Elliptikus görbék

PPKE, ITK
Csapodi Márton

Használatuk

Az elliptikus görbék kriptográfiai alkalmazását 1985-ben két kutató javasolta:

- Neal Koblitz (University of Washington)
- Victor Miller (IBM)

A jelenlegi nyilvános kulcsú eljárások elsősorban:

- egészek faktorizációja
- diszkrét logaritmus

problémákon alapulnak.

A diszkrét logaritmus számítható "elliptikus görbe felett".

Használatuk

Az alábbi táblázatban három eljárás általánosan vagy szabvány szerint használt kulcsméreteit láthatjuk (ECC: elliptikus görbe feletti diszkrét logaritmus alapú).

NIST·javaslata·az·egyes·kriptorendszerek·kulcshosszának·összehasonlítására:¤			
ECC·modulus¤	AES¤	RSA↵modulus¤	RSA:ECC¤
112¤	56¤	512¤	5:1¤
161¤	80¤	1024¤	6:1¤
256¤	128¤	3072¤	12:1¤
384¤	192¤	7680¤	20:1¤
512¤	256¤	15630¤	30:1¤

Az egy sorban lévő kulcsméretek közel azonos biztonságot nyújtanak (a NIST ajánlása szerint).

Használatuk

Az ECC sokkal kisebb kulcsmérettel is biztonságos:

- gyorsabb algoritmusok
- kevesebb továbbítandó és kezelendő adat
- kisebb tárigény
- kisebb tanúsítványok.

Használatuk a nyilvános kulcsú eljárásokon kívül:

- prímtényezőkre bontás
- prímteszt

Definíció

Elliptikus görbe: $y^2 = f(x)$ alakú egyenlettel definiált síkbeli görbe, ahol

- f(x) egy $x^3+ax+ b$ alakú kifejezés
- x, y valós változók (egyelőre)
- a, b egész számok (egyelőre)
- a görbe nemszinguláris

Általános képlet: $y^2+a_1xy+a_2y=x^3+a_3x^2+a_4x+a_5$

Izomorfizmus erejéig visszavezethető az előbbire.

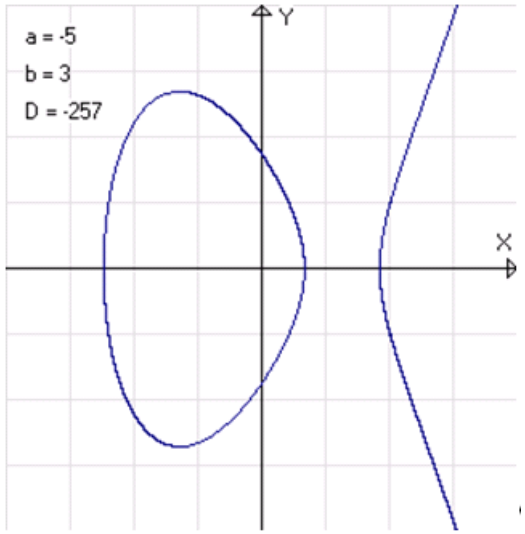
(a, b) változtatása

1. a=0, b=0
2. a=0, b=1
3. a=0, b=-1
4. a=1, b=0
5. a=-1, b=0
6. a=1, b=1
7. a=1, b=-1
8. a=-1, b=1
9. a=-1, b=-1

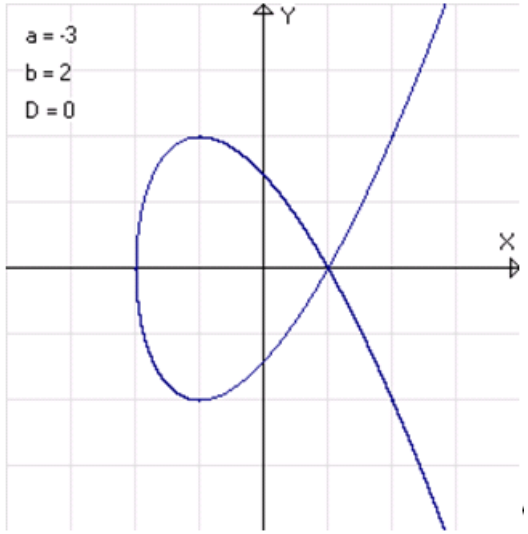
diszkrimináns

diszkrimináns: $D = 4*a^3 + 27*b^2$

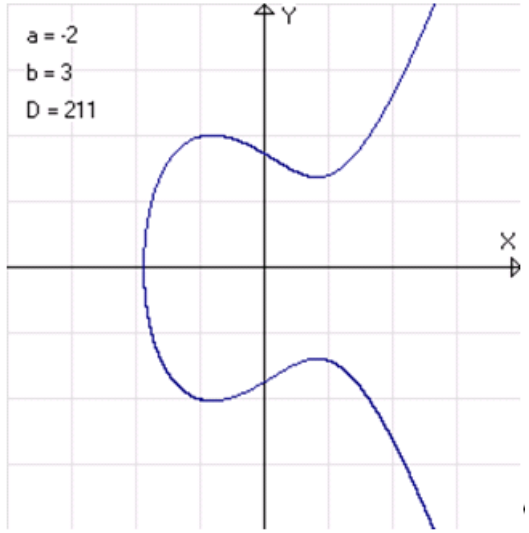
a=-5, b=3



a=-3, b=2

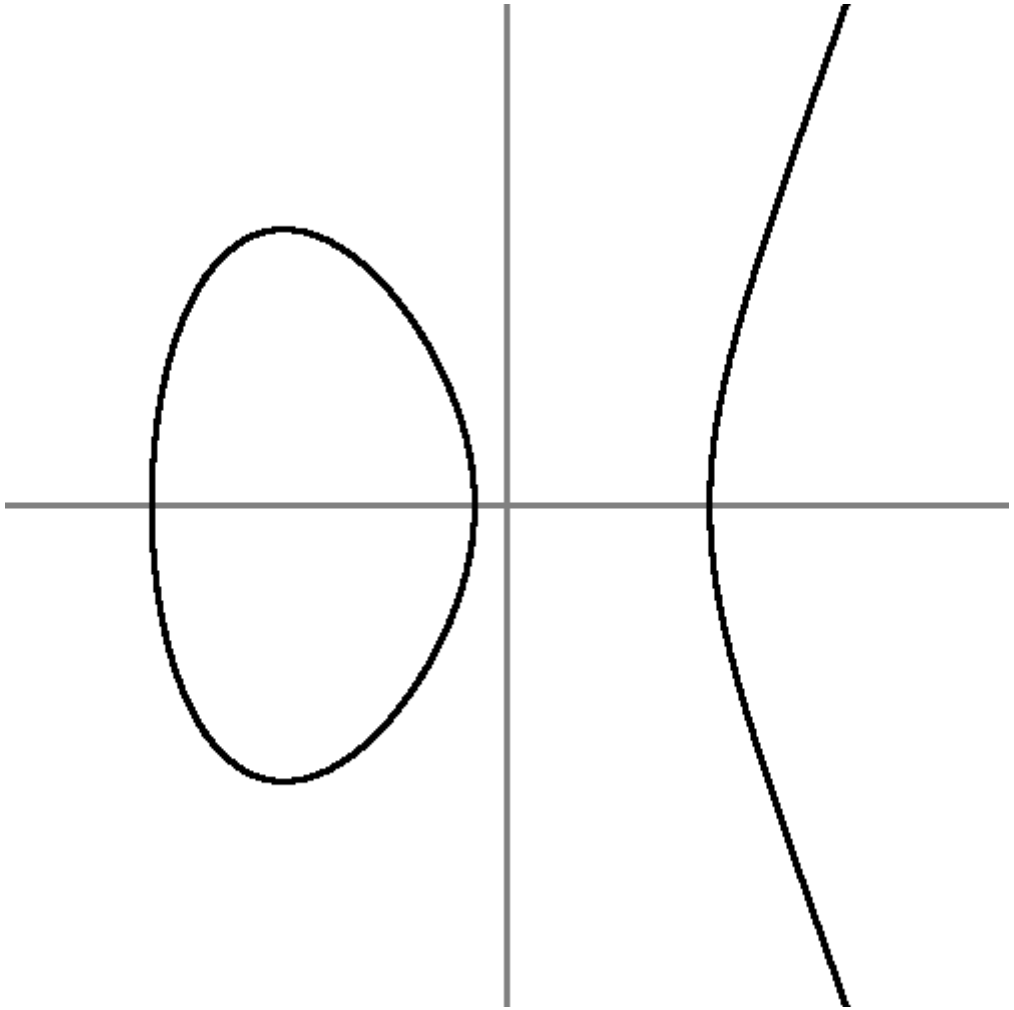


a=-2, b=3



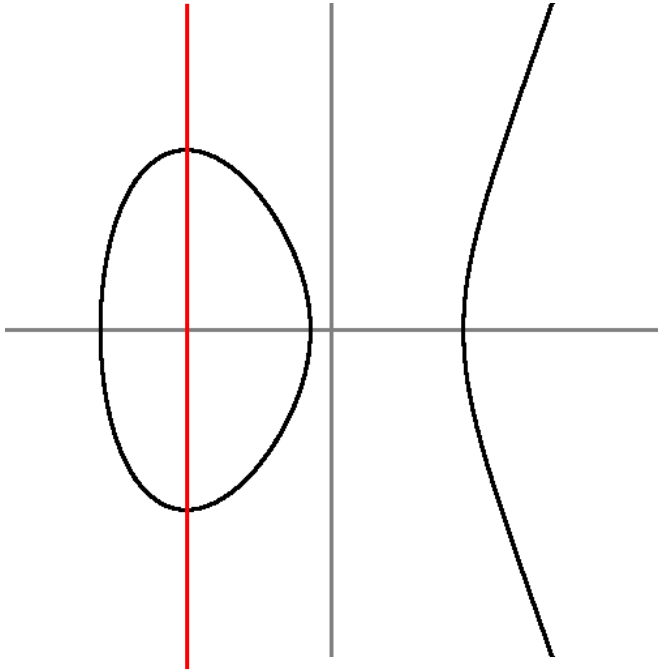
D = 0 esetén szinguláris

(a, b) változtatása



Húrok, érintők, ideális pont

Az érintő és metszéspontok számát tekintve a függőleges egyenes másképpen viselkedik



Legyen a görbe része a függőleges egyenesek ideális (végtelen távoli) pontja is

Ekkor már egyformán viselkednek (az érintő két metszéspontnak számít).

Műveletek

A görbe pontjain műveletet értelmezünk.

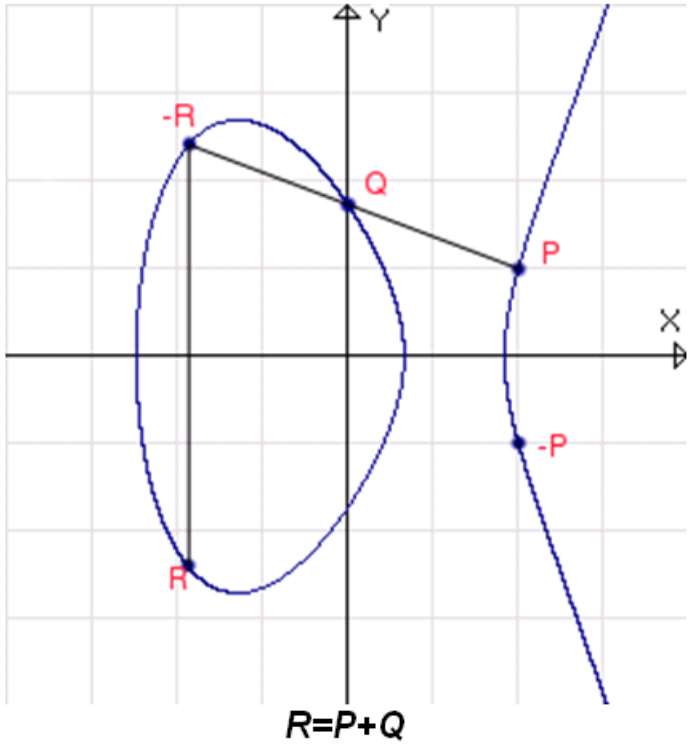
Az ideális pontról feltételezzük, hogy rajta van minden függőleges (az y-tengellyel párhuzamos) egyenesen és hogy az x-tengelyre vonatkozó tükörképe önmaga.

A görbe P és Q pontjainak P + Q összege:

a P, Q pontokon átmenő egyenes és a görbe harmadik metszéspontja -R; ennek az x-tengelyre való R tükörképe (ami szintén pontja a görbének) a P + Q összeg.

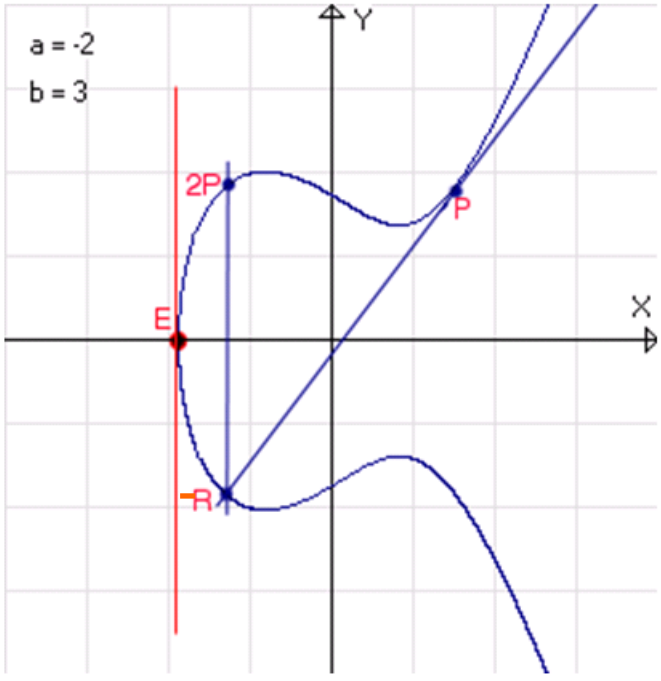
R + -R =?

az ideális pont (O)



Műveletek

Ha P = Q, akkor az összekötő egyenesükön a görbe P-beli érintőjét kell érteni.



Ha -R megegyezik a P, Q pontok valamelyikével, ekkor az egyenes -R-ben érinti a görbét.

Műveletek

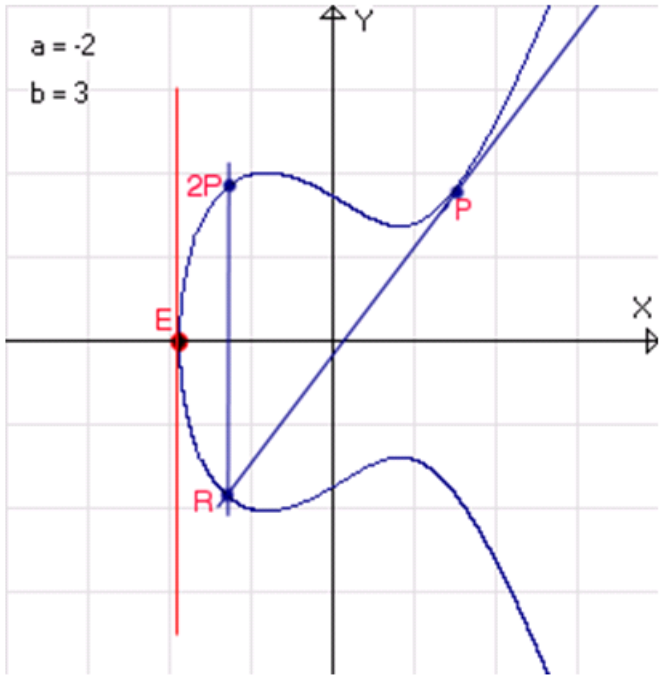
O + O = O

P + O = P

2*E = E + E = O

3*E = E + E + E = E

4*E = E + E + E + E = O



Csoport tulajdonság

Van egységelem: O

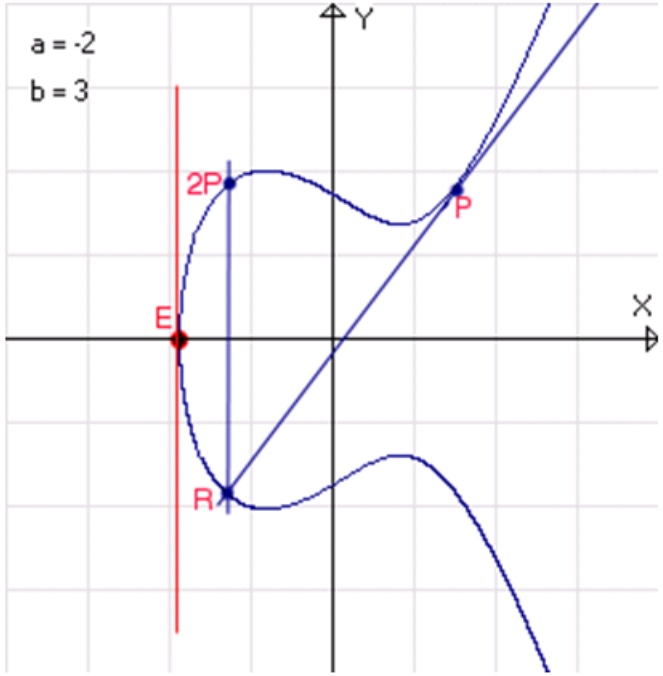
Van inverz: tükörkép

Asszociatív: (A + B) + C = A + (B + C) (nem bizonyítjuk)

Miért fontos?

gyorsan számítható az összeadás:

29*A = 2*2*2*2*A + 2*2*2*A + 2*2*A + A



Algebrai formula az összegre

Ha

P: (x_P, y_P)

Q: (x_Q, y_Q)

R: (x_R, y_R)

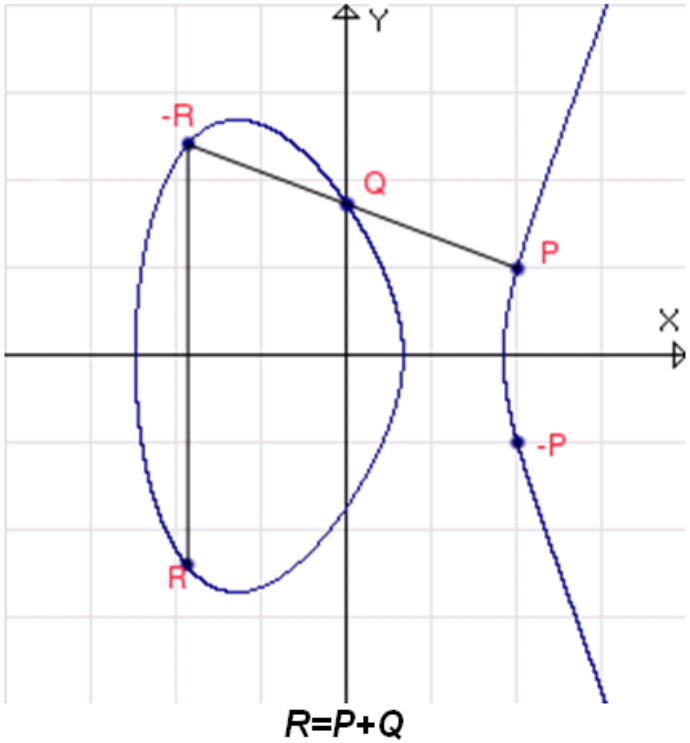
R = P + Q esetén:

$x_R = m^2 - x_P - x_Q$

$y_R = m*(x_P - x_R) - y_P$

ahol: $m = (y_P - y_Q) / (x_P - x_Q)$

az átmenő egyenes meredeksége



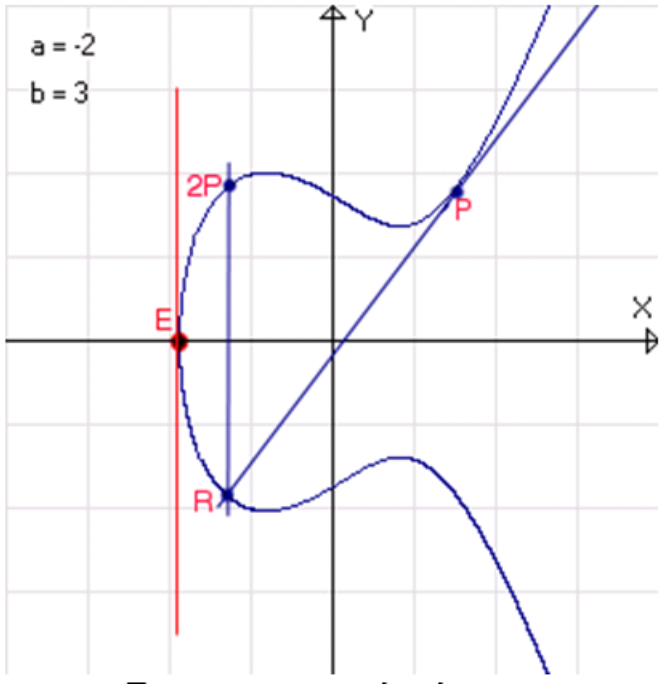
Algebrai formula az összegre

$R = 2*P$

$x_R = m^2 - 2*x_P$

$y_R = m*(x_P - x_R) - y_P$

ahol: $m = (3*x_P^2 + a) / (2*y_P)$



Elliptikus görbék mod p

Eddig:

x, y valós változók

a, b egész számok

Mostantól:

x, y mod p egészek

a, b mod p egészek

ahol p: prím

Valós számok / mod p egészek:

Mindkettő test, tehát ugyanúgy lehet számolni a görbe pontjaival

A diszkrimináns: $D = 4*a^3 + 27*b^2$ itt se lehet 0

Elliptikus görbék mod p

Miért ezzel számolunk:

- A valós számokkal való számolás lassú és pontatlan. A moduláris aritmetika gyors és pontos, csak egész számokkal dolgozik.
- A „valós” görbének végtelen sok pontja van, a modulárisnak véges.
- A moduláris aritmetikában behatárolható a számok értelmezési tartománya, mert a műveletek operandusa(i) és eredménye mindig $0 \leq x \leq p-1$ közé esik.

A "görbe" alakja

legyen

p = 11

a = 1

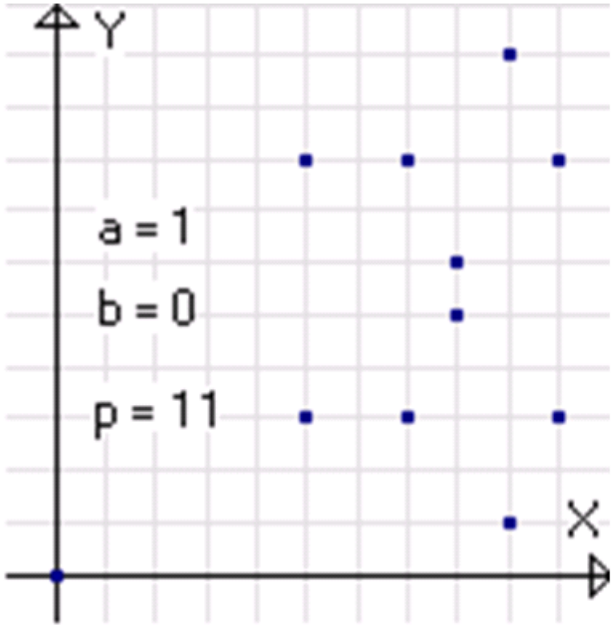
b = 0

$y^2 \equiv x^3 + x \bmod 11$

11 pont (nem mindig p-vel egyenlő!)

az x = y = 0 kivételével szimmetrikus

(minden x-hez 2 y érték)



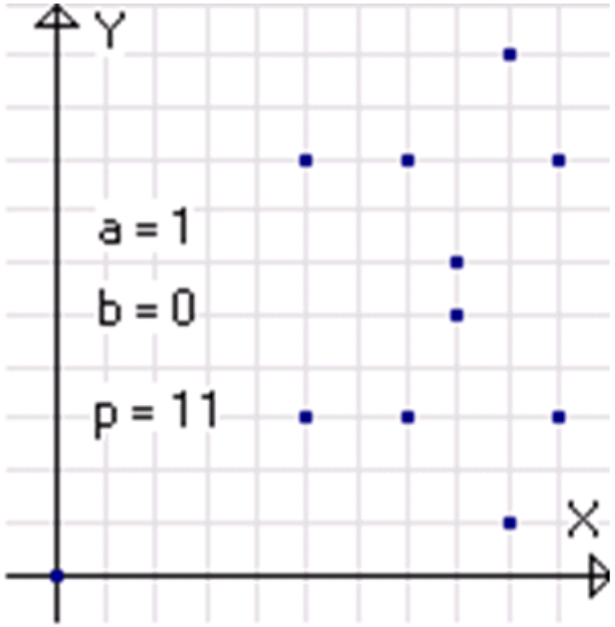
Műveletek

P: (x_P, y_P)
Q: (x_Q, y_Q)
R: (x_R, y_R)

R = P + Q esetén:

$x_R \equiv m^2 - x_P - x_Q \mod p$
$y_R \equiv m*(x_P - x_R) - y_P \mod p$

ahol: $m \equiv (y_P - y_Q) * (x_P - x_Q)^{-1} \mod p$



Műveletek

P: (x_P, y_P)

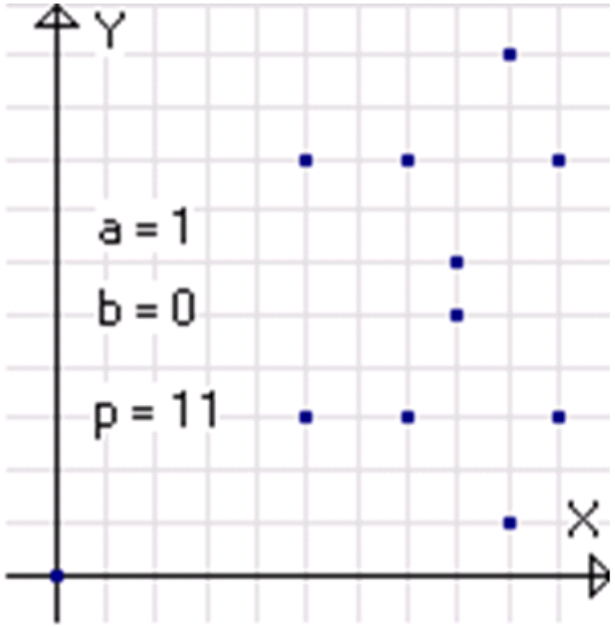
-P: $(x_P, -y_P \bmod p)$

$R = 2*P : (x_R, y_R)$

$x_R \equiv m^2 - 2*x_P \bmod p$

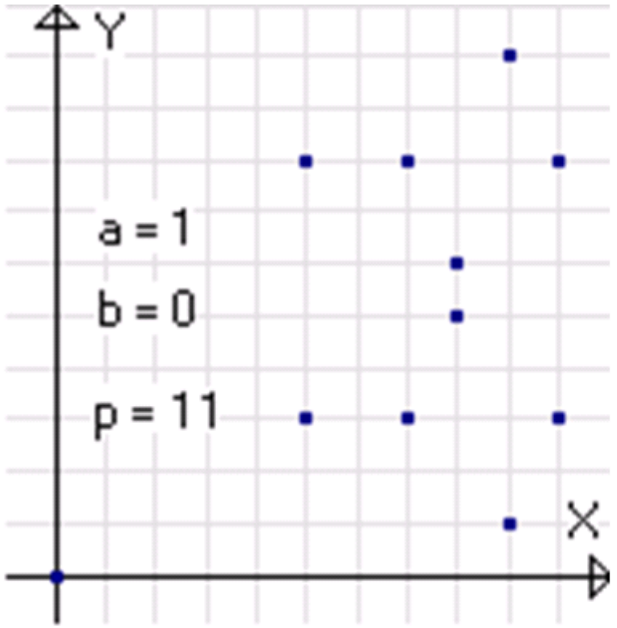
$y_R \equiv m*(x_P - x_R) - y_P \bmod p$

ahol: $m \equiv (3*x_P^2 + a) * (2*y_P)^{-1} \bmod p$



Generátor pont

p-szer összeadva előállít minden pontot



Példa

Legyen egy elliptikus görbe egyenlete:

$y^2 = x^3 + 9x + 17 \bmod 23$

Mennyi az R=(16,5) alapú diszkrét logaritmusa Q = (4,5) pontnak? (Q=nR)

Első megközelítésben n kiszámolásához addig adogassuk össze a R pontot önmagával, amíg meg nem kapjuk Q-t:

1R=(16,5) 2R=(20,20) 3R=(14,14) 4R=(19,20)

5R=(13,10) 6R=(7,3) 7R=(8,7) 8R=(12,17)

9R=(4,5)

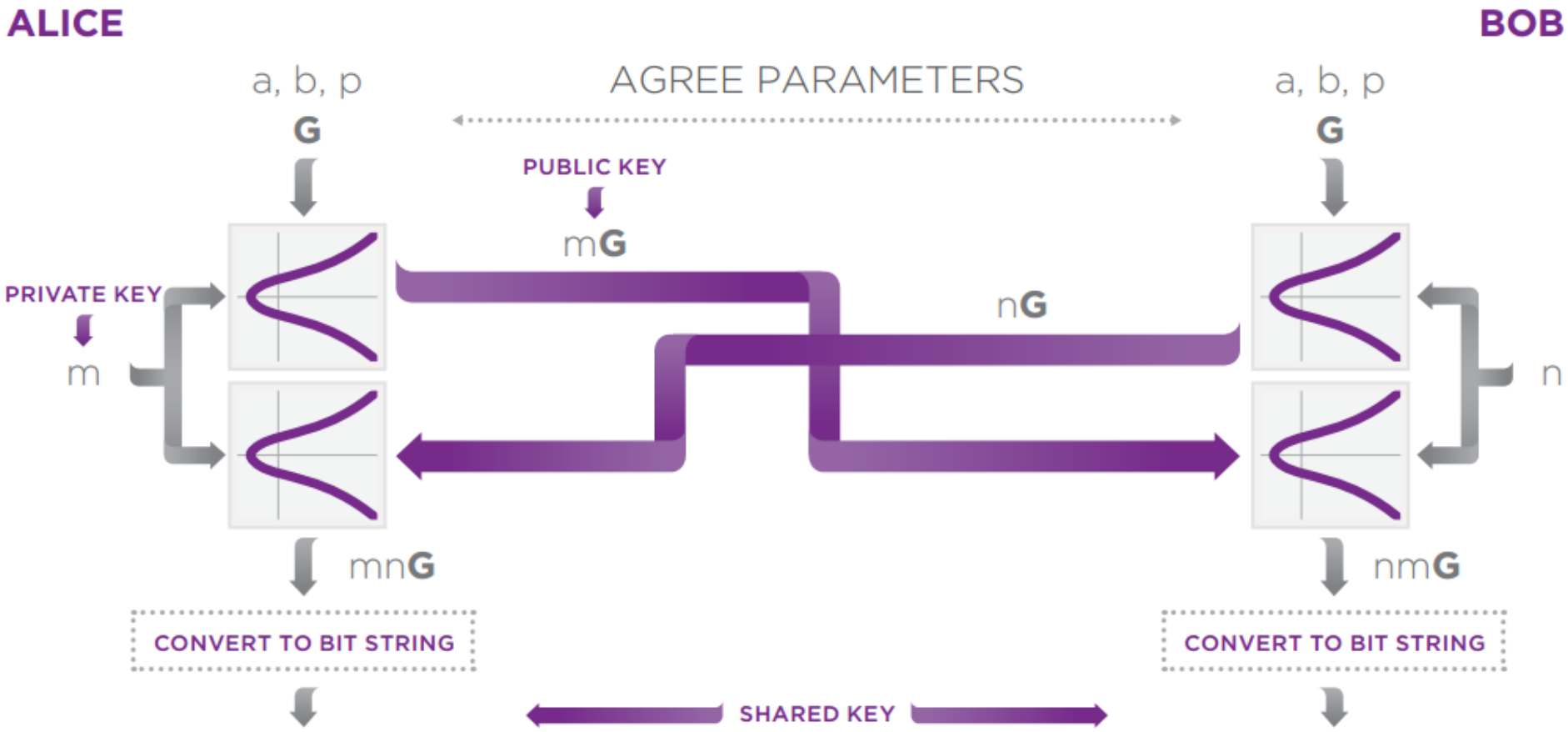
Mivel Q(4,5)=9R, ezért a Q pont R alapú diszkrét logaritmusa mod 23 felett: 9.

Miért hívjuk ezt logaritmusnak?

Lehetne osztásnak is hívni, mert a művelet összeadások sorozata.

A mod p egészek feletti diszkrét logaritmus problémához való hasonlóság miatt hívjuk itt is így.

ECDH
Elliptic-curve Diffie-Hellman



ECDSA: Elliptic-curve Digital Signature Algorithm

Alice wants to sign a message with her private key (d_A), and Bob wants to validate the signature using Alice's public key ($H_A = d_A G$).

The algorithm performed by Alice to sign the message works as follows:

1. Take a random integer k chosen from {1,…,n−1} (where n is the subgroup order).
2. Calculate the point P=kG (where G is the base point of the subgroup).
3. Calculate the number $r=x_P \bmod n$ (where x_P is the x coordinate of P).
4. If r=0, then choose another k and try again.
5. Calculate $s=k^{-1}(z+rd_A) \bmod n$ (where k^{-1} is the multiplicative inverse of k modulo n and z is the hash of the message to be signed).
6. If s=0, then choose another k and try again.

The pair (r,s) is the signature.

ECDSA: Elliptic-curve Digital Signature Algorithm

In order to verify the signature we'll need Alice's public key H_A, the hash of the message z and, obviously, the signature (r,s).

1. Calculate the integer $u_1=s^{-1}z \bmod n$
2. Calculate the integer $u_2=s^{-1}r \bmod n$
3. Calculate the point $P=u_1G+u_2H_A$

The signature is valid only if $r=x_P \bmod n$

$P=u_1G+u_2H_A=u_1G+u_2d_AG=(u_1+u_2d_A)G=(s^{-1}z+s^{-1}rd_A)G=s^{-1}(z+rd_A)G=kG$

mivel: $s=k^{-1}(z+rd_A) \bmod n$, vagyis $k=s^{-1}(z+rd_A) \bmod n$