UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

Didàctica del criptosistema GGH

Autora: Júlia Guitart Torra

Directors: Xavier Guitart Morales
Jordi Font González
Realitzat a: Facultat de Matemàtiques i Informàtica

Barcelona, 10 de juny de 2024

Hauríem d'ensenyar unes matemàtiques que facin madurar el pensament
i que siguin útils per a la vida.
Maria Antònia Canals

Abstract

Lattice-based cryptography is one of the most promising in the near future of postquantum cryptography. In this paper, we will study in particular the GGH cryptosystem, first exposing the key concepts of lattice theory necessary for its understanding. We will also see lattice-based algorithms, which are useful for the development of the cryptosystem and others designed to break it and attack its security. This research is carried out with the aim to create an activity for the baccalaureate classroom in order to bring current mathematics closer to students. In this second part, we can find the detailed description of the activity and some practical materials with ICT resources.

Resum

La criptografia basada en reticles és una de les més prometedores en el futur pròxim de la criptografia postquàntica. En aquest treball, estudiarem en concret el criptosistema GGH, tot exposant primer els conceptes claus de la teoria de reticles necessaris per a la seva comprensió. També veurem algorismes amb reticles útils per al desenvolupament del criptosistema i d'altres pensats per trencar-lo i atacar la seva seguretat. Aquesta recerca es du a terme per finalment crear una activitat per l'aula de batxillerat i d'aquesta manera, apropar matemàtiques actuals als alumnes. En aquesta segona part, podrem trobar la descripció detallada de l'activitat i materials útils amb recursos TIC.

2020 Mathematics Subject Classification. 11G05, 11G10, 14G10

Agraïments

Vull agrair, primer de tot, al Xavier Guitart i al Jordi Font, tutors d'aquest treball, per guiar-me, animar-me, donar respostes alhora que fer les preguntes adequades i fer-me un camí fàcil. Treballar amb el Jordi i poder rebre els seus consells per l'aula i aprendre com ensenyar matemàtiques ha sigut un honor. D'altra banda, que el Xavier m'introduís a la criptografia va ser tot un regal. Treballar i aprendre d'un matemàtic com és ell ha sigut un honor.

També m'agradaria agrair a l'escola Daina-Isard, l'escola de la meva vida i des de sempre, casa. Gràcies per obrir-me sempre les portes i tenir un sí. Gràcies per ser inici de tot a la meva vida i en concret, de la vocació de docent.

Gràcies a la Maria i el Joan i a totes les amigues per la comprensió i l'acompanyament constant al llarg d'aquests anys.

Finalment, gràcies als pares i al Ferran. Sou incondicionals. Gràcies per tenir fortalesa quan jo no podia.

Índex

1 Introducció **1**

2 Reticles **3**

2.1 Definicions i propietats bàsiques 3

2.2 Vectors curts en reticles 8

2.2.1 Problema del vector més curt i problema del vector més proper . . 8

2.2.2 Variacions dels problemes del vector més curt i del més proper . . 8

2.3 Teorema d'Hermite i teorema de Minkowski 9

3 Algorismes de resolució **11**

3.1 Resolució del problema del vector més curt amb una base ortogonal . . . 11

3.2 Resolució del problema del vector més proper amb una base ortogonal . . 11

3.3 Algorisme del vèrtex més proper de Babai 12

4 Algorismes de reducció de reticles **13**

4.1 Algorisme LLL 13

5 Criptosistemes basats en reticles **16**

5.1 Introducció 16

5.2 Criptosistema Goldreich, Goldwasser i Halevi (GGH) 16

5.2.1 Introducció 16

5.2.2 Descripció del criptosistema 17

5.2.3 Esquema GGH 18

5.2.4 Exemple GGH 19

5.2.5 Exemple LLL 21

5.3 Programa criptosistema GGH 23

6 Didàctica **24**

6.1 Antecedents didàctics 24

6.2 Fitxa de l'activitat 26

6.3 Fitxa pel professorat 28

6.4 Fitxa per l'alumnat 29

6.5 Implementació de l'activitat 30

6.6 Propostes de millora o ampliació 32

7 Conclusions **33**

8 Apèndix A: Programa criptosistema GGH **34**

9 Apèndix B: Fitxa pel professorat **41**

9.1 Definicions bàsiques 41

9.2 Esquema GGH 41

9.3 Esquema GGH per l'activitat a l'aula en dues dimensions 42

9.4 GeoGebra 43

1 Introducció

La paraula criptografia és un híbrid entre dos termes grecs: *kryptós*, que significa ocult i *graphein*, que significa escriure. Així doncs, la traducció literal seria escriptura oculta, però en definitiva, el que volem de la criptografia, és tenir una transmissió segura d'informació. Al llarg de la història de la humanitat, hem pogut veure com la transmissió de missatges secrets tenia un paper molt important, sobretot per motius bèl·lics. Però abans del 1977, l'enfocament de la criptografia tenia un hàndicap: en algun punt del procés, els dos interlocutors havien de veure's per acordar la clau secreta o enviar-se-la. A aquest model, poc pràctic i segur, se'l denomina de clau simètrica.

Aleshores, la pregunta més sensata a fer-se, va ser si es podia crear un mètode per enviar informació, on no fos necessària una prèvia comunicació. El 1976, Whitfield Diffie i Martin Hellman van parlar per primera vegada de la criptografia de clau pública, tot i que no van donar un algorisme concret per dur-la a terme. El 1977, Ron Rivest, Adi Shamir i Len Adleman van descriure l'algorisme RSA. Aquest algorisme, va ser el percussor dels criptosistemes de clau pública, en els quals només es fa pública una part de la clau i l'altra es manté privada. La clau pública és útil per a xifrar missatges, però ineficaç a l'hora de desxifrar-los, mentre que la clau privada et permet desxifrar de manera eficient.

La creació d'aquest tipus de criptosistemes també va venir amb el canvi de raons per les quals interessava la criptografia. Ja no es buscava la confidencialitat de missatges, sinó la codificació de texts per l'autentificació o integritat de la informació i la confidencialitat d'aquesta. Per tant, va passar a ser una eina important per la ciberseguretat.
Amb aquests nous criptosistemes, la seva seguretat venia d'utilitzar problemes que no tenen solucions computacionalment eficients. Com per exemple, la factorització d'enters al l'RSA, o de logaritmes discrets.

Actualment, tornem a estar davant d'un repte pel que fa a la criptografia com la coneixíem fins ara. La computació quàntica, que permet computar de forma paral·lela sobre diferents valors, i, per tant, la creació d'algorismes quàntics com el de Shor (algorisme que podria deixar obsolet el RSA si es posés en pràctica), han fet que el paradigma sencer de la criptografia canviés.
Encara no hi ha ordinadors quàntics prou eficients per posar en pràctica aquests tipus d'algorismes, però es preveu que en uns anys ja podrien ser aquí. És per això que el que ocupa actualment a molts matemàtics i científics, és buscar nous criptosistemes resistents a atacs quàntics, que no suposin un empitjorament a nivells de temps d'execució o espai necessari d'emmagatzematge respecte als vigents.
De fet, el 2016, el NIST (National Institute of Standards and Technology) va llençar una competició per trobar el millor criptosistema postquàntic. Es van entregar 82 propostes i finalment, el 2022, en van seleccionar 4 de finalistes. D'aquestes, 3 es basaven en matemàtica de reticles. És per això, que en aquest treball ens centrem en aquests criptosistemes i en estudiar què són els reticles i quines eines proporcionen, que siguin útils per a la criptografia.

Encara estem davant d'un problema sense solució, perquè no s'ha trobat l'algorisme definitiu a implementar en un futur. Tot i això, en aquest treball, ens hem centrat a entendre l'algorisme GGH, un dels algorismes de clau pública basats en reticles més rellevants.
Veurem com s'estructura el criptosistema, un exemple de dimensió 4 d'aquest i veurem també per a quines raons no s'implementa. A més a més, veurem algorismes que podrien

arribar a trencar-lo en dimensions petites i, per tant, per claus petites.
Per una millor comprensió i experimentació amb el criptosistema, també s'ha realitzat un programa amb sage que es pot consultar a l'annex A.

A part de tenir en compte la rellevància d'aquest criptosistema, per ser un dels primers a basar-se en reticles, hi ha una altra raó per la qual ens hem centrat en ell en aquest treball.
L'algorisme GGH, és un dels de més fàcil comprensió i fàcilment adaptable a l'aula per les eines matemàtiques que utilitza. És per això que ens ha brindat una gran oportunitat per fer una activitat didàctica per batxillerat tot portant a l'aula el criptosistema per a dimensió dos o tres. L'activitat creada podria ser un bon recurs a tall de petit projecte de recerca de tancament de la unitat de geometria que fan als cursos de batxillerat, està pensada per aplicar el que s'ha après al llarg del tema, per donar-li una contextualització i una perspectiva real.
La segona part d'aquest treball consta d'uns antecedents didàctics sobre els quals ens hem inspirat per elaborar l'activitat, una descripció detallada d'aquesta juntament amb una fitxa per l'alumnat, també conclusions i reflexions un cop feta la implementació a l'aula i finalment, als annexos, podem trobar la fitxa pel professorat, on hi ha el resum necessari per poder dur a terme l'activitat així com l'explicació de les eines informàtiques que s'han utilitzat.

Tal com es diu en el llibre [3] *Tres professors de matemàtiques*, "*En ensenyar matemàtiques podem crear sorpreses docents en la manera de presentar conceptes o resultats, i també tenim la possibilitat de sorprendre amb els mateixos resultats o amb l'ús o l'aparició inesperada d'aquests. Podem fer sentir la sorpresa d'un resultat geomètric curiós o d'una bonica regularitat aritmètica o podem sorprendre amb un recurs didàctic que cridi l'atenció i aporti una experiència inoblidable*".
Deixem-nos, doncs, sorprendre per la possibilitat d'entrar a l'aula matemàtiques, eines i conceptes que no ens havíem imaginat, i poder-los relacionar de forma molt estreta amb una part essencial de les matemàtiques de batxillerat.

Us convido a fer aquest viatge per la criptografia postquàntica i l'adaptació a l'aula d'aquesta.

2 Reticles

2.1 Definicions i propietats bàsiques

Definició 2.1. *Siguin $v_1, \dots, v_n \in \mathbb{R}^m$ vectors linealment independents. El* ***reticle*** *L* ***generat*** *per aquests vectors, és el conjunt de combinacions lineals de $v_1, \dots, v_n$ amb coeficients en $\mathbb{Z}$,*

$$L = \{a_1 v_1 + \cdots + a_n v_n : a_1, \dots, a_n \in \mathbb{Z}\}.$$

Definició 2.2. *Una* ***base*** *B* ***d'un reticle*** *L és qualsevol conjunt de vectors linealment independents que generin L.*

Si dues bases generen el mateix reticle, tindran el mateix nombre d'elements.

Definició 2.3. *La* ***dimensió del reticle*** *ve donada pel nombre de vectors de la seva base.*

Proposició 2.4. *Dues bases d'un reticle L estan relacionades per una matriu amb coeficients enters i determinant igual a ± 1.*

Demostració. Suposem que tenim $v_1, \dots, v_n$ base del reticle L i $w_1, \dots, w_n \in L$. Per tant, podem escriure els w_j com a combinació lineal dels vectors de la base:

$$\begin{aligned} w_1 &= a_{11} v_1 + \cdots + a_{1n} v_n \\ &\vdots \\ w_n &= a_{n1} v_1 + \cdots + a_{nn} v_n. \end{aligned}$$

Sabem que els a_{ij} són coeficients enters, ja que estem treballant amb reticles.
Aquests coeficients els podem expressar en forma d'una matriu

$$\mathrm{A} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}.$$

Veiem que si volem expressar els v_i en funció dels w_j haurem d'utilitzar la inversa de la matriu A i aquesta haurà de tenir coeficients enters. Per tant,

$$1 = \det(I) = \det(AA^{-1}) = \det(A)\det(A^{-1}).$$

Aleshores, $\det(A) = \pm 1$ ja que $\det(A)$ i $\det(A^{-1})$ són enters.
Finalment, si $\det(A) = \pm 1$, pel teorema de la matriu adjunta, A^{-1} tindrà components enteres. □

Observació 2.5. És útil veure un reticle com un conjunt discret de punts a $\mathbb{R}^n$.

Definició 2.6. *Sigui L un reticle de dimensió n i $B = \{v_1, \dots, v_n\}$ una base de L, el* ***paral·lelepípede fonamental*** *de L corresponent a aquesta base és el conjunt*

$$F(v_1, \dots, v_n) = \{t_1 v_1 + \cdots + t_n v_n : 0 \le t_i < 1\}.$$

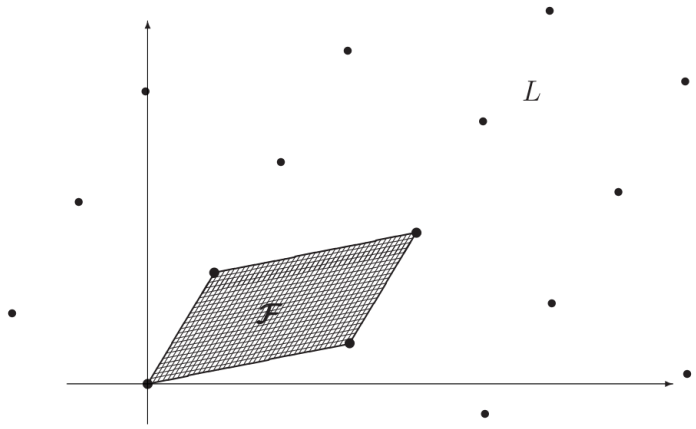


Figura 1: Un paral·lelepípede fonamental F del reticle L.

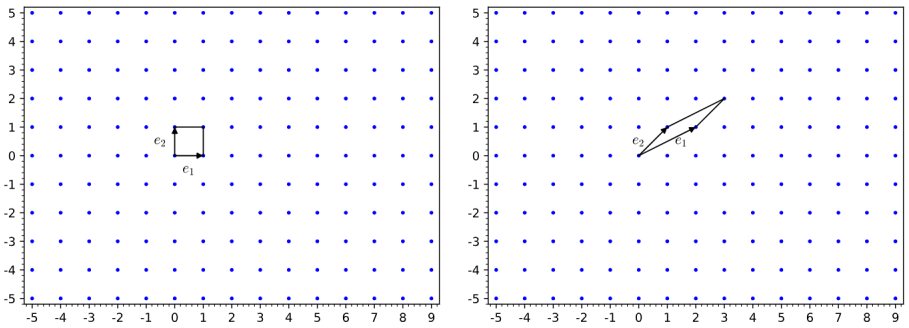


Figura 2: Dos paral·lelepípedes fonamentals amb diferents bases en $\mathbb{Z}^2$.

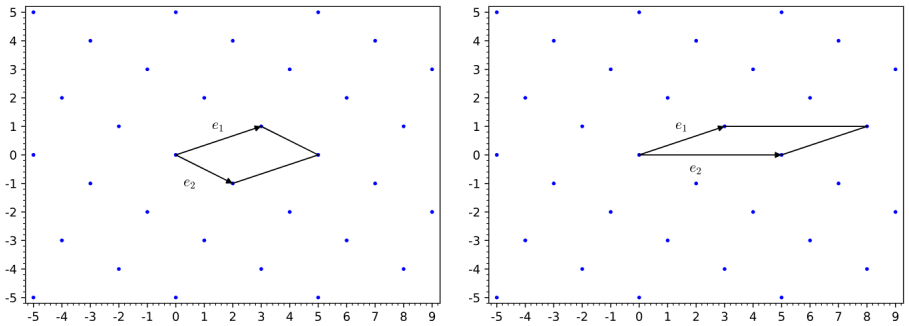


Figura 3: Dos paral·lelepípedes fonamentals amb diferents bases en el reticle generat pels vectors $(3,1),(2,-1)$.

Observació 2.7. Veiem que aquest conjunt no depèn únicament del reticle L, sinó també de la base B. A través de les figures 2 i 3, podem observar com canvia la forma del paral·lelepípede fonamental en funció de la base que escollim. Més endavant, aquesta observació ens serà útil.

Proposició 2.8. *Sigui $L \subset \mathbb{R}^n$ un reticle de dimensió n i F un paral·lelepípede fonamental de L. Qualsevol vector $w \in \mathbb{R}^n$ es pot escriure de la forma*

$$w = t + v$$

per uns únics $t \in F$ i $v \in L$. Equivalentment, la unió dels paral·lelepípedes fonamentals traslladats

$$F + v = \{t + v : t \in F\},$$

on v recorre tots els elements de L, recobreix $\mathbb{R}^n$.

Demostració. Sigui $v_1, \ldots, v_n$ una base de L que dona el paral·lelepípede fonamental F. Aleshores, $v_1, \ldots, v_n$ són vectors linealment independents en $\mathbb{R}^n$, per tant, també són una base de $\mathbb{R}^n$. Això vol dir que podem expressar qualsevol $w \in \mathbb{R}^n$ de la forma

$$w = \alpha_1 v_1 + \cdots + \alpha_1 v_n,\ \alpha_1, \ldots, \alpha_n \in \mathbb{R}.$$

Ara, separem la part decimal de cada α_i obtenint

$$\alpha_i = t_i + a_i,\ \text{amb}\ \ 0 \leq t_i < 1 \ \text{i}\ \ a_i \in \mathbb{Z}.$$

Per tant, veiem que podem escriure w com

$$w = t_1 v_1 + \cdots + t_n v_n + a_1 v_1 + \cdots + a_n v_n \in F + L.$$

Ara, anem, a demostrar la unicitat:
Suposem que $w = t + v = t' + v'$ amb $t, t' \in F,\ v, v' \in L$. Aleshores, tenim que

$$(t_1 + a_1)v_1 + \cdots + (t_n + a_n)v_n = (t'_1 + a'_1)v_1 + \cdots + (t'_n + a'_n)v_n.$$

Com que els vectors són linealment independents, tenim que

$$t_i + a_i = t'_i + a'_i \text{ per } i = 1, \ldots, n.$$

Per tant, $t_i - t'_i = a_i - a'_i$ és un enter i com que $0 \leq t_i, t'_i < 1$, $t_i - t'_i$ serà un enter si i només si $t_i = t'_i$. És a dir, $t = t'$ i en conseqüència, $v = w - t = w - t' = v'$.
Això demostra la unicitat de t i v. □

A continuació, introduirem el concepte de volum d'un reticle. Que és un invariant important d'aquests.

Definició 2.9. *Sigui L un reticle de dimesió n i F un paral·lelepípede fonamental de L. El volum n-dimensional de F es diu el* ***determinant de*** *L i es denota com* $\det(L)$.

Proposició 2.10. *Sigui $L \subset \mathbb{R}^n$ un reticle de dimensió n, $v_1, \dots, v_n$ una base de L i $F = F(v_1, \dots, v_n)$ el paral·lelepípede fonamental associat. Escrivim les coordenades del i-èssim vector de la base com*

$$v_i = (r_{i1}, r_{i2}, \dots, r_{in}).$$

Si utilitzem aquestes coordenades com a files d'una matriu, resulta

$$\mathcal{F} = \mathcal{F}(v_1, \dots, v_n) = \begin{pmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & \ddots & \vdots \\ r_{n1} & \cdots & r_{nn} \end{pmatrix}.$$

Aleshores, la fórmula del volum de F ve donada per

$$\mathrm{Vol}(F(v_1, \dots, v_n)) = |\det(\mathcal{F}(v_1, \dots, v_n))|.$$

Demostració. Podem calcular el volum de F com

$$\mathrm{Vol} = \int_F dx_1\, dx_2 \dots\, dx_n$$

Com que F es un paral·lelepípede fonamental, podem fer el canvi de variables de $x = (x_1, \dots, x_n)$ a $t = (t_1, \dots, t_n)$ seguint la fórmula

$$(x_1, \dots, x_n) = t_1 v_1 + \cdots + t_n v_n.$$

En termes de la matriu $\mathcal{F} = \mathcal{F}(v_1, \dots, v_n)$, el canvi de variables ve donat per l'equació $x = t\mathcal{F}$. La matriu Jacobiana d'aquest canvi de variables és $\mathcal{F}$, i el paral·lelepípede fonamental F és la imatge de $\mathcal{F}$ al cub unitat $C_n = [0,1]^n$. Per tant, la fórmula del canvi de variable per integrals ens porta a

$$\int_F dx_1\, dx_2 \dots\, dx_n = \int_{FC_n} dx_1\, dx_2 \dots\, dx_n = \int_{C_n} |\det \mathcal{F}|\, dx_1\, dx_2 \dots\, dx_n = \\ = |\det \mathcal{F}| \mathrm{Vol}(C_n) = |\det \mathcal{F}|.$$

□

Sigui $v_1, \dots, v_n$ la base d'un reticle L, si els pensem com els vectors que descriuen un paral·lelepípede F, assolirem el volum màxim quan els vectors siguin ortogonals dos a dos. Això ens porta al següent resultat.

Proposició 2.11. *(Desigualtat de Hadamard). Sigui L un reticle, $v_1, \dots, v_n$ una base qualsevol de L i F el paral·lelepípede fonamental de L. Aleshores,*

$$\det(L) \leq \|v_1\| \dots \|v_n\|.$$

Si la base és ortogonal,

$$\det(L) = \|v_1\| \dots \|v_n\|.$$

Demostració. Sigui $\mathcal{F} = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$ la matriu on $v_1, \dots, v_n$ són les seves files. Anomenarem p_i a la projecció ortogonal del vector v_i sobre el subespai generat pels vectors v_j, $\forall j =$

$1, \ldots, n$, $j \neq i$. Com que $p_i \in \langle v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n \rangle$, $\det(\mathcal{F}) = \det[v_1, \ldots, v_{i-1}, v_i - p_i, v_{i+1}, \ldots, v_n]$. A més a més, $(v_i - p_i)$ és ortogonal a p_i, per tant, usant el teorema de pitàgores, tenim

$$v_i = (v_i - p_i) + p_i \Rightarrow \|v_i\|^2 = \|v_i - p_i\|^2 + \|p_i\|^2 \Rightarrow \|v_i - p_i\| \leq \|v_i\|.$$

Ara, repetint el procés restant a tots els v_i la seva projecció sobre les files restants, arribem a la matriu U de la forma

$$U = \begin{bmatrix} v_1 - p_1 \\ v_2 - p_2 \\ \vdots \\ v_{n-1} - p_{n-1} \\ v_n \end{bmatrix}$$

Per definició de projecció ortogonal, tenim

$$v_i = p_i + x_i \text{ amb } p_i \in \langle v_{i+1}, \ldots, v_n \rangle, \text{ i } x_i \in \langle v_{i+1}, \ldots, v_n \rangle^\intercal.$$

És a dir, $v_i - p_i$ és ortogonal a les files $v_{i+1}, \ldots, v_n$ i com a conseqüència, a les files $v_{i+1} - p_{i+1}, \ldots, v_{n-1} - p_{n-1}, v_n$. Per tant, la matriu U està formada per files ortogonals dos a dos. Si denotem $U = \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix}$. Aleshores,

$$UU^\intercal = \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} [u_1^\intercal, \ldots, u_n^\intercal] = \begin{bmatrix} u_1 u_1^\intercal & \cdots & u_1 u_n^\intercal \\ \vdots & \ddots & \vdots \\ u_n u_1^\intercal & \cdots & u_n u_n^\intercal \end{bmatrix} = \begin{bmatrix} \|u_1\|^2 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \|u_n\|^2 \end{bmatrix}.$$

Per tant,

$$\det(\mathcal{F})^2 = (\det(U))(\det(U^\intercal)) = \det(UU^\intercal) = \|u_1\|^2 \cdots \|u_n\|^2 \leq \|v_1\|^2 \cdots \|v_n\|^2.$$

□

Observació 2.12. Veiem que com més s'acosti la desigualtat de Hadamard a una igualtat, més ortogonal serà la base.

Definició 2.13. *Sigui L un reticle de dimensió n i $B = \{v_1, \ldots, v_n\}$ una base de L. Definim el* ***quocient de Hadamard*** *de la base B com*

$$\mathcal{H}(B) = \left(\frac{\det(L)}{\|v_1\| \cdots \|v_n\|} \right)^{1/n}.$$

Observació 2.14. Veiem que $0 < \mathcal{H}(B) \leq 1$, i per tant, com més proper a 1 sigui $\mathcal{H}(B)$, més ortogonal serà la base B.

Corolari 2.15. *Sigui $L \subset \mathbb{R}^n$ un reticle de dimensió n. Aleshores, cada paral·lelepípede fonamental de L tindrà el mateix volum. Per tant,* $\det(L)$ *és invariant al domini que s'utilitzi.*

Demostració. Sigui L un reticle de dimensió n, $v_1, \ldots, v_n$, $w_1, \ldots, w_n$ dues bases de L i $\mathcal{F}(v_1, \ldots, v_n)$, $\mathcal{F}(w_1, \ldots, w_n)$ les matrius associades obtingudes utilitzant les coordenades dels vectors de la base com a files. Aleshores, la Proposició 2.4 ens diu que

$$\mathcal{F}(v_1, \ldots, v_n) = A\mathcal{F}(w_1, \ldots, w_n)$$

per alguna matriu A $n \times n$ amb coeficients enters i $det(A) = \pm 1$. Ara, utilitzant la Proposició 2.10, i sabent que estem en el cas que $\det(A) = \pm 1$, obtenim

$$\begin{aligned} \operatorname{Vol}(F(v_1, \ldots, v_n)) = |\det(\mathcal{F}(v_1, \ldots, v_n))| = |\det(A\mathcal{F}(w_1, \ldots, w_n))| = \\ = |\det(A)||\det(\mathcal{F}(w_1, \ldots, w_n))| = |\det(\mathcal{F}(w_1, \ldots, w_n))| = \operatorname{Vol}(F(w_1, \ldots, w_n)). \end{aligned}$$

Per tant, veiem que el volum és invariant a la base escollida. □

2.2 Vectors curts en reticles

Els problemes computacionals fonamentals associats als reticles són: trobar el vector no nul més curt, i trobar el vector del reticle més proper a un vector que no sigui del reticle. A continuació veurem aquests problemes des d'una perspectiva teòrica.

2.2.1 Problema del vector més curt i problema del vector més proper

Definició 2.16. *Sigui L un reticle, el **problema del vector més curt** consisteix a trobar el vector $v \in L$ no nul, tal que la norma euclídea $\|v\|$ sigui mínima.*

Definició 2.17. *Sigui L un reticle i $w \in \mathbb{R}^n$, $w \notin L$. El **problema del vector més proper** consisteix a trobar el vector $v \in L$ tal que la norma euclídea $\|w-v\|$ sigui mínima. Per tant, $v \in L$ serà el vector de L més proper a w.*

Les solucions a aquests problemes poden ser útils per l'atac contra diversos criptosistemes. Els dos es tornen computacionalment complicats com més gran sigui la dimensió del reticle.

Hi ha variacions dels problemes que acabem de veure, que més endavant seran útils pels algorismes de resolució.

2.2.2 Variacions dels problemes del vector més curt i del més proper

Definició 2.18. *Sigui L un reticle, el **problema de la base més curta** consisteix a trobar la base $v_1, \ldots, v_n$ del reticle tal que*

$$\max_{1 \leq i \leq n} \|v_i\| \ \ o \ \ \sum_{i=1}^{n} \|v_i\|^2$$

siguin mínims.

Definició 2.19. *Sigui L un reticle de dimensió n i $\psi(n)$ una funció de n. Si v_{curt} és el vector no nul més curt de L, el **problema aproximat del vector més curt**, consisteix a trobar el vector no nul $v \in L$ tal que*

$$\|v\| \leq \psi(n)\|v_{curt}\|.$$

Definició 2.20. *Sigui L un reticle de dimensió n i $\psi(n)$ una funció de n. El* ***problema aproximat del vector més proper*** *consisteix a trobar el vector $v \in L$ tal que*

$$\|v\| \leq \psi(n).$$

2.3 Teorema d'Hermite i teorema de Minkowski

Per trobar el vector més curt, necessitem saber la seva longitud, i aquesta depèn de la dimensió i del determinant de L. A continuació, veurem una fita superior de la norma euclidiana en funció d'aquests dos paràmetres.

Teorema 2.21. ***(Teorema de Minkowski)*** *Sigui $L \subset \mathbb{R}^n$ un reticle de dimensió n i sigui $S \subset \mathbb{R}^n$ un conjunt simètric i convex tal que el seu volum satisfà*

$$\mathrm{Vol}(S) > 2^n \det(L).$$

Aleshores, S conté un vector no nul del reticle.
Si a més a més S és tancat, aleshores serà suficient tenir

$$\mathrm{Vol}(S) \geq 2^n \det(L).$$

Demostració. Sigui F un paral·lelepípede fonamental de L. Sabem que qualsevol vector $v \in S$ es pot escriure de manera única com

$$v = a_v + b_v \text{ amb } a_v \in L \text{ i } b_v \in F.$$

Dilatem S pel factor $\frac{1}{2}$ obtenint

$$\frac{1}{2}S = \left\{ \frac{1}{2}a : a \in S \right\}.$$

Sabem que S satisfà $\mathrm{Vol}(S) > 2^n \det(L)$. Per tant, amb S dilatat pel factor $\frac{1}{2}$, tenim

$$\mathrm{Vol}\left(\frac{1}{2}S\right) = \frac{1}{2^n}\mathrm{Vol}(S) > \det(L) = \mathrm{Vol}(F).$$

Considerem l'aplicació $\frac{1}{2}S \to F$, $\frac{1}{2}v \mapsto b_{\frac{1}{2}a}$. Com que S és acotat, sabem que l'aplicació tindrà un nombre finit de translacions i es conservarà el seu volum.
Donat que $\mathrm{Vol}\left(\frac{1}{2}S\right) > \mathrm{Vol}(F)$, existeixen vectors diferents $\frac{1}{2}v_1 = a_1 + b$, $\frac{1}{2}v_2 = a_2 + b \in S$ tal que $a_1, a_2 \in L$ i $b \in F$. Per tant, vectors que tenen la mateixa imatge en F.
Si els restem, obtenim un vector no nul $\frac{1}{2}v_1 - \frac{1}{2}v_2 = a_1 - a_2 \in L$.

□

Definició 2.22. *Sigui L un reticle de dimensió n, anomenem γ_n a la* ***constant d'Hermite****. γ_n és el valor més petit tal que L conté un vector $v \in L$ no nul satisfent*

$$\|v\|^2 \leq \gamma_n \det(L)^{2/n}.$$

Teorema 2.23. ***(Teorema d'Hermite)*** *Tot reticle L de dimensió n conté un vector $v \in L$ no nul tal que*

$$\|v\| \leq \sqrt{n} \det(L)^{2/n}.$$

Demostració. Sigui $L \subset \mathbb{R}^n$ un reticle i S el conjunt definit com

$$S = (x_1, \ldots, x_n) \in \mathbb{R}^n : -B \leq x_i \leq B \text{ per qualsevol } 1 \leq i \leq n.$$

El conjunt S és simètric, tancat i acotat i el seu volum és

$$\text{Vol}(S) = (2B)^n.$$

Per tant, si posem $B = \det(L)^{1/n}$, tenim $\text{Vol}(S) = 2^n \det(L)$ i aplicant el teorema de Minkowski, es dedueix que existeix un vector $v = (v_1, \ldots, v_n)$ no nul tal que $v \in S \cap L$. Aleshores,

$$\|v\| = \sqrt{v_1^2 + \cdots + v_n^2} \leq \sqrt{n}B = \sqrt{n}\det(L)^{1/n}.$$

□

Observació 2.24. Aquest teorema ens diu que $\gamma_n \leq n$.
Per propòsits criptogràfics, ens interessa el valor γ_n per valors de n grans. En aquests casos, tenim

$$\frac{n}{2\pi \text{e}} \leq \gamma_n \leq \frac{n}{\pi \text{e}}$$

Teorema 2.25. ***(Variació teorema d'Hermite)*** *Sigui L un reticle de dimensió n, aleshores L conté una base $\{v_1, \ldots, v_n\}$ tal que*

$$\|v_1\| \cdots \|v_n\| \leq n^{n/2}(\det(L)).$$

Demostració. Similar a la demostració del teorema d'Hermite. □

Observació 2.26. Si completem la desigualtat de la variació del teorema d'Hermite amb la desigualtat de Hadamard, tenim que

$$\begin{aligned} \|v_1\| \cdots \|v_n\| &\leq n^{n/2}(\det(L)), \\ \det(L) &\leq \|v_1\| \cdots \|v_n\|. \end{aligned}$$

3 Algorismes de resolució

Els següents algorismes poden ser utilitzats per resoldre versions aproximades del problema del vector més proper i del problema del vector més curt.
Abans, veurem quines condicions són necessàries sobre els elements de la base d'un reticle per resoldre aquests problemes.
Sigui $L \subset \mathbb{R}^n$ un reticle i $B = \{b_1, \ldots, b_n\}$ la seva base. Si $\langle b_i, b_j \rangle = 0$ per $i \neq j$, aleshores resoldre el problema del vector més proper i el del vector més curt resulta senzill en les seves versions exactes. Veiem com es resolen.

3.1 Resolució del problema del vector més curt amb una base ortogonal

Sigui $w \in L$, existeixen $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$ tal que,

$$\|w\|^2 = \|\alpha_1 b_1 + \cdots + \alpha_n b_n\|^2.$$

Ara, utilitzant que la base és ortogonal, tenim,

$$\begin{aligned} \|w\|^2 = \langle \alpha_1 b_1 + \cdots + \alpha_n b_n, \alpha_1 b_1 + \cdots + \alpha_n b_n \rangle = \\ = \alpha_1 \alpha_1 \langle b_1, b_1 \rangle + \cdots + \alpha_n \alpha_n \langle b_n, b_n \rangle = \\ = \alpha_1^2 \|b_1\|^2 + \cdots + \alpha_n^2 \|b_n\|^2. \end{aligned}$$

Com que els coeficients són enters, tenim que els vectors més curts en L són el conjunt $\{\pm b_1, \ldots, \pm b_n\}$.

3.2 Resolució del problema del vector més proper amb una base ortogonal

Sigui $t \in \mathbb{R}^n$, existeixen $\beta_1, \ldots, \beta_n \in \mathbb{R}$ tal que,

$$t = \beta_1 b_1 + \cdots + \beta_n b_n.$$

Donat $w \in L$, podem expressar w com

$$w = \alpha_1 b_1 + \cdots + \alpha_n b_n.$$

Ara, agafem w i t i fem el càlcul següent:

$$\begin{aligned} \|w - t\|^2 = \|(\alpha_1 - \beta_1) b_1 + \cdots + (\alpha_n - \beta_n) b_n\|^2 = \\ = \langle (\alpha_1 - \beta_1) b_1 + \cdots + (\alpha_n - \beta_n) b_n, (\alpha_1 - \beta_1) b_1 + \cdots + (\alpha_n - \beta_n) b_n \rangle = \\ = (\alpha_1 - \beta_1)^2 \|b_1\|^2 + \cdots + (\alpha_n - \beta_n)^2 \|b_n\|^2. \end{aligned}$$

Com que els $\alpha_i \in \mathbb{Z}$, l'expressió que acabem d'escriure es minimitza quan $\alpha_i = \lfloor \beta_i \rceil$. Per tant, agafant l'enter més proper al β_i corresponent.

3.3 Algorisme del vèrtex més proper de Babai

L'algorisme que presentem a continuació ens permet resoldre el problema del vector més proper amb qualsevol base bastant ortogonal però no necessàriament ortogonal del tot.

Algorisme de Babai

Sigui $L \subset \mathbb{R}^n$ un reticle, $v_1, \ldots, v_n$ base de L i $w \in \mathbb{R}^n$ un vector qualsevol.
Si els vectors de la base són ortogonals o quasi ortogonals entre ells, aleshores el següent algorisme resol el problema del vector més proper.

$$\text{Escrivim } w = t_1 v_1 + t_2 v_2 + \cdots + t_n v_n,\ t_1, \ldots, t_n \in \mathbb{R}.$$
$$\text{Definim } a_i = \lfloor t_i \rceil,\ i = 1, \ldots, n.$$
$$\text{Retornem el vector } v = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n.$$

Conceptualment, l'algorisme agafa el vèrtex del paral·lelepípede fonamental (traslladat on faci falta) més proper a w. Aquest enfocament funciona bé si els vectors de la base són bastant ortogonals entre ells i falla si l'angle entre els vectors és molt petit.

Veiem de forma gràfica com falla l'algorisme de Babai si s'utilitza una base molt poc ortogonal.

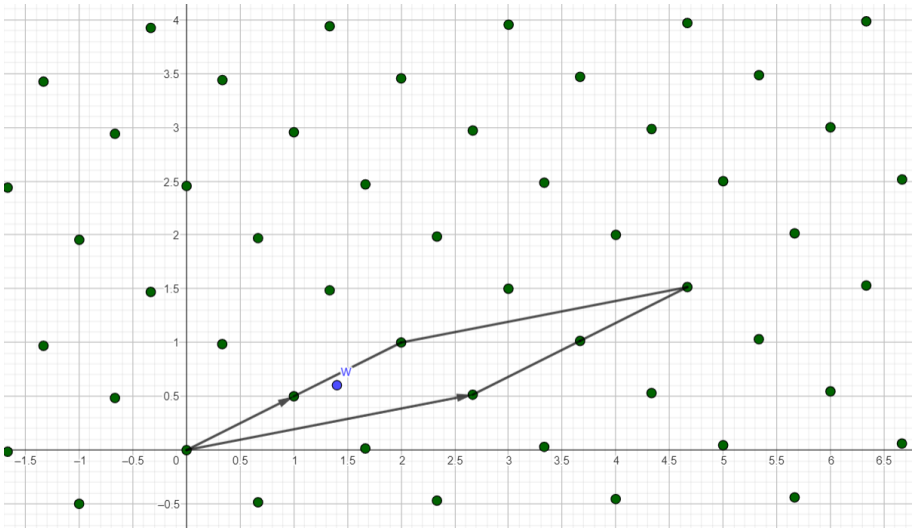


Figura 4: Resolució amb l'algorisme de Babai amb una base molt poc ortogonal.

Veiem, doncs, que si els vectors de la base proporcionats són bastant ortogonals entre ells, l'algorisme resol el problema aproximat del vector més proper. Però si els vectors de la base són molt poc ortogonals, l'algorisme de Babai ens retornara un vector del reticle lluny del vector w. Això ens confirma la necessitat de tenir una base bastant ortogonal.

4 Algorismes de reducció de reticles

A continuació, veurem un algorisme que ens permet reduir una base qualsevol d'un reticle a una que quasi compleixi les condicions necessàries per resoldre el problema del vector més proper.

4.1 Algorisme LLL

L'algorisme LLL no ens retorna una base ortogonal, però si una quasi ortogonal, per tant, si combinem l'algorisme LLL juntament amb el de Babai, podem formar un algorisme que solucioni el problema aproximat del vector més proper.

Abans d'enunciar l'algorisme, introduirem una sèrie de definicions i proposicions que ens ajudaran a la comprensió d'aquest.

Proposició 4.1. *Sigui $\mathcal{B} = \{v_1, \dots, v_n\}$ una base del reticle L i $\mathcal{B}^* = \{v_1^*, \dots, v_n^*\}$ la base ortogonal de Gram-Schmidt associada. Aleshores,*

$$\det(L) = \prod_{i=1}^{n} \|v_i^*\|.$$

Demostració. Sigui $\mathcal{F} = \mathcal{F}(v_1, \dots, v_n)$ la matriu descrita a la Proposició 2.10 i sigui $\mathcal{F}^* = \mathcal{F}(v_1^*, \dots, v_n^*)$ la matriu anàloga que té per files els vectors $v_1^*, \dots, v_n^*$.
Aleshores, les matrius $\mathcal{F}$ i $\mathcal{F}^*$ estan relacionades per una matriu

$$M = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ \mu_{2,1} & 1 & 0 & \cdots & 0 & 0 \\ \mu_{3,1} & \mu_{3,2} & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mu_{n-1,1} & \mu_{n-1,2} & \mu_{n-1,3} & \cdots & 1 & 0 \\ \mu_{n,1} & \mu_{n,2} & \mu_{n,3} & \cdots & \mu_{n-1,n} & 1 \end{pmatrix},$$

matriu de canvi de base, triangular inferior amb $\det(M) = 1$, tal que

$$M\mathcal{F}^* = \mathcal{F}.$$

Aleshores,

$$\det(L) = |\det \mathcal{F}| = |\det(M\mathcal{F}^*)| = |(\det M)(\det \mathcal{F}^*)| = |\det \mathcal{F}^*| = \prod_{i=1}^{n} \|v_i^*\|.$$

□

Definició 4.2. *Sigui $\mathcal{B} = \{v_1, \dots, v_n\}$ una base del reticle L i $\mathcal{B}^* = \{v_1^*, \dots, v_n^*\}$ la base ortogonal de Gram-Schmidt associada.*
*Diem que la base $\mathcal{B}$ és **LLL reduïda** si satisfà les dues condicions següents:*

- $|\mu_{i,j}| = \frac{|v_i \cdot v_j^*|}{\|v_j^*\|^2} \leq \frac{1}{2}$, *per qualsevol* $1 \leq j < i \leq n$.
- *Condició de Lovász:* $\|v_i^*\|^2 \geq \left(\frac{3}{4} - \mu_{i,i-1}^2\right) \|v_{i-1}^*\|^2$, *per qualsevol* $1 < i \leq n$.

A continuació, veiem que una base LLL reduïda té propietats bones per després descriure l'algorisme LLL.

Teorema 4.3. *Sigui L un reticle de dimensió n i $\mathcal{B} = v_1, \ldots, v_n$ una base LLL reduïda de L. Aleshores, $\mathcal{B}$ satisfà:*

$$\prod_{i=1}^{n} \|v_i\| \leq 2^{n(n-1)/4} \det(L), \tag{4.1}$$

$$\|v_j\| \leq 2^{(i-1)/2} \|v_i^*\|, \text{ per qualsevol } 1 \leq j \leq i \leq n. \tag{4.2}$$

Finalment, el primer vector de la base LLL reduïda satisfà:

$$\|v_1\| \leq 2^{(n-1)/4} |\det L|^{1/n}, \|v_1\| \leq 2^{(n-1)/2} \min_{0 \neq v \in L} \|v\|. \tag{4.3}$$

Demostració. Comencem veient que la condició de Lovász i la condició $|\mu_{i,i-1}| \leq \frac{1}{2}$ impliquen que

$$\|v_i^*\|^2 \geq \left(\frac{3}{4} - \mu_{i,i-1}^2\right) \|v_{i-1}^*\| \geq \frac{1}{2} \|v_{i-1}^*\|.$$

Aplicant successivament aquesta desigualtat, arribem a la conclusió que:

$$\|v_j^*\|^2 \leq 2^{i-j} \|v_i^*\|^2.$$

Ara, observem la següent seqüència d'igualtats i desigualtats:

$$\|v_i\|2 = \|v_i^*\| + \sum_{j=1}^{i-1} \mu_{i,j} \|v_j^*\|^2 \leq \|v_i^*\|^2 + \sum_{j=1}^{i-1} \frac{1}{4} \|v_j^*\|^2$$

$$\leq \|v_i^*\|^2 + \sum_{j=1}^{i-1} 2^{i-j-2} \|v_i^*\|^2 = \frac{1 + 2^{i-1}}{2} \|v_i^*\|^2 \leq 2^{i-1} \|v_i^*\|^2.$$

A continuació, multiplicant $\|v_i\|^2$ per ell mateix per $1 \leq i \leq n$ ens porta a:

$$\prod_{i=1}^{n} \|v_i\|^2 \leq \prod_{i=1}^{n} 2^{i-1} \|v_i^*\|^2 = 2^{n(n-1)/2} \prod_{i=1}^{n} \|v_i^*\|^2 = 2^{n(n-1)/2} (\det(L))^2.$$

Agafant les arrels quadrades, queda demostrat que

$$\prod_{i=1}^{n} \|v_i\| \leq 2^{n(n-1)/4} \det(L),$$

Finalment, agafant les arrels n-èssimes, ens dona la condició que buscàvem per al vector inicial de la base LLL reduïda.

A continuació, sigui $v \in L$ un vector del reticle no nul. Escrivim $v = \sum_{j=1}^{i} a_j v_j = \sum_{j=1}^{i} b_j v_j^*$, on $a_i \neq 0$, $a_1, \ldots, a_i$ són enters, $b_1, \ldots, b_i$ són reals i $|a_i| \geq 1$. Per construcció, per qualsevol k, sabem que els vectors $v_1^*, \ldots, v_k^*$ són ortogonals dos a dos i que generen el mateix espai que els vectors $v_1, \ldots, v_n$. Per tant,

$$v \cdot v_i^* = a_i v_i \cdot v_i^* = b_i v_i^* \cdot v_i^* \text{ i } v_i \cdot v_i^* = v_i^* \cdot v_i^*.$$

D'aquesta manera, podem concloure que $a_i = b_i$. De fet, $|b_i| = |a_i| \geq 1$. Utilitzant la segona propietat del teorema amb $j = 1$, obtenim

$$\|v\|^2 = \sum_{j=1}^{i} b_j^* \|v_j^*\|^2 \geq b_i^2 \|v_i^*\|^2 \geq \|v_i^*\|^2 \geq 2^{-(i-1)} \|v_1\|^2 \geq 2^{-(n-1)} \|v_1\|^2.$$

Finalment, agafant arrels quadrades, obtenim la segona estimació de les condicions del vector inicial de la base LLL reduïda. □

Esquema LLL

- Agafem una base $v_1, \ldots, v_n$ del reticle L
- Fixem $k = 2$
- Fixem $v_1^* = v_1$
- Mentre $k \leq n$
- Mentre $j = 1, 2, \ldots k-1$
- Fixem $v_k = v_k - \lfloor \mu_{k,j} \rceil v_j^*$
- Acaba el bucle de les j
- *Si* $\|v_k^*\|^2 \geq \left(\frac{3}{4} - \mu_{k,k-1}^2\right) \|v_{k-1}^*\|^2$
- Fixem $k = k + 1$
- *Si no*
- Intercanvia v_{k-1} i v_k
- Fixem $k = \max(k-1, 2)$
- Acabem el bucle del *Si*
- Acabem el bucle de les k
- Retorna la base LLL reduïda $v_1, \ldots, v_n$.

Observació 4.4. A cada passa de l'algorisme, $v_1^*, \ldots, v_k^*$ és el conjunt de vectors que s'obtenen aplicant Gram-Schmidt als vectors $v_1, \ldots, v_n$, i $\mu_{i,j} = (v_i v_j)/\|v_j^*\|^2$.

Teorema 4.5. ***(Algorisme LLL)*** *Sigui $v_1, \ldots, v_n$ una base del reticle L. L'algorisme LLL acaba en un nombre finit de passos, en temps polinomial i retorna una base LLL reduïda de L.*

Demostració. Consultar al llibre [8]. □

Observació 4.6. El problema o complicació principal d'aquest algorisme, és que es compleixin les condicions de mida i de Lovász. A més a més, si s'intenta aplicar el LLL en un reticle enter utilitzant valors exactes, els càlculs involucraran nombres molt grossos amb els que serà difícil treballar.

5 Criptosistemes basats en reticles

5.1 Introducció

A mitjans dels anys 90, es van introduir varis criptosistemes basats en el problema del vector més curt i el problema del vector més proper. Un dels més importants va ser el criptosistema GGH de Goldreich, Goldwasser i Halevi, el qual explicarem a continuació.

Els motius d'introduir aquests criptosistemes, van ser principalment dos. Primer, és interessant tenir criptosistemes basats en diferents problemes matemàtics difícils per millorar la seguretat. Segon, els criptosistemes basats en reticles utilitzen menys operacions, comptant xifratge i desxifratge, que els basats en la factorització o logaritmes discrets, com podrien ser el RSA o el ElGamal entre d'altres. Per tant, els criptosistemes basats en reticles són més ràpids.

Tot i això, la implementació d'aquests criptosistemes ha sigut molt poca comparada amb la resta de criptosistemes. La raó principal és que la seguretat dels criptosistemes basats en reticles encara s'està estudiant.

Actualment, l'evolució que estan tenint els ordinadors quàntics, suposa la fi imminent dels criptosistemes basats en la factorització o logaritmes discrets esmentats abans. És per això que s'està fent molta recerca sobre criptosistemes resistents a atacs quàntics. De fet, el 2016, el NIST (National Institute of Standars and Technology), va llençar una competició i es van entregar 82 propostes de criptosistemes postquàntics. D'aquestes, van quedar quatre finalistes de les quals tres es basaven en matemàtica de reticles. Per tant, criptosistemes basats en reticles, semblants al GGH, podrien ser el futur pròxim de la criptografia.

A continuació, ens centrarem en el criptosistema GGH i en explicar el procés de creació de claus, procés de xifratge i desxifratge i la prova de la seva seguretat.

5.2 Criptosistema Goldreich, Goldwasser i Halevi (GGH)

5.2.1 Introducció

Aquest criptosistema va ser publicat el 1997. Al principi, els creadors van conjecturar que per dimensions més grans que 300, el problema del vector més proper era impossible de resoldre, problema en el qual es basa el criptosistema.

Després de ser publicat, es van presentar diversos atacs al criptosistema que portaven a incrementar la dimensió per tal de garantir la seguretat d'aquest. Per exemple, el 1999 Phong Nguyen, Han, Daewan, Kim Myung Han i Yeom Yongjin van presentar diversos atacs al criptosistema que van acabar demostrant que en certes ocasions, el criptosistema no era segur fins a dimensions tan grans com 1000. El problema principal del GGH és que com més s'incrementa la dimensió per tal de garantir la seguretat, menys eficient es torna, ja que les claus es tornen quasi impracticables.

També, la introducció d'algorismes de reducció de reticles com el LLL, suposa una amenaça contra el GGH. Un cop més, només en dimensions molt elevades aquests algorismes no serien perillosos, tot i que, en contraposició, com ja hem dit abans, el criptosistema deixa de ser eficient.

A continuació, farem una descripció detallada d'aquest criptosistema. Per facilitar el

procés de descripció, utilitzarem els termes "base bona" i "base dolenta" per referir-nos a una base bastant ortogonal i a una molt poc ortogonal respectivament. Finalment, també utilitzarem els noms Alice, Bob i Eve per referir-nos a la persona que construeix una clau pública i una privada i rep missatges els quals pot desxifrar, la persona que envia un missatge i la persona que intercepta i intenta desxifrar el missatge respectivament.

5.2.2 Descripció del criptosistema

Construcció de claus

Per començar, l'Alice escull un conjunt de vectors linealment independents

$$v_1, \ldots, v_n \in \mathbb{Z}^n$$

que siguin bastant ortogonals entre ells. Per construir aquests n vectors amb aquestes dues propietats, l'Alice pot escollir un paràmetre d petit i agafar les coordenades dels vectors de forma aleatòria entre $-d$ i d. D'aquesta manera, és molt probable que els vectors resultants siguin linealment independents. Tot i això, va bé comprovar-ho. Finalment, amb el quocient de Hadamard, l'Alice pot comprovar que els vectors escollits siguin prou ortogonals. Ha de veure que el quocient sigui proper a 1.

Ara, l'Alice ja té la seva **clau privada**, que seran els vectors $v_1, \ldots, v_n$.

A continuació, denotem V com la matriu que té per files les coordenades de la base $v_1, \ldots, v_n$. I denotem com a L el reticle generat per la mateixa base.

Finalment, per generar la clau pública, l'Alice escollirà una matriu U $n \times n$ amb coeficients enters i $\det(U) = \pm 1$. Una manera d'obtenir U, seria multiplicant un gran nombre de matrius elementals aleatòries. Quan tenim U, la multipliquem per V i obtenim una matriu $W = UV$, que serà una nova base del mateix reticle L, però molt poc ortogonal. Calculant el quocient de Hadamard i veient que és proper a 0, podem assegurar la poca ortogonalitat.

Ara, l'Alice ja té la seva **clau pública**, que seran els vectors fila de la matriu W, $w_1, \ldots, w_n$.

Procés de xifratge

Ara, el Bob vol enviar un missatge a l'Alice que estigui encriptat. Per fer-ho, utilitzarà la seva clau pública.

El Bob, escull el seu missatge, que serà un vector m de dimensió n de coordenades enteres. També escollirà un vector r aleatori amb valors molt petits i enters. Aquest vector es diu clau efímera o vector pertorbació.

Aleshores, el Bob calcularà el vector e, que serà el seu **missatge xifrat**, d'aquesta manera:

$$e = mW + r = \sum_{i=1}^{n} m_i w_i + r.$$

Notem que e no és un punt del reticle per la pertorbació r, però com que r és petit, és el punt més proper a mW, que si que és del reticle.

Procés de desxifratge

L'Alice rebrà e i el desxifrarà utilitzant l'algorisme de Babai amb la seva clau privada $v_1, \ldots, v_n$.

L'algorime de Babai, com que r és petit i $v_1, \ldots, v_n$ és una "bona base", li retornarà el vector $v = mW$, que és el vector del reticle més proper a e.

Finalment, l'Alice ha de multiplicar v per la matriu inversa de W per recuperar el missatge original m.

Prova de seguretat

Per últim, imaginem que l'Eve intercepta el missatge e que el Bob ha enviat a l'Alice.

L'Eve només coneix la clau pública de l'Alice, per tant, si l'Eve aplica l'algorisme de Babai amb la base $w_1, \ldots, w_n$, obtindrà un punt del reticle m' que estarà molt allunyat del punt m original. Això és a causa del fet que la clau pública és una "base dolenta", per tant, molt poc ortogonal.

5.2.3 Esquema GGH

A continuació, presentem un esquema del criptosistema.

Construcció de claus

- Escollir una "bona base" $v_1, \ldots, v_n$ que serà la clau privada.
- Denotar V com la matriu que té per files $v_1, \ldots, v_n$.
- Escollir una matriu U entera amb $\det(U) = \pm 1$.
- Calcular la matriu $W = UV$. Les seves files $w_1, \ldots, w_n$ seran la clau pública.

Procés de xifratge

- Escollir el vector m petit que es vol enviar.
- Escollir un vector r aleatori amb valors molt petits.
- Utilitzar la clau pública per calcular $e = mW + r$, el missatge xifrat.
- Enviar a l'Alice el missatge e.

Procés de desxifratge

- Utilitzar l'algorisme de Babai per obtenir $v = mW \in L$.
- Calcular vW^{-1} per obtenir m.

5.2.4 Exemple GGH

A continuació, farem un exemple de com funciona el criptosistema amb dimensió quatre.

Construcció de claus

Generem la clau privada de l'Alice amb els vectors

$$v_1 = (0, -3, 2, 1),\ v_2 = (3, -1, 0, -2),\ v_3 = (2, 0, 0, 3),\ v_4 = (-3, -2, -1, 0).$$

Per veure que els podem considerar una "bona base", cal comprovar que són bastant ortogonals. Per fer-ho, calcularem el quocient de Hadamard.

El reticle L de dimensió 4 generat pels vectors v_1, v_2, v_3, v_4 té determinant $\det(L) = 111$. Aleshores, el quocient de Hadamard és

$$\mathcal{H}(v_1, v_2, v_3, v_4) = \left(\frac{\det(L)}{\|v_1\|\|v_2\|\|v_3\|\|v_4\|}\right)^{1/4} \approx 0.875568.$$

Com que el quocient de Hadamard ens dona proper a 1, podem considerar v_1, v_2, v_3, v_4 la clau privada de l'Alice.

Considerem la matriu V com la matriu que té per files els vectors de la base:

$$V = \begin{pmatrix} 0 & -3 & 2 & 1 \\ 3 & -1 & 0 & -2 \\ 2 & 0 & 0 & 3 \\ -3 & -2 & -1 & 0 \end{pmatrix}.$$

Ara, volem construir la clau pública de l'Alice multiplicant aquesta matriu (que representa la seva clau privada) per una matriu U amb $\det(U) = \pm 1$. Veiem que la matriu

$$U = \begin{pmatrix} 5313 & 2572 & 8 & 1252 \\ 2580 & 1249 & 4 & 608 \\ 628 & 304 & 1 & 148 \\ 100 & 50 & 6 & 25 \end{pmatrix},$$

té $\det(U) = 1$. Per tant, calculem la matriu

$$W = U \cdot V = \begin{pmatrix} 3976 & -21015 & 9374 & 193 \\ 1931 & -10205 & 4552 & 94 \\ 470 & -2484 & 1108 & 23 \\ 87 & -400 & 175 & 18 \end{pmatrix}.$$

Les seves files

$$w_1 = (3976, -21015, 9374, 193),\ w_2 = (1931, -10205, 4552, 94),$$
$$w_3 = (470, -2484, 1108, 23),\ w_4 = (87, -400, 175, 18),$$

també generen L.

Podem comprovar amb el quocient de Hadamard que aquesta base és una "base dolenta".

$$\mathcal{H}(w_1, w_2, w_3, w_4) = \left(\frac{\det(L)}{\|w_1\|\|w_2\|\|w_3\|\|w_4\|}\right)^{1/4} \approx 0,0007640584.$$

Com que el quocient de Hadamard ens dona proper a 0, podem considerar w_1, w_2, w_3, w_4 la clau pública de l'Alice.

Procés de xifratge

Ara, el Bob vol enviar a l'Alice el missatge $m = (63, -25, -32, 46)$ utilitzant la pertorbació $r = (1, 1, 0, -2)$.

Calculem el missatge xifrat e.

$$e = mW + r = (63, -25, -32, 46) \begin{pmatrix} 3976 & -21015 & 9374 & 193 \\ 1931 & -10205 & 4552 & 94 \\ 470 & -2484 & 1108 & 23 \\ 87 & -400 & 175 & 18 \end{pmatrix} + (1, 1, 0, -2) =$$
$$= (191176, -1007731, 449356, 9899).$$

El Bob enviarà e a l'Alice.

Procés de desxifratge

L'Alice utilitza l'algorisme de Babai per desencriptar el missatge.

Primer, expressa e com a combinació lineal de la base privada amb coeficients reals.

$$e \approx 254722,8198v_1 + 123383,2613v_2 + 647,5676v_3 + 60089,6396v_4.$$

A continuació, arrodoneix els coeficients a l'enter més pròxim i troba un vector v del reticle proper a e.

$$v = 254723v_1 + 123383v_2 + 648v_3 + 60090v_4 = (191175, -1007732, 449356, 9901).$$

Ara, recupera m expressant v com a combinació lineal de la base pública, que és el mateix que multiplicar per W^{-1}.

$$m = vW^{-1} = (63, -25, -32, 46)$$

Prova de seguretat

Suposem que l'Eve intercepta i intenta desxifrar el missatge del Bob utilitzant l'algorisme de Babai, però l'Eve només disposa de la clau pública.

Primer, expressa e com a combinació lineal de la base pública amb coeficients reals.

$$e \approx -26,1532w_1 + 159,6216w_2 - 35,6396w_3 + 42,3243w_4.$$

A continuació, arrodoneix els coeficients a l'enter més pròxim i troba un vector v' del reticle.

$$v' = -26w_1 + 160w_2 - 36w_3 + 42w_4 = (192318, -1013786, 452058, 9950).$$

Ara, fa l'últim pas per recuperar el missatge, que és expressar v com a combinació lineal de la base pública.

$$m = v'W^{-1} = (-26, 160, -36, 42)$$

Veiem que no ha obtingut el missatge m original. Això és degut a aplicar l'algorisme de Babai amb una "base dolenta". Fixem-nos en l'error que es produeix quan hem utilitzat la clau privada i quan hem utilitzat la pública.

$$\|e - v\| = \|(1, 1, 0, -2)\| \approx 2,5.$$

$$\|e - v'\| = \|(-1142, 6055, -2702, -51)\| \approx 6728,34.$$

Com ja sabíem, l'error és molt més gran quan hem aplicat Babai amb una base molt poc ortogonal.

Com ja hem comentat, l'algorisme GGH no és prou segur, ja que existeixen algorismes, com els que hem vist en seccions anteriors, capaços de trobar bases prou ortogonals a través d'una clau pública i això afecta la seguretat del criptosistema.

5.2.5 Exemple LLL

A continuació, seguint amb l'exemple que acabem de fer, provarem de trencar el criptosistema GGH amb l'algorisme LLL. Per tant, veurem si tenint només la clau pública, podem trobar una base prou ortogonal amb l'algorisme LLL, amb la qual recuperar el missatge original utilitzant l'algorisme de Babai.

La clau pública de l'Alice és

$$w_1 = (3976, -21015, 9374, 193),\ w_2 = (1931, -10205, 4552, 94),$$
$$w_3 = (470, -2484, 1108, 23),\ w_4 = (87, -400, 175, 18).$$

Ara, el Bob vol enviar a l'Alice el missatge $m = (154, -200, 97, -45)$. Com abans, l'encripta utilitzant la base pública i el vector pertorbació $r = (1, -1, 0, 0)$ i envia el missatge

$$e = (267780, -1418259, 632797, 12343).$$

A continuació, l'Eve intercepta el missatge e i en comptes d'aplicar directament l'algorisme de Babai amb la clau pública, que ja hem vist abans que retorna un missatge diferent de l'original, utilitza primer l'algorisme LLL.

L'algorisme li retorna la base

$$u_1 = (-2, 0, 0, -3), u_2 = (0, -3, -1, -2), u_3 = (2, 0, -3, 0), u_4 = (-3, -2, -1, 0).$$

Amb el quocient de Hadamard, podem comprovar que realment es tracta d'una base bastant ortogonal. En efecte,

$$\mathcal{H}(u_1, u_2, u_3, u_4) = \left(\frac{\det(L)}{\|u_1\|\|u_2\|\|u_3\|\|u_4\|}\right)^{1/4} \approx 0,61,$$

és bastant proper a 1 i veiem que ha millorat molt respecta la base W.

A continuació, l'Eve aplica l'algorisme de Babai amb aquesta base i troba el vector

$$u = (267779, -1418258, 632797, 12343).$$

Finalment, expressa u en funció de la base pública i obté

$$u = 154w_1 - 200w_2 + 97w_3 - 45w_4.$$

D'aquesta manera, l'algorisme LLL juntament amb el de Babai, ha permès a l'Eve obtenir el missatge original $m = (154, -200, 97, -45)$ disposant només de la clau pública.

5.3 Programa criptosistema GGH

Per poder experimentar amb el criptosistema i fent ús del software SageMath, hem creat un programa que executa tot el procés del criptosistema.

Als annexos hi ha el codi, però en aquest apartat fem una descripció de les variables utilitzades i l'estructura del programa.

1. Decidim si volem introduir manualment una clau pública, una privada i el missatge a encriptar o si volem que ens creï una situació en què les claus siguin aleatòries.

   Si volem les claus aleatòries el codi segueix els següents passos:

2. Donem el paràmetre n, la dimensió i d un enter no molt gran.

3. Es generen n vectors $(v_1, \ldots, v_n)$ aleatoris de coeficients enters entre $-d$ i d.

4. Es calcula el quocient de Hadamard H d'aquests n vectors. Si H és proper a 1 (>0,7) considerem la base bona. Si és més petit, es creen uns nous vectors.

5. Donem num el nombre de matrius elementals que volem utilitzar per crear la matriu U.

6. Es generen num matrius elementals i es fa el producte de totes elles per obtenir U.

7. Es comprova que $\det(U) = \pm 1$

8. Es calcula la matriu $W = UV$ i denotem com a $w_1, \ldots, w_n$ els seus vectors fila.

9. Es calcula el quocient de Hadamard H' d'aquests n vectors. Si H' és proper a 0 (<0,1) considerem la base dolenta. Si és més gran, es crea una nova matriu U i, per tant, una nova matriu W.

10. Donem el missatge m que volem encriptar, un vector de n coordenades enteres.

11. Es genera un vector r de pertorbació de n coordenades enteres petites entre -2 i 2.

12. Es calcula $e = mW + r$.

13. Es calcula $(t_1, \ldots, t_n) = eV^{-1}$.

14. Es calcula $v = (\lfloor t_1 \rceil, \ldots, \lfloor t_n \rceil)V$.

15. Es calcula $m = vW^{-1}$.

    Si haguéssim preferit donar nosaltres les claus, hauríem introduït n, V, W. El programa ens calcula els quocients de Hadamard de cada base i commprova que siguin adequades. Després introduïm m i fa el mateix procés de xifratge i desxifratge.

6 Didàctica

6.1 Antecedents didàctics

Per plantejar i donar sentit a l'activitat didàctica basada en el criptosistema GGH, ens hem basat en el llibre *tres professors de matemàtiques* [3], escrit pel Claudi Alsina, l'Anton Aubanell i la Carme Burgués.

En aquest llibre, hi ha una secció que se centra en la idea de la matematització i la modelització dins les aules. La matematització és el procés de treballar la realitat a través d'idees i conceptes matemàtics. La modelització es caracteritza per l'atenció al principi d'un procés. Anar des del problema fora del món matemàtic a la seva formulació matemàtica. A través d'això, es dona importància al món extern i al matemàtic, obtenint resultats matemàticament correctes i raonables en el context del món real.

Com crear contextos adequats per poder ensenyar matematitzant?...
Necessitem problemes metemàtics que tinguin
un context significatiu per als estudiants.
Hans Freudental

La realitat de debò, la de casa, la de la vida, la del país
és el gran material didàctic a explorar!
Tres professors de matemàtiques

La criptografia i, en concret, la postquàntica, és un tema que està present i agafant forma actualment. Contextualitzant els alumnes i endinsant-los en el problema actual que hi ha amb la criptografia, ens porta a desenvolupar una activitat sobre una realitat i a poder-la entendre. Tot això, mentre introduïm i donem una altra visió a continguts que estudien durant el curs.

En aquest llibre, també es parla sobre les activitats contextualitzades que es fan a l'aula de matemàtiques.

Sovint, per contextualitzar, s'utilitzen realitats falsejades,
manipulades, inusuals, caducades o inventades.
Tres professors de matemàtiques

Aquesta activitat, s'allunya molt d'això, ja que es tracta bàsicament d'entendre un problema real amb un fonament matemàtic, que, tot i que es faci en dimensions petites, segueix tenint el mateix funcionament.

Henry O. Pollak, en el llibre *Why Numbers Count: Quantitative Literacy* [7], dona una descripció detallada de la modelització matemàtica i ens descriu els vuit passos que s'han de donar en aquesta. A continuació, fem un resum d'aquests passos:

- Identifiquem alguna cosa al món real que volem conèixer.
- Identifiquem conceptes clau en la situació del món real.
- Decidim què considerem i què ignorem sobre els objectes.
- Fem el model matemàtic.

- Identifiquem els apartats de la matemàtica que poden ser rellevants pel model.
- Fem servir mètodes matemàtics i idees per obtenir resultats.
- Prenem els resultats i els traslladem al principi.
- Verifiquem la realitat i veiem si els resultats són raonables.

Els autors del llibre, a través d'aquests passos i aquesta descripció, ens proposen una llarga llista de tipus de problemes que poden ser adequats per treballar els processos de modelització o matematització. Entre aquests problemes, n'hi ha de modelització funcional, discreta, algebraica, geomètrica i estadística. Dins del bloc de modelització algebraica, esmenten problemes del tipus:

- Possibilitats computacionals.
- Encriptació de missatges.
- Geometria computacional.
- Codis lineals.

Veiem, que aquestes descripcions, encaixen bé amb el tipus d'activitat que s'ha realitzat en aquest treball.

A vegades, hem sentit alumnes que preguntaven:
≪ I això per a què serveix? ≫
Com posant paraules a la necessitat de veure aplicacions.
Tres professors de matemàtiques

Aquesta activitat, ens pot fer veure una aplicació útil i present a la vida quotidiana de la geometria. Entendre les matemàtiques que hi ha darrere d'una simple contrasenya i veure la relació estreta que té amb el coneixement que estan adquirint, pot provocar, com a mínim, una estimació interessada cap al tema. Com diuen els autors del llibre.

Estimar ara i avui els avantatges que donen les matemàtiques és important.
I integrar-hi la tecnologia també ho és.
Tres professors de matemàtiques

Aquesta activitat ens dona una perspectiva que les matemàtiques poden ser clau en temes d'impacte social o en processos tecnològics o científics que formen part del dia a dia. I que, a més a més, a través d'elles hi ha actualitzacions i avenços.

6.2 Fitxa de l'activitat

Objectius

- Entendre què és la criptografia i el problema amb l'actual sistema.
- Entendre què és un reticle en el pla.
- Connectar el criptosistema GGH amb els coneixements que tenen de vectors.
- Crear la seva pròpia clau pública i privada.
- Plantejar conjectures.

Descripció de la proposta

Aquesta activitat consisteix a conèixer el concepte de reticle en el pla, trobar una base d'aquest i experimentar amb un criptosistema.

Comencem amb una introducció sobre que és la criptografia i context històric, parlem breument del sistema RSA. Expliquem el problema actual amb els ordinadors quàntics i que, per tant, necessitem un nou sistema.

Comencem a explicar el sistema GGH, sense preàmbuls, ja aniran sortint les conclusions i conceptes de geometria. Amb el suport del GeoGebra, agafem dos vectors (ortogonals), i visualitzem el reticle que generen. Aquí hi entren els conceptes de base, combinació lineal i ortogonalitat.

Ara, reflexionem sobre aquest reticle, si uns altres dos vectors el podrien generar, i veiem que sí. Aquí els guiem per distingir entre dos generadors ortogonals i dos que no ho siguin. A continuació, fem l'esquema Alice-Bob-Eve i reflexionem sobre quina serà la clau pública, la privada i com enviarem un missatge, un punt del reticle amb "soroll".

Finalment, farem la part pràctica. Els alumnes necessitaran cada un la seva tauleta amb el GeoGebra. Hauran de crear la seva pròpia clau pública i la privada a través de la creació d'un reticle i, per tant, l'experimentació amb el GeoGebra. Quan les tinguin fetes, farem un joc de rol. Cada alumne haurà de ser l'Alice, el Bob i l'Eve. Per fer el joc, no podràn tenir suport tecnològic, ja que si el tinguessin, com que estem treballant en el pla i no en dimensions grans, els hi seria fàcil desencriptar un missatge com a Eve. En canvi, sense el suport, veuran que no poden i que obtenen un missatge diferent de l'original.

Aspectes didàctics i metodològics

L'activitat està pensada per fer amb tot el grup de forma cooperativa. La primera sessió de dues hores serà de caràcter teòric i introductori. Aquí es demanarà intervencions per part dels alumnes en veu alta. La segona sessió, també de dues hores, serà de caràcter pràctic. Cada alumne treballarà amb la seva tauleta i es posaran en comú reflexions i conclusions.

Recursos emprats

- Una tauleta per cada alumne per utilitzar el GeoGebra en línia.

- Projector de l'aula.
- Malla de reixa extensible.
- Pissarra.
- Fitxa per l'alumnat.

Continguts i processos que es treballen de forma destacada

- Vectors en el pla.
- Combinació lineal de dos vectors amb coeficients enters.
- Vectors linealment independents i concepte de base.
- Producte escalar de dos vectors.
- Base ortogonal.
- Reticle en el pla.
- Construcció de dues bases que generin el mateix reticle.
- Esquema bàsic d'un criptosistema.

Competències

- Traduir un problema a llenguatge matemàtic o a una representació matemàtica utilitzant variables, símbols i models adequats.
- Generar preguntes de caràcter matemàtic i plantejar problemes.
- Identificar les matemátiques implicades en situacions properes i cercar situacions que es puguin relacionar amb idees matemàtiques concretes.
- Emprar la comunicació i el treball col·laboratiu per compartir i construir coneixement a partir d'idees matemàtiques.
- Seleccionar i usar tecnologies diverses per gestionar i mostrar informació, i visualitzar i estructurar idees o processos matemàtics.

Alumnat a qui s'adreça especialment

L'activitat està pensada per alumnes de 1r de Batxillerat, tot i que també pot ser adequada per 2n de Batxillerat, ja que podria incloure més conceptes relacionats amb matrius o incrementar la dimensió dels reticles.

Interdisciplinarietat, transversalitat, relacions amb l'entorn

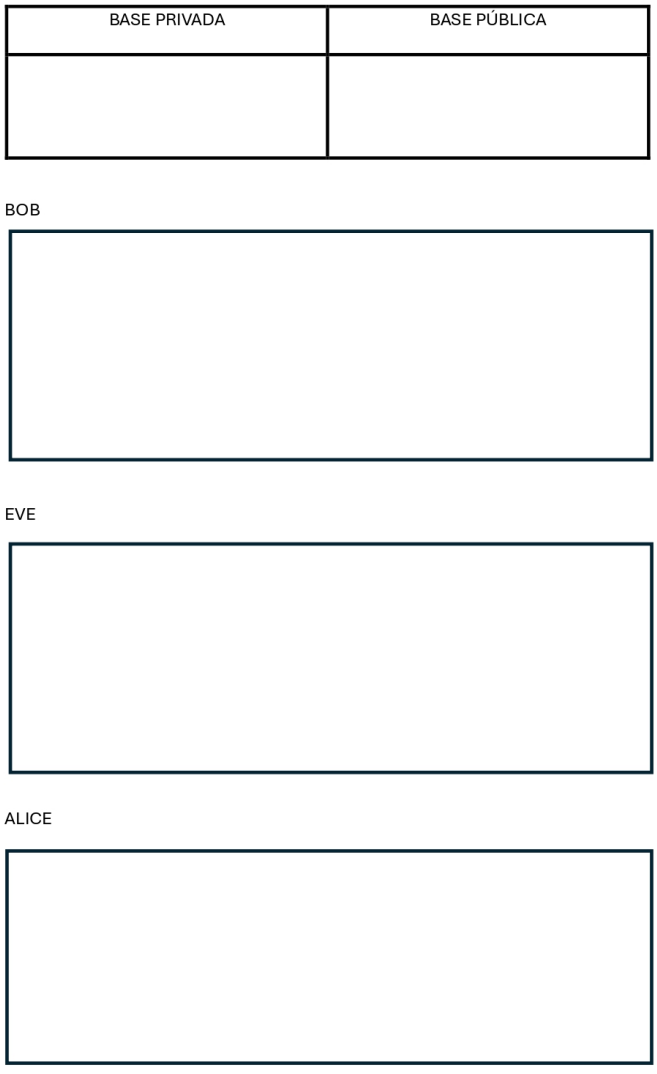
Aquesta activitat és rica perquè contextualitza els coneixements de geometria del curs amb un problema que està passant actualment. Es dona també un context històric tot parlant de criptografia i dels seus inicis. Veiem que les matemàtiques intervenen en temes que s'utilitzen en el nostre dia a dia.

6.3 Fitxa pel professorat

Es deixa com a annex un document amb un resum dels coneixements bàsics sobre el criptosistema GGH que hauria de saber el docent per portar l'activitat a l'aula. També s'hi inclou el suport de GeoGebra que s'ha utilitzat.

6.4 Fitxa per l'alumnat

Volem que el treball que facin sigui col·laboratiu. Durant les primeres dues hores, es fa una introducció als reticles tot repassant de forma conjunta els conceptes que utilitzem de geometria (que ja han vist a matemàtiques). Aquí volem participació activa i en veu alta dels alumnes. És per això que els alumnes no necessiten el suport d'una fitxa. Finalment, la sessió pràctica comença amb la creació individual d'una base pública i una de privada, seguida d'un joc de rol entre ells on seràn l'Alice, el Bob o l'Eve. En aquesta part, podem portar la següent plantilla per després jugar.



6.5 Implementació de l'activitat

L'escola Daina-Isard em va obrir les portes per poder experimentar amb l'activitat que havia construït. Vaig poder estar amb els alumnes de 1r de batxillerat tecnològic durant dues sessions de dues hores cada una.

La primera sessió va ser el 29 d'abril. Aquell dia, vam començar parlant de criptografia, dels seus inicis i de la seva evolució al llarg dels anys fins a arribar a l'actualitat. Vam parlar d'ordinadors quàntics i del que suposava la seva evolució.

Alguns dels alumnes havien sentit a parlar d'ordinadors quàntics, dos d'ells havien llegit sobre els nous criptosistemes que s'estan buscant i la majoria havia sentit a parlar de criptografia en algun moment, sobretot del criptosistema RSA. Que tinguessin un cert context va ser positiu per tenir un debat entre tots sobre el tema.

A continuació, vam anar construint junts el criptosistema GGH, amb el GeoGebra davant. Mentre construíem i enteníem el criptosistema, vam aprendre què era un reticle i vam repassar conceptes que havien fet feia poc a matemàtiques.

Figura 5: Primera sessió del taller a l'escola Daina-Isard.

El següent dia que ens vam veure, va ser el 22 de maig. Va haver-hi un espai de temps bastant gran entre les dues sessions, però vam mantenir un canal obert i alguns d'ells em van contactar durant aquells dies demanant informació complementària, com per exemple, informació del RSA.

Com, he dit, el 22 de maig vam fer les últimes dues hores. Durant aquesta part, els alumnes van recordar tot el que havíem après l'últim dia i de seguida ens vam endinsar en el món del GeoGebra. L'havien fet servir poc, així que va ser una activitat significativa per ells. Primer vam anar construint de forma individual els reticles de cada un.

Finalment, amb l'ajuda del meu GeoGebra, que inclou els valors dels coeficients de Hadamard, cada un va escollir les seves claus i vam començar amb el joc de rol, on cada un d'ells passava per cada paper: Alice, Bob o Eve.

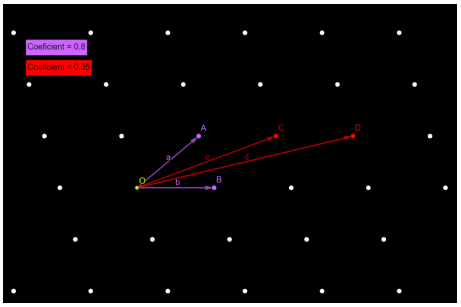


Figura 6: GeoGebra 2 dimensions.

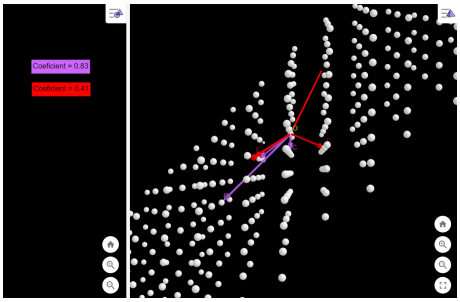


Figura 7: GeoGebra 3 dimensions.

Figura 8: Alumnes experimentant amb el GeoGebra.

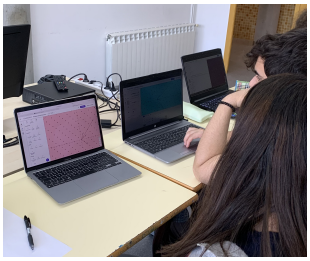


Figura 9: Alumnes creant els seus propis reticles.

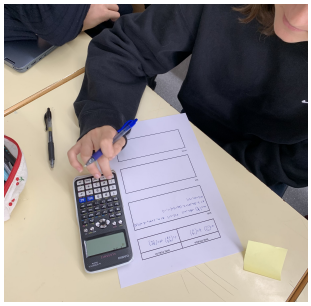


Figura 10: Alumnes xifrant i desxifrant missatges.

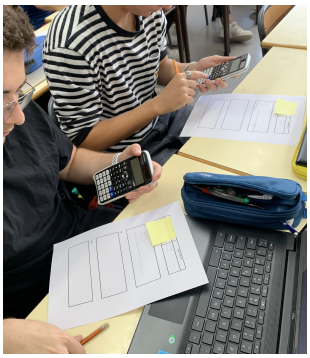


Figura 11: Alumnes xifrant i desxifrant missatges.

La reacció a l'activitat per part dels alumnes va ser molt positiva. Els va interessar molt que fos un tema d'actualitat. Per altra banda, molts d'ells van valorar posar en pràctica d'una manera intuïtiva i contextualitzada els coneixements de geometria que havien adquirit feia poc. No s'imaginaven la importància que podia tenir la combinació lineal, les bases o l'ortogonalitat de vectors. També, utilitzar el GeoGebra els va agradar molt, i fins i tot un alumne va utilitzar Python mentre fèiem l'activitat. Això em va cridar molt l'atenció i a l'apartat següent de propostes de millora ho comentaré.

6.6 Propostes de millora o ampliació

Havent realitzat ja l'activitat, puc dir que la recomanaria sobretot per estudiants de 2n de batxillerat. Poder introduir de forma més natural el quocient de Hadamard, ja que han treballat amb matrius o poder incrementar les dimensions, hagués fet que l'activitat fos més significativa i adaptada pels alumnes.

També, si es disposa de més temps, recomanaria explorar altres criptosistemes. El RSA, que és el vigent, els interessa molt i de fet molts d'ells em van demanar que al principi de la segona sessió fes un apunt d'aquest.

Un altre tema a explorar i a introduir a l'activitat, és la programació, com he comentat a la secció anterior. Un alumne va utilitzar Python mentre experimentàvem amb el criptosistema per poder fer les operacions més ràpides i poder experimentar amb diferents missatges i bases. Això em va cridar l'atenció i em va fer pensar que en una escola on es treballi la programació o fins i tot si no és així, incorporar-la a l'activitat és una gran idea i una gran oportunitat. Treballant amb claus tan curtes, sovint el criptosistema no retorna exactament el missatge enviat, ja que depèn del vector pertorbació que s'utilitzi pot no sortir bé. Si es treballa amb un programa, es pot experimentar i raonar amb aquest fet. De nou, això ens faria tenir una activitat contextualitzada que utilitza matemàtiques de l'aula i que, a més a més utilitzaríem recursos computacionals.

Finalment, també es podria utilitzar aquesta activitat per raonar i explorar el pensament abstracte amb els alumnes a través de les dimensions amb les quals es duu a terme el criptosistema a la realitat. Alguns dels alumnes, al principi, van qüestionar el criptosistema, ja que l'estaven veient en dues dimensions i veien molt fàcil trobar el punt més proper, disposessin de la base que fos. És per això que vaig crear el GeoGebra amb tres dimensions, perquè de seguida, només incrementant una dimensió, van poder observar com es complicava el problema. Tot i això, es pot raonar més de com incrementen de forma exponencial la quantitat de punts en un cert tros del reticle a mesura que incrementem les dimensions.

7 Conclusions

Conclusions matemàtiques

Hem pogut veure que el criptosistema GGH no ens ofereix una bona seguretat combinada amb eficiència, ja que en arribar a les dimensions on seria segur, les claus passen a ser massa grans i complicades de tractar. Tot i això, també hem pogut comprendre per què la nova forma de criptografia es basarà en matemàtica de reticles i els problemes computacionalment complexos que la sostenen. Per la banda matemàtica, ha sigut molt interessant estudiar un tema encara obert i en constant canvi. Durant el procés del treball, he pogut anar llegint discussions i algorismes que anaven sortint per trencar-ne d'altres i com es revisaven i se'ls hi anava donant forma. Serà interessant en un futur no molt llunyà, recuperar aquest treball i poder-lo completar amb la resolució definitiva al problema de la criptografia postquàntica.

Conclusions didàctiques

Pel que fa a la part didàctica, tot i que havia cursat l'assignatura de Didàctica de les Matemàtiques, fins aquest moment no havia experimentat les complicacions que et pots trobar en elaborar una activitat d'aquest tipus per l'aula. Aprendre a fer-te les preguntes adequades, posar-te en totes les situacions en què l'alumne es pot trobar i dominar i haver fet repetides vegades abans l'activitat són essencials abans de portar-la a l'aula.

D'altra banda, ha sigut molt bonic veure com es poden introduir temes i matemàtiques que no són convencionals a l'aula o que es creuen massa complexes. De fet, la conclusió que extrec d'aquesta experiència, és que amb un context i un apropament a temes reals, els alumnes assoleixen una comprensió i una satisfacció molt més gran a l'hora d'aprendre i experimentar amb les matemàtiques.

8 Apèndix A: Programa criptosistema GGH

Programa criptosistema GGH

May 31, 2024

[ ]:
```
from sage.all import *
```

Aquesta funció demana a l'usuari si vol introduir manualment la clau privada i pública (Si) o si vol que el programa les generi (No).

[ ]:
```
def input_user():
    user_input = input("Vols introduir les claus (Si) o calcular-les (No)? (Si/
 ↪No): ").strip().lower()

    if user_input == "si":
        return 1
    elif user_input == "no":
        return 2
    else:
        print("Has de respondre Si o No.")
        return input_user()
```

Aquesta funció demana un enter n que serà la dimensió.

[ ]:
```
def input_integer(prompt):
    while True:
        try:
            return int(input(prompt))
        except ValueError:
            print("Entrada no vàlida. Si us plau, introdueix un número enter.")
```

Si es volen introduir manualment les claus, es crida aqeusta funció, que comprova que les bases siguin adequades i les guarda en les matrus V i W.

[ ]:
```
def input_private_key(n):
    private = []
    for i in range(n):
        while True:
            try:
                vec = vector(ZZ, [int(x) for x in input(f"Introdueix el vector␣
 ↪de la fila {i+1} de la clau privada com una llista d'enters separats per␣
 ↪espais: ").split()])
```

```
                if len(vec) == n:
                    private.append(vec)
                    break
                else:
                    print(f"El vector ha de tenir {n} components.")
            except ValueError:
                print("Entrada no vàlida. Si us plau, introdueix números enters␣
↪separats per espais.")
    return matrix(private)

def input_public_key(n):
    public = []
    for i in range(n):
        while True:
            try:
                vec = vector(ZZ, [int(x) for x in input(f"Introdueix el vector␣
↪de la fila {i+1} de la clau pública com una llista d'enters separats per␣
↪espais: ").split()])
                if len(vec) == n:
                    public.append(vec)
                    break
                else:
                    print(f"El vector ha de tenir {n} components.")
            except ValueError:
                print("Entrada no vàlida. Si us plau, introdueix números enters␣
↪separats per espais.")
    return matrix(public)
```

Si es vol que el programa generi les claus, es criden les següents funcions.

Aquesta funció genera un vector v de dimensió n de coeficients enters aleatoris entre $-d$ i d.

[ ]:
```
def create_random_vectors(n, d):
    vectors = [vector(ZZ, [randint(-d, d) for _ in range(n)]) for _ in range(n)]
    if all(v.norm() != 0 for v in vectors):
        return vectors
    else:
        vectors = create_random_vectors(n,d)
        return vectors
```

Aquesta funció calcula el quacient de Hadamard d'n vectors $v_1, \dots, v_n$. Aquest quocient és $\mathcal{H}(\mathcal{B}) = \left(\frac{\det(L)}{\|v_1\| \cdots \|v_n\|}\right)^{1/n}$.

[ ]:
```
def hadamard_ratio(vectors):
    n = len(vectors)
    det_L = abs(matrix(vectors).determinant())
    norms_product = prod(v.norm() for v in vectors)
```

```
    return (det_L / norms_product)**(1/n)
```

Aquesta funció genera una matriu U $n \times n$ fent el producte de num matrius elementals.

[ ]:
```
def create_elementary_matrices(n, num):
    U = identity_matrix(ZZ, n)
    for i in range(num):
        d=0
        while d not in [-1,1]:
            K=identity_matrix(ZZ,n)
            operation_type = randint(1, 2)
            if operation_type == 1:
                # Intercanvi de files
                j = randint(0, n-1)
                i = randint(0, n-1)
                if n>1:
                    while i==j:
                        i = randint(0,n-1)
                K.swap_rows(j, i)
            elif operation_type == 2:
                # Suma d'una fila amb un múltiple d'una altre.
                j = randint(0, n-1)
                k = randint(0, n-1)
                if n>1:
                    while k == j:
                        k = randint(0, n-1)
                scalar = randint(0, 999999)  # un múltiple aleatori entre 1 y␣
 ↪999999.
                K[j] += scalar * K[k]
            d=det(K)
        U=U*K
    return U
```

Aquesta funció genera la clau privada. Crida n vegades la funció create_random_vectors per generar els vectors $v_1, \dots, v_n$, comprova amb la funció hadamard_ratio que el quocient de Hadamard d'aquests vectors sigui més gran que $0,7$ i genera la matriu V, que és la matriu que té per files els vectors $v_1, \dots, v_n$.

[ ]:
```
def private_key_calculation(n,d):
    while True:
        # Generem un vector de dimensió n i valors en rang +-d.
        vectors = create_random_vectors(n, d)
        # Comprovem que quocient de Hadamard sigui major a 0.7
        H = hadamard_ratio(vectors)
        print(f"Coeficient de Hadamard (H): {H}")
        if 0.7 <= H:
            print("\n")
```

```
            break
        else:
            print("Reiniciant la creació de vectors...")

    # Creem la matriu V amb els vectors de la clau privada.
    V = matrix(vectors)
    return V
```

Aquesta funció genera la clau pública. Primer crida la funció create_elementary_matrices per generar una matriu U i comprova que $\det(U) = \pm 1$. A continuació, calcula la matriu $W = UV$. Finalment, crida la funció hadamard_ratio i comrova que els vectors fila $w_1, \ldots, w_n$ de la matriu W, tinguin un quocient de Hadamard més petit que $0,0001$.

[ ]:
```
def public_key_calculation(n, num, V):
    while True:
        # Calculem matriu U, producte de "num" matrius elementals.
        U = create_elementary_matrices(n, num)
        assert U.determinant() in [-1, 1], "Determinant de U no és +/-1"

        # Creem la matriu W.
        W = U*V

        # Comprovem que W es tracta d'una base dolenta, amb un quocient de Hadamard proper a 0.
        H_prime = hadamard_ratio(W.rows())
        print(f"Coeficient de Hadamard (H') de W: {H_prime}")

        if H_prime < 0.0001:
            print("\n")
            break
        else:
            print("Error en el càlcul de la base, H' massa alt. Recalculant matrius elementals.")

    return W
```

Aqueat funció, demana el vector missatge m. Un vector de n components enteres.

[ ]:
```
def input_message(n):
    while True:
        try:
            m = vector(ZZ, [int(x) for x in input("Introdueix el vector m (missatge) com una llista d'enters separats per espais: ").split()])
            if len(m) == n:
                break
            else:
                print(f"El vector ha de tenir {n} components.")
```

```
        except ValueError:
            print("Entrada no vàlida. Si us plau, introdueix números enters␣
↪separats per espais.")
    return m
```

Finalment, i fent ús de les funcions anteriors, fem le main del programa.

[ ]:
```
def main():

    opcio = input_user()

    n = input_integer("Introdueix la dimensió n: ")

    if opcio == 1: #Opcio 1 significa que l'usuari ens dona la clau pública i␣
↪privada.

        # Introduim clau privada.
        V = input_private_key(n)

        # Introduim clau pública.
        W = input_public_key(n)

    elif opcio == 2: #Opcio 2 significa que no ens donen la clau pública i␣
↪privada, les calculem.
        d = input_integer("Introdueix un paràmetre enter petit d: ")

        # Càlcul clau privada.
        V = private_key_calculation(n,d)

        num = input_integer("Quantes matrius elementals vols utilitzar? ")

        # Càlcul clau pública.
        W = public_key_calculation(n,num,V)

    print("Clau privada:", V.rows(),"\n")
    print("Clau pública:", W.rows(),"\n")

    # Introduim el vector m missatge de manera correcte
    m = input_message(n)

    # Generem un vector pertorbació de dimensió n i rang +-2.
    r = vector(ZZ, [randint(-2, 2) for _ in range(n)])

    # Càlculem el missatge xifrat e.
    e = m*W + r

    print("Missatge xifrat e:", e, "\n")
```

```
    # Procés de desxifratge:

    T=vector(e*V.inverse())
    coefficients = vector([round(x) for x in T])
    v = coefficients * V

    print("El vector més proper a e és v:", v, "\n")

    m_decrypted = v * W.inverse()

    print("El missatge original era:", m_decrypted,"\n")

if __name__ == "__main__":
    main()
```

9 Apèndix B: Fitxa pel professorat

Primer, farem una breu introducció als reticles. Posarem les definicions claus perquè el professorat tingui una base.

9.1 Definicions bàsiques

Definició 9.1. *Siguin $v_1, \dots, v_n \in \mathbb{R}^m$ vectors linealment independents. El* ***reticle*** *L* ***generat*** *per aquests vectors, és el conjunt de combinacions lineals de $v_1, \dots, v_n$ amb coeficients en $\mathbb{Z}$,*

$$L = \{a_1 v_1 + \cdots + a_n v_n : a_1, \dots, a_n \in \mathbb{Z}\}.$$

Definició 9.2. *Una* ***base*** *B* ***d'un reticle*** *L és qualsevol conjunt de vectors linealment independents que generin L.*

Si dues bases generen el mateix reticle, tindran el mateix nombre d'elements.

Definició 9.3. *La* ***dimensió del reticle*** *ve donada pel nombre de vectors de la seva base.*

Definició 9.4. *Sigui L un reticle de dimensió n i $B = \{v_1, \dots, v_n\}$ una base de L, el* ***paral·lelepípede fonamental*** *de L corresponent a aquesta base és el conjunt*

$$F(v_1, \dots, v_n) = \{t_1 v_1 + \cdots + t_n v_n : 0 \leq t_i < 1\}.$$

Definició 9.5. *Sigui L un reticle de dimensió n i $\mathcal{B} = \{v_1, \dots, v_n\}$ una base de L. Definim el* ***quocient de Hadamard*** *de la base $\mathcal{B}$ com*

$$\mathcal{H}(\mathcal{B}) = \left(\frac{\det(L)}{\|v_1\| \cdots \|v_n\|} \right)^{1/n}.$$

Direm que $v_1, \dots, v_n$ serà una "bona base"o la clau privada quan els vectors siguin bastant ortogonals, i per tant el quocient de Hadamard sigui proper a 1. Direm que és una "base dolenta"o la clau pública quan els vectors siguin molt poc ortogonals, i per tant el quocient de Hadamard sigui proper a 1.

9.2 Esquema GGH

Construcció de claus

- Escollir una "bona base" $v_1, \dots, v_n$ que serà la clau privada.
- Denotar V com la matriu que té per files $v_1, \dots, v_n$.
- Escollir una matriu U entera amb $\det(U) = \pm 1$.
- Calcular la matriu $W = UV$. Les seves files $w_1, \dots, w_n$ seran la clau pública.

Procés de xifratge

- Escollir el vector m petit que es vol enviar.
- Escollir un vector r aleatori amb valors molt petits.
- Utilitzar la clau pública per calcular $e = mW + r = m_1w_1 + \cdots + m_nw_n +$, el missatge xifrat.
- Enviar a l'Alice el missatge e.

Procés de desxifratge

- Calcular $(t_1, \ldots, t_n) = eV^{-1}$.
- Calcular $v = \lfloor t_1 \rceil v_1 + \ldots + \lfloor t_n \rceil v_n$.
- Calcular vW^{-1} per obtenir m.

9.3 Esquema GGH per l'activitat a l'aula en dues dimensions

Construcció de claus

- Escollir una base bastant ortogonal a, b vectors de coordenades enteres amb el GeoGebra.
- Escollir una base molt poc ortogonal c, d vectors de coordenades enteres amb el GeoGebra.

Procés de xifratge

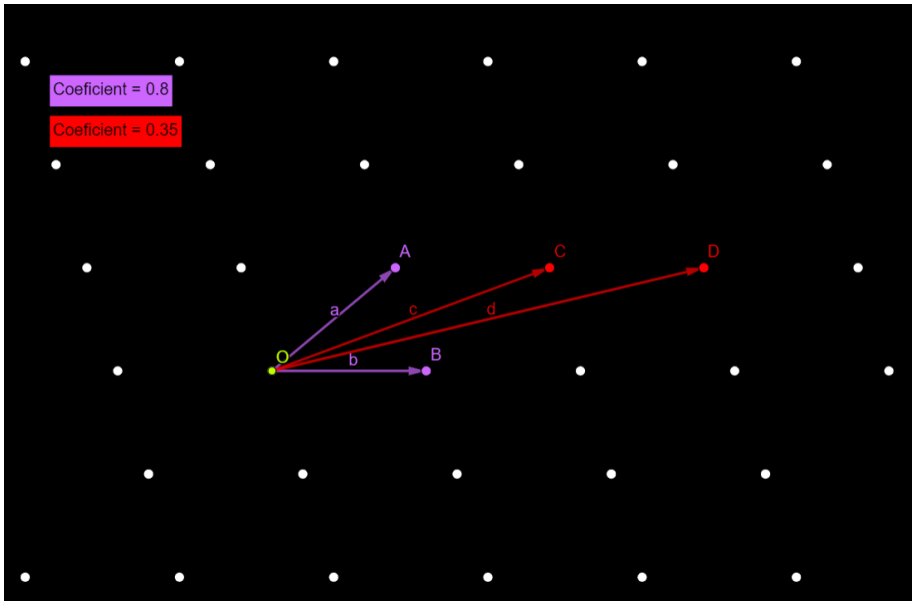
- Escollir un vector $m = (m_1, m_2)$ de coordenades enteres.
- Escollir un vector r de pertorbació molt petit i enter.
- Utilitzar la clau pública per calcular $e = m_1c + m_2d + r$.

Procés de desxifratge

- Expressar e com a combinació lineal dels vectors a, b. Aleshores, obtenim t_1, t_2 tals que $e = t_1a + t_2b$.
- Agafar la part entera de t_1, t_2.
- Calcular $v = \lfloor t_1 \rceil v_1 + \lfloor t_2 \rceil v_2$.
- Expressar $v = (v_1, v_2)$ com a combinació lineal dels vectors c, d. Aleshores, obtenim $v = m_1c + m_2d$ on m_1, m_2 és el missatge original.

9.4 GeoGebra

Per portar l'activitat a l'aula, serà important un suport visual durant l'explicació teòrica i un GeoGebra ja construït per la part del "joc de rol". El Geogebra en dues dimension és el següent.

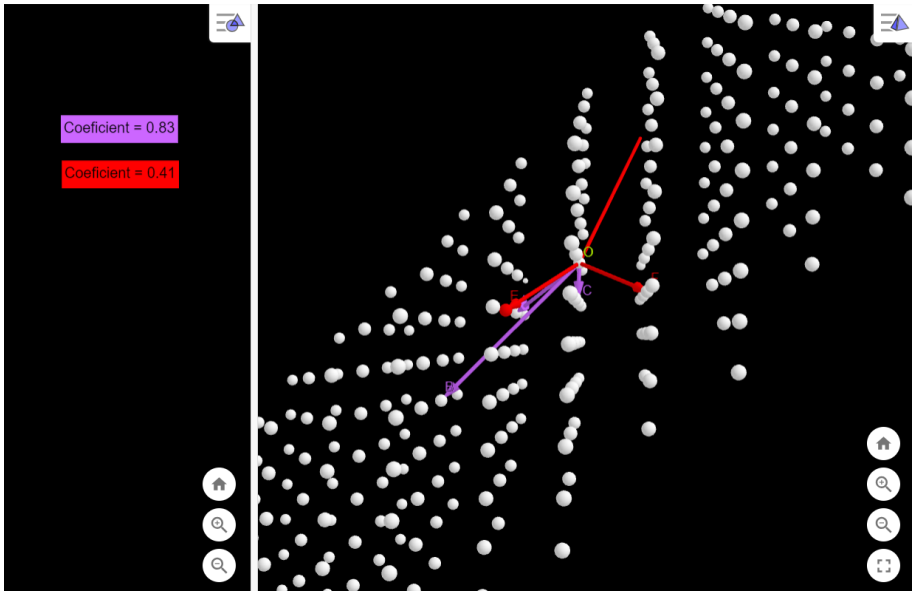


Per crear el reticle hem utilitzat la comanda:

Aplana(Seqüència(Seqüència(O+i a+j b, i, -20,20), j, -20,20)) .

Els alumnes poden anar movent els vectors de les bases i veient com fluctua el coeficient de Hadamard de cada una per poder escollir una bona clau pública i una de privada. És recomanable que el GeoGebra el creïn els alumnes.

També hem creat el GeoGebra en tres dimensions:



Per crear el reticle hem utilitzat la comanda:

Aplana(Seqüència(Seqüència(Seqüència(O+i a+j b+k c,i,-4,4),j,-4,4),k,-4,4)).

Referències

[1] A. C. de Albornoz Torres i I. Ll. Centeno. *Matemáticas con GeoGebra*. Edició 2021. Grupo Editorial RA-MA.

[2] *Advances in Cryptology-Eurocrypt 2005*. 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques Aarhus, Denmark, May 2005, Proceedings. Ronald Cramer.

[3] C. Alsina, A. Aubanell, C. Burgués. *Tres professors de matemàtiques: Com fer estimar i aprendre bé les matemàtiques*. 1a Edició. Rosa Sensat. Barcelona, 2014.

[4] C. W. Curtis. *Linear algebra. An introductory approach*. 4a Edició. Undergradu ate Texts in Mathematics. Springer-Verlag, New York, 1984.

[5] D. A. Brihuega. *Criptografía sin secretos con Python*. Edició 2017. Grupo Editorial RA-MA.

[6] D. Micciancio, S. Goldwasser. *Complexity of Lattice Problems. A cryptographic perspective*. The Kluwer International Series in Engineering and Computer Science, 671. Kluwer Academic Publishers, Boston, MA, 2002.

[7] H. O. Pollak. *Why numbers count: quantitative literacy for tomorrow's America, Solving problems in the real world* . College Entrance Examination Board. New York, 1997.

[8] J. Hoffstein, J. Pipher, J. H. Silverman. *An Introduction to Mathematical Cryptography*. 2a Edició. Undergraduate Texts in Mathematics. Springer, 2014.

[9] S. D. Galbraith. *Mathematics of public key cryptography*. Cambridge University Press. Cambridge, 2012.

[10] P. Biniés. *Converses matemàtiques amb Maria Antònia Canals: o com fer de les matemàtiques un aprenentatge apassionant.*. 1a Edició. Graó. Barcelona, 2008.

[11] P. Nguyen. *Cryptanalysis of the goldreich-goldwasser-halevi cryptosystem from crypto '97*, 1999.

[12] Y. Chen *Quantum Algorithms for Lattice Problems*, 2024.