplicitása.

**3.3. Állítás.** *Egy $a \in \mathbb{C}$ az $f(x)$ polinomnak legalább kétszeres gyöke akkor, és csak akkor, ha $f(a) = 0$ és $f'(a) = 0$.*

Legyen $\Gamma:\ f(x, y) = 0$ görbe, irányvektora $(v_1, v_2)$, $g(t) = f(u_1 + tv_1, u_2 + tv_2)$.

**3.4. Tétel.** *Ha $e$ érinti $P$-ben $\Gamma$-t, akkor a $\tau$ többszörös gyöke $g(t)$-nek.*

**Megjegyzés.** $\tau$ többszörös gyöke $g(t)$-nek $\Leftrightarrow g(\tau) = g'(\tau) = 0$.
**Bizonyítás.** A $g(t)$ deriváltja $g'(t) = \frac{\mathrm{d}f}{\mathrm{d}x}(u_1+tv_1, u_2+tv_2)u_1+\frac{\mathrm{d}f}{\mathrm{d}y}(u_1+tv_1, u_2+tv_2)u_2$. Ha $\tau = 0$, akkor $u_1 + tv_1, u_2 + tv_2$ megegyezik $(a, b)$-vel, így $P(a, b)$ a $\tau$-hoz tartozó egyenespont, $a = u_1 + tv_1, b = u_2 + tv_2$.

$$0 = g'(\tau) = \frac{\mathrm{d}f}{\mathrm{d}x}(a, b)v_1 + \frac{\mathrm{d}f}{\mathrm{d}y}(a, b)v_2$$

amiből

$$\left(\frac{\mathrm{d}f}{\mathrm{d}x}(a, b), \frac{\mathrm{d}f}{\mathrm{d}y}(a, b)\right) \perp (v_1, v_2)$$

**3.5. Tétel.** *Legyen $P(a, b)$ a $\Gamma:\ f(x, y) = 0$ görbe pontja, és legyen $(u_1t + v_1, u_2t + v_2)$ az $e$ egyenes egy paraméterezése. Legyen $g(t) = f(u_1t+v_1, u_2t+v_2)$ és tegyük fel, hogy $g(t) = (a, b)$, azaz $P$ a $\tau$ ponthoz tartozó egyenespont. Ekkor $\tau$ a $g$ többszörös gyöke $\Leftrightarrow$ $e$ érinti $\Gamma$-t $P$-ben vagy $P$ szinguláris pontja $\Gamma$-nak.*

Elliptikus görbe fogalmán egy **F** test felett értelmezett nemszinguláris kétváltozós kubikus (harmadfokú) görbét értünk: $f(X, Y) = 0$. Az **F** test szokásosan lehet $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Q}$ algebrai bővítései vagy egy véges test. Vegyünk hozzá a görbéhez egy végtelen távoli pontot, jelöljük ezt $O$-val. A kúpszeletekkel ellentétben az elliptikus görbék nem írhatók fel racionális függvényekkel, helyette elliptikus függvényeket használunk.

Andrew Wiles a Nagy Fermat-tételt elliptikus görbék segítségével bizonyította be 1995-ben.

Az elliptikus görbék a következő alakban írhatók fel homogén koordinátázásban:

$$E:\quad Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Mindazonáltal a jelölés könnyítése céljából a Weierstrass-egyenletet nem homogén koordinátákkal szokás felírni: $x = X/Z$ és $y = Y/Z$ esetén

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

ahol $a_1, \ldots, a_6 \in \mathbf{F}$. Ekkor azt mondjuk, hogy $E$ $\mathbf{F}$ felett értelmezett. Figyelnünk kell azonban arra, hogy a görbéhez az $O = [0, 1, 0]$ pont is hozzátartozik a végtelenben.

Legyenek adottak $f, g : \mathbf{F} \to \mathbf{F}$, $\mathbf{F}$ test, $f(y) = g(x), f^* = 2, g^* = 3$, úgy, hogy egyiknek sincs többszörös gyöke.

Legyen $\operatorname{char} \mathbf{F} = 2$. Ekkor a görbe az

$$y^2 + ay = x^3 + bx^2 + cxy + dx + e$$

alakban adható meg, ahol $a, b, c, d, e \in \mathbf{F}$.

Tegyük fel, hogy $\mathbf{F}$ karakterisztikája $\operatorname{char} \mathbf{F} \neq 2$, ekkor

$$y \mapsto \frac{1}{2}(y - a_1 x - a_3)$$

teljes négyzetté alakítással adódik, hogy

$$E: \quad y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6,$$

ahol

$$b_2 = a_1^2 + 4a_4, \quad b_4 = 2a_4 + a_1 a_3, \quad b_6 = a_3^2 + 4a_6.$$

Továbbá definiáljuk a következő mennyiségeket:

$$b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2,$$

$$c_4 = b_2^2 - 24b_4,$$

$$c_6 = -b_2^3 + 36 b_2 b_4 - 216 b_6,$$

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6,$$

$$j = c_4^3/\Delta,$$

$$\omega = \frac{dx}{2y + a_1 x + a_3} = \frac{dy}{3x^2 + 2a_2 x + a_4 - a_1 y}.$$

Ebből könnyen látszik, hogy igazak a

$$4b_8 = b_2 b_6 - b_4^2 \text{ és } 1728\Delta = c_4^3 - c_6^2$$

relációk. Legyen most $\operatorname{char} \mathbf{F} = 3$. Ekkor a függvényegyenlet a fentiek alapján a következő alakban írható fel:

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

ahol $a, b, c \in \mathbf{F}$.

Továbbá, ha $\operatorname{char} \mathbf{F} \neq 2, 3$, akkor behelyettesítve, hogy

$$(x, y) \mapsto \left( \frac{x - 3b_2}{36}, \frac{y}{108} \right),$$

eltűnik $x^2$, és az

$$E: \quad y^2 = x^3 - 27c_4x - 54c_6$$

egyszerűsített egyenletet kapjuk, amit az

$$E: \quad y^2 = x^3 - Ax - B$$

alakban is szokás írni. Utóbbi használata esetén $\Delta$ és $j$ a következőképp változik:

$$\Delta = -16(4A^3 + 27B^2) \quad \text{és} \quad j = -1728\frac{(4A)^3}{\Delta}.$$

Ebben az esetben a görbe Legendre normál alakban is írható: $y^2 = x(x-1)(x-\lambda)$.

**3.4. Definíció.** *A fenti $\Delta$ mennyiséget a Weierstrass-egyenlet diszkriminánsának, $j$-t az elliptikus görbe $j$-invariánsának, $\omega$-t pedig a Weierstrass-egyenlethez tartozó invariáns differenciálnak nevezzük.*

Figyeljük meg, hogy a görbe szimmetrikus lesz az Descartes-féle koordinátarendszer $x$ tengelyére.

Vegyük a görbe egy szelőjét (esetleg érintőjét). Jelöljük $A$, $B$, $C$-vel a görbével vett metszéspontjait. A szelőt úgy válasszuk meg, hogy legalább egy metszéspont legyen. Mivel a végtelen távoli pontot is értelmezzük, így legalább két metszéspontot kapunk.

Legyenek $A, B \in E$ a görbe pontjai, legyen az általuk meghatározott egyenes. Ha $A = B$, akkor legyen $L$ a $A$-ból E-hez húzott érintő. Legyen továbbá a harmadik pont $C$, ahol L és E metszik egymást. Legyen $L'$ a $C$-n és $O$-n átmenő egyenes (párhuzamos az y tengellyel), ekkor a harmadik pontot, ahol $L$ metszi $E$-t, definiáljuk $A$ és $B$ összegeként: $A+B$. A görbén való összeadást a következő módon értelmeztük: $A + B + C = O$ (amennyiben egy egyenesen vannak). Definiáljuk az additív inverz fogalmát: $-O = O$, $O = X + (-X)$, ahol $-X$ $X$ ellentettje.

**3.6. Tétel.** *A fenti összeadással a görbe pontjainak halmaza Abel-csoportot alkot.*

**Megjegyzés.** A kommutativitás triviális, ellenben az asszociativitás bizonyítása nehéz.

**3.7. Tétel (Struktúratétel).** *Legyen $\mathbb{Q}$ az alaptest, azaz adott $A$ pont esetén $A$ mindkét koordinátája racionális. Ekkor $\mathbb{Q}$ felett ez egy végesen generált Abel-csoport, vagyis a csoport ciklikus csoportok véges szorzatával izomorf.*

Legyen az alaptest $\mathbf{GF}(q)$ ($q$ rendű véges test, ahol $q$ "elég nagy": $q \approx 2^{300}$). Ekkor az Abel-csoport ciklikus, vagy kettő ciklikus csoport direkt szorzata. Van nagy elemszámú ciklikus részcsoport, azaz létezik $g$ úgy, hogy $o(g)$ nagy.

Ha az elliptikus görbe alapteste algebrailag zárt, akkor az egyenes három pontban metszi az elliptikus görbét (beleszámítva a többszörös gyököket is).

Tekintsük a $\mathbf{GF}(q)$ véges testet, $q = p^n$.

**3.5. Definíció.** *Legyen* $\mathbf{F}$ *alaptest,* $\operatorname{char}\mathbf{F} \neq 2, 3$. *Legyen*

$$E: \quad Y^2 = X^3 + AX + B$$

*elliptikus görbe az* $\mathbf{F}$ *test felett. A* $\Gamma$ *görbe endomorfizmusa* $\mathbf{F}$ *felett a következő racionális leképezés:*

$$\phi: \quad \Gamma \to \Gamma$$

$\mathbf{F}$ *test felett értelmezett, amelyre* $\phi(O) = O$. *Ha* $x$ $\Gamma$ *egy általános pontja, akkor* $\chi = \phi(x)$, *és* $\mathbf{F}(x)/\mathbf{F}(\chi)$ *egy algebrai testbővítés. Definiáljuk* $\phi$ *fokát:*

$$\deg(\phi) = [\mathbf{F}(x) : \mathbf{F}(\chi)].$$

*Megegyezés szerint a konstans endomorfizmus foka* 0.

**3.8. Tétel.** *Legyen* $E$ *elliptikus görbe* $\mathbf{GF}(q)$ *fölött. Ekkor létezik egy* $\mathbf{GF}(q)$ *felett definiált pontja.*

**Bizonyítás.** Legyen $\Gamma$ $E$ Jacobija és legyen $\mathbf{G}$ $\Gamma$ pontjainak halmaza $\overline{\mathbf{GF}(q)}$ felett. Elegendő megmutatni, hogy $H^1(\mathbf{C}, \mathbf{G})$ teljesül, ahol

$$\mathbf{C} = Gal(\overline{\mathbf{GF}(q)}/\mathbf{GF}(q))$$

. A $C$ csoportot a Frobenius automorfizmus generálja, $\gamma : a \to a^q$. Elegendő megmutatni, hogy

$$a_\gamma = \gamma b - b$$

valamely $b \in G$. Most

$$\gamma b - b = (\phi - 1)b,$$

ahol $\phi$ a "geometriai Frobenius", így $\phi - 1$ nemkonstans endomorfizmus. Bármely $c \in \mathbf{G}$ esetén megoldható a $(\phi - 1)b = c$ egyenlet $b$-re, mivel algebrailag zárt testről van szó. Általánosságban ez teljesül $c = a_\gamma$-ra. Kapjuk, hogy

$$a_\sigma = \sigma b - b, \sigma = \gamma, \gamma^2, \gamma^3, \ldots$$

Ezzel tételünket beláttuk.

**3.6. Definíció.** *Az izogénia egy leképezés két elliptikus görbe között:* $\Gamma \to E$ *amely az* $o_\Gamma$ *racionális pontot* $o_E$*-be viszi.*

**3.9. Tétel.** *Legyen*

$$\lambda : \Gamma_1 \to \Gamma_2$$

*elliptikus görbék közötti izogénia, mind* $\mathbf{GF}(q)$ *felett definiálva. Ekkor* $N_1 = N_2$*, ahol* $N_1, N_2$ *rendre* $\Gamma_1, \Gamma_2$ *pontjainak számai* $\mathbf{GF}(q)$ *felett.*

**Bizonyítás.** Legyen $\phi_j$ a Frobenius endomorfizmus $\Gamma_j$ felett. A fokszámok:

$$\deg(\phi_1 - 1) = \deg(\phi_2 - 1)$$

egyenlőek. Előbbi tétel bizonyításából ez csak $N_1 = N_2$ lehet.

**3.1. Lemma (Cauchy-Scwarz egyenlőtlenség).** *Legyen* $A$ *Abel-csoport, és legyen* $d : A \to Z$ *egy pozitív definit kvadratikus alak. Ekkor*

$$|d(\psi - \phi) - d(\phi) - d(\psi)| \leq 2\sqrt{d(\phi)d(\psi)} \forall \psi, \phi \in A.$$

**Bizonyítás.** Minden $\psi, \phi \in A$ esetén legyen

$$L(\psi, \phi) = d(\psi - \phi) - d(\phi) - d(\psi)$$

bilineáris alak a $d$ kvadratikus alakhoz. Mivel $D$ pozitív definit, így minden $m, n \in Z$ esetén

$$q \leq d(m\psi - n\phi) = m^2 d(\psi) + mnL(\psi, \phi) + n^2 d(\phi).$$

Speciálisan legyen $m = -L(\psi, \phi)$ és $n = 2d(\psi)$, ahonnan $0 \leq d(\psi)(4d(\psi)d(\phi) - L(\psi, \phi)^2)$. Ezzel igazoltuk a kívánt egyenlőtlenséget $\psi \neq 0$ esetre, mivel $\psi = 0$ fennállása esetén az triviális.

**3.2. Lemma.** *Legyenek* $E_1$ *és* $E_2$ *elliptikus görbék. Ekkor a fokszám leképezés*

$$\deg : \quad \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$$

*pozitív definit kvadratikus alak.*

**3.3. Lemma.** *Legyen* $E$ *egy elliptikus görbe* $\mathbf{F}_q$ *véges test felett,* $p$ *karakterisztikával, és legyen* $\phi$*:* $E \to E$ *a* $q$*-adik hatványú Frobenius-morfizmus. Ekkor az* $1 - \phi$ *leképezés szeparábilis.*

**3.4. Lemma.** *Legyen* $\phi : E \to E$ *egy nemnulla szeparábilis izogénia. Ekkor*

$$\#\ker\phi = \deg\phi.$$

**3.10. Tétel (Hasse).** *Legyen $E(\mathbf{F}_q)$ egy elliptikus görbe az $\mathbf{F}_q$ véges test felett, ahol $q$ prímhatvány. Ekkor*

$$|\#E(\mathbf{F}_q) - q - 1| \leq 2\sqrt{q}.$$

**Bizonyítás.** Válasszunk $\mathbf{F}_q$-beli együtthatókkal Weierstrass-egyenletet $E$-re, és legyen

$$\phi: \quad E \to E, (x, y) \mapsto (x^q, y^q),$$

a $q$-adik Frobenius morfizmus. Mivel a $G_{\overline{\mathbf{F}}_q/\mathbf{F}_q}$ Galois-csoportot $\overline{\mathbf{F}}_q$-n a $q$-adik leképezés állítja elő, ezért $E(\overline{\mathbf{F}}_q)$ bármely pontjára teljesül, hogy $P \in E(\mathbf{F}_q)$ akkor és csak akkor, ha $\phi(P) = P$. Vagyis $E(\mathbf{F}_q) = \mathrm{Ker}(1 - \phi)$, így azt kapjuk, hogy $\#E(\mathbf{F}_q) = \#\,\mathrm{Ker}(1-\phi) = \deg(1-\phi)$ az előbbi két lemma miatt. Mivel $\mathrm{End}(E) - n$ a fokszám leképezés egy pozitív definit kvadratikus alak (felhasználtuk a lemmát), és így $\deg \phi = q$, a Cauchy-Schwarz-egyenlőtlenségből következik az állítás.

A következőkben megfogalmazzuk a zeta-függvényre vonatkozó Weil-sejtést.

Minden $n \geq 1$ egész szám esetén legyen $\mathbf{F}_{q^n}$ $\mathbf{F}_q$ n-edfokú kiterjesztése, így $\#\mathbf{F}_{q^n} = q^n$. Legyen $V/\mathbf{F}_q$ projektív változó úgy, hogy V az

$$f_1(x_0, \ldots, x_N) = \ldots = f_m(x_0, \ldots, x_N) = 0$$

megoldáshalamaza legyen, ahol $f_1, \ldots, f_m$ homogén polinomok $F_q$-ból vett együtthatókkal. Ekkor $V(\mathbf{F}_{q^n})$ $V$ $\mathbf{F}_{q^n}$-beli koordinátájú pontjainak halmaza. Kódoljuk minden $n \geq 1$ esetén $V$ $\mathbf{F}_{q^n}$ pontjainak számát egy generátorfüggvénnyel.

**3.7. Definíció.** *A $V/F_q$-hoz tartozó zeta-függvény a következő hatványsor:*

$$Z(V/F_q; T) = \exp\left(\sum_{n=1}^{\infty} (\#V(F_{q^n}))\frac{T^n}{n}\right).$$

*Itt bármely $F(T) \in Q[[T]]$ hatványsorra $\exp(F(T)) := \sum_{k\geq 0} F(T)^k/k!$. Ennek ismeretében a $\#V(F_{q^n})$ kiszámítható:*

$$\#V(F_{q^n}) = \frac{1}{(n-1)!}\frac{d^n}{dT^n}\log Z(V/F_q; T)|_{T=0}.$$

**3.11. Tétel (Weil-sejtés).** *Legyen $V/\mathbf{F}_q$ egy $N$-dimenziós sima projektív görbe. Ekkor*

$$Z(V/\mathbf{F}_q; T) \in Q(T),$$

*valamint $\exists \varepsilon$, $V$ úgynevezett Euler karakterisztikája, úgy, hogy*

$$Z(V/\mathbf{F}_q; 1/q^N T) = \pm q^{N\varepsilon/2} T^{\varepsilon} Z(V/\mathbf{F}_q; T),$$

*továbbá*

$$Z(V/\mathbf{F}_q; T) = \frac{P_1(T)\ldots P_{2N-1}(T)}{P_0(T)P_2(T)\ldots P_{2N}(T)},$$

*ahol* $\forall i\ P_i(T) \in Z[T], P_(T) = 1 - T$ *és* $P_{2N}(T) = 1 - q^N T$, *és minden* $0 \leq i \leq 2N$ *esetén a C feletti* $P_i(T)$ *polinomok előállnak a*

$$P_i(T) = \prod_{j=1}^{b_i} = (1 - \alpha_{ij} T)$$

*alakban, ahol* $|\alpha_{ij}| = q^{1/2}$.

Legyen l prím úgy, hogy $l \neq p = \mathrm{char}(\mathbf{F}_q)$. Létezik egy előállítás

$$\mathrm{End}(E) \to \mathrm{End}(T_l(E)), \psi \mapsto \psi,$$

és $Z_l$-ből bázist választva $T_l(E)$-hez felírhatjuk $\psi_l$-t $2x2$-es mátrixként és kiszámíthatjuk a determinánsát és nyomát, $\det(\psi_l), tr(\psi_l) \in Z_l$.

**3.4. Állítás.** *Legyen* $\psi \in \mathrm{End}(E)$. *Ekkor*

$$\det(\psi_l) = \deg(\psi) \text{ és } tr(\psi_l) = 1 + \deg(\psi) - \deg(1 - \psi).$$

*Speciálisan,* $\det(\psi_l)$ *és* $\mathrm{tr}(\psi_l)$ *egész számok és l függvényei.*

Az állítás bizonyítása a Weil-párosításból adódik, amivel a dolgozat véges keretein belül nem foglalkozunk. Alkalmazzuk a fenti állítást egy véges test feletti elliptikus görbére, így kiszámíthatjuk a pontok számát és következtethetünk a Frobenius endomorfizmus egy fontos tulajdonságára.

**3.12. Tétel.** *Legyen* $E/\mathbf{F}_q$ *elliptikus görbe, valamint* $\phi : E \to E, (x, y) \mapsto (x^q, y^q)$ *a q-adik hatványú Frobenius-endomorfizmus, és legyen* $a = q + 1 - \#E(F_q)$. *Legyenek a* $T^2 - aT + q$ *polinom gyökei* $\alpha, \beta \in C$. *Ekkor* $\alpha$ *és* $\beta$ *egymás komplex konjugáltjai,* $|\alpha| = |\beta| = \sqrt{q}$, *és minden* $n \geq 1$ *esetén teljesül, hogy*

$$\#E(\mathbf{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n.$$

**Bizonyítás.** A korábbi két lemma miatt: $\#E(\mathbf{F}_q) = \deg(1 - \phi)$. Korábbi állítás miatt:

$$\det(\phi_l) = \deg(\phi) = q, \mathrm{tr}(\phi_l) = 1 + \deg(\phi) - \deg(1 - \phi) = 1 + q - \#E(F_q) = a.$$

Így $\phi_l$ karakterisztikus polinomja

$$\det(T - \phi_l) = T^2 - tr(\phi_l)T + \det(\phi_l) = T^2 - aT + q.$$

Minthogy $\phi_l$ karakterisztikus polinomja együtthatói egészek, faktorizálhatjuk C felett:

$$\det(t - \phi_l) = T^2 - aT + q = (T - \alpha)(T - \beta).$$

Minden $m/n \in \mathbb{Q}$ esetén

$$\det(\frac{m}{n} - \phi_l) = \frac{\det(m - n\phi_l)}{n^2} = \frac{\deg(m - n\phi)}{n^2} \geq 0.$$

Ennélfogva a kvadratikus polinom $\det(t - \phi_l) = T^2 - aT + q \in Z[T]$ nemnegatív minden $T \in R$-re, így gyökei komplex konjugáltak, vagy egy kétszeres gyöke van. Mindkét esetben $|\alpha| = |\beta|$, és az $\alpha\beta = \det(\phi_l) = \deg \phi = q$ összefüggésből $|\alpha| = |\beta| = \sqrt{q}$, amiből következik az állítás első része.

Hasonlóan, minden $n \geq 1$ egészre a $q^n$-edik kitevőjű Frobenius endomorfizmusra igaz, hogy

$$\#E(F_{q^n}) = \deg(1 - \phi^n).$$

Ez alapján $\phi_l^n$ karakterisztikus polinomja:

$$\det(T - \phi_l^n) = (T - \alpha^n)(T - \beta^n).$$

(Ehhez $\phi_l$-t tegyük normálalakba, így felső trianguláris mátrixot kapunk $\alpha$-val és $\beta$-val a diagonálisban.) Speciálisan

$$\#E(F_{q^n}) = \deg(1 - \phi^n) = \det(1 - \phi_l^n)$$

korábbi állítás miatt
$= 1.\alpha^n - \beta n + q^n$. Utóbbi tételből egyszerűen következik a Weil-sejtés.

# 4. Kriptográfiai alkalmazás

Az elliptikus görbék az utóbbi évtizedekben egyre nagyobb jelentőséggel bírnak a titkosírások területén, köszönhetően azon tulajdonságaiknak, hogy nagyon bonyolultak, viszont kevés paraméterrel megadhatóak és jelenleg nincsenek rájuk hatékony módszerek. Fontos alkalmazásuk nagy számok faktorizációja, egészen pontosan nagy prímek szorzatának felbontása. Azt ugyanis általában könnyű megmutatni, hogy egy adott szám összetett. Nemtriviális osztót találni sokszor nagyon nehéz feladat, erre épül például a nyílt kulcsú RSA titkosírás biztonsága. A jelenleg ismert leggyorsabb faktorizációs eljárás a számtestszita, előtte pedig a négyzetes (kvadratikus) szita töltötte be ezt a szerepet. Hendrik Lenstra eljárásának futási ideje a négyzetes szitáéhoz mérhető.

Ha $N$ a faktorizálandó összetett szám, $p$ pedig a legkisebb prímosztója, akkor a Lenstra-algoritmus

$$\exp(c\sqrt{(\log p)(\log\log p)}$$

lépésben fut le. Habár ez azt jelenti, hogy $\sqrt{N}$-nél jóval kisebb $p$ esetén a Lenstra gyorsan lefut, jegyezzük meg, hogy az RSA-ban használt összetett szám két egymáshoz viszonylag közel álló prím szorzata, így ilyen esetekben a szita algoritmusok hatásosabbak.

Egy adott $n$ szám faktorizációja az elliptikus görbék segítségével azt az algoritmust takarja, ami egy véletlenül kiválasztott elliptikus görbe egy pontjának többszörösét számítja ki modulo $n$. Ezt más néven Lenstra elliptikus görbe módszerének nevezzük, mely Pollard $p-1$-módszerén alapszik, amely akkor működik, ha $p|n$ úgy, hogy $p-1$ minden prímosztója elég kicsi.

**Pollard $p-1$ algoritmusa.** Legyen $n$ egy nagy egész összetett szám egy ismeretlen $p$ prímosztóval, továbbá legyen $p-1$ prímfelbontása

$$p-1 = q_1^{e_1} q_2^{e_2} \dots q_t^{e_t}.$$

Legyen $L$ a következő mennyiség:

$$L = \max_{1\le j\le t} e_j q_j.$$

Ekkor a következő algoritmus a legtöbb alapértékre talál $N$-hez nemtriviális osztót valamely $i \le L$-re.

(*) Legyen az alapérték egy $a$ egész szám ($2 \le a < N$), állítsuk be $A$ értékét $a$-ra. Vegye fel $i$ sorban a következő értéket: $i = 1, 2, \dots, L$. Legyen $A = A^i \bmod N$. Számítsuk ki az m számot: $m = lnko(A-1, N)$ Ha $1 < m < N$, akkor $F$ nemtriviális osztója $N$-nek. Ha $m = N$, akkor térjünk vissza (*)-hoz és válasszunk $a$-nak új értéket.

Az $i$ szám kiszámítható a

$$i = i(b) = \Pi_{q \leq b} p^{e(q)}$$

formulával. A módszer sikere azon múlik, hogy a legkisebb $p$ prímosztó lényegesen kisebb legyen $\sqrt{n}$-nél.

**Bizonyítás.** A ciklus $i$-edik iterációjában $A$ értéke $a^{i!}$ mod $N$. $L$ úgy lett definiálva, hogy $q_j^{e_j} | L!$ minden $j$-re, $1 \leq j \leq t$, így $p - 1 | L!$ is teljesül. Ez a kis Fermat-tételből következik, ami kimondja, hogy $a^{L!} \equiv 1 \pmod{p}$, így $m$ értéke osztható $p$-vel. Mivel nem valószínű, hogy $a^{L!} \equiv 1 \pmod{N}$, megkaptuk $N$ egy nemtriviális osztóját.

Lenstra megmutatta, hogy a Pollard-módszer attól függ, hogy a *modp* osztályok csoportot alkotnak, és hogy erre a célra az elliptikus görbék is használhatóak.

**Lenstra elliptikus görbe faktorizációs algoritmusa.** Legyen $N$ a felbontandó pozitív egész szám, és használjuk a lenti algoritmust. Tegyük fel, hogy $N$-nek van nemtriviális $p$ prímosztója úgy, hogy az $E$ görbére és az $L$ számra

$$\#E(F_p) = q_1^{e_1} q_2^{e_2} \dots q_t^{e_t} \text{ és } L \geq \max\{e_1 q_1, \dots, e_t q_t\},$$

ahol $q_1, \dots, q_t$ páronként különböző prímek. Ekkor az alábbi algoritmus nagy valószínűséggel talál az $N$ számhoz osztót.

Válasszunk a ciklusnak felső határt, jelöljük ezt $L$-lel. (*) Válasszunk egy $E$ elliptikus görbét mod $N$ és egy $P \in E(Z/NZ)$ pontot. Legyen $Q = P$. Legyen $i = 2, 3, \dots, L$. Cseréljük ki $Q$-t $[i]Q$-ra $E(Z/NZ)$-ben. Ha ezalatt egy $a \in Z/NZ$ inverzére van szükségünk, és ez az elem nem létezik, akkor lnko($a$,$N$) valószínűleg osztója $N$-nek. Vége az $i$-edik iterációnak. Térjünk vissza (*)-hoz, válasszunk új görbét és pontot.

Legyen

$$\Gamma : Y^2 Z = X^3 + AXZ^2 + BZ^3$$

egy elliptikus görbe és legyen $P(x, y, z)$ a görbe egy pontja, $x, y, z \in Z$. Legyen

$$k(x, y, z) = (x_k, y_k, z_k)$$

, ahol $k > 1$ egész és $x_k, y_k, z_k$ egészek. Legyen $p$ prím, és tegyük fel, hogy $\Gamma$ mod $p$ egy elliptikus görbe $\mathbf{Z}$ felett mod $p$. A mod $p$ pontok csoportot alkotnak, aminek rendje

$$|G| = N = N_p = N_p(A, B)$$

, $N$-re igaz, hogy $|N - (p + 1)| < 2\sqrt{p}$. Ha $N | k$, akkor a $(x_k, y_k, z_k)$ pont mod $p$ az $O$ pont a végtelenben, így $p | z_k$. Adott $A, B, x, y, z$ esetén az $(x_k, y_k, z_k)$ koordinátái $\mathrm{O}(\log k)$ lépésben kiszámíthatóak.

Legyen $n$ a nagy faktorizálandó egész szám és legyen $k = k(b)$ valamely megfelelő $b$-re. Ekkor $(x_k, y_k, z_k) mod n$ kiértékelhető $O(\log k)$ lépésben, modulo $n$ összeadással, szorzással és kivonással. Mivel $p | z_k mod n$, így $N_p | k$, ezért

$$p | m = \text{lnko}(n, z_k).$$

Ha $z_k \equiv 0 \pmod{n}$, akkor nincs szerencsénk, különben $m$ megfelelő osztó lesz.

A következőkben megnézzük, hogyan számolhatjuk meg egy véges test feletti elliptikus görbe pontjait, ami a kriptográfiában sokszor fontos. Legyen $E/\mathbf{F}_q$ egy véges test feletti elliptikus görbe. A Hasse-tétel szerint a görbepontok száma

$$\#E(\mathbf{F}_q) = q + 1 - a_q, \text{ ahol } |a_q| \leq 2\sqrt{q}.$$

Az egyszerűség kedvéért tegyük fel, hogy q páratlan és E felírható a következő alakban:

$$E : y^2 = f(x) = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

**Schoof-algoritmus.** Legyen $E/\mathbf{F}_q$ egy véges test feletti elliptikus görbe. Az alábbi algoritmus polinom időben kiszámítja $\#E(\mathbf{F}_q)$-t, mégpedig $\mathrm{O}((\log q)^8)$ lépésben.

Legyen $A = 1$ és $l = 3$. Ciklus, addig tart, amíg $A < 4\sqrt{q}$. Ciklus: $n = 0, 1, 2, \ldots, l-1$-re ha az $R_l$ gyűrűben

$$(x^{q^2}, y^{q^2}) + [q](x, y) = [n](x^q, y^q),$$

akkor kilépünk az n ciklusból. n szerinti ciklus vége. Legyen $A = lA$. Legyen $n_l = n$. Cseréljük ki $l$-et a következő legnagyobb prímre. A ciklus vége. A kínai maradéktétel segítségével keresünk a-t úgy, hogy $a \equiv n_l (mod l)$ $n_l$ minden értékére. Visszatérési érték: $\#E(\mathbf{F}_q) = q + 1 - a$.

A nyílt kulcsú titkosírás gondolata Diffie és Hellman által született meg. Elképzelésüket elsőként Rivest, Shamir és Adleman valósította meg az RSA-val. Diffie és Hellman ötlete a diszkrét logaritmus problémán alapult egy $\mathbf{F}_q^*$-ban, majd ElGamal is hasonló alapokra fektetve alkotta meg titkosírását. Koblitz és Miller kicserélték az $\mathbf{F}_q$ testet egy E elliptikus görbére annak reményében, hogy az $E(\mathbf{F}_q)$ elliptikus görbe csoportban a diszkrét logaritmus problémája nehezebbenk bizonyul majd.

**4.1. Definíció.** *Legyen* $\mathbf{G}$ *csoport, legyenek* $x$ *és* $y$ *elemei úgy, hogy* $y \in [x]$. *Ekkor diszkrét logaritmus problémának (DLP) nevezzük az* $x^m = y$ *megoldását* $m \geq 1$*-re.*

**Diffie–Hellman-kulcsváltás.** A következőkben annak módja szerepel, hogy Alice és Bob hogyan adhatja meg egymásnak biztonságosan egy elliptikus görbe egy pontjának értékét anélkül, hogy bármelyikük ismerné azt.

Először Alice és Bob megegyeznek egy $\mathbf{F}_q$ véges testben, egy $E/\mathbf{F}_q$ elliptikus görbében, és egy $P \in E/\mathbf{F}_q$ pontban. Alice kiválaszt egy titkos a egészet és kiszámítja az $A = [a]P \in E/\mathbf{F}_q$-t. Bob kiválaszt egy titkos b egészet és kiszámítja a $B = [b]P \in E/\mathbf{F}_q$-t. Ezután Alice és Bob megosztják egymással A és B értékét (nem feltétlenül titkos úton). Alice kiszámítja [a]B-t és Bob kiszámítja [b]A-t. Ekkor mindketten tudják az [ab]P pont értékét.

**ElGamal titkosírás.** A következőkben azt fogjuk látni, hogyan küldhet Bob üzenetet Alice-nak biztonságosan.

Először Alice és Bob megegyeznek egy $\mathbf{F}_q$ véges testben, egy $E/\mathbf{F}_q$ elliptikus görbében, és egy $P \in E/\mathbf{F}_q$ pontban. Alice kiválaszt egy titkos $a$ egészet és kiszámítja az $A = [a]P \in E/\mathbf{F}_q$-t. Alice nyilvánosságra hozza az A pontot a saját publikus kulcsaként, titkos kulcsa az a lesz. Bob kiválaszt egy $M \in E(\mathbf{F}_q)$ szöveget és egy véletlen $k$ egészet. Kiszámítja a

$$B_1 = [k]P \in E(\mathbf{F}_q) s B_2 = M + [k]A \in E(\mathbf{F}_q)$$

pontokat. Bob elküldi a $(B_1, B_2)$ szöveget Alice-nek (nem feltétlenül titkos úton). Alice a titkos kulcsa segítségévelkiszámítja a $B_2 - [a]B_1 \in E(\mathbf{F}_q) - t$, ami megegyezik Bob eredeti üzenetével.

**Digitális aláírás elliptikus görbe segítségével (Elliptic Curve Digital Signature Algorithm, ECDSA).** A következők megmutatják Alice-nak, hogy hogyan írjon alá egy digitális dokumentumot úgy, hogy az az aláírás Bob számára hiteles legyen.

Először Alice és Bob megegyeznek egy $\mathbf{F}_q$ véges testben, egy $E/\mathbf{F}_q$ elliptikus görbében, és egy N prímrendű $P \in E/\mathbf{F}_q$ pontban. Alice kiválaszt egy titkos $a$ egészet és kiszámítja az $A = [a]P \in E/\mathbf{F}_q$-t. Alice nyilvánosságra hozza az $A$ pontot, az ő nyilvános hitelesítési kulcsát. A titkos $a$ lesz az ő privát aláíró kulcsa. Alice kiválaszt egy d digitális dokumentumot mod $N$ és egy $k$ véletlen egészet mod $N$. Alice kiszámítja $[k]P$-t és

$$s_1 \equiv x([k]P) (mod N) s s_2 \equiv (d + a s_1) k^{-1} \pmod{N}.$$

Bob kiszámítja

$$v_1 \equiv d s_2^{-1} (mod N) s v_2 \equiv s_1 s_2^{-1} \pmod{N}.$$

Ezután kiszámítja $[v_1]P + [v_2]A \in E(F_q)$-t és megbizonyosik arról, hogy

$$x([v_1]P + [v_2]A) \equiv s_1 \pmod{N}.$$

# Hivatkozások


[1] Bálintné Szendrei Mária: *Alkalmazott algebra*, Egyetemi előadás-vázlatok, Szeged, 2009.

[2] J. W. S. Cassels: *Lectures on elliptic curves*, Cambridge University Press, Cambridge, 1991

[3] Czédli Gábor: *Matematikai titkosírások*, Egyetemi előadás-vázlatok, Szeged, 2009.

[4] C. G. Gibson *Elementary Geometry of Algebraic Curves: an Undergraduate Introduction*, Cambridge University Press, Cambridge, 1998

[5] R. Lidl és H. Niederreiter: *Introduction to finite fields and their applications*, Cambridge University Press, Cambridge, 1986

[6] Nagy Gábor Péter: *Algebrai görbék*, Egyetemi előadás-vázlatok, Szeged, 2009.

[7] Joseph H. Silverman: *The Arithmetic of Elliptic Curves*, Springer, New York, 2009.

[8] Rédei László: *Algebra I.*, Akadémiai Kiadó, Budapest, 1954.

# Nyilatkozat

Alulírott Vörös Anett, Matematika BSc szakos hallgató, kijelentem, hogy a szakdolgozatban foglaltak saját munkám eredményei, és csak a hivatkozott forrásokat (szakirodalom, eszközök, stb.) használtam fel.

Tudomásul veszem azt, hogy szakdolgozatomat a Szegedi Tudományegyetem könyvtárában, a kölcsönözhető könyvek között helyezik el.

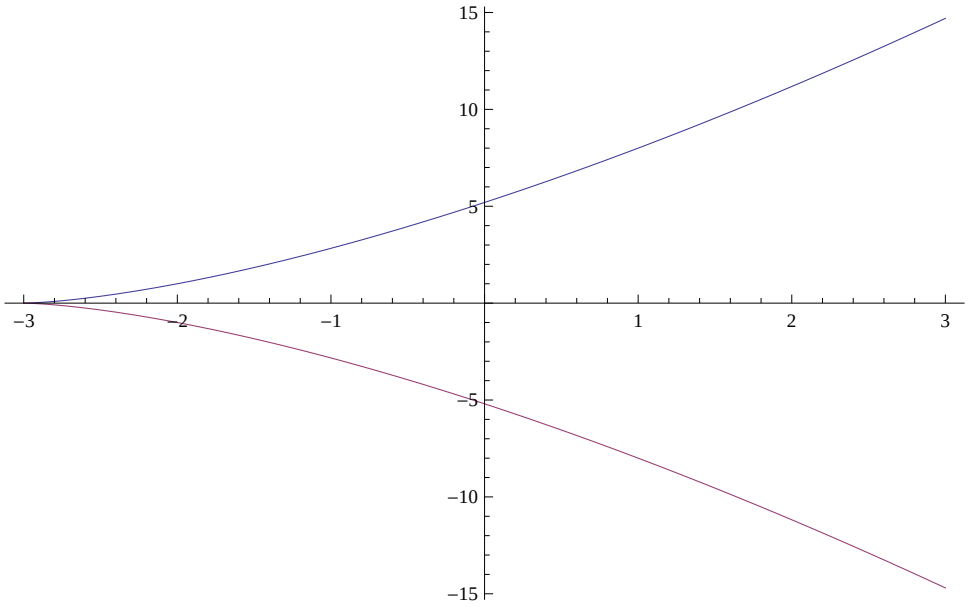
Szeged, 2011. 05. 13.

Vörös Anett

# Melleklet

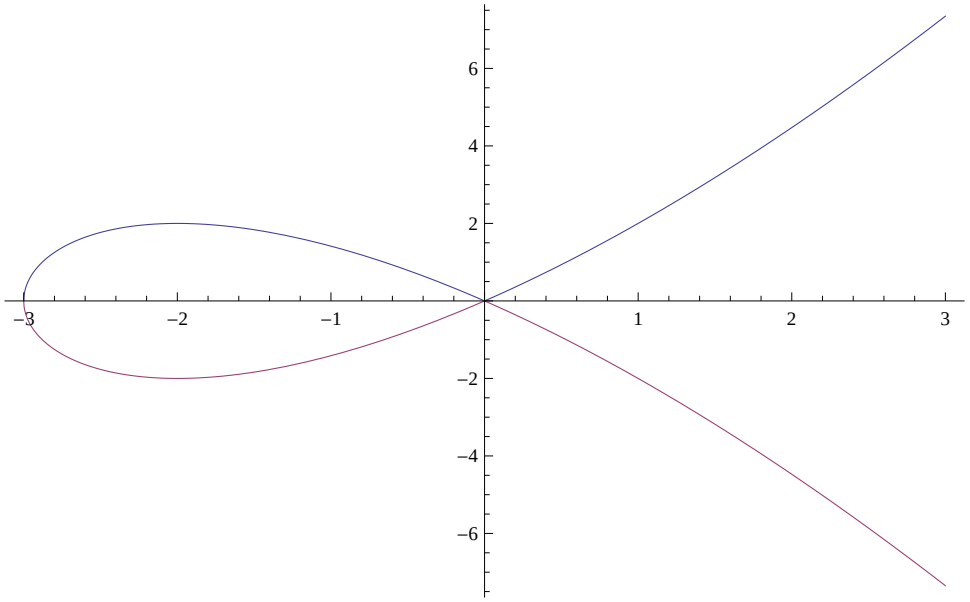
## Szingularis kubikus gorbek

```
Plot[{Sqrt[(x + 3)^3], -Sqrt[(x + 3)^3]}, {x, -3, 3}]
```




1. Csuccsal rendelkezo gorbe: $y^2 = (x + 3)^3$

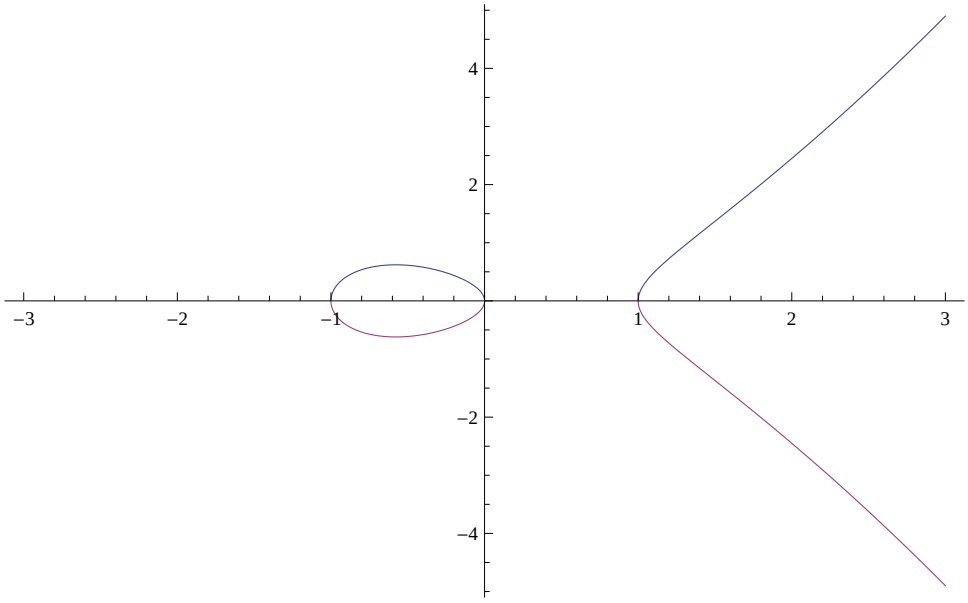
```
Plot[{Sqrt[x^3 + 3 x^2], -Sqrt[x^3 + 3 x^2]}, {x, -3, 3}]
```




2. Szingularis gorbe, csomoval: $y^2 = x^3 + 3\,x^2$

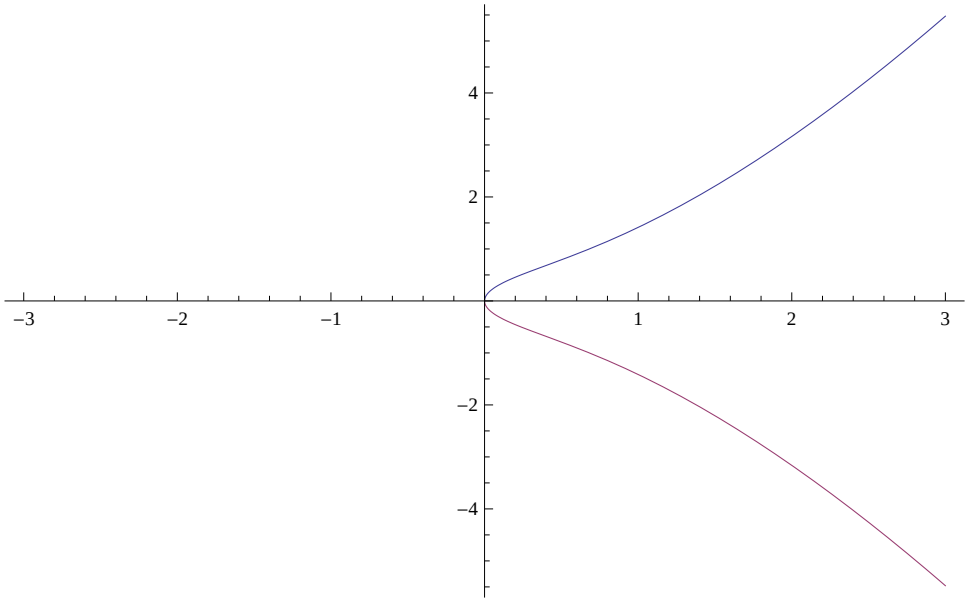
## Elliptikus gorbek

```
Plot[{Sqrt[x^3 - x], -Sqrt[x^3 - x]}, {x, -3, 3}]
```



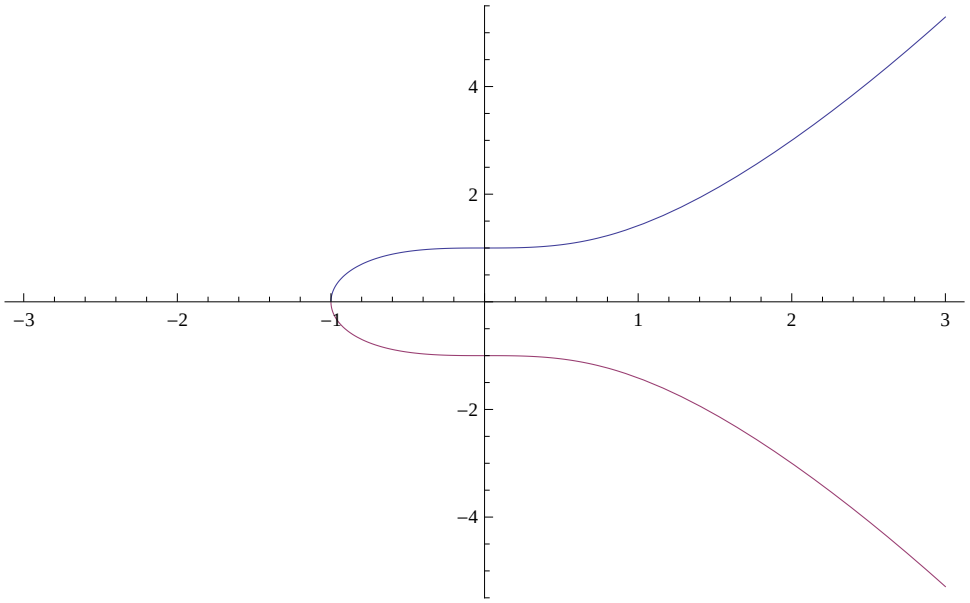

3. E: $y^2 = x^3$ - x

```
Plot[{Sqrt[x^3 + x], -Sqrt[x^3 + x]}, {x, -3, 3}]
```



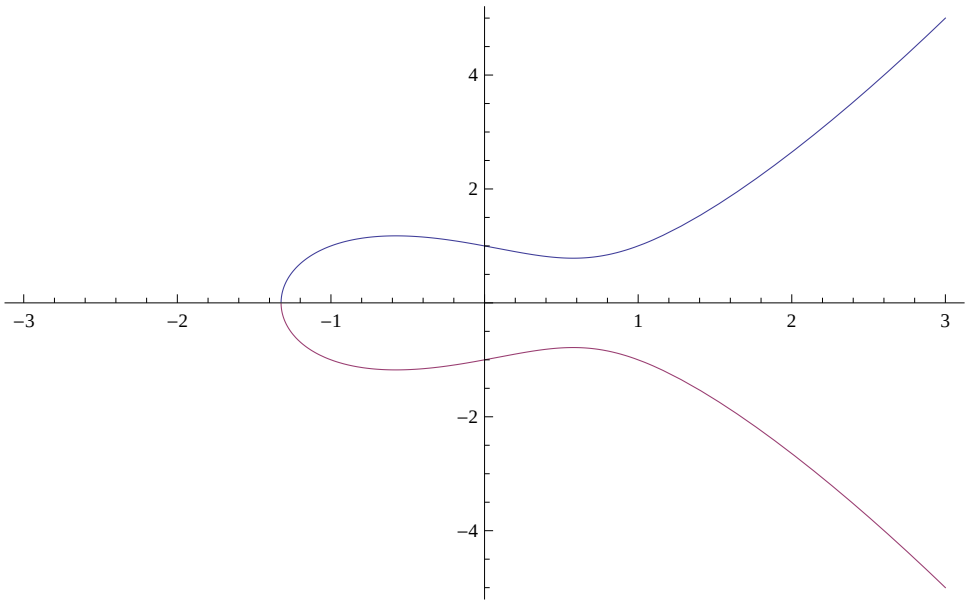

4. E: $y^2 = x^3$ + x

```
Plot[{Sqrt[x^3 + 1], -Sqrt[x^3 + 1]}, {x, -3, 3}]
```




5. E: $y^2 = x^3 + 1$

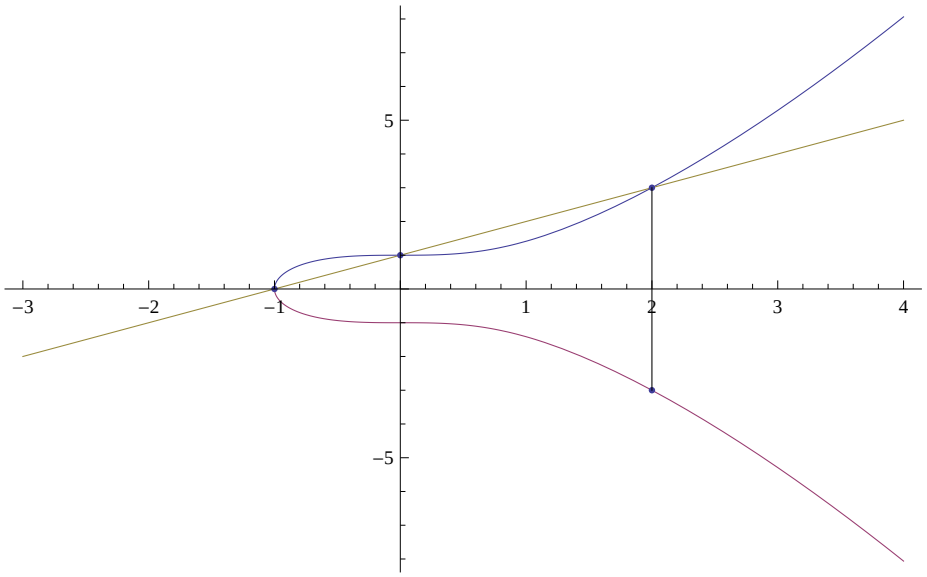
```
Plot[{Sqrt[x^3 - x + 1], -Sqrt[x^3 - x + 1]}, {x, -3, 3}]
```




6. E: $y^2 = x^3$ - x + 1

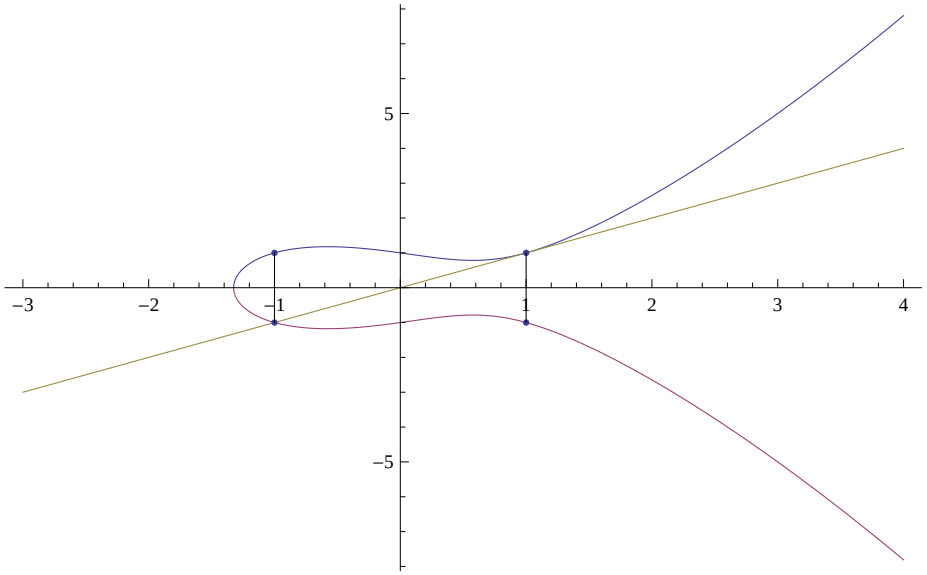
## Pontok osszeadasa, mint csoportmuvelet

```
Show[Plot[{Sqrt[x^3 + 1], -Sqrt[x^3 + 1], x + 1}, {x, -3, 4}],
 ListPlot[{{2, -3}, {2, 3}, {0, 1},
   {-1, 0}}], Graphics[Line[{{2, -3}, {2, 3}}]]]
```



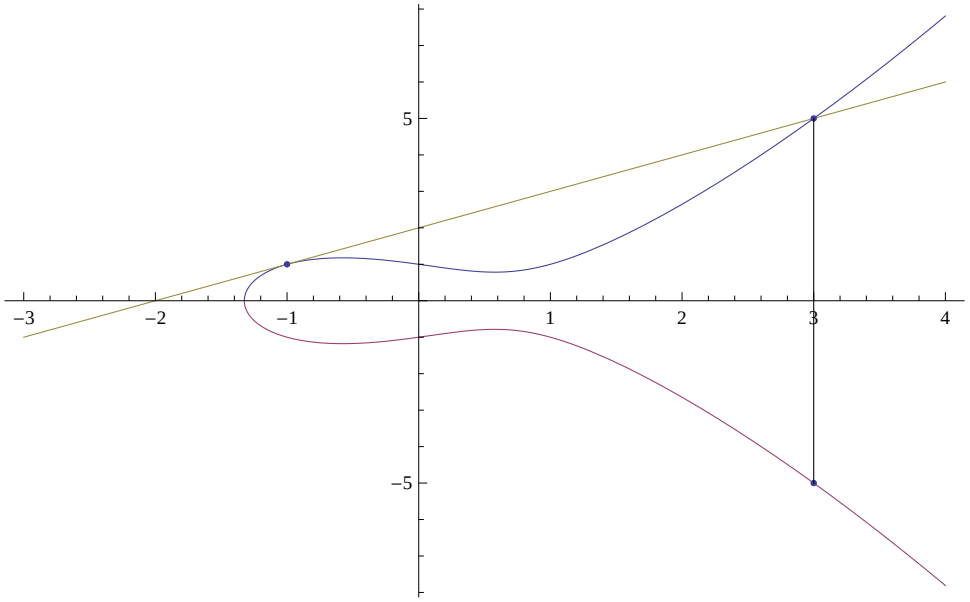

7. E: $y^2 = x^3 + 1$, L: y = x + 1; A (-1, 0), B (0, 1), C (2, 3), D (2, -3);
   A + B = D, A + B + C = O

```
Show[Plot[{Sqrt[x^3 - x + 1], -Sqrt[x^3 - x + 1], x}, {x, -3, 4}], ListPlot[{{1, -1}, {1, 1},
   {-1, -1}, {-1, 1}}], Graphics[Line[{{1, 1}, {1, -1}}]],
 Graphics[Line[{{-1, -1}, {-1, 1}}]]]
```



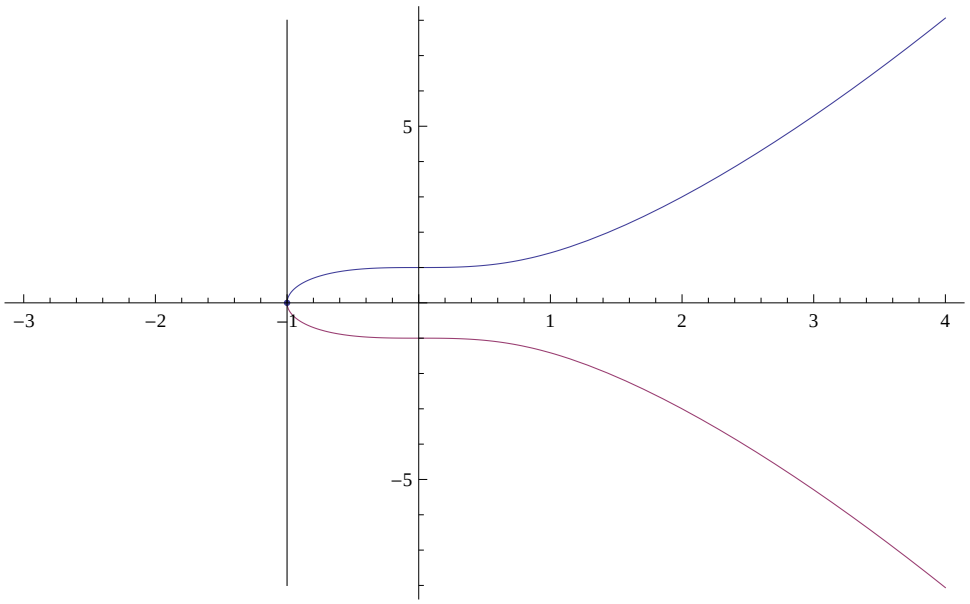

8. E: $y^2 = x^3 + 1$, L: y = x + 1;A (-1, -1), B (1, 1), C (1, -1), D (-1, 1);
   A + B = C, B + B = D, A + B + B = O

```
Show[Plot[{Sqrt[x^3 - x + 1], -Sqrt[x^3 - x + 1], x + 2}, {x, -3, 4}],
 ListPlot[{{-1, 1}, {3, 5},
   {3, -5}}], Graphics[Line[{{3, 5}, {3, -5}}]]]
```




9. E: $y^2 = x^3$ - x + 1, L: y = x + 2; A (-1, 1), B (3, 5), C (3, -5);
   A + A = C, A + A + B = O

```
Show[Plot[{Sqrt[x^3 + 1], -Sqrt[x^3 + 1]}, {x, -3, 4}], ListPlot[{{-1, 0}}],
 Graphics[Line[{{-1, 8}, {-1, -8}}]]]
```




10. E: $y^2 = x^3$ + 1, L: x = -1; A (-1, 0);
    A + A = O