Criptografia amb corbes el·líptiques

Llorenç Huguet Rotger
Josep Rifà Coma
Juan Gabriel Tena Ayuso

PID_00185091

UOC
Universitat Oberta de Catalunya

Índex

Introducció

La teoria de corbes el·líptiques sobre cossos finits ha estat aplicada a diverses branques com ara la teoria de nombres o la criptografia. Resulten sorprenents les relacions amb altres problemes tan diversos com la realització de tests de primalitat, la factorització de nombres o la demostració de l'últim teorema de Fermat, entre altres.

Veurem unes pinzellades d'aquestes relacions i estudiarem les corbes el·líptiques aplicades a la criptografia. En un principi podem pensar en una corba el·líptica com en el conjunt de solucions d'una equació de la forma:

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

Relacionades amb la teoria de nombres en podem destacar dues aplicacions:

- **Nombres congruents**. Un nombre racional N es diu que és congruent si existeix un triangle amb arestes racionals l'àrea del qual és N. Durant molt de temps ha esdevingut un problema sense cap algorisme per a resoldre'l i comprovar si un cert nombre N era congruent o no. Actualment, està demostrat que N és un nombre congruent si i només si la corba el·líptica $y^2 = x^3 - N^2x = x(x-N)(x+N)$ té algun punt racional diferent de $(0,0)$, $(\pm N,0)$ i el punt de l'infinit.

- **Teorema de Fermat**. El 1985 Gerhard Frey va veure que si $A^n + B^n = C^n$ era un contraexemple a l'últim teorema de Fermat, llavors la corba el·líptica $y^2 = x(x - A^n)(x + B^n)$ tenia per discriminant $-(A^nB^n(A^n + B^n))^2 = -(ABC)^{2n}$. Aquesta corba contradeia l'anomenada conjectura de Taniyama. Posteriorment, A. Wiles va provar que cap corba no podia contradir aquesta conjectura i, per tant, es va provar que no existeix cap contraexemple a l'últim Teorema de Fermat.

El problema dels nombres congruents

Va ser enunciat per primer cop pel matemàtic persa Al-Karaji (cap al segle X aC). Actualment, la solució del problema depèn de la conjectura de Birch-Swinnerton-Dyer sobre corbes el·líptiques. És un dels set problemes del mil·leni que el Clay Mathematics Institute va dotar, el 2000, amb un premi d'un milió de dòlars per a qui n'aportés la solució.

Discriminant

El discriminant d'una corba el·líptica $y^2 = x^3 + ax + b$ és $\Delta = 4a^3 + 27b^2$ i és nul si i només sí la corba té punts singulars (punts amb la derivada no definida).

En el camp de la criptografia, l'aplicació d'aquestes corbes la podem trobar en la descomposició d'un nombre en factors, en els sistemes criptogràfics i en els tests de primalitat, aquests desenvolupats per Bosma, Goldwasser-Killian, Atkin i Lenstra, entre altres.

H. W. Lenstra ha obtingut un nou mètode de factorització que és, en molts aspectes, millor que els coneguts anteriorment. La millora i eficiència d'aquest nou mètode encara no és significant en la pràctica (el temps per factoritzar continua essent el mateix); tot i això, el fet d'haver trobat un mecanisme diferent fa que el problema de factoritzar no resulti, al cap i a la fi, tan segur

com semblava. L'algorisme de factorització de corbes el·líptiques de Lenstra és anàleg al mètode clàssic ρ de Pollard.

Els avanços en els mètodes i les prestacions d'ordinadors exigeixen l'ús de nombres cada cop més grans per a poder garantir la seguretat en el mètodes criptogràfics, fet que representa un greu inconvenient a l'hora de fer la generació i distribució de les claus secretes. Aquest problema se soluciona, en part, fent servir sistemes de xifratge amb corbes el·líptiques. Aquests sistemes ofereixen un nivell de seguretat equivalent al dels mètodes tradicionals (RSA, ELGamal...) però fent servir un nombre menor de dígits. El resultat són claus més petites, característica que resulta especialment útil per a la seguretat en aplicacions basades en circuits integrats i targetes intel·ligents.

Objectius

En els materials didàctics d'aquest mòdul l'estudiant trobarà els continguts necessaris per a assolir els objectius següents:

1. Conèixer el concepte de corba en l'espai projectiu i en l'espai afí.
2. Conèixer el concepte de corba el·líptica sobre un cos finit i els paràmetres que la defineixen.
3. Conèixer l'ús de les corbes el·líptiques en criptogràfia i els principals problemes que cal tenir en compte en la seva utilització.
4. Conèixer els principals algorismes i protocols basats en corbes el·líptiques (Diffie-Helman, Shamir, ElGamal, signatura digital)).
5. Conèixer els estàndards i les aplicacions més corrents que utilitzen les corbes el·líptiques.

1. Corbes i punts racionals

1.1. Definicions prèvies

Ja hem estudiat alguns dels conceptes que farem servir en aquest mòdul. Anem a recordar-ne només alguns:

Vegeu també

En el mòdul "Cossos finits" d'aquesta assignatura trobareu de manera detallada alguns dels conceptes que també farem servir en aquest mòdul.

- La característica d'un cos K és el mínim nombre p tal que per tot $x \in K$ es compleix $\underbrace{1+1+\cdots+1}_{p} = 0$, en què 0 és l'element neutre de la suma i 1 és l'element neutre del producte en el cos K. Escriurem $char(K) = p$.

  Si per a tot $n \in \mathbb{N}$ $\underbrace{1+1+\cdots+1}_{n} \neq 0$ llavors diem que $char(K) = 0$.

  Si $K = \mathbb{F}_q$ on $q = p^m$, p primer, llavors $char(K) = p$.

  Per exemple, si $K = \mathbb{F}_q$ en què $q = p^m$, p primer, llavors $char(K) = p$. Per als cossos $\mathbb{Q}$ dels nombres racionals, $\mathbb{R}$ dels nombres reals i $\mathbb{C}$ dels nombres complexos tenim $char(\mathbb{Q}) = char(\mathbb{R}) = char(\mathbb{C}) = 0$.

- Sigui K un cos i $x \in K^* = K - \{0\}$. L'ordre de x és el mínim nombre $r > 0$ tal que $x^r = 1$.

- Sigui K un cos. La clausura algebraica de K és el cos més petit que conté K i tal que qualsevol polinomi amb coeficients en K té totes les arrels en aquest cos.

1.2. Pla projectiu

Definició 1.1 (Pla afí i pla projectiu).

Sigui K un cos. El pla afí sobre K, que anomenarem $\mathbb{A}^2$ (o $\mathbb{A}^2(K)$) és el conjunt de punts de K^2. El pla projectiu sobre K, $\mathbb{P}^2$ (o $\mathbb{P}^2(K)$), és el conjunt de punts $(x,y,z) \in K^3 - \{(0,0,0)\}$ amb la relació $\sim$ tal que:

$(x,y,z) \sim (x',y',z')$ si i només si $\exists \lambda \in K^* = K - \{0\}$ tal que $x = \lambda x'$, $y = \lambda y'$, $z = \lambda z'$.

Així definim $\mathbb{P}^2 = K^3 - \{0\}/\sim$. Cadascuna de les classes d'equivalència es diu *punt projectiu* i el denotarem per $(x : y : z)$. Per a tot $\lambda \in K^*$, direm que (x,y,z) i $(\lambda x,\lambda y,\lambda z)$ són dos representants de la mateixa classe $(x : y : z)$.

Donat un punt projectiu $(x_0 : x_1 : x_2)$ sabem que per a alguna $i = 0,1,2$ $x_i \neq 0$. Definim el conjunt obert $U_i = \{(x_0 : x_1 : x_2) | x_i \neq 0\}$

Nota

Anàlogament es defineix l'espai projectiu n-dimensional $\mathbb{P}^n = K^{n+1} - \{0\}/\sim$, les classes d'equivalència del qual s'anomenen punts y s'escriuen com $(x_0 : x_1 : \cdots : x_n)$.

Considerem $(x : y : z) \in U_3$. Hi ha un únic representant d'aquest punt de la forma $(\frac{x}{z}, \frac{y}{z}, 1)$. D'aquesta manera, atès que $z \neq 0$, podem identificar punts projectius amb punts afins:

Algorisme 1.2

$\mathbb{P}^2 \cap U_3 \longrightarrow K^2$
$(x : y : z) \longrightarrow (\frac{x}{z}, \frac{y}{z})$

Els punts projectius en què $z = 0$ formen el que s'anomena la recta de l'infinit.

Definició 1.3 (Polinomi homogeni).

Un polinomi $F(z_0, \ldots, z_n) \in K[z_0, \ldots, z_n]$ direm que és un polinomi homogeni si tots els monomis tenen el mateix grau. El denotarem per $F[z_0, \ldots, z_n]$.

Observació

El pas del pla projectiu al pla afí es podria fer amb qualsevol coordenada. En general, ho farem amb la z o amb la x_0 si escrivim els punts amb la notació $(x_0 : x_1 : \cdots : x_n)$.

Exemple 1.1

- $z_0 z_3 - {z_2}^2$ és un polinomi homogeni de grau 2.
- $z_1 - z_3$ és un polinomi homogeni de grau 1.
- ${z_2}^3$ és un polinomi homogeni de grau 3.

Donat $F[x,y,z]$, un polinomi homogeni de grau r en el pla projectiu, no té sentit *donar valors* a F. Per exemple, si $F[x,y,z] = x^3 + 3y^2z + z^3$, llavors $(1 : 1 : 1) = (2 : 2 : 2)$, però $F[1,1,1] = 5 \neq 40 = F[2,2,2]$.

Ara bé, sí que té sentit dir que $F[x,y,z]=0$ ja que si $\lambda \neq 0$, $F[\lambda x, \lambda y, \lambda z] = \lambda^r F[x,y,z]$, ja que F és un polinomi homogeni de grau r; llavors $F[\lambda x, \lambda y, \lambda z] = 0$ si i només si $F[x,y,z] = 0$.

Relació afí-projectiu

Com abans, considerem el conjunt $U_i := \{(x_0 : \cdots : x_n) \in \mathbb{P}^n | x_i \neq 0\} \subset \mathbb{P}^n$.

Relació de coordenades entre els punts considerats en l'espai afí i en l'espai projectiu.

Algorisme 1.4

$\mathbb{A}^n \longrightarrow U_i \subset \mathbb{P}^n$

$(a_1, \ldots, a_n) \longrightarrow (a_1;\ \ldots;\ a_{i-1};\ 1;\ a_{i+1};\ \ldots, a_n)$

$(\frac{z_0}{z_i}, \ldots, \frac{z_{i-1}}{z_i}, \frac{z_{i+1}}{z_i}, \ldots, \frac{z_n}{z_i}) \longleftarrow (z_0;\ \ldots;\ z_n)$

Relació de polinomis. Donat $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ en l'espai afí, tenim $F[x_0, \ldots, x_n] \in K[x_0, \ldots, x_n]$, el seu homogeneïtzat en l'espai projectiu, el qual es crea a partir de f multiplicant per x_0 a cada monomi per aconseguir un polinomi homogeni de grau $gr(f)$. Recíprocament, per a passar d'un polinomi de l'espai projectiu a l'espai afí, donarem valor 1 a la coordenada x_0 (o a la coordenada que prèviament hàgim fixat).

Exemple 1.2

- Coordenades:

  Algorisme 1.5.

  $\mathbb{A}^2 \longrightarrow U_2 \subset \mathbb{P}^2$
  $(1,2) \longrightarrow (x : y : z) = (1 : 2 : 1)$
  $(2, \frac{1}{2}) \longleftarrow (x : y : z) = (4 : 1 : 2)$

- Polinomis:

  Algorisme 1.6.

  $K[x,y] \longrightarrow K[x,y,z]$
  $x^2 + x^3 + xy \longrightarrow x^2z + x^3 + xyz$
  $x + x^2y + 1 \longleftarrow xz^2 + x^2y + z^3$

1.3. Corbes afins i projectives

Definició 1.7 (Corba afí i corba projectiva).

Siguin $f(x,y) \in K[x,y]$ i $F[x,y,z] \in K[x,y,z]$ no constants. Llavors $C_f(K) = \{(x,y) | f(x,y) = 0\}$ és una corba afí i $C_F(K) = \{(x : y : z) | F[x,y,z] = 0\}$ és una corba projectiva.

Recordeu

Un cos K' és la clausura algebraica d'un cos K si $K \subseteq K'$ i K' és el més petit amb la propietat de que qualsevol polinomi de $K'[x]$ és descomponible en factors de grau u.

Definició 1.8 (Components irreductibles d'una corba).

Sigui $f \in K[x,y]$. Podem descompondre f en producte de factors irreductibles $f = f_1^{e_1} \ldots f_s^{e_s}$. (De la mateixa manera per a $F \in K[x,y,z]$).

Amb aquesta descomposició, podem escriure la corba com a reunió dels seus components irreductibles: $C_f(K) = C_{f_1}(K) \cup \cdots \cup C_{f_s}(K)$.

Definició 1.9 (Punt singular).

Sigui $C = C_f(K) \subseteq \mathbb{A}^2$ una corba afí i $p = (a,b) \in C$. Diem que p és un **punt múltiple** o **punt singular** de C si satisfà les equacions:

$$\begin{cases} \dfrac{\partial f}{\partial x}(p) = 0 \\ \dfrac{\partial f}{\partial y}(p) = 0 \end{cases}$$

Definició 1.10 (Corba no singular).

Una corba és no singular si tots els seus punts són simples (o sigui, no singulars).

Recordeu

La notació $\dfrac{\partial f}{\partial x}(p)$ significa calcular la derivada parcial de $f(x)$ respecte a la variable x i donar valors en el punt p.

Definició 1.11 (Recta tangent).

Sigui $p = (a,b) \in C = C_f(K)$ un punt simple. Definim la **recta tangent** a C en el punt p com la recta donada per l'equació:

$$\frac{\partial f}{\partial x}(p)(x-a) + \frac{\partial f}{\partial y}(p)(y-b) = 0$$

Sigui $C = C_f(K)$, $p = (a,b)$. Podem escriure f com a suma de components homogenis:

$$f(x-a,y-b) = f_0(x-a,y-b) + \cdots + f_m(x-a,y-b),$$

en què $gr(f_i(x-a,y-b)) = i$.

Definició 1.12 (Multiplicitat en un punt).

Definim la multiplicitat de C, en el punt $p = (a,b)$, com el mínim k tal que $f_k(x-a,y-b) \neq 0$ (com a polinomi); ho denotarem per $m_p(C)$.

Observació

- $m_p(C) = 0 \iff p \notin C$.
- $m_p(C) = 1 \iff p$ és un punt simple de C.
- Si $m_p(C) = 2$, diem que p és un punt doble.

Definició 1.13 (Nodes i cúspides).

Si $m_p(C) = 2$, llavors $f_2(x-a,y-b)$ es pot descompondre en producte de 2 factors: $f_2(x-a,y-b) = \alpha\beta$.

- Si $\alpha \neq \beta$, direm que p és un node.
- Si $\alpha = \beta$, direm que p és una cúspide.

Noteu que l'anterior igualtat o desigualtat de α i β és llevat de factors constants.

Observació

Noteu que els factors α i β en la definició 1.13 no necessàriament han de tenir els coeficients en el cos K. Pot passar que els tinguin en alguna extensió quadràtica de K.
En el cas d'un node distingirem un *node racional* si α i β tenen coeficients en K, d'un *node irracional* en cas contrari.

Exemple 1.3

Suposem que $char(K) \neq 2,3$ (característica del cos). Considerem la corba $C: y^2 = x^3 + ax^2$. D'una altra manera, $f(x,y) = x^3 + ax^2 - y^2$, en què a és un valor constant $a \in K$.

La corba C té punts singulars? I, en cas afirmatiu, quina multiplicitat tenen?

- Per a la primera qüestió, tal com hem dit a la definició 1.9, calcularem les derivades i, a més a més, el valor de la funció $f(x,y)$ ha de ser zero en tots els punts de la corba:

$$\begin{cases} \dfrac{\partial f}{\partial x} = 3x^2 + 2ax = 0 \\ \dfrac{\partial f}{\partial y} = -2y = 0 \\ f = x^3 + ax^2 - y^2 = 0 \end{cases}$$

  Resolent aquest sistema trobem $y = 0$ i $x(3x + 2a) = 0$, $x^3 + ax^2 - y^2 = 0$. Finalment, $y = 0, x = 0$. Per tant, (0,0) és un punt singular.

- Per a estudiar la multiplicitat del punt singular (0,0) utilitzarem la definició 1.12, però abans descompondrem $f(x,y)$ en suma de funcions homogènies $f_0(x-0,y-0)$, $f_1(x-0,y-0)$, $f_2(x-0,y-0)$, $f_3(x-0,y-0)$, de graus 0,1,2,3, respectivament.

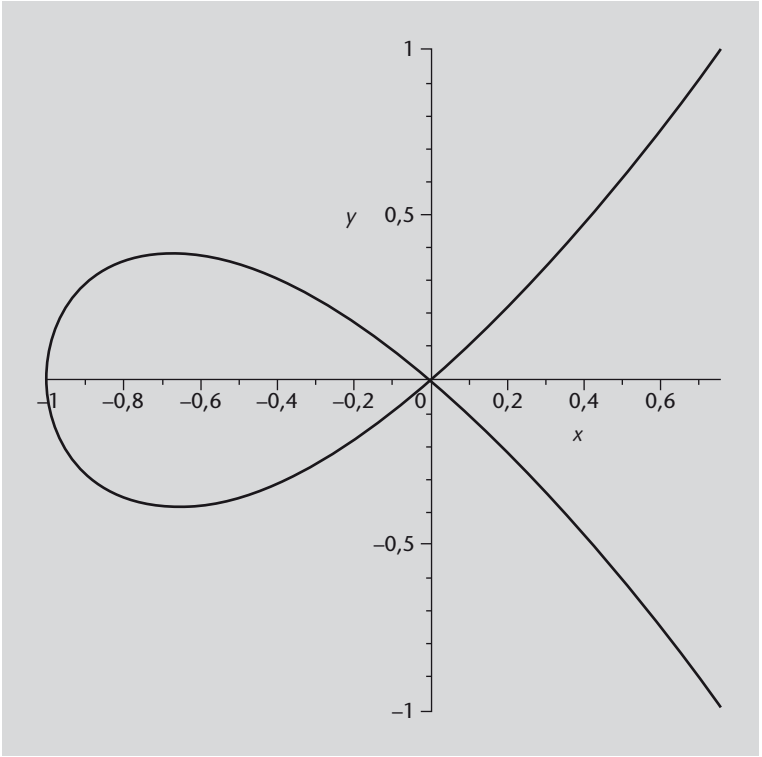
  Veiem que $f(x-0,y-0) = f(x,y) = 0 + 0 + (ax^2 - y^2) + x^3$.

  Per tant, $f_0(x,y) = f_1(x,y) = 0$, $f_2(x,y) = ax^2 - y^2 = (\sqrt{a}x + y)(\sqrt{a}x - y)$, $f_3(x,y) = x^3$.

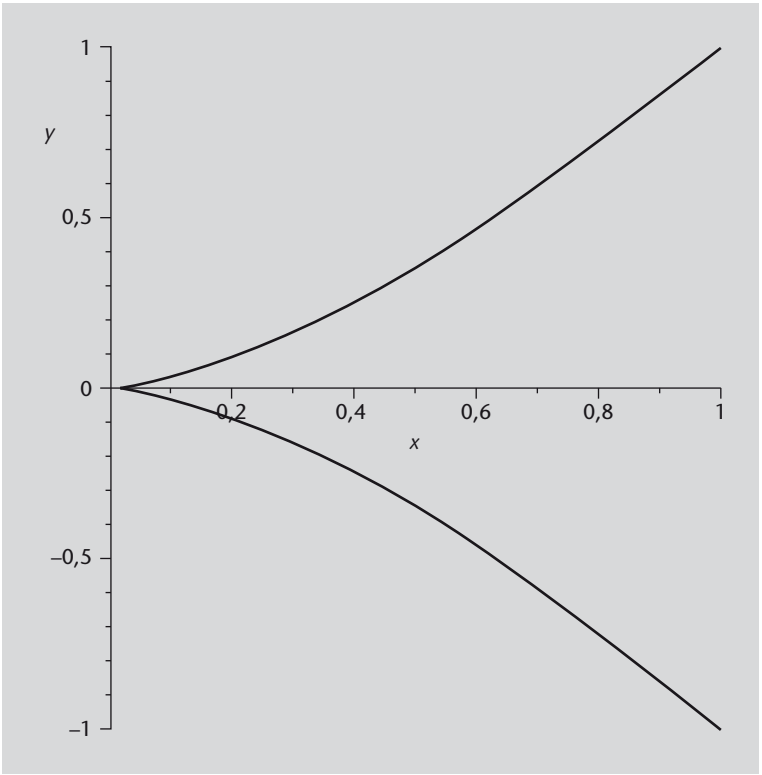
  Així, segons la definició 1.12, veiem que $m_p(C) = 2$ i, per tant, $p = (0,0)$ és un punt doble. Ara, segons la definició 1.13 veiem que per a $a = 0$ el punt $p = (0,0)$ és una cúspide i per a tots els valors $a \neq 0$, el punt $p = (0,0)$ és un node. Depenent de si $\sqrt{a} \in K$ el node serà racional o irracional.

  Les figures següents corresponen a la corba $y^2 = x^3 + ax^2$ per a $a = 1$ i $a = 0$, respectivament.

Node racional en el punt $(0,0)$ de la corba $y^2 = x^3 + x^2$



Cúspide en el punt $(0,0)$ de la corba $y^2 = x^3$



Una pregunta que potser ens hem fet a aquestes alçades és: per què ens interessarà mirar les corbes al pla projectiu?

Suposem la mateixa corba que en l'exemple anterior per al cas $a = 2$. La podem veure com una corba projectiva donada per un polinomi homogeni, $F[x,y,z] =$

$x^3 + 2x^2z - y^2z = 0$. Podem passar la corba projectiva al pla afí donant el valor $z = 1$; així, obtenim la corba $f(x,y) = x^3 + 2x^2 - y^2 = 0$, que és la mateixa equació que ja havíem vist en l'exemple anterior i de la qual ja sabem que el punt $(x = 0, y = 0)$ és un punt singular. Per a evitar aquest punt singular podem passar a l'afí fent servir una altra coordenada; per exemple, $y = 1$, i obtenim una "nova corba": $g(x,z) = x^3 + 2x^2z - z = 0$ en la qual el punt $(x = 0, z = 0)$ pertany a la corba i no és singular.

Observació

També, l'ús de les coordenades projectives permet fer càlculs en corbes el·líptiques sobre cossos finits sense necessitat de fer operacions de dividir en el cos. Això és important, ja que les operacions de dividir són computacionalment costoses.

Aquestes dues corbes afins (les donades per f i g) són corbes associades a la mateixa corba projectiva. Així, encara que una de les corbes afins contingui un punt singular podríem trobar una altra corba afí associada a la mateixa corba projectiva que no en tingui cap.

Teorema 1.14 (Teorema de Bezout).

Siguin $C = \{(x : y : z) \in \mathbb{P}^2 | F[x,y,z] = 0\}$ i $D = \{(x : y : z) \in \mathbb{P}^2 | G[x,y,z] = 0\}$ dues corbes projectives de graus m i n, respectivament ($m = gr(F)$, $n = gr(G)$). Si C i D no tenen components irreductibles en comú, llavors C i D tenen $\boldsymbol{mn}$ punts en comú comptant multiplicitats.

Exemple 1.4

- Dues rectes diferents (corbes projectives de grau 1) es tallen sempre en un punt. Si ho mirem al pla afí, sabem que dues rectes diferents o bé es tallen en un punt o bé són paral·leles i, en aquest cas, es tallen en el punt de l'infinit al pla projectiu.
- Dues còniques diferents (corbes projectives de grau 2) es tallen exactament en 4 punts.

Corol·lari 1.15.

Una cònica definida por un polinomi irreductible F de grau 2 té punts singulars.

Demostració: Una cònica és una corba projectiva de grau 2. Ara, suposem que tenim una cònica amb un punt singular. Prenem un altre punt de la cònica i considerem la recta que passa per aquests dos punts; aquesta recta és una corba projectiva de grau 1.

La nostra cònica és una corba projectiva de grau 2; per tant, pel teorema de Bezout, la recta i la cònica tenen 2 punts en comú, però com el punt singular té multiplicitat més gran o igual que 2, el nombre de punts en comú serà de 3 o més (això contradiu el teorema de Bezout). ∎

1.4. Punts racionals

El cos dels nombres racionals el representarem per $\mathbb{Q}$.

Definició 1.16 (Successió fonamental).

Una successió de nombres a_n, $a_i \in \mathbb{Q}$ diem que és una successió fonamental si $\forall \epsilon > 0\ \exists n_\epsilon \in \mathbb{N}$ tal que $|a_n - a_m| < \epsilon\ \forall m,n > n_\epsilon$, en què estem fent servir la norma euclidiana.

Definició 1.17 (Cos *p*-àdic).

Sigui p primer. Tot nombre $a \in \mathbb{Q}$ es pot escriure de la manera $a = p^r \frac{m}{n}$, en què $mcd(m,p) = 1$ i $mcd(n,p) = 1$. Llavors, definim la **norma *p*-àdica** de a com: $|a|_p = \frac{1}{p^r}$.

Definim el cos p-àdic $\mathbb{Q}_p$ com el conjunt de totes les successions fonamentals amb aquesta norma, mòdul una certa relació d'equivalència.

Observació

El cos $\mathbb{R}$ dels nombres reals es pot definir com el conjunt de totes les successions fonamentals, mòdul una certa relació d'equivalència.

Definició 1.18 (Punts racionals d'una corba).

Sigui K un cos, i $C = C_f(K)$ una corba. Diem que $p = (p_1,p_2)$ és un punt racional de la corba si $f(p) = 0$ i si $p \in K^2$.

Teorema 1.19 (Teorema de Legendre).

Una cònica (amb coeficients en $\mathbb{Q}$) té un punt racional si i només si té un punt zero en $\mathbb{R}$ i en tots els $\mathbb{Q}_p$

Observació

El teorema 1.19 és fals per a corbes de grau més gran que 2. Per a corbes de grau 2, és cert per a qualsevol nombre de variables, o sigui, per a corbes planes o no, però definides per una forma quadràtica (Hasse-Minkowski).

1.4.1. Punts racionals d'una corba de grau 1

Una corba de grau 1 és una recta. L'equació d'una recta es pot escriure com $Ax + By + C = 0$.

Ara considerarem una parametrització de la recta, o sigui, expressarem els punts de la recta en funció d'un paràmetre. Una manera de fer-ho seria:

Algorisme 1.20.

$t \longrightarrow (t, \frac{C-At}{B})$

Ara, donant valors a t obtenim punts racionals de la nostra recta. Per tant, si el cos base és infinit, com $\mathbb{Q}$, $\mathbb{R}$, ..., les rectes tenen infinits punts racionals.

1.4.2. Punts racionals d'una corba de grau 2

Una corba de grau 2 és una cònica. L'equació d'una cònica, després de canvis de coordenades apropiats, es pot deixar escrita d'una de les maneres següents:

1) $x^2 + y^2 = c < 0 \Longrightarrow \emptyset$.

2) $x^2 + y^2 = 0 \Longrightarrow$ un punt.

3) $x^2 = 0 \Longrightarrow$ recta doble.

4) $xy = 0 \Longrightarrow$ dues rectes.

5) $y = x^2 \Longrightarrow$ paràbola.

6) $xy = 1 \Longrightarrow$ hipèrbola.

7) $x^2 + y^2 = c > 0 \Longrightarrow$ el·lipse.

Els casos 2, 3 i 4 són corbes degenerades o no irreductibles i, per tant, no els tractarem.

Els casos 5, 6 i 7 són projectivament equivalents; és a dir, en el pla projectiu, podem passar d'una a l'altra via un canvi de variables.

Exemple 1.5. Càlcul de punts racionals en una cònica

Considerem, com a exemple, la cònica afí $x^2 + y^2 = 1$ i en calcularem els punts racionals. Primer de tot, ja veiem fàcilment que el punt $p = (0,1)$ és un punt racional de la corba. Ara, anem a veure si podem calcular tots els altres.

Els punts de la cònica els podem pensar com a interseccions de la cònica amb rectes que passen per aquest punt fixat $p = (0,1)$.

Considerem la recta $r : Ax + By + C = 0$, una de les infinites rectes del feix de rectes que passen pel punt p. Com que el punt $p = (0,1)$ pertany a la recta, ja veiem que $B + C = 0$, o sigui $C = -B$.

Ara podem escriure l'equació de la recta r com $Ax + By - B = 0$ o, també, $\frac{A}{B}x + y - 1 = 0$.

Fem $A' = \dfrac{A}{B}$ i, llavors la recta és $A'x + y - 1 = 0$.

Així, el feix de rectes que passen per $p = (0,1)$ és $\{A'x + y - 1 = 0\}_{A'}$ (o sigui, variant els valor del paràmetre A', trobem totes les rectes del feix).

Fem ara intersecció de les rectes del feix amb la cònica. O sigui, resolem el sistema d'equacions:

$$\begin{cases} A'x + y - 1 = 0 \\ x^2 + y^2 = 1 \end{cases}$$

Fent operacions, $y = 1 - A'x$

$x^2+(1-A'x)^2 = 1 \rightarrow\ x^2+1-2A'x+A'^2x^2 = 1\ \rightarrow x^2(1+A'^2)-2A'x = 0\ \rightarrow x(x(1+A'^2)-2A') = 0.$
Llavors

$$\begin{cases} x = 0 \rightarrow \text{ punt } (0,1) \\ x(1+A'^2) - 2A' = 0,\ x = \dfrac{2A'}{1+A'^2} \rightarrow \text{ punt } \left(\dfrac{2A'}{1+A'^2}, \dfrac{1-A'^2}{1+A'^2}\right) \end{cases}$$

Així, escollint com a punt fix $p = (0,1)$, parametritzem la còrnica inicial de la manera següent:

Algorisme 1.21.

$t \longrightarrow \left(\frac{2t}{1+t^2}, \frac{1-t^2}{1+t^2}\right)$

Ara, si t és racional, el punt de la corba $\left(\dfrac{2t}{1+t^2}, \dfrac{1-t^2}{1+t^2}\right)$ també ho és; per tant, la corba donada per $f(x,y) = x^2 + y^2 - 1$ té infinits punts racionals.

1.4.3. Punts racionals d'una corba de grau 3

Una corba de grau 3 és una cúbica.

Observació

Hem demostrat que si existeix un punt racional, llavors n'existeixen infinits. Amb això no podem dir que tota còrnica té infinits punts racionals perquè hi ha corbes en què no podem trobar cap punt racional; per exemple, $x^2 + y^2 = -1$ sobre $\mathbb{Q}$.

Proposició 1.22.

Si $F[x,y,z] = 0$ és una corba projectiva irreductible de grau 3 amb un punt singular, llavors aquest és únic. A més, aquest únic punt singular té multiplicitat 2.

Demostració: Suposem que tenim una cúbica amb dos punts singulars. Considerem la recta que passa per aquests dos punts. La corba i la recta tenen, com a mínim, 4 punts en comú comptant multiplicitats; però, pel Teorema de Bezout, només en podien tenir 3. Llavors, la cúbica només pot tenir un punt singular, com a màxim.

Suposem ara que aquest punt singular té multiplicitat més gran que dos. Llavors una recta que passi per aquest punt i un altre punt qualsevol de la cúbica té, com a mínim, 4 punts en comú amb la corba i això, pel Teorema de Bezout, no pot passar. ∎

Proposició 1.23.

Un punt singular és sempre racional.

Resumint, una corba de grau 3 o no té punts singulars o té exactament un punt singular que és un node o una cúspide i, a més, és racional.

Si tenim una corba de grau 3 no singular, sabem que una recta que passa per dos punts de la cúbica talla en un tercer punt. A més, si dos d'aquests punt són racionals, llavors el tercer també ho és. (Diofant, segle III AC).

Teorema 1.24 (Teorema de la base finita de Mordell (1923)).

Si C és una cúbica no singular sobre $\mathbb{Q}$, existeix un conjunt finit de punts racionals sobre C tal que tots els altres punts de la corba es poden trobar fent construccions de tangents i secants a partir d'aquests.

1.4.4. Punts racionals d'una corba de grau 4

Teorema 1.25 (Teorema de Faltings (1983)).

Les corbes de grau ≥ 4 tenen un nombre finit de punts racionals.

Resumint el que hem dit fins ara sobre els punts racionals en $\mathbb{Q}$:

- **Corba de grau 1**: hi ha infinits punts racionals.
- **Corba de grau 2**: si hi ha un punt racional, n'hi ha infinits. Hilbert i Hurwitz (1890) ho demostren per les corbes de gènere zero (les de grau 1, 2 ho són).
- **Corba de grau 3**: hi ha un conjunt infinit de punts racionals, finitament generat. Mordell, 1923.
- **Corba de grau 4**: hi ha un nombre finit de punts racionals. Conjecturat per Mordell, demostrat per Faltings, 1983.

2. Geometria de les corbes el·líptiques

Començarem donant una definició més explícita de corba el·líptica.

Definició 2.1 (Corba el·líptica).

Una **corba el·líptica** és una corba plana no singular de grau 3 juntament amb un punt fixat, que anomenarem *punt base*.

2.1. Equació de Weierstrass

Qualsevol corba el·líptica pot ser escrita en $\mathbb{P}^2$ com una equació cúbica de la manera següent:

$$Ax^3 + Bx^2y + Cx^2z + Dxyz + Ey^2z + Fy^2x + Gy^3 + Hz^3 + Iz^2x + Jz^2y = 0$$

Prenent un sistema de referència adequat, totes les corbes es poden expressar segons l'**equació de Weierstrass**:

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \quad (1)$$

amb $a_1, \ldots, a_6 \in K$

Suposem que tenim una corba de grau 3 en el pla afí:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (2)$$

Si $char(K) \neq 2$, llavors

$$(y + \frac{1}{2}a_1x + \frac{1}{2}a_3)^2 = y^2 + a_1xy + a_3y + \frac{1}{4}a_1x^2 + \frac{1}{4}a_3^2 + \frac{1}{2}a_1a_3x$$

$$(y + \frac{1}{2}a_1x + \frac{1}{2}a_3)^2 - (\frac{1}{4}a_1x^2 + \frac{1}{4}a_3^2 + \frac{1}{2}a_1a_3x) = x^3 + a_2x^2 + a_4x + a_6$$

Podem simplificar més l'equació (1) fent el canvi

$$y := y + \frac{1}{2}a_1 x + \frac{1}{2}a_3$$

i ens queda:

$$y^2 = x^3 + (a_2 + \frac{1}{4}a_1)x^2 + (a_4 + \frac{1}{2}a_1 a_3)x + (a_6 + \frac{1}{4}a_3^2)$$

Per tant, si $char(K) \neq 2$, l'equació de Weierstrass es pot escriure:

$$y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4} \tag{3}$$

Suposem ara que la característica del cos és diferent de 3,

$$(x + \frac{b_2}{3 \cdot 4})^3 = x^3 + \frac{b_2}{4}x^2 + \frac{b_2^2}{4^2 \cdot 3}x + \frac{b_2^3}{(3 \cdot 4)^3}$$

$$y^2 = (x + \frac{b_2}{3 \cdot 4})^3 - 3x\frac{b_2^2}{(3 \cdot 4)^2} - (\frac{b_2}{3 \cdot 4})^3 + 2b_4 x + b_6$$

Ara fem el canvi

$$x := x + \frac{b_2}{3 \cdot 4}$$

i ens queda l'equació:

$$y^2 = x^3 + 27c_4 x - 54c_6$$

Hem simplificat més encara l'equació ja que hem eliminat el coeficient de x^2.
Si $char(K) \neq 2,3$, l'equació (1) es pot escriure de manera més simple com:

$$y^2 = x^3 + Ax + B \tag{4}$$

De manera similar, quan tenim un cos de característica 2 o 3, també es pot simplificar l'equació 1.

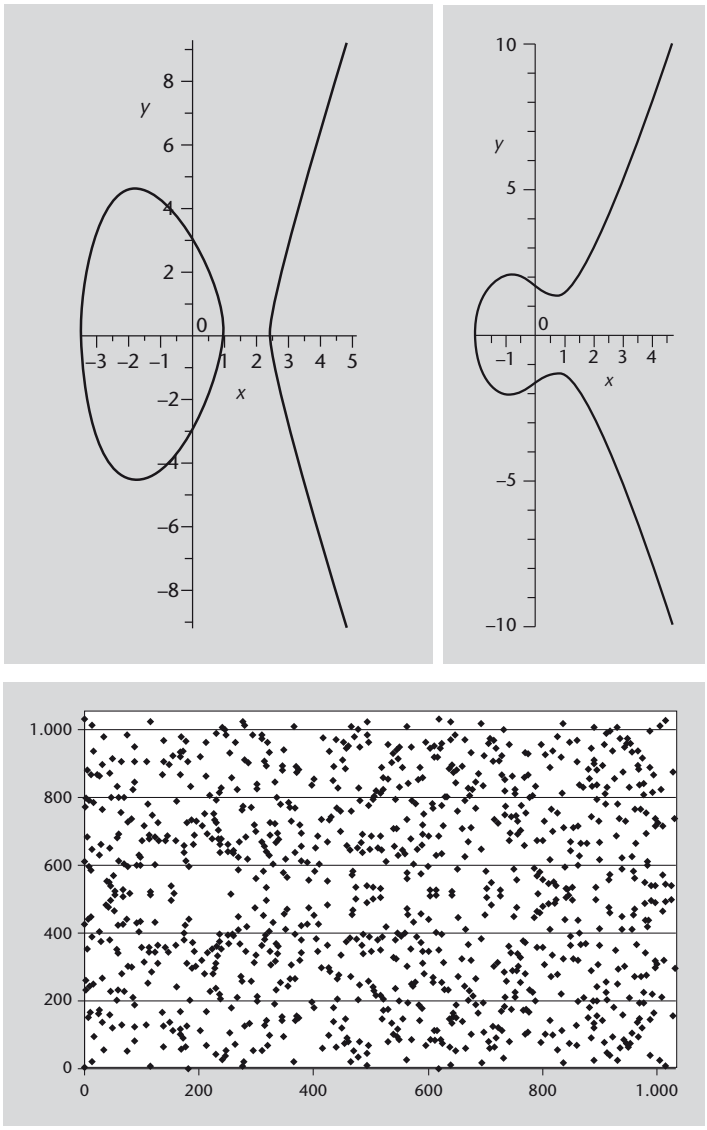
Si $char(K) = 2$, llavors tenim:

$$\begin{aligned} &y^2 + xy = x^3 + b_2 x^2 + b_6, \text{ si } \Delta = b_6 \neq 0 \\ &y^2 + b_3 y = x^3 + b_4 x + b_6, \text{ si } \Delta = b_3^4 \neq 0 \end{aligned} \tag{5}$$

Si *char*(*K*) = 3, llavors tenim:

$$y^2 = x^3 + a_2x^2 + a_6 \qquad (6)$$

Les dues primeres corbes $y^2 = x^3 - 10x + 9$ i $y^2 = x^3 - 2x + 3$ sobre els nombres reals. L'última, $y^2 = x^3 + 10x + 9$ sobre $\mathbb{F}_{1031}$.



Proposició 2.2.

Sigui *K* cos amb *char*(*K*) $\neq$ 2,3, sigui *C* una corba sobre *K*, és a dir, *C* : $y^2 = x^3 + Ax + B$. Sigui $\Delta = 4A^3 + 27B^2$ el discriminant de la corba. Llavors:

1) $\Delta \neq 0 \Leftrightarrow$ *C* no té punts singulars.

2) $\Delta = 0$ i $A = 0 \Longrightarrow$ *C* té una cúspide.

3) $\Delta = 0$ i $A \neq 0 \Longrightarrow$ *C* té un node.

Demostració: Sigui $C : y^2 = x^3 + Ax + B$, $f(x,y) = x^3 + Ax + B - y^2$. C té punts singulars si i només si $\frac{\partial f}{\partial x}(p) = 0$, $\frac{\partial f}{\partial y}(p) = 0$.

$$\begin{cases} \frac{\partial f}{\partial x} = 3x^2 + A \\ \\ \frac{\partial f}{\partial y} = -2y \end{cases}$$

Punts singulars:

$$\begin{cases} \frac{\partial f}{\partial x} = 0 \iff x = \pm\sqrt{\frac{-A}{3}}, \\ \\ \frac{\partial f}{\partial y} = 0 \iff y = 0 \end{cases}$$

$$x^3 + Ax + B - y^2 = 0 \to \frac{-A}{3}x + Ax + B = 0 \to x = \frac{3B}{2A}$$

llavors

$$x^2 = \frac{9B^2}{4A^2} = \frac{-A}{3} \to 4A^3 + 27B^2 = 0$$

1) C no té punts singulars si i només si $4A^3 + 27B^2 \neq 0$.

2) Suposem que $4A^3 + 27B^2 = 0$ i $A = 0$, llavors $B = 0$ i $f(x,y) = x^3 - y^2$. El punt (0,0) és un punt singular, a més a més, segons la definició 1.13, podem dir que és una cúspide.

3) Tenim $4A^3 + 27B^2 = 0$ i $A \neq 0$. El punt $\left(\frac{3B}{2A},0\right)$ és un punt singular. $f(x,y) = x^3 + Ax + B - y^2$ es pot escriure com $f(x,y) = \left(x - \frac{3B}{2A}\right)^3 + \frac{9B}{2A}\left(x - \frac{3B}{2A}\right)^2 - (y-0)^2$, llavors $f_2\left(x - \frac{3B}{2A}, y - 0\right) = \frac{9B}{2A}x^2 - y^2 = \left(\sqrt{\frac{9B}{2A}}x - y\right)\left(\sqrt{\frac{9B}{2A}}x + y\right)$. Així, el punt $\left(\frac{3B}{2A},0\right)$ és un punt doble i, segons la definició 1.13, sabem que és un node.

∎

2.2. La llei de grup d'una corba el·líptica

Sigui $C \in \mathbb{P}^2$ una corba el·líptica donada per l'equació de Weierstrass. Anomenem O al punt base de la corba. Sigui $L \in \mathbb{P}^2$ una recta. Ara, com que l'equació té grau 3, L i C s'intersequen, exactament, en 3 punts, direm $L \cap C = \{P,Q,R\}$. Observem, però, que si L és tangent a C, llavors P,Q,R no seran tres punts diferents; n'hi haurà un de doble (el punt de tangència). El fet que $L \cap C$, comptant multiplicitats, doni tres punts, es dedueix del teorema de Bezout (teorema 1.14).

2.2.1. Llei de grup de C

Siguin $P,Q \in C$ i L la recta que passa per aquests dos punts (la tangent en el cas $P = Q$), i R el tercer punt d'intersecció de L i C. Sigui L' la recta que uneix R i O. Llavors $L' \cap C = \{R,O,P+Q\}$; és a dir, $P+Q$ és el tercer punt d'intersecció de la corba i la recta que passa per R i O.

Definim una operació sobre els punts de la corba el·líptica de manera que $P+Q$ serà el punt calculat a partir de P i Q tal com acabem de descriure en el paràgraf anterior. L'operació que hem definit dóna a C estructura de grup abelià.

Proposició 2.3.

La llei de grup de C té les propietats següents:

- Si $L \cap C = \{P,Q,R\}$ (no necessàriament diferents), llavors $(P+Q)+R = O$.
- $P + O = P$, $\forall P \in C$.
- $P + Q = Q + P$, $\forall P,Q \in C$.
- $\forall P \in C\ \exists(-P) \in C$ tal que $P + (-P) = O$.
- $(P + Q) + R = P + (Q + R)$ $\forall P,Q,R \in C$

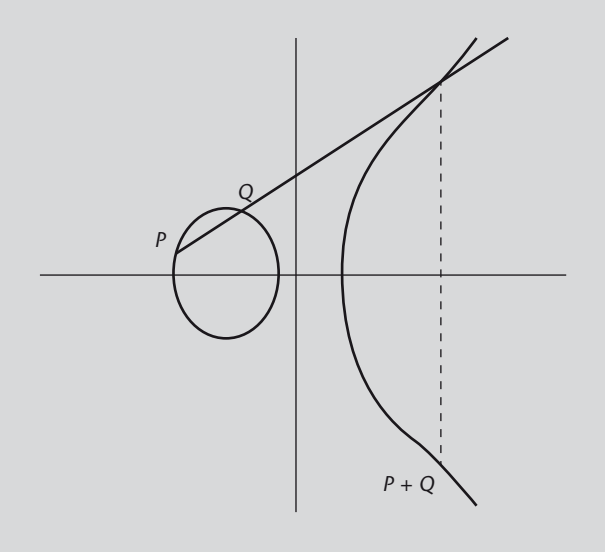
Per facilitar els càlculs, prenem com a punt base un punt de l'infinit, com per exemple $O = (0 : 1 : 0)$. Donats dos punts de la corba, P i Q, calculem la suma $P+Q = R$ (a la figura següent, R és el tercer punt on la recta que passa per P i Q talla la corba). Si ara volem calcular la intersecció de la recta que passa per R i O amb la corba el·líptica, només hem de trobar el simètric de R respecte l'eix de les x.

Notació

Per a $n \in \mathbb{Z}$, $P \in C$ escriurem:

- $nP = P + \cdots + P$ n vegades, si $n > 0$.
- $nP = (-P) + \cdots + (-P)$ $|n|$ vegades, si $n < 0$
- $0P = O$

Suma de dos punts



Finalment, veurem un algorisme, anàleg a l'algorisme de multiplicar i elevar, per a calcular nP amb el mínim nombre possible d'operacions.

Primer de tot calcularem l'expansió binària de n: $n \leftrightarrow b_1 b_2 \dots b_r$, $b_i \in \{0,1\}$ (b_r és el bit menys significatiu, o sigui, les unitats).

Algorisme 2.4.

```
function Suma(n)
    begin
        for j ← 1 to n
            if b_j = 1 then parcial ← parcial + P endif
            if j < r then parcial ← 2·parcial endif
        endfor
        return(parcial)
end
```

Exemple 2.1

Calcular $19P$.

El nombre 19 escrit en binari és 10011. Llavors, seguint l'algorisme anterior $19P = 2\Big(2\Big(2\big(2(0+P)\big)\Big)+P\Big)+P$.

Exemple 2.2

Sigui $K = \mathbb{F}_{23}$, $C : y^2 = x^3 + x + 1$, $P_1 = (3,10)$, $P_2 = (9,7)$.

- Calculeu $P_1 + P_2$.
- Calculeu $10 \cdot P_1$

Començarem calculant la recta que passa per P_1 i P_2, que anomenarem $L : y = \alpha x + \beta$

$$\alpha = \frac{7-10}{9-3} = -\frac{1}{2} = -12 = 11$$

$$10 = 11 \cdot 3 + \beta \Longrightarrow \beta = 10 - 10 = 0$$

Per tant $L : y = 11x$.

Ara calcularem la intersecció d'aquesta recta amb la corba, o sigui $L \cap C$:

$$\begin{cases} y = 11x \\ y^2 = x^3 + x + 1 \end{cases}$$

Substituint la y en l'equació de la corba tenim

$$6x^2 = x^3 + x + 1$$

llavors

$$0 = x^3 + 17x^2 + x + 1 = (x-3)(x-9)(x-x_3)$$

ja que sabem que passa pels punts P_1 i P_2.

Mirem el coeficient de grau 2:

$$17 = -3 - 9 - x_3 \Longrightarrow x_3 = -11 - 17 = 17$$

$$y_3 = 11 \cdot 17 = 3$$

Recordeu

Segons el teorema de Bezout, una recta interseca amb una corba el·líptica en tres punts P, Q, R. Si dos d'aquests punts són iguals, diguem $P = Q$, llavors la recta és tangent a la corba en el punt P.

El punt d'intersecció és (17,3).

Finalment, calcularem el punt simètric, a $\mathbb{F}_{23}$, respecte l'eix d'abscisses: $P_1 + P_2 = (17,20)$

Per a calcular $10P_1$ començarem escrivint en binari $10 \leftrightarrow 1010$. Aplicant l'algorisme anàleg al de multiplicar i elevar, tenim: $10P_1 = 2(2(2P_1) + P_1)$

Càlcul de la tangent que passa per P_1:

L'equació de la tangent per un punt P és:

$$\frac{\partial f}{\partial x}(P)(x - x_1) + \frac{\partial f}{\partial y}(P)(y - y_1) = 0$$

Tenim $f(x,y) = y^2 - x^3 - x - 1$

$$\begin{cases} \frac{\partial f}{\partial x}(P_1) = -4 - 1 = 18 \\ \frac{\partial f}{\partial y}(P_1) = 20 \end{cases}$$

Per tant $18(x-3) + 20(y-10) = 18x + 20y + 22 = 0 \rightarrow 10y = 14x + 12 \rightarrow 5y = 7x + 6 \rightarrow y = 6x + 15$, $(5^{-1} = 14)$.

$L_{P_1} : y = 6x + 15$ recta tangent per P_1.

Ara calcularem la intersecció $L_{P_1} \cap C$

$$\begin{cases} y = 6x + 15 \\ y^2 = x^3 + x + 1 \end{cases}$$

Substituint la y en l'equació de la corba tenim

$$(6x + 15)^2 = x^3 + x + 1$$

llavors

$$0 = x^3 - 13x^2 + 5x + 6 = (x - 3)^2(x - x_3)$$

ja que el punt P_1 té multiplicitat 2.

Mirem el coeficient de grau 2:

$$-13 = -3 - 3 - x_3 \Longrightarrow x_3 = -6 + 13 = 7$$

$$y_3 = 6 \cdot 7 + 15 = 11$$

El punt d'intersecció és (7,11) i el simètric a $\mathbb{F}_{23}$, és (7,12).

Per tant: $Q = 2P_1 = (7,12)$

Seguim..., ara la tangent a la corba que passa per Q:

$$\begin{cases} \dfrac{\partial f}{\partial x}(Q) = 13 \\ \dfrac{\partial f}{\partial y}(Q) = 1 \end{cases}$$

Per tant, $13(x - 3) + (y - 12) = 13x + y + 12 = 0 \rightarrow y = 10x + 11$.

$L_Q : y = 10x + 11$ recta tangent per Q.

La intersecció d'aquesta tangent amb la corba $L_Q \cap C$

$$\begin{cases} y = 10x + 11 \\ y^2 = x^3 + x + 1 \end{cases}$$

$$0 = x^3 - 8x^2 - 12x - 5 = (x - 7)^2(x - x_3)$$

Mirem el coeficient de grau 2:

$$-8 = -7 - 7 - x_3 \Longrightarrow x_3 = 17$$

$$y_3 = 10 \cdot 17 + 11 = 20$$

El punt d'intersecció és (17,20) i, el simètric a $\mathbb{F}_{23}$, és (17,3).

O sigui: $R = 2Q = (17,3)$

Ara, la recta que passa per P_1 i R, $L_{P_1,R} : y = \alpha x + \beta$

$$\alpha = \frac{3-10}{17-3} = -\frac{8}{7} = 8 \cdot 10 = 11$$

$$10 = 11 \cdot 3 + \beta \Longrightarrow \beta = 10 - 10 = 0$$

Per tant $L_{P_1,R} : y = 11x$.

Ara la intersecció amb la corba: $L_{P_1,R} \cap C$:

$$\begin{cases} y = 11x \\ y^2 = x^3 + x + 1 \end{cases}$$

El punt d'intersecció és (9,7) i el simètric a $\mathbb{F}_{23}$, és $S = R + P_1 = (9,16)$.

Calcularem la tangent que passa per S:

$$\begin{cases} \frac{\partial f}{\partial x}(Q) = 9 \\ \frac{\partial f}{\partial y}(Q) = 9 \end{cases}$$

Per tant, $9(x-9) + 9(y-16) = 0 \rightarrow x - 9 + y - 16 = 0 \rightarrow y = 22x + 2$.

$L_S : y = 22x + 2$ recta tangent per S.

Ara toca calcular la intersecció d'aquesta recta L_S amb la corba: $L_S \cap C$

$$\begin{cases} y = 22x + 2 \\ y^2 = x^3 + x + 1 \end{cases}$$

$$0 = x^3 - x^2 + 3x - 3 = (x-9)^2(x - x_3)$$

Mirem el coeficient de grau 2:

$$-1 = -9 - 9 - x_3 \Longrightarrow x_3 = 6$$

$$y_3 = -6 \cdot +2 = 19$$

El punt d'intersecció és (6,19) i el simètric a $\mathbb{F}_{23}$, és $2S = (6,4)$. Aquesta és la solució que cercàvem:

$$10P_1 = (6,4)$$

Exemple 2.3

Sigui $K = \mathbb{F}_{16}$, $C : y^2 + xy = x^3 + \alpha^4 x^2 + 1$, $P_1 = (\alpha^6, \alpha^8)$, $P_2 = (\alpha^3, \alpha^{13})$.

- Construïu el cos $\mathbb{F}_{16}$ (utilitzant el polinomi primitiu $x^4 + x + 1$)
- Calculeu $P_1 + P_2$
- Calculeu $2 \cdot P_1$

Primer de tot construirem el cos finit $\mathbb{F}_{16} = \mathbb{Z}_2[x] \,/\, x^4 + x + 1$.

Sigui $\alpha = [x]$, la llista dels elements en forma exponencial i el seu equivalent polinòmic és:

$\alpha = [x]$

$\alpha^2 = [x]^2 = [x^2]$

$\alpha^3 = [x]^3 = [x^3]$

$\alpha^4 = [x]^4 = [x^4] = [x+1] = [x] + 1 = \alpha + 1$

$\alpha^5 = \alpha \cdot \alpha^4 = \alpha^2 + \alpha$

$\alpha^6 = \alpha^3 + \alpha^2$

$\alpha^7 = \alpha^4 + \alpha^3 = \alpha^3 + \alpha + 1$

$\alpha^8 = \alpha^2 + 1$

$\alpha^9 = \alpha^3 + \alpha$

$\alpha^{10} = \alpha^2 + \alpha + 1$

$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$

$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1$

$\alpha^{13} = \alpha^3 + \alpha^2 + 1$

$\alpha^{14} = \alpha^3 + 1$

$\alpha^{15} = 1$

Ara calcularem $P_1 + P_2 =$

- Recta que passa per P_1 i P_2, $L_{P_1,P_2} : y = ax + b$

$$a = \frac{\alpha^{13} - \alpha^8}{\alpha^3 - \alpha^6} = \frac{\alpha^3 + \alpha^2 + 1 + \alpha^2 + 1}{\alpha^3 + \alpha^3 + \alpha^2} = \frac{\alpha^3}{\alpha^2} = \alpha$$

Per tant, $y = \alpha x + b$. El punt P_1 pertany a L_{P_1,P_2}:

$$\alpha^8 = \alpha \cdot \alpha^6 + b \Longrightarrow b = \alpha^8 + \alpha^7 = \alpha^{11}$$

$$L_{P_1,P_2} : y = \alpha x + \alpha^{11}$$

- $L_{P_1,P_2} \cap C$

$$\begin{cases} y = \alpha x + \alpha^{11} \\ y^2 + xy = x^3 + \alpha^4 x^2 + 1 \end{cases}$$

Substituint el valor de y en la segona equació, tenim:

$$\alpha^2 x^2 + \alpha^{10} + \alpha x^2 + \alpha^{11} x = x^3 + \alpha^4 x^2 + 1$$

$$0 = x^3 + \alpha^8 x^2 + \alpha^{12} x + \alpha^{10} + 1 = (x - \alpha^6)(x - \alpha^3)(x - x_3)$$

Mirem el coeficient de grau 2:

$$\alpha^8 = \alpha^6 + \alpha^3 + x_3 \Longrightarrow x_3 = \alpha^8 + \alpha^6 + \alpha^3 = \alpha^2 + 1 + \alpha^3 + \alpha^2 + \alpha^3 = 1$$

$$y_3 = \alpha + \alpha^{11} = \alpha^6$$

A $\mathbb{F}_4$, el simètric d'un punt és ell mateix.

Solució:

$$P_1 + P_2 = (1, \alpha^6)$$

En segon lloc, anem a calcular $2P_1$

– Tangent que passa per P_1:

$$\begin{cases} \dfrac{\partial f}{\partial x}(P_1) = \alpha^9 \\ \dfrac{\partial f}{\partial y}(P_1) = \alpha^6 \end{cases}$$

$$\alpha^9(x - \alpha^6) + \alpha^6(y - \alpha^8) = 0 \rightarrow \alpha^3 x + \alpha^9 + y + \alpha^8 = 0$$

$LP_1 : y = \alpha^3 x + \alpha^{12}$

– $L_{P_1} \cap C$

$$\begin{cases} y = \alpha^3 x + \alpha^{12} \\ y^2 + xy = x^3 + \alpha^4 x^2 + 1 \end{cases}$$

Substituint el valor de y en la segona equació, tenim:

$$\alpha^6 x^2 + \alpha^9 + \alpha^3 x^2 + \alpha^{12} x = x^3 + \alpha^4 x^2 + 1$$

$$0 = x^3 + \alpha^{10} x^2 + \alpha^{12} x + \alpha^7 = (x - \alpha^6)^2 (x - x_3)$$

Mirem el coeficient de grau 2:

$$\alpha^{10} = \alpha^6 + \alpha^6 + x_3 = x_3$$

$$y_3 = \alpha^{13} + \alpha^{12} = \alpha$$

Solució:

$$2P_1 = (\alpha^{10}, \alpha)$$

2.2.2. Equació general de *P*+*Q*

Donada una corba el·líptica, per a calcular el resultat de fer operacions segons la llei de grup definida al subapartat 2.2.1. podem fer servir una fórmula que resumeix els càlculs que acabem de fer en els exercicis anteriors.

Considerem la corba el·líptica C sobre K amb $char(K) \neq 2,3$. L'equació de la corba és $C : y^2 = x^3 + Ax + B$. El punt base (de la recta de l'infinit) és $O = (0 : 1 : 0)$ de manera que el simètric $-P$ d'un punt $P = (x,y)$ es pot calcular com $-P = (x, -y)$. Siguin $P = (x_1,y_1)$, $Q = (x_2,y_2)$, $P + Q = (x_3,y_3)$, amb $P,Q \in C$, $-P = (x_1, -y_1)$. Suposem que $Q \neq -P$. Llavors:

Observació

Verifiqueu, si us plau, que el punt base $O = (0,1,0)$ pertany a la corba $C : y^2 = x^3 + Ax + B$.

$$\text{a) } P \neq Q \begin{cases} x_3 = \left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ y_3 = \left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1 \end{cases}$$

$$\text{b) } P = Q \begin{cases} x_3 = \left(\dfrac{3x_1^2 + A}{2y_1}\right)^2 - x_1 - x_2 \\ y_3 = \left(\dfrac{3x_1^2 + A}{2y_1}\right)(x_1 - x_3) - y_1 \end{cases}$$

Si $Q = -P$, $P + Q = O$ (punt base de C).

Si $char(K) = 2$, tenim dos casos (vegeu l'equació 5):

- $E : y^2 + cy = x^3 + ax + b$, $c \neq 0$

$-P = (x_1, y_1 + c)$

$$a) P \neq Q \begin{cases} x_3 = \left(\frac{y_1 + y_2}{x1 + x_2}\right)^2 + x_1 + x_2 \\ y_3 = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) + y_1 + c \end{cases}$$

$$b) P = Q \begin{cases} x_3 = \frac{x_1^4 + a^2}{c^2} \\ y_3 = \left(\frac{x_1^2 + a}{c}\right)(x_1 + x_3) + y_1 + c \end{cases}$$

- $E : y^2 + xy = x^3 + ax + b,\ b \neq 0$
  $-P = (x_1, y_1 + x_1)$

$$a) P \neq Q \begin{cases} x_3 = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)^2 + \frac{y_1 + y_2}{x_1 + x_2} + x_1 + x_2 + a \\ y_3 = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) + x_3 + y_1 \end{cases}$$

$$b) P = Q \begin{cases} x_3 = x_1^2 + \frac{b}{x_1^2} \\ y_3 = x_1^2 + \left(x_1 + \frac{y_1}{x_1}\right) x_3 + x_3 \end{cases}$$

Exemple 2.4

Donada la corba $y^2 = x^3 + 10x + 13$ sobre $\mathbb{F}_{23}$ i els punts d'aquesta $P = (7,9)$, $Q = (17,6)$, calculeu $P + Q$.

Fent servir les fórmules anteriors, si fem $P + Q = (x_3, y_3)$, resulta:

$x_3 = (\frac{6-9}{17-7})^2 - 7 - 17 = \frac{9}{8} - 1 = 3,$

$y_3 = \frac{6-9}{17-7}(7-3) - 9 = \frac{-3}{4}4 - 9 = 22.$

Fixem-nos que hem fet sumes i multiplicacions al cos finit $\mathbb{F}_{23}$ però, també, divisions. O, d'una altra manera, hem hagut de calcular inversos a $\mathbb{F}_{23}$.

El càlcul d'inversos en un cos finit és una operació costosa que es pot obviar fent servir coordenades projectives en lloc de coordenades afins.

3. Corbes el·líptiques sobre cossos finits

3.1. Nombre de punts d'una corba el·líptica

En tot aquest apartat, $K = \mathbb{F}_q$ serà un cos finit, en què $q = p^m$ per a un cert $m \in \mathbb{N}$ i p primer. Si E és una corba el·líptica sobre K escriurem E o $E(q)$ per a designar-la.

Teorema 3.1.

$(E(q), +)$, on $+$ és la llei de grup definida al subapartat 2.2.1., és un grup cíclic que pot ser generat per un sol element o es pot descompondre com a suma directa de dos subgrups cíclics amb ordres n_1 i n_2, respectivament, de manera que

$$E(q) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

en què n_2 divideix n_1 i $N = n_1 n_2$.

Recordeu que $\mathbb{Z}_n$ vol dir el grup dels enters mòdul n.

Notació

Escriurem $N = \#E(q)$ per a indicar el nombre de punts racionals de E.

Definició 3.2 (Residus quadràtics).

Sigui $x \in \mathbb{F}_q$. Si existeix $z \in \mathbb{F}_q$ tal que $x = z^2$, direm que x és un residu quadràtic (QR). En cas contrari, x és un residu no quadràtic (QNR).

Definició 3.3 (Símbol de Legendre).

Sigui p un nombre primer i sigui $n \in \mathbb{F}_p$. Definim el símbol de Legendre de n respecte de p, i ho denotarem per $\left(\frac{n}{p}\right)$, com:

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{si } n \text{ és QR} \pmod p \\ -1 & \text{si } n \text{ és QNR} \pmod p \end{cases}$$

Suposem que $char(K) \neq 2,3$, $E : y^2 = x^3 + Ax + B$. La corba E conté el punt de l'infinit $(0 : 1 : 0)$; per tant, el nombre de punts de la corba és $N \geq 1$. Ara prenem $x \in \mathbb{F}_q$ (x pot tenir q valors diferents), si $\exists y \in \mathbb{F}_q$ tal que $y^2 = x^3 + Ax + B$, llavors $-y$ també ho compleix. Per tant, podem dir que $N \leq 1 + 2q$.

Definim ara el caràcter quadràtic χ:

Algorisme 3.4.

$\mathbb{F}_q^* \longrightarrow \{1, -1\}$
$x \longrightarrow 1$, si x és QR
$x \longrightarrow -1$, si x és QNR

Sigui $f(x) = x^3 + Ax + B$. Fixat $x \in \mathbb{F}_q$, si $f(x)$ és QR, llavors tenim 2 punts de la corba; en canvi, si és QNR no en tenim cap. Així, podem escriure N en funció de $f(x)$:

$$N = 1 + \sum_{x \in \mathbb{F}_q} (\chi(f(x)) + 1) = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(f(x))$$

Veiem el cas $q = p$, $\mathbb{F}_q = \mathbb{Z}/p$.

$$\forall x \in \mathbb{Z}/p \quad x^{p-1} = 1 \pmod{p} \Longrightarrow x^{\frac{p-1}{2}} = \begin{cases} +1, \text{ si } x \text{ és QR} \\ \\ -1, \text{ si } x \text{ és QNR} \end{cases}$$

Recordeu

Un caràcter quadràtic χ és un morfisme del grup multiplicatiu del cos finit $\mathbb{F}_q$ (que escriurem $\mathbb{F}_q^*$) al grup multiplicatiu $\{1, -1\}$.

Si q és un nombre primer, llavors $\chi(x) = \left(\frac{x}{q}\right)$.

Lema 3.5.

Sigui p un nombre primer.

$$\sum_{x \in (\mathbb{Z}/p)^*} x^i = \begin{cases} p-1, \text{ si } i = 0 \text{ o } i = p-1 \\ \\ 0, \text{ si } i \neq 0, p-1 \end{cases}$$

Demostració: Si $i = 0$, és clar que $\sum_{x \in (\mathbb{Z}/p)^*} x = p - 1$. Amb $i = p - 1$ ens trobem en la mateixa situació, ja que $x^{p-1} = 1 \pmod{p}$.

Considerem el cas $i \neq 0, p-1$:

$\forall x \in (\mathbb{Z}/p)^*$ tenim $x^p - x = 0$. Per tant, podem escriure $x^p - x = (x - x_1) \cdots (x - x_p)$, on $\mathbb{Z}/p = \{x_1, \ldots, x_p\}$.

Mirant el coeficient de x^{p-1} en l'equació $x^p - x = 0$, tenim $0 = x_1 + \cdots + x_n$. També, mirant el coeficient de x^{p-2} tenim $\sum_{i,j} x_i x_j = 0$. Però $\sum x_i^2 = (\sum x_i)^2 - 2\sum x_i x_j = 0$. Així faríem el mateix per a cada exponent i trobaríem: $\sum_{x \in (\mathbb{Z}/p)^*} x^i = 0, \quad \forall i \notin \{0, p-1\}$. ∎

Farem servir aquest lema per a trobar el valor de N:

$$N = 1 + p + \sum_{x \in \mathbb{F}_p} \chi(f(x)) = 1 + p + \sum_{x \in \mathbb{F}_p} (f(x))^{\frac{p-1}{2}}$$

$$= 1 + p + \sum_{x \in \mathbb{F}_p} (x^3 + Ax + B)^{\frac{p-1}{2}} = 1 + p + \sum_{x \in \mathbb{F}_p} \sum_{i=0}^{3 \cdot \frac{p-1}{2}} f_i x^i$$

$$= 1 + p + \sum_{i=0}^{3 \cdot \frac{p-1}{2}} f_i \sum_{x \in \mathbb{F}_p} x^i = 1 + p + \sum_{i=0}^{3 \cdot \frac{p-1}{2}} f_i \sum_{x \in \mathbb{F}_p^*} x^i + f_0$$

$$= 1 + p + (p-1) f_0 + (p-1) f_{p-1} + f_0.$$

Per tant, $N = 1 - f_{p-1} \pmod{p}$.

Casos especials:

- Si $f_{p-1} = 0 \pmod{p}$ i, més concretament, si $N = 1 + p$, E s'anomena *corba supersingular*. Aquest tipus de corbes són importants, ja que hi ha un algorisme per a trencar el logaritme el·líptic.

- Si $f_{p-1} = 1 \pmod{p}$ i, concretament, si $N = p$, E s'anomena *corba anòmala*. En aquest cas també és senzill trencar el logaritme el·líptic (Semaev-Smart-Satoh-Araki).

Definició 3.6 (Corbes supersingulars i anòmales).

Donat el cos $K = \mathbb{F}_q$, amb $q = p^m$, p primer, llavors:

- Si $N = 1 + q \pm t$, en què $p \mid t$, direm que E és una corba supersingular.

- Si $N = 0 \pmod{p}$, direm que E és una corba anòmala.

Teorema 3.7 (Teorema de Hasse, 1930).

Considerem la corba el·líptica $E(q)$ i sigui N el nombre de punts racionals de $E(q)$. Es compleix:

$$|N-(1+q)| \leq 2\sqrt{q}$$

Observació

El teorema de Hasse ens dóna un fita força ajustada: $1+q-2\sqrt{q} \leq N \leq 1+q+2\sqrt{q}$.

Per a fer la demostració d'aquest teorema, es necessita la hipòtesi de Riemann.

Definició 3.8 (La funció de Riemann).

La funció de Riemann és:

$$\zeta(s) = \prod_{p \text{ primer}} \left(\frac{1}{1-\frac{1}{p^s}}\right) = \sum_{n\in\mathbb{N}} \frac{1}{n^s}$$

Per a valors reals de s tenim:

$$\zeta(s) = \begin{cases} 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots = \infty, \text{ si } s=1 \\ \text{té solució, si } s>1 \\ \text{divergeix, si } s<1. \end{cases}$$

La hipòtesi de Riemann diu que en el cos dels complexos, els zeros no trivials de $\zeta(s)$ es troben a la recta $Re(s) = \frac{1}{2}$.

Hipòtesi de Riemann

És un dels problemes oberts més importants i famosos de la matemàtica contemporània. És el quart problema del mil·leni que el Clay Mathematics Institute va dotar amb un premi d'un milió de dòlars per a la primera persona que aporti una demostració correcta de la conjectura.

Ara ens plantegem el problema invers. Donat un valor N, existeix una corba el·líptica que tingui aquest nombre de punts?

Teorema 3.9.

En el cos finit $\mathbb{F}_q$, en què $q = p^m$ i p primer, si t és qualsevol valor tal que:

$$\begin{cases} |t| \leq 2\sqrt{q} \\ si \;\; p|t \rightarrow p^n|t, \;\; on \;\; n = \left\lfloor \frac{m+1}{2} \right\rfloor \end{cases}$$

llavors, podem trobar una corba que tingui $N = 1+q+t$ punts.

Exemple 3.1

Les corbes el·líptiques sobre $\mathbb{Z}_2$ es poden escriure com:

$$y^2 + xy = x^3 + b_2x^2 + b_6, \text{ si } \Delta = b_6 \neq 0$$

$$y^2 + b_3y = x^3 + b_4x + b_6, \text{ si } \Delta = b_3^4 \neq 0$$

Pel teorema de Hasse, $3 - 2\sqrt{2} \leq N \leq 3 + 2\sqrt{2} \rightarrow 1 \leq N \leq 5$.

- $E : y^2 + y = x^3 + x + 1$, $N = 1$ (només té el punt de l'infinit).
- $E : y^2 + y = x^3 + x$, $N = 5$.
- $E : y^2 + xy = x^3 + x^2 + 1$, $N = 2$.
- $E : y^2 + xy = x^2 + 1$, $N = 4$.
- $E : y^2 + y = x^3 + 1$, $N = 3$.
- $E : y^2 + y = x^3$, $N = 3$.

Les dues últimes corbes són corbes supersingulars, ja que $N = 1 + p$ i la tercera és una corba anòmala.

Com podem calcular el nombre de punts N d'una corba el·líptica? Hi ha diferents mètodes:

1) Per força bruta, provant tota parella de punts $(x,y) \in \mathbb{F}_q^2$.

2) A partir de $P = (x,y) \in E$, $y \neq 0$, calculem $2P$, $3P, \cdots$ fins a obtenir el subgrup $\langle P \rangle \subset E$. Si E fos cíclic ($n_1 = N, n_2 = 1$) i P fos un generador de E, obtindríem $\langle P \rangle = E$. En el cas que N fos un nombre primer, tindríem que tots els $P \neq O$ són generadors.

3) Algorisme de Schoof (1985). Calcula el nombre de punts d'una corba amb una complexitat $O(log_2^8(q))$.

Hi ha casos particulars una mica més senzills; per exemple, corbes del tipus $y^2 = x^3 + Ax$ o $y^2 = x^3 + B$. En aquests casos es fa servir l'algorisme de Munuera-Tena (1993) que és de l'ordre de $O(log_2^3(p))$.

3.2. Extensió d'una corba sobre un cos a una corba sobre un cos estès

Una corba el·líptica definida sobre tot $\mathbb{F}_p$ es pot considerar també definida sobre $\mathbb{F}_q$ on $q = p^m$. Diguem $N = \#E(p) = p + 1 - t$ i $N_m = \#E(q)$.

Conjectura de Weil: (de fet, és un teorema de Schmidt de 1925, previ a Weil). Siguin $\alpha, \beta \in \mathbb{C}$ les arrels conjugades de l'equació $x^2 + tx + p = 0$. Aleshores:

$$N_m = 1 + p^m - \alpha^m - \beta^m$$

Exemple 3.2

Considerem la corba $E : y^2 + y = x^3$. Sabem que E té 3 punts sobre $Z/2$. Anem a calcular quants punts té la corba definida per la mateixa funció, sobre $\mathbb{F}_{2^m}$.

Calculem α i β, fent $A = \big(N - (q+1)\big)$ en l'equació anterior:

$$x^2 + (3-3)x + 2 = 0 \rightarrow \begin{cases} \alpha = \sqrt{2}i \\ \beta = -\sqrt{2}i \end{cases}$$

- Si $m = 0 \pmod 4$, llavors $N_m = 1 + 2^m - 2\sqrt{2^m}$
- Si $m = 2 \pmod 4$, llavors $N_m = 1 + 2^m + 2\sqrt{2^m}$
- Si $m = 1,3 \pmod 4$, llavors $N_m = 1 + 2^m$

4. L'ús de les corbes el·líptiques en criptografia

El 1985, Koblitz i Miller van proposar, de manera independent, la utilització del grup de punts d'una corba el·líptica definida sobre un cos finit per a criptosistemes basats en el problema de trencar el logaritme.

4.1. El problema del logaritme el·líptic

Com hem vist en l'apartat anterior, els punt d'una corba el·líptica formen un grup amb la suma. Donat un punt P d'una corba el·líptica E, podem calcular $Q = sP$, $s \in \mathbb{Z}$, en què Q torna a ser un punt de la corba E.

Definició 4.1 (Problema del logaritme el·líptic).

Sigui E una corba el·líptica sobre el cos finit $\mathbb{F}_q$ amb $q = p^m$, p primer, $m \in \mathbb{N}$, i sigui $P \in E$ d'ordre n. El problema del logaritme el·líptic en E (respecte a la base P) donat $Q \in E$, es basa a trobar $s \in \mathbb{Z}$ tal que $Q = sP$ en cas que existeixi.

En aquest subapartat veurem alguns mètodes i algorismes coneguts per a trencar el logaritme el·líptic.

L'algorisme de Silver-Polhig-Hellman per a trencar el logaritme discret en el cos F_p té una complexitat de $\mathcal{O}(\sqrt{N_1})$, en què $p-1 = N_1 \cdot \ldots \cdot N_r$ és la factorització de $(p-1)$ en primers i N_1 és el primer més gran. En el logaritme el·líptic tenim que $N = N_1 \cdot \ldots \cdot N_r$, és la factorització de N en primers i N_1 és el primer més gran i, de la mateixa manera, trencar aquest logaritme té una complexitat de $\mathcal{O}(\sqrt{N_1})$.

Suposem que $K = \mathbb{F}_q$, en què $q = p^m$ i p primer petit. Sigui $N = \#E(q)$ i $N_1 = \#E(p)$. Sabem que els punts que pertanyen a la corba sobre el cos base, també són punts de la corba en el cos gran i el grup de punts de la corba sobre el cos base és un subgrup del grup de punts de la corba sobre el cos gran. Així, $N_1 | N$ i existeix un enter d tal que $N = N_1 \cdot d$. Volíem $N = N_1 \cdot \ldots \cdot N_r$, amb algun N_i primer gran; així, si N_1 és primer gran, ja hem acabat. Si N_1 és petit, llavors d és gran, si a més d és primer ja tenim una bona descomposició. En el cas que $N = N_1 \cdot d$ amb d primer, es diu que E és quasiprima.

Observació

Si $K = \mathbb{Z}/p$, p primer gran i $N = p$, llavors tenim que $N = N_1 (= p)$ és un primer gran i a més, qualsevol punt és generador amb ordre N. D'altra banda, hem vist que si $N = p$, llavors E és una corba anòmala i el logaritme és fàcil de trencar en aquests casos. També és fàcil de trencar en el cas $N = p + 1$, que són les corbes supersingulars.

Teorema 4.2 (Tena, 1994).

Sigui $K = \mathbb{F}_q$, en què $q = p^m$ i p primer petit, E corba el·líptica sobre K. Una condició necessària per a ser E quasiprima és que m sigui primer.

El millor algorisme conegut per a trencar el logaritme el·líptic és el mètode ρ de Pollard, que necessita $\frac{\sqrt{\pi n}}{2}$ passos (sumes de punts en corbes el·líptiques). Aquest mètode es pot paral·lelitzar a r processadors i aconseguir baixar el nombre de passos necessaris a $\frac{\sqrt{\pi n}}{2r}$.

Teorema 4.3 (MOV –Menezes, Okamoto i Vanstone–, 1993).

El càlcul de logaritme el·líptic sobre $\mathbb{Z}/p$ és equivalent al càlcul del logaritme discret sobre $\mathbb{F}_{p^k}$ per a algun enter k.

Aquesta equivalència es dóna fent la immersió del grup de punts de la corba sobre el cos base dins del grup multiplicatiu $\mathbb{F}^*_{p^k}$ que només és possible si N divideix $p^k - 1$. Un cop en $\mathbb{F}^*_{p^k}$ es pot fer servir l'algorisme *index-calculus* o l'algorisme NFS (*number field sieve*) per a trencar el logaritme, que és un algorisme subexponancial de l'ordre de

Si $k = 6$ tenim que quan $p \simeq \mathcal{O}(160)$ bits, llavors $p^k \simeq \mathcal{O}(2000)$ bits.

$$exp\left[\left(c + o(s)\right) \cdot \left(log(p^k)\right)^{\frac{1}{3}} \cdot \left(log\left(log(p^k)\right)\right)^{\frac{2}{3}}\right]$$

El mètode *xedni-calculus* (Silverman) és la idea inversa de l'*index-calculus*. Donada $E(\mathbb{Z}/p)$ es projecten r combinacions lineals al pla racional $\mathbb{Q}$ i es considera la corba $E(\mathbb{Q})$ que conté aquests r punts. En el cas que aquests r punts obtinguts siguin linealment dependents, se soluciona el problema el·líptic. Actualment es fa servir aquest mètode amb $r \leq 9$ i la probabilitat que els punts obtinguts siguin linealment dependents és molt petita. La importància de *xedni-calculus* és que és fàcilment adaptable al problema del logaritme discret i la factorització, i llavors podria atacar tots els criptosistemes de clau pública en cas que es trobés algun algorisme eficient.

Observació

En l'equivalència donada pel MOV, normalment, el valor del paràmetre k serà molt gran i, per tant, no guanyarem gaire fent la conversió del logaritme el·líptic en logaritme discret. Però, en alguns casos, sí que podrem trencar el logaritme el·líptic per mitjà dels algorismes per a trencar el logaritme discret (això és el que passa en les corbes supersingulars, on es conegut que $k \leq 6$).

4.2. Elecció de la corba

L'elecció de la corba s'ha de fer tenint en compte els atacs comentats en el subapartat anterior:

- Per a resistir l'atac del mètode ρ de Pollard, el nombre de punts de la corba ha de ser divisible per un nombre primer prou gran ($> 2^{160}$).

- Per a resistir l'atac Semaev-Smart-Araki, el nombre de punts de la corba no ha de ser múltiple de p.

- Per a resistir la reducció MOV n (ordre del punt escollit) no ha de dividir $p^k - 1$.

- Per a resistir els atacs contra corbes el·líptiques supersingulars, el nombre de punts de la corba no ha de ser igual a -1 mòdul p.

Ara veurem diferents mètodes coneguts per a escollir una corba adient:

1) El **teorema de Hasse** i la **conjectura de Weil** ens proporcionen una tècnica per a triar corbes sobre $\mathbb{F}_{2^m}$, en què m és divisible per un enter l petit. De fet, com que aquests resultats són vàlids per a qualsevol $\mathbb{F}_{p^m}$, podríem estendre aquesta tècnica a tots aquests cossos.

Recordem que donada una corba el·líptica E, definida sobre $\mathbb{F}_p$, llavors la podem tractar com una corba el·líptica sobre qualsevol extensió $\mathbb{F}_{p^m}$ de $\mathbb{F}_p$. A més, sabem calcular el nombre de punts de la corba sobre el cos estès, a partir del nombre de punts de la corba sobre el cos base.

Per a triar una corba adequada sobre $\mathbb{F}_{2^m}$, primer agafarem una corba sobre $\mathbb{F}_{2^l}$ amb l dividint m i calcularem el nombre de punts de la corba sobre $\mathbb{F}_{2^l}$ (que es pot fer de manera exhaustiva, ja que hem triat l de manera que el cos $\mathbb{F}_{2^l}$ sigui petit). Llavors calcularem el nombre de punts de la corba sobre el cos estès i comprovarem si resisteix els atacs anteriors. En cas que no resisteixi algun dels atacs anteriors repetim el procés fins a trobar una corba adient.

El principal problema que presenta aquesta tècnica és el nombre de corbes sobre $\mathbb{F}_{2^l}$, que serà relativament petit, i per tant, és possible que donats m i l no aconseguim trobar cap corba adequada fent servir aquest mètode.

2) Mètode global. Aquesta manera de triar la corba està basada a agafar una corba sobre els racionals i reduir-la mòdul un ideal primer per a tenir la corba sobre un cos finit i comprovar si satisfà els atacs anteriors.

Per exemple, si comencem amb $E : y^2 = x^3 + Ax + B$, en què A,B són nombres racionals (o reals, o complexos o ...), podem considerar la mateixa equació mòdul un primer p. Aleshores, tindrem la corba sobre $\mathbb{F}_p$ amb N_p punts. Hi ha resultats teòrics que asseguren que per a p prou gran N_p és múltiple del nombre de punts d'ordre finit de la corba original sobre els racionals. Així, coneixent el nombre de punts d'ordre finit sobre el cos inicial tindrem una cota inferior del nombre de punts que tenim per a la corba en $\mathbb{F}_p$.

3) Mètode de la multiplicació complexa. Aquest mètode permet l'elecció de l'ordre de la corba abans de construir-la. S'ha de comprovar que l'ordre que volem superi els atacs donats. Aquest mètode és eficient quan la mida q del cos i el valor t tal que $\#E = 1 + q - t$ són escollits de manera que el cos $\mathbb{Q}(\sqrt{t^2 - 4q})$

té un nombre petit de classes. Per a corbes el·líptiques sobre $\mathbb{F}_p$ aquest mètode s'anomena mètode d'Atkin-Morain i, sobre $\mathbb{F}_{2^m}$, mètode de Lay-Zimmerman.

4) Mètode d'elecció aleatòria. Com el seu nom indica, en aquest mètode triem la corba de manera aleatòria. Fixat un cos finit $\mathbb{F}_q$, suposem que $char(K) \neq 2,3$ i la corba $E : y^2 = x^3 + Ax + B$. Seleccionem $A,B \in \mathbb{F}_q$ de manera aleatòria, però satisfent $4A^3 + 27B^2 \neq 0$. Llavors calculem el nombre de punts de la corba sobre $\mathbb{F}_q$ i el factoritzem. Aquest procés es repetirà fins a trobar una corba que pugui resistir els atacs anteriors.

Aquest mètode és especialment usat en el cas de treballar amb corbes el·líptiques sobre $\mathbb{F}_p$, ja que els resultats de Lenstra en demostren la funcionalitat. Per a corbes el·líptiques sobre $\mathbb{F}_{2^m}$ hi ha resultats similars en treballs de Waterhouse i Schoof.

4.3. Assignació de missatges a punts

Un dels problemes pràctics que es plantegen a l'hora de fer servir aquest tipus de criptografia és el de definir una correspondència entre els missatges que es volen transmetre i els punts de la corba. Hi ha diferents procediments per a fer-ho; en veurem dos. Suposem que $char(K) \neq 2,3$. $E : y^2 = f(x) = x^3 + Ax + B$.

4.3.1. Creació d'una taula

Sigui m el missatge que volem transmetre, $0 \leq m \leq C$ en què C és una cota superior del nombre de missatges diferents. Prenem k arbitrari (en direm *grau de fiabilitat*), escollim p primer tal que $p > Ck$, p de 160 bits per a donar fortalesa al sistema. Podem ficar els elements $1,\ldots,Ck$ dins de $\mathbb{Z}/p$ fent servir la taula següent:

$$\begin{bmatrix} & 1 & 2 & \ldots & k-1 \\ k & k+1 & k+2 & \ldots & 2k-1 \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ mk & mk+1 & mk+2 & \ldots & (m+1)k-1 \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ \ldots & \ldots & \ldots & \ldots & Ck \end{bmatrix}$$

en què cada fila representa una classe.

Donat m, prenem $x = mk$ i calculem $y^2 = f(x)$. Si $f(x)$ no té arrel quadrada, llavors necessitem un altre valor de x, prenem $x = mk + 1$ i repetim el mateix procés fins a trobar x tal que $f(x)$ té arrel quadrada, prenent $y = \sqrt{f(x)}$.

Ara ens podríem preguntar; aquest valor x es troba en la classe de m? Sabem que la meitat dels elements de $\mathbb{Z}/p$ tenen arrel quadrada i estan repartits aleatòriament. La probabilitat que en una fila no hi hagi un quadrat és $\frac{1}{2^k}$. Per tant, la probabilitat que en una fila no hi hagi una x vàlida es pot fer tan petita com volem, augmentant el valor de K.

Així doncs, donat m, existeix un valor $j \in \{1,\ldots,k-1\}$ tal que el punt $P = (mk + j, y)$ pertany a la corba. Tenim la correspondència:

Algorisme 4.4.

Corba $\longrightarrow \mathbb{Z}/p$
$m \longrightarrow (mk + j, y)$
$\left\lfloor \frac{\alpha}{k} \right\rfloor \longleftarrow (\alpha, \beta)$

4.3.2. Mètode de corbes entrellaçades

Definició 4.5 (Corbes entrellaçades).

Sigui $E : y^2 = x^3 + Ax + B$ una corba el·líptica sobre $\mathbb{Z}/p$, p primer. Sigui $E' : y^2 = x^3 + A\beta^2 x + B\beta^3$, amb $\beta \in \mathbb{Z}/p$, β NQR. Direm que E i E' són corbes entrellaçades.

Teorema 4.6.

Siguin E i E' corbes entrellaçades. Aleshores

$$\#E + \#E' = 2(p + 1)$$

Observació

Fixant una corba E, hi ha una gran quantitat de parelles (E,E') de corbes entrellaçades.

El concepte de parell de corbes entrellaçades permet definir una aplicació bijectiva entre el conjunt de valors $\{0,1,\ldots,2p+1\}$ i el format pel total de punts de totes dues corbes. Així, a cada punt $P = (x,y)$ que pot pertànyer a E o a E', li assignem un punt de $m \in \{0,1,\ldots,2p+1\}$ de la manera següent:

$$m = \begin{cases} 2x, & \text{si } P \in E,\ 0 \le y \le \dfrac{p-1}{2} \\ 2x+1, & \text{si } P \in E,\ \dfrac{p-1}{2} < y \le p \\ 2p, & \text{si } P = (\infty,\infty) \in E \\ \dfrac{2x}{\beta}, & \text{si } P \in E',\ 0 \le y \le \dfrac{p-1}{2} \\ \dfrac{2x}{\beta}+1, & \text{si } P \in E',\ \dfrac{p-1}{2} < y \le p \\ \dfrac{2x}{\beta}+1, & \text{si } P = (x,0) \in E' \\ 2p+1, & \text{si } P = (\infty,\infty) \in E' \end{cases}$$

en què $\dfrac{2x}{\beta}$ s'ha d'operar mòdul $2p$.

Suposem ara que tenim el missatge m. El punt associat és:

$$P = \begin{cases} (\dfrac{m}{2}, \sqrt{\omega}) \in E, & \text{si } m \text{ és parell i } \omega \neq 0 \text{ és QR} \pmod p \\ (\beta\dfrac{m}{2}, \sqrt{\beta^3\omega}) \in E', & \text{si } m \text{ és parell i } \omega \neq 0 \text{ és NQR} \pmod p \\ (\dfrac{m}{2}, 0) \in E, & \text{si } m \text{ és parell, } \dfrac{m}{2} \neq p \text{ i } \omega = 0 \\ (\infty,\infty) \in E, & \text{si } m \text{ és parell, } \dfrac{m}{2} = p \\ (\dfrac{m-1}{2}, -\sqrt{\omega}) \in E, & \text{si } m \text{ és senar i } \omega \neq 0 \text{ és QR} \pmod p \\ (\beta\dfrac{m-1}{2}, -\sqrt{\beta^3\omega}) \in E', & \text{si } m \text{ és senar i } \omega \neq 0 \text{ és NQR} \pmod p \\ (\beta\dfrac{m-1}{2}, 0) \in E', & \text{si } m \text{ és senar, } \dfrac{m}{2} \neq p \text{ i } \omega = 0 \\ (\infty,\infty) \in E', & \text{si } m \text{ és parell, } \dfrac{m}{2} = p \end{cases}$$

en què $\omega \equiv x^3 + Ax + B \pmod p$ i $\sqrt{\alpha}, -\sqrt{\alpha}$ són les arrels quadrades d'un element α.

Exemple 4.1

Prenem $p = 31$ i la parella de corbes entrellaçades (hem agafat $\beta = 13$):

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

$$E' : y^2 = x^3 + 3 \cdot 13^2 + 1 \cdot 13^3 = x^3 + 11x + 27$$

E té 39 punts i E' en té 25:

Punts de E:

(0,1)	(0,30)	(1,6)	(1,25)	(6,7)	(6,24)
(8,14)	(8,17)	(10,15)	(10,16)	(11,1)	(11,30)
(13,6)	(13,25)	(14,11)	(14,20)	(17,6)	(17,25)
(18,11)	(18,20)	(19,2)	(19,29)	(20,1)	(20,30)
(21,5)	(21,26)	(22,12)	(22,19)	(24,3)	(24,28)
(26,4)	(26,27)	(27,7)	(27,24)	(29,7)	(29,24)
(30,11)	(30,20)	(∞,∞)			

Punts de E':

(1,15)	(1,16)	(3,5)	(3,26)	(8,10)	(8,21)
(9,7)	(9,24)	(15,8)	(15,23)	(20,1)	(20,30)
(21,8)	(21,23)	(22,6)	(22,25)	(23,4)	(23,27)
(24,14)	(24,17)	(26,8)	(26,23)	(29,11)	(29,20)
(∞,∞)					

Entre les dues corbes tenim 64 punts. La correspondència entre missatges i punts es mostra a la taula següent.

punt de E	missatge	punt de E'	missatge
(0,1)	0	(1,15)	24
(0,30)	1	(1,16)	25
(1,6)	2	(3,5)	10
(1,25)	3	(3,26)	11
(6,7)	12	(8,10)	6
(6,24)	13	(8,21)	7
(8,14)	16	(9,7)	30
(8,17)	17	(9,24)	31
(10,15)	20	(15,8)	50
(10,16)	21	(15,23)	51
(11,1)	22	(20,1)	46
(11,30)	23	(20,30)	47
(13,6)	26	(21,8)	8
(13,25)	27	(21,23)	9
(14,11)	28	(22,6)	32
(14,20)	29	(22,25)	33
(17,6)	34	(23,4)	56
(15,25)	35	(23,27)	57
(18,11)	36	(24,14)	18
(18,20)	37	(24,17)	19
(19,2)	38	(26,8)	4
(19,29)	39	(26,23)	5
(20,1)	40	(29,11)	14
(20,30)	41	(29,30)	15
(21,5)	42	(∞,∞)	63
(21,26)	43	-	-
(22,12)	44	-	-
(22,19)	45	-	-
(24,3)	48	-	-
(24,28)	49	-	-
(26,4)	52	-	-
(26,27)	53	-	-
(27,7)	54	-	-
(27,24)	55	-	-
(29,7)	58	-	-
(29,24)	59	-	-
(30,10)	60	-	-
(30,20)	61	-	-
(∞,∞)	62	-	-

5. Criptografia i protocols criptogràfics basats en corbes el·líptiques

5.1. Protocols criptogràfics

Escriurem $E_U(m)$ quan parlem de xifrar el missatge m fent servir la clau pública de l'usuari U i $D_U(c)$ i quan parlem de desxifrar el missatge c.

5.1.1. Protocol de Diffie-Helman

Versió clàssica. Sigui p un nombre primer, $\alpha \in \mathbb{Z}_p$ primitiu. Cada usuari U cerca a l'atzar un nombre secret $n_U \in \mathbb{Z}_p^*$ i fa públic el valor α^{n_U}. Els usuaris A i B volen compartir una clau secreta:

Algorisme 5.1.

$A \xrightarrow{\alpha^{n_A}} B$
$A \xleftarrow{\alpha^{n_B}} B$

La clau secreta serà $K = \alpha^{n_A \cdot n_B}$, que només és coneguda per A i B.

Versió amb corbes el·líptiques. Sigui E una corba el·líptica sobre $\mathbb{F}_p$ i $P \in E$ conegut. Cada usuari U cerca a l'atzar un nombre secret $n_U \in \mathbb{F}_p$ i fa públic el valor $n_U P$. Per a compartir una clau secreta, A i B han de fer:

Algorisme 5.2.

$A \xrightarrow{n_A P} B$
$A \xleftarrow{n_B P} B$

La clau secreta serà $K = (n_A \cdot n_B)P$, que només és coneguda per A i B.

Exemple 5.1. Acord de claus de Diffie-Helman usant corbes el·líptiques

En primer lloc, els usuaris A i B trien una corba el·líptica E sobre un cos finit $\mathbb{Z}_p$. També trien un punt P de la corba de manera que el seu ordre sigui un nombre primer gran.

Suposem que la corba el·líptica és $E : y^2 = x^3 + 5x + 7$ sobre $\mathbb{Z}_{113}$. El nombre de punts racionals d'aquesta corba és de 127, que és un nombre primer i, per tant, els punts de la corba el·líptica constitueixen un grup isomorf a $\mathbb{Z}_{127}$.

Agafem $P = (16,51)$, que té ordre $ord(P) = 127$, o sigui P és un generador de la corba E.

Protocol

- $A \to B$. L'usuari A tria un enter gran n_A, calcula $K_A = n_A \cdot P$ i envia K_A a B.

  Si A agafa, per exemple, $n_A = 98$, aleshores, $K_A = n_A \cdot P = (24,74)$.

- $B \to A$. L'usuari B tria un enter gran n_B, calcula $K_B = n_B \cdot P$ i envia K_B a A.

  Si B agafa, per exemple, $n_B = 101$; aleshores, $K_B = n_B \cdot P = (3,7)$.

- $A \to B$. L'usuari A calcula $K = n_A \cdot K_B = n_A \cdot n_B \cdot P = 98 \cdot (3,7) = (5,48)$.

- $B \to A$. L'usuari B calcula $K = n_B \cdot K_A = n_B \cdot n_A \cdot P = 101 \cdot (24,74) = (5,48)$.

Al finalitzar l'algoritme, tant A com B disposen del mateix punt, que prendran com a clau de sessió: $K = (5,48)$.

Utilització del programari SAGE

En aquest exemple podem seguir els càlculs numèrics fent ús del programari SAGE. Es pot utilitzar instrucció a instrucció, però també és pot llençar un *script* que ens calculi directament el resultat que volem.

Simulador de càlculs en corbes el·líptiques

Per a comprovar els càlculs d'aquest exemple podeu usar el programa SAGE, que trobareu a l'adreça http://www.sagemath.org/.

Primer de tot definirem el cos finit $\mathbb{F}_{113}$, que anomenarem F, amb l'ordre:

```
sage: F = FiniteField(113)
```

A continuació definirem la corba el·líptica $y^2 = x^3 + 5 * x + 7$. En general, la corba definida amb els paràmetres $[a,b,c,d,e]$ és $y^2 + axy + cy = x^3 + bx^2 + dx + e$.

```
sage: E = EllipticCurve(F,[0,0,0,5,7])
Elliptic Curve defined by y^2 = x^3 + 5*x + 7 over Finite Field of size 113
```

Si volem saber l'odre de la corba el·líptica:

```
sage: print(E.cardinality())
127
```

A continuació, per a indicar-li el punt $P = (16,51)$ escriurem el següent (i calcularem, també, el seu ordre):

```
sage: P = E.point((16,51))
sage: P.order()
```

en l'ordre anterior estem explicant que s'agafi el punt $P = (16,51)$ dintre del domini de punts de la corba E.

L'usuari A calcula $KA := 98P$ i l'usuari B $KB := 101 * P$:

```
sage: KA = 98*P
sage: KB = 101*P
```

Finalment, podem comprovar que tots dos usuaris poden utilitzar la mateixa clau comuna: $K = n_A * K_B = n_B * K_A$:

```
print 101*KA,98*KB
```

Després d'aquesta última instrucció SAGE contesta amb els dos valors que li hem demanat d'imprimir:

```
(5 : 48 : 1) (5 : 48 : 1)
```

Noteu que SAGE està fent les operacions en coordenades projectives.

5.1.2. Protocol de tres passos de Shamir

Versió clàssica. Aquest protocol pretén enviar el missatge m de A a B.

Algorisme 5.3.

$A \xrightarrow{E_A(m)} B$
$A \xleftarrow{E_B(E_A(m))} B$
$A \xrightarrow{E_B(m)} B$

És fonamental suposar que la funció criptogràfica utilitzada compleix, per a cada parella d'usuaris, $E_A \cdot E_B = E_B \cdot E_A$. Un exemple de funció criptogràfica amb aquesta característica és $E_A(x) = x^{n_A}$ a $\mathbb{Z}/p$, amb p primer i n_A clau privada de l'usuari A. En aquest cas concret, el protocol s'anomena protocol de Massey-Omura:

Algorisme 5.4.

$A \xrightarrow{m^{n_A}} B$
$A \xleftarrow{(m^{n_A})^{n_B}} B$
$A \xrightarrow{m^{n_B}} B$

Versió amb corbes el·líptiques. Veurem la traducció del protocol de Massey-Omura. Sigui E una corba el·líptica sobre $\mathbb{F}_q$, $N = \#E(q)$. Sigui $P \in E$ el missatge que l'usuari A vol enviar a B. Cada usuari U té una clau privada n_U tal que $\text{mcd}(n_U, N) = 1$.

Algorisme 5.5.

$A \xrightarrow{n_A P} B$
$A \xleftarrow{n_B(n_A P)} B$
$A \xrightarrow{n_B P} B$

5.2. Criptosistema ElGamal

Versió clàssica. Es basa en el problema del logaritme discret sobre un cos finit $\mathbb{Z}/p$ amb p primer. Sigui $\alpha \in \mathbb{Z}/p$ un element primitiu que es fa públic. Cada usuari U té una clau privada $n_U \in \mathbb{Z}/p - \{0,1,p-1\}$ i fa pública la clau pública $\alpha_U = \alpha^{n_U}$. Suposem que l'usuari A vol enviar el missatge m a l'usuari B. A ha de seguir els passos següents:

- A tria un nombre $k \in \mathbb{Z}/p - \{0,1,p-1\}$ a l'atzar i calcula α^k,
- xifra m com $c = E_B(m) = m \cdot (\alpha_B)^k$,
- envia a B (c,α^k).

B per a desxifrar el missatge haurà de fer:

- calcula $\beta = (\alpha^k)^{n_B}$,
- $m = c \cdot \beta^{-1}$.

Versió amb corbes el·líptiques. Sigui E una corba el·líptica sobre $\mathbb{Z}/p$, sigui P un punt de la corba d'ordre gran (seria desitjable que $\langle P \rangle = E$) i $N = \#E(p)$. Per a cada usuari U, sigui n_U la seva clau privada, $1 < n_U < N$; n'hi ha prou amb $n_U < p + 1 - 2\sqrt{p}$. La clau pública de U serà $P_U = n_U P$. Suposem que l'usuari A vol enviar el missatge m xifrat a l'usuari B:

- A tria a l'atzar un nombre $k \in \mathbb{Z}/p$,
- calcula P_m, el punt de la corba associat al missatge m,
- xifra P_m com a $C = E_B(P_m) = P_m + k \cdot P_B$,
- envia a B (C,kP).

B per a desxifrar el missatge haurà de fer:

- $P_m = C - n_B(kP)$,
- troba el missatge m associat al punt P_m.

5.3. Criptosistema RSA

Versió clàssica. Es basa en la funció unidireccional de la potenciació: $E_{(e,n)}(x) = x^e \pmod n$ en què $1 < x < n = pq$, $1 < e < \varphi(n)$ amb el $mcd(e,\varphi(n)) = 1$ i $d = e^{-1} \pmod{\varphi(n)}$. La robustesa del criptosistema es basa en el fet que p i q siguin nombres primers grans i, per tant, n sigui difícilment factoritzable, fet que impossibilita calcular $\varphi(n)$.

Recordeu

que la funció d'Euler $\varphi(n)$ ens dóna la quantitat de nombres primers amb n entre 1 i n. En el cas que n sigui un nombre primer $n = p$, tenim $\varphi(p) = p - 1$. En el cas que $n = p \cdot q$ és el producte de dos primers tenim $\varphi(n) = (p-1)\cdot(q-1)$.

Suposem que un usuari A vol enviar un missatge m a B. Els paràmetres públics de B són (e,n), i els privats $(p,q,\varphi(n),d)$. A haurà de seguir els passos següents:

- L'usuari A xifra m calculant $c = E_{(e,n)}(x) = x^e \pmod n$ (amb el mètode de multiplicar i elevar, per exemple),
- L'usuari A envia c a B.

Observació

Actualment no es coneix cap algorisme de factorització de complexitat menor que la subexponencial.

L'usuari B per a desxifrar el missatge c haurà de fer:

- $m = D_{(d,n)}(c) = c^d \pmod n$

Versió amb corbes el·líptiques (esquema de KMOV, 1991). En aquest esquema es representen els punts de la corba $y^2 = x^3 + ax + b$ a $\mathbb{Z}/n$ com $E_n(b)$, on $a = 0$. Per a generar la clau pública l'usuari B escollirà dos nombres primers grans (p,q) tals que $p = q = 2 \pmod 3$ i, com en l'esquema clàssic, calcularà i publicarà (e,n), en què $n = p \cdot q$ i mantindrà en secret les claus privades $(p,q,\varphi(n),d)$.

Cada vegada que A vol enviar un missatge m a B haurà de seguir els passos següents:

- L'usuari A divideix el seu missatge m en dues parts $m = (m_1,m_2)$ en què $m_1,m_2 \in \mathbb{Z}_n$.
- L'usuari A determina el valor de b a la corba de manera que $m \in E_n(b)$. Específicament, calcula $b = m_2^2 - m_1^3 \pmod n$.
- xifra el punt m calculant $c = E(m) = e \cdot m$ sobre $E_n(b)$,
- envia el text xifrat $c = (c_1,c_2)$ a B.

L'usuari B per a desxifrar el missatge c haurà de fer:

- A partir del missatge xifrat $c = (c_1,c_2)$ l'usuari B pot determinar el valor de b, ja que aquest no canvia en el procés de xifratge. Específicament, calcula $b = c_2^2 - c_1^3 \pmod n$ i construeix la corba $y^2 = x^3 + b$.
- A partir de la clau privada calcula $m = D(c) = d \cdot c$ sobre $E_n(0,b)$.

Observació

L'esquema de KMOV (Koyama, Maurer, Okamoto, Vanstone) fa servir corbes el·líptiques definides sobre $\mathbb{Z}_n$, en què $n = p \cdot q$ és el producte de dos nombres primers que es mantenen en secret. La seguretat de KMOV és la mateixa que la de l'esquema RSA. Nogensmenys, el xifratge en l'esquema KMOV és més fluix que en l'RSA; per exemple, la construcció de la corba el·líptica no es fixa, sinó que es construeix a cada nou missatge. Per a solucionar aquest inconvenient hi ha altres esquemes com el de Demytko (1993), Meyer i Müller (1996), Paillier (1999), etc.

5.4. Signatura digital

En 1991 el NIST (National Institute of Standards and Technology) va proposar el DSS (*digital signature standard*), basat en el DSA (*digital signature algorithm*) com a estàndard de signatura digital. El DSS es basa en el criptosistema ElGamal. Tot i que podem fer la traducció d'aquest sistema de signatura a les corbes el·líptiques, el que veurem és la versió anàloga al DSA, anomenada *ECDSA* (*elliptic curve digital signature algorithm*), ja que aquest ha esdevingut l'estàndard de signatura digital amb corbes el·líptiques.

Versió clàssica: DSS. Farem servir la mateixa nomenclatura que en el criptosistema ElGamal que ja hem vist anteriorment.

Vegeu també

El criptosistema ElGamal s'estudia al mòdul "Elements de criptografia".

L'usuari A vol signar un missatge m:

- A tria un nombre $k \in \mathbb{Z}/p - \{0,1,p-1\}$ a l'atzar tal que $mcd(k,p-1) = 1$ i calcula α^k,
- calcula $h(m)$, en què $h(.)$ és una funció resum,
- calcula $s \in \mathbb{Z}/(p-1)$, que verifica

$$h(m) = n_A \cdot \alpha^k + k \cdot s \pmod{(p-1)}.$$

- La signatura de m és la parella (α^k, s).

Un usuari que vulgui verificar la firma del missatge m haurà de fer:

- calcular el resum de m, $h(m)$,
- obtenir del directori públic la clau pública de A: α^{n_A},
- validar la signatura comprovant la igualtat següent:

$$\alpha^{h(m)} = (\alpha^{n_A})^{\alpha^k} \cdot (\alpha^k)^s \pmod{p}.$$

Versió clàssica: DSA. Sigui q un primer d'uns 160 bits i p un altre nombre primer d'uns 500 bits tal que $p = 1 \pmod{q}$. Sigui α un generador del subgrup cíclic d'ordre q de $(\mathbb{Z}/p)^*$. Per a cada usuari U, la seva clau privada és n_U, un nombre escollit a l'atzar amb $0 < n_U < q$, i la clau pública és $\alpha_U = \alpha^{n_U}$.
L'usuari A vol signar un missatge m:

- A tria un nombre $0 < k < q$ a l'atzar i calcula $r = (\alpha^k \pmod{p}) \pmod{q}$
- calcula el resum de m, $0 < h(m) < q$,
- calcula s, que verifica

$$h(m) + n_A \cdot r = k \cdot s \pmod{q},$$

- La signatura de m és la parella (r,s).

Un usuari que vulgui verificar la firma del missatge m haurà de fer:

- calcular el resum de m, $h(m)$,
- obtenir del directori públic la clau pública de A: $\alpha_A = \alpha^{n_A}$,
- calcular $u_1 = s^{-1}h(m)$, $u_2 = s^{-1}r \pmod{q}$,
- validar la signatura si i només si $r = \alpha^{u_1} \cdot \alpha_A^{u_2} \pmod{p}$.

Versió amb corbes el·líptiques: ECDSA. Sigui E una corba el·líptica sobre $\mathbb{Z}/p$, sigui P un punt de la corba d'ordre primer n. Cada usuari U pren a l'atzar un nombre $n_U \in [1, n-1]$ que serà la seva clau privada; la clau pública de U és $P_U = n_U P$. L'usuari A vol signar un missatge m:

- A tria un nombre $k \in [1, n-1]$ a l'atzar,
- calcula $h(m)$, en què $h(.)$ és l'algorisme SHA-1 (*secure hash algorithm*),
- calcula $kP = (x_1, y_1)$ i $r = x_1 \pmod{n}$. Si $r = 0$, llavors tornem a escollir un altre k i fem el mateix procés.
- calcula $k^{-1} \pmod{n}$,
- calcula $s = k^{-1}\{h(m) + n_A r\} \pmod{n}$. Si $s = 0$, tornem a escollir un altre k i fem el mateix procés.
- La signatura de m és la parella (r,s).

Un usuari que vulgui verificar la firma del missatge m haurà de fer:

- obtenir del directori públic la clau pública de A: $P_A = n_A P$,
- verificar que $r,s \in [1,n-1]$,
- calcular $w = s^{-1} \pmod{n}$ i el resum de m: $h(m)$,
- calcular $u_1 = h(m) \cdot w \pmod{n}$ i $u_2 = r \cdot w \pmod{n}$,
- calcular $(x_0,y_0) = u_1 P + u_2 P_A$ i $v = x_0 \pmod{n}$,
- validar la signatura si i només si $v = r$.

Seguint les recomanacions del NIST (National Institute of Standards and Technology, Digital Signature Standard, FIPS, PUB 186-2, 2000) s'hauria de verificar que l'ordre d'una corba el·líptica sobre $\mathbb{F}_p$ fos de la forma $a \cdot q$ en què q és primer i a és un enter petit; d'aquesta manera la corba no és vulnerable a l'atac Pohlig-Hellman. També és convenient que la corba no sigui supersingular ni anòmala.

O sigui que, donada una corba el·líptica, n'hauríem de calcular el cardinal i veure si satisfà les condicions anteriors. Encara que hi ha un algorisme polinòmic (Schoof, 1985) per a fer aquest càlcul, com que la seva complexitat és de l'ordre de $\log^8(p)$ per a valors gaire grans de p no és útil.

5.5. Comparació dels sistemes de clau pública

5.5.1. Seguretat

Per a arribar a un grau acceptable de seguretat l'RSA i el DSA haurien de fer servir claus de 1.024 bits, mentre que els ECC en tenen prou amb 160.

A mesura que la clau creix, augmenta la distància entre la seguretat de cada proposta. Per exemple, l'ECC a 380 bits és molt més segur que l'RSA o el DSA a 2.000 bits (de fet, per a aquesta longitud de clau, l'ECC és comparable a l'RSA de 7.600 bits).

5.5.2. Eficiència

Per a situar els nivells d'eficiència, hauríem de tenir en compte:

1) Costos computacionals, o sigui, la quantitat de computació requerida per a xifrar i desxifrar.

En cadascun dels tres sistemes, ECC, RSA, DSA, s'ha de fer un gran esforç computacional. En l'RSA es pot fer servir un exponent públic petit (tot i que s'haurien de discutir els riscos en els quals es pot incórrer) per a millorar la rapidesa en la verificació de signatures i en el xifratge, però no la generació de la signatura i el desxifratge. Tant en el DSA com en l'ECC es poden precalcular

Vegeu també

Les bases normals s'estudien al mòdul "Cossos finits".

diverses taules per a millorar el rendiment. També es poden utilitzar bases normals i òptimes per a treballar en cossos finits de la forma $\mathbb{F}_{2^m}$.

Utilitzant l'estat actual de l'art en les implementacions resulta que l'ECC és un ordre de magnitud més ràpid que l'RSA i, també, que el DSA.

2) Mida de la clau, o sigui, la quantitat de bits necessaris per a desar la parella de claus i els altres paràmetres del sistema.

La taula següent compara la mida dels paràmetres del sistema i de les claus (pública i privada) per als diferents sistemes.

Mida dels paràmetres i claus

	System parameters (bits)	Public key (bits)	Private key (bits)
RSA	2208	1088	2048
DSA	2208	1024	160
ECC	481	161	160

3) Amplada de banda, o sigui, la quantitat de bits que s'han de transmetre per a comunicar un missatge xifrat o una signatura digital.

Els tres tipus de criptosistema requereixen la mateixa amplada de banda quan es fan servir per a xifrar o signar missatges llargs. De totes maneres, quan els missatges no són llargs s'ha d'observar amb més atenció (i, de fet, aquest tipus de missatges són els que usualment són utilitzats en la criptografia de clau pública).

Per a poder fer comparacions, suposem que volem signar un missatge de 2.000 bits o xifrar un missatge de 100 bits. Les taules següents comparen les longituds de les signatures i dels missatges xifrats, respectivament.

Mida de les signatures en missatges de 2.000 bits

	Mida de la signatura (bits)
RSA	1024
DSA	320
ECC	320

Mida dels missatges de 100 bits, xifrats

	Missatge xifrat (bits)
RSA	1024
ElGamal	2048
ECC	321

En resum, el sistema ECC té una gran eficiència i, en les implementacions, això significa rapidesa, baix consum i reducció de la mida del codi transmès.

6. ECC estàndards i aplicacions

6.1. ECC estàndards

Els avenços fets en la criptografia de corba el·líptica des de la seva aparició a la dècada dels vuitanta, fins avui dia, l'han transformat en quelcom més pràctic que els esquemes proposats inicialment. Les millores introduïdes han permès la creació d'implementacions que donen la possibilitat de començar a estendre l'ús d'aquest tipus de criptografia.

Per tal de promoure la difusió de les millors tècniques conegudes i també la interoperabilitat entre aplicacions, han anat sorgint esforços per estandarditzar la criptografia de corba el·líptica. Aquest esforç ha estat liderat per la corporació Certicom*, que ha fet les principals aportacions en matèria de criptografia de corba el·líptica sobre els principals estàndards de clau pública existents.

* http://www.certicom.com

A continuació n'anomenarem alguns dels més importants i també d'altres més específics, basats en els primers.

6.1.1. Estàndards principals

Els primers fruits importants de l'esforç per estandarditzar la criptografia de corba el·líptica es tradueixen en l'adopció dels principals algorismes dins d'alguns dels estàndards més importants de criptografia de clau pública.

ANSI X9.62, X9.63

L'American National Standards Institute ha estat una de les organitzacions de pes a adoptar la corba el·líptica dins dels seus estàndards de criptografia. Els estàndards d'aquesta organització són referència directa per a serveis financers i la indústria en general.

La primera aparició de la criptografia de corba el·líptica fou en l'estàndard X9.62 amb l'adopció de l'esquema de signatura digital ECDSA (*elliptic curve digital signature algorithm*) el gener de 1999. Algunes de les característiques inicials que s'adoptaren foren una longitud mínima per a les claus de 80 bits, i l'ús de bases normals i polinòmiques sobre F_{2^m}.

Posteriorment (2000) s'amplià aquest estàndard amb l'X9.63. El nucli d'aquest estàndard està basat en l'anterior, però s'adopten alguns esquemes per a l'intercanvi de claus com ECDH (*elliptic curve Diffie-Hellman*), ECMQV (*elliptic*

curve Menezes-Qu-Vastone) o ECUM (*elliptic curve unified model key agreement*). A part d'aquests també s'introdueix l'esquema de xifratge ECAES (Bellare-Rogaway).

IEEE P1363 i P1363A

L'IEEE va incloure la criptografia de corba el·líptica en el seu estàndard de criptografia de clau pública P1363 el febrer del 2000. L'estàndard és molt general i va ser desenvolupat principalment per investigadors de Certicom (Vanstone i Menezes). En aquest es descriuen algorismes típics de criptografia de clau pública sobre corbes el·líptiques. Algunes de les característiques d'aquest estàndard són les següents:

- Suporta corbes el·líptiques sobre F_p i F_{2^m}
- Suport per a esquemes de signatura ECDSA (*elliptic curve digital signature algorithm*) i ECNR (*elliptic curve Nyberg-Rueppel*) *signature scheme*.
- Suport per a algorismes d'intercanvi de claus ECDH (*elliptic curve Diffie-Hellman*) *key agreement* i ECMQV (*elliptic curve Menezes-Qu-Vastone*) *key agreement*.

Posteriorment, en un esbós que complementa aquest estàndard, anomenat P1363A ("Standard Specifications For Public Key Cryptography: Additional Techniques") s'introdueix la possibilitat d'utilitzar l'esquema de xifratge ECIES. També, en l'esbós P1363.3 s'introdueixen els esquemes basats en la identitat fent servir *pairings*.

Vegeu també

Els *pairings* s'estudien en el mòdul "*Pairings* i les seves aplicacions".

ISO 14888, 9796-4, 15946

La International Organization for Standarization (ISO) fou una altra de les principals organitzacions per a l'estandardització que va apostar per afegir la criptografia de corba el·líptica en els seus estàndards sobre criptografia. La descripció principal de l'ús d'aquestes tècniques es fa en l'estàndard 15946 ("Cryptographic Techniques Based on Elliptic Curves"). Mentre que la primera part de l'estàndard fa una descripció general dels mètodes basats en corbes el·líptiques, la segona part i la tercera part ja introdueixen l'ús de l'esquema ECDSA per a les signatures digitals, i alguns algorismes d'intercanvi de claus (ECDH, ECMQV).

Aquesta, però, no és l'única repercussió de la criptografia de corba el·líptica sobre els estàndards de l'ISO. També podem trobar modificacions en altres estàndards sobre signatura digital, concretament en el 14888 ("Digital Signature with Appendix Part 3: Certificate-based Mechanisms") i el 9796-4 ("Digital Signature with Message Recovery, Discrete Logarithm-based Mechanisms").

FIPS 186-2

Un dels primers èxits de l'estandardització dels algorismes criptogràfics sobre corbes el·líptiques fou l'adopció d'aquesta tecnologia que va fer el National Institute of Standards and Technology (NIST). L'estàndard FIPS (*federal information processing standard*) 186-2 va ser estès el febrer del 2000 ampliant l'apartat dedicat al DSS (*digital signature standard*) per a incloure la versió de l'ECDSA especificada en l'estàndard d'ANSI X9.62.

Aquest estàndard és un punt de referència per a la comercialització de productes que continguin criptografia de corba el·líptica, ja que des de la seva creació, les agencies governamentals americanes poden comprar productes basats en aquest tipus de criptografia sense demanar permisos especials. El NIST ha inclòs també especificacions per a algorismes de criptografia de corba el·líptica en el seu document MISPC ("Minimum Interoperability Specification").

SEC 1, SEC 2, SEC 3 i SEC4

El SECG (Standards for Efficient Cryptography Group) va ser creat per l'empresa Certicom. Aquest grup fou creat per promoure estàndards de corba el·líptica i promoure la difusió dels millors mètodes per a implementar aquest tipus de criptografia. El seu principal objectiu és crear un estàndard, basat en els més importants que hi ha, però fent restriccions sobre els paràmetres que aquests demanen sobre cadascun dels esquemes de signatura, xifratge o d'intercanvi de claus que fan servir. L'objectiu d'aquestes restriccions és fer possible la interoperabilitat de les aplicacions basades en aquest estàndard amb les que es basen en qualsevol dels altres estàndards principals.

Els fruits d'aquesta organització queden reflectits en dos estàndards. El primer, recollit el 2009 en el document SEC 1 ("Elliptic Curve Criptography") fa una descripció dels esquemes permesos (ECDSA, ECDH, ECMQV i ECIES). A més, es descriuen totes les primitives criptogràfiques que es fan servir en aquests esquemes i la notació ASN1 (*abstract syntax notation one*) per tal de representar les estructures necessàries (claus, certificats, continguts xifrats, etc.) que utilitzen.

L'esquema de xifrat ECIES té una llarga història en la seva nomenclatura i ha anat patint alhora petites modificacions. El podem trobar a la literatura com a ECAES (*elliptic curve augmented encryption scheme*) o simplement com a ECES (*elliptic curve encryption scheme*). La versió definida en el document SEC 1 és la més estesa i actualitzada. Aquest esquema es basa a utilitzar criptografia simètrica per a xifrar el missatge que volem a partir d'una clau generada en el procés d'inicialització del mètode. Una vegada s'ha xifrat el missatge es transmet el contingut xifrat i es passa la clau generada utilitzant l'esquema ECDH.

En el segon document, SEC 2 ("Recommended Elliptic Curve Domain Parameters"), es fa una proposta sobre els paràmetres que cal utilitzar sobre els esquemes definits en el SEC 1 i també en altres estàndards com l'ANSI X9.63 o l'IEEE P1363. L'ús d'aquestes recomanacions augmenten en gran mesura la interoperabilitat de les aplicacions que els facin servir.

SEC 3 és sobre esquemes de signatura basats en EC amb reconstrucció parcial del missatge (ECPVS i ECAOS).

SEC 4 incorpora l'esquema de certificació de Qu-Vanstone.

RSA

Els laboratoris RSA publiquen dos documents PKCS11 i PKCS13 per a l'estandardització de l'ús de les corbes el·líptiques (generació de claus, signatures digitals, xifratge amb clau pública, etc.). L'objectiu dels dos documents és crear un nou estàndard criptogràfic a l'estil dels altres PKCS (*public key criptography standard*) desenvolupats pels Laboratoris RSA. La línia de la proposta inicial feta el gener de 1998 tenia els mateixos objectius que els del grup SECG creat per Certicom. A hores d'ara, però, no s'ha avançat més enllà de la proposta inicial de 1998 i sembla que el desenvolupament d'aquest estàndard està congelat.

NSA

L'NSA (National Security Agency) dels EUA va anunciar, el 2005, el paquet B Cryptography, que inclou la criptografia basada en corbes el·líptiques en la seguretat dels sistemes de dades dels EUA. Aquesta paquet B incorpora la col·lecció d'algorismes següents: SHA256 i SHA384 (FIPS 180-3); AES128 i AES256 (FIPS 197); ECDH (ANSI X9.63) i ECDSA (ANSI X9.62, SEc 1).

Més endavant s'ha proposat el paquet E per a sistemes incrustats (amb codis de mida petita i requisits de maquinari, potència i amplada de banda).

6.1.2. Estàndards d'aplicació

Els estàndards descrits en el subapartat anterior han estat els principals promotors de l'esforç per estandarditzar la criptografia de corba el·líptica. Tot i així, n'hi ha d'altres més específics que es basen en el treball aportat pels anteriors. La majoria d'aquestes iniciatives solen definir protocols criptogràfics basats en la criptografia de clau pública, però estan expressats de manera que l'algorisme de xifratge per utilitzar pot ser canviat mentre compleixi certes propietats. Molts d'aquests treballs han inclòs els esquemes de criptografia de corba el·líptica proposats en l'apartat anterior com a noves solucions per a optimitzar aquests protocols, sobretot en entorns en què la mida de clau no pot ser gaire gran. A continuació n'enumerarem alguns.

IETF (IPSec, TLS, S/MIME, SSH, DNSSEC)

El grup de treball de la IETF (Internet Engineering Task Force) ha adoptat també la criptografia de corbes el·líptiques en els seus estàndards. Les especificacions més importants fan referència als protocols IPSec, TLS, S/MIME, SSH i DNSSEC.

El protocol d'intercanvi de claus OAKLEY (RFC 2412), basat en l'algorisme de Diffie-Hellman, ha estat modificat per a suportar la variant ECDH sobre corbes el·líptiques. Les corbes per defecte que s'utilitzen en aquest protocol són sobre $F_{2^{155}}$ i $F_{2^{185}}$.

WAP WTLS

WTLS (*wireless transport security layer*) és la capa de seguretat per a WAP (*wireless application protocol*). Aquesta especificació ha esdevingut l'estàndard *de facto* per a proveir seguretat, integritat i autenticitat per a aplicacions de telèfons mòbils i altres petits dispositius. Els esquemes de signatura (DSA) i d'intercanvi de claus (DH) descrits en aquesta especificació han estat ampliats per a suportar ECDSA per a les signatures i ECDH per a l'intercanvi de claus. Els paràmetres utilitzats per a aquests dos algorismes segueixen els descrits en l'estàndard de l'IEEE P1363 descrit a l'apartat anterior. Aquesta especificació, juntament amb l'estàndard FIPS del NIST, demostren la voluntat per part de la indústria d'adoptar aquest tipus de criptografia.

ATM

El *security specification draft* per a xarxes ATM (*asyncronous transfer mode*) és el document que especifica els mecanismes de seguretat que poden ser aplicats sobre aquest tipus de xarxes. Entre aquests mecanismes hi ha sistemes per a garantir la confidencialitat, l'autenticitat, la integritat o el control d'accés. Alguns dels mecanismes es basen en criptografia de clau pública i, en aquests, s'ha inclòs la criptografia de corba el·líptica com a possible candidata per utilitzar.

6.2. Aplicacions de l'ECC. Targetes intel·ligents

Actualment el lloc on més s'utilitzen les noves tecnologies basades en corbes el·líptiques són:

1) Aplicacions que requereixen operacions de clau pública de manera intensiva. Per exemple, el comerç electrònic basat en Internet, etc.

2) Aplicacions que requereixen la utilització de canals amb restriccions. Per exemple, xarxes sense fil, etc.

3) Aplicacions que requereixen l'ús de targetes intel·ligents.

Totes aquestes aplicacions comparteixen que en el seu escenari sempre hem de suposar unes restriccions més severes en l'ús del processador. Comentarem, bàsicament, les aplicacions basades en targetes intel·ligents, tot i que són fàcilment extrapolables a les altres aplicacions esmentades.

El 2001, Europay, Mastercard i VISA donen a conèixer un informe tècnic sobre corbes el·líptiques, l'EMV40. En aquest s'introdueix l'ús de corbes el·líptiques en lloc d'RSA per a l'autenticació i xifratge.

La implementació d'aplicacions segures per a targetes intel·ligents presenta una sèrie d'inconvenients a causa de les restriccions existents d'aquests dispositius. Aquestes limitacions són degudes principalment a la seva disponibilitat de memòria, d'amplada de banda i de potència de càlcul.

Les targetes intel·ligents són petits dispositius portables que ofereixen a l'usuari integritat de la informació emmagatzemada al seu interior i capacitat de processament. Aquesta capacitat de processament fa que les targetes intel·ligents siguin de gran utilitat per a la implementació d'un gran nombre d'aplicacions relacionades amb el comerç electrònic, la identificació de persones, etc.

Per a la major part d'aquestes aplicacions, és necessari l'ús d'uns serveis criptogràfics que no encareixin el producte final. Aquests serveis criptogràfics són necessaris per diverses raons. En primer lloc, la targeta requereix una sèrie de característiques de seguretat que permeti la protecció de la informació sensible emmagatzemada al seu interior. En segon lloc, han de proporcionar un entorn de procés segur.

La generació d'una clau pública i privada a l'interior d'una targeta intel·ligent, i també la protecció de la clau privada al seu interior, és crítica. Per a poder proporcionar serveis criptogràfics, la clau emmagatzemada a la targeta mai no ha de ser revelada. Per aquest motiu, la targeta s'haurà de autoprotegir fent ús dels seus serveis criptogràfics.

6.2.1. Restriccions de les targetes intel·ligents

Implementar criptografia de clau pública en aplicacions basades en targetes intel·ligents representa un gran repte, en part per les restriccions d'implementació que aquests dispositius requereixen (memòria molt reduïda i capacitat de càlcul molt limitada).

La major part de targetes intel·ligents disponibles avui dia en el mercat disposen d'una memòria RAM al voltant de 1.024 bytes, d'uns 16 quilobytes de memòria EPROM i d'uns 24 quilobytes de memòria ROM. La seva capacitat de processament és també molt reduïda. Normalment, trobarem CPU de 32 bits a una freqüència d'uns 5 megahertzs.

Finalment, la velocitat de transmissió d'aquestes targetes és també molt limitada. Per a aconseguir una velocitats d'aplicació acceptables, la informació transmesa per la targeta hauria de ser la mínima necessària.

6.2.2. Avantatges de l'ECC

Els avantatges de la utilització de l'ECC per a la construcció dels serveis criptogràfics necessaris per a targetes intel·ligents són bàsicament el següents:

- **Mínims requisits de memòria i de taxa de transmissió**. La utilització de l'ECC permet reduir la mida de les claus i dels certificats. Això es tradueix en una reducció de la memòria necessària per part de la targeta intel·ligent. Per altra banda, també permet una reducció en les dades que s'han de transmetre entre targeta i aplicació. Per aquest motiu, la taxa de transmissió necessària es redueix considerablement.

- **Escalabilitat**. Les aplicacions basades en targetes intel·ligents requereixen un nivell de seguretat bastant elevat (amb la qual cosa, la longitud de les claus augmenta considerablement). La criptografia de corbes el·líptiques pot proporcionar un nivell de seguretat semblant destinant menys recursos per a aconseguir-ho. Això significa que amb l'ús de l'ECC, les targetes intel·ligents poden proporcionar un nivell de seguretat molt elevat sense necessitat d'incrementar el seu cost de producció.

- **No requereix coprocessadors**. La major part de dispositius que ofereixen criptografia de clau pública requereixen un component de maquinari conegut com a *criptocoprocessador* per a donar suport als intensos càlculs que el sistema ha de fer. Aquest component de maquinari addicional no només redueix l'espai disponible a la targeta sinó que incrementa el seu cost d'un 20 a un 30%.

  La naturalesa dels càlculs necessaris per a implementar l'ECC, amb uns temps de processament bastant reduïts, no requereixen aquest coprocessador. Per tant, els algorismes necessaris poden ser implementats a la ROM de la targeta, sense necessitat d'un maquinari addicional.

- **Generació de claus interna**. La clau privada d'una parella de clau pública ha de romandre emmagatzemada de manera secreta. A més, per a garantir un no-repudi autèntic, la clau privada hauria de ser completament inaccessible per a terceres parts.

  Amb la utilització d'altres algoritmes, la introducció de claus dins de la targeta s'ha de fer de manera personalitzada en un entorn segur. A causa de la complexitat dels càlculs necessaris, la generació de claus dins de la targeta mateixa és ineficient i generalment impracticable.

Utilitzant ECC s'aconsegueix que el temps necessari per a generar una parella de claus sigui tan reduït que fins i tot dispositius de característiques de càlcul tan modestes com les targetes intel·ligents poden generar aquesta parella. Això significa que el procés de personalització pot ser evitat en aquelles aplicacions en què el no-repudi sigui realment important.

6.2.3. Conclusions

Les targetes intel·ligents tenen unes restriccions d'implementació molt rígides a causa de les seves limitacions de càlcul, els paràmetres d'emmagatzemament i les taxes de transferència. Com a resultat d'aquestes restriccions, implementar un sistema de clau pública amb targetes intel·ligents requereix l'ús de targetes intel·ligents de més alt nivell, amb més capacitat d'emmagatzemament i amb coprocessador criptogràfic.

La reducció de mida de clau i de certificats que ofereix l'ús d'ECC per a construir sistemes de clau pública ofereix uns avantatges inqüestionables per a la implementació d'aplicacions segures per a targetes intel·ligents.

Exercicis d'autoavaluació

1. Donada la cònica $x^2 + xy + y^2$ sobre $\mathbb{F}_2$, calculeu-ne el punts racionals.

2. Donada la cònica $x^2 + xy + y^2$ sobre $\mathbb{F}_8$, calculeu-ne el punts racionals.

3. Donada la corba $y^2 = x^3 + 3x + 2$ sobre $\mathbb{F}_{23}$ i dos punts d'aquesta $P = (16,11), Q = (8,20)$, calculeu $P + Q$, $2P$, $4P$.

4. Donada la corba $y^2 + xy = x^3 + \alpha x^2 + 1$ sobre $\mathbb{F}_4$.
a) Comproveu que no té punts singulars.
b) Doneu un punt P de la corba. Per exemple, fixeu un valor per a x (com exemple $x = 0$) i llavors resoleu l'equació quadràtica resultant per veure si trobem un valor per a y (en el nostre exemple, $y^2 = 1$).

5. Donada la corba $y^2 + xy = x^3 + \alpha x^2 + \alpha$ sobre $\mathbb{F}_4$.
a) Comproveu que no té punts singulars.
b) Doneu un punt P de la corba.
c) Calculeu l'ordre del punt P. O sigui, calculeu el mínim a, tal que $aP = 0$, en què 0 és el punt de l'infinit.
d) Podem saber quants punts té la corba, utilitzant els teoremes que coneixeu?

6. Implementeu usant el SAGE el sistema criptogràfic ElGamal sobre corbes el·líptiques. Useu un nombre primer de més de 10 xifres i xifreu el text

'Xifrar amb ElGamal el·líptic fa difícil el desxifratge.'

tot i ensenyant el text en clar i el text xifrat.

El mètode de codificació serà una variant deguda a Menezes i Vanstone coneguda com a MV-ElGamal. Un punt P d'ordre gran i la corba E són informació pública. La clau privada és un enter n_U més petit que l'ordre de P i la clau pública és $P_U = n_U P$. El missatge m el dividirem en dos blocs mòdul p, o sigui, $(m_1,m_2) \in \mathbb{F}_p \times \mathbb{F}_p$. La funció de xifratge està determinada per

$$E_U(m) = (rP, c_1, c_2) \in E \times P \times P,$$

en què r és un nombre aleatori, $(x,y) = rP_U$ i $c_1 = xm_1 \pmod p$, $c_2 = ym_2 \pmod p$. Suposarem que $x,y \neq 0$ i, en cas contrari cercarem un altre valor de r.

La funció de desxifratge corresponent és:

$$D_U(C,c_1,c_2) = (c_1x^{-1}, c_2y^{-1}), \text{ en què } (x,y) = n_U C.$$

Solucionari

1) Els únics punts de la corba poden ser (0,0),(0,1),(1,0),(1,1). Només cal provar quins valors satisfan l'equació i veure que els punts racionals són (0,1),(1,0),(1,1).

2) El problema, ara, no és tan senzill com l'anterior. Si en el cos hi ha molts elements no podem pas anar-los provant tots d'un en un. Podem fer com en l'exemple 1.5.

Suposem que el cos finit l'hem construït utilitzant el polinomi primitiu x^3+x+1. Ja sabem de l'exercici anterior que (0,1) és un punt de la corba. L'eix de rectes que passen per aquest punt és $Ax + By + C = 0$. Donant valors en el punt (0,1) obtenim $B + C = 0$, o sigui, $B = C \neq 0$ (si B i C fossin zero la recta seria $x = 0$ i no passaria pels altres punts que coneixem (els (1,0)*i*(1,1)). Llavors si tallem aquesta recta amb la corba inicial obtenim els punts que cerquem, o sigui, les solucions del sistema d'equacions:

$$\begin{cases} Dx + y + 1 &= 0 \\ x^2 + xy + y^2 + 1 &= 0 \end{cases}$$

Resolent aquest sistema obtenim: $x = \frac{1}{D^2+D+1}$; $y = \frac{D^2+1}{D^2+D+1}$ i, en anar donant valors a $D \in \mathbb{F}_8$ obtenim les vuit solucions (1,0); (1,1); (α^2,α); (α,α^2); (α^4,α); (α,α^4); (α^2,α^4); (α^4,α^2) que, juntament amb la solució inicial (0,1) dóna els nou punts racionals que cercàvem.

3) $2P = (20,14)$, $4P = (19,15)$, $P + Q = (15,8)$.

4)

a) Efectivament, l'únic punt singular seria (0,0), que no pertany a la corba.

b) Fixem $x = \alpha$. Llavors obtenim $y^2 + \alpha y + 1 = 0$, que no té solució. Això vol dir que no hi ha cap punt a la corba de la forma $P = (\alpha,?)$.

Si anem cercant altres possibles punts, arribarem a la conclusió que només hi ha solucions quan $x = 0$, que és un valor que té dues solucions. En el projectiu escriuríem les solucions com a (0,1,0) i (0,1,1).

5)

a) Efectivament, l'únic punt singular seria (0,0), que no pertany a la corba.

b) Fixem $x = \alpha^2$. Llavors obtenim $y^2 + \alpha^2 y = 0$, que té dues solucions (α^2,0) i (α^2,α^2).

c) Comencem pel punt $P = (\alpha^2,0)$ i calculem $2P = (\alpha^2,\alpha^2)$, $3P = 0$. L'ordre del punt P és 3.

d) Segons el teorema de Hasse el nombre de punts de la corba és $1 \leq N \leq 9$. Segons el teorema 3.1, com que l'ordre del punt P és 3, $3|N$. O sigui, que N pot ser 3, 6 o 9. Però coneixem més punts a part de P, $2P$, $3P$ (per exemple, (α^2,α^2)). O sigui, que $N \in \{6,9\}$. Per a acabar de calcular N necessitem calcular algun altre punt.

6) Començarem per cercar un nombre primer de més de 10 dígits i definir una corba el·líptica sobre el cos finit $\mathbb{F}_p$. També agafarem un punt P (fàcil de calcular) sobre aquesta corba.

```
sage: p= next_prime(10^10+10^8+10^5+1)
sage: E = EllipticCurve(GF(p),[1975,4])
sage: P = E([0,2])
sage: print p
sage: print(E.cardinality())
sage: print P.additive.order()
10100100007
10100137808
1262517226
```

La corba és $E : y^2 = x^3 + 1975x + 4$ i l'ordre del punt P és prou alt.

Les funcions de xifratge i desxifratge les podríem definir com:

```
def cipher(PU ,m1 ,m2):
    x=0,y=0
    while ((x==0) or (y==0)):
        r = floor(p*random())
        x = (r* Kpub)[0]
        y = (r* Kpub)[1]
    return r*P, m1*x, m2*y
```

```
def uncipher(NU ,ciph):
    x = (NU*ciph[0])[0]
    y = (NU*ciph[0])[1]
    return ciph[1]*x^(-1), ciph[2]*y^(-1)
```

Per a veure'n el seu funcionament agafem, per exemple, com a clau privada $n_U = 10000$:

```
sage: private_key = 10000
sage: public_key = private_key*P
sage: cipher(public_key,999,1999)
((5871087149 : 8478284639 : 1), 571107865, 7072444218)

sage: uncipher(private_key,cipher(public_key,999,1999))
(999,1999)
```

Podem convertir un text de caràcters en enters:

```
def codificar(text):
    valor_numeric = 0
    for c in text:
        valor_numeric = 256* result + ord(c)
    return valor_numeric
```

I, al revés, per a convertir un nombre en un text alfabètic:

```
def descodificar(nombre):
    nombre = Integer(nombre)
    text = ''
    for i in nombre.digits(256):
        text = chr(i) + text
    return text
```

Finalment, com que estem codificant/descodificant utilitzant el codi ASCII, per a la taula que ens demanen, hem de fer blocs en el text que no superin $log_{256}p$ caràcters.

```
text = 'Xifrar amb ElGamal elliptic fa dificil el dexifratge'
L=len(text)
k = floor(log(p,256))
NU = 10000
for i in range(0,L,2*k):
    t1 = text[i:i+k]
    m1 = codificar(t1)
    t2 = text[i+k:i+2*k]
    m2 = codificar(t2)
    textciph = cipher(NU*P,m1,m2)
    d1 = descodificar(uncipher(NU,textciph)[0])
    d2 = descodificar(uncipher(NU,textciph)[1])
    print d1+d2 , m1 ,m2, textciph, t1+t2
```

Aquest és el resultat. A la primera columna el text per xifrar. A la segona i tercera columnes el text codificat (m_1,m_2). A la quarta columna els valors xifrats. I a la cinquena columna el resultat de desxifrar.

Xifrar a	1483302514	1634869345	((9885468744 : 4672391911 : 1), 2619907688, 3690218101)	Xifrar a
mb ElGam	1835147333	1816617325	((5688334248 : 4646987141 : 1), 7964174488, 783430096)	mb ElGam
al ellip	1634476133	1819044208	((510285904 : 6896899989 : 1), 2343178415, 1637076365)	al ellip
tic fa d	1953063712	1717641316	((7012185169 : 1401052502 : 1), 645047635, 3222657121)	tic fa d
ificil e	1768319331	1768693861	((9603283989 : 6128947821 : 1), 2957872999, 9337401495)	ificil e
l dexifr	1814062181	2020173426	((7403725707 : 3526027318 : 1), 3827147844, 3922674600)	l dexifr
atge	1635018597	0	((132470872 : 9797171507 : 1), 9963732301, 0)	atge

Bibliografia

Blake, I.; Seroussi, G.; Smart, N. (2000). "Elliptic Curves in Cryptography". *London Mathematical Society Lecture Note Series* (núm. 265). Cambridge: Cambridge U. Press.

Fulton, W. (1969). *Algebraic Curves. An Introduction to Algebraic Geometry*. Nova York: Benjamin Inc. (Versió en castellà: *Curvas algebraicas* (1972). Barcelona: Ed. Reverte.)

Hankerson, D.; Menezes, A.; Vanstone, S. (2004). *Guide to Elliptic Curve Cryptography*. Nova York: Springer-Verlag.

Koblitz, N. (2004). "Algebraic Aspects of Cryptography". *Algorithms and computations in Mathematics* (vol. 3). Berlin, Heidelberg, Nova York: Springer-Verlag.

Menezes, A. (1993). *Elliptic Curve Public Key Cryptosystems*. Massachusetts: Kluwer Academic Publishers, Norwell.

Silverman, J. H. (1986). "The Arithmetic of Elliptic Curves". *Graduate Texts in Mathematics* (núm. 106). Nova York: Springer-Verlag.

Washington, L. C. (2008). "Elliptic Curves: Number Theory and Cryptography". *Discrete Mathematics and its Applications*. Nova York: Chapman & Hall/CRC.