Butlletí de la Societat Catalana de Matemàtiques
Vol. 34, núm. 2, 2019. Pàg. 125–151. DOI: 10.2436/20.2002.01.88

Isogènies, codis i reticles en criptografia postquàntica

Ramsès Fernàndez-València

> Que feliç que era la cigala a l'estiu! El sol lluïa, les flors desprenien la seva aroma embriagadora i la cigala cantava i cantava. El futur no la preocupava gens: el cel era tan blau sobre el seu cap i les seves cançons tan alegres... però l'estiu no és etern.
>
> **Isop (620–564 a. C.)**

Resum: En aquest article presentem una breu introducció a alguns dels conceptes i de les tècniques matemàtiques que estan essent utilitzades en criptografia postquàntica. S'introdueixen la teoria de reticles, la teoria de codis i la teoria d'isogènies de corbes el·líptiques supersingulars.

Paraules clau: reticle, codi, isogènia, corba el·líptica supersingular.

Classificació MSC2010: 11T71, 14G50, 94A60.

1 Introducció

Actualment qualsevol transferència de dades comporta un procés de xifratge per tal de fer aquesta informació ininteL·ligible quan s'envia a través de canals que no sempre són segurs. Els mecanismes de xifratge que més s'estan utilitzant, com RSA, ElGamal o ECC, fonamenten la seva seguretat i resistència principalment en els problemes següents:

1. Factorització en producte de dos primers: donat un número $a \in \mathbb{Z}$, trobar dos números primers $p, q \in \mathbb{Z}$ tals que $a = p \cdot q$.
2. Logaritmes discrets: donats un grup $(G, \cdot)$ i dos elements $a, b \in G$, trobar $k \in \mathbb{Z}$ tal que $a = b^k$.

Se sap que aquests dos problemes són computacionalment complexos per als ordinadors actuals, la qual cosa vol dir que els mètodes de xifratge que recolzen sobre aquests problemes resistirien atacs informàtics amb l'objectiu de desxifrar els missatges xifrats sempre que la implementació fos correcta, fet que pot assolir-se, per exemple, fent servir els números primers adequats.

Fins ara s'ha considerat que els mètodes de xifratge fonamentats en els problemes 1 i 2 són segurs però, a començament dels anys vuitanta, Richard Feynman i Yuri Manin, entre d'altres, van començar a teoritzar sobre la possibilitat de fer servir idees de la física quàntica en computació.

El món de la ciberseguretat va viure amb una certa tranquil·litat fins que Peter Shor va presentar un algorisme quàntic que resolia en temps polinomial no només el problema de la factorització en primers, sinó també el problema del logaritme discret [19]. De sobte, els problemes sobre els quals recolzaven els sistemes criptogràfics més emprats deixaven de ser, teòricament, computacionalment complexos: tan bon punt arribés una computadora quàntica programable capaç d'executar l'algorisme de Shor, tots els missatges xifrats podrien ser desxifrats.

D'ençà que es va presentar l'algorisme de Shor, la preocupació per mantenir la privadesa de les dades mitjançant nous algorismes ha anat creixent fins al punt de passar de ser una petita preocupació a una prioritat en algunes empreses. Per què? Degut a la possibilitat de tenir ordinadors quàntics en qüestió de pocs anys. Actualment Microsoft, Google, IBM i D-Wave Systems són les empreses que lideren la recerca en l'anomenada *supremacia quàntica*; de fet, D-Wave Systems ha creat ordinadors quàntics, tot i que cal aclarir que són ordinadors que resolen un tipus concret de problema. L'objectiu final de la supremacia quàntica és la creació d'un ordinador quàntic universal, capaç de resoldre qualsevol tipus de problema; en aquesta direcció IBM i Microsoft estan fent passes cada cop més grans, amb tècniques que involucren conceptes de la topologia algebraica en el cas de la recerca duta a terme per Microsoft.

Davant l'aparició imminent dels primers ordinadors quàntics, cal buscar les eines matemàtiques adequades per generar algorismes de xifratge resistents als atacs d'un ordinador quàntic. Si abans la teoria de nombres era la font principal d'eines per a la creació d'algorismes criptogràfics, ara ho és la geometria algebraica. En són exemples:

1. La teoria de reticles: els problemes del vector més curt i del vector més proper estan generant algorismes de xifratge de clau pública, de signatura digital i d'intercanvi de claus.
2. La teoria de codis algebraics: bàsicament parlem de codis de Goppa. L'algorisme més famós fonamentat en aquesta teoria és el McEliece.
3. La teoria d'isogènies de corbes el·líptiques supersingulars: és un camp nou en criptografia, però molt prometedor. Els algorismes que se'n deriven són focus de recerca actual en l'àmbit de la seguretat.

La criptografia postquàntica ha esdevingut un camp de recerca molt actiu que ha obert una gran quantitat de fronts, tant en l'àmbit aplicat com en el teòric, que atrauen un nombre creixent d'empreses, centres tecnològics i grups de recerca.

L'objectiu d'aquestes notes és concentrar en una font única les principals tècniques matemàtiques involucrades en criptografia postquàntica. En particular estudiarem les tres teories esmentades abans: les teories de reticles, d'isogènies i de codis.

És important observar dos aspectes pel que fa a aquest article: d'una banda, aquestes notes no inclouen un estudi entre la complexitat computacional dels problemes que es deriven de les diferents tècniques matemàtiques i la seva resistència a la computació quàntica. Els interessats en aquests aspectes trobaran una molt bona introducció en [17]. D'una altra banda, la secció sobre els codis s'estudia àmpliament a [18] i [25]. Els interessats en els codis correctors d'errors poden complementar la informació que trobin en aquestes notes amb l'estudi contingut en la referència.

2 Reticles

2.1 Definicions fonamentals

Un reticle és un subconjunt discret i additiu $\Lambda \subseteq \mathbb{R}^n$, és a dir, tal que:

(1) és tancat respecte de la suma i de la resta: $x \pm y \in \Lambda$, $\forall x, y \in \Lambda$, i

(2) existeix $\epsilon > 0$ tal que $\forall x, y \in \Lambda$, $x \neq y$, se satisfà $\|x - y\| \geq \epsilon$. Dit d'una altra manera, $\forall x \in \Lambda$ existeix una bola tancada $B_\epsilon(x)$ amb centre en x i amb radi $\epsilon > 0$ tal que $\Lambda \cap B_\epsilon(x) = \{x\}$.

EXEMPLE. El conjunt $\mathbb{Q}^n \subseteq \mathbb{R}^n$ és un subconjunt tancat respecte de la suma i de la resta, però no és un reticle ja que $\mathbb{Q}$ no és discret. L'exemple de reticle més senzill és $\mathbb{Z}^n$.

Donat un conjunt $B = \{b_1, \ldots, b_m\}$ amb m vectors linealment independents de $\mathbb{R}^n$, el reticle generat per B és:

$$\Lambda(B) := \left\{ \sum_{i=1}^{m} z_i b_i \mid z_i \in \mathbb{Z} \right\}.$$

Habitualment B s'anomena *base del reticle* $\Lambda(B)$ i es diu que Λ és generat per B. Anomenarem *rang de* Λ el valor m, i *dimensió de* Λ el valor n. Quan $m = n$ parlem de *reticles de rang màxim*.

Si pensem en el conjunt B com una matriu $n \times m$

$$B = \begin{pmatrix} b_{1,1} & \ldots & b_{m,1} \\ \vdots & \ddots & \vdots \\ b_{1,n} & \ldots & b_{m,n} \end{pmatrix},$$

amb columnes formades pels vectors $\{b_1, \ldots, b_m\}$, aleshores s'escriu

$$\Lambda := \Lambda(B) = \{B \cdot z \mid z \in \mathbb{Z}^m\} = B \cdot \mathbb{Z}^m.$$

Donada una base B per a un reticle Λ, definim

$$\operatorname{span}(\Lambda) := \operatorname{span}(B) = \{B \cdot y \mid y \in \mathbb{R}^m\}.$$

OBSERVACIÓ. La principal diferència entre $\Lambda(B)$ i $\operatorname{span}(\Lambda)$ és que en el primer cas es fan servir elements enters, i en el segon en fem servir de reals.

Centrem tot seguit la nostra atenció en les bases que generen el mateix reticle.

LEMA 1 ([15, lema 2.5]). *Dues bases $B = \{b_1, \dots, b_m\}$ i $B' = \{b'_1, \dots, b'_m\}$ de $\mathbb{R}^n$ generen el mateix reticle Λ si, i només si, existeix una matriu unimodular U (i.e. invertible a $M_{m\times m}(\mathbb{Z})$) tal que $B = B' \cdot U$. En aquest cas direm que les bases B i B' són equivalents.*

COROL·LARI 2 ([11, teorema 2]). *Si dues bases B, B' generen el mateix reticle de rang màxim, aleshores* $\det(B) = \pm \det(B')$.

COROL·LARI 3. *Dues bases B, B' generen el mateix reticle de rang màxim si, i només si, $(B')^{-1}B$ és unimodular.*

PROVA. En efecte, suposem que U és una matriu unimodular d'ordre n. Aleshores: $\Lambda(B) = \Lambda(B') \Leftrightarrow B = B' \cdot U \Leftrightarrow (B')^{-1}B = U$. □

2.2 Regions fonamentals

Donat un reticle Λ, una *regió fonamental* de Λ és un subconjunt $F \subseteq \mathbb{R}^n$ tal que $\forall x \in \Lambda$ el conjunt $x + F = \{x + y \mid y \in F\}$ genera una partició de $\mathbb{R}^n$, és a dir: $\bigsqcup_{x\in\Lambda} x + F = \mathbb{R}^n$.

Donat un reticle $\Lambda(B)$, definim el *paral·lelepípede fonamental* associat a B com el conjunt $P(B) = \{\sum_i z_i b_i \mid z_i \in [0, 1)\}$.

LEMA 4 ([15, lema 2.10]). *Considerem un reticle $\Lambda(B)$ i una regió fonamental F del reticle $\mathbb{Z}^n$. Aleshores el conjunt $B \cdot F = \{B \cdot z \mid z \in F\}$ és una regió fonamental de $\Lambda(B)$. En particular, $P(B)$ és una regió fonamental de $\lambda(B)$.*

El resultat següent ens permet establir una condició per determinar si un conjunt format per vectors linealment independents de Λ n'és una base:

LEMA 5 ([16, lema 1]). *Donat un reticle Λ de rang màxim i $B = \{b_1, \dots, b_n\}$ un conjunt de vectors de Λ linealment independents, aleshores B és una base de Λ si, i només si, $\Lambda \cap P(B) = \{0\}$.*

Per a un reticle $\Lambda = \Lambda(B)$ generat per una base B, definim el seu determinant com el volum del paral·lelepípede fonamental associat a B i el denotarem per $\operatorname{vol}(P(B))$ o bé $\det(\Lambda)$. El resultat següent és immediat:

PROPOSICIÓ 6 ([11, proposició 2]). *Per a qualsevol base $B = \{b_1, \dots, b_m\}$, amb $b_i \in \mathbb{R}^n$, tenim la igualtat* $\det(\Lambda(B)) = \sqrt{\det(B^T B)}$. *En particular, si $B \in M_{n\times n}(\mathbb{R})$ és no singular, aleshores:* $\det(\Lambda) = |\det(B)|$.

OBSERVACIÓ. Notem l'abús de notació: escrivim B tant per denotar la base com la matriu associada.

El resultat següent prova que el volum és un invariant reticular:

COROL·LARI 7. *Donades dues bases equivalents B_1 i B_2, el volum dels paral·lelepípedes associats és el mateix.*

PROVA. En efecte, com que les bases són equivalents existeix una matriu unimodular U tal que $B_2 = B_1 \cdot U$. Es dedueix el resultat tot calculant determinants.□

2.3 Ortogonalització de Gram-Schmidt

El procediment d'ortogonalització de Gram-Schmidt té un paper important en la teoria de reticles necessària en criptografia ja que s'empra en la creació de bases que es fan servir com a clau privada en alguns algorismes, com el GGH [28].

Recordem que el procés permet trobar, a partir d'un conjunt de vectors B, un conjunt de vectors $B^\star$ tal que els seus elements són ortogonals entre si i tal que $\text{span}(B^\star) = \text{span}(B)$.

Si tenim $B = \{b_1, \dots, b_n\}$, amb $b_i \in \mathbb{R}^n$, els elements de $B^\star$ es calculen fent

$$b_1^\star = b_1, \quad b_i^\star = b_i - \sum_{j<i} \frac{\langle b_i, b_j^\star \rangle}{\langle b_j^\star, b_j^\star \rangle} b_j^\star = b_i - \sum_{j<i} \mu_{i,j} b_j^\star, \quad i \geq 2. \tag{1}$$

El procés el podem interpretar com la descomposició de la matriu B en forma $B = B^\star \cdot M$, on M és la matriu triangular superior tal que $\text{diag}(M) = \{1, \dots, 1\}$ i $m_{i,j} = \mu_{j,i}$ per a $j < i$. Com que $B^\star T B^\star = D^2$, on D és la matriu diagonal amb entrades $\|b_i^\star\|$ per a $i \in \{1, \dots, n\}$, s'obté també la descomposició de $B^\star$ com $B^\star = QD$, amb Q matriu ortogonal.

PROPOSICIÓ 8 ([15, lema 2.1]). *Per a tot reticle $\Lambda = \Lambda(B)$ de rang màxim tenim la igualtat* $\det(\Lambda) = \prod_i \|b_i^\star\|$.

Considerem ara, per a cada i, l'aplicació $\pi_i \colon \mathbb{R}^n \to \text{span}(b_1, \dots, b_{i-1})^\perp$ definida com

$$\pi_i(v) = \sum_{j=i}^{n} \frac{\langle v, b_j^\star \rangle}{\langle b_j^\star, b_j^\star \rangle} b_j^\star.$$

Observem que $\pi_1(b_1), \pi_2(b_2), \dots, \pi_n(b_n)$ són els vectors ortogonals entre si, obtinguts mitjançant el procediment de Gram-Schmidt (1), de $\{b_1, \dots, b_n\}$.

2.4 Forma normal d'Hermite

De la mateixa manera que el procés de Gram-Schmidt genera bases que es fan servir com a claus privades en alguns algorismes de xifratge, la forma normal d'Hermite té un paper rellevant en aquests algorismes degut a la seva importància a l'hora de crear les claus públiques [11].

Una matriu $B \in M_{m\times n}(\mathbb{R})$ està en forma normal d'Hermite (escriurem HNF) si, i només si, per a tot $1 \leq i, j \leq m$ tenim

$$\begin{cases} b_{i,j} = 0 & \text{si } i < j, \\ b_{i,j} \geq 0 & \text{si } i \geq j, \\ b_{i,j} \leq b_{j,j} & \text{si } i > j. \end{cases}$$

Els resultats següents són estàndard (vegeu [11]):

LEMA 9. *Per a tota matriu B i tota matriu unimodular U existeix una matriu H en HNF tal que $H = BU$.*

LEMA 10. *Si dues matrius H_1 i H_2 estan en HNF i són equivalents, aleshores $H_1 = H_2$.*

2.5 Reticle dual

Donat un reticle $\Lambda(B)$ generat per una base $B = \{b_1, \ldots, b_m\}$ amb $b_i \in \mathbb{R}^n$, el *reticle dual* associat és el conjunt

$$\widehat{\Lambda(B)} := \{y \in \operatorname{span}(B) \mid \langle x, y\rangle \in \mathbb{Z},\ \forall x \in \Lambda(B)\}.$$

Mantenint les notacions, la *base dual* de B és el conjunt $D = \{d_1, \ldots, d_m\} \subseteq \mathbb{R}^n$ tal que:

(1) $\operatorname{span}(B) = \operatorname{span}(D)$ i

(2) $B^T D = \mathrm{Id}_m$.

Utilitzant (1) i (2), tenim que $D = B \cdot (B^T B)^{-1}$.

El resultat següent dona al reticle dual, tal com indica el seu nom, l'estructura de reticle:

PROPOSICIÓ 11 ([16, afirmació 11]). *Si D és la base dual de B, aleshores tenim $\widehat{\Lambda(B)} = \Lambda(D)$.*

A continuació presentem una afirmació habitual en espais vectorials duals:

LEMA 12 ([16, afirmació 2]). *El doble dual d'un reticle és el reticle original: $\widehat{\widehat{\Lambda(B)}} = \Lambda(B)$.*

LEMA 13 ([11, proposició 6]). *Per a tot reticle de rang màxim tenim la igualtat $\det(\widehat{\Lambda(B)}) = (\det(\Lambda(D)))^{-1}$.*

La relació existent entre la base dual i el procés de Gram-Schmidt és estreta i s'estableix mitjançant els resultats següents, el primer dels quals prova que el procés d'ortogonalització no afecta la dualitat:

PROPOSICIÓ 14 ([11, proposició 12]). *Si considerem dues bases* $B = \{b_1, \dots, b_n\}$ *i* $D = \{d_1, \dots, d_n\}$ *duals, les bases* $B' = \{\pi_i(b_i), \dots, \pi_i(b_n)\}$ *i* $D' = \{d_i, \dots, d_n\}$ *també són duals, per a tot* $i \in \{1, \dots, n\}$.

PROPOSICIÓ 15 ([16, afirmació 7]). *Considerem* $B = \{b_1, \dots, b_n\}$ *una base i la seva base ortogonal, obtinguda mitjançant el procediment de Gram-Schmidt,* $B^\star = \{b_1^\star, \dots, b_n^\star\}$. *Considerem també la base dual* $D = \{d_1, \dots, d_n\}$ *de* B *i la seva base ortogonal, obtinguda mitjançant el procediment de Gram-Schmidt,* $D^\star = \{d_1^\star, \dots, d_n^\star\}$. *Aleshores, per a tot* $i \in \{1, \dots, n\}$ *es compleix* $d_i^\star = \frac{b_i^\star}{\|b_i^\star\|^2}$.

2.6 Reticles q-aris

Els reticles q-aris tenen un paper important en criptografia basada en reticles ja que permeten relaxar les hipòtesis sobre els reticles sense perdre propietats relatives a la seguretat. Els sistemes que recolzen sobre aquesta mena de reticle tenen una complexitat computacional similar a la de problemes com el SIS o LWE [13], dels quals se sap que són tan complexos com els problemes més complexos en teoria de reticles.

Donat un enter q, un reticle Λ s'anomena *q-ari* si existeix $q \in \mathbb{Z}$ tal que $q \cdot \mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$, és a dir, Λ defineix un subgrup del grup additiu $\mathbb{Z}_q^n$.

LEMA 16 ([11, teorema 3]). *Si* $B \in M_{n\times n}(\mathbb{Z})$ *és una matriu no singular, aleshores* $\det(\Lambda(B)) \cdot \mathbb{Z}^n \subseteq \Lambda(B)$.

Donat un enter q, dos naturals $m < n$ i una matriu $A \in M_{n\times m}(\mathbb{Z})$ de rang màxim per columnes, considerem els reticles q-aris

- $\Lambda_q(A) = \{x \in \mathbb{Z}^n \mid x \equiv Ay \pmod q \text{ per a un cert } y \in \mathbb{Z}^m\} = A \cdot \mathbb{Z}^m + q\mathbb{Z}^n = \Lambda(A) + q\mathbb{Z}^n$.
- $\Lambda_q^\perp(A) = \{x \in \mathbb{Z}^n \mid A^t x = 0 \pmod q\}$.

LEMA 17 ([12, proposició 9]). *Amb les notacions anteriors tenim:*

(1) $q \cdot \widehat{\Lambda_q^\perp(A)} = \Lambda_q(A)$.

(2) $q \cdot \widehat{\Lambda_q(A)} = \Lambda_q^\perp(A)$.

PROVA. Només demostrarem el punt (1). La prova del punt (2) és anàloga:

$$\Lambda_q^\perp(A) = \{y \in \mathbb{Z}^m \mid Ay \equiv 0 \bmod q\} = \{y \in \mathbb{Z}^m \mid A^T Ay = A^T qx,\, x \in \mathbb{Z}^n\} =$$
$$= \{y \in \mathbb{Z}^m \mid y = (A^T A)^{-1} A^T qx,\, x \in \mathbb{Z}^n\}.$$

De manera que la base de $\Lambda_q^\perp(A)$ és $(A^T A)^{-1} A^T q$, per tant, la base per a $q \cdot \Lambda_q^\perp(A)$ és $(A^T A)^{-1} A^T$. Si $(A^T A)^{-1} A^T$ és la base de $q \cdot \Lambda_q^\perp(A)$, la seva dual serà:

$$(A^T A)^{-1} A^T (((A^T A)^{-1} A^T)^T (A^T A)^{-1} A^T)^{-1} = \cdots = A^T,$$

que és la base de $\Lambda_q(A)$. □

2.7 Mínims successius

Considerem, donat un reticle Λ, la longitud del vector no nul més curt de Λ, i denotem-la per $\lambda_1(\Lambda)$:

$$\lambda_1(\Lambda) := \min_{v \in \Lambda - \{0\}} \|v\| = \min_{x \neq y \in \Lambda} \|x - y\|.$$

Observem que $\lambda_1(\Lambda)$ és el paràmetre r més petit tal que els punts de Λ que pertanyen a una bola tancada de radi r generen un espai vectorial de dimensió 1. Podem generalitzar aquest concepte i introduir el concepte de mínims successius. Donat un reticle Λ de rang n, definim el *i-èsim mínim successiu* com:

$$\lambda_i(\Lambda) := \inf\{r \in \mathbb{R} \mid \dim(\operatorname{span}(\Lambda \cap \overline{B}_r(0))) \geq i\}, \quad i \in \{1, \dots, n\}.$$

Les proposicions següents ens permetran fitar $\lambda_1(\Lambda)$, tant superiorment com inferior. La primera de les proposicions estableix una fita inferior:

PROPOSICIÓ 18 ([16, teorema 5]). *Per a qualsevol base B i la seva ortogonal per Gram-Schmidt associada $B^\star$ tenim $\lambda_1(\Lambda) \geq \min_{i \in \{1,\dots,n\}} \|b_i^\star\|$.*

PROPOSICIÓ 19 (BLICHFELD, [11, teorema 5]). *Donats un conjunt $S \subseteq \mathbb{R}^n$ i un reticle $\Lambda(B)$ de rang màxim tals que $\operatorname{vol}(S) > \det(\Lambda)$, existeix un parell de punts $z_1, z_2 \in S$ tal que $z_1 - z_2 \in \Lambda$.*

PROPOSICIÓ 20 (COS CONVEX DE MINKOWSKI, [16, teorema 9]). *Mantenint les notacions de la proposició anterior, si $S \subseteq \mathbb{R}^n$ és un subconjunt simètric (i. e. $x \in S \Rightarrow -x \in S$), convex tal que $\operatorname{vol}(S) > 2^n \det(\Lambda)$, aleshores $\exists x \neq 0$ tal que $x \in S \cap \Lambda(B)$.*

El resultat anterior ens assegura l'existència d'un punt de Λ dintre d'un conjunt convex i simètric S, sempre que S sigui prou gran. Com a corol·lari de les dues proposicions anteriors obtenim aquesta fita superior per a $\lambda_1(\Lambda)$:

PROPOSICIÓ 21 ([16, corol·lari 2]). *Per a qualsevol reticle $\Lambda(B)$ de rang màxim n tenim $\lambda_1(\Lambda) \leq \sqrt{n}\, \sqrt[n]{\det(\Lambda)}$.*

2.8 Problemes en teoria de reticles

Els problemes en teoria de reticles poden dividir-se principalment en dos blocs: els problemes resolubles de forma eficient i aquells que són computacionalment complexos. Començarem descrivint breument els problemes que són resolubles de forma eficient per encarregar-nos després d'estudiar amb més detall els problemes computacionalment complexos, que són font de propostes criptogràfiques postquàntiques.

2.8.1 Problemes resolubles eficientment

1. El problema de la base: a partir d'un conjunt de vectors B, determinar un subconjunt que generi una base B' per a Λ. Aquest és un problema que es pot resoldre, en temps polinòmic, calculant $\mathrm{HNF}(B)$.
2. El problema de les bases equivalents: donades dues bases reticulars B i B', determinar si són equivalents. Aquest problema es pot resoldre, en temps polinòmic, calculant $H = \mathrm{HNF}(B)$, $H' = \mathrm{HNF}(B')$ i comprovant si $H = H'$.
3. El problema de la unió: donades dues bases reticulars B i B', determinar una base per al reticle més petit que contingui tant $\Lambda(B)$ com $\Lambda(B')$. El reticle mínim és generat per $B'' := B \cup B'$, de manera que podem determinar una base si calculem $\mathrm{HNF}(B'')$.
4. El problema de la subbase: donades dues bases reticulars B i B', determinar si $\Lambda(B') \subseteq \Lambda(B)$. Aquest problema es pot reduir als problemes de la unió i de les bases equivalents; en efecte: $\Lambda(B') \subseteq \Lambda(B)$ si, i només si, $\Lambda(B \cup B') = \Lambda(B)$. Si volem comprovar la inclusió, només cal calcular $\mathrm{HNF}(B \cup B')$, $\mathrm{HNF}(B)$ i comprovar si les formes coincideixen.
5. Pertinença a un reticle: donat $v \in \mathbb{Z}^n$, determinar si $v \in \Lambda(B)$. Aquest problema pot reduir-se al problema de la subbase tot comprovant si $\Lambda(v) \subseteq \Lambda(B)$. El problema es pot resoldre per a un conjunt de vectors $\{v_1, \ldots, v_k\}$ tot calculant $\mathrm{HNF}(B)$, calculant després, per a cada $i \in \{1, 2, \ldots, k\}$, $\mathrm{HNF}(B \cup v_i)$, i comprovant si $\mathrm{HNF}(B) = \mathrm{HNF}(B \cup v_i)$.
6. El problema del nucli: donada una base $A \in M_{n\times m}(\mathbb{Z})$, determinar una base que generi $\Lambda(A)$ a partir de $\ker(A)$. Aquest problema es redueix al problema de la base un cop determinat un conjunt generador de $\ker(A)$. Observem que el mateix procediment resol el problema següent.
7. El problema del nucli modular: donats una matriu $A \in M_{n\times m}(\mathbb{Z})$ i $q \in \mathbb{Z}$, determinar una base que generi el reticle $\Lambda_q^{\perp}(A)$.

2.8.2 Problemes computacionalment complexos Entre els problemes que són computacionalment complexos destaquen:

1. Vector més curt: en el problema del vector més curt (escriurem SVP) es vol determinar, per a una base B i un reticle $\Lambda(B)$, el vector no trivial més curt de Λ. Aquest problema té dues versions:

   - La versió exacta, en què es pretén resoldre alguna de les preguntes següents:
     — Decisió: per a $0 < d \in \mathbb{R}$, decidir si $\lambda_1(\Lambda(B)) \leq d$ o bé si $\lambda_1(\Lambda(B)) > d$.
     — Càlcul: determinar $\lambda_1(\Lambda(B))$.
     — Cerca: trobar $v \in \Lambda(B) - \{0\}$ tal que $\|v\| = \lambda_1(\Lambda(B))$.

- La versió aproximada (escriurem SVP_γ), en la qual tenim una funció real $\gamma = \gamma(\dim(\Lambda)) \geq 1$, en què es pretén resoldre alguna de les preguntes següents:
  - Decisió: per a $0 < d \in \mathbb{R}$, decidir si $\lambda_1(\Lambda(B)) \leq d$ o bé si $\lambda_1(\Lambda(B)) > \gamma \cdot d$.
  - Estimació: trobar $d \in [\lambda_1(\Lambda(B)), \gamma \cdot \lambda_1(\Lambda(B))]$.
  - Cerca: trobar $v \in \Lambda(B) - \{0\}$ tal que $\|v\| = \gamma \cdot \lambda_1(\Lambda(B))$.

2. Vector més proper: en el problema del vector més proper (escriurem CVP) volem trobar, per a una base B, un reticle $\Lambda(B)$ i un vector $w \in \mathbb{R}^n$, el vector $v \in \Lambda(B)$ més proper a w. Com en el cas anterior, aquest problema admet dues versions:
   - La versió exacta, en la qual es pretén resoldre alguna de les preguntes següents:
     - Decisió: donat un nombre real $r \in \mathbb{R}$, decidir si $\mathrm{dist}(w, \Lambda(B)) \leq r$ o bé si $\mathrm{dist}(w, \Lambda(B)) > r$, on $\mathrm{dist}(w, \Lambda(B)) = \min_{v \in \Lambda(B)} \|w - v\|$.
     - Càlcul: trobar $r \in \mathbb{R}$ tal que $r = \mathrm{dist}(w, \Lambda(B))$.
     - Cerca: trobar $v \in \Lambda(B)$ tal que $\mathrm{dist}(w, v) \leq \mathrm{dist}(w, \Lambda(B))$.
   - La versió aproximada (escriurem CVP_γ), en la qual tenim una funció real $\gamma = \gamma(\dim(\Lambda)) \geq 1$, en què es pretén resoldre alguna de les preguntes següents:
     - Decisió: donat un nombre real $r \in \mathbb{R}$, decidir si $\mathrm{dist}(w, \Lambda(B)) \leq r$ o bé si $\mathrm{dist}(w, \Lambda(B)) > \gamma \cdot r$.
     - Càlcul: trobar $r \in \mathbb{R}$ tal que $r \in [\mathrm{dist}(w, \Lambda(B)), \gamma \cdot \mathrm{dist}(w, \Lambda(B))]$.
     - Cerca: trobar $v \in \Lambda(B)$ tal que $\mathrm{dist}(w, v) \leq \gamma \cdot \mathrm{dist}(w, \Lambda(B))$.

3. Enters petits: en el problema de la solució mitjançant enters petits (escriurem SIS) considerem un enter $q \in \mathbb{Z}$, una matriu $A \in M_{n \times m}(\mathbb{Z}_q)$ i $\beta \in \mathbb{R}$ amb l'objectiu de trobar un vector $z \in \mathbb{Z}^m - \{0\}$ tal que $Az \equiv 0 \bmod q$ amb $\|z\| \leq \beta$.

El lema següent garanteix, sota certes condicions, l'existència de solucions per al problema SIS.

LEMA 22 ([12, lema 5.2]). *Per a tot $q \in \mathbb{Z}$, $A \in M_{n \times m}(\mathbb{Z}_q)$ i $\beta \geq \sqrt{m}\, \sqrt[m]{q^n}$ existeix $z \in \mathbb{Z}^m - \{0\}$ tal que $\|z\| \leq \beta$ i $Az \equiv 0 \bmod q$.*

El problema SIS admet una variant anomenada *no homogènia* (escriurem ISIS) en la qual, donats $q \in \mathbb{Q}$, una matriu $A \in M_{n \times m}(\mathbb{Z}_q)$, $\beta \in \mathbb{R}$ i $u \in \mathbb{Z}_q^n$ es vol trobar $z \in \mathbb{Z}_q^m$ tal que $Az \equiv u \bmod q$ i $\|z\| \leq \beta$.

2.8.3 Relació entre SVP i CVP El problema CVP pot interpretar-se com una versió no homogènia del problema SVP ja que, mentre que en el problema SVP busquem un punt del reticle proper a l'origen, en el problema CVP busquem un punt del reticle proper a un punt arbitrari.

La diferència principal entre SVP i CVP la trobem en el fet que, mentre que la solució del SVP no pot ser el vector nul, el CVP sí que l'admet. Aquest fet fa que puguem fer servir el problema CVP per trobar el vector més proper al vector 0 per tal de resoldre el problema SVP.

El problema SVP pot reduir-se al problema CVP. Aquest procés es fonamenta en els resultats següents. Considerem un reticle $\Lambda(B)$, de rang màxim, generat per una base $B = \{b_1, \dots, b_n\}$:

LEMA 23 ([9, proposició 3]). *Considerem* $0 \neq v = \sum_{i=1}^{n} c_i b_i$ *un vector més curt d'un reticle* $\Lambda(B)$. *Existeix un índex* $i \in \{1, \dots, n\}$ *tal que* c_i *és senar.*

Considerem un índex $j \in \{1, \dots, n\}$ i definim les bases per a $\Lambda(B)$ següents: $B^{(j)} := \{b_1, \dots, b_{j-1}, 2b_j, b_{j+1}, \dots, b_n\}$. Aleshores tenim:

PROPOSICIÓ 24 ([9, proposició 4]). *Considerem* $v = \sum_{i=1}^{n} c_i b_i$ *un vector de* $\Lambda(B)$ *per al qual existeix* $j \in \{1, \dots, n\}$ *tal que* c_j *és senar. Aleshores el vector* $u := \frac{c_j+1}{2} 2b_j + \sum_{i \neq j} c_i b_i = 2c'_j b_j + \sum_{i \neq j} c_i b_i$ *és un vector de* $\Lambda(B^{(j)})$ *tal que* $\operatorname{dist}(u, b_j) = \|v\|$.

PROPOSICIÓ 25 ([9, proposició 5]). *Considerem* $u = 2c'_j b_j + \sum_{i \neq j} c_i b_i$ *un vector de* $\Lambda(B^{(j)})$. *Aleshores* $v = (2c'_j - 1)b_j + \sum_{i \neq j} c_i b_i$ *és un vector no nul de* $\Lambda(B)$ *tal que* $\operatorname{dist}(u, b_j) = \|v\|$.

Observem que el lema 23, juntament amb la proposició 24, ens permet deduir l'existència, per a cada $j \in \{1, \dots, n\}$, d'un vector de $\Lambda(B^{(j)})$ tal que la distància amb el vector objectiu b_j coincideix amb la norma d'un vector més curt de $\Lambda(B)$. Finalment, fent servir la proposició 25, es pot determinar un vector de $\Lambda(B)$ tal que la distància amb el vector objectiu coincideix amb la norma d'un vector més curt de $\Lambda(B)$. Formalment, tenim:

TEOREMA 26 ([9, teorema 6]). *Donat* $\gamma = \gamma(n) \in \mathbb{R}$, *el problema* SVP_γ *pot reduir-se al problema* CVP_γ.

2.9 L'algorisme Lenstra-Lenstra-Lóvasz

Considerem $B = \{b_1, \dots, b_m\} \subset \mathbb{R}^n$ una base i $B^\star = \{b_1^\star, \dots, b_m^\star\}$ la seva base associada obtinguda amb el procediment de Gram-Schmidt. Direm que B és δ-LLL reduïda, per a $\frac{1}{4} < \delta < 1$, si satisfà les condicions següents:

1. Condició de mida: $\forall 1 \leq i \leq n$ i $j < i$: $|\mu_{i,j}| \leq \frac{1}{2}$, on $\mu_{i,j}$ són els coeficients involucrats en el procediment de Gram-Schmidt.
2. Condició de Lóvasz: $\forall 1 \leq i < n : \delta \|b_i^\star\|^2 \leq \|\mu_{i+1,i} b_i^\star + b_{i+1}^\star\|^2$.

L'algorisme Lenstra-Lenstra-Lóvasz (LLL) és un algorisme de reducció que retorna, donada una base, una base constituïda per vectors curts que satisfan la condició de Lóvasz. Pot entendre's com una versió vectorial de l'algorisme d'Euclides per al càlcul del màxim comú divisor. El funcionament essencial de

l'algorisme LLL es fonamenta en el procediment de Gram-Schmidt (vegeu la secció 6.12 de [10]).

TEOREMA 27 ([10, teorema 6.68]). *Sigui $\{v_1, \dots, v_n\}$ una base per a un reticle Λ. L'algorisme LLL ([10, figura 6.7]) acaba en un nombre finit de passos i retorna una base δ-LLL reduïda per a Λ. En particular, l'algorisme LLL és un algorisme polinòmic.*

Tot i que l'aplicació original de l'algorisme era la factorització de polinomis sobre $\mathbb{Q}$, les aplicacions més destacables de l'algorisme LLL també inclouen la criptoanàlisi dels sistemes criptogràfics basats en reticles ja que l'algorisme LLL resol la versió exacta del problema SVP en temps $2^{O(n^2)}$ [1] i també té un paper important en la resolució de la versió aproximada del problema CVP en temps d'ordre $2^{O(n)}$ (vegeu [10, teorema 6.73] per a una referència).

3 Codis

3.1 Conceptes bàsics

Un *missatge* és una seqüència finita d'elements d'un cos finit $\mathbb{F}_q$ d'ordre q, per a $q = p^r$ on p és un nombre primer i $r \in \mathbb{N}$. Un *codi C de longitud n* és un conjunt $C \subset \mathbb{F}_q^n$. Si C només té un element, direm que C és un codi trivial. Si prenem $q = 2$ parlarem de codis binaris. Els elements $c \in C$ s'anomenen *paraules codi*.

El procés de codificació d'un missatge es pot interpretar com una aplicació injectiva, que anomenem *codificador*, $f\colon \mathbb{F}_q^k \to \mathbb{F}_q^n$, per a $n > k > 0$. Un codi de longitud n és la imatge $f(\mathbb{F}_q^k) := C \subset \mathbb{F}_q^n$. Un codificador té associada una funció injectiva $g\colon \mathbb{F}_q^n \to \mathbb{F}_q^k$ tal que $g \circ f = \mathrm{Id}$,[1] que anomenarem *descodificador*.

EXEMPLE. Per tal de motivar els propers conceptes ens centraren en una situació en què volem codificar un missatge $a \in \mathbb{F}_q^k$ mitjançant un codificador $f\colon \mathbb{F}_q^k \to \mathbb{F}_q^n$. El resultat és un element $f(a) \in C$, que és enviat a través d'un canal. El codi arriba al descodificador associat g, que retorna un missatge amb la forma $g(b) \in \mathbb{F}_q^k$. Siguin $q = 2$, $k = 1$, $n = 3$ i $C = (0,0,0), (1,1,1) \in \mathbb{F}_2^3$. Suposem que el missatge «No» es correspon amb 0 i que es codifica com $f(0) = (0,0,0)$. Suposem que un missatge «Sí» es correspon amb 1 i que es codifica com $f(1) = (1,1,1)$. Enviem un «No» a través d'un canal que genera interferències tals que el descodificador rep el codi $(0,1,0)$. És raonable pensar que el descodificador retorni el missatge «No» ja que l'element $(0,1,0) \in F_2^3$ és més semblant a $(0,0,0)$ que no pas a $(1,1,1)$ ja que $(0,1,0)$ i $(0,0,0)$ només difereixen en una component, mentre que $(0,1,0)$ i $(1,1,1)$ difereixen en dues. En aquest cas direm que el codi ha corregit un error.

1 Observem que la composició és la identitat amb una certa probabilitat que depèn de la longitud de la *paraula codi* ([24, secció 2.1]).

Considerem $x \in \{x_1, \ldots, x_n\} \in \mathbb{F}_q^n$. El *pes* $w(x)$ és el nombre de components no nul·les de x. En l'exemple anterior $w(f(0)) = 0$, $w(f(1)) = (1,1,1) = 3$, $w((0,1,0)) = 1$.

Donats dos elements $x, y \in \mathbb{F}_q^n$, la *distància de Hamming* és

$$d(x,y) = \#\{1 \leq i \leq n \mid x_i \neq y_i\} = w(x-y).$$

EXEMPLE. Per a $x = (1,1,1)$ i $y = (0,1,0)$ tenim $d(x,y) = w(1,0,1) = 2$.

Si C és un codi no trivial, la distància mínima de C és $\min_{x \neq y \in C} d(x,y)$; el pes mínim és $\min_{x \in C - \{0\}} w(x)$.

Un (n,m,d)-codi és un codi amb longitud n, m *paraules codi* i distància mínima d. El codi C de l'exemple és un $(3,2,3)$-codi.

El radi de cobriment d'un codi C és $\rho(C) = \max_{x \in \mathbb{F}_q^n} \min_{c \in C} d(x,c)$. Observem que el concepte formalitza la idea de com d'allunyat està un element rebut $x \in \mathbb{F}_q^n$ de la *paraula codi* més propera.

Donat un codi $C \subset \mathbb{F}_q^n$ de longitud n, el *codi estès* associat és

$$\overline{C} := \left\{ (c_1, \ldots, c_{n+1}) \mid (c_1, \ldots, c_n) \in C,\ c_{n+1} = \sum_{i=1}^{n} c_i \right\}.$$

Un *codi lineal* és un subespai vectorial de $\mathbb{F}_q^n$. Una forma alternativa de definir-lo és mitjançant successions exactes, la qual cosa ens conduirà a alguns conceptes fonamentals. En efecte, considerem la successió exacta curta:

$$0 \longrightarrow \mathbb{F}_q^k \xrightarrow{A} \mathbb{F}_q^n \xrightarrow{B} \mathbb{F}_q^{n-k} \longrightarrow 0.$$

Per ser exacta, tenim $rk(A) = k$, $rk(B) = n - k$ i $B \circ A = 0$. D'una altra banda:

1. Definim $C := A(\mathbb{F}_q^k) \subset \mathbb{F}_q^n$. L'aplicació lineal A es descriu amb una matriu de mida $n \times k$. Les seves columnes formen una base de C. La matriu A^T s'anomena *matriu generatriu*.
2. Per ser una successió exacta, $C = \ker(B)$, per tant, $x \in C \Leftrightarrow Bx = 0$. L'aplicació B es defineix amb una matriu de mida $(n-k) \times n$, les files de la qual són les relacions que defineixen C. La matriu B rep el nom de *matriu de paritat* o *de control*. Donat un element $x \in \mathbb{F}_q^n$, la *síndrome* de x és $Bx \in \mathbb{F}_q^{n-k}$.

Com que els espais són tots de dimensió finita, la successió anterior indueix una successió curta dual

$$0 \longrightarrow \mathbb{F}_q^{n-k} \xrightarrow{B^T} \mathbb{F}_q^n \xrightarrow{A^T} \mathbb{F}_q^k \longrightarrow 0.$$

Aquesta successió, de forma anàloga, ens permet definir un codi $\widehat{C} := B^T(\mathbb{F}_q^{n-k})$ anomenat *codi dual* o *codi ortogonal de* C. Si $\dim(C) = k \Rightarrow \dim(\widehat{C}) = n - k$.

Si definim, donats $x, y \in \mathbb{F}_q^n$, $x \cdot y := \sum_i x_i y_i$, obtenim la següent caracterització de $\widehat{C}$:

LEMA 28 ([7, lema 1.1]). *Es compleix* $\widehat{C} = \{y \in \mathbb{F}_q^n \mid x \cdot y = 0,\ \forall x \in C\}$.

Un codi binari C és *parell* si el pes $w(x)$ és divisible entre 2 per a tot $x \in C$; s'anomena *doblement parell* si el pes $w(x)$ és divisible entre 4.

El grup simètric Σ_n actua sobre $\mathbb{F}_q^n$ mitjançant permutacions de coordenades. Dos codis C, C' sobre $\mathbb{F}_q^n$ són *equivalents* si $\exists \sigma \in \Sigma_n$ tal que $\sigma(C) = C'$.

3.2 Codis cíclics

La importància dels codis cíclics en criptografia postquàntica rau en el fet que les seves propietats els fan particularment útils a l'hora de dur a terme implementacions i calcular síndromes.

Un codi lineal C de longitud n s'anomena *cíclic* si per a qualsevol *paraula codi* $c = (c_0, \ldots, c_{n-1}) \in C$, $c' = (c_{n-1}, c_0, \ldots, c_{n-2}) \in C$. Podem identificar les *paraules codi* d'un codi cíclic amb cinc classes de polinomis de $\mathbb{F}_q^n[x]/(x^n - 1)$ mitjançant el següent isomorfisme:

$$\mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n[x]/(x^n - 1), \quad (c_0, \ldots, c_{n-1}) \longmapsto c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}.$$

El resultat següent aporta una definició alternativa per al concepte de codi cíclic i en motiva el nom:

TEOREMA 29 ([24, teorema 6.1.3]). *Un codi lineal C de longitud n és cíclic si, i només si, és un ideal de $\mathbb{F}_q^n[x]/(x^n - 1)$.*

Si C és un codi cíclic, aleshores tenim que, com que és un ideal de $\mathbb{F}_q^n[x]/(x^n - 1)$: $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in C \Rightarrow x \cdot c(x) \in C$, ara bé:

$$x \cdot c(x) = c_{n-1} + c_0 x + \cdots + c_{n-2} x^{n-2}.$$

Per ser un ideal principal, existeix un polinomi mònic $g \in \mathbb{F}_q^n[x]/(x^n - 1)$ amb grau mínim que genera l'ideal. Aquest polinomi rep el nom de *polinomi generador*.

La descomposició en factors irreductibles de $x^n - 1 = f_1(x) \cdots f_t(x)$ ens porta al concepte de *codi cíclic maximal*, que és un codi generat per $f_i(x)$ i que denotarem per M_i^+, per a $i = 1, \ldots, t$. Els codis generats per $\frac{x^n-1}{f_i(x)}$ reben el nom de *codis cíclics minimals* i els denotarem per M_i^-.

TEOREMA 30 ([24, teorema 6.4.1]). *Per a tot codi cíclic C existeix un element $c \in C$ únic, anomenat* idempotent*, que és el neutre del producte de C.*

TEOREMA 31 ([24, teorema 6.4.3]). *Si C_1, C_2 són codis cíclics amb idempotents c_1 i c_2 respectius, aleshores:*

(1) El codi $C_1 \cap C_2$ té idempotent $c_1 \cdot c_2$.

(2) El codi $C_1 + C_2$ té idempotent $c_1 + c_2 - c_1 \cdot c_2$.

L'idempotent d'un codi minimal M_i^- s'anomena *idempotent primitiu* i el denotem per $\theta_i(x)$. El lema següent en dona una caracterització:

LEMA 32 ([24, teorema 6.4.4]). *Amb les notacions anteriors, els idempotents primitius satisfan:*

(1) Si $i \neq j$, aleshores $\theta_i(x)\theta_j(x) = 0$.

(2) $\sum_{i=1}^{t} \theta_i(x) = 1$.

(3) L'idempotent generador del codi $f_{i_1}(x) \cdots f_{i_r}(x)$ és $1 + \theta_{i_1}(x) + \cdots + \theta_{i_r}(x)$.

3.3 Codis de Goppa i la seva descodificació

Sigui $L = \{\gamma_0, \gamma_1, \ldots, \gamma_{n-1}\} \subset \mathbb{F}_q$ tal que $g(\gamma_i) \neq 0$ per a $0 \leq i \leq n-1$, essent $g(x)$ un polinomi mònic de grau t sobre $\mathbb{F}_q$. Un *codi de Goppa* $\Gamma(L, g)$, amb *polinomi de Goppa* associat $g(x) = \sum_{i=0}^{t} g_i x^i$, és el conjunt $(c_0, \ldots, c_{n-1}) \in \mathbb{F}_p^n$ tals que $\sum_{i=0}^{n-1} \frac{c_i}{x-\gamma_i} \equiv 0 \bmod g(x)$. Si fem $h_j := (g(\gamma_j))^{-1}$, una matriu de paritat per a $\Gamma(L, g)$ és (vegeu [24]):

$$B = \begin{pmatrix} h_0 & h_1 & \ldots & h_{n-1} \\ h_0\gamma_0 & h_1\gamma_1 & \ldots & h_{n-1}\gamma_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ h_0\gamma_0^{t-1} & h_1\gamma_1^{t-1} & \ldots & h_{n-1}\gamma_{n-1}^{t-1} \end{pmatrix}.$$

TEOREMA 33 ([24, teorema 9.2.7]). *Amb les notacions anteriors, un codi de Goppa $\Gamma(L, g)$ té distància mínima més gran o igual que $t+1$ i dimensió més gran o igual que $n - mt$.*

Considerem un codi de Goppa $\Gamma(L, g)$, una *paraula codi* $c=(c_0, c_1, \ldots, c_{n-1}) \in \Gamma(L, g)$ i un missatge $r = (r_0, r_1, \ldots, r_{n-1}) \in \mathbb{F}_p^n$. Sigui $e = r - c = (e_0, e_1, \ldots, e_{n-1})$. Considerem $M := \{0 \leq i \leq n-1 \mid e_i \neq 0\}$. Suposem que $\deg(g(x)) = t$ i que $\#M = e \leq t/2$. Considerem un polinomi $S(x)$ tal que

$$\begin{cases} S(x) \equiv \sum_{i=0}^{n-1} \frac{e_i}{x-\gamma_i} \bmod q, \\ \deg(S(x)) < t. \end{cases}$$

Definim el polinomi *localitzador d'errors* com $\sigma(x) := \prod_{i \in M} x - \gamma_i$. Definim el *polinomi avaluador* d'errors com $\omega(x) := \sum_{i \in M} e_i \prod_{j \in M - \{i\}} (x - \gamma_j)$.

Considerem el producte $S\sigma$:

$$S(x)\sigma(x) = \sum_{i=0}^{n-1} \frac{e_i}{x-\gamma_i} \prod_{i \in M} x - \gamma_i \equiv \sum_{i=0}^{n-1} e_i \prod_{j \in M-\{i\}} x - \gamma_i \equiv \omega(x) \bmod g(x).$$

Si assumim que tenim un algorisme capaç de calcular un polinomi mònic no nul $\sigma_1(x)$ i un polinomi $\omega_1(x)$ tals que $S(x)\sigma_1(x) \equiv \omega_1(x) \bmod g(x)$,

on $\sigma_1(x)$ té el grau més baix entre tots els polinomis mònics no nuls que satisfan la congruència, i $\deg(\omega_1(x)) < \deg(\sigma_1(x))$, aleshores pot deduir-se

$$\omega_1(x)\sigma(x) - \omega(x)\sigma_1(x) \equiv 0 \bmod g(x).$$

Observem que aquest polinomi té grau menor que el grau de $g(x)$, de manera que $\omega_1(x)\sigma(x) - \omega(x)\sigma_1(x) = 0$. Com que els polinomis σ, ω no tenen factors comuns, la igualtat implica $\sigma|\sigma_1$, d'on es dedueix $\sigma = \sigma_1$. Una vegada es coneixen σ i ω podem recuperar el vector e i descodificar la *paraula codi* c.

3.4 Relació entre codis i reticles

Considerem un reticle $\mathbb{Z}^n \subset \mathbb{R}^n$ i l'aplicació

$$\pi\colon \mathbb{Z}^n \longrightarrow \mathbb{F}_2^n, \quad (x_1, \dots, x_n) \longmapsto (\overline{x}_1, \dots, \overline{x}_n).$$

Considerem C un (n,k,d)-codi lineal de $\mathbb{F}_2^n$. Com que $\mathbb{F}_2^n/C \cong \mathbb{F}_2^{n-k}$, podem deduir que C és un subgrup de $\mathbb{F}_2^n$ amb cardinalitat 2^k. Per tant,

$$\pi^{-1}(C) = \{x + 2k \mid x \in C,\, k \in \mathbb{Z}\}$$

és un subgrup de $\mathbb{Z}^n$ d'índex 2^{n-k}. Tenim que $\pi^{-1}(C)$ és un reticle de $\mathbb{R}^n$ pel fet de ser un conjunt discret tancat per a la suma i la resta.

El reticle associat al codi C es defineix com $\Lambda_C = \frac{1}{\sqrt{2}}\pi^{-1}(C)$. Dos elements qualssevol de Λ_C tenen la forma

$$\begin{cases} x = \frac{1}{\sqrt{2}}(c + 2z), \\ y = \frac{1}{\sqrt{2}}(c' + 2z') \end{cases}$$

per a $c, c' \in \{0,1\}^n$ i $z, z' \in \mathbb{Z}^n$. Cometem un abús de notació tot identificant $\mathbb{F}_2^n \leftrightarrow \{0,1\}^n$ i escrivint $c, c' \in C$. Tenim

$$\begin{cases} x^2 = \frac{1}{2}(c^2 + 4cz + 4z^2), \\ x \cdot y = \frac{1}{2}(c \cdot c'). \end{cases}$$

És immediat deduir que per a tot $x, y \in \Lambda_C$ es compleix:

$$x \cdot y \in \mathbb{Z} \iff c \cdot c' \in 2\mathbb{Z}, \quad \forall c, c' \in C.$$

Per tant, Λ_C és un reticle integral (*i. e.* en el qual per a tot $x, y \in \Lambda_C$ es compleix $x \cdot y \in \mathbb{Z}$) si, i només si, $C \subset \widehat{C}$. A més a més, $x^2 \in 2\mathbb{Z} \Leftrightarrow c^2 \in 4\mathbb{Z}$ per a tot $c \in C$, de manera que Λ_C és parell si, i només si, C és doblement parell. Finalment, si $k = n/2$, aleshores $\operatorname{vol}(\mathbb{R}^n/\pi^{-1}(C)) = 2^{\frac{n}{2}} \Leftrightarrow \operatorname{vol}(\mathbb{R}^n/\Lambda_C) = 1$, de manera que C és autodual (*i. e.* $C = \widehat{C}$) si, i només si, Λ_C és autodual. Tot plegat prova el resultat següent:

PROPOSICIÓ 34 ([7, proposició 1.3]). *Per a un codi lineal C tenim:*

(1) $C \subset \widehat{C} \Leftrightarrow \Lambda_C$ *és un reticle integral.*
(2) C *és doblement parell si, i només si,* Λ_C *és parell.*
(3) C *és autodual si, i només si,* Λ_C *és autodual.*

3.5 Apunt final sobre problemes computacionalment complexos

A diferència del que passa amb la teoria de reticles i, com veurem tot seguit, amb la teoria d'isogènies de corbes el·líptiques supersingulars, la teoria de codis no té una llista de problemes computacionalment complexos. La seguretat dels algorismes que recolzen sobre la teoria de codis la fonamentem en el fet que tant el problema de la descodificació de codis lineals com el problema del càlcul de pesos de codis lineals són tots dos problemes NP-complets [2]. Cal destacar que, fins ara, no s'han presentat algorismes capaços de resoldre els problemes en un temps inferior a l'exponencial; no es coneixen encara algorismes quàntics que puguin fer-ho.

4 Isogènies de corbes el·líptiques supersingulars

Sigui $\mathbb{K}$ un cos, una *corba el·líptica* és un parell (E, O_E), on E és una corba a $\mathbb{P}^2_{\mathbb{K}}$ no singular de gènere 1 i $O_E \in E$ és un punt distingit. Si $\mathbb{K}$ és tal que $\mathrm{char}(\mathbb{K}) \neq 2, 3$, una corba el·líptica pot ser descrita[2] mitjançant l'equació de Wierstrass

$$E := \{(x : y : z) \in \mathbb{P}^2_{\mathbb{K}} \mid y^2 z = x^3 + axz + bz^3\},$$

on $a, b \in \mathbb{K}$ i $4a^3 + 27b^2 \neq 0$. Aquesta darrera condició és necessària per tal d'evitar singularitats. En aquest cas, $O_E = (0 : 1 : 0)$.

Si fem el canvi de variables $\frac{x}{z} \mapsto x$, $\frac{y}{z} \mapsto y$ obtenim la *forma afí*

$$E = \{(x, y) \in \mathbb{A}^2_{\mathbb{K}} \mid y^2 = x^3 + ax + n\}.$$

Per a una corba el·líptica E, descrita per una equació de Weierstrass, es defineix el j-invariant com

$$j(E) = j(a, b) = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

PROPOSICIÓ 35 ([22, proposició 1.4]). *Dues corbes el·líptiques E_1, E_2 són isomorfes en la clausura algebraica $\overline{\mathbb{K}}$ si, i només si, $j(E_1) = j(E_2)$.*

EXEMPLE. Donat un $j_0 \in \overline{\mathbb{K}} - \{0, 1728\}$, la corba el·líptica

$$E : y^2 = x^3 + \frac{3j_0}{1728 - j_0} x + \frac{2j_0}{1728 - j_0}$$

satisfà $j(E) = j_0$.

2 Existeixen altres formes de descriure una corba el·líptica, com l'equació de Huff o la d'Edwards; vegeu [14] per a una referència.

Per tal de definir el concepte de morfisme entre corbes el·líptiques ens cal introduir alguns conceptes bàsics de caire tècnic.

Sigui C una corba projectiva plana donada per $f(x,y,z) = 0$ amb $f \in \mathbb{K}[x,y,z]$ irreductible sobre la clausura algebraica. El *cos de funcions* $\mathbb{K}(C)$ és el conjunt de funcions racionals $\frac{g}{h}$ tal que

- Els polinomis g, h són homogenis a $\mathbb{K}[x,y,z]$ i tenen el mateix grau.
- $f \nmid h$.
- $\frac{g_1}{h_1} \equiv \frac{g_2}{h_2} \Leftrightarrow f \mid (g_1h_2 - g_2h_1)$.

Donada una corba projectiva plana C, direm que una funció racional $f = \frac{g}{h}$, amb $g,h \in \mathbb{K}[x,y,z]$, és definida, o que és *regular*, en un punt $P \in C(\overline{K})$ si $h(P) \neq 0$.

Si C_1, C_2 són corbes projectives planes definides sobre $\mathbb{K}$, una aplicació *racional* $\phi\colon C_1 \to C_2$ és una terna $\phi = (\phi_x : \phi_y : \phi_z) \in \mathbb{P}^2_{\mathbb{K}(C_1)}$ tal que per a tot punt $P \in C_1(\overline{\mathbb{K}})$ on ϕ és regular tenim $\phi(P) \in C_2(\overline{\mathbb{K}})$.

Considerem un parell de corbes projectives planes C_1, C_2. Una aplicació racional $\phi\colon C_1 \to C_2$ regular en tot $P \in C_1(\overline{\mathbb{K}})$ s'anomena *morfisme entre* C_1 *i* C_2.

4.1 Conceptes fonamentals sobre isogènies

Donades dues corbes el·líptiques (E_1, O_1), (E_2, O_2), una *isogènia* entre elles és un morfisme $\phi\colon E_1 \to E_2$ tal que $\phi(O_1) = O_2$. Dues corbes el·líptiques són *isògeniques* si existeix una isogènia entre elles.

LEMA 36 ([23, lema 5.21]). *Siguin E_1, E_2 corbes el·líptiques sobre $\mathbb{K}$. Una isogènia $\phi\colon E_1 \to E_2$ admet la representació*

$$\phi(x,y) = \left(\frac{p(x)}{q(x)}, \frac{s(x)}{t(x)}y\right),$$

on $p,q,s,t \in \mathbb{K}[x]$ són polinomis tals que p, q i s, t són primers entre ells dos a dos.

LEMA 37 ([8, lema 9.6.3]). *Si $\phi\colon E_1 \to E_2$ és una isogènia no nul·la entre E_1 i E_2, corbes el·líptiques sobre $\mathbb{K}$, aleshores $\phi\colon E_1(\overline{\mathbb{K}}) \to E_2(\overline{\mathbb{K}})$ és una aplicació exhaustiva.*

El *grau* d'una isogènia $\phi\colon E_1 \to E_2$ és $\deg(\phi) := \max\{p(x), q(x)\}$. Si la isogènia és tal que $\frac{d}{dx}\frac{p(x)}{q(x)} \neq 0$ direm que ϕ és *separable*. Altrament direm que ϕ és *inseparable*.

EXEMPLE. Considerem un cos finit $\mathbb{F}_q$ d'ordre q. Donada una corba el·líptica E sobre $\mathbb{F}_q$, l'aplicació de Frobenius $\pi_E\colon E \to E$, $(x,y) \mapsto (x^q, y^q)$ és una isogènia de grau q.

Mantenint les notacions de l'exemple, la traça de l'aplicació de Frobenius es defineix com $\tau_E = q+1-\#E(\mathbb{F}_q)$. El polinomi característic de Frobenius associat a E és el polinomi $p_E(x) = x^2 - \tau_E x + q$.

El resultat següent aporta un criteri de molta utilitat a l'hora de determinar si dues corbes el·líptiques són isogèniques:

TEOREMA 38 (TEOREMA DE LA ISOGÈNIA DE TATE). *Amb les notacions anteriors, dues corbes el·líptiques E_1 i E_2 són isogèniques si, i només si, tenen el mateix polinomi característic de Frobenius. En particular, E_1 i E_2 són isogèniques si, i només si, $\#E_1(\overline{\mathbb{F}}_q) = \#E_2(\overline{\mathbb{F}}_q)$.*

El *nucli* d'una isogènia $\phi\colon (E_1, O_1) \to (E_2, O_2)$ és el conjunt

$$\ker(\phi) := \{P \in E_1(\overline{\mathbb{K}}) \mid \phi(P) = O_2\}.$$

La relació entre el nucli d'una isogènia i el seu grau és forta, com podem comprovar en el resultat següent:

PROPOSICIÓ 39 ([27, proposició 12.8]). *Si $\phi\colon E_1 \to E_2$ és una isogènia separable, aleshores* $\deg(\phi) = \#\ker(\phi)$. *Si és inseparable, aleshores* $\deg(\phi) > \#\ker(\phi)$.

PROPOSICIÓ 40 ([22, corol·lari 4.8]). *Si $\phi\colon E_1 \to E_2$ és una isogènia no nul·la entre corbes el·líptiques (E_1, O_1), $(E_2, 0_2)$, aleshores* $\ker(\phi) = \phi^{-1}(O_2)$ *és un subgrup finit de $E_1(\overline{\mathbb{K}})$.*

EXEMPLE. Considerem (E, O_E) una corba el·líptica i $n \in \mathbb{Z}$, aleshores l'aplicació $[n]\colon E \to E$, $P \mapsto [n]P = \underbrace{P + \cdots + P}_{n \text{ vegades}}$ és una isogènia.

EXEMPLE. El *problema del logaritme discret sobre corbes el·líptiques* requereix trobar $n \in \mathbb{Z}$ tal que $Q = [n](P)$, donats dos punts P, Q en una corba el·líptica E. Aquest problema es pot reformular com el problema de trobar, donats P i Q de $E(\overline{\mathbb{K}})$, la isogènia $\phi\colon E \to E$ tal que $\phi(P) = Q$. L'algorisme de Shor resol el problema del logaritme discret amb un algorisme polinòmic en un ordinador quàntic.

El problema de la determinació d'isogènies entre corbes el·líptiques, del qual el logaritme discret és un exemple bàsic, té algorismes quàntics capaços de resoldre'l en temps subexponencials en el cas de corbes el·líptiques ordinàries [5]. En el cas de considerar corbes el·líptiques supersingulars, només existeix un algorisme quàntic capaç de resoldre el problema en temps exponencial [3].

Denotarem el conjunt d'isogènies entre dues corbes el·líptiques E_1, E_2 per $\mathrm{Hom}(E_1, E_2) = \{\phi\colon E_1 \to E_2 \mid \phi \text{ és una isogènia}\}$. Per a $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$ i $P \in E_1(\overline{\mathbb{K}})$ definim $(\phi + \psi)(P) := \phi(P) + \psi(P)$. La suma d'isogènies dona a $\mathrm{Hom}(E_1, E_2)$ estructura de grup.

Si a més definim el producte d'isogènies $\phi \cdot \psi$ com la composició $\phi \circ \psi$, podem dotar el conjunt $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ d'endomorfismes amb estructura d'anell. Els elements amb invers multiplicatiu de $\mathrm{End}(E)$ formen el grup d'automorfismes $\mathrm{aut}(E)$.

Considerem les corbes el·líptiques E_1, E_2 i les isogènies $\phi\colon E_1 \to E_2$ i $\phi'\colon E_2 \to E_1$. Direm que E_1 i E_2 són isomorfes si $\phi \circ \phi' = \mathrm{Id}_{E_2}$ i $\phi' \circ \phi = \mathrm{Id}_{E_1}$; ho denotarem per $E_1 \cong E_2$.

PROPOSICIÓ 41 ([22, proposició 4.2]). *Si E_1, E_2 són corbes el·líptiques, aleshores el grup d'isogènies $\mathrm{Hom}(E_1, E_2)$ és un $\mathbb{Z}$-mòdul lliure de torsió: donats $a \in \mathbb{Z}$ i $\phi \in \mathrm{Hom}(E_1, E_2)$, aleshores $[a] \circ \phi = 0 \Rightarrow a = 0$ o bé $\phi = 0$.*

Els divisors de zero a $\mathrm{End}(E)$ són isogènies no nul·les $\phi\colon E \to E$ tals que la seva composició amb una altra isogènia no nul·la $\psi\colon E \to E$ és 0.

PROPOSICIÓ 42 ([22, proposició 4.2]). *Donada una corba el·líptica E, $\mathrm{End}(E)$ és un anell no necessàriament abelià i sense divisors de zero.*

PROPOSICIÓ 43 ([22, corol·lari 4.11]). *Considerem una isogènia $\phi\colon E_1 \to E_2$ no constant i separable i ψ una isogènia no constant. Aleshores $\ker(\phi) \subset \ker(\psi) \Rightarrow \exists!\, \lambda \in \mathrm{Hom}(E_2, E_3) : \psi = \lambda \circ \phi$.*

TEOREMA 44. *Considerem $\phi \in \mathrm{Hom}(E_1, E_2)$ una isogènia de grau m. Existeix una única isogènia $\hat{\phi} \in \mathrm{Hom}(E_2, E_1)$, anomenada* isogènia dual*, tal que:*

(1) $\hat{\phi} \circ \phi = [m]\colon E_1 \to E_1$ *i* $\phi \circ \hat{\phi} = [m]\colon E_2 \to E_2$.

(2) $\forall \psi \in \mathrm{Hom}(E_2, E_3)$, $\widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}$ *i* $\widehat{\psi + \phi} = \hat{\phi} + \hat{\psi}$.

(3) $\deg(\phi) = \deg(\hat{\phi})$.

(4) $\hat{\hat{\phi}} = \phi$.

El següent resultat estableix un dels punts clau de la criptografia basada en isogènies: les isogènies factoritzen. A la pràctica aquest fet es tradueix en el fet que hom pot definir una isogènia de grau alt com una composició d'isogènies amb grau petit, la qual cosa fa que sigui més fàcil de manipular.

PROPOSICIÓ 45 ([23, corol·lari 6.18]). *Una isogènia separable $\phi\colon E \to E'$ descompon com la composició d'isogènies $\phi = \phi_0 \circ \phi_1 \circ \cdots \phi_n$ tals que $\phi_i\colon E_i \to E_{i+1}$ té grau primer per a tot $i \in \{0, \ldots, n\}$, posant $E_0 \cong E$ i $E_{n+1} \cong E'$.*

4.2 Fórmules de Vélu

Com que tota isogènia $\phi \in \mathrm{Hom}(E_1, E_2)$ té associat un nucli $\ker(\phi) = G$ que és un subgrup finit de $E_1(\overline{\mathbb{K}})$, és natural preguntar-se quan la isogènia ϕ queda determinada per G o bé quins subgrups finits de $E_1(\overline{\mathbb{K}})$ són el nucli d'una isogènia. La resposta la dona la proposició següent:

PROPOSICIÓ 46 ([8, teorema 9.6.19]). *Considerem una corba el·líptica E i un subgrup finit $G \subset E(\overline{\mathbb{K}})$. Aleshores existeix un única corba el·líptica E' i una isogènia separable $\phi\colon E \to E'$ tal que $\ker(\phi) = G$ i $E' \cong E/\langle G \rangle$.*

Les fórmules de Vélu són expressions que ens permetran construir isogènies a partir d'una corba el·líptica i un subgrup finit. Observem que si combinem el resultat següent amb el teorema anterior deduïm que una isogènia queda completament determinada pel seu nucli. Cal notar que sempre parlem d'isogènies separables.

PROPOSICIÓ 47 ([8, proposició 25.1.6]). *Considerem un subgrup finit $G \subset E(\overline{\mathbb{K}})$ on E és una corba el·líptica sobre $\mathbb{K}$ donada per l'equació de Weierstrass. Una isogènia separable $\phi\colon E \to E'$ amb $\ker(\phi) = G$ es pot escriure com*

$$\phi(P) = \left(x_P + \sum_{Q \in G - \{O_E\}} x_{P+Q} - x_Q, y_P + \sum_{Q \in G - \{O_E\}} y_{P+Q} - y_Q \right),$$

amb $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$ i $P + Q = (x_{P+Q}, y_{P+Q})$ i essent la corba $E' : y^2 = x^3 + a'x + b'$ on

$$\begin{cases} a' = a - 5 \sum_{Q \in G - \{O_E\}} (3x_Q^2 + a), \\ b' = b - 7 \sum_{Q \in G - \{O_E\}} (5x_Q^3 + 2ax_Q + b). \end{cases}$$

4.3 Polinomis modulars

Els polinomis modulars són una forma alternativa per al càlcul de nuclis. Donat un enter $l > 2$, un polinomi modular és un polinomi $\Phi_l(x, y) \in \mathbb{K}[x, y]$ per al qual un parell $j_1, j_2 \in \mathbb{K}$ satisfà $\Phi_l(j_1, j_2) = 0$ si, i només si, existeixen corbes el·líptiques E_1, E_2 sobre $\mathbb{K}$ tals que $j(E_1) = j_1$, $j(E_2) = j_2$ i per a les quals existeix $\phi \in \mathrm{Hom}(E_1, E_2)$ de grau l.

És immediat observar que, donada una corba el·líptica E, hom pot trobar j-invariants de corbes l-isogèniques[3] trobant les arrels, a $\mathbb{K}$, del polinomi $\Phi_l(j(E), y) \in \mathbb{K}[y]$.

4.4 Corbes el·líptiques supersingulars

Un *polinomi de divisió* és un element $\psi \in \mathbb{K}[x, y, a, b, (2y)^{-1}]$, on a i b són els coeficients de l'equació de Weierstrass definida sobre $\mathbb{K}$. Els definim de forma recursiva:

- $\psi_1 = 1$.
- $\psi_2 = 2y$.
- $\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2$.
- $\psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3)$.
- Per a $m \geq 2$: $\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$.
- Per a $m \geq 3$: $\psi_{2m} = (2y)^{-1}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)$.

3 Fem notar l'abús de llenguatge: les isogènies involucrades són de grau l.

TEOREMA 48 ([20, teorema 1.8]). *Si* $\mathrm{char}(\mathbb{K}) \nmid m$, *aleshores*

$$[m](x,y) = \left(\frac{\phi_m(x)}{\psi_m^2}(x), \frac{\omega_m(x,y)}{\psi_m^3(x,y)}\right),$$

on $\phi_m := x\psi_m^2 - \psi_{m+1}\psi_{m-1}$ *i* $\omega_m := \psi_{m+2}\psi_{m-1}^2 + \psi_{m-2}\psi_{m+1}^2$.

Els punts $P \in E(\overline{\mathbb{K}})$ d'ordre m són aquells tals que $[m]P = O_E$. Formen un subgrup de $E(\overline{\mathbb{K}})$ amb la suma i el producte anomenat *subgrup de m-torsió*, que denotem per $E[m]$. El subgrup de torsió de E és el conjunt $E_{\mathrm{tors}} = \bigcup_{m\geq 1} E[m]$.

La relació entre els polinomis de divisió i el subgrup de m-torsió queda determinada pel lema següent:

LEMA 49 ([20, corol·lari 1.10]). *Donada una corba el·líptica E sobre un cos $\mathbb{K}$ tenim: si* $\mathrm{char}(\mathbb{K}) \nmid m$, *aleshores un punt $P \in E(\overline{\mathbb{K}})$ és una arrel ψ_m si, i només si, $P \in E[m]$.*

Pel que fa a l'estructura del subgrup de m-torsió, tenim:

LEMA 50. *En les condicions del lema anterior, $E[m] \cong \mathbb{Z}_m \times \mathbb{Z}_m$.*

El resultat següent aporta una primera caracterització de les corbes el·líptiques supersingulars:

TEOREMA 51 ([8, teorema 9.11.2]). *Considerem una corba el·líptica (E, O_E) sobre un cos finit $\mathbb{F}_q$, amb $q = p^m$ i p primer. Les afirmacions següents són equivalents:*

(1) $\#E(\mathbb{F}_q) = q + 1 - \tau_E$ *on* $p \mid \tau_E$.
(2) $E[p] = O_E$.
(3) $\mathrm{End}_{\overline{\mathbb{F}_q}}(E)$ *té estructura d'anell no commutatiu.*
(4) El polinomi característic de Frobenius de E factoritza sobre $\mathbb{C}$ amb arrels α_1, α_2 tals que $\frac{\alpha_i}{\sqrt{q}}$ és una arrel de la unitat per a $i \in \{1,2\}$.

Una corba que satisfà qualsevol dels punts anteriors rep el nom de *supersingular*. Altrament s'anomena *ordinària*.

OBSERVACIÓ. Una forma accessible de definir una corba el·líptica supersingular és com a corba tal que compleix qualsevol de les condicions següents:

1. $\#E(\mathbb{F}_q) \equiv 1 \bmod p$.
2. $\tau_E \equiv 0 \bmod p$.

Ambdues condicions es dedueixen immediatament del teorema anterior.

La condició d'ésser supersingular o ordinària és un invariant isogènic. En efecte:

PROPOSICIÓ 52 ([23, teorema 14.1]). *Donada una isogènia $\phi\colon E_1 \to E_2$ entre corbes el·líptiques, E_1 és supersingular (resp. ordinària) si, i només si, E_2 és supersingular (resp. ordinària).*

4.5 Relació entre reticles i corbes el·líptiques

Un *reticle complex* és un subconjunt discret i additiu $\Lambda \subseteq \mathbb{C}^n$. Considerem $R = \{a + bi \mid a, b \in \mathbb{Z}\}$ l'anell d'enters gaussians. Donat un conjunt amb m vectors linealment independents de $\mathbb{C}^n$, $\{v_1, \ldots, v_m\}$, un *reticle complex de rang m i dimensió n* és un conjunt generat per aquests vectors:

$$\Lambda(v_1, \ldots, v_m) := \left\{ \sum_{i=1}^{m} c_i v_i \mid c_i \in R \right\}.$$

EXEMPLE. Donat un reticle complex Λ, l'espai quocient $\mathbb{T} = \mathbb{C}^n/\Lambda$ s'anomena *tor complex*.

Dos reticles complexos Λ_1, Λ_2 són homotètics si existeix $\alpha \in \mathbb{C} - \{0\}$ tal que $\Lambda_1 = \alpha\Lambda_2$.

Donat un reticle complex Λ, la sèrie d'Eisenstein amb pes $2k$ es defineix com $G_{2k}(\Lambda) = \sum_{\omega \in \Lambda - \{0\}} \omega^{-2k}$. S'escriu $g_2(\Lambda) = 60G_4(\Lambda)$ i $g_3(\Lambda) = 140G_6(\Lambda)$. El j-invariant modular es defineix com $j(\Lambda) = 1728\frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2}$.

TEOREMA 53 ([21, teorema 4.1]). *Dos reticles complexos són homotètics si, i només si, els j-invariants modulars associats coincideixen.*

El teorema anterior classifica els tors complexos tret d'homotècia ja que sempre podem associar un tor a un reticle. Estableix les condicions sota les quals dos reticles són homotètics, la qual cosa, en el cas dels tors, es tradueix a saber sota quines condicions dos tors són isomorfs.

Tant el j-invariant d'una corba el·líptica com el j-invariant modular d'un reticle són classificadors: en el primer cas classifiquen corbes tret d'isomorfisme, mentre que en el segon cas classifiquen reticles tret d'homotècia. El morfisme $\Lambda \to \mathbb{C}$, $g_2 \mapsto 4a^3$, $g_3 \mapsto b$ envia $j(\Lambda)$ a $j(E : y^2 = 4x^3 - g_2x - g_3)$. De manera que per a tota classe d'homotècia d'un tor complex tenim una classe d'isomorfia de corbes el·líptiques sobre $\mathbb{C}$. Recíprocament:

TEOREMA 54 (TEOREMA D'UNIFORMITZACIÓ, [21, corol·lari 4.3]). *Donat un parell $a, b \in \mathbb{C}$ tal que $4a^3 + 27b^2 \neq 0$ existeix un reticle complex Λ únic tal que $g_2(\Lambda) = -4a$ i $g_3(\Lambda) = -4b$.*

Observem que el teorema estableix un morfisme entre corbes el·líptiques i tors complexos de manera que, donada una classe d'isomorfia de corbes el·líptiques complexes, es té una classe d'homotècia de tors complexos. Aquest fet, amb l'observació anterior, defineix una bijecció entre classes d'isomorfia de corbes el·líptiques complexes i classes d'homotècia de tors complexos.

Considerem tot seguit dos reticles complexos Λ_1, Λ_2 per als quals existeix $\alpha \in \mathbb{C}$ tal que $\Lambda_1 \subset \alpha\Lambda_2$. Definim un morfisme $\phi_\alpha \colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$, $z \mapsto \alpha z \bmod \Lambda_2$. El resultat següent estableix que els morfismes de la forma ϕ_α es corresponen amb les isogènies entre les corbes el·líptiques associades:

TEOREMA 55 ([22, teorema 4.1]). *Si E_1, E_2 són corbes el·líptiques complexes i Λ_1, Λ_2 els reticles associats, aleshores existeix una bijecció entre* $\mathrm{Hom}(E_1, E_2)$ *i el conjunt de morfismes ϕ_α, amb $\alpha \in \mathbb{C}$ tal que $\Lambda_1 \subset \alpha\Lambda_2$.*

4.6 Problemes computacionalment complexos

Els següents problemes són els principals candidats a problema computacionalment complex sobre el qual recolzar protocols criptogràfics.

1. Càlcul d'isogènies: considerant $p \neq l$ números primers i $n \in \mathbb{N}$, trobem les versions següents per al problema del càlcul d'isogènies.
   - Trobar un parell de corbes el·líptiques supersingulars E_1, E_2 sobre un cos finit $\mathbb{F}_{p^2}$ d'ordre p^2, i dues isogènies diferents $f_{1,2}\colon E_1 \to E_2$ de grau l^n.
   - Donada una corba el·líptica supersingular E sobre un cos finit $\mathbb{F}_{p^2}$ d'ordre p^2, trobar $f \in \mathrm{End}(E)$ de grau l^{2n} tal que $f \neq [l^n]$.
   - Donades dues corbes el·líptiques supersingulars sobre un cos finit $\mathbb{F}_{p^2}$ d'ordre p^2, trobar una isogènia $f\colon E_1 \to E_2$ de grau l^n.
2. Càlcul d'ordres maximals: aquest problema presenta les variants següents.
   - Donat un número primer p, una base estàndard per a l'àlgebra de quaternions $B_{p,\infty}$, ramificada en p i ∞[4] i E, una corba el·líptica supersingular sobre un cos finit $\mathbb{F}_{p^2}$ d'ordre p^2, trobar una base per a l'ordre maximal $\mathcal{O}$ de $B_{p,\infty}$ tal que $\mathrm{End}(E) \cong \mathcal{O}$.
   - Donat un número primer p, una corba el·líptica supersingular E, un cos finit $\mathbb{F}_{p^2}$ d'ordre p^2 i quatre elements $\{\beta_1, \beta_2, \beta_3, \beta_4\}$ en un ordre maximal $\mathcal{O}$ de $B_{p,\infty}$ tals que existeix un isomorfisme $\iota\colon \mathrm{End}(E) \to \mathcal{O}$, trobar vuit parells de punts de E, $(P_1, Q_{1r}), (P_2, Q_{2r}), r \in \{1,2,3,4\}$, tals que P_1, P_2 formen una base per a $E[l]$ i tals que $Q_{1r} = \iota^{-1}(\beta_r)(P_1)$ i $Q_{2r} = \iota^{-1}(\beta_r)(P_2)$ per a $r \in \{1,2,3,4\}$.
3. Càlcul de l'anell d'endomorfismes: considerem un número primer p i $n > 0$. Per a una corba el·líptica supersingular E sobre un cos finit $\mathbb{F}_{p^n}$, d'ordre p^n, calcular l'anell d'endomorfismes $\mathrm{End}(E)$.

4.6.1 La correspondència de Deuring Considerem H una $\mathbb{Q}$-àlgebra finitament generada. Un *ordre* R de H és un subanell de H que és finitament generat com a $\mathbb{Z}$-mòdul i tal que $H = R \otimes \mathbb{Q}$.

El resultat següent caracteritza l'anell d'endomorfismes:

TEOREMA 56 ([6, teorema 29]). *Donada una corba el·líptica E sobre un cos $\mathbb{F}$ amb característica p, l'anell d'endomorfismes de E és isomorf a:*

(1) $\mathbb{Z}$ si $p = 0$, o bé

(2) un ordre R en una extensió de la forma $\mathbb{Q}[\sqrt{d}]$, per a $d < 0$, o bé

(3) un ordre maximal en l'àlgebra quaterniònica $B_{p,\infty}$ que ramifica en p i en ∞.

4 Una referència per a àlgebres quaterniòniques és [26].

TEOREMA 57 (CORRESPONDÈNCIA DE DEURING, [4, teorema 2.1]). *Sigui p un nombre primer i un cos finit $\mathbb{F}_p$ de característica p. Per a tot $j_0 \in \overline{\mathbb{F}_p}$, sigui $E(j_0)$ una corba elíptica en la classe d'isomorfisme de les corbes amb j-invariant j_0. Per a tot $j_i \in \overline{\mathbb{F}_p}$ existeix una bijecció entre els ordres maximals de $B_{p,\infty}$ i* $\mathrm{End}_{\overline{\mathbb{F}_p}}(E(j_i))$.

La correspondència de Deuring estableix un diccionari entre isogènies i ordres d'àlgebres quaterniòniques que permet una estratègia interessant per a l'estudi dels problemes relacionats amb la seguretat dels sistemes criptogràfics basats en isogènies. Aquesta estratègia es compon dels passos següents:

1. Traslladar un problema d'isogènies al seu equivalent en ordres;
2. resoldre el problema d'ordres;
3. traslladar la solució d'ordres al seu equivalent en isogènies.

Pel que fa al problema del càlcul de l'anell d'endomorfismes, existeixen dues maneres d'atacar-lo:

1. Determinar $\mathrm{End}(E)$ explicitant les isogènies, la qual cosa no és recomanable ja que isogènies de grau alt requeriran molt d'espai computacional per a la seva descripció.
2. Fer servir la correspondència de Deuring per descriure $\mathrm{End}(E)$ com un $\mathbb{Z}$-mòdul en una àlgebra quaterniònica.

Agraïments

L'autor desitja agrair els comentaris realitzats pel revisor, que han fet millorar sensiblement aquest article.

Referències

[1] AGGARWAL, D.; DADUSH, D.; REGEV, O.; STEPHENS-DAVIDOWITZ, N. «Solving the shortest vector problem in 2^n time via discrete Gaussian sampling (extended abstract)». A: *STOC'15—Proceedings of the 2015 ACM Symposium on Theory of Computing*. Nova York: ACM, 2015, 733–742.

[2] BERLEKAMP, E. R.; MCELIECE, R. J.; VAN TILBORG, H. C. A. «On the inherent intractability of certain coding problems». *IEEE Trans. Information Theory*, IT-24 (3) (1978), 384–386.

[3] BIASSE, J.-F.; JAO, D.; SANKAR, A. «A quantum algorithm for computing isogenies between supersingular elliptic curves». A: *Progress in cryptology—INDOCRYPT 2014*. Cham: Springer, 2014, 428–442. (Lecture Notes in Comput. Sci.; 8885)

[4] CERVIÑO, J. M. «Supersingular elliptic curves and maximal quaternionic orders». Preprint, 2004.

[5] Childs, A.; Jao, D.; Soukharev, V. «Constructing elliptic curve isogenies in quantum subexponential time». *J. Math. Cryptol.*, 8 (1) (2014), 1–29.

[6] De Feo, L. «Mathematics of isogeny based cryptography». Preprint, 2017.

[7] Ebeling, W. *Lattices and Codes. A Course Partially Based on Lectures by F. Hirzebruch*. 3a ed. Wiesbaden: Springer Spektrum, 2013. (Advanced Lectures in Mathematics)

[8] Galbraith, S. D. *Mathematics of Public Key Cryptography*. Cambridge: Cambridge University Press, 2012.

[9] Goldreich, O.; Micciancio, D.; Safra, S.; Seifert, J.-P. «Approximating shortest lattice vectors is not harder than approximating closest lattice vectors». *Inform. Process. Lett.*, 71 (2) (1999), 55–61.

[10] Hoffstein, J.; Pipher, J.; Silverman, J. H. *An Introduction to Mathematical Cryptography*. Nova York: Springer, 2008. (Undergraduate Texts in Mathematics)

[11] Micciancio, D. «Lattices Algorithms and Applications». Apunts d'un curs, 2010.

[12] Micciancio, D.; Regev, O. «Worst-case to average-case reductions based on Gaussian measures». *SIAM J. Comput.*, 37 (1) (2007), 267–302.

[13] Micciancio, D.; Peikert, C. «Hardness of SIS and LWE with small parameters». A: *Advances in Cryptology—CRYPTO 2013*. Part I. Heidelberg: Springer, 2013, 21–39. (Lecture Notes in Comput. Sci.; 8042)

[14] Moody, D.; Shumow, D. «Analogues of Vélu's formulas for isogenies on alternate models of elliptic curves». *Math. Comp.*, 85 (300) (2016), 1929–1951.

[15] Peikert, C. «Lattices: ... to Cryptography». Transparències, 2013.

[16] Regev, O. «Lattices in Computer Science». Apunts, 2004.

[17] Rué, J.; Xambó, S. «Introducció matemàtica a la computació quàntica». *Butlletí de la Societat Catalana de Matemàtiques*, 28 (2) (2013), 183–231.

[18] Sayols, N.; Xambó, S. «Codis correctors d'errors i criptografia postquàntica». *Butlletí de la Societat Catalana de Matemàtiques*, 33 (2) (2018), 147–171.

[19] Shor, P. W. «Algorithms for quantum computation: discrete logarithms and factoring». A: *35th Annual Symposium on Foundations of Computer Science* (Santa Fe, NM, 1994). Los Alamitos, CA: IEEE Comput. Soc. Press, 1994, 124–134.

[20] Shumow, D. «Isogenies of elliptic curves: a computational approach». Preprint, 2009.

[21] Silverman, J. H. *Advanced Topics in the Arithmetic of Elliptic Curves*. Nova York: Springer-Verlag, 1994. (Graduate Texts in Mathematics; 151)

[22] Silverman, J. H. *The Arithmetic of Elliptic Curves*. 2a ed. Dordrecht: Springer, 2009. (Graduate Texts in Mathematics; 106)

[23] SUTHERLAND, A. «Isogeny kernels and division polynomials». Apunts, 2017.

[24] VAN LINT, J. H. *Introduction to Coding Theory*. 2a ed. Berlín: Springer-Verlag, 1992. (Graduate Texts in Mathematics; 86)

[25] VILLANUEVA, M.; FERNÁNDEZ-CÓRDOBA, C. «Codis detectors i correctors d'errors i algunes de les seves aplicacions a la societat de la informació». *Butlletí de la Societat Catalana de Matemàtiques*, 34 (1) (2019), 53–89.

[26] VOIGHT, J. «Quaternion algebras». Apunts d'un curs, 2019.

[27] WASHINGTON, L. C. *Elliptic Curves. Number Theory and Cryptography*. 2a ed. Boca Raton, FL: Chapman & Hall/CRC, 2008. (Discrete Mathematics and its Applications (Boca Raton))

[28] ZHAOFEI, T. «GGH Cryptosystem and Lattice Reduction Algorithms». Tesi de màster. McMaster University, 2011.

EURECAT, CENTRE TECNOLÒGIC DE CATALUNYA, UNITAT IT SECURITY
GRUP DE RECERCA EN NOUS MODELS DE CIBERSEGURETAT (2017 SGR 01239)
CARRER DE BILBAO, 72, 08005 BARCELONA, CATALUNYA
ramses.fernandez@eurecat.org