# Courbes Elliptiques, Graphes et Cycles d'Isogénies *par des Exemples* et le Cryptosystème de Rostovtsev et Stolbunov

Emmanuel FOUOTSA

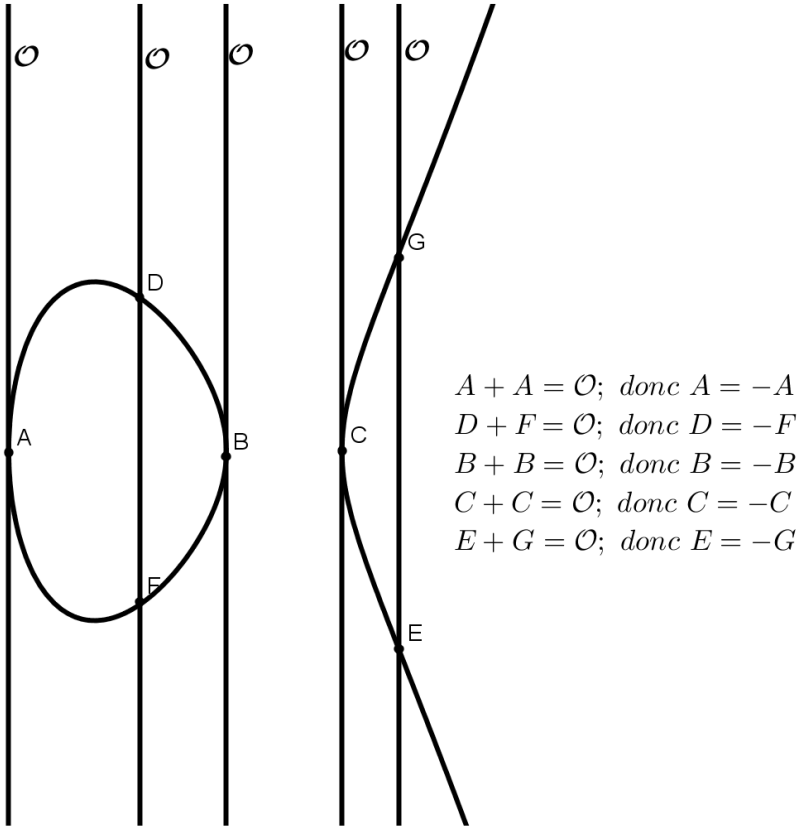
Université de Bamenda, Cameroun
Ecole Normale Supérieure de Bambili
Département de Mathématiques

FAST- Institut de Mathématiques de Bordeaux, France

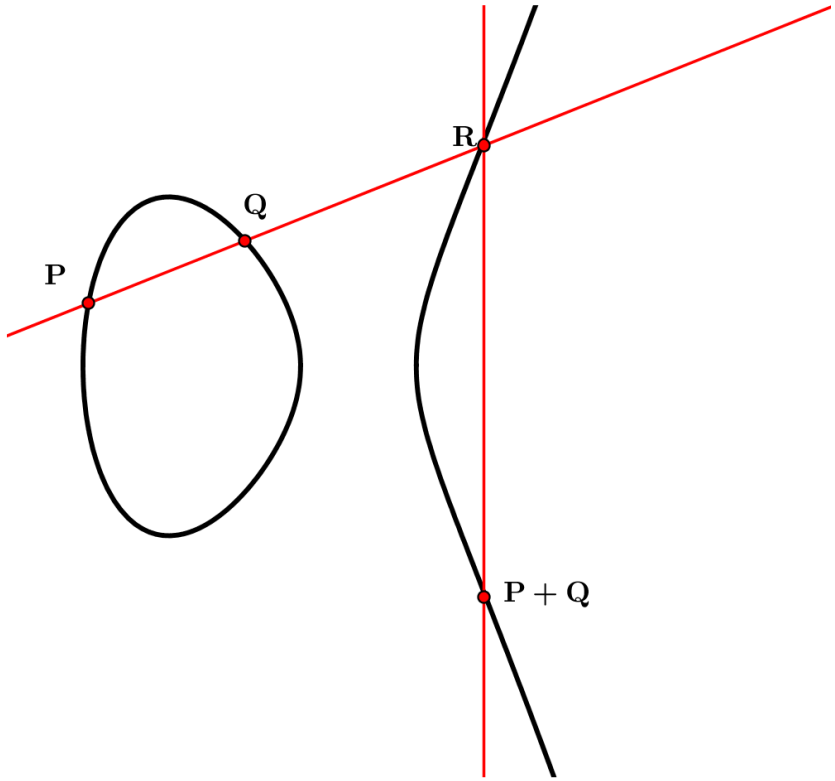
September 6, 2017

# Sommaire

# Partie 1: Bref Rappel sur les Courbes Elliptiques et Isogénies




$A + A = \mathcal{O};\ donc\ A = -A$
$D + F = \mathcal{O};\ donc\ D = -F$
$B + B = \mathcal{O};\ donc\ B = -B$
$C + C = \mathcal{O};\ donc\ C = -C$
$E + G = \mathcal{O};\ donc\ E = -G$




Soient $P(x_P, y_P)$ et $Q(x_Q, y_Q)$ deux points de $E$ et $P + Q(x_{P+Q}, y_{P+Q}$.

- $\lambda = \frac{y_Q - y_P}{x_Q - x_P}$ si $P \neq Q$
- $\lambda = \frac{dy}{dx}|_P = \frac{3x_P^2 + A}{2y_P}$ si $P = Q$.

D'où

$$x_{P+Q} = x_R = \lambda^2 - x_P - x_Q \text{ et } y_{P+Q} = -y_R = -\lambda(x_R - x_P) - y_P$$

Soit $F$ un corps, $\mathbb{P}^2(F)$ désigne l'ensemble des triplets projectifs $(x : y : z)$, $(x, y, z) \neq (0, 0, 0)$ avec $x, y, z \in F$ tels que $(x : y : z)$ et $(\lambda x : \lambda y : \lambda z)$ sont équivalents pour tout $\lambda \in F^\star$

## Definition 1

Soient $C_1$ et $C_2$ deux courbes du plan projectif définies sur $k$.

1. Une application rationnelle $\varphi : C_1 \longrightarrow C_2$ est un triplet projectif $(\varphi_x : \varphi_y : \varphi_z) \in \mathbb{P}^2(k(C_1))$, tel que pour tout point $P \in C_1(\bar{k})$ $(\varphi_x(P) : \varphi_y(P) : \varphi_z(P)) \in C_2(\bar{k})$
2. Soient $E_1$ et $E_2$ deux courbes elliptiques sur un corps $k$. Une **isogénie** de $E_1$ dans $E_2$ est une application rationnelle $\phi$ non constante et telle que $\phi(\mathcal{O}) = \mathcal{O}'$. Cela induit un homomorphisme de groupe $\phi$ de $E_1(\bar{k})$ dans $E_2(\bar{k})$ de groupes.

## Exemple 1

*Soit $E/k$ une courbe elliptique définie par l'équation réduite de Weierstrass:* $y^2 = x^3 + Ax + B$.

1. ***L'opposé.*** *En coordonnées projective, l'application $\phi : E \longrightarrow E$ qui à $(x : y : z) \longmapsto (x : -y : z)$ est un morphisme ($E$ est une courbe projective lisse ) qui est évidemment une application rationnelle. De plus $\phi(0 : 1 : 0) = (0 : 1 : 0)$ et est non constant, d'où $\phi$ est une isogénie.*
2. ***La multiplication par n.***
3. ***L'endomorphisme de Frobenius.*** *Soit $E$ une courbe elliptique définie sur un corps fini $\mathbb{F}_q$. L'endomorphisme de Frobenius de $E$ est l'application $\pi_E : (x : y : z) \longmapsto (x^q : y^q : z^q)$.*

## Theorem 2

*Soient $E_1$ et $E_2$ deux courbes elliptiques définies sur $k$ par l'équation réduite de Weierstrass, soit $\alpha : E_1 \longrightarrow E_2$ définie sur $k$. Alors $\alpha$ peut être définie par l'application rationnelle de la forme*

$$\alpha(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right),$$

*avec $u, v, s, t \in k[x]$ et $pgcd(u,v) = pgcd(s,t) = 1$.*

1. Alors $v^3 \mid t^2$ et $t^2 \mid v^3 f_1$. De plus $v$ et $t$ ont le même nombre de racines dans $\bar{k}$.
2. Le degré de $\alpha$ est définit par $deg\,\alpha := \max\{deg\,u, deg\,v\}$, on dit que $\alpha$ est **séparable** si $(\frac{u}{v})' \neq 0$, sinon $\alpha$ est **inséparable**.
3. $(x_0, y_0) \in ker\,\alpha \Longleftrightarrow v(x_0) = 0$.
4. $\alpha : E_1 \longrightarrow E_2$ une isogénie de courbes elliptiques définie sur $k$. Alors $ker\alpha$ est un sous groupe fini de $E_1(\bar{k})$.
5. L'ordre du noyau d'une isogénie est égal à son degré séparable.
6. Tout isogénie de degré composé peut toujours se décomposer en une suite d'isogénies de degré premier.

## Definition 3

Soit $E$ une courbe elliptique définie sur un corps $k$ de caractéristique non nulle $p$.
On dit que la courbe $E$ est ordinaire si $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$.
On dit que la courbe $E$ est super-singulière si $E[p] \simeq \{0\}$.

## Theorem 4

*Soit $E/\mathbb{F}_q$ une courbe elliptique, alors*

1. *(Hasse)*
$$\#E(\mathbb{F}_q) = q + 1 - tr(\pi_E) \text{ et } |tr(\pi_E)| < 2\sqrt{q}$$
2. *$E/\mathbb{F}_q$ est super-singulière si et seulement si $tr(\pi_E) \equiv 0 \ mod \ p$*

Soient $E_1$ et $E_2$ deux courbes elliptiques, alors $Hom(E_1, E_2) = \{\phi : E_1 \longrightarrow E_2\}$ est un groupe avec $(\phi_1 + \phi_2)(P) = \phi_1(P) + \phi_1(P)$. Si $E_1 = E_2$, on peut aussi composer les isogénies.

## Definition 5

Soit $E$ une courbe elliptique sur $K$ , on définit alors l'anneau d'endomorphisme de $E$ , par $End_K(E) = Hom(E, E)$ avec la multiplication donnée par la composée des isogénies $\left((\phi_1\phi_2)(P) = \phi_1(\phi_2(P))\right)$ et l'addition celle du groupe sous-jacent.

## Definition 6

Soient $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ un corps quadratique imaginaire avec $d < 0$, $\mathcal{O}$ l'anneau des entiers de $\mathbb{K}$ ($\mathcal{O} = \{\alpha \in \mathbb{K} :$ le polynôme minimal de $\alpha$ est dans $\mathbb{Z}[X]\}$ ). Alors pour chaque entier $f > 0$, l'anneau $\mathbb{Z} + f\mathcal{O}$ est un ordre de $\mathbb{K}$.
Une algèbre de quaternion sur $\mathbb{Q}$ est une algèbre de la forme $\mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$ avec la règle de multiplication $\alpha^2, \beta^2 \in \mathbb{Q}$, $\alpha^2, \beta^2 < 0$ et $\alpha\beta = -\beta\alpha$.

# L'anneau d'endomorphisme d'une courbe elliptique

## Theorem 7

*Soit $E$ une courbe elliptique sur $\mathbb{K}$. $End_K(E)$ peut être soit:*

(i) $\mathbb{Z}$,

(ii) *un ordre dans un corps quadratique imaginaire ($E$ est dite ordinaire),*

(iii) *un ordre dans une algèbre de quaternion ($E$ est dite super-singulière).*

*Si $\mathbb{Z} \subsetneq End_K(E)$, on dit que la $E$ est à multiplication complexe.*

Partie 2: Corps quadratiques imaginaires, ordres et formes quadratiques binaires

# Définition et exemples

## Définition 2.1

*Un **discriminant fondamental** est un entier $D$ vérifiant $(i)$ ou $(ii)$:*

(i) $D \equiv 1 \ (mod\ 4)$ *et $D$ est sans diviseur carré;*

(ii) $D \equiv 0 \ (mod\ 4)$*; $D/4$ est sans diviseur carré et $D/4 \equiv 2, 3 \ (mod\ 4)$.*

## Exemple 2

$-19$*;* $-15$*,* $-11$*;* $-8$*;* $-7$*;* $-4$*;* $-3$*;* $1$*;* $5$*;* $8$*;* $12$*;* $13$*;* $17$*;* .... *sont des discriminants fondamentaux.*
$-5$*;* $-2$*;* $-1$*;* $0$*,* $2$*,* $3$ *et* $4$ *ne sont pas des discriminants fondamentaux.*

## Définition 2.2

*Un **corps quadratique imaginaire** est une extension de degré 2 de $\mathbb{Q}$ de la forme*

$$K_D = \mathbb{Q}(\sqrt{D}) = \{\alpha + \beta\sqrt{D} | \alpha, \beta \in \mathbb{Q}\}$$

*où $D$ est un discriminant fondamental négatif. $D$ est appelé le discriminant de $K_D$.*

## Notation 2.1

*On pose*

$$\delta = \begin{cases} \frac{1+\sqrt{D}}{2} \; si \; D \equiv 1 \; (mod \; 4) \\ \sqrt{D/4} \; si \; D \equiv 0 \; (mod \; 4) \end{cases}$$

.

## Définition 2.3

*On appelle* ***ordre*** *de $K_D$ tout sous-anneau $O_f$ de $K_D$ de la forme*

$$O_f = \mathbb{Z}[f\delta] = \{a + bf\delta | a, b \in \mathbb{Z}\}$$

*où $f$ est un entier positif. $f$ est appelé le conducteur de l'ordre $O_f$ et $f^2D$ est le discriminant de l'ordre $O_f$.*
*$O_1 = O_{K_D}$ est appelé* ***l'ordre maximal de*** *$K_D$. Il contient tous les ordres de $K_D$.*

## Proposition 2.1 (Henri Cohen)

*Tout nombre négatif $A$ tel que $A \equiv 0, 1 \; (mod \; 4)$ s'écrit de façon unique $A = f^2D$ où $D$ est un discriminant fondamental et $A$ est le discriminant d'un unique ordre de $K_D$.*

## Exemple 3

*$-3$ est un discriminant fondamental négatif et on a:*

$$K_{-3} = \mathbb{Q}(\sqrt{-3}) = \{\alpha + \beta\sqrt{-3} | \alpha, \beta \in \mathbb{Q}\}$$

*Puisque* $-3 \equiv 1 \ (mod\ 4)$, *alors* $\delta = \frac{1+\sqrt{-3}}{2}$. *L'ordre maximal de* $K_{-3}$ *est*

$$O_{K_{-3}} = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}] = \{a + b(\frac{1+\sqrt{-3}}{2}) | a, b \in \mathbb{Z}\}$$

$O_2$ *est un ordre de conducteur* 2, *de discriminant* $2^2 \times (-3) = -12$ *et a la forme*

$$O_2 = \mathbb{Z}[2(\frac{1+\sqrt{-3}}{2})] = \mathbb{Z} + (1+\sqrt{-3})\mathbb{Z} = \mathbb{Z} + \sqrt{-3}\mathbb{Z} = \mathbb{Z}[\sqrt{-3}]$$

## Exemple 4

*$-8$ est un discriminant fondamental négatif et on a:*

$$K_{-8} = \mathbb{Q}(\sqrt{-8}) = \{\alpha + \beta\sqrt{-8} | \alpha, \beta \in \mathbb{Q}\}$$

*Puisque* $-8 \equiv 0 \ (mod\ 4)$, *alors* $\delta = \sqrt{-8/4} = \sqrt{-2}$. *L'ordre maximal de* $K_{-8}$ *est*

$$O_{K_{-8}} = \mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} | a, b \in \mathbb{Z}\}$$

$O_5$ *est un ordre de conducteur* 5, *de discriminant* $5^2 \times (-8) = -200$ *et a la forme*

$$O_5 = \mathbb{Z}[5\sqrt{-2}] = \mathbb{Z} + 5\sqrt{-2}\mathbb{Z} = \{a + 5b\sqrt{-2} | a, b \in \mathbb{Z}\}$$

## Proposition 2.2

*Les idéaux d'un ordre $\mathcal{O}$ de discriminant $\Delta$ sont de la forme $n\left(a\mathbb{Z}+\left(\frac{b+\sqrt{\Delta}}{2}\right)\mathbb{Z}\right)$, où $n$ est un entier et $\exists c \in \mathbb{Z}$ tel que $a$, $b$ et $c$ soient des entiers premiers entre eux et $b^2-4ac=\Delta$.*

Soit $D$ un discriminant fondamental négatif et $O_f$ un ordre de $K_D$.

## Définition 2.4

*Deux idéaux $I$ et $J$ de $O_f$ sont dits équivalents s'il existe un $\alpha \in K_D^*$ tel que $I=\alpha J$.*

Il est donc clair que tous les idéaux de la forme $n\left(a\mathbb{Z}+\left(\frac{b+\sqrt{\Delta}}{2}\right)\mathbb{Z}\right)$ sont équivalents à l'idéal $a\mathbb{Z}+\left(\frac{b+\sqrt{\Delta}}{2}\right)\mathbb{Z}$. L'on peut donc s'intéresser unique aux idéaux de la forme $a\mathbb{Z}+\left(\frac{b+\sqrt{\Delta}}{2}\right)\mathbb{Z}$.

## Définition 2.5

*On appelle* ***forme quadratique binaire****(FQB) toute fonction de la forme* $f(X,Y) = aX^2 + bXY + cY^2$ *où a, b et c sont des entiers. On la note* $f = (a,b,c)$.
*L'entier* $\Delta(f) = b^2 - 4ac$ *est appelé le* ***discriminant*** *de la forme f.*
*Une FQB* $f = (a,b,c)$ *est dite* ***définie positive*** *si* $\Delta(f) < 0$ *et* $a > 0$.
*Une FQB* $f = (a,b,c)$ *est dite* ***primitive*** *si a, b et c sont premiers entre eux.*

## Définition 2.6

*La représentation matricielle de la FQB* $f = (a,b,c)$ *est donnée par*

$$\mathcal{M}_f = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \text{ et } f(X,Y) = (X,Y)\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\begin{pmatrix} X \\ Y \end{pmatrix}$$

*et on a* $\Delta(f) = b^2 - 4ac = -4det(\mathcal{M}_f)$.

## Définition 2.7

*Deux FQB f et g sont dites équivalentes s'il existe une* $U \in \mathcal{M}(2,\mathbb{Z})^\times$ *telle que*

$$g(X,Y) = f(U(X,Y)) \text{ ou bien } \mathcal{M}_g = {}^tU\mathcal{M}_f U$$

## Exemple 5

*Considérons les formes* $f = (1,1,1)$ *et* $g = (195751, 37615, 1807)$. *Soit la matrice*

$$U = \begin{pmatrix} -22 & -49 \\ 229 & 510 \end{pmatrix}, det(U) = -22 \times 510 + 229 \times 49 = 1$$

*On a:*

$$\mathcal{M}_f = \begin{pmatrix} 1 & 1/2 \\ 1/2 & 1 \end{pmatrix}, \mathcal{M}_g = \begin{pmatrix} 195751 & 37615/2 \\ 37615/2 & 1807 \end{pmatrix} \text{ et } \Delta(f) = \Delta(f) = -3$$

*Et,*

$$\begin{aligned} {}^tU\mathcal{M}_g U &= \begin{pmatrix} -22 & 229 \\ -49 & 510 \end{pmatrix} \begin{pmatrix} 195751 & 37615/2 \\ 37615/2 & 1807 \end{pmatrix} \begin{pmatrix} -22 & -49 \\ 229 & 510 \end{pmatrix} \\ &= \begin{pmatrix} -22 & 229 \\ -49 & 510 \end{pmatrix} \begin{pmatrix} 791/2 & 26 \\ 38 & 5/2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1/2 \\ 1/2 & 1 \end{pmatrix} \\ &= \mathcal{M}_f \end{aligned}$$

*Donc* $f$ *et* $g$ *sont deux formes équivalentes de discriminant commun* $-3$.

## Proposition 2.3

*Deux formes équivalentes ont le même discriminant, mais la réciproque est fausse.*

## Proof.

On utilise la représentation matricielle des formes et le fait que $det(U) = \pm 1$ pour la première partie de la proposition.
Pour la deuxième partie de la proposition, les formes $f = (2, -1, 3)$ et $g = (2, 1, 3)$ ont le même discriminant qui est $-23$ mais elles ne sont pas équivalentes.(car elles sont réduites et distinctes)
Toute forme non nulle de discriminant 0 a le même discriminant que la forme nulle, mais les deux formes ne sont pas équivalentes. □

## Conséquence 2.1

*Si $f$ et $g$ sont deux FQB équivalentes, alors $f$ est définie si et seulement si $g$ l'est aussi.*

## Définition 2.8

*Un entier $n$ est dit représentable par une forme $f$ s'il existe deux entiers $x$ et $y$ tels que $f(x, y) = n$.*

## Proposition 2.4

*Si $f$ et $g$ sont deux FQB équivalentes, alors $n$ est représentable par $f$ si et seulement si $n$ est représentable par $g$.*

## Proof.

Puisque $f(X,Y) = g(U(X,Y))$, on a $n = f(x,y) = g(U(x,y))$. □

## Proposition 2.5

*Si $f$ et $g$ sont deux FQB équivalentes, alors $f$ est primitive si et seulement si $g$ l'est aussi.*

## Proof.

Par contraposition. utiliser la proposition 2.4 et le fait que $g(1,0)$, $g(0,1)$ et $g(1,1)$ sont représentables par $g$. □

## Notation 2.2

*Soit $\Delta < 0$ tel que $\Delta \equiv 0,1 \ (mod\ 4)$. On note $Cl_\Delta$ l'ensemble des classes d'équivalence des FQB primitives et définies positives discriminant $\Delta$.*

## Définition 2.9

*Soit $f = (a, b, c)$ une FQB primitive et définie positive. On dit que $f$ est réduite si*

$$|b| \leq a \leq \sqrt{|\Delta|/3}, a \leq c \text{ et si } |b| = a \text{ ou } a = c, \text{ alors } 0 \leq b$$

## Théorème 2.1

*Toute FQB primitive et définie positive de discriminant $\Delta$ est équivalente à une unique forme réduite.*

## Conséquence 2.2

*Le nombre de classes d'équivalence $h_\Delta = |Cl_\Delta|$ est fini.*

## Proof.

Puisque toute classe d'équivalence contient une unique forme réduite, alors le nombre de classes est égal au nombre de formes réduites. Pour un discriminant $\Delta$ donné, $a$ et $b$ sont bornés (par définition de forme réduite), et par conséquent $c = \frac{b^2 - \Delta}{4a}$ est aussi borné. D'où le nombre de formes réduites de discriminant $\Delta$ est fini. □

## Exemple 6 ( **Déterminons** $h_{-3}$)

*Soit* $f = (a, b, c)$ *une FQB primitive et définie positive de discriminant* $b^2 - 4ac = -3$.
*Alors* $|b| \leq a \leq \sqrt{|-3|/3}$ *et* $a \leq c$, *donc* $|b| \leq a \leq 1$ *et* $a \leq c$. *Mais puisque* $a \neq 0$, *alors* $a = 1$. *Donc* $b^2 - 4c = -3$, *d'où* $b \neq 0$ *(car si* $b = 0$, *alors* $-4c = -3$ *absurde). Ainsi,* $b = \pm 1$. *Dans ce cas on a* $|b| = a$ *donc* $0 \leq b$ *(par définition de forme réduite); d'où* $b = 1$ *et par conséquent* $c = 1$.
*L'unique FQB primitive et définie positive de discriminant* $-3$ *est* $f = (1, 1, 1)$. *Ainsi,* $h_{-3} = 1$

## Exemple 7 ( **Déterminons** $h_{-20}$)

*Soit* $f = (a, b, c)$ *une FQB primitive et définie positive de discriminant* $b^2 - 4ac = -20$.
*Alors* $|b| \leq a \leq \sqrt{|-20|/3}$ *et* $a \leq c$, *donc* $|b| \leq a \leq 2$ *et* $a \leq c$. *Mais puisque* $a \neq 0$, *alors* $a = 1$ *ou* $a = 2$.
*Si* $a = 1$, *alors* $b^2 - 4c = -20$ *et* $b$ *est pair. D'où* $b = 0$ *(car* $|b| \leq 1$*) et* $c = 5$. *On a* $f = (1, 0, 5)$
*Si* $a = 2$, *alors* $b^2 - 8c = -20$ *et* $b$ *est pair. D'où* $b = 0$ *ou* $b = \pm 2$. *Mais si* $b = 0$, *alors* $-8c = -20$, *absurde. Ainsi,* $b = \pm 2$. *Dans ce cas on a* $|b| = a$ *donc* $0 \leq b$ *(par définition de forme réduite); d'où* $b = 2$ *et par conséquent* $c = 3$. *On a* $f = (2, 2, 3)$
*Ainsi,* $h_{-20} = 2$
*on utilise qfbclassno (D) dans Pari GP*

## Proposition 2.6

*Si* $(a, b, c)$ *est une FQB primitive et définie positive de discriminant* $\Delta$, *alors* $a\mathbb{Z} + \left(\frac{b+\sqrt{\Delta}}{2}\right)\mathbb{Z}$ *est un idéal de l'ordre* $O_f$. *Réciproquement, si* $a\mathbb{Z} + \left(\frac{b+\sqrt{\Delta}}{2}\right)\mathbb{Z}$ *est un idéal de l'ordre* $O_f$, *alors* $(a, b, \frac{b^2-\Delta}{4a})$ *est une forme de discriminant* $\Delta$.
*De plus les formes sont équivalentes si et seulement si les idéaux correspondants le sont aussi.*

## Exemple 8

*Nous avons vu que les FQB primitives et définies positives* $f = (1,1,1)$ *et* $g = (195751, 37615, 1807)$ *sont équivalentes et la matrice* $U$ *est donnée par:*

$$U = \begin{pmatrix} -22 & -49 \\ 229 & 510 \end{pmatrix}$$

*Leur idéaux correspondants sont respectivement*

$$I_f = \mathbb{Z} + \left(\frac{1+\sqrt{-3}}{2}\right)\mathbb{Z} \text{ et } I_g = 195751\mathbb{Z} + \left(\frac{37615+\sqrt{-3}}{2}\right)\mathbb{Z}$$

*On montre que*

$$I_f = \left(-22 + 229\frac{1-\sqrt{-3}}{2}\right) I_g$$

*De façon générale, si deux FQB primitives et définies positives* $f = (a,b,c)$ *et* $g = (a',b',c')$ *sont équivalentes et* $U$ *est donnée par:* $U = \begin{pmatrix} u & v \\ w & z \end{pmatrix}$, *alors*

$$I_f = \alpha I_g \qquad \text{où } \alpha = u + w\frac{b-\sqrt{\Delta}}{2a}$$

## Partie 3: Sur les Réseaux et courbes elliptiques sur $\mathbb{C}$

## Définition 3.1

*On appelle* ***réseau*** *tout sous groupe additif $L$ de $\mathbb{C}$ de la forme*

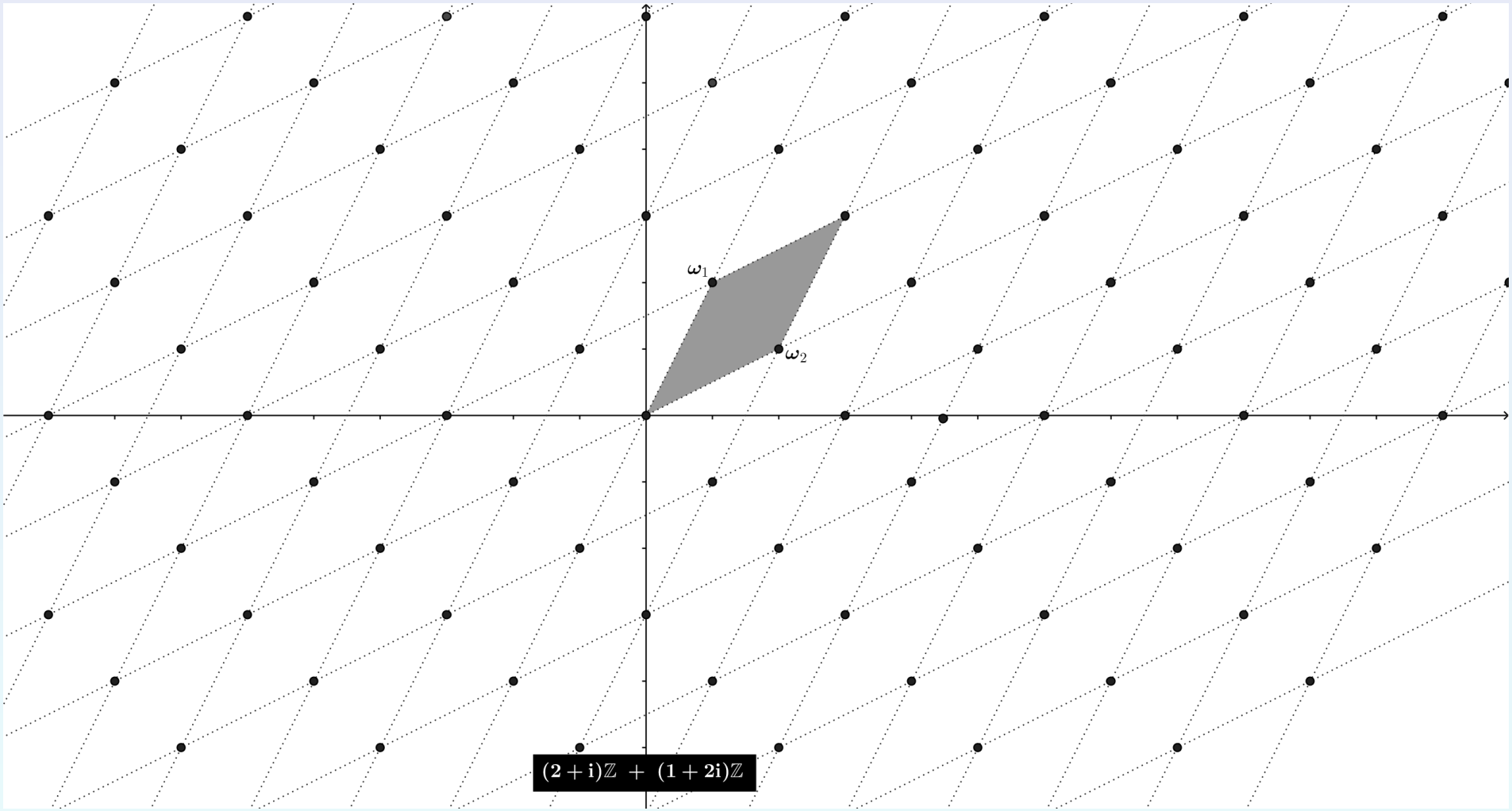
$$L = w_1\mathbb{Z} + w_2\mathbb{Z}$$

*où $w_1$ et $w_2$ sont linéairement indépendants sur $\mathbb{R}$*

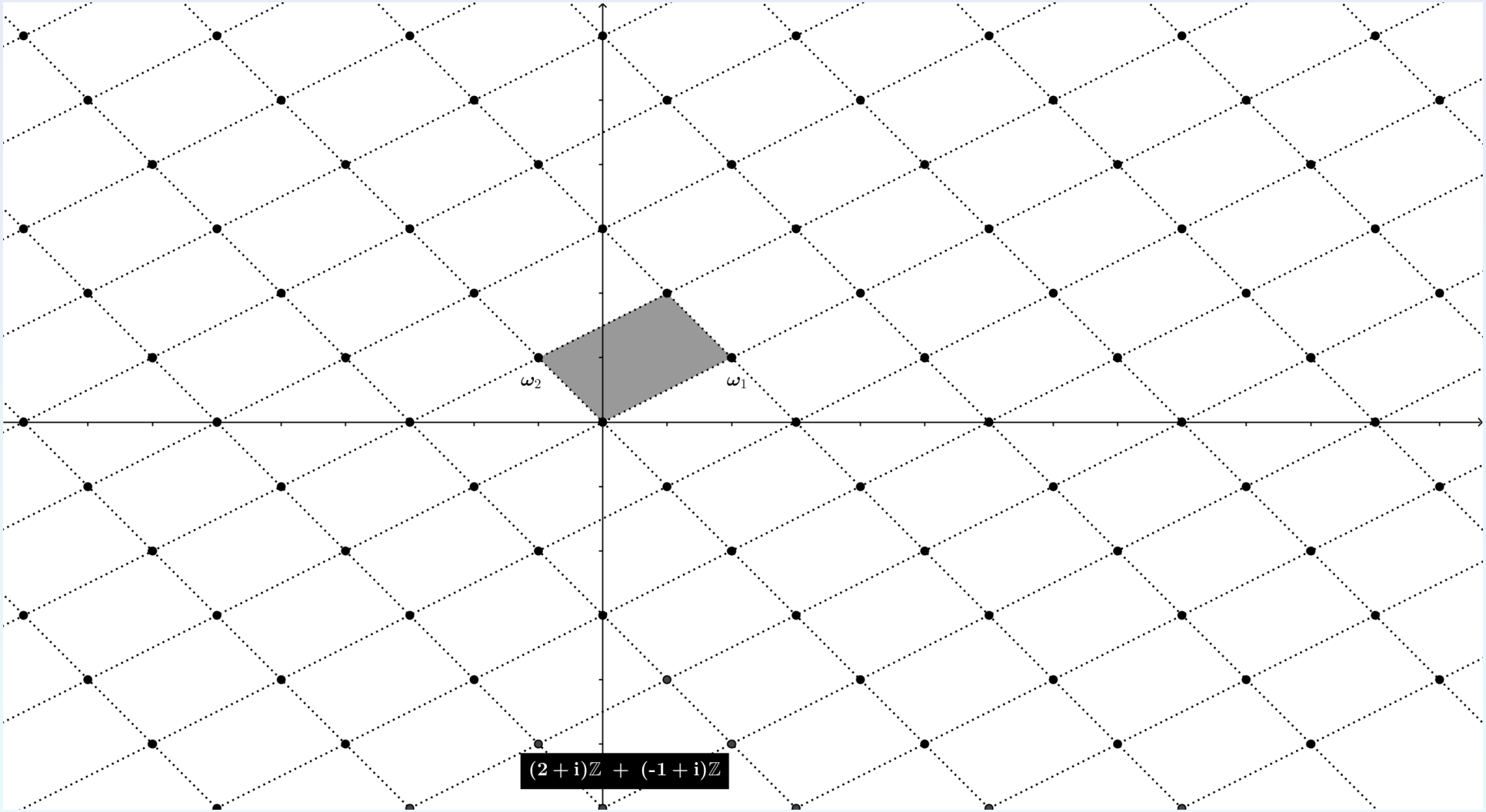
## Exemple 9

*$(2+i)\mathbb{Z} + (1+2i)\mathbb{Z}$, $(2+i)\mathbb{Z} + (-1+i)\mathbb{Z}$, $\mathbb{Z} + i\mathbb{Z}$ et $(1+i)\mathbb{Z} + (1-i)\mathbb{Z}$ sont des réseaux.*
*$(1-i)\mathbb{Z} + (i-1)\mathbb{Z}$ n'est pas un réseaux car $1-i$ et $i-1$ sont linéairement dépendants sur $\mathbb{R}$: $1-i = -(i-1)$.*

# Représentation graphique du réseau $(2+i)\mathbb{Z}+(1+2i)\mathbb{Z}$



# Représentation graphique du réseau $(2+i)\mathbb{Z}+(-1+i)\mathbb{Z}$



## Définition 3.2

*On appelle **parallélogramme fondamental** d'un réseau $L = w_1\mathbb{Z} + w_2\mathbb{Z}$ tout ensemble de la forme*

$$P_f = \{\alpha + t_1 w_1 + t_2 w_2 | \alpha \in \mathbb{C}, 0 \leq t_1, t_2 \leq 1\}.$$

## Définition 3.3

*Deux réseaux $L_1$ et $L_2$ sont dits équivalents s'il existe un nombre complexe $\alpha$ tel que $L_1 = \alpha L_2$.*

Notons que dans le plan complexe, multiplier l'affixe d'un point $M$ par $\alpha = re^{i\theta}$ revient à trouver l'affixe de l'image $M'$ de $M$ par $H \circ R$ où $H = h(O, r)$ et $R = r(O, \theta)$. Donc deux réseaux sont équivalents si et seulement si l'un est l'image de l'autre par la composée d'une rotation de centre $O$ et d'une homothétie de centre $O$. Cela justifie la proposition suivante.

## Proposition 3.1

*Deux réseaux $L_1$ et $L_2$ sont équivalents si et seulement si leurs parallélogrammes fondamentaux sont semblables.*

## Proposition 3.2

*Tout réseau $L = w_1\mathbb{Z} + w_2\mathbb{Z}$ est équivalent à un réseau $L_\tau$ de la forme $L_\tau = \tau\mathbb{Z} + \mathbb{Z}$ avec $Im(\tau) > 0$*

## Proof.

Puisque $L = w_1\mathbb{Z} + w_2\mathbb{Z}$ est un réseau, alors $w_2$ est non nul (sinon $w_1$ et $w_2$ seraient linéairement dépendants sur $\mathbb{R}$). Ainsi, $w_2$ est inversible et on a:

$$L = w_1\mathbb{Z} + w_2\mathbb{Z} = w_2\left(\frac{w_1}{w_2}\mathbb{Z} + \mathbb{Z}\right) = w_2 L_\tau \text{ où } \tau = \frac{w_1}{w_2}$$

Puisque $w_1$ et $w_2$ sont linéairement indépendants sur $\mathbb{R}$, alors $\tau = \frac{w_1}{w_2} \notin \mathbb{R}$, donc $Im(\tau) \neq 0$. Si $Im(\tau) < 0$ il suffit de remplacer $w_1$ par $-w_1$. □

## Exemple 10

*$(1+i)\mathbb{Z} + (1-i)\mathbb{Z}$ est équivalent à $\mathbb{Z} + i\mathbb{Z}$*

## Définition 3.4

*Soit $L$ un réseau. La famille des séries d'Eisenstein est la famille $(G_k)_{2<k}$ des séries définies en $L$ par*

$$G_k(L) = \sum_{z \in L \setminus \{0\}} z^{-k}$$

## Proposition 3.3

*Pour tout réseau $L$, la série $G_k(L)$ converge absolument pour tout $k > 2$.*

## Définition 3.5

*Soit $L$ un réseau. On appelle* ***fonction elliptique*** *par rapport à $l$ toute fonction complexe $f$ qui est méromorphe et $L-$périodique ( c-à-d $\forall w \in L, \forall z \in \mathbb{C}$, $f(z+w) = f(z)$).*

## Proposition 3.4

*Soit $L = w_1\mathbb{Z} + w_2\mathbb{Z}$ un réseau. Une fonction complexe $f$ est $L-$périodique si et seulement si elle est $w_1-$périodique et $w_2-$périodique.*

## Définition 3.6

*Soit $L$ un réseau. La **fonction de Weierstrass** de $L$ est la fonction complexe définie par*

$$\wp_L(z) = \frac{1}{z^2} + \sum_{w \in L \setminus \{0\}} \left( \frac{1}{(z-w)^2} - \frac{1}{w^2} \right)$$

## Theorem 8

*Pour tout réseau $L$, $\wp_L(z)$ est paire et méromorphe, ses pôles sont exactement les éléments de $L$ et sont tous doubles. La dérivée de $\wp_L$ est donnée par*

$$\wp_L{}'(z) = -2 \sum_{w \in L} \frac{1}{(z-w)^3}$$

*$\wp_L{}'$ est impaire et méromorphe, ses pôles sont exactement les éléments de $L$ et sont tous triples.*

## Proof.

□

## Theorem 9

*Pour tout réseau $L$, $\wp_L$ et sa dérivée satisfont l'équation différentielle*

$$\wp_L{}'^2 = 4\wp_L^3 - 60G_4(L)\wp_L - 140G_6(L)$$

En posant $y = \wp_L{}'$, $x = \wp_L$, $g_2(L) = 60G_4(L)$ et $g_3(L) = 140G_6(L)$, on obtient

$$y^2 = 4x^3 - g_2(L)x - g_3(L) \text{ ou bien } (y/2)^2 = x^3 - \frac{g_2(L)}{4}x - \frac{g_3(L)}{4}$$

Et cette courbe a pour discriminant

$$\Delta(L) = -16\left(4(-\frac{g_2(L)}{4})^3 + 27(-\frac{g_3(L)}{4})^2\right) = g_2(L)^3 - 27g_3(L)^2$$

## Proposition 3.5

*Pour tout réseau $L$, on a :*

$$\Delta(L) = g_2(L)^3 - 27g_3(L)^2 \neq 0$$

## Conséquence 3.1

*Tout réseau $L$ induit une courbe elliptique sur $\mathbb{C}$ notée $E_L$ et dont une équation est donnée par*

$$E_L : y^2 = x^3 - \frac{g_2(L)}{4}x - \frac{g_3(L)}{4}$$

## Theorem 10

*Pour tout réseau $L$, l'application*

$$\begin{array}{rccc} \Phi : & \mathbb{C}/L & \longrightarrow & E_L \\ & z \neq 0 & \longmapsto & (\wp_L(z), \wp_L{}'(z)) \\ & 0 & \longmapsto & \mathcal{O} \end{array}$$

*est un isomorphisme de groupes additifs.*

## Définition 3.7

*On appelle* ***j-fonction*** *la fonction notée j qui à un réseau L associe*

$$j(L) = 1728\frac{g_2(L)^3}{g_2(L)^3 - 27g_3(L)^2}$$

C'est en fait le $j-$invariant de la courbe elliptique $E_L$.

## Proposition 3.6

*Deux réseaux $L_1$ et $L_2$ sont équivalents si et seulement si $j(L_1) = j(L_2)$*

## Proof.

□

## Conséquence 3.2

*Deux réseaux $L_1$ et $L_2$ sont équivalents si et seulement si leurs courbes associées $E_{L_1}$ et $E_{L_2}$ sont isomorphes.*

Ainsi, pour tout réseau $L$, $\exists \tau \in \mathbb{H} = \{x + iy \in \mathbb{C} | y > 0\}$ tel $j(L) = j(L_\tau) = j(\tau)$.

## Proposition 3.7

*Soient $\tau, \tau' \in \mathbb{H}$, alors $j(\tau) = j(\tau')$ si et seulement si il existe $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}$ tel que $\tau' = \frac{a\tau+b}{c\tau+d}$.*

## Theorem 11

*La $j-$fonction définit une bijection de $\mathbb{H}/SL_2(\mathbb{Z})$ vers $\mathbb{C}$*

## Theorem 12

*Pour toute courbe $E/\mathbb{C}$, il existe un réseau $L$ tel que $E/\mathbb{C}$ soit isomorphe à $E_L$.*

## Proof.

Puisque $j(E) \in \mathbb{C}$, alors il existe $\tau \in \mathbb{H}$ tel que $j(E) = j(\tau) = j(L_\tau) = j(E_{L_\tau})$. Donc $E$ et $E_{L_\tau}$ sont isomorphes. □

## Exemple 11

*Pour tout nombre complexe $\tau$, Pari GP calcule $j(\tau)$ en utilisant la commande ellj($\tau$). la commande ellfromj($j$) permet de déterminer les coefficients de l'équation de Weierstrass d'une courbe sur $\mathbb{C}$ de j-invariant j.*

| $\tau$ | $L_\tau$ | $j(\tau) = j(L_\tau)$ | *équation de Weierstrass de* $E_L$ |
|---|---|---|---|
| $i$ | $\mathbb{Z}[i]$ | 1728 | $y^2 = x^3 + x$ |
| $e^{2\pi i/3}$ | $\mathbb{Z}[\frac{-1+\sqrt{3}i}{2}]$ | 0 | $y^2 = x^3 + 1$ |
| $\sqrt{3}i$ | $\mathbb{Z}[\sqrt{3}i]$ | 54000 | $y^2 = x^3 - 8468064000x + 295095094272000$ |

## Theorem 13

*Soit $L$ un réseau et $\alpha$ un nombre complexe. Alors les deux assertions suivantes sont équivalentes :*

(i) $\alpha L \subset L$

(ii) *Il existe une unique isogénie $\phi = \phi_\alpha \in End(E_L)$ telle que le diagramme suivant commute.*

$$\begin{array}{ccccc} \mathbb{C}/L & - & \Phi & \to & E_L/\mathbb{C} \\ | & & & & | \\ \alpha & & & & \phi_\alpha \\ \downarrow & & & & \downarrow \\ \mathbb{C}/L & - & \Phi & \to & E_L/\mathbb{C} \end{array}$$

*De plus, pour tout $\phi \in End(E_L) \simeq \{\alpha \in \mathbb{C} | \alpha L \subset L\}, \exists \alpha = \alpha_\phi$ vérifiant $(i)$ et $(ii)$. Les applications $\alpha \mapsto \phi_\alpha$ et $\phi \mapsto \alpha_\phi$ sont des isomorphismes d'anneaux entre $End(E)$ et $End(E_L) \simeq \{\alpha \in \mathbb{C} | \alpha L \subset L\}$; et on a $deg(\phi_\alpha) = [L : \alpha L]$*

A partir de ce théorème, on a:

$$End(E_L) \simeq \{\alpha \in \mathbb{C} | \alpha L \subset L\} \simeq End(\mathbb{C}/L)$$

## Corollaire 3.1

*Pour toute courbe elliptique $E/\mathbb{C}$, $End(E)$ est un anneau commutative. Dès lors $End(E)$ est soit $\mathbb{Z}$ soit un ordre dans un corps quadratique imaginaire.*

# Caractérisation des courbes elliptiques sur $\mathbb{C}$ telles que $End(E) = \mathbb{Z}$

## Proposition 3.8

*Soit $E/\mathbb{C} = E_{L_\tau}$ une courbe elliptique. les propositions suivantes sont équivalentes:*

(i) $End(E) = \mathbb{Z}$

(ii) $\mathbb{Q}(\tau)$ *n'est pas une extension quadratique de* $\mathbb{Q}$

(iii) $Re(\tau) \notin \mathbb{Q}$ *ou* $|\tau|^2 \notin \mathbb{Q}$.

# Caractérisation des courbes elliptiques sur $\mathbb{C}$ telles que $End(E) = \mathcal{O}_f$

Dans le cas où $End(E)$ est un ordre $\mathcal{O}_f$ dans un corps quadratique imaginaire, quels sont les réseaux $L$ tels que $End(E_L) \simeq \mathcal{O}_f$?
On a

$$End(E_{\mathcal{O}_f}) \simeq \{\alpha \in \mathbb{C} | \alpha\mathcal{O}_f \subset \mathcal{O}_f\} = \mathcal{O}_f$$

et ainsi pour tout réseau équivalent à $\mathcal{O}_f$ car deux réseaux équivalents définissent la même courbe elliptique à isomorphisme près.
Le théorème suivant nous dit que ce ne sont pas les seuls.

## Theorem 14 (sutherland, lec 17, page 7)

*Soit $\mathcal{O}_f$ un ordre dans un corps quadratique imaginaire. Il y a une bijection entre les éléments du groupe des classes d'idéaux de $\mathcal{O}_f$ d'une part, et l'ensemble des classes d'équivalence des réseaux $L$ vérifiant $End(E_L) \simeq \mathcal{O}_f$ d'autre part.*

Cela signifie qu'il y a $h_\Delta$ ($\Delta$ est le discriminant de $\mathcal{O}_f$) courbes elliptiques sur $\mathcal{C}$ vérifiant $End(E) = \mathcal{O}_f$.

De façon récapitulative, pour tout ordre $\mathcal{O}_f$ de discriminant $\Delta$ dans corps quadratique imaginaire, nous avons :

| | | | |
|---|---|---|---|
| $E$ | $L$ | idéaux de $\mathcal{O}_f$ | $f=(a,b,c);\Delta(f)=\Delta$ |
| \| | \| | \| | \| |
| iso | equiv. par hom | equiv. par hom | $SL_2(\mathbb{Z})-equiv.$ |
| \| | \| | \| | \| |
| $j(E)$ | $j(L)$ | idéal reduit | forme reduite |
| \| | \| | \| | \| |
| $\{j(E)\|End(E)=\mathcal{O}_f\}$ | $\{j(L)\|End(E_L)=\mathcal{O}_f\}$ | $cl(\mathcal{O}_f)$ | $cl_\Delta$ |

Les courbes elliptiques de ce diagramme sont toute les courbes elliptiques sur $\mathbb{C}$ à multiplication complexe par $\mathcal{O}_f$.

## Partie 4: Graphes d'isogénies des courbes elliptiques ordinaires

## Proposition 4.1

*Soit $E$ une courbe elliptique sur un corps fini $\mathbb{F}_q$ et $\pi_E : E \to E$ l'endomorphisme de Frobenius. On a les résultats suivants:*

- *$\pi_E$ est solution de l'équation $x^2 - tx + q = 0$ où $t = \pi_E + \widehat{\pi_E} = tr(\pi_E)$ et on pose $D_{\pi_E} = t^2 - 4q$ le discriminant de cette équation.*
- *(Théorème de Hasse) $|E(\mathbb{F}_q)| = q + 1 - t$ et $|t| \leq 2\sqrt{q}$*
- *(Théorème de Tate) $E$ et $E'/\mathbb{F}_q$ sont isogènes si et seulement si $|E(\mathbb{F}_q)| = |E'(\mathbb{F}_q)|$*

Plaçons nous dans le cas des courbes ordinaires.
A partir du théorème de Hasse, on a $D_{\pi_E} = t^2 - 4q \leq 0$. $\pi_E \notin \mathbb{Z}$ (sinon $\pi_E = \widehat{\pi_E}$, $deg(\pi_E) = \pi_E\widehat{\pi_E} = {\pi_E}^2 = q$, donc $q = p^{2k}$ et $\pi_E = \pm p^k$, d'où $t = \pm 2p^k \equiv \quad 0 \quad mod \quad p$, donc $E$ est super-singulière; absurde), donc $\mathbb{Z}[\pi_E]$ est un ordre dans le corps quadratique imaginaire $\mathbb{Q}(\sqrt{\Delta_{\pi_E}})$ où $D_{\pi_E} = f_{\pi_E}^2 \Delta_{\pi_E}$, $\Delta_{\pi_E}$ est un discriminant fondamental et $f_{\pi_E}$ est le conducteur de $\mathbb{Z}[\pi_E]$. Mais puisque $\mathbb{Z} \subset End(E)$ et $\pi_E \in End(E)$, alors $\mathbb{Z}[\pi_E] \subset End(E) \subset \mathbb{Q}(\sqrt{\Delta_{\pi_E}})$. Donc l'ordre $f$ de $End(E)$ est un diviseur de $f_{\pi_E}$.

# Polynôme de classe d'Hilbert

Nous avons vu que pour tout ordre $\mathcal{O}$ de discriminant $\Delta$ d'un corps quadratique imaginaire, il y a exactement $h_\Delta$ courbes elliptiques $(E_i)_{i=1,\dots,h_\Delta}$ sur $\mathbb{C}$ admettant $\mathcal{O}$ comme anneau d'endomorphisme.

## Définition 4.1

*On appelle* ***polynôme de classes d'Hilbert*** *le polynôme (à coefficients entiers)*

$$H_\Delta(X) = \prod_{i=1}^{h_\Delta} (X - j(E_i))$$

# Comment le calcule t-on ?

## Rappels 4.1

| $E$ | $L$ | *idéaux de* $\mathcal{O}_f$ | $f=(a,b,c);\Delta(f)=\Delta$ |
|---|---|---|---|
| $\Big\vert$ | $\Big\vert$ | $\Big\vert$ | $\Big\vert$ |
| *iso* | *equiv. par hom* | *equiv. par hom* | $SL_2(\mathbb{Z})-$ *equiv.* |
| $\Big\vert$ | $\Big\vert$ | $\Big\vert$ | $\Big\vert$ |
| $j(E)$ | $j(L)$ | *idéal reduit* | *forme reduite* |
| $\Big\vert$ | $\Big\vert$ | $\Big\vert$ | $\Big\vert$ |
| $\{j(E)\vert End(E)=\mathcal{O}_f\}$ | $\{j(L)\vert End(E_L)=\mathcal{O}_f\}$ | $cl(\mathcal{O}_f)$ | $cl_\Delta$ |

*On a donc une famille* $(E_i)_{i=1,\dots,h_\Delta}$ *de courbes elliptiques d'un coté, et une famille* $(f_i=(a_i,b_i,c_i))_{i=1,\dots,h_\Delta}$ *de formes quadratique binaires primitives réduites de discriminant* $\Delta$. *Chaque courbe* $E_i$ *correspond à une unique forme* $f_i$ *et cette correspondance se traduit par le fait que*

$$j(E_i)=j(\tfrac{b_i+\sqrt{\Delta}}{2a_i})=j(\tau_i)=j(L_{\tau_i})\ avec\ \tau_i=\tfrac{b_i+\sqrt{\Delta}}{2a_i};$$
$$On\ a\ donc:\ H_\Delta(X)=\prod_{i=1}^{h_\Delta}(X-j(\tau_i))$$

En utilisant la définition des formes réduites primitives, on détermine toutes les formes primitives de discriminant $\Delta$ $f_i = (a_i, b_i, c_i)$. On calcule les $\tau_i$ et à l'aide la commande $ellj(\tau_i)$ dans pari gp, on détermine les $j(\tau_i)$. On développe $H_\Delta(X) = \prod_{i=1}^{h_\Delta}(X - j(\tau_i))$ pour effectivement a voir un polynôme à coefficients entiers.

## Exemple 12

*Nous allons déterminer* $H_{-7}(X)$, $H_{-20}(X)$ *et* $H_{-59}(X)$.
*on utilise polclass (D) dans Pari GP*
$\underline{\Delta = -7}$.
*Comme* $h_{-7} = 1$, *on a une seule forme quadratique binaire définie positive primitive et réduite de discriminant* $-7$ *qui est* $f = (1, 1, 2)$. *On a* $\tau = \frac{1+\sqrt{-7}}{2}$ *et* $j(\tau) = -3375$ *Donc*

$$H_{-7}(X) = X + 3375$$

$\underline{\Delta = -20}$.
*Comme* $h_{-20} = 2$, *on a deux formes quadratiques binaires définies positives primitives et réduites de discriminant* $-20$ *qui sont* $f_1 = (1, 0, 5)$ *et* $f_2 = (2, 2, 3)$. *On a* $\tau_1 = \sqrt{-5}$ *et* $\tau_2 = \frac{1+\sqrt{-5}}{2}$ . *Donc*

$$H_{-20}(X) = X^2 - 1264000X + 681472000$$

## Exemple 13

$\underline{\Delta = -59}$.

*Comme* $h_{-59} = 3$, *on a trois formes quadratiques binaires définies positives primitives et réduites de discriminant* $-20$ *qui sont* $f_1 = (3,1,5)$, $f_2 = (3,-1,5)$ *et* $f_3 = (1,1,15)$. *On a* $\tau_1 = \frac{1+\sqrt{-59}}{6}$, $\tau_2 = \frac{-1+\sqrt{-59}}{6}$ *et* $\tau_3 = \frac{1+\sqrt{-59}}{2}$ . *Donc*

$$H_{-59}(X) = X^3 + 30197678080X^2 - 1408115765411184X + 37464319400188313 6$$

Constatons que $h_{-59} = 3$ mais le terme constant de $H_{-59}(X)$ s'écrit avec 18 chiffres décimaux. En effet, les coefficients de $H_\Delta(X)$ explosent au fur et à mesure que $h_\Delta$ et $D$ deviennent grands, ce qui rend le calcul de $H_\Delta(X)$ impossible pour des discriminants très grands.

## Proposition 4.2

*Soit $\mathcal{O}$ un ordre de discriminant $\Delta$ d'un corps quadratique imaginaire et $p$ un nombre premier ne divisant pas $\Delta$. Alors il y a équivalence entre:*

- $\left(\frac{\Delta}{p}\right) = 1$ *et* $H_\Delta(X)$ *(réduit modulo $p$) se décompose entièrement dans* $\mathbb{F}_p[X]$
- *il existe deux entiers $t$ et $v$ tels que* $4p = t^2 - v^2\Delta$ *et* $t \neq\equiv 0 \mod p$

## Exemple 14

*Considérons le discriminant fondamental $-59$ et soit $\mathcal{O}$ l'ordre maximal du corps quadratique imaginaire $\mathbb{Q}(\sqrt{-59})$. Le discriminant de $\mathcal{O}$ est donc $\Delta = -59$ et on a:*

$$H_{-59}(X) = X^3 + 30197678080X^2 - 1408115765411184X + 37464319400188 3136$$

*qui est bel et bien un polynôme de degré $h_{-59} = 3$. Comme on souhaite avoir $4p = t^2 - v^2\Delta$, alors $-v^2\Delta \leqslant 4p$ et $p$ est distinct de 59 (puisque $p$ ne doit pas diviser $\Delta$).*
*Dans le tableau suivant, nous étudions le cas 6 nombres premiers:* 17, 43, 61, 71, 149, 197.

## Exemple 15

| $p$ | $(t;v)$ | $\left(\frac{-59}{p}\right)$ | $H_{-59}(X) \mod p$ | *fact. ds.* $\mathbb{F}_p[X]$ | *racines* |
|---|---|---|---|---|---|
| 17 | $(3;1)$ | 1 | $X^3+12X^2+12X+5$ | $(X+4)(X+10)(X+15)$ | $2;7;13$ |
| 43 | $--$ | $-1$ | $X^3+11X^2+36X+1$ | $(X+35)(X^2+19X+16)$ | 8 |
| 61 | $--$ | $-1$ | $X^3+58X^2+52X+53$ | $(X+20)(X^2+38X+24)$ | 41 |
| 71 | $(15;1)$ | 1 | $X^3+41X^2+62X+11$ | $(X+4)(X+17)(X+20)$ | $51;54;67$ |
| 149 | $--$ | $-1$ | $X^3+60X^2+105X+117$ | $(X+81)(X^2+128X+18)$ | 68 |
| 197 | $(27;1)$ | 1 | $X^3+195X^2+160X+139$ | $(X+2)(X+67)(X+126)$ | $71;130;195$ |

## Proposition 4.3 (rappel)

*Tout élément $j$ de $\mathbb{F}_q$ est le $j$-invariant d'une courbe elliptique $E$ définie sur $\mathbb{F}_q$. De plus cette courbe elliptique a une équation de la forme:*

- $E : y^2 = x^3 + c$ $(c \in \mathbb{F}_q^*)$ *si* $j = 0$;
- $E : y^2 = x^3 + cx$ $(c \in \mathbb{F}_q^*)$ *si* $j = 1728$;
- $E : y^2 = x^3 + 3kc^2x + 2kc^3$ $(c \in \mathbb{F}_q^*$ *et* $k = \frac{j}{1728-j})$ *si* $j \neq 0, 1728$.

# Graphe d'isogénies de courbes ordinaires

## Proposition 4.4

*Soit $E/k$ une courbe elliptique ayant pour anneau d'endomorphisme un ordre $\mathcal{O}$ de conducteur $f$ d'un corps quadratique imaginaire $K_D$, et $E'/\mathbb{F}_q$ une courbe elliptique telle qu'il existe une isogénie séparable $\phi : E \longrightarrow E'$ de degré premier $l$ $(l \neq \ caract(k))$.*
*Alors l'anneau d'endomorphisme $\mathcal{O}'$ de $E'$ est un ordre de conducteur $f'$ de $K_D$ tel que l'une des conditions suivantes soit satisfaite:*

$$(i)\mathcal{O} = \mathcal{O}' \quad (f = f') \quad (ii)[\mathcal{O}' : \mathcal{O}] = l \quad (f = lf') \quad (iii)[\mathcal{O} : \mathcal{O}'] = l \quad (f' = fl)$$

## Définition 4.2

*Avec les notation de la proposition précédente, on dit que*

- *$\phi$ est une isogénie horizontale si $\mathcal{O} = \mathcal{O}'$*
- *$\phi$ est une isogénie ascendante si $[\mathcal{O}' : \mathcal{O}] = l$*
- *$\phi$ est une isogénie descendante si $[\mathcal{O} : \mathcal{O}'] = l$*

*Les deux dernières sont communément appelées isogénies verticales.*

## Proposition 4.5

*Soit $E/k$ une courbe elliptique ayant pour anneau d'endomorphisme un ordre $\mathcal{O}$ de conducteur $f$ d'un corps quadratique imaginaire $K_D$, et soit $l \neq caract(k)$ un nombre premier.*
*Si $l$ divise $f$, alors il n'existe pas d'isogénie horizontale de degré $l$ et de domaine $E$.*
*Sinon, le nombre d'isogénies horizontales de degré $l$ et de domaine $E$ est $1 + \left(\frac{\Delta}{l}\right) \in \{0, 1, 2\}$ où $\Delta = disc(\mathcal{O})$.*

## Proposition 4.6

*Soit $E/\mathbb{F}_p$ une courbe elliptique ayant pour anneau d'endomorphisme un ordre $\mathcal{O}$, sous ordre d'indice $l$ ($l \neq caract(k)$) de $\mathcal{O}'$ avec $disc(\mathcal{O}') < -4$.*
*Alors, à isomorphisme près, il existe une unique isogénie ascendante de $E$ vers une courbe $E'/\mathbb{F}_p$ telle que $End(E') = \mathcal{O}'$.*

## Définition 4.3

*Graphe d'Isogénies*
*Un graphe d'isogénies de degré $l$ est un graphe constitué de nœuds, qui représentent les j-invariants des courbes, et des segments liant les nœuds deux à deux, qui symbolisent l'existence d'une isogénie de degré $l$ entre les deux nœuds qu'ils relient.*

# Graphe d'isogénies: terre à terre

Dans un graphe d'isogénies de degré $l$, les nœuds sont classés par niveaux du haut vers le bas, en commençant par 0. Dans un niveau $i$, toutes les courbes ont le même anneau d'endomorphisme $\mathcal{O}_i$ de conducteur $f_i$ et de discriminant $\Delta_i$; et il y a exactement $h_{\Delta_i}$ nœuds. Ainsi, pour savoir à combien de nœuds du niveau $i+1$ un nœuds du niveau $i$ sera relié, on fait juste

$$\frac{h_{\Delta_{i+1}}}{h_{\Delta_i}}$$

De plus, un nœud du niveau $i+1$ n'est relié qu'à un seul nœud du niveau $i$ (d'après la proposition 4.6).

Lorsqu'on passe du niveau $i$ au niveau $i+1$, le conducteur $f_i$ du niveau $i$ est multiplié par $l$ et on a $f_{i+1} = lf_i$ (d'après la proposition 4.4).

Au niveau 0, c-à-d au sommet, $l$ ne divise pas $f_0$, donc on la possibilité d'avoir des isogénies horizontales. Si $0 < i$, alors il est impossible d'avoir des isogénies horizontales au niveau $i$ car $l$ divise $f_i = lf_{i-1}$ (par application de la proposition 4.5).

## Proposition 4.7

*Si* $\Delta_i < -4$, *alors* $\frac{h_{\Delta_{i+1}}}{h_{\Delta_i}} = l - \left(\frac{\Delta_i}{l}\right)$

## Conséquence 4.1

*Dans un graphe d'isogénies de degré l, tout nœuds est relié à* $l+1$ *autres nœuds (pas forcement distincts)*

## Proof.

Au niveau 0, le nombre de liaisons d'un nœud est égal nombre de liaisons horizontales $1 + \left(\frac{\Delta_0}{l}\right)$ plus le nombre de liaisons descendantes $\frac{h_{\Delta_1}}{h_{\Delta_0}} = l - \left(\frac{\Delta_0}{l}\right)$. On a donc en tout

$$1 + \left(\frac{\Delta_0}{l}\right) + l - \left(\frac{\Delta_0}{l}\right) = l + 1$$

Au niveau $i > 0$, il y 0 liaison horizontale, 1 liaison verticale et $\frac{h_{\Delta_{i+1}}}{h_{\Delta_i}} = l - \left(\frac{\Delta_i}{l}\right) = l - 0 = l$ car $l$ divise $\Delta_i$ pour $i > 0$. On a donc en tout $l+1$ liaisons. □

# Après combien de niveaux s'arrête t-on?

Nous avons vu que pour que $H_\Delta(X)$ se décompose entièrement sur $\mathbb{F}_p[X]$, il suffit qu'il existe deux entiers $t$ et $v$ tels que $4p = t^2 - v^2\Delta$ et $t \neq\equiv 0 \mod p$ (d'après la proposition 4.2). Ainsi, pour s'assurer qu'il existe effectivement $h_{\Delta_i}$ courbes elliptiques sur $\mathbb{F}_p$ d'anneau d'endomorphisme $\mathcal{O}_i$, il faut et il suffit que $H_{\Delta_i}(X)$ se décompose entièrement sur $\mathbb{F}_p[X]$, c-à-d qu'il existe deux entiers $t_i$ et $v_i$ tels que $4p = t_i^2 - v_i^2\Delta_i$ et $t_i \neq\equiv 0 \mod p$.

Toutes les courbes situées sur un graphe sont isogènes deux à deux, et ont dont le même nombre de points (d'après le théorème de Tate); leurs morphismes de Frobenius ont donc la même trace $t = t_i, \forall i$.

Nous avons vu au début de l'exposé que

$$4p = t^2 - D_\pi = t^2 - f_\pi^2\Delta_\pi$$

Donc tous les $\Delta_i$ sont des diviseurs de $D_\pi$ (ou bien $f_i | f_\pi$).
Si $d = v_l(f_\pi)$, alors $f_\pi = l^d v$ avec $l \wedge v = 1$; et $D_\pi = l^{2d}v^2\Delta_\pi$.
Alors le graphe s'arrête au niveau $d$ et

$$\forall i = 1, ..., d; \quad \Delta_i = l^{2i}\Delta_0 = l^{2i}v^2\Delta_\pi \quad \text{et} \quad f_i = l^i f_0 = l^i v$$

## Exemple 16

*Avec un petit programme on peut déterminer plusieurs listes (p,t,v,$\Delta_\pi = -59$) vérifiant l'équation de la norme:* $4p = t^2 - f_\pi^2 \Delta_\pi$. *Parmi celles-ci, nous retenons les suivantes:*

- $p = 1201, t = 5, f_\pi = 9 = 3^2, l = 3$ *et* $d = 2$
- $p = 9221, t = 3, f_\pi = 25 = 5^2; l = 5$ *et* $d = 2$
- $p = 35597, t = 27, f_\pi = 49 = 7^2; l = 7$ *et* $d = 2$
- $p = 746749, t = 11, f_\pi = 225 = 3^2.5^2; l_1 = 3, l_2 = 5$ *et* $d_1 = d_2 = 2$

*Pour les trois premiers cas, on a un seul diviseur du conducteur* $f_\pi$ *et on a* $v_l(f_\pi) = 2$; *donc ce sont des graphes d'auteur 2. Et on a* $\mathcal{O}_0 = \mathcal{O}_K$ *car l est le seul diviseur de* $f_\pi$. *Au sommet, on aura donc* $h(-59) = 3$ *nœuds.*
*pour le dernier cas,* $f_\pi$ *a deux diviseurs premiers distincts* $l_1 = 3, l_2 = 5$. *on peut donc construire deux graphes. L'un est constitué des isogénies de degré 3, a pour de hauteur* $v_3(f_\pi) = 2$, *avec* $\mathcal{O}_0 \neq \mathcal{O}_K$ *(car* $\Delta_0 = 5^4(-59) \neq -59$*) et a* $h(5^4(-59)) = 60$ *nœuds au sommet. L'autre est constitué des isogénies de degré 5, a pour de hauteur* $v_5(f_\pi) = 2$, *avec* $\mathcal{O}_0 \neq \mathcal{O}_K$ *(car* $\Delta_0 = 3^4(-59) \neq -59$*) et a* $h(3^4(-59)) = 18$ *nœuds au sommet.*

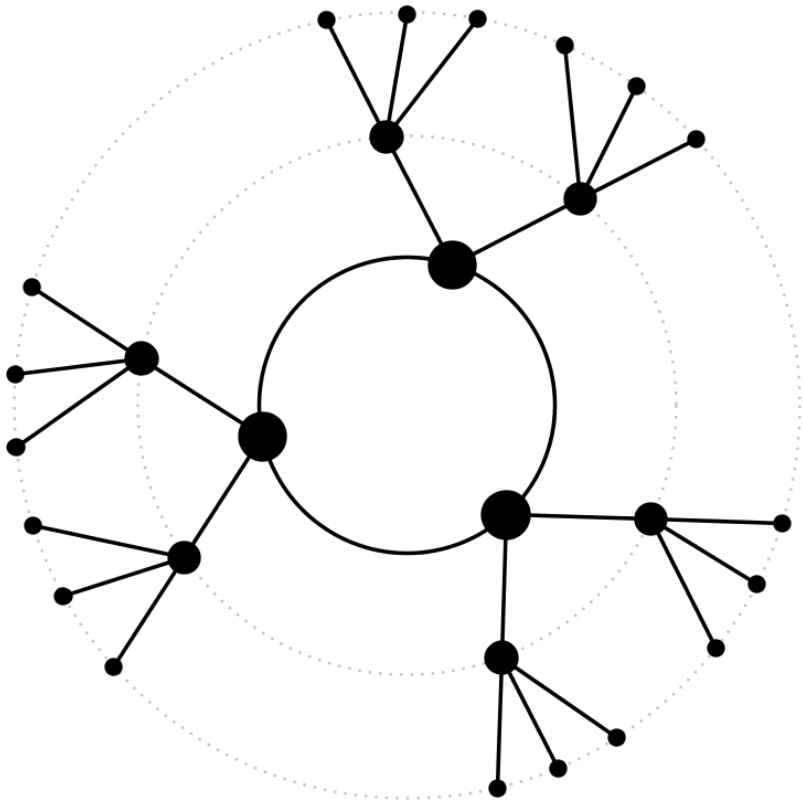
# $p = 1201, t = 5, f_\pi = 9 = 3^2, l = 3$ et $d = 2$

$K = \mathbb{Q}(\sqrt{-59})$

$\mathcal{O}_0 = \mathcal{O}_K$
$f_0 = 1$
$\Delta_0 = -59$
$h_{\Delta_0} = 3$

$\mathcal{O}_1$
$f_1 = 3$
$\Delta_1 = 3^2(-59)$
$h_{\Delta_1} = 6$

$\mathcal{O}_2 = \mathbb{Z}[\pi]$
$f_2 = f_\pi = 3^2$
$\Delta_2 = 3^4(-59) = D_\pi$
$h_{\Delta_2} = 18$



**Graphe d'isogénies de degré 3 sur $\mathbb{F}_{1201}$**
**$4 \times 1201 = 5^2\text{-}2^4(\text{-}59)$**

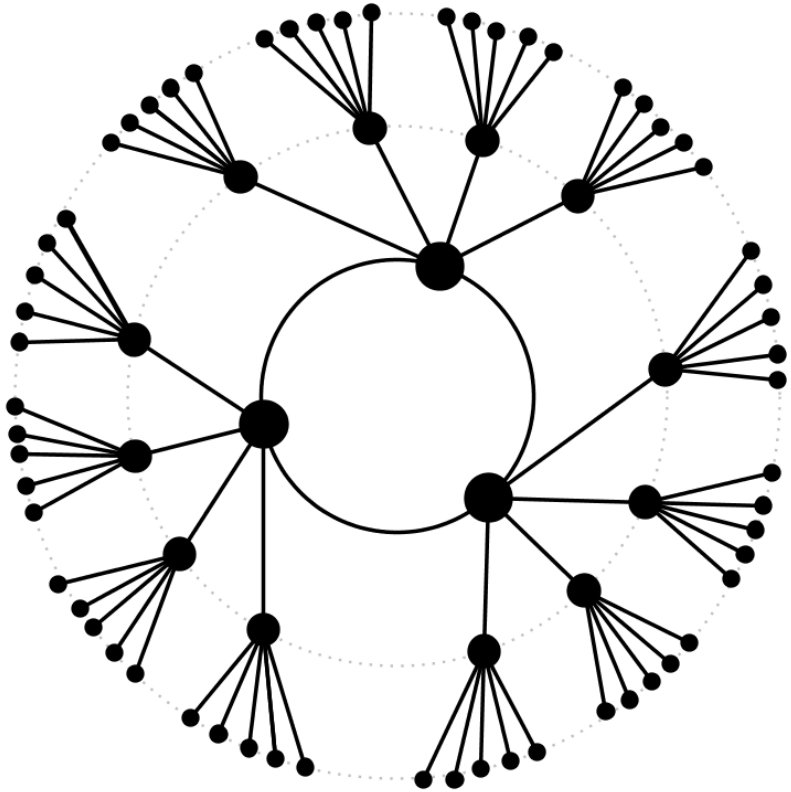
# $p = 9221, t = 3, f_\pi = 25 = 5^2; l = 5$ et $d = 2$

$K = \mathbb{Q}(\sqrt{-59})$

$\mathcal{O}_0 = \mathcal{O}_K$
$f_0 = 1$
$\Delta_0 = -59$
$h_{\Delta_0} = 3$

$\mathcal{O}_1$
$f_1 = 5$
$\Delta_1 = 5^2(-59)$
$h_{\Delta_1} = 12$

$\mathcal{O}_2 = \mathbb{Z}[\pi]$
$f_2 = f_\pi = 5^2$
$\Delta_2 = 5^4(-59) = D_\pi$
$h_{\Delta_2} = 60$



**Graphe d'isogénies de degré 5 sur $\mathbb{F}_{9221}$**
**$4 \times 9221 = 3^2\text{-}5^4(\text{-}59)$**

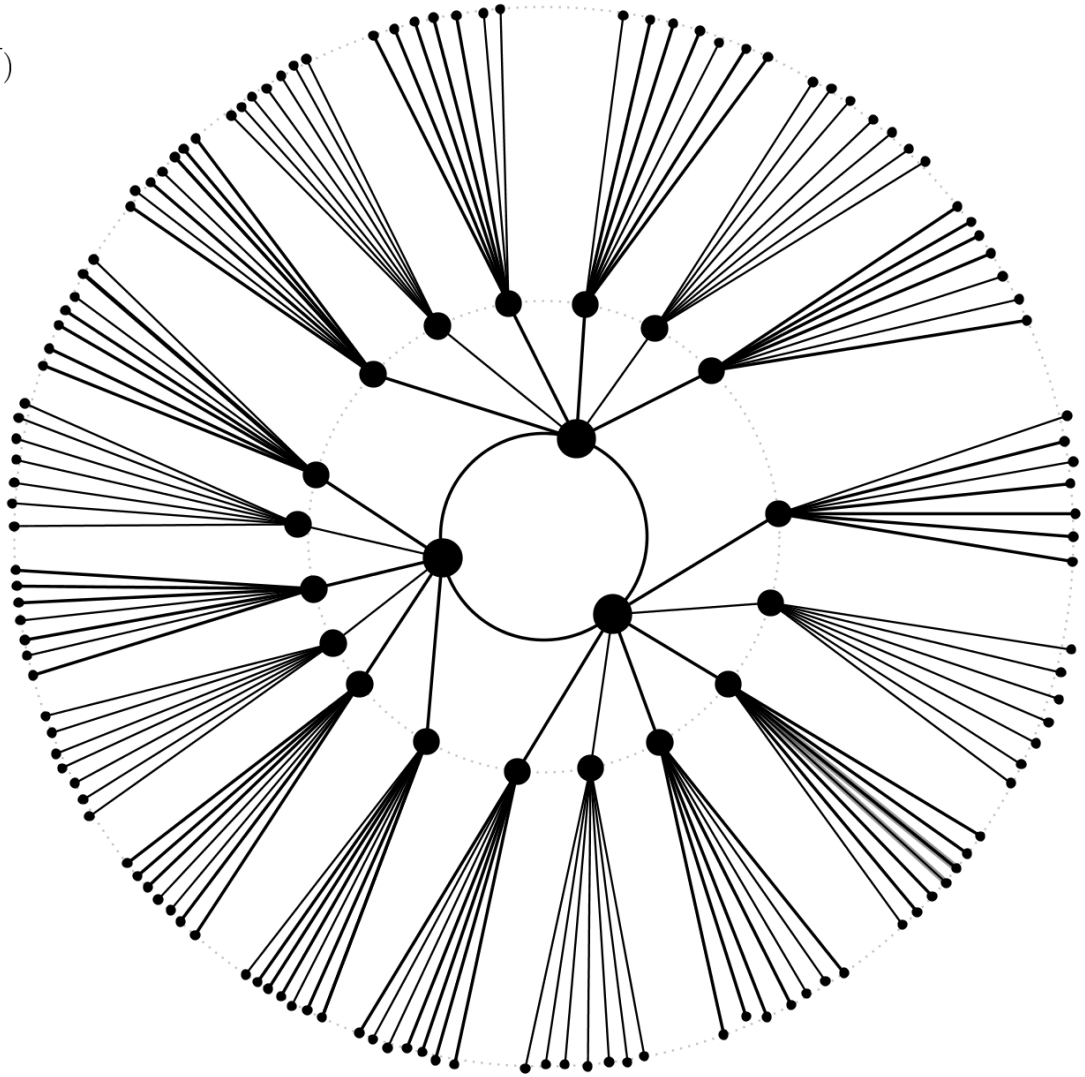
# $p = 35597, t = 27, f_\pi = 49 = 7^2; l = 7$ et $d = 2$

$K = \mathbb{Q}(\sqrt{-59})$

$\mathcal{O}_0 = \mathcal{O}_K$
$f_0 = 1$
$\Delta_0 = -59$
$h_{\Delta_0} = 3$

$\mathcal{O}_1$
$f_1 = 7$
$\Delta_1 = 7^2(-59)$
$h_{\Delta_1} = 18$

$\mathcal{O}_2 = \mathbb{Z}[\pi]$
$f_2 = f_\pi = 7^2$
$\Delta_2 = 7^4(-59) = D_\pi$
$h_{\Delta_2} = 126$



**Graphe d'isogénies de degré 7 sur $\mathbb{F}_{35597}$**
**$4 \times 35597 = 27^2\text{-}7^4(\text{-}59)$**

# $p = 746749, t = 11, f_\pi = 225 = 3^2.5^2; l_1 = 3, l_2 = 5$ et $d_1 = d_2 = 2$

$K = \mathbb{Q}(\sqrt{-59})$

$\mathcal{O}_0 \neq \mathcal{O}_K$
$f_0 = 5^2$
$\Delta_0 = 5^4(-59)$
$h_{\Delta_0} = 60$

$\mathcal{O}_1$
$f_1 = 3.5^2$
$\Delta_1 = 3^2.5^4(-59)$
$h_{\Delta_1} = 120$

$\mathcal{O}_2 = \mathbb{Z}[\pi]$
$f_2 = f_\pi = 3^2.5^2$
$\Delta_2 = 3^2.5^4(-59) = D_\pi$
$h_{\Delta_2} = 360$

**Graphe d'isogénies de degré 3 sur $\mathbb{F}_{746749}$**
**$4 \times 746749 = 11^2 - 3^4.5^4(-59)$**

$K = \mathbb{Q}(\sqrt{-59})$

$\mathcal{O}_0 \neq \mathcal{O}_K$
$f_0 = 3^2$
$\Delta_0 = 3^4(-59)$
$h_{\Delta_0} = 18$

$\mathcal{O}_1$
$f_1 = 5.3^2$
$\Delta_1 = 5^2.3^4(-59)$
$h_{\Delta_1} = 72$

$\mathcal{O}_2 = \mathbb{Z}[\pi]$
$f_2 = f_\pi = 3^2.5^2$
$\Delta_2 = 3^2.5^4(-59) = D_\pi$
$h_{\Delta_2} = 360$

**Graphe d'isogénies de degré 5 sur $\mathbb{F}_{746749}$**
**$4 \times 746749 = 11^2 - 3^4.5^4(-59)$**

## Partie 5: Cycles et étoiles d'isogénies

# Cycle d'isogénies

## Définition 5.1

*Un cycle d'isogénies est un graphe d'isogénies de hauteur* 0. *En d'autre termes, c'est un graphe d'isogénies qui ne comporte que des isogénies horizontales.*

Soit $\mathcal{O}$ un ordre de discriminant $\Delta$, $p$ un nombre premier, et t un entier tel que $4p = t^2 - \Delta$. Alors $H_\Delta(X)$ se décompose entièrement sur $\mathbb{F}_p[X]$. Soient $j_1, j_2, \cdots, j_{h_\Delta}$ les racines de $H_\Delta(X)$ dans $\mathbb{F}_p$ et $E_1, E_2, \cdots, E_{h_\Delta}$ les courbes elliptiques correspondantes. Soit $l$ un nombre premier distinct de $p$; alors d'après la proposition 4.2 de l'exposé précédent, un cycle d'isogénies de degré $l$ existe entre les $E_i$ si et seulement si $\left(\frac{\Delta}{l}\right) = 1$.
Ayant déjà les $j$-invariants $j_1, j_2, \cdots, j_{h_\Delta}$, il faut déterminer les arrêtes du cycle. Pour cela, on utilise le polynôme modulaire d'ordre $l$, $\Phi_l(X, Y)$, dont $\Phi_l(j_a, j_b) = 0$ si et seulement $j_a$ et $j_b$ sont les $j$-invariants de deux courbes $l$-isogènes. Lorsque $\left(\frac{\Delta}{l}\right) = 1$, $\Phi_l(X, j_i)$ admet exactement deux racines dans $\mathbb{F}_p$, ces racines sont les voisins de $j_i$ dans le cycle.

## Exemple 17

*Pour* $\Delta = -251$, $t = 9$ *et* $p = 83$, *l'équation de la norme est vérifiée:*
$4 \times 83 = 332 = 81 + 251 = 9^2 - (-251)$.
*On a* $h_{-251} = 7$ *et dans* $\mathbb{F}_{83}$,

$$\begin{aligned} H_{-251}(X) &= X^7 + 57X^6 + 44X^5 + 73X^4 + 19X^3 + 57X^2 + 40X + 60 \\ &= (X-15)(X-23)(X-29)(X-34)(X-48)(X-55)(X-71) \end{aligned}$$

*Donc* $j_1 = 15$; $j_2 = 23$; $j_3 = 29$; $j_4 = 34$; $j_5 = 48$; $j_6 = 55$; $j_7 = 71$

*Nous avons* $\left(\frac{\Delta}{2}\right) = \left(\frac{-251}{2}\right) = -1$, *donc il n'existe pas de cycle d'isogénies de degré 2.*
*Nous avons* $\left(\frac{\Delta}{3}\right) = \left(\frac{-251}{3}\right) = 1$ *et* $\left(\frac{\Delta}{5}\right) = \left(\frac{-251}{5}\right) = 1$, *donc il existe un cycle d'isogénies de degré 3 et un cycle d'isogénies de degré 5.*

**Cas** $l = 3$ **:**

*Dans* $\mathbb{F}_{83}$, *le polynôme modulaire d'ordre 3 est donné par (gp: polmodular()) :*

$$\begin{aligned} \Phi_3(X,Y) &= x^4 + y^4 + 82x^3y^3 + 74(x^3y^2 + y^2x^3) + 80(x^3y + xy^3) + 48(x^3 + y^3) \\ &\quad +81x^2y^2 + 40(x^2y + xy^2) + 21(x^2 + y^2) + 28xy + 29(x + y) \end{aligned}$$

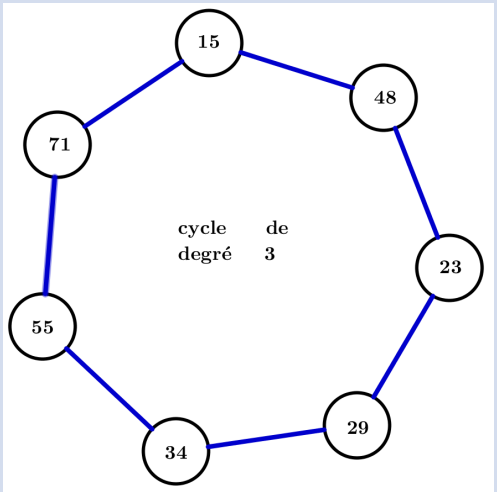
# Exemple 18

$$\begin{aligned}\Phi_3(X, j_1) &= \Phi_3(X, 15) &&= X^4 + 81X^3 + 8X^2 + 71X + 76 \\ &&&= (X - 48)(X - 71)(X^2 + 34X + 65)\end{aligned}$$

*Donc les voisins de* $j_1 = 15$ *dans le cycle sont* $j_5 = 48$ *et* $j_7 = 71$.

$$\begin{aligned}\Phi_3(X, j_5) &= \Phi_3(X, 48) &&= X^4 + 48X^3 + 80X^2 + 50X + 29 \\ &&&= (X - 15)(X - 23)(X^2 + 3X + 15)\end{aligned}$$

*Donc les voisins de* $j_5 = 48$ *dans le cycle sont* $j_1 = 15$ *et* $j_2 = 23$.
*Avec même processus, on obtient que les voisins de* $j_2 = 23$ *sont* $j_5 = 48$ *et* $j_3 = 29$, *ceux de* $j_3 = 29$ *sont* $j_2 = 23$ *et* $j_4 = 34$, *ceux de* $j_4 = 34$ *sont* $j_3 = 29$ *et* $j_6 = 55$ , *et en fin, ceux de* $j_6 = 55$ *sont* $j_4 = 34$ *et* $j_7 = 71$. *On aboutit au cycle suivant:*



## Exemple 19

***Cas*** $l = 5$ **:**

*Dans* $\mathbb{F}_{83}$*, le polynôme modulaire d'ordre* 5 *est donné par :*

$$\begin{aligned}\Phi_5(X,Y) = {} & x^6+y^6+82x^5y^5+68(x^5y^4+x^4y^5)+33(x^5y^3+x^3y^5)\\ & +75(x^5y^2+x^2y^5)+37(x^5y+xy^5)+21(x^5+y^5)+17x^4y^4\\ & +17(x^4y^3+x^3y^4)+6(x^4y^2+x^2y^4)+66(x^4y+xy^4)+34(x^4+y^4)\\ & +14x^3y^3+48(x^3y^2+x^2y^3)+72(x^3y+xy^3)+6(x^3+y^3)\\ & +14x^2y^2+11(x^2y+xy^2)+75(x^2+y^2)+32xy+25(x+y)+79\end{aligned}$$

$$\begin{aligned}\Phi_5(X,j_1) = \Phi_5(X,15) &= X^6+77X^5+33X^4+53X^3+43X^2+17X+15\\ &= (X-29)(X-34)(X^4+57X^3+65X^2+70X+40)\end{aligned}$$

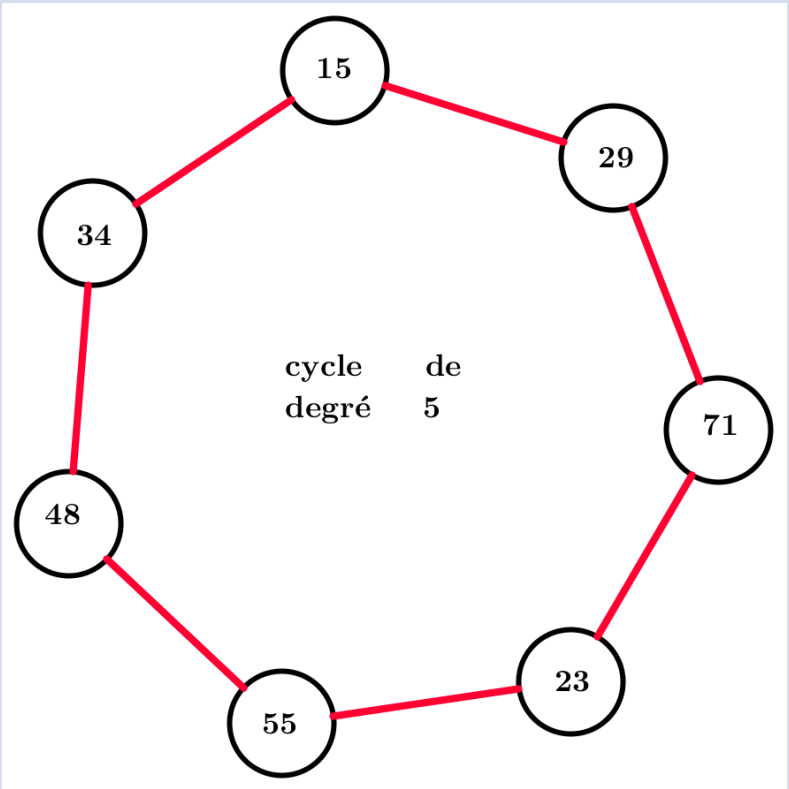
*Donc les voisins de* $j_1 = 15$ *dans le cycle sont* $j_3 = 29$ *et* $j_4 = 34$.

$$\begin{aligned}\Phi_5(X,j_3) = \Phi_5(X,29) &= X^6+67X^5+19X^4+27X^3+51X^2+11X+9\\ &= (X-15)(X-71)(X^4+70X^3+77X^2+76X+29)\end{aligned}$$

*Donc les voisins de* $j_3 = 29$ *dans le cycle sont* $j_1 = 15$ *et* $j_7 = 71$.

## Exemple 20

*Avec même processus, on obtient que les voisins de* $j_7 = 23$ *sont* $j_3 = 29$ *et* $j_2 = 23$, *ceux de* $j_2 = 23$ *sont* $j_7 = 71$ *et* $j_6 = 55$, *ceux de* $j_6 = 55$ *sont* $j_2 = 23$ *et* $j_5 = 48$, *et en fin, ceux de* $j_5 = 48$ *sont* $j_6 = 55$ *et* $j_4 = 64$. *On obtient donc le cycle suivant:*



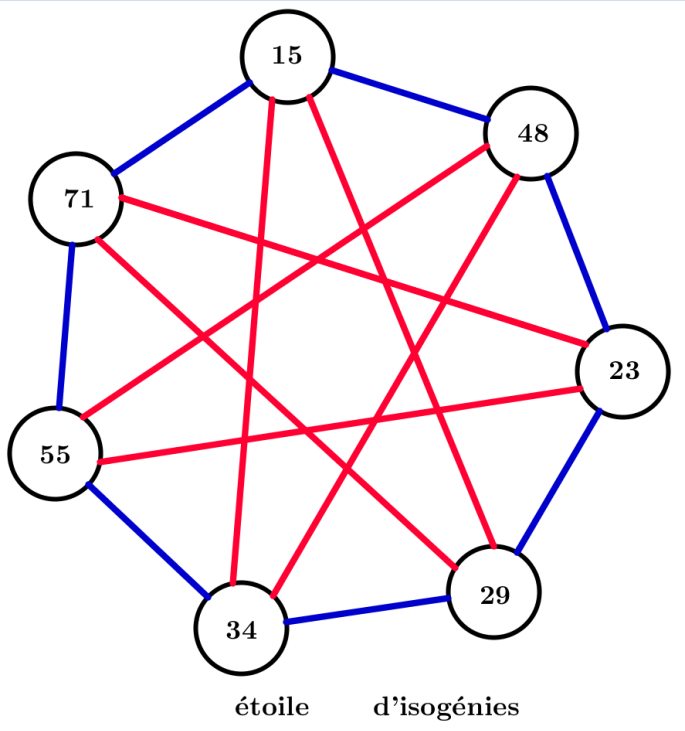
# Étoile d'isogénies

## Définition 5.2

*Un étoile d'isogénie est une superposition de plusieurs cycles d'isogénies faisant intervenir les même j-invariants.*

## Exemple 21

*En superposant les deux cycles précédents, on obtient l'étoile suivante :*



# Direction dans une étoile d'isogénies

Nous nous plaçons en une courbe $E$ d'un cycle $\mathcal{E}$ de degré $l$ défini sur un corps fini $\mathbb{F}_p$, $E$ est reliée à deux courbes $E_1$ et $E_2$. On veut une information qui permettra de savoir si l'on va de $E$ vers $E_1$ ou de $E$ vers $E_2$.

$$E_1 \quad \leftarrow I_1 - \quad E \quad -I_2 \rightarrow \quad E_2$$

Couveignes, Dawaghe et Morain proposent dans [4] l'utilisation de l'action du morphisme de Frobenius sur le noyau d'une isogénie.

# Construction d'un cycle à partir de la courbe E

Supposons que $E : y^2 = x^3 + Ax + B$ est définie sur $\mathbb{F}_p$, a pour $j$-invariant $j_0$ et que l'équation de la norme est vérifiée ($\Delta = t^2 - 4p$). Soit $l$ un nombre premier impair tel que $\left(\frac{\Delta}{l}\right) = 1$. Pour construire le cycle orienté de degré $l$, on peut procéder comme suit:

- Calculer le polynôme modulaire de degré $l$ $\phi_l(X, Y)$.
- Factoriser $\phi_l(X, j_0)$ dans $\mathbb{F}_p$ et choisir une racine $j_1$.
- Déterminer une courbe $E_1$ de $j$-invariant $j_1$.
- Déterminer une isogénie $I_1 : E \to E_1$.
- Reprendre les 4 étapes précédentes $h_\Delta - 1$ fois car après $h_\Delta$ reprises, on aura $E_{h_\Delta} = E$.
- ??? Determiner la direction du cycle !!

# Parcours dans une étoile d'isogénie

Soit $\mathcal{E}$ une étoile d'isogénies composée de $d$ cycles d'isogénies, dont l'ensemble des degrés est $L = \{l_i; 1 \leq i \leq d\}$.

## Définition 5.3

*un parcours dans $\mathcal{E}$ est la donnée d'une suite $R = \{r_i, 1 \leq i \leq d\}$ de $d$ entiers relatifs, où $r_i$ représente le nombre de pas faits dans le cycle de degré $l_i$.*

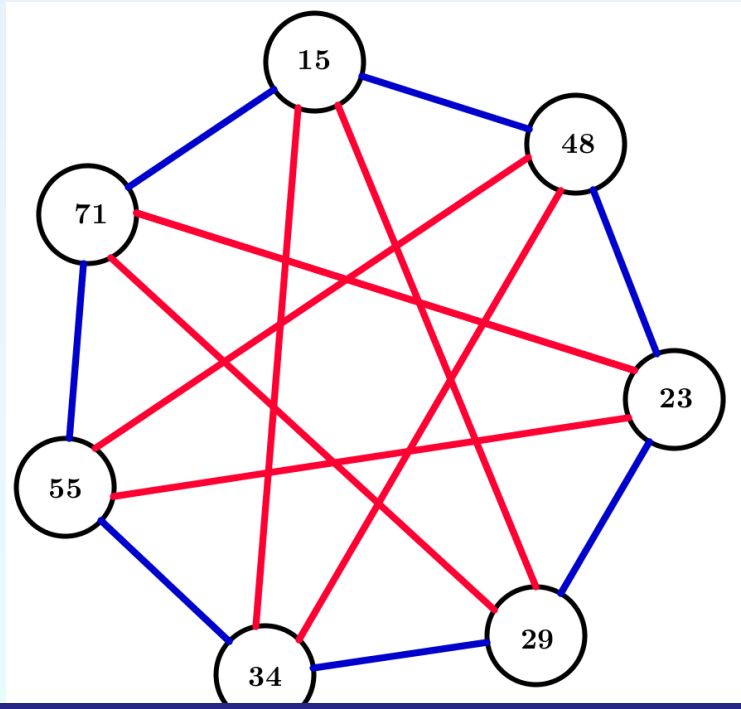
## Exemple de parcours

En considérant notre étoile comme ci contre, nous dirigeons tous nos cycle dans le sens trigonométrique.

Soit le parcours $R_1 = \{1, 3\}$, alors en commençant par le noeud 15, on a:

$$R_1(15) = 34, \text{ et le chemin suivi est :}$$

$$15 \to 71 \to 29 \to 15 \to 34$$



## Partie 6: Le crytosystème de Rostovtsev et Stolbunov

# Les paramètres et clés du système

**Paramètres du système:**

- $\mathbb{F}_p$: le corps de base, spécifié par $p$;
- $E_{init} : y^2 = x^3 + A_{init}x + B_{init}$ une courbe initiale spécifiée par $(A_{init}, B_{init})$;
- $d$ : le nombre de cycles d'isogénies utilisés dans l'étoile d'isogénie;
- $L = \{l_i; 1 \leq i \leq d\}$ : l'ensemble des degrés des cycles;
- $F = \{\pi_i; 1 \leq i \leq d\}$ : un ensemble constitué d'une valeur propre du morphisme de Frobénius dans chaque cycle (orientation des cycles);
- $k$ : le nombre limite de pas faits dans un cycle; tout parcours $R = \{r_i, 1 \leq i \leq d\}$ vérifie $|r_i| \leq k \; \forall i$.

**Clé privée:** un parcours $R_{priv}$;

**Clé publique:** une courbe $E_{pub} = R_{priv}(E_{init}) : y^2 = x^3 + A_{pub}x + B_{pub}$ spécifiée par $(A_{pub}, B_{pub})$.

# Schéma de chiffrement

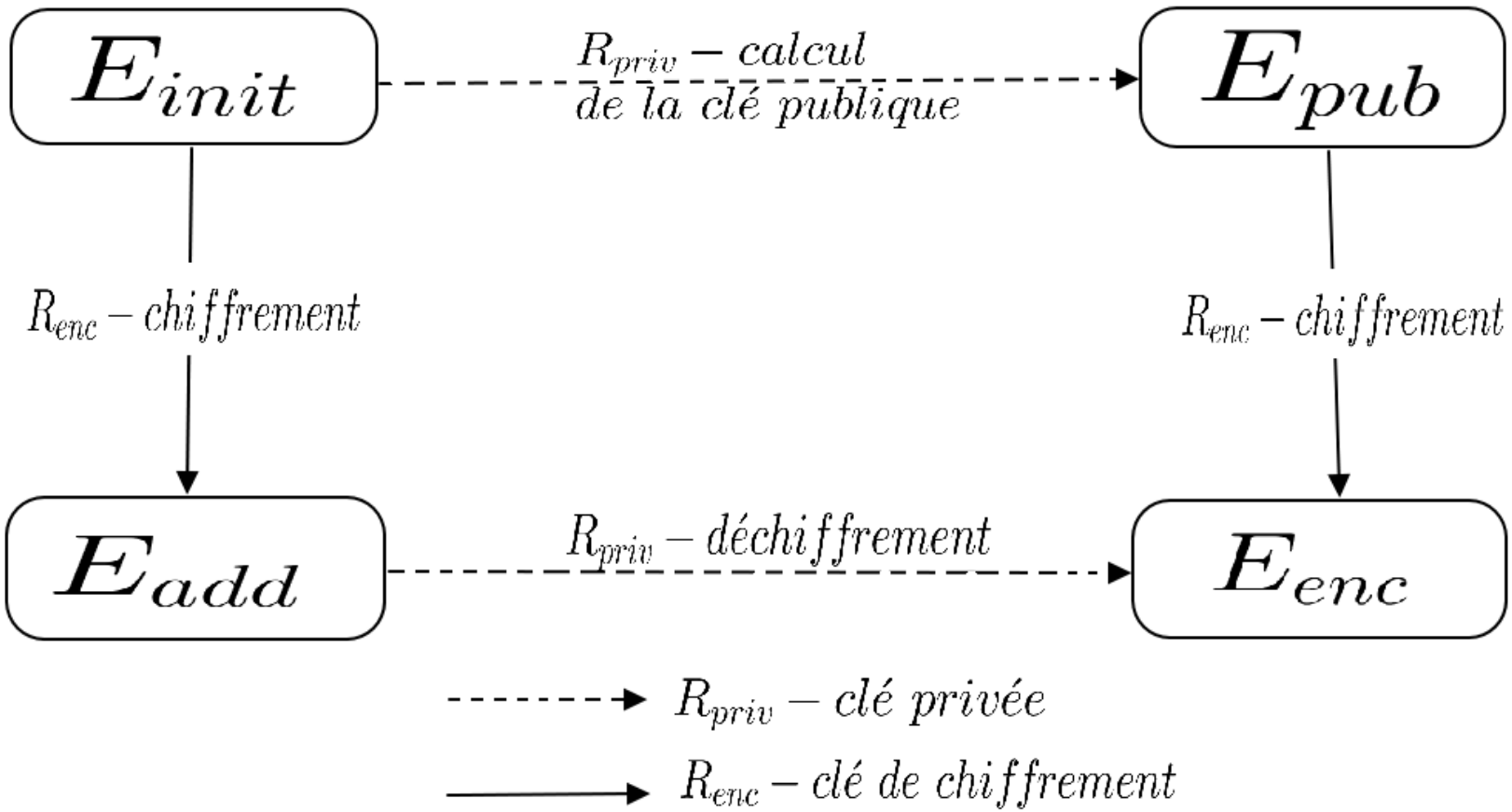



***Schéma de chiffrement***

# Chiffrement

**Entrées :**

- Les paramètres du cryptosystème;
- $E_{pub}$ spécifiée par $(A_{pub}, B_{pub})$;
- $m \in \mathbb{F}_p$ : le message clair;

**Algorithme:**

- Choisir aléatoirement un parcours $R_{enc} = \{r_i, 1 \leq i \leq d\}$, si $R_{enc} = \{0, 0, \cdots, 0, 0\}$, répéter cette étape;
- calculer $E_{enc} = R_{enc}(E_{pub})$;
- calculer le chiffré $c = m * j_{enc} \pmod{p}$;
- calculer $E_{add} = R_{enc}(E_{init})$;

**Sorties:**

- le chiffré $c$;
- $E_{add}$, spécifié par $(A_{add}, B_{add})$.

# Déchiffrement

**Entrées :**

- Les paramètres du cryptosystème;
- la clé privée $R_{priv}$;.
- le chiffré $c$;
- $E_{add}$, spécifié par $(A_{add}, B_{add}$.

**Algorithme:**

- calculer $E_{enc} = R_{priv}(E_{add})$;
- calculer le message clair $m = \frac{c}{j_{enc}} \pmod{p}$;

**Sortie:**

- le message clair $m$.

# Un petit exemple

Nous allons faire une illustration (sans point rationnel) en utilisant notre étoile conçu précédemment.

**Paramètres du système:**

- $\mathbb{F}_{83}$: ;
- $E_{init} : y^2 = x^3 + 70x + 81; j_{init} = 55;$
- $d = 2;$
- $L = \{3, 5\};$
- nous considérons le sens trigonométrique;
- $k = 2$ le nombre limite de pas faits dans un cycle;

**Clé privée:** $R_{priv} = \{2, -1\};$

**Calcul de la clé publique:** Nous omettons les calculs d'isogénies. En effet à ce niveau, on construit les portions des cycles à utiliser en utilisant la méthode décrite à la diapositive 5, afin d'avoir la courbe $E_{pub}$. Mais puisque nous avons déjà note cycle (ou du moins les $j$-invariants des courbes utilisées) et que nous avons

juste besoin du $j$-invariant dans le chiffrement sans point rationnel, nous déterminons rapidement $j_{pub}$. $E_{pub} = R_{priv}(E_{init})$ est une courbe de $j$-invariant $j_{pub} = R_{priv}(j_{init}) = R_{priv}(55) = 71$. Donc $E_{pub} : y^2 = x^3 + 25x + 33$

**Chiffrement:** Soit $m = 60$ le message clair

- $R_{enc} = \{1, 1\}$
- $j_{enc} = R_{enc}(j_{pub}) = R_{enc}(71) = 23$. Donc $E_{enc} : y^2 = x^3 + 34x + 24$
- le chiffré: $c = 52 = 60 * 23 \pmod{83}$
- $j_{add} = R_{enc}(j_{init}) = R_{enc}(55) = 48$. Donc $E_{add} : y^2 = x^3 + 58x + 54$

**déchiffrement:**

- $j_{enc} = R_{priv}(j_{add}) = R_{priv}(48) = 23$. Donc $E_{enc} : y^2 = x^3 + 34x + 24$
- le message clair: $m = 60 = \frac{52}{23} \pmod{83}$

# Sécurité du cryptosystème et attaques

La sécurité de ce cryptosystème est essentiellement basée dur la difficulté du calcul d'isogénies entre deux courbes elliptiques.....

# Sécurité du cryptosystème et attaques

Merci pour votre attention

# Bibliographie

[1] David Kohel, Endomorphisms rings of elliptic curves over finite fields, PhD thesis, Univ. Cali. 1996 [2] J.G.I. Noordsij, *Primes of the form* $x^2 + ny^2$, Bachelor Thesis, Mathematical Institute, Leiden University, June 2015.
[3] Johannes Buchmann, Ulrich Vollmer, *Binary Quadratic Forms, An Algorithmic Approach*, Springer.
[4] J. H. Silverman, *The arithmetic of elliptic curves*, second edition, Springer 2009
[5] Raza Ali Kazmi, *Isogenies and Cryptography*, A thesis in the departement of Computer Science and Software Engineering, Concordia University, September 2008.
[6] A. Bostan and F. Morain and B. Salvy AND E. Schost, Fast algorithms for computing isogenies between elliptic curves, 5 May 2006
[7] Alexander Rostovtsev and Anton Stolbunov, *Public key cryptosystem based on isogenies*, Saint-Petersburg State Polytech. Univ., Dept. of Sec. & Inf. Protec. in Computer System Russia.
[8] Couveignes J.M., Dewaghe L., Morain F., *Isogeny cycles and the Schoof-Elkies-Atkin algorithm*. Ecole polytechnique, France, 1996.
[9] Enea Milio, *Calcul de polynômes modulaires en dimension 2*, Thèse de Doctorat, Univ. Bordeaux, 2015.
[10] Luca De Feo, A lecture note on Isogeny-Based Crypto, Afr. Math. School, Senegal http://ema2017.lacgaa.com/cours/ (2017)