UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

CRIPTOLOGIA BASADA EN CORBES EL·LÍPTIQUES

Autor: Néstor Dougàs Chavarria

Director: Dr. Xavier Guitart Morales
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 19 de gener de 2020

Abstract

Cryptology is the branch of mathmatics that studies secret comunication. This end of grade work deals with the concept of cryptology. To be more precise, we will study the cryptology that is based on elliptic curves. This is the reason why we include a previous study of elliptic curves, focusing on the elliptic curves over finite fields. Finally we will study the aplications of the elliptic curves over finite fields in criptology.

Resum

La criptologia és la branca de les matemàtiques que estudia a l'escriptura secreta. En aquest treball ens introduirem en el concepte de la criptologia, més concretament, en la que és basada en corbes el·líptiques. Per això farem un estudi de les corbes el·líptiques, centrant-nos en les corbes el·líptiques sobre cossos finits. Finalment estudiarem l'aplicació d'aquestes últimes a la criptologia.

Índex

1 Introducció

Es pot definir etimològicament la Criptologia, del grec "kryptos" (amagat, ocult) i "logos" (paraula, estudi) com l'estudi de les "escriptures secretes". Aquest concepte general, entès aquí com "disciplina de l'àmbit de les matemàtiques i la informàtica" s'ha de posar en relació amb la nostra realitat, cada vegada més digitalitzada. Fins al punt que la informàtica intervé en multitud d'accions quotidianes com ara enviar un missatge, comprar un producte o buscar feina. Per això, mantenir la seguretat ha esdevingut una preocupació fonamental i, en aquest àmbit, les matemàtiques són cabdals. Si les eines que possibiliten aquesta seguretat són matemàtiques, paradoxalment també els atacs que rep es basen en algoritmes matemàtics. Aquesta és l'objectiu d'aquest treball, estudiar les eines matemàtiques utilitzades actualment en criptologia a fi i efecte d'entendre, des d'un punt de vista matemàtic, els algoritmes que fan possible la seguretat i els que vehiculen els atacs de tercers per a vulnerar-la. Al llarg d'aquest treball, en la primera secció, definirem què és la criptologia tot centrant-nos en la criptologia asimètrica, que és la que s'utilitza actualment. Seguidament estudiem el concepte de logaritme discret i la seva aplicació en la criptologia asimètrica, focalitzant en els algoritmes d'encriptació basats en el logaritme discret i els algoritmes per a trencar la seva seguretat. Tot això ens durà a intuir la importància de les corbes el·líptiques en la criptologia. En la segona secció presentem un estudi introductori sobre corbes el·líptiques. Començarem parlant de la seva estructura de grup, sense el qual les corbes el·líptiques no tindrien interès matemàtic. També veurem diverses propietats dels seus endomorfismes i els seus punts de torsió, les quals resultaran claus per a la següent secció. Conjuntament amb els punts de torsió també veurem l'aparellament de Weil, el qual utilitzarem en l'última secció del treball. Tot seguit, en la tercera secció, centrarem el nostre estudi en les corbes el·líptiques sobre cossos finits, ja que aquestes corbes són les utilitzades en criptologia. Demostrarem el Teorema de Hasse i veurem la seva importància, també veurem l'algoritme de Schoff, sense el qual no es podria fer criptologia actualment. Acabada aquesta secció, tindrem totes les eines necessàries per a fer criptologia basada en corbes el·líptiques. Finalment, aplicant els conceptes explicats en les seccions anteriors, passarem a la criptologia basada en corbes el·líptiques pròpiament dita. Parlarem dels problemes pràctics que hem de solucionar per a configurar els criptosistemes i d'un algoritme aplicat només a aquest tipus de criptologia, que utilitza l'aparellament de Weil.

2 Introducció a la Criptologia

2.1 Elements d'un criptosistema

La criptografia, o ciència que estudia les comunicacions xifrades, és l'estudi dels mètodes per enviar missatges entre usuaris de manera confidencial. El seu objectiu és fer els missatges inintel·ligibles per a destinataris no desitjats i així garantir la seguretat de la informació que es vulgui transmetre. D'altra banda, els usuaris no autoritzats o atacants disposen de tècniques per a llegir aquests missatges. L'estudi d'aquestes tècniques s'anomena criptoanàlisi. Anomenem criptologia al conjunt format per la criptografia i el criptoanàlisi.
L'èxit d'un sistema de criptoanàlisi obliga a enfortir els sistemes criptogràfics coneguts i, de la mateixa manera, la conseqüència d'una millora de la criptologia condueix a la necessitat de trobar mètodes de criptoanàlisi més potents. La criptologia és una ciència viva.

La criptologia té una forta relació amb les matemàtiques, doncs les tècniques utilitzades actualment, tant en els algoritmes d'encriptació com les tècniques de criptoanàlisi, utilitzen una gran quantitat de càlculs i enginy matemàtic. A més, un missatge entre usuaris no ha de ser necessàriament un conjunt de paraules o un conjunt de frases. De fet, actualment els missatges són nombres, conjunts de nombres o bits d'un nombre en format binari. Aquests poden servir per a definir una clau d'autentificació, una firma electrònica o enviar un missatge alfabetitzat utilitzant una correspondència lletra-nombre, per exemple la correspondència $(0- > a, 1- > b, ..., 25- > z)$ en l'alfabet català.
Actualment la ciència de la criptologia és considerada una branca de les matemàtiques.

Per tal de començar el nostre estudi, haurem d'introduir el concepte de *criptosistema*.

Definició 2.1. *Un criptosistema és una terna (M, X, C) tal que M és el conjunt de missatges originals, X és el conjunt de missatges xifrats i C es un conjunt finit de claus, junt amb dos funcions:*

$$c : M \times C \longrightarrow X \ i \ d : X \times C \longrightarrow M$$

tals que $d(c(m, c), c) = M$ per tot $(m, c) \in M \times C$.

Ara ens cal distingir els sistemes criptogràfics en dos tipus: els simètrics i els asimètrics. En la criptografia simètrica, també anomenada criptografia de clau privada, els dos usuaris comparteixen una clau secreta que els permet fer l'encriptat i el desencriptat. D'altra banda, en la criptografia asimètrica, també anomenada criptografia de clau pública o criptografia de dos claus, cada individu té una pública i una privada. La clau pública és utilitzada per xifrar el missatge i la clau privada per desxifrar-lo.

Aquest treball dedicarà el seu estudi a la criptografia de clau asimètrica.

2.2 Criptografia asimètrica

La criptografia asimètrica va ser introduïda l'any 1976 per Whitfield Diffie i Martin Hellman. El seu principal objectiu és permetre a 2 usuaris intercanviar informació confidencial encara que no s'hagin vist abans. Aquest tipus de criptografia és la que s'utilitza actualment i es basa en funcions matemàtiques fàcilment computables amb inverses que requereixen una gran quantitat d'operacions i temps per obtenir-les. D'aquesta manera, a la pràctica, els missatges transmesos es fan inaccessibles per a usuaris no autoritzats. El missatge xifrat és enviat de manera que qualsevol usuari pot rebre-la però només l'emissor i el receptor poden obtenir el missatge original.

El criptosistema de clau asimètrica més conegut és el criptosistema RSA:

Criptosistema RSA

Pren el nom RSA per les inicials dels seus creadors, Ron Rivest, Adi Shamir i Len Adleman, que el van proposar l'any 1979. Es basa en la difícil factorització de nombres enters grans. El sistema és el següent:

1. S'escullen 2 nombres primers, p i q. En el moment d'escriure aquest text, per assegurar la seguretat, p i q són de l'ordre de 10^{300}.

2. Es calcula $n = p \cdot q$.

3. Sent ϕ la funció d'Euler (on $\phi(n)$ indica el nombre de divisors de n), es calcula $\phi(n) = (p-1)(q-1)$, utilitzant les propietats següents:

- Si p és primer, llavors $\phi(p) = p - 1$.

- Si m i n són coprimers, llavors $\phi(mn) = \phi(m)\phi(n)$.

4. S'escull un enter $e \leq \phi(n)$, coprimer amb $\phi(n)$, el qual es donarà a conèixer.

5. Es determina d tal que $e \cdot d \equiv 1 \pmod{\phi(n)}$, amb l'algoritme d'Euclides.

Aleshores, la clau pública és el parell (n, e) i la clau privada és (n, d). Llavors, si l'usuari 2 vol enviar un missatge M a l'usuari 1 es segueix el següent procediment:

1. L'usuari 2 converteix M en m, on m és un nombre enter menor a n tal que $(m, n) = 1$. La conversió de M a m haurà de ser reversible i el mètode de conversió haurà de ser pactat amb antelació pels els dos usuaris.

2. L'usuari 2 envia $c = m^e \pmod{n}$ a l'usuari 1.

3. L'usuari 1 calcula $m = c^d = (m^e)^d = m^{ed} \equiv m^{1+k\phi(n)} \pmod{n} = m(m^{\phi(n)k}) \equiv m \pmod{n}$.

2.3 Criptosistemes basats en el problema del logaritme discret

Existeix una altra categoria de criptosistemes els quals es basen en la dificultat de trobar la solució al problema del logaritme discret, el qual descriurem a continuació.

Definició 2.2. *Sigui $G = \langle g \rangle$ un grup finit cíclic generat per g amb l'operació *. Sigui y un element de G, llavors el logaritme discret de y en la base g és qualsevol nombre enter x tal que $g^x = y$. Trobar aquest enter x és resoldre el problema del logaritme discret i escrivim $x = \log_g y$.*

Observació 2.3. G pot ser qualsevol grup cíclic, normalment s'utilitza el grup multiplicatiu $\mathbf{F}_q^*$ d'el cos finit $\mathbf{F}_q$, on q és una potència d'un nombre primer, o el grup de punts d'una corba el·líptica, el qual veurem més en detall durant el transcurs d'aquest treball.

Observació 2.4. La seguretat dels criptosistemes depenen del grup escollit, doncs els algoritmes de criptoanàlisi no són sempre aplicables a tots els grups i la seva eficàcia també varia segons el grup escollit. Per raons que veurem més endavant, el grup més segur actualment és el de punts d'una corba el·líptica. D'altra banda, hi ha grups cíclics que no garanteixen seguretat. Per exemple, si el $G = (\mathbf{Z}/n\mathbf{Z}, +)$, llavors 1 genera el grup amb l'operació de la suma d'enters. Llavors, trobar x tal que $y = 1^x$ és trivial, doncs $1^x = (1 + ... + 1) = x$, per tant $x = y$.

Seguidament veurem alguns dels mètodes criptogràfics basats en el logaritme discret:

L'intercanvi de claus de Diffie-Hellman:

Va ser proposat per Whitfield Diffie i Martin Hellman l'any 1976.

Sigui G un grup finit cíclic d'ordre n i g un generador dels elements de G.

1. La clau pública és el parell (n, g).

2. L'usuari 1 escull un nombre natural aleatori a tal que $1 < a < n - 1$ i envia g^a a l'usuari 2. Veiem que que és recomanable que a no sigui igual a 0,1,$n - 1$ o n ja que $g^1 = g^n = g$ i $g^0 = g^{n-1} = 1$.

3. L'usuari 2 escull un nombre natural aleatori b tal que $1 < b < n$ i envia g^b a l'usuari 1.

4. L'usuari 1 calcula $(g^a)^b := m$ i l'usuari 2 calcula $(g^b)^a = m$. Aleshores m és la clau secreta.

Observem que, igual que en els següents criptosistemes, en cap moment ha sigut necessari que els dos usuaris es comuniquin secretament entre sí i que sabent n i g es fa difícil trobar m, ja que cal calcular un logaritme discret.

El criptosistema de Massey-Omura:

Va ser proposat per James Massey i Jim K.Omura l'any 1982.

Sigui G un grup finit (no necessàriament cíclic) d'ordre n i $m \in G$ el missatge que es vol enviar.

1. L'usuari 1 escull un enter c i calcula $x = m^c$ i ho envia a l'usuari 2.

2. L'usuari 2 escull un enter d i calcula $y = x^d$ i ho envia a l'usuari 1.

3 L'usuari 1 envia $z = y^{c^{-1}}$ a l'usuari 2. Aquí c^{-1} és l'enter tal que $cc^{-1} \equiv 1 \pmod{n}$, i així $z = y^{c^{-1}} = x^{dc^{-1}} = m^{cdc^{-1}} = m^d$.

4. Finalment, l'usuari 2 calcula $z^{d^{-1}} = m$ i així troba m.

Observem que aquí no resolem ben bé el problema del logaritme discret, sinó el de trobar g tal que $g^x = y$, sabent x i y.

El criptosistema d'ElGamal:

Va ser proposat per Taher ElGamal l'any 1985.

Sigui G un grup finit cíclic d'ordre n, g un generador dels elements de G, a la clau secreta de l'usuari 2 i g^a la seva clau pública. Sigui $m \in G$ el missatge que es vol enviar. Aquest criptosistema té dos fases, corresponents als dos usuaris.

1.1. L'usuari 1 escull un enter k tal que $1 < k < n-1$.

1.2. L'usuari 1 calcula $g^{ak} = (g^a)^k$ i envia el parell (g^k, mg^{ak}) a l'usuari 2.

2.1. L'usuari 2 calcula $g^{ak} = (g^k)^a$.

2.2. L'usuari 2 troba $m = (mg^{ak})(g^{ak})^{-1}$, on $(g^{ak})^{-1}$ és l'element de G tal que $g^{ak}(g^{ak})^{-1} = e_G$.

Una manera d'optimitzar la segona fase és evitar haver de calcular l'invers de g^{ak}. Llavors, es podrien fer els passos següents:

2.1. L'usuari 2 calcula $(g^k)^{n-a}$.

2.2. L'usuari 2 troba $(g^k)^{n-a}mg^{ak} = mg^{kn-ka+ak} = mg^{kn} = m(g^n)^k = m(1^k) = m$.

2.4 Atacs al logaritme discret

Per tal d'intentar trencar la seguretat dels criptosistemes esmentats a la secció anterior i així accedir a la informació confidencial cal resoldre el problema del logaritme discret. Un atac al logaritme discret és un algoritme criptoanalític que té com a resultat la solució al problema del logaritme discret. El primer atac que podem pensar és l'atac a força bruta, el qual es basa en intentar provar valors de x fins que ens surt el y buscat. Òbviament l'atac no és gens eficient. Per això, estudiarem altres atacs millors.

Algoritme de Shanks "Baby step-Giant step"

Aquest algoritme va ser ideat per Daniel Shanks i el nombre d'operacions que es necessiten és de l'ordre de $O(\sqrt{n})$ i la quantitat de memòria necessària també és de l'ordre de $O(\sqrt{n})$, on n és l'ordre del grup.

Sigui $G = \langle g \rangle$ un grup cíclic d'ordre n. Sigui y un element de G i volem trobar x tal que $g^x = y$.

1. Sigui $m = [\sqrt{n-1}]$ on [ ] indica la part entera.

2. Calculem $\alpha_0 = e_G$, $\alpha_1 = g^m$, $\alpha_2 = g^{2m}$,..., $\alpha_{m-1} = g^{(m-1)m}$. Els α's s'han de guardar. Aquest és l'anomenat "Baby step".

3. Calculem $\beta_0 = y$, $\beta_1 = yg^{-1}$, $\beta_2 = y(g^{-1})^2$,..., fins a trobar un $\beta_i = \alpha_j$ per algun j. Aquest és l'anomenat "Giant step".

4. Si $\beta_i = \alpha_j$ llavors $g^{jm} = yg^{-i}$ i per tant $g^{jm+i} = y$ i $x = jm + i$.

Observació 2.5. Veiem que sempre existeix un i adequat ja que $x < n = qm + r$, per definició de divisió entera. Per tant $0 \leq q < m$ (ja que $x < n \leq m^2$) i $0 \leq r < m$. Aleshores tot element $y \in G$ es pot expressar com $y = q_1 m + r_1$ on $0 \leq q_1 \leq q$ i $0 \leq r_1 \leq r$. També notem que hem fet $m = [\sqrt{n-1}]$ càlculs en el Baby Step i, com a màxim, $m-1 = [\sqrt{n-1}] - 1$ càlculs en el Giant Step. Per tant, efectivament, el nombre d'operacions que

es necessiten és de l'ordre de $O(\sqrt{n})$ i la quantitat de memòria necessària també és de l'ordre de $O(\sqrt{n})$.

Exemple 2.6. Suposem que $G = \mathbf{Z}_{23}$ i volem trobar $x \in G$ tal que $7^x = 5$.

1. $m = [\sqrt{23-1}] = 4$.
2. $\alpha_0 = 1$, $\alpha_1 = 7^4 \equiv 9 \pmod{23}$, $\alpha_2 = 7^{2\cdot 4} \equiv 12 \pmod{23}$, $\alpha_3 = 7^{3\cdot 4} \equiv 16 \pmod{23}$.
3. Veiem que $7 \cdot 10 \equiv 1 \pmod{23}$, per tant $7^{-1} \equiv 10 \pmod{23}$.
4. $\beta_0 = 5$, $\beta_1 = 5 \cdot 10 \equiv 4 \pmod{23}$, $\beta_2 = y(g^{-1})^2 = 5 \cdot 10^2 \equiv 17 \pmod{23}$, $\beta_3 = y(g^{-1})^3 = 5 \cdot 10^3 \equiv 9 \pmod{23} \equiv 7^4$. Per tant, $x = 1 \cdot 4 + 3 = 7$.

Algoritme ρ (*rho*) de Pollard

Aquest algoritme va ser publicat per John Pollard l'any 1978 i el nombre d'operacions que es necessiten és de l'ordre de $O(\sqrt{n})$ on n és l'ordre del grup. Aquest mètode necessita aproximadament el mateix nombre d'operacions que el Baby step-Giant step, però necessita menys memòria. Cal remarcar que existeix un algoritme ρ de Pollard per a factoritzar nombres enters.

Sigui $G = \langle g \rangle$ un grup cíclic d'ordre n. Sigui y un element de G i volem trobar x tal que $g^x = y$.

La idea és escollir una funció $f : G \longrightarrow G$ que doni valors pseudoaleatoris, després començar amb un element aleatori g_0 i anar calculant $g_{i+1} = f(g_i)$. En cas que trobem $i_0 < j_0$ tals que $g_{i_0} = g_{j_0}$ llavors

$$g_{i_0+l} = f^l(g_{i_0}) = f^l(g_{j_0}) = g_{j_0+l}$$

així que podem trobar altres punts $i_1, ..., i_n$ que compleixin aquesta relació. Utilitzant la forma de f, la qual haurem escollit adequadament, trobarem x mòdul n/d, on d és un divisor de n.

Per tal d'estalviar memòria, els únics valors que es guardaran són els parells (g_i, g_{2i}) i es calculen els següents

$$(g_{i+1}, g_{2(i+1)}) = (f(g_i), f(f(g_{2i})))$$

descartant llavors (g_i, g_{2i}). Veiem que així la quantitat de memòria necessària és molt baixa, ens fa falta veure que, per algun i, $g_i = g_{2i}$. Suposem que $g_{i_0} = g_{j_0}$, $i \geq i_0$ i que i és un múltiple de $j_0 - i_0$, llavors els índexs $2i$ i i difereixen per un múltiple de $j_0 - i_0$, per tant $g_i = g_{2i}$.

Ara exposarem el mètode original proposat per Pollard, tot i que algunes millores han estat proposades amb el temps.

Primer es realitza una partició en G en tres subconjunts disjunts $G = S_1 \cup S_2 \cup S_3$ de manera que el neutre del grup no pertanyi a S_2 amb S_1, S_2, S_3 aproximadament de la mateixa mida. Aleshores, es defineix la successió (x_k, a_k, b_k) a $G \times \mathbf{Z}_n \times \mathbf{Z}_n$ inductivament de la manera següent:

$$(x_0, a_0, b_0) = (e_G, 0, 0), \qquad (x_{i+1}, a_{i+1}, b_{i+1}) = \begin{cases} (yx_i, a_i, b_i + 1) & \text{si } x_i \in S_1 \\ (x_i^2, 2a_i, 2b_i) & \text{si } x_i \in S_2 \\ (gx_i, a_i + 1, b_i) & \text{si } x_i \in S_3 \end{cases}$$

La successió està feta de forma que per a cada $i \in \mathbf{N}$ es té $x_i = g^{a_i} y^{b_i}$. Llavors, si

trobem $i_0 < j_0$ tal que $g^{a_{i_0}} y^{b_{i_0}} = g^{a_{j_0}} y^{b_{j_0}}$, aleshores tenim que $g^{a_{i_0}-a_{j_0}} = y^{b_{j_0}-b_{i_0}}$ i $g^x = y$ i per tant

$$(a_{i_0} - a_{j_0})(b_{j_0} - b_{i_0})^{-1} \equiv x \pmod{n}.$$

Per tant d'aquesta manera trobem el valor de x mòdul $n/((b_{i_0} - b_{j_0}), n)$. Així, trobant x mòdul $n/((b_{i_0+l} - b_{j_0+l}), n)$ per diversos valors de l i després aplicant el teorema xinès del residu trobem x mòdul n.

Veiem que el temps que necessitem per a resoldre el problema depèn en gran part de la sort que tinguem. Edlyn Teske va provar empíricament que el nombre d'operacions necessàries és aproximadament $1,37\sqrt{n}$.

Algoritme de Pohlig-Hellmann

Aquest algoritme va ser publicat per Stephen Pohlig i Martin Hellman l'any 1978 tot i ser descobert de manera independent per Roland Silver, per això a vegades és anomenat *Silver-Pohlig-Hellman*. L'algoritme es pot aplicar si l'ordre del grup n té divisors primers petits.

Sigui $G = \langle g \rangle$ un grup cíclic d'ordre n. Sigui y un element de G i volem trobar x tal que $g^x = y$.

1. Sigui $n = p_1^{e_1} p_2^{e_2} ... p_n^{e_n}$, el nostre objectiu serà calcular $x \pmod{p_i^{e_i}}$ per tot $i = 1, ..., n$ i trobar x utilitzant el teorema xinès del residu.

2. Per cada p^e divisor de n tal que p^{e+1} no divideix n:

   a) Calculem, per cada p divisor de n, $r_{p,j} = g^{jn/p}$ per tot $j = 0, ..., p-1$.

   b) Per cada p^e escrivim $x \equiv x_0 + x_1 p + ... + x_{e-1} p^{e-1} \pmod{p^e}$.

   c) Per trobar x_0 calculem

$$y^{n/p} = g^{xn/p} = g^{x_0 n/p} \cdot g^{(x_1 + ... + x_{e-1} p^{e-2})n} = g^{x_0 n/p} = r_{p,x_0}$$

i per tant només ens cal comparar $y^{n/p}$ amb les $r_{p,j}$ prèviament calculades i així establir $x_0 = j$ pel j trobat.

   d) De la mateixa manera si tenim

$$y_i = y / g^{x_0 + x_1 p + ... + x_{i-1} p^{i-1}} = g^{x_i p^i + .. + x_{e-1} p^{e-1}}$$

llavors

$$y_i^{n/p^i} = g^{(x_i + ... + x_{e-1} p^{e-i-1})n} = 1$$

i aleshores

$$y_i^{n/p^{i+1}} = g^{(x_i + ... + x_{e-1} p^{e-i-1})n/p} = g^{x_i n/p} = r_{p,x_i}.$$

Així prenem x_i igual al valor de j tal que $y_i^{n/p^{i+1}} = r_{p,j}$. D'aquesta manera obtenint els coeficients $x_0, ..., x_{e-1}$ calculem $x \pmod{p^e}$.

3. Havent calculat $x \pmod{p_i^e}$ per tot $i = 1, .., n$ emprem el teorema xinès del residu per trobar $x \pmod{n}$.

Algoritme de càlcul de l'índex

Aquest algoritme només es pot aplicar a un determinat tipus de grups, normalment s'utilitza en el grup cíclic $\mathbf{F}_q^*$, on $q = p^m$, p és un nombre primer i m un nombre natural major a 1.

Llavors, sent g un generador del grup G i, donat, $y \in G$ volem trobar $x \in \mathbf{Z}$ tal que $g^x = y$. Sabem que $x \equiv \log_g y$, el mètode es fonamenta en la relació següent:

$$g^x = y \Leftrightarrow x \equiv \log_g y \,(\mathrm{mod}\, n), \tag{2.1}$$

on n és l'ordre del grup. En el cas de $\mathbf{F}_q^*$ té ordre $q-1$.

Suposem que tenim y_1 i y_2 tals que

$$g^{\log_g(y_1 y_2)} = y_1 y_2 = g^{\log_g(y_1)+\log_g(y_2)}$$

aleshores deduïm que

$$x \equiv \log_g(y_1 y_2) \equiv \log_g(y_1) + \log_g(y_2) \pmod{n}.$$

La idea del mètode és calcular $\log_g(l)$ per diversos primers l i utilitzar aquesta informació per trobar $\log_g(y)$ per un element del grup y.

Exemple 2.7. Sigui el grup $\mathbf{F}_{503}^*$ i $g = 5$. Volem resoldre $g^x = 282$. Sabem que l'ordre de $\mathbf{F}_{503}^*$ és $503 - 1 = 502$.

1. Comencem escollint una base P de nombres primers. Hem de tenir en compte que P no pot ser massa gran ni massa petita. Si P és massa petita no podrem calcular suficients $L(l)$ però si P és massa gran llavors l'àlgebra necessària per a trobar y serà massa complicada. En aquest cas escollim $P = \{2, 3, 5, 7, 11\}$.

2. Trobem les relacions

$$5^1 = 5$$
$$5^6 = 2^5$$
$$5^7 = 5 \cdot 2^5$$
$$5^8 = 11 \cdot 3^3$$
$$5^9 = -1 \cdot 2^3 \cdot 3$$
$$5^{12} = 2 \cdot 3^2$$
$$5^{14} = 2 \cdot 3^2 \cdot 5^2$$
$$5^{21} = -1 \cdot 2^4 \cdot 3^2$$
$$5^{25} = -1 \cdot 7^2 \cdot 2^3$$

també sabem que $5^{(q-1)/2} = -1$ així que $5^{251} = -1$ i per tant $\log_5(-1) = 251$.

Observem que no totes les relacions són útils, veiem que la tercera equació és equivalent a la segona i que, a partir de la segona i la cinquena ja obtenim la mateixa informació que ens donen la sisena, la setena i la vuitena. Així no utilitzarem la tercera, la sisena, la setena i la vuitena equació.

3. Utilitzant 2.deduïm

$$1 \equiv \log_5(5) \,(\mathrm{mod}\, 502)$$

$$6 \equiv 5\log_5(2) \,(\mathrm{mod}\, 502)$$

$$8 \equiv \log_5(11) + 3\log_5(3) \,(\mathrm{mod}\, 502)$$

$$9 \equiv \log_5(-1) + 3\log_5(2) + \log_5(3) \,(\mathrm{mod}\, 502)$$

$$25 \equiv \log_5(-1) + 2\log_5(7) + 3\log_5(2) \,(\mathrm{mod}\, 502).$$

Sabem que $5 \cdot 201 = 1005 \equiv 1 \,(\mathrm{mod}\, 502)$, així que $201 \equiv 5^{-1} \,(\mathrm{mod}\, 502)$. Aquest raonament també es podria fer fàcilment amb l'algoritme d'Euclides. Així, de la segona equació deduïm que

$$\log_5(2) \equiv 6 \cdot 201 = 1206 \equiv 204 \,(\mathrm{mod}\, 502).$$

De la quarta equació deduïm que

$$\log_5(3) \equiv 9 - \log_5(-1) - 3\log_5(2) = 9 - 251 - 3 \cdot 204 \equiv 155 \,(\mathrm{mod}\, 502).$$

De la tercera equació deduïm que

$$\log_5(11) \equiv 8 - 3\log_5(3) = 3 - 3 \cdot 155 \equiv 45 \,(\mathrm{mod}\, 502).$$

Finalment veiem que de la cinquena equació deduïm que

$$2\log_5(7) \equiv 25 - \log_5(-1) - 3\log_5(2) = 25 - 251 - 3 \cdot 204 \equiv 83 \,(\mathrm{mod}\, 502).$$

Llavors, ja tenim els logaritmes discrets per tots els elements de la base.

4. Per acabar calculem $5^j \cdot 282 \,(\mathrm{mod}\, 502)$ per diversos valors de j. En aquest fàcilment trobem

$$5^1 \cdot 282 \equiv -1 \cdot 3^2 \cdot 11 \,(\mathrm{mod}\, 502).$$

Així:

$$\log_5(282) \equiv \log_5(-1) + 2L(3) + L(11) - 1 = 251 + 2 \cdot 155 + 45 - 1 \equiv 102 \,(\mathrm{mod}\, 502)$$

i així $5^{102} = 282$ a $\mathbf{F}^*_{503}$.

Proves empíriques han demostrat que el temps necessari per a resoldre el problema del logaritme discret és de l'ordre de $O(\exp\sqrt{2\ln n \ln\ln n})$, que és força més petit que $O(\sqrt{n}) = O(\exp\frac{1}{2}\ln n)$ per a grups grans. Per tant, a la pràctica aquest és el mètode aplicat per a atacar el logaritme discret. D'altra banda, veiem que al pas 2. fem una factorització en nombres primers, la qual cosa no podem fer en tots els grups. Per això aquest mètode no es pot aplicar a tots els grups i aquesta és la raó per la qual s'utilitzen els grups de punts d'una corba el·líptica sobre un cos finit.

A continuació farem un estudi introductori a les corbes el·líptiques el qual aplicarem a la criptologia.

3 Corbes el·líptiques

3.1 Introducció

Començarem introduint la noció de corba el·líptica, no sense abans parlar d'uns termes necessaris per la seva definició.

Definició 3.1. *Sigui K un cos i A, B constants pertanyents a K. L'equació de Weierstrass és l'equació $y^2 = x^3 + Ax + B$.*

Definició 3.2. *Sigui K un cos i $a_1, a_2, a_3, a_4, a_5, a_6$ constants pertanyents a K. L'equació generalitzada de Weierstrass és l'equació*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Observació 3.3. Si el cos K no és de característica 2, llavors l'expressió

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

la podem escriure com

$$y^2 + a_1xy + a_3y + \frac{a_1^2x^2}{4} + \frac{a_3^2}{4} + \frac{a_1a_3x}{2} = x^3 + a_2x^2 + a_4x + a_6 + \frac{a_1^2x^2}{4} + \frac{a_3^2}{4} + \frac{a_1a_3x}{2}$$

i així podem completar el quadrat de manera que queda

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(a_6 + \frac{a_3^2}{4}\right).$$

Tot seguit, fem els canvis:

$$y_1 = y + \frac{a_1x}{2} + \frac{a_3}{2},$$

$$a_2' = a_2 + \frac{a_1^2}{4},$$

$$a_4' = a_4 + \frac{a_1a_3}{2}$$

i

$$a_6' = a_6 + \frac{a_3^2}{4}$$

i així ens queda l'equació

$$y_1^2 = x^3 + a_2'x^2 + a_4'x + a_6'.$$

Finalment, si el cos no és de característica 3 podem fer el canvi $x_1 = x + a_2'/3$ i per tant

$$x_1^3 = x^3 + a_2'x^2 + \frac{a_2'^2}{3}x + \left(\frac{a_2'}{3}\right)^3.$$

Així, l'equació ens queda com

$$y_1^2 = x_1^3 + \left(a_4' - \frac{a_2'^2}{3}\right)\left(x_1 - \frac{a_2'}{3}\right) + \left(a_6' - \left(\frac{a_2'}{3}\right)^3\right).$$

Ara definim:

$$A = a'_4 - \frac{{a'_2}^2}{3}$$
$$B = a'_6 - \left(\frac{a'_2}{3}\right)^3 - \frac{a'_4 a'_2}{3} + \frac{{a'_2}^3}{9}$$

i llavors ens queda

$$y_1^2 = x_1^3 + Ax_1 + B$$

que és precisament l'equació de Weierstrass.

Observació 3.4. El discriminant d'una equació cúbica de la forma $ax^3+bx^2+cx+d=0$ és $\Delta = 18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2$. Així que si K és un cos de característica diferent a 2 llavors el discriminant de l'equació generalitzada de Weierstrass és $\Delta = 18a'_2a'_4a'_6 - 4a'^3_2a'_6 + a'^2_2a'^2_4 - 4a'^3_4 - 27a'^2_6$.

Observació 3.5. El discriminant d'una equació de Weierstrass és el discriminant d'una equació cúbica de la forma $ax^3 + bx^2 + cx + d = 0$ on $b = 0$ i $a = 1$. Expressant l'equació de Weierstrass com $y^2 = x^3 + Ax + B$ el discriminant ens queda $-4A^3 - 27B^2$.

Definició 3.6. *Sigui $f(x, y) = 0$ una corba sobre un cos K, diem que un punt (x_0, y_0) és singular si $f(x, y) = 0$ i $\frac{\partial}{\partial x}f(x_0, y_0) = 0 = \frac{\partial}{\partial y}f(x_0, y_0)$.*

Definició 3.7. *Una corba el·líptica E sobre un cos K és el conjunt de punts no singulars de la corba donada per una equació generalitzada de Weierstrass.*

Aleshores, si el cos K no és de característica 2, la definició de corba el·líptica equival a la següent:

Definició 3.8. *Sigui K un cos de característica diferent a 2 i a'_2, a'_4 i a'_6 constants pertanyents a K. Una corba el·líptica E sobre K és el conjunt de punts de la corba donada per l'equació $y^2 = x^3 + a'_2x^2 + a'_4x + a'_6$ tal que el discriminant de $x^3 + a'_2x^2 + a'_4x + a'_6$ és diferent a 0, és a dir $\Delta = 18a'_2a'_4a'_6 - 4a'^3_2a'_6 + a'^2_2a'^2_4 - 4a'^3_4 - 27a'^2_6 \neq 0$.*

D'igual manera, en cas que el cos K sigui de característica diferent a 2 i 3, utilitzarem la següent definició:

Definició 3.9. *Sigui K un cos de característica diferent a 2 o 3 i A i B constants pertanyents a K. Una corba el·líptica E sobre K és el conjunt de punts de la corba donada per l'equació $y^2 = x^3 + Ax + B$ tal que el discriminant de $x^3 + Ax + B$ és diferent a 0, és a dir $-4A^3 - 27B^2 \neq 0$.*

3.2 El punt ∞

Veiem ara què passa si interpretem una corba el·líptica E sobre un cos K de manera projectiva.

Definició 3.10. *Un polinomi de m variables sobre un cos K és homogeni de grau n si és la suma de termes de la forma $ax_0^{i_0}x_1^{i_1}...x_m^{i_m}$ on $a \in K$ i $i_0 + i_1 + ... + i_m = n$.*

Recordem que existeix una inclusió entre l' espai afí de dimensió n sobre un cos K A_K^n i l'espai projectiu de dimensió n sobre un cos K P_K^n donada per:

$$(x_1, ..., x_n) \hookrightarrow (x_1 : ... : x_n, 1).$$

En particular, en l'espai 2-dimensional, existeix la inclusió $(x, y) \hookrightarrow (x : y : 1)$. Així, si tenim la funció $f(x, y) = y^2 - x^3 - Ax - B$ a A_k^2 podem obtenir la funció $F(x, y, z) = y^2z - x^3 - Axz^2 - Bz^3$, que és un polinomi homogeni de grau 3 sobre l'espai P_k^2.

Sabem que, donada la inclusió anterior, els punts a l'infinit de P_k^2 són els que compleixen $z = 0$. En el cas de la corba el·líptica sobre P_k^2, els punts a l'infinit són els que compleixen

$$0 = F(x, y, 0) = y^20 - x^3 - Ax0^2 - B0^3 = x^3.$$

Per tant, $x = 0$, així que els punts a l'infinit d'una corba el·líptica sobre P_k^2 són els de la forma $(0 : \lambda : 0)$, on $0 \neq \lambda \in K$. Però al estar a P_k^2, tots els punts de la forma $(0 : \lambda : 0)$ són equivalents entre si, per tant, només existeix un punt a l'infinit. Aquest punt el denotarem com ∞.

Corol·lari 3.11. *: Podem definir una corba el·líptica E sobre un cos K de característica diferent a 2 i 3 com*

$$E(K) = \{(x, y) \in K \times K | y^2 = x^3 + Ax + B\} \cup \{\infty\}.$$

On A, $B \in K$.

3.3 La propietat de Grup

Sigui E una corba el·líptica sobre un cos K de característica diferent a 2 i 3 i siguin $P_1 = (x_1, y_1)$ i $P_2 = (x_2, y_2)$ dos punts de la corba E diferents entre si, podem definir la seva suma com P_1 i P_2 com $P_1 + P_2 = (P_1P_2)'$ on (P_1P_2) representa la intersecció entre la recta P_1P_2 i E i P' és el conjugat de P, és a dir, si $P = (x, y)$ llavors $P' = (x, -y)$. Com veurem més endavant, sempre existeix (P_1P_2). D'altra banda, si $P = (x, y)$ pertany a la corba, llavors

$$y^2 = x^3 + Ax + B.$$

Per tant, com que

$$(-y)^2 = y^2 = x^3 + Ax + B,$$

P' també pertany a la corba. Definim $P + P' = \infty$.
En cas que $P_1 = P_2$ llavors definim $P_1 + P_2$ com el punt conjugat del punt intersecció entre la recta tangent en P_1 i E, el qual també veurem que existeix. En cas que la coordenada y de P_1 sigui igual a 0, definim $P_1 + P_1 = \infty$.
Per conveni, definim $P + \infty = P$.

Proposició 3.12. *L'operació suma que hem descrit està ben definida.*

Demostració. Siguin $P_1 = (x_1, y_1) \neq P_2 = (x_2, y_2)$.

En cas que $x_1 = x_2$ llavors P_1 i P_2 són conjugats, per tant $P_1 + P_2 = \infty$, que és únic. En cas que $x_1 \neq x_2$, llavors la pendent de la recta és:

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{y_1 - y_2}{x_1 - x_2}.$$

Llavors l'equació de la recta que uneix P_1 i P_2 és $y = m(x - x_1) + y_1$. Per trobar la intersecció amb E substituïm y i ens queda l'equació

$$x^3 + Ax + B = (m(x - x_1) + y_1)^2,$$

per tant

$$x^3 - m^2x^2 + (A + 2m^2x_1 - 2my_1)x + (B - m^2x_1^2 - y_1^2 + 2mx_1y_1) = 0$$

que es pot reduir a una equació cúbica $x^3 + ax^2 + bx + c = 0$ per algunes constants a, b i c. Sabem que x_1 i x_2 són arrels d'aquesta equació cúbica, per tant, existeix una altra arrel pertanyent a K, x_3, que serà precisament el punt P_1P_2. Per tant, la intersecció de la recta P_1P_2 i E és un únic punt. En conseqüència, com hem vist abans que el conjugat d'un punt de E també es troba a E, la suma de dos punts d'una corba el·líptica és un únic punt de la corba el·líptica.

Per trobar les coordenades del punt recordem que

$$x^3 + ax^2 + bx + c = (x - r)(x - s)(x - t).$$

El terme corresponent a x^2 és $-r - s - t$ i per tant $-r - s - t = a$.
Llavors, sent t l'arrel desconeguda (i per tant, la coordenada x del punt que volem trobar) deduïm que $t = -a - r - s$ on a és el terme corresponent a x^2, el qual resulta ser $-m^2$, per tant

$$x_3 = m^2 - x_1 - x_2,$$

i com

$$y = m(x - x_1) + y_1,$$

deduïm que $y_3 = m(x_1 - x_3) - y_1$, ja que el resultat és el conjugat de la intersecció entre la corba i la recta tangent als dos punts sumats.

Veiem ara el resultat de sumar un punt $P_1 = (x_1, y_1)$ amb si mateix, és a dir, trobar $P_2 = (x_2, y_2) = (x_1, y_1) + (x_1, y_1)$.
Per definició, si $y = 0$ llavors $P_1 + P_1 = \infty$. Llavors, si $y \neq 0$, per a trobar el pendent de la recta derivem respecte x l'equació $y^2 = x^3 + Ax + B$ i ens surt:

$$2y\frac{dy}{dx} = 3x^2 + A$$

i per tant

$$\frac{dy}{dx} = \frac{3x^2 + A}{2y}$$

i en conseqüència

$$m = \frac{3x_1^2 + A}{2y_1}.$$

Per tant la recta tangent és

$$y = m(x - x_1) + y_1 = \frac{3x_1^2 + A}{2y_1}(x - x_1) + y_1$$

i així l'equació de la intersecció és

$$x^3 + Ax + B = \left(\frac{3x_1^2 + A}{2y_1}(x - x_1) + y_1\right)^2$$

llavors queda

$$x^3 - \left(\frac{3x_1^2 + A}{2y_1}\right)^2 x^2 + \left(-3x_1^2 + 2x_1\left(\frac{3x_1^2 + A}{2y_1}\right)^2 - A\right)x +$$

$$\left(B + Ax_1 - x_1^2\left(\frac{3x_1^2 + A}{2y_1}\right)^2 - y_1^2 + 3x_1^3\right) = 0.$$

Com la recta és tangent a E en P_1, P_1 és una arrel doble de l'equació anterior i, per tant, existeix una única arrel, que és la intersecció buscada.

Així, igual que en el cas $P_1 \neq P_2$, les coordenades d'el punt $P_3 = (x_3, y_3)$ són

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

i

$$y_3 = m(x_3 - x_1) - y_1.$$

Així queda provat que l'operació suma de dos punts d'una corba el·líptica anteriorment descrita està ben definida i, a més, hem calculat explícitament el resultat de la suma de dos punts d'una corba el·líptica E.

Observació 3.13. Sabem que la recta P_1P_2 és la mateixa recta que P_2P_1 i, efectivament, la intersecció entre la recta P_1P_2 i la corba el·líptica E és

$$P_1P_2 = (m^2 - x_1 - x_2, m(x_3 - x_1) + y_1).$$

Com l'equació de la recta és

$$y = m(x - x_1) + y_1 = m(x - x_2) + y_2$$

veiem que

$$y_1 = m(x - x_2) + y_2 - m(x - x_1) = y_2 + m(x_1 - x_2)$$

i, per tant

$$P_1P_2 = (m^2 - x_1 - x_2, m(x_3 - x_1) + m(x_1 - x_2) + y_2) = (m^2 - x_2 - x_1, m(x_3 - x_2) + y_2) = P_2P_1.$$

Teorema 3.14. *Sigui un cos K i una corba el·líptica E sobre K, llavors $(E, +)$ és un grup abelià.*

Demostració. La propietat commutativa està vista en l'observació anterior. Per definició, l'element neutre és ∞ i l'invers d'un punt és el seu conjugat. La prova de l'associativitat no és complicada però si llarga i considero que no és necessària per al transcurs de l'estudi d'aquest treball. Podeu trobar-la a la secció 2.4. de [1].

Observació 3.15. Podem definir el conjugat d'un punt P de la corba com $-P$, doncs compleix que $P' + P = P + P' = \infty$, que és el neutre.

3.4 L'invariant j

Definició 3.16. *Sigui $y^2 = x^3 + Ax + B$ una corba el·líptica E definida sobre un cos K de característica diferent a 2 o 3, definim l'invariant j com*

$$j := j(E) := 1728\frac{4A^3}{4A^3 + 27B^2}$$

.

Recordem que $4A^3 + 27B^2 \neq 0$, per el qual el denominador no s'anul·la.

Sigui una corba el·líptica E definida sobre un cos K de característica diferent a 2 o 3 definida per l'equació $y^2 = x^3 + Ax + B$ i sigui $\mu \in \overline{K}^*$, on $\overline{K}$ és la clausura algebraica de K i K^* indica el conjunt d'elements invertibles de K.

Fent el canvi de variables $x_1 = \mu^2 x$ i $y_1 = \mu^3 y$ obtenim

$$y_1^2 = (\mu^3 y)^2 = \mu^6(x^3 + Ax + B) = x_1^3 + \mu^4 A x_1 + \mu^6 B,$$

que resulta ser una corba el·líptica.

Teorema 3.17. *Siguin $y_1^2 = x_1^3 + A_1 x_1 + B_1$ i $y_2^2 = x_2^3 + A_2 x_2 + B_2$ definides sobre el mateix cos K. Si el seu invariant j coincideix, llavors existeix $\mu \in \overline{K}^*$ tal que el $x_2 = \mu^2 x_1$, $y_2 = \mu^3 y_1$, $A_2 = \mu^4 A_1$ i $B_2 = \mu^6 B_1$.*

Demostració. Si $A_1 = 0$ llavors $j_1 = 0 = j_2$ i per tant $A_2 = 0$. També veiem que tant B_1 com B_2 són diferents a 0 i així ens és suficient escollir μ tal que $B_2 = \mu^6 B_1$.

Si $A_1 \neq 0$, llavors $A_2 \neq 0$, llavors escollim μ_1 tal que $A_2 = \mu_1^4 A_1$, llavors veiem que $\mu_2 = \sqrt{-1}\mu_1$ també compleix aquesta condició. Llavors, com els dos invariants j coincideixen:

$$1728\frac{4A_2^3}{4A_2^3 + 27B_2^2} = 1728\frac{4A_1^3}{4A_1^3 + 27B_1^2}$$

i així:

$$\frac{4A_2^3}{4A_2^3 + 27B_2^2} = \frac{4A_1^3}{4A_1^3 + 27B_1^2} = \frac{4\mu_i^{-12}A_2^3}{4\mu_i^{-12}A_2^3 + 27B_1^2} = \frac{4A_2^3}{4A_2^3 + 27\mu_i^{12}B_1^2}$$

per $i = 1, 2$.

En conseqüència $B_2^2 = \mu_i^{12} B_1^2$, per tant $B_2 = \pm\mu_i^6 B_1$. En cas que $B_2 = \mu^6 B_1$ llavors $\mu = \mu_1$ i en cas que $B_2 = -\mu^6 B_1$ llavors $\mu = \mu_2$.

3.5 Endomorfismes

Definició 3.18. *Un endomorfisme de corbes el·líptiques és un morfisme de grups $\alpha : E(\overline{K}) \longrightarrow E(\overline{K})$ donat per funcions racionals. És a dir, $\alpha(x, y) = (R_1(x, y), R_2(x, y))$, on R_1 i R_2 són funcions racionals.*

Observació 3.19. Al ser α un morfisme, es compleix:

1) $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$.

2) $\alpha(\infty) = \infty$.

L'endomorfisme trivial, el que envia tot punt (x, y) a ∞, el denotarem com 0.

Proposició 3.20. *Un endomorfisme de corbes el·líptiques donades en la forma de Weierstrass es pot escriure de la forma $\alpha = (r_1(x), r_2(x)y)$, on r_1 i r_2 són funcions racionals amb coeficients a $\overline{K}$.*

Demostració. Com $y^2 = x^3 + Ax + B$, podem substituir y^{2n}, per tot $n > 1$, per un polinomi en x, així que podem escriure

$$R_i(x, y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}$$

per $i = 1, 2$. On p_1, p_2, p_3 i p_4 són polinomis. Encara, multiplicant numerador i denominador per $p_3(x) - p_4(x)y$ llavors

$$R(x,y) = \frac{(p_1(x) + p_2(x)y)(p_3(x) - p_4(x)y)}{(p_3(x) + p_4(x)y)(p_3(x) - p_4(x)y)} =$$

$$\frac{p_1(x)p_3(x) + (p_2(x)p_3(x) - p_4(x)p_1(x))y - p_2(x)p_4(x)y^2}{p_3^2(x) - p_4^2(x)y^2} =$$

$$\frac{p_1(x)p_3(x) + (p_2(x)p_3(x) - p_4(x)p_1(x))y - p_2(x)p_4(x)(x^3 + Ax + B)}{p_3^2(x) - p_4^2(x)(x^3 + Ax + B)}$$

que es pot escriure com

$$R(x,y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}$$

on q_1, q_2 i q_3 també són polinomis. Per tant,

$$\alpha(x,y) = \left(\frac{q_1(x) + q_2(x)y}{q_3(x)}, \frac{q_4(x) + q_5(x)y}{q_6(x)}\right).$$

D'altra banda, α és un morfisme, així que $\alpha(x,-y) = \alpha(-(x,y)) = -\alpha(x,y)$. En conseqüència,

$$\left(\frac{q_1(x) + q_2(x)(-y)}{q_3(x)}, \frac{q_4(x) + q_5(x)(-y)}{q_6(x)}\right) = \left(\frac{q_1(x) + q_2(x)y}{q_3(x)}, -\frac{q_4(x) + q_5(x)y}{q_6(x)}\right).$$

Llavors, si

$$R_1(x,y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}$$

tenim que

$$q_1(x) - q_2(x)y = q_1(x) + q_2(x)y.$$

Aleshores, $q_2 = 0$.
També, si

$$R_2(x,y) = \frac{q_4(x) + q_5(x)y}{q_6(x)},$$

deduïm que $q_4(x) - q_5(x)y = -q_4(x) - q_5(x)y$
Per tant, $q_4 = 0$.
Com a conclusió tenim que el morfisme es pot escriure de la forma $\alpha(x,y) = (r_1(x), r_2(x)y)$, on r_1 i r_2 són funcions racionals.

Exemple 3.21. Sigui E definida per $y^2 = x^3 + Ax + B$ en un cos K de característica diferent a 2 i 3 i sigui $\alpha(P) = 2(P)$. Llavors α és un endomorfisme de E i $\alpha(x,y) = (R_1(x,y), R_2(x,y))$ on

$$R_1(x,y) = \left(\frac{3x^2 + A}{2y}\right)^2 - 2x$$

$$R_2(x,y) = \left(\frac{3x^2 + A}{2y}\right)\left(x - \left(\left(\frac{3x^2 + A}{2y}\right)^2 - 2x\right)\right) - y$$

$$= \left(\frac{3x^2 + A}{2y}\right)\left(3x - \left(\frac{3x^2 + A}{2y}\right)^2\right) - y$$

Aleshores, fent unes senzilles manipulacions obtenim que $\alpha(x,y) = (r_1, r_2 y)$ on

$$r_1(x) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}$$

$$r_2(x) = \frac{x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2}{8(x^3 + Ax + B)^2}.$$

Definició 3.22. *Sigui* $\alpha(x,y) = (r_1(x), r_2(x)y) = \left(\frac{p_1(x)}{q_1(x)}, \frac{p_2(x)}{q_2(x)}y\right)$ *un morfisme de corbes el·líptiques. Si existeix* $(x_0, y_0) \in E(\overline{K})$ *tal que* $q_1(x_0) = 0$*, definim* $\alpha(x_0, y_0) = \infty$*.*

Ara caldria preguntar-se què passa si $q_2 = 0$, per això ens cal parlar del següent resultat amb el qual podrem acabar de definir el resultat d'un endomorfisme de corbes el·líptiques per tot punt $(x_0, y_0) \in E(\overline{K})$.

Proposició 3.23. *Sigui* $\alpha(x,y) = (r_1(x), r_2(x)y) = \left(\frac{p_1(x)}{q_1(x)}, \frac{p_2(x)}{q_2(x)}y\right)$*, en cas que existeixi* $(x_0, y_0) \in E(\overline{K})$ *tal que* $q_2(x_0) = 0$ *, llavors* $q_1(x_0) = 0$*.*

Demostració. Sigui

$$\alpha(x,y) = (r_1(x), r_2(x)y) = \left(\frac{p_1(x)}{q_1(x)}, y\frac{p_2(x)}{q_2(x)}\right).$$

On p_1 i q_1 són polinomis sense arrels en comú i p_2 i q_2 són polinomis sense arrels en comú. Com $\alpha(x,y) \in E$,

$$\left(y\frac{p_2(x)}{q_2(x)}\right)^2 = \left(\frac{p_1(x)}{q_1(x)}\right)^3 + A\left(\frac{p_1(x)}{q_1(x)}\right) + B = \frac{p_1^3(x) + Ap_1(x)q_1^2(x) + Bq_1^3(x)}{q_1^3(x)}.$$

Definim com

$$u(x) = p_1^3(x) + Ap_1(x)q_1^2(x) + Bq_1^3(x).$$

Veiem que, com p_1 i q_1 són polinomis sense arrels en comú, $u(x)$ i $q_1(x)$ tampoc tenen arrels en comú.
Així, tenim la igualtat

$$q_2^2(x)u(x) = q_1^3(x)p_2^2(x)y^2 = q_1^3(x)p_2^2(x)(x^3 + Ax + B).$$

Suposem ara, que existeix x_0 tal que $q_2(x_0) = 0$, llavors x_0 és arrel doble de $q_2(x)^2$, com $(x^3 + Ax + B)$ no té arrels dobles i x_0 no és arrel de $p_2(x)$ (ja que ho és de $q_2(x)$) x_0 és també arrel de $q_1(x)$.
Per tant, si $q_2(x_0) = 0$, llavors $q_1(x_0) = 0$.

Definició 3.24. *Sigui* $\alpha(x,y) = (r_1(x), r_2(x)y)$ *i* $r_1(x) = \frac{p_1(x)}{q_1(x)}$*, definim el grau del endomorfisme com* $\mathrm{gr}(\alpha) = \max(\mathrm{gr}(p_1(x)), \mathrm{gr}(q_1(x))$*.*

Definició 3.25. *Sigui* $\alpha = (r_1(x), r_2(x)y) \neq 0$ *un endomorfisme de corbes el·líptiques. Diem que* α *és separable si* $r_1'(x) \neq 0$*.*

Teorema 3.26. *Sigui* $\alpha \neq 0$ *un morfisme separable d'una corba el·líptica* E *sobre un cos* K*. Llavors:*

$$\mathrm{gr}(\alpha) = \#\ker(\alpha).$$

En cas que $\alpha \neq 0$ *sigui no separable, llavors:*

$$\mathrm{gr}(\alpha) > \#\ker(\alpha).$$

Demostració. Sabem que el cardinal del nucli d'un morfisme coincideix amb el cardinal de l'antiimatge d'un punt qualsevol del conjunt d'arribada. Llavors:
Suposem que α sigui un morfisme separable:
Escrivim

$$\alpha(x, y) = (r_1(x), yr_2(x))$$

on $r_1(x) = p(x)/q(x)$. Llavors, per definició, $\text{gr}(\alpha) = \max(\text{gr}(p(x)), \text{gr}(q(x))$ i, al ser separable, $r_1'(x) = p'(x)q(x) - p(x)q'(x) \neq 0$.
Ara, sigui $S = \{x \in \overline{K} | (p'(x)q(x) - p(x)q'(x))q(x) = 0\}$, com que $p'(x)q(x) - p(x)q'(x) \neq 0$, S és un conjunt finit.
Aleshores, sigui $(a, b) \in E(\overline{K})$ tal que:

1. $(a, b) \neq \infty$ i $a \neq 0 \neq b$,
2. $\text{gr}(p(x) - aq(x)) = \text{gr}(\alpha) = \max(\text{gr}(p(x)), \text{gr}(q(x))$,
3. a no pertany a $r_1(S)$,
4. $(a, b) \in \alpha(E(\overline{K}))$.

Per a trobar el cardinal del nucli d'α trobarem el nombre de punts que són antiimatge de (a, b). Primer ens cal provar que tal punt (a, b) existeix:
Comencem veient que el nombre de punts que no compleixen les condicions 1 i 2 és finit. També és clar que $r_1(x)$ pren una quantitat infinita de valors si $x \in \overline{K}$. D'altra banda, com que S és un conjunt finit, la seva imatge per α també ho és, així que el nombre de punts que no compleix la condició 3 és finit. A més, com per cada $(x, y) \in E(\overline{K})$ existeix $\alpha(x, y) \in E(\overline{K})$ veiem que $\alpha(E(\overline{K}))$ és un conjunt infinit, així que la quantitat de punts que poden complir la condició 4 és infinita. En conclusió, que tal punt (a, b) existeix.
Ara, siguin (x_1, y_1) tals que

$$(a, b) = \alpha(x_1, y_1) = \left(\frac{p(x_1)}{q(x_1)}, y_1 r_2(x_1)\right),$$

com que $(a, b) \neq \infty$, deduïm que $q_1(x) \neq 0$. Com hem vist anteriorment, $r_2(x)$ està definida. D'altra banda, com que $b \neq 0$, $y_1 = b/r_2(x_1)$, així que per cada y_1 existeix un x_1 corresponent, per tant ens és suficient comptar els valors de x_1 tals que $a = \frac{p(x_1)}{q(x_1)}$, és a dir, els que compleixen $p(x_1) - aq(x_1) = 0$
Per la condició 2 tenim que $p(x) - aq(x)$ té $\text{gr}(\alpha)$ arrels, comptant multiplicitat. Per tant, només cal veure que $p(x) - aq(x)$ no té arrels múltiples.
Suposem que x_0 és una arrel múltiple de $p(x) - aq(x)$, llavors:

$$p(x_0) - aq(x_0) = 0 \qquad \text{i} \qquad p'(x_0) - aq'(x_0) = 0.$$

Multiplicant $p(x_0) = aq(x_0)$ i $p'(x_0) = aq'(x_0)$ ens surt:

$$p(x_0)aq'(x_0) = aq(x_0)p'(x_0).$$

Com que $a \neq 0$, a és arrel de $p'(x_0)q(x_0) - p(x_0)q'(x_0)$ i per tant $x_0 \in S$, en conseqüència $a = r_1(x_0) \in r_1(S)$, la qual cosa contradiu la condició 3.
Per tant $p(x) - aq(x)$ no té arrels múltiples, i per tant té $\text{gr}(\alpha)$ punts diferents.
Llavors, acabem de provar que $\text{gr}(\alpha) = \#\ker(\alpha)$ en el cas que α sigui separable.
Si α no és separable, llavors la demostració és la mateixa, excepte que la (a, b) no necessàriament han de complir la condició 3 i que $p'(x) - aq'(x)$ és el polinomi 0, per tant $p(x) - aq(x)$ té arrels múltiples i, en conseqüència, $gr(\alpha) > \#Ker(\alpha)$ en el cas que α no sigui separable.

3.6 Punts de torsió

Sabem que el subgrup de torsió d'un grup abelià és el subgrup format pel conjunt d'elements d'ordre finit.

Definició 3.27. *Sigui E una corba el·líptica definida sobre un cos K. Sigui n un enter positiu. Definim els punts de n-torsió de la corba com*

$$E[n] = \{P \in E(\overline{K}) | nP = \infty\}.$$

Els punts de torsió tenen un rol fonamental en la teoria de corbes el·líptiques. Nosaltres l'utilitzarem per explicar l'algoritme de Schoof.
Amb tal de trobar punts de torsió, s'utilitzen els polinomis de divisió.

Definició 3.28. *Es defineixen els polinomis de divisió ψ_m recursivament com:*

$\psi_0 = 0$

$\psi_1 = 1$

$\psi_2 = 2y$

$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$

$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$

$\psi_{2_m} = \frac{\psi_m}{2y}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)$ *per* $2 \leq m$

$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$ *per* $2 \leq m$

Lema 3.29. *Si n és senar, llavors $\psi_n = nx^{(n^2-1)/2}+$ termes d'ordre menor. Per tant ψ_n té $n^2 - 1$ arrels diferents.*

Demostració. Ho demostrarem per inducció, per definició

$$\psi_1 = 1 = 1x^{1-1}$$

i també

$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2 = 3x^{(9-1)/2} + ...$$

Llavors, suposem que el lema és veritat per $2n - 1$ per $n > 3$, llavors

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3$$

Sabem, per la hipòtesis d'inducció que:

$$\psi_{n+2} = (n+2)x^{((n+2)^2-1)/2} + ...$$
$$\psi_n^3 = n^3x^{3(n^2-1)/2} + ...$$
$$\psi_{n-1} = (n-1)x^{((n-1)^2-1)/2} + ...$$
$$\psi_{n+1}^3 = (n+1)^3x^{3((n+1)^2-1)/2} + ...$$

llavors

$$\psi_{n+2}\psi_n^3 = (n+2)n^3x^{((n+2)^2-1+3(n^2-1))/2}+... = (n+2)n^3x^{2n^2+2n}+... = (n^4+2n^3)x^{2n^2+2n}+...,$$

$$\psi_{n-1}\psi_{n+1}^3 = (n-1)(n+1)^3x^{2n^2+2n} + ... = (n^4 + 2n^3 - 2n - 1)x^{2n^2+2n} + ...,$$

i al final obtenim

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 = (2n+1)x^{2n^2+2n} = (2n+1)x^{((2n+1)^2-1)/2}$$

i així, per inducció, queda demostrat el lema.

La importància d'aquests polinomis es veu en el següent resultat:

Teorema 3.30. *Sigui $P = (x, y)$ un punt d'una corba el·líptica $y^2 = x^3 + Ax + B$ sobre un cos K de cardinal diferent a 2, i sigui n un enter positiu. Llavors:*

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n(x,y)^3}\right)$$

on $\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}$ i $\omega_n = (4y)^{-1}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{2n+1})$.

Aquest resultat no el demostrarem, doncs es necessiten coneixements força superiors als utilitzats a aquest treball. Es pot trobar la demostració a la secció 9.5. de [1].

Així deduïm que trobar punts de torsió d'una corba el·líptica equival a trobar les arrels dels polinomis de divisió. El primer resultat no immediat d'aquest Teorema és el següent:

Teorema 3.31. *Sigui E una corba el·líptica definida sobre un cos K. Sigui n un enter positiu i $\mathbf{Z}_n = \mathbf{Z}/n\mathbf{Z}$.*
Si la característica de K no divideix n o és 0, llavors

$$E[n] \simeq \mathbf{Z}_n \oplus \mathbf{Z}_n.$$

En cas que la característica de K sigui $p > 0$ i $p|n$, escrivim $n = p^r n'$ on $n' \nmid n$, llavors:

$$E[n] \simeq \mathbf{Z}_{n'} \oplus \mathbf{Z}_{n'} \text{ o } E[n] \simeq \mathbf{Z}_n \oplus \mathbf{Z}_{n'}.$$

Aquest resultat tampoc el demostrarem. La demostració no és complicada però si llarga. Es pot trobar la demostració a la secció 3.2. de [1].

Teorema 3.32. *Sigui E una corba el·líptica definida sobre un cos K. Sigui n un enter no divisible per la característica de K i sigui $\mu_n = \{x \in \overline{K} | x^n = 1\}$ el conjunt d'arrels n-èsimes de la unitat.*
Llavors existeix un aparellament $e_n : E[n] \times E[n] \longrightarrow \mu_n$ que satisfà les següents propietats:

1. e_n és bilineal en cada variable. És a dir:

$$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T) \text{ i } e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2)$$

per tot $S, S_1, S_2, T, T_1, T_2 \in E[n]$.

2. e_n és no degenerat en cada variable. És a dir:

Si $E_n(S, T) = 1$ per tot $T \in E[n]$ llavors $S = \infty$ i també si $E_n(S, T) = 1$ per tot $S \in E[n]$ llavors $T = \infty$.

3. $e_n(T, T) = 1$ per tot $T \in E_n$.

4. $e_n(S, T) = e_n(T, S)^{-1}$ per tot $S, T \in E[n]$.

5. $e_n(\sigma S, \sigma T) = \sigma(E_n(S, T))$ per tot automorfisme σ de $\overline{K}$ tal que deixa constants els coeficients d'E. Per exemple, si és descrita amb l'equació de Weierstrass, llavors $\sigma(A) = A$ i $\sigma(B) = B$.

6. $e_n(\alpha(S), \alpha(T)) = e_n(S, T)^{gr(\alpha)}$ per tot endomorfisme separable.

La demostració d'aquest Teorema és llarga i es necessiten coneixements força superiors als utilitzats durant el transcurs del treball. Es pot trobar a la secció 11.2. de [1].

Definició 3.33. *L'aparellament esmentat anteriorment s'anomena aparellament de Weil.*

Tot seguit demostrarem uns resultats que ens seran útils més endavant per fer criptografia en corbes el·líptiques.

Corol·lari 3.34. *Sigui $\{T_1, T_2\}$ una base de $E[n]$. Llavors $e_n(T_1, T_2)$ és una arrel primitiva n-èssima de la unitat.*

Demostració. Suposem que $e_n(T_1, T_2) = \zeta$ on $\zeta^d = 1$. Llavors $e_n(T_1, dT_2) = e_n(T_1, T_2)^d = 1$, per la bilinealitat de les variables. D'altra banda, $e_n(T_2, dT_2) = e_n(T_2, T_2)^d = 1$ per la propietat 3. Llavors, sigui $S \in E[n]$, tenim que $S = aT_1 + bT_2$ per uns enters a, b. Aleshores,

$$e_n(S, dT_2) = e_n(T_1, dT_2)^a e_n(T_2, dT_2)^b = 1$$

Com aquesta igualtat es compleix per tot $S \in E[n]$, la no degeneració en cada variable (propietat 2) implica que $dT_2 = \infty$. Sabem que $dT_2 = \infty$ si i només si $n|d$, així que ζ és una arrel primitiva n-èssima de la unitat.

Corol·lari 3.35. *Si $E[n] \subseteq E(K)$, llavors $\mu_n \subseteq K$*

Demostració. Sigui $\zeta \in \mu_n$ i σ un automorfisme de $\overline{K}$ tal que σ és la identitat en K. Sigui T_1, T_2 una base de $E[n]$. Com $E[n] \subseteq E(K)$, podem assumir que T_1 i T_2 tenen coordenades a K, per tant $\sigma T_1 = T_1$ i $\sigma T_2 = T_2$ per la propietat 5 de l'aparellament de Weil, aleshores

$$\zeta = e_n(T_1, T_2) = e_n(\sigma T_1, \sigma T_2) = \sigma(e_n(T_1, T_2)) = \sigma(\zeta)$$

Per tant, ζ és fix per tot automorfisme de $\overline{K}$ i aleshores, pel Teorema de Galois, $\zeta \in K$. Com aquest resultat val per tot $\zeta \in \mu_n$, deduïm que $\mu_n \subseteq K$.

4 Corbes el·líptiques sobre cossos finits

L'objectiu principal d'aquesta secció serà trobar l'ordre dels grups abelians $(E, +)$, on E és una corba el·líptica sobre un cos finit $\mathbf{F}_q$.

4.1 El Teorema de Hasse

La finalitat d'aquest capítol és demostrar el Teorema de Hasse, el qual ens dona una fita de l'ordre de $O(\sqrt{q})$ d'el nombre de punts d'una corba el·líptica sobre un cos de cardinal q finit. El Teorema de Hasse és el següent:

Teorema 4.1. *Sigui E una corba el·líptica sobre un cos $\mathbf{F}_q$ de cardinal q finit. Llavors:*

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

Definició 4.2. *Sigui $\mathbf{F}_q$ el cos finit de cardinal q i $\overline{\mathbf{F}_q}$ la seva clausura algebraica. Definim l'endomorfisme de Frobenius sobre corbes el·líptiques com:*

$$\begin{aligned} \phi_q : \overline{\mathbf{F}_q} &\longrightarrow \overline{\mathbf{F}_q} \\ (x, y) &\longrightarrow (x^q, y^q). \end{aligned}$$

Lema 4.3. *Sigui E una corba el·líptica definida sobre un cos $\mathbf{F}_q$, i sigui $(x, y) \in E(\overline{\mathbf{F}_q})$. Llavors:*

1. $\phi_q(x, y) \in E(\overline{\mathbf{F}_q})$.
2. $(x, y) \in E(\mathbf{F}_q) \Leftrightarrow \phi_q(x, y) = (x, y)$

Demostració. Sabem que si $\mathbf{F}_q$ és un cos finit, $a^q = a$ per tot $a \in E(\mathbf{F}_q)$. També sabem que $(a + b)^q = a^q + b^q$ per tot $a \in E(\mathbf{F}_q)$. Llavors sigui $(x, y) \in E(\mathbf{F}_q)$ complint

$$y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6$$

on $a_i \in F_q$. Elevant l'equació a la q-èsima potència obtenim:

$$y^{2q} + a_1^q(xy)^q + a_3^q = x^{3q} + a_2x^{2q} + a_4^qx^q + a_6^q.$$

La qual equival a

$$(y^q)^2 + a_1(x^q)(y^q) + a_3 = (x^q)^3 + a_2(x^q)^2 + a_4x^q + a_6,$$

ja que $a^q = a$ per tot $a \in E(\mathbf{F}_q)$.
Per tant $(x^q, y^q) \in E(\overline{\mathbf{F}_q})$.
D'altra banda, $(x, y) \in E(\mathbf{F}_q) \Leftrightarrow x, y \in \mathbf{F}_q \Leftrightarrow \phi_q(x) = x$ i $\phi_q(y) = y \Leftrightarrow \phi_q(x, y) = (x, y)$, on hem tornat a utilitzar el fet que $a^q = a$ per tot $a \in \mathbf{F}_q$.
Per tant $(x, y) \in E(\mathbf{F}_q) \Leftrightarrow \phi_q(x, y) = (x, y)$.

Lema 4.4. *L'endomorfisme de Frobenius és un endomorfisme no separable.*

Demostració. El lema anterior ens confirma que la imatge d'un punt de $E(\overline{\mathbf{F}_q})$ pertany a $E(\overline{\mathbf{F}_q})$. Per tant ens és suficient comprovar que $\phi_q(P_1 + P_2) = \phi_q(P_1) + \phi_q(P_2)$ per veure que és un endomorfisme. Siguin (x_1, y_1) i (x_2, y_2) dos punts diferents d'una corba el·líptica E sobre un cos $\mathbf{F}_q$ d'ordre q. La seva suma és (x_3, y_3) amb

$$x_3 = m^2 - x_1 - x_2,\ y_3 = m(x_1 - x_3) - y_1,$$

on

$$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

Llavors, utilitzant que $(a+b)^q = a^q + b^q$:

$$\phi_q(x_3, y_3) = (m'^2 - x_1^q - x_2^q, m'(x_1^q - x_3^q) - y_1^q) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2),$$

on

$$m' = \frac{y_2^q - y_1^q}{x_2^q - x_1^q}.$$

D'altra banda, si $(x_1, y_1) = (x_2, y_2)$ llavors $2(x_1, y_1) = (x_3, y_3)$, amb

$$x_3 = m^2 - 2x_1,\ y_3 = m(x_1 - x_3) - y_1,$$

on

$$m = \frac{3x_1^2 + A}{2y_1}.$$

Aleshores, com $2, 3, A \in F_q$, $2^q = 2, 3^q = 3, A^q = A$:

$$\phi_q(x_3, y_3) = (m'^2 - 2x_1^q, m'(x_1^q - x_3^q) - y_1^q) = \phi_q(x_1, y_1) + \phi_q(x_1, y_1) = 2\phi_q(x_1, y_1)$$

on

$$m' = \frac{3^q (x_1^q)^2 + A^q}{2^q y_1^q} = \frac{3(x_1^q)^2 + A}{2y_1^q}.$$

Per tant, ϕ_q és un morfisme. Per acabar, com $\phi_q' = qx^{q-1} = 0$, veiem que l'endomorfisme és no separable.

Observació 4.5. $(\phi_q - 1) := \phi_q(x, y) - (x, y)$ és suma de endomorfismes i, per tant, endomorfisme. També veiem que $(\phi_q - 1)' = qx^{q-1} - 1 = -1 \neq 0$, per tant $\phi_q - 1$ és un endomorfisme separable.

Corol·lari 4.6. *Sigui E una corba el·líptica definida sobre un cos $\mathbf{F}_q$, llavors $\#E(\mathbf{F}_q) = gr(\phi_q - 1)$.*

Demostració. Utilitzant que $(x, y) \in E(\mathbf{F}_q) \Leftrightarrow \phi_q(x, y) = (x, y)$:

$(x, y) \in E(\mathbf{F}_q) \Leftrightarrow \phi_q(x, y) = (x, y) \Leftrightarrow \phi_q(x, y) - (x, y) = (\phi_q - 1)(x, y) = 0 \Leftrightarrow (x, y) \in ker(\phi_q - 1)$.

Per tant,

$$\#E(\mathbf{F}_q) = \#ker(\phi_q - 1).$$

Com hem vist abans, $(\phi - 1)$ és separable i, aplicant el Teorema 3.26. deduïm que:

$$\#E(\mathbf{F}_q) = gr(\phi_q - 1)$$

Proposició 4.7. *Siguin α i β endomorfismes i a i b nombres enters. Llavors $(a\alpha + b\beta)(P) = a\alpha(P) + b\beta(P)$ és un endomorfisme i*

$$gr(a\alpha + b\beta) = a^2 gr(\alpha) + b^2 gr(\beta) + ab(gr(\alpha + \beta) - gr(\alpha) - gr(\beta)).$$

Es pot trobar la demostració d'aquest resultat a la secció 3.3. de [1].

Corol·lari 4.8. *Siguin r, s nombres enters coprimers entre ells. Llavors*

$$gr(r\phi_q - s) = r^2 q + s^2 - rs(q + 1 - gr(\phi_q - 1)).$$

Demostració. Utilitzant el Lema anterior i sabent que $gr(\phi_q = q)$ i $gr(-1) = 1$ veiem que:

$$gr(r\phi_q - s) = r^2 gr(\phi_q) + s^2 gr(-1) + rs(gr(\phi_q - 1) - gr(\phi_q) - gr(-1)) = r^2 q + s^2 + rs(gr(\phi_q - 1) - q - 1).$$

Després de veure aquests resultats, podem demostrar el Teorema de Hasse:

Teorema 4.9. *Sigui E una corba el·líptica sobre un cos $\mathbf{F}_q$ d'ordre q finit. Llavors:*

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

Demostració. Utilitzant el Corol·lari anterior:

$$0 \leq gr(r\phi_q - s) = r^2 q + s^2 + rs(gr(\phi_q - 1) - q - 1).$$

Dividint per s^2 obtenim:

$$0 \leq (r/s)^2 q + 1 + r/s(gr(\phi_q - 1) - q - 1).$$

Sabem que el conjunt dels nombres racionals és dens en els reals, per tant, per tot nombre real x es compleix que:

$$0 \leq x^2 q + x(gr(\phi_q - 1) - q - 1) + 1.$$

Per tant, el discriminant és menor o igual a 0. És a dir:

$$(gr(\phi_q - 1) - q - 1)^2 - 4q \leq 0$$

i per tant,

$$|(gr(\phi_q - 1) - q - 1)| \leq 2\sqrt{q}.$$

Com $\#E(\mathbf{F}_q) = gr(\phi_q - 1)$:

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

4.2 L'algoritme de Schoof

Per acabar aquesta secció estudiarem l'algoritme de Schoof, el qual ens permet trobar el nombre de punts d'una corba el·líptica en temps polinomial. Aquest algoritme és fonamental per a poder fer criptografia en corbes el·líptiques, doncs ens permet saber el nombre de punts del grup $E(\mathbf{F}_q)$ amb un nombre total d'operacions de l'ordre de $O(log^8 q)$.

Sigui $P = \{2, 3, ..., L\}$ un conjunt de nombres primers tal que

$$\prod_{l \in P} l > 4\sqrt{q}.$$

Anomenarem $a := |q + 1 - \#E(\mathbf{F}_q)| \leq 2\sqrt{q}$, la idea del algoritme és trobar $a \pmod l$ per cada $l \in P$, i així calcular $a \pmod{\prod_{l \in P} l}$. Primer necessitem un resultat previ:

Proposició 4.10. *Sigui q una potència d'un nombre primer i E una corba el·líptica definida sobre $\mathbf{F}_q$. Sigui $(x, y) \in E(\overline{\mathbf{F}_q})$, llavors*

$$((x^q)^2, (y^q)^2) - a(x^q, y^q) + q(x, y) = \infty$$

Es pot trobar la demostració d'aquest resultat a la secció 4.2. de [1].
A continuació ja podem començar amb l'explicació del mètode per trobar $a \pmod l$, separant-lo en dos casos.

Cas $l = 2$

Assumirem que q és senar, així que la paritat de a és la mateixa que la de $\#E(\mathbf{F}_q)$. Llavors $E(\mathbf{F}_q)$ té ordre parell si i només si $E(\mathbf{F}_q)$ té elements d'ordre 2. Aleshores, sigui $P = (x_0, y_0) \in E(\mathbf{F}_q)$, si $P \in E[2]$ llavors $P+P = \infty$ i, per definició, $0 = y_0 = x_0^3 + Ax_0 + B$. Una opció seria provar tots els elements de $\mathbf{F}_q$, però no resulta eficient. Sabem que els elements de $\mathbf{F}_q$ són les arrels de $x^q - x$, per tant, calcularem

$$(x^q - x, x^3 + Ax + B) = (x_q - x, x^3 + Ax + B),$$

on $x_q \equiv x^q \pmod{x^3 + Ax + B}$. Per fer aquest càlcul, utilitzarem l'algoritme d'Euclides. En cas que el resultat sigui 1, llavors $a \equiv 1 \pmod 2$, en cas contrari, $a \equiv 0 \pmod 2$.

En cas que q sigui parell, podem fer un raonament anàleg a aquest i així veiem que si el resultat de

$$(x_q - x, x^3 + Ax + B),$$

és 1, llavors $a \equiv 0 \pmod 2$ i en cas contrari, $a \equiv 1 \pmod 2$.

Cas $l > 2$

Aquest cas és més costós, usarem els polinomis de divisió ψ_n. També utilitzarem la Proposició 4.10. que hem mencionat abans.

Aleshores, sigui $(x, y) \in E[l]$. Llavors

$$(x^{q^2}, y^{q^2}) + q(x, y) = a(x^q, y^q).$$

Considerem $q_l = q \pmod l$, $|q_l| < l/2$ així que

$$(x^{q^2}, y^{q^2}) + q_l(x, y) = a(x^q, y^q).$$

Calcularem tots els elements menys a, i així trobarem $a \pmod l$. Aquí haurem de diferenciar 2 casos:

1) $(x^{q^2}, y^{q^2}) \neq \pm q_l(x,y)$.

2) $(x^{q^2}, y^{q^2}) = \pm q_l(x,y)$.

Comencem pel cas 1): La suma $(x', y') = (x^{q^2}, y^{q^2}) + q_l(x,y)$ es calcula amb les fórmules de la Secció 3.3. Definim

$$j(x,y) = (x_j, y_j)$$

per enters j, trobarem x_j i y_j utilitzant els polinomis de divisió.

Ara ens cal veure com calcular x' de manera eficient. Primer pensem la suma de dos punts iguals com un endomorfisme, tal com hem fet en l'exemple 3.21. obtenim $2(x,y) = (r_1(x), y r_2(x))$, on

$$r_1(x) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}$$

$$r_2(x) = \frac{x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2}{8(x^3 + Ax + B)^2}.$$

Llavors definim $r_{1,j}$ i $r_{2,j}$ tals que $x_j = r_{1,j}(x)$ i $y_j = r_{2,j}(x)y$

$$x' = \left(\frac{y^{q^2} - y_{ql}}{x^{q^2} - x_{ql}}\right)^2 - x^{q^2} - x_{q_l}.$$

D'aquesta manera podem calcular x' només en termes d' x escrivint

$$(y^{q^2} - y_{ql})^2 = y^2(y^{q^2-1} - r_{2,q_l})^2 = (x^3 + Ax + B)\left((x^3 + Ax + B)^{(q^2-1)/2} - r_{2,q_l}\right)^2,$$

aleshores hem de trobar j tal que $(x', y') = (x_j^q, y_j^q)$.
Primer, mirem a la coordenada x. Com $(x,y) \in E[l]$, tenim $(x', y') = \pm(x_j^q, y_j^q)$ si i només si $x' = x_j^q$. Les arrels de ψ_l són les coordenades x dels punts de $E[l]$, la qual cosa implica que

$$x' - x_j^q \equiv 0 \pmod{\psi_l}.$$

En aquest punt hem de provar que ψ_l no té arrels dobles, ja que sinó ϕ_l dividiria alguna potència de $x' - x_j^q$. Com hem vist al Teorema 3.31, existeixen $l^2 - 1$ punts d'ordre l, doncs suposem que l no és la característica de $\mathbf{F}_q$. Per tant, existeixen $(l^2-1)/2$ coordenades x d'aquests punts, que són les arrels de ψ_l, com hem vist al Lema 3.29.
Suposem que hem trobat j enter tal que $x' - x_j^q \equiv 0 \pmod{\psi_l}$, llavors $(x', y') = \pm(x_j^q, y_j^q) = (x_j^q, \pm y_j^q)$. Per determinar el signe, hem de mirar la coordenada y. Podem escriure y'/y i y_j^q/y en termes d'x ja que:

$$y'/y = \frac{m(x_{ql} - x') - y_{ql}}{y} = \frac{m}{y}(x_{ql} - x') - \frac{y_{ql}}{y} = \frac{y^{q^2} - y_{ql}}{y}(x^{q^2} - x_{ql})^{-1}(x_{ql} - x') - r_{2,q_l} =$$

$$(y^{q^2-1} - r_{2,q_l})(x^{q^2} - x_{ql})^{-1}(x_{q_l} - x') - r_{2,q_l} = ((x^3 + Ax + B)^{\frac{q^2-1}{2}} - r_{2,q_l})(x^{q^2} - x_{ql})^{-1}(x_{q_l} - x') - r_{2,q_l},$$

apart que

$$y_j^q/y = (r_{2,j}(x)y)^q/y = y^{q-1} r_{2,j}^q = (x^3 + Ax + B)^{\frac{q-1}{2}} r_{2,j}^q.$$

D'aquesta manera calcularem

$$(y' - y_j^q)/y \equiv (\text{mod } \psi_l).$$

Així que si el resultat és 0, llavors $(x', y') = (x_j^q, y_j^q)$ i en cas contrari $(x', y') = (x_j^q, -y_j^q)$.

Suposem ara que no hem trobat $j \in \{0, ..., (l-1)/2\}$ tal que $(x', y') = (x_j^q, y_j^q)$. Llavors estem en el cas 2), és a dir, $((x^q)^2, (y^q)^2) = \pm q(x, y)$.
Pressuposem primer que

$$(x^{q^2}, y^{q^2}) = q(x, y).$$

Llavors

$$2q(x, y) = a(x^q, y^q).$$

En conseqüència,

$$a^2 q(x, y) = a^2(x^{q^2}, y^{q^2}) = (2q)^2(x, y)$$

Aleshores, $a^2 q \equiv 4q^2 \pmod{l}$. Per tant, q era un quadrat mòdul l. Si no és així, llavors estem en el cas que

$$(x^{q^2}, y^{q^2}) = -q(x, y).$$

Llavors, sigui w tal que $w^2 \equiv q \pmod{l}$, llavors $((x^q, y^q) + w(x, y))((x^q, y^q) - w(x, y)) = (x^{q^2}, y^{q^2}) - q(x, y)$, aleshores tenim que $(x^q, y^q) - w(x, y) = \infty$ o $(x^q, y^q) + w(x, y) = \infty$.
Suposem que $(x^q, y^q) - w(x, y) = \infty$, és a dir, $(x^q, y^q) = w(x, y)$, llavors

$$\infty = (x^{q^2}, y^{q^2}) - a(x^q, y^q) + q(x, y) = w^2(x, y) - aw(x, y) + q(x, y) = q(x, y) - aw(x, y) + q(x, y)$$

Per tant $aw \equiv 2q \equiv 2w^2 \pmod{l}$ i en conclusió $a \equiv 2w \pmod{l}$.
En cas que $(x^q, y^q) = -w(x, y) = w(x, -y)$ d'una manera anàloga, trobem que $a \equiv -2w \pmod{l}$.
Llavors, sabem que $(x^{q^2}, y^{q^2}) = \pm q_l(x, y)$ i ens queda determinar quin signe és.
Sigui $(x_w, y_w) := w(x, y)$, executem l'algoritme d'Euclides per polinomis i trobem

$$(\text{numerador}(x^q - x_w), \psi_l).$$

Si el resultat és 1, llavors no podem estar en el cas

$$(x^{q^2}, y^{q^2}) = q(x, y),$$

així que estem en el cas

$$(x^{q^2}, y^{q^2}) = -q(x, y).$$

En aquest cas, $a(x, y) = (x^{q^2}, y^{q^2}) + q(x, y) = \infty$ i per tant $a \equiv 0 \pmod{l}$ i en cas contrari aleshores $(x^q, y^q) = \pm w(x, y)$. Per acabar, en aquest últim cas, calculem

$$(\text{numerador}(y^q - y_w)/y, \psi_l)$$

i, si el resultat és 1 llavors $(x^q, y^q) + w(x, y) = \infty$ i $a \equiv -2w \pmod{l}$, en cas contrari trobem que $a \equiv 2w \pmod{l}$ d'una manera anàloga.

El mètode es pot resumir en els següents punts: Sigui $E(\mathbf{F}_q)$ una corba el·líptica sobre $\mathbf{F}_q$, volem calcular $\#\mathbf{F}_q = q + 1 - a$.

Resum del mètode

1. Escollim un conjunt de nombres primers $P = \{2, 3, ..., L\}$ tal que

$$\prod_{l \in S} l > 4\sqrt{q}.$$

2. Si $l = 2$, llavors $a \equiv 0 \pmod 2$ si i només si $(x^3 + Ax + B, x^q - x) \neq 1$.

3. Per tot primer senar l, fem el següent:

a) Sigui $q_l \equiv q \pmod l$ tal que $|q_l| < l/2$. Tot seguit calculem $q_l(x, y) = (x_{q_l}, y_{q_l})$ i així trobem $r_{1,q_l} = x_{q_l}$ i $r_{2,q_l} = y_{q_l}/y$.

b) Trobem ψ_l i calculem la coordenada x' de $(x', y') = ((x^q)^2, (y^q)^2) + q_l(x, y) \pmod{\psi_l} = (x^3 + Ax + B)((x^3 + Ax + B)^{\frac{q^2-1}{2}} - r_{2,q_l})^2((x^{q^2} - x_{q_l})^{-1})^2 - x^{q^2} - x_{q_l} \pmod{\psi_l}$.

c) Per $j = 1, 2, ..., (l-1)/2$, fem el següent.

i. Trobem la coordenada x_j de $(x_j, y_j) = j(x, y)$.

ii. Si $x' - x_j^q \equiv 0 \pmod{\psi_l}$, llavors avancem al pas iii. sinó anem provant amb el següent valor de j. Si hem provat tots els valors de j des de 1 a $(l-1)/2$, llavors avancem al pas d).

iii. Trobem

$$y'/y = ((x^3 + Ax + B)^{\frac{q^2-1}{2}} - r_{2,q_l})(x^{q^2} - x_{ql})^{-1}(x_{q_l} - x') - r_{2,q_l}$$

i

$$y_j^q/y = (x^3 + Ax + B)^{\frac{q-1}{2}} r_{2,j}^q.$$

Si $(y' - y_j^q)/y \equiv 0 \pmod{\psi_l}$, llavors $a \equiv j \pmod l$. En cas contrari, $a \equiv -j \pmod l$.

d) Si hem provat tots els valors de j des de 1 a $(l-1)/2$ sense èxit, llavors trobem w tal que $w^2 \equiv q \pmod l$. En cas que no el puguem trobar, llavors $a \equiv 0 \pmod l$.

e) Si el trobem, llavors calculem

$$(numerador(x^q - x_w), \psi_l),$$

si el resultat és 1, llavors $a \equiv 0 \pmod l$. En cas contrari, calculem

$$(numerador(y^q - y_w)/y, \psi_l).$$

Si el resultat és 1, llavors $a \equiv 2w \pmod l$, sinó $a \equiv -2w \pmod l$.

4. Utilitzem tots els valors de $a \pmod l$ per tot $l \in P$ per calcular $a \pmod{\prod_{l \in P} l}$ i utilitzant el Teorema de Hasse per trobar el valor de a que satisfà $|a| \leq 2\sqrt{q}$. El nombre de punts és $\#E(\mathbf{F}_q) = q + 1 - a$.

A continuació veurem un exemple il·lustratiu de l'aplicació de l'algoritme de Schoof. Els càlculs han estat fets amb el programa informàtic Sage.

Exemple 4.11. Sigui E la corba el·líptica definida per $y^2 = x^3 + 2x + 6$ sobre el cos $\mathbf{F}_{23}$. Volem trobar $\#E(\mathbf{F}_q) = q + 1 - a$.

1. Escollim el conjunt $P = \{2, 3, 5\}$ de nombres primers, notem que $2 \cdot 3 \cdot 5 = 30 > 4\sqrt{23}$.

2. Sigui $l = 2$, veiem que

$$(x^3 + 2x + 6, x^{23} - x) = 1.$$

En conseqüència $a \equiv 1 \pmod 2$.

3($l = 3$). Sigui $l = 3$.

a) $q_l = -1 \equiv 23 \pmod 3$, observem que $|-1| < 3/2$. Així $(x_{q_l}, y_{q_l}) = q_l(x, y) = -(x, y) = (x, -y)$ i per tant $r_{1,q_l} = 1$ i $r_{2,q_l} = -1$.

b) Calculem

$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2 = 3x^4 + 12x^2 + 72x - 4$$

i

$$(x^{23^2} - x_{q_l})^{-1} = 12x^3 + 11x^2 + 9x + 8 \pmod{\psi_3}.$$

Amb aquests resultats trobem

$$x' = (x^3 + 2x + 6)((x^3 + 2x + 6)^{\frac{23^2-1}{2}} - (-1))^2(12x^3 + 11x^2 + 9x + 8)^2 - x^{23^2} - x$$

$$= 18x^3 + 18x^2 + 11x + 15 \pmod{\psi_3}.$$

c) Per $1 \leq j \leq \frac{3-1}{2} = 1$:

i) Trobem $(x_1, y_1) = (x, y)$.

ii) $x' - x_1^{23} = 0 \pmod{\psi_3}$. Per tant, $a \equiv 1 \pmod 3$ o $a \equiv -1 \pmod 3$.

iii)Trobem

$$y'/y = ((x^3+2x+6)^{\frac{23^2-1}{2}} - (-1))(x^{23^2} - x)^{-1}(x - x') - (-1) = 3x^3 + 13x^2 + 6x + 4 \pmod{\psi_3}$$

i

$$y_1^{23}/y = y^{23}/y = y^{22} = (x^3 + 2x + 6)^{11} = 3x^3 + 13x^2 + 6x + 4 \pmod{\psi_3}.$$

Aleshores $(y' - y_1^{23}/y) = 0 \pmod{\psi_3}$ i per tant $a \equiv 1 \pmod 3$.

3($l = 5$). Sigui $l = 5$.

a) $q_l = -2 \equiv 23 \pmod 5$. Així

$$(x_{q_l}, y_{q_l}) = q_l(x, y) = -2(x, y) = (r_{1,q_l}, r_{2,q_l} y)$$

on

$$r_{1,q_l} = \frac{x^4 - 4x^2 - 48x + 4}{4(x^3 + 2x + 6)}$$

i

$$r_{2,q_l} = -\frac{x^6 + 10x^4 + 120x^3 - 20x^2 - 48x - 8 - 288}{8(x^3 + 2x + 6)^2}.$$

b) Calculem

$$\psi_5 = \psi_4 \cdot \psi_2^3 - \psi_1 \psi_3^3 = 9x^{12} + 11x^{10} + 15x^9 + 5x^7 + 22x^6 + 5x^5 + 12x^4 + 17x^3 + 18x^2 + 18x + 13$$

i

$$(x^3 + 2x + 6)^{-1} = 15x^{11} + 19x^{10} + 5x^9 + 2x^8 + 3x^7 + 19x^6 + 7x^5 + 14x^4 + 10x^2 + 21x + 10 \pmod{\psi_5}.$$

Gràcies a aquests resultats podem calcular

$$r_{1,q_l} = (x^3+2x+6)^{-1}\frac{x^4-4x^2-48x+4}{4} =$$

$$20x^{11}+2x^9+13x^8+22x^7+7x^6+x^5+11x^3+18x^2+14 \,(\mathrm{mod}\,\psi_5),$$

$$r_{2,q_l} = ((x^3+2x+6)^{-1})^2\frac{x^6+10x^4+120x^3-20x^2-48x-8-288}{8} =$$

$$13x^{10}+x^8+x^7+9x^6+18x^4+x^3+7x^2+13x+12 \,(\mathrm{mod}\,\psi_5)$$

i

$$(x^{23^2}-x_{q_l})^{-1} = 19x^{11}+7x^{10}+4x^9+19x^8+15x^7+4x^6+11x^5+11x^4+21x^3+15x^2+4x+4 \,(\mathrm{mod}\,\psi_5).$$

Ara trobem

$$x' = (x^3+2x+6)((x^3+2x+6)^{\frac{23^2-1}{2}} - r_{2,q_l})^2((x^{23^2}-x_{q_l})^{-1})^2 - x^{23^2} - x_{q_l}$$

$$= 22x^{11}+6x^{10}+10x^9+6x^8+12x^7+14x^6+8x^5+5x^4+2x^3+8x^2+1x+15 \,(\mathrm{mod}\,\psi_5).$$

c) Per $1 \leq j \leq \frac{5-1}{2} = 2$ fem:

i) $j=1$. Trobem $(x_j, y_j) = (x_1, y_1) = (x, y)$.

ii) $x' - x_1^{23} = 4x^{11}+7x^{10}+9x^9+17x^8+14x^7+13x^6+6x^5+19x^4+7x^3+x^2+20x+6 \neq 0 \,(\mathrm{mod}\,\psi_5)$.

i) $j=2$. Trobem $(x_j, y_j) = (x_2, y_2) = 2(x, y) = -(-2(x, y)) = (r_{1,q_l}, -r_{2,q_l}y)$.

ii) $x' - x_2^{23} = x' - r_{1,q_l}^{23} = 13x^{11}+12x^{10}+22x^9+12x^8+3x^7+7x^6+19x^5+12x^4+13x^3+x^2+10x+9 \neq 0 \,(\mathrm{mod}\,\psi_5)$.

d) Veiem que no existeix w tal que $w^2 \equiv 23 \,(\mathrm{mod}\,5)$, doncs el Símbol de Legendre

$$\left(\frac{23}{5}\right) = -1.$$

Per tant $a \equiv 0 \,(\mathrm{mod}\,5)$.

4. Així concluim que $a \equiv 1 \,(\mathrm{mod}\,2)$, $a \equiv 1 \,(\mathrm{mod}\,3)$ i $a \equiv 0 \,(\mathrm{mod}\,5)$. Per tant $a \equiv 25 \,(\mathrm{mod}\,30)$. Com $|a| < 2\sqrt{23}$, deduïm que $a = -5$ i així el grup $E(\mathbf{F}_{23})$ té 23+1-(-5)=29 elements.

5 Criptologia basada en corbes el·líptiques

5.1 Problema del logaritme discret en corbes el·líptiques

Com hem mencionat al final de la secció *Introducció a la Criptologia*, tot l'estudi fet sobre corbes el·líptiques l'emprarem en l'àmbit de la criptologia. Per la definició del grup $E(\mathbf{F}_q)$, no podem fer una factorització en nombres primers, per tant no té sentit l'atac del càlcul de l'índex, l'atac més potent, en aquest grup. Aquí veiem la raó per la qual volem aplicar l'estudi de les corbes el·líptiques a la criptologia.

Observació 5.1. El grup $(E(\mathbf{F}_q), +)$ no és, en general, cíclic, així que el grup escollit per a fer criptografia és un subgrup generat per un punt de $E(\mathbf{F}_q)$, el qual sí serà cíclic.

D'una manera anàloga a la Definició 2.2., podem definir el problema del logaritme discret per a corbes el·líptiques.

Definició 5.2. *Sigui $E(\mathbf{F}_q)$ una corba el·líptica definida sobre el cos finit $\mathbf{F}_q$, P un punt de la corba el·líptica i Q un altre punt de la corba, definim el logaritme discret de Q en la base P sobre $\langle P\rangle \subseteq E(\mathbf{F}_q)$ com l'enter a tal que $Q = aP$. Trobar aquest enter a és resoldre el problema del logaritme discret en corbes el·líptiques.*

Observació 5.3. Veiem que resoldre el problema del logaritme discret en corbes el·líptiques és equivalent a resoldre'l en un grup cíclic qualsevol, amb la desavantatge de no poder utilitzar l'atac del càlcul de l'índex.

Observació 5.4. En el criptosistema de Massey-Omura no necessitem que el grup sigui cíclic, per tant podem escollir el grup $E(\mathbf{F}_q)$, del qual podem calcular l'ordre utilitzant l'algoritme de Schoof, explicat a la secció 4.2.

5.2 Computació del criptosistema en corbes el·líptiques

Dos factors importants que cal tenir en compte és com computar eficientment aP i l'elecció de $\langle P\rangle$ per a un punt P de la corba.

Per a computar aP utilitzarem la representació binària de $a = a_0 + 2a_1 + ... + 2^m a_m$, on $a_i \in 0, 1$ i $m = [\log_2 a]$. Així, tenim l'algoritme següent: Sigui $P \in E(\mathbf{F}_q)$ i un enter $a \geq 1$:

1. Definim $n = P$ i $Q = \infty$.
2. Iterem i des de 0 a m:
   Si $a_i = 1$ llavors redefinim $Q = Q + n$.
   Redefinim $n = 2n$.
3. Retornem Q, on $Q = aP$.

D'altra banda el punt P ha de ser escollit pels dos usuaris prèviament. En aquest moment el millor atac al logaritme discret en corbes el·líptiques és una combinació de l'algoritme de *Pohling-Hellman* i l'algoritme *rho de Pollard*, el qual necessita un temps de resolució de l'ordre de $O(\sqrt{d})$, on d és el divisor primer major de l'ordre de $\langle P\rangle$, per tant convé escollir un punt P tal que d sigui d'ordre suficientment gran. En aquests moments d ha de ser major a 2^{160}. Llavors, el problema és com calcular eficientment l'ordre d'un punt p en una corba $E(\mathbf{F}_q)$. Farem els passos següents:

1. Calculem $N = \#E(\mathbf{F}_q)$, utilitzant l'algoritme de Schoof.

2. Escollim l'ordre n del subgrup, caldrà que n sigui primer i, pel Teorema de Lagrange, sabem que serà un divisor d'N.

3. Calculem l'índex $[N : n] = N/n$.

4. Escollim un punt aleatori P de la corba.

5. Computem $g = [N : n]P$.

6. Si $g = 0$, llavors tornem al pas 4. En cas contrari g és un generador d'un subgrup de $E(\mathbf{F}_q)$ d'ordre n ja que $ng = n(N/n)P = NP = \infty$.

Observació 5.5. La importància de la primeritat d'n radica en que si n té un divisor n_1 llavors potser $n_1 g = \infty$ i per tant l'ordre de g no seria de l'ordre desitjat.

Observació 5.6. Veiem que és necessari factoritzar N, per tant l'eficiència del mètode depèn del grup $E(\mathbf{F}_q)$ escollit.

5.3 L'atac MOV

Gràcies a la teoria matemàtica darrere les corbes el·líptiques també existeix un atac al logaritme discret en corbes el·líptiques, l'atac MOV. Aquest atac va ser ideat per Menezes, Okamoto i Vanstone l'any 1993. La idea de l'atac és utilitzar l'aparellament de Weil per convertir un problema del logaritme discret en $E(\mathbf{F}_q)$ a un en $\mathbf{F}_{q^m}^*$, $m \geq 1$. Llavors, atacant amb l'algoritme del càlcul de l'índex podem resoldre el problema a $\mathbf{F}_{q^m}^*$.

Sigui $E(\mathbf{F}_q)$ una corba el·líptica a $\mathbf{F}_q$. Siguin P, $Q \in E(\mathbf{F}_q)$. Sigui n l'ordre de P. Assumim que $(n, q) = 1$, volem trobar k tal que $Q = kP$. Primer ens cal comprovar que k existeix.

Lema 5.7. *Existeix k tal que $Q = kP$ si i només si $nQ = \infty$ i l'aparellament de Weil $e_n(P, Q) = 1$.*

Demostració. Si $Q = kP$, llavors $nQ = knP = k\infty = \infty$. També:

$$e_n(P, Q) = e_n(P, kP) = e_n(P, P)^k = 1^k = 1$$

on hem utilitzat el fet que l'aparellament de Weil és bilineal en cada variable per a la segona igualtat. D'altra banda, si $nQ = \infty$, llavors $Q \in E[n]$. Com $(n, q) = 1$, tenim que $E[n] \simeq \mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/n\mathbf{Z}$. pel Teorema 3.31. Llavors, escollim un punt R tal que P, R sigui una base de $E[n]$. Llavors

$$Q = aP + bR$$

per alguns enters a, b. Pel Corol·lari 3.34. $e_n(P, R) = \zeta$ és una arrel primitiva n-èssima de la unitat. Per tant, si $e_n(P, Q) = 1$, tenim

$$1 = e_n(P, Q) = e_n(P, aP)e_n(P, bR) = e_n(P, P)^a e_n(P, R)^b = \zeta^b.$$

on tornem a utilitzar la bilinealitat de cada variable de l'aparellament de Weil. Això implica que $b \equiv 0 \pmod{n}$ així que $bR = \infty$. Per tant, $Q = aP$, com es volia demostrar.

Havent provat aquest lema, comencem escollim m tal que

$$E[n] \subseteq E(\mathbf{F}_{q^m})$$

Com tots els punts de $E[n]$ tenen coordenades a $\overline{\mathbf{F}_q} = \bigcup_{j\geq 1} \mathbf{F}_{q^j}$ existeix tal m. Pel Corol·lari 3.35, $\mu_N \subseteq \mathbf{F}_{q^m}$. Llavors l'algoritme és:

1. Escollim un punt aleatori $T \in E(\mathbf{F}_{q^m})$.

2. Computem l'ordre M de T.

3. Sigui $d = (M, n)$ i sigui $T_1 = (M/d)T$. Llavors T_1 té ordre d i, com $d|n$ deduïm que $T_1 \in E[n]$.

4. Computem $\zeta_1 = e_n(P, T_1)$ i $\zeta_2 = e_n(Q, T_1)$, llavors tan ζ_1 com ζ_2 pertanyen a $\mu_d \subseteq \mathbf{F}^*_{q^m}$.

5.Resolem el problema del logaritme discret $\zeta_2 = \zeta_1^k$ a $\mathbf{F}^*_{q^m}$.

6.Repetim el procés amb punts aleatoris T fins que el mínim comú múltiple de suficients "d"s sigui n. Això determina $k \pmod n$. Per tant, hem reduït el problema del logaritme discret en $E(\mathbf{F}_q)$ a un en $\mathbf{F}^*_{q^m}$.

L'atac MOV ens imposa una condició addicional alhora d'escollir el grup $E(\mathbf{F}_q)$, doncs si m és massa petit llavors l'atac MOV i posteriorment l'algoritme del càlcul de l'índex simplifica molt el problema del logaritme discret en corbes el·líptiques. Sabem que $\mathbf{F}^*_{q^m}$ té ordre $q^m - 1$ i que l'algoritme del càlcul de l'índex per a $\mathbf{F}^*_{q^m}$ necessita un temps de l'ordre de $O(\exp\sqrt{2\ln(q^m-1)\ln\ln(q^m-1)})$. També sabem que el millor atac al logaritme discret en corbes el·líptiques necessita un temps de l'ordre de $O(\sqrt{d}) = (\exp\frac{1}{2}\ln d)$, on d és el divisor primer major de l'ordre del subgrup cíclic P de $E(\mathbf{F}_q)$ escollit per a fer criptografia. Llavors, suposant que q^m és un nombre molt gran, podem aproximar $q^m - 1$ a q^m per a fer els càlculs següents:

$$(\exp\sqrt{2\ln q^m \ln\ln q^m}) > (\exp\sqrt{\ln q^{2m}}),$$

suposem ara que $E(\mathbf{F}_q) > q + 1$, llavors

$$2\sqrt{q} \geq |q + 1 - \#E(\mathbf{F}_q)| = \#E(\mathbf{F}_q) - (q + 1),$$

per tant

$$\#E(\mathbf{F}_q) \leq q + 1 + 2\sqrt{q} = (\sqrt{q} + 1)^2.$$

Al ser d el divisor primer major de l'ordre d'un subgrup P de $E(\mathbf{F}_q)$, clarament $d < \sqrt{\#E(\mathbf{F}_q)} \leq \sqrt{(\sqrt{q}+1)^2} = \sqrt{q} + 1$. Aleshores, al ser q un nombre molt gran, podem afirmar també que $d < \sqrt{q}$ i així:

$$\exp\frac{1}{2}\ln d < \exp\frac{1}{2}\ln\sqrt{q} < \exp\sqrt{\ln q^{2m}} \Leftrightarrow \frac{1}{2}\ln\sqrt{q} < \sqrt{\ln q^{2m}}$$

$$\Leftrightarrow \frac{1}{4}\ln^2\sqrt{q} < \ln q^{2m} \Leftrightarrow \ln^2\sqrt{q} < \ln q^{8m} \Leftrightarrow q^{\frac{1}{4}\ln q} < q^{8m} \Leftrightarrow \ln q < 32m.$$

Per tant imposant que $m > \frac{1}{32}\ln q$ i que $E(\mathbf{F}_q) > q + 1$ ens assegurem que l'atac MOV no és més eficaç que intentar resoldre el problema del logaritme discret en corbes el·líptiques.

Aleshores, sigui $E(\mathbf{F}_q)$ una corba el·líptica a $\mathbf{F}_q$. Siguin P, $Q \in E(\mathbf{F}_q)$. Sigui n l'ordre de P i volem trobar k tal que $Q = kP$, sabem que

$$\langle P\rangle \subset E[n] \subseteq E(\mathbf{F}_{q^m}).$$

Llavors $n|\#E(\mathbf{F}_{q^m})$, pel Teorema de Lagrange. Així, per comprovar que el grup $\langle P\rangle$ és segur trobem $\#E(\mathbf{F}_{q^m})$ amb l'algoritme de Schoof i comprovem que n no divideix $E(\mathbf{F}_q^m)$ per als valors m tals que $m < \frac{1}{32}\ln q$.

6 Conclusions

Aquest treball és un estudi de la criptologia basada en corbes el·líptiques. Hem començat introduint-nos en el concepte de criptologia i després hem parlat de la criptografia asimètrica, on hem vist els primers algoritmes matemàtics. Més tard ens hem centrat en la criptografia basada en el problema del logaritme discret, on hem vist diversos algoritmes criptogràfics, seguit d'alguns algoritmes de criptoanàlisi que tenen com a objectiu trencar la seguretat d'aquest tipus de criptografia. El més potent d'aquests algoritmes de criptoanàlisi ens ha donat una idea de l'interès de la criptologia basada en corbes el·líptiques. Tot seguit, hem començat amb un estudi introductori de les corbes el·líptiques. Hem vist les seves propietats bàsiques, les quals hem utilitzat posteriorment. A continuació ens hem centrat en l'estudi de les corbes el·líptiques sobre cossos finits, acabant amb l'algoritme de Schoof del qual hem fet un exemple il·lustratiu. Finalment hem utilitzat l'estudi anterior per a fer criptologia en corbes el·líptiques, enllaçant-ho amb el principi del treball.

Els coneixements bàsics que s'han fet servir pertanyen a les assignatures d'Estructures algebràiques, Equacions Algebràiques i Introducció a la Criptologia, de segon, tercer i quart curs del Grau de Matemàtiques, respectivament. Ha estat necessari consultar diversos materials bibliogràfics, a més de necessitar un programa informàtic per a fer els càlculs de l'exemple il·lustratiu.

Considero que s'han complert els objectius previstos tot i que encara hi hagi molt per aprendre, tant en criptologia com en corbes el·líptiques.

Referències

[1] Washington, L.C.: *Elliptic Curves: Number Theory and Cryptography*, 5a edició, *2007*.

[2] Pohlig, S. i Hellman, M.: *An Improved Algorithm for Computing Logarithms over GF(p) and its Cryptographic Significance*, IEEE Transactions on Informacion Theory 24, 106, 110, *1978*.

[3] Caballero, P.: *Introducción a la Criptografia*, 2a edició, *2002*.

[4] Diffie, W. i Hellman, M.: *New directions in Cryptography*, IEEE Transactions on Informacion Theory 22, 644- 654, *1976*.

[5] Balasubramanian, R. i Koblitz, N.: *The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm.* J. Cryptology, 11(2):141–145, *1998*.

[6] Hoffstein, J., Pipher, J. i Silverman, J.: *An Introduction To Mathematical Cryptography*, 1a edició, *2008*.

[7] Silverman, H. i Suzuki, J.: *Elliptic Curve Discrete Logarithms and the Index Calculus.* K. Ohta and D. Pei (Eds.): ASIACRYPT'98, LNCS 1514, 110-125, *1998*.

[8] Teske, E.: *Speeding up Pollard's method for computing discrete logarithms*, Algorithmic Number Theory Symposium (ANTS IV), LNCS 1423, 541-553, *1998*.

[9] Santamaria, J.: *El logaritmo discreto y sus aplicaciones en Criptografía* (tesi de llicenciatura), Universitat de Cantàbria, Santander.

[10] Koblitz, N.: *A Course in Number Theory and Cryptography*, 2a edició, *1987*.

[11] Corbellini, A.: Elliptic Curve Cryptography: finite fields and discrete logarithms, *https://math.stackexchange.com/questions/1257988/hasses-theorem-for-elliptic-curves-over-finite-fields-proof-clarification*.