Kódoláselmélet 2020 október 14

Diszkrét logaritmus probléma

$$[g] = GF^*(p^k) \cong (\mathbb{Z}_{p^k-1}, +) = [1] \text{ ciklikus csoport}$$

" mult. csop

$$\{1, g, g^2, \dots, g^{p^k-2}\}$$

itt nehéz számolni logaritmust

itt könnyű számolni "logaritmust"

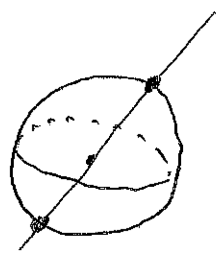
Elliptikus görbéken alapuló titkosítások

Véges test multiplikatív csoportja helyett más ciklikus csoportot keresünk amelyben nehéz számolni a logaritmust.

Def: Legyen F számtest és $f \in F[x,y]$ 2-határozatlanú polinom. Az f gyökeit

$$V(f) = \{(x,y) \in F^2 \mid f(x,y) = 0\}$$

affin algebrai görbének nevezzük.



Def: homogén polinom $\Longleftrightarrow$ minden monomja ugyanolyan fokszámú.

$$f(x,y) = g(x,y,1)$$

Példa: $f = x^3 + 2xy + 7$ homogenizációja

$$g = x^3 + 2xyz + 7z^3 \in F[x,y,z]$$

Def: projektív algebrai görbe $g \in F[x,y,z]$ homogén

$(tx : ty : tz)$

$$V(g) = \{(x : y : z) \mid g(x,y,z) = 0\}$$

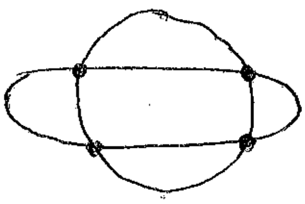
homogén koordináták!

Tétel (Bézout) Ha $f, g \in F[x,y]$ relatív prím polinomok (nincs nem egység közös osztójuk), akkor

$$|V(f) \cap V(g)| \leq \deg f \cdot \deg g,$$

azaz legfeljebb $\deg f \cdot \deg g$ közös gyökük van az affin F^2 síkon.

Példa: $x^2+y^2=1$, $(1x)^2+(2y)^2=3$



kör és ellipszis
másodfokú görbék

Tétel (Bézout) Ha F algebrailag zárt és $f, g \in F[x,y,z]$ relatív prím, akkor a projektív algebrai görbéknek pontosan $\deg f \cdot \deg g$ közös metszéspontja van (multiplicitással) a projektív síkon.

Def: elliptikus görbe $f(x,y) = g(x) - h(y)$ ahol $\deg(g) = 3$ és $\deg(h) = 2$. ~~(főpolinomok)~~

Megj: Tehát az elliptikus görbe nem más, mint az

$$y^2 + ay + b = x^3 + cx^2 + dx + e$$

megoldásainak halmaza. Megfelelő $x' = \alpha x$ és $y' = \beta y$ helyettesítéssel elérhető, hogy főpolinomot kapjunk, és $x' = x + \alpha$ és $y' = y + \beta$ helyettesítéssel hogy $a = 0$ és $c = 0$ legyen.

$$(y')^2 - 2\beta y' + \beta^2 + ay' - a\beta + b = (y'-\beta)^2 + a(y'-\beta) + b \qquad y = y' - \beta$$

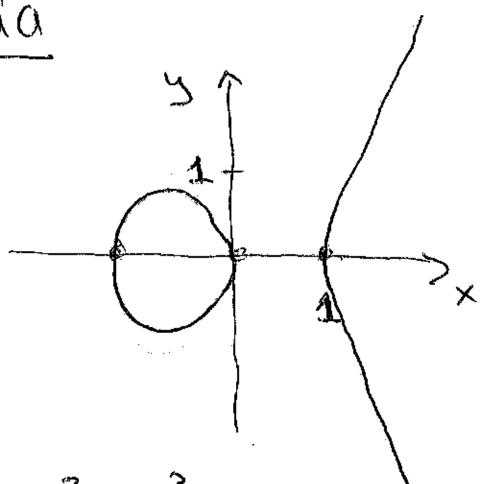
Áll: Ha a test karakterisztikája nem 2 és nem 3, akkor minden elliptikus görbe

$$y^2 = x^3 + ax + b$$

alakra hozható.

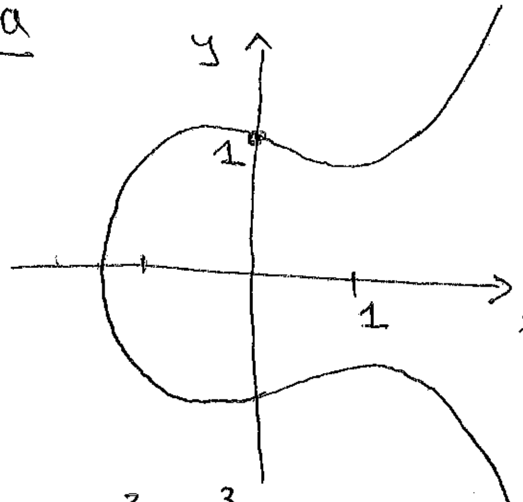
szimmetrikus az x-tengelyre

Példa



$y^2 = x^3 - x$

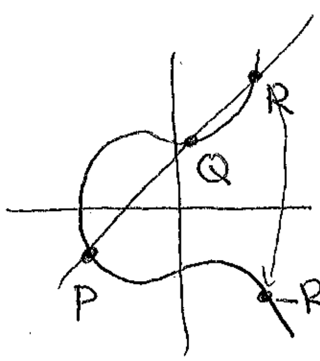
Példa



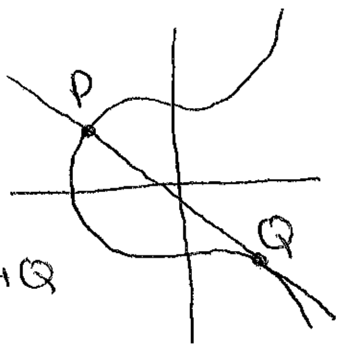
$y^2 = x^3 - x + 1$

A Bézout tétel következménye: Minden elliptikus görbét minden egyenes 3 pontban metsz a projektív síkon (multiplicitással).

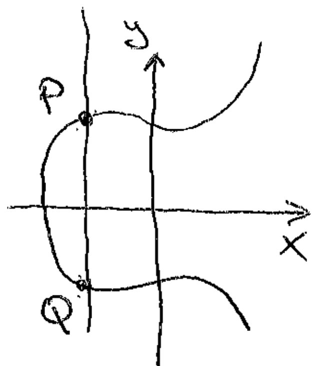
Def: Legyen O a végtelen távoli pont. Az elliptikus görbe pontjain és a O-n definiálunk egy Abel-csoportot az alábbi szabályok szerint:



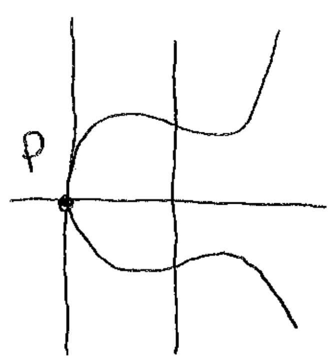
$P+Q+R=O$



$P+Q+Q=O$



$P+Q+O=O$



$P+P+O=O$

<u>Áll</u>: Adott $P, Q \in V(f)$ elliptikus görbe két pontja, ekkor kiszámolható a PQ egyenes harmadik metszéspontja $R \in V(f)$. Így

$$P + Q = -R$$ ← R-nek az x tengelyre való tükrözése.

<u>Biz</u> $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $y^2 = x^3 + ax + b$

(1) egyenes meredeksége $s = \dfrac{y_1 - y_2}{x_1 - x_2}$ feltéve hogy $x_1 \neq x_2$

az egyenes meg $y = sx + d$ ahol d valamilyen paraméter.

a metszéspont teljesíti az

$$(sx + d)^2 = x^3 + ax + b$$ egyenletet, azaz

$$0 = x^3 - s^2x^2 + (\quad)x + (\quad)$$

Ennek 3 megoldása van: P, Q és R első koordinátája azaz

$$(x - x_1)(x - x_2)(x - x_3) = x^3 - s^2x^2 + \dots$$

$$-x_1 - x_2 - x_3 = -s^2$$

$R = (x_3, y_3)$

$$x_3 = s^2 - x_1 - x_2$$

$$y_3 = y_1 + s(x_3 - x_1)$$

(2) $x_1 = x_2$ és $Q = -P$. Ekkor $R = O$ (függőleges egyenes)

(3) érintő egyenes $Q = P$.

$$s = \frac{3x_1^2 + a}{2y_1} \qquad x_3 = s^2 - 2x_1$$

$$y_3 = y_1 + s(x_3 - x_1)$$

Tétel: Az elliptikus görbén előbb definiált + művelet egy $(G;+)$ Abel-csoport, melynek O a zéruseleme.

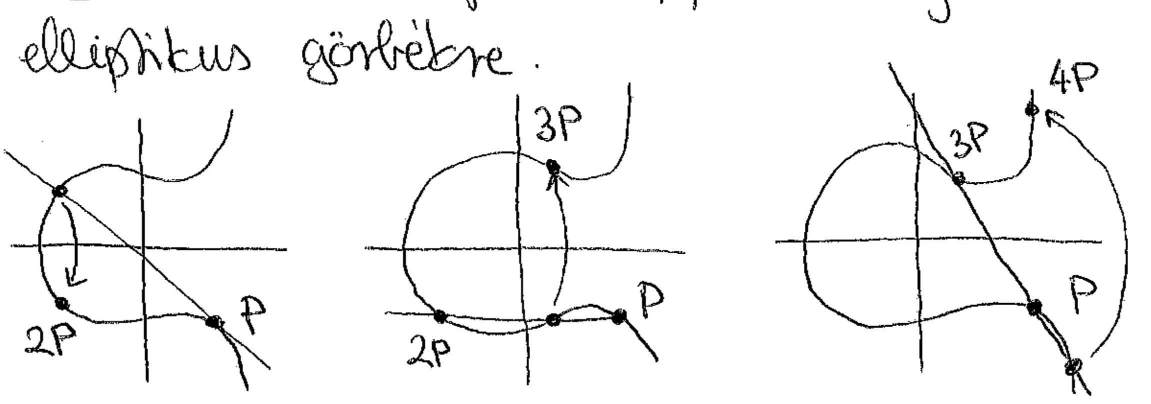
Tétel: Minden tetszőleges véges test felett is működik, melynek karakterisztikája nem 2 vagy 3.

Tétel (Mordell) Ha $F = \mathbb{Q}$, akkor az elliptikus görbén kapott Abel-csoport végesen generált.

Tétel (Hasse) Ha $F = GF(q)$ véges test, akkor a G csoport természetesen véges, de közel q pontja van:

$$\big||G| - (q+1)\big| \leq 2\sqrt{q}.$$

Továbbá a G csoport vagy ciklikus, vagy kettő ciklikus csoport direkt szorzata. Tehát legalább az egyik direkt tényezőnek elég sok eleme van (közel $\sqrt{q}$). Megvan a keresett "csúnya" ciklikus csoportunk, ahol nehezen lehet "logaritmust" számolni. Minden diszkrét logaritmuson alapuló rejtjelezési alg átvihető elliptikus görbékre.



stb.

$\boxed{q=7,\ g=3}$ $g^0=1$ $g^5=5$ ⑥

$g^2=2$ $g^6=1$

$g^3=6$

$g^4=4$

Fej vagy írás telefonon

Hogyan lehet nyílt csatornán n résztvevő közül egyet igazságosan kisorsolni.

$k_1=2$, $k_2=3$

$g^2=\boxed{2}$ $g^3=\boxed{6}$

Vegyünk egy $GF(q)$ véges testet és abban egy g primitív elemet. Mindenki választ magának egy $0 \leq k_i \leq q-1$ egészet, és mindenkinek megmondja g^{k_i}-t. Ha már mindenki megkapta mindenkitől a hatványt, akkor közzé teszi k_i-t is. A keresett sorsolás eredménye $k_1+k_2+\ldots+k_n \pmod n$ lesz. Nem csalhat senki sem, mert mindenki ellenőrizheti a g^{k_i} hatványt, és mivel a diszkrét logaritmus nehéz, ezért a hatvány ismeretében sem tudja kiszámolni k_i-t, így nem nyer azzal valaki semmit sem ~~hogy~~ ha a többiek publikus g^{k_i} értékei ismeretében választ magának k_j-t.

Vigyázni kell, hogy milyen sorrendben mondják be az értékeket. Például g^{k_1} ismeretében a második játékos bemondja $(g^{k_1})^{-1}$-et anélkül hogy tudná k_1-et. Miután az első játékos megmondja k_1-et akkor a második $(q-1)-k_1$-et mond ami átmegy az ellenőrzésen, és az eredmény ~~g~~ garantáltan ~~q-1~~ $q-1 \bmod n$ lesz!!!

Meggyőző bizonyítás részletek nélkül

Tegyük fel, hogy A egy nagy felfedezést tesz (mondjuk bebizonyította, hogy P = NP). Ha közzéteszi a bizonyítást és algoritmust, akkor mindenki fel tud mindent törni, és ezt nem akarja. Ha csak egy publikus kóddal bekódolt verziót tesz közzé, akkor később be tudja bizonyítani, hogy ő volt a feltaláló, de senki se hinné addig neki. Létezik olyan protokoll, amellyel be tudja úgy kódolni a bizonyítást, hogy az ellenőrizhető legyen, de semmilyen olyan információt nem tartalmaz, amelyből az eredeti bizonyítás megkapható volna.

fully homomorphic encryption

Cloud computing alkalmazás

Más: Meg tudnuk valakit győzni, hogy két 4k-1 alakú prím szorzata összetett szám anélkül, hogy felfednénk a prímeket.

Irodalom:

1. Salooma: Public Key Cryptography, 1990.
2. Koblitz: A Course in Number Theory and Cryptography, 1994.
3. Fulton: Algebraic Curves, an Introduction to Algebraic Geometry, 2008.