Agrégation externe de mathématiques — Sujet Lyon
Épreuve de modélisation, option C : Algèbre et Calcul Formel

COURBES ELLIPTIQUES ET CRYPTOGRAPHIE : MODÈLES ET EFFICACITÉ DU CALCUL

Résumé. Ce texte étudie la loi de groupe sur les courbes elliptiques à travers plusieurs modèles dans la perspective de leur utilisation en cryptographie. Partant du protocole de Diffie-Hellman et du choix des courbes elliptiques sur $\mathbb{F}_q$ comme support du logarithme discret, on présente la loi de groupe sur le modèle de Weierstrass, puis on discute l'efficacité du calcul pour chaque modèle : coordonnées jacobiennes, courbe de Montgomery, courbe d'Edwards tordue. On termine par l'algorithme de l'échelle de Montgomery pour le calcul de $[k]P$.

Mots-clés. Courbes elliptiques, corps finis, loi de groupe, logarithme discret, cryptographie.

Il est rappelé que le jury n'exige pas une compréhension exhaustive du texte. La présentation, bien que totalement libre, doit être organisée et le jury apprécie qu'un plan soit annoncé en préliminaire. L'exposé doit être construit en évitant la paraphrase et mettant en lumière les connaissances, à partir des éléments du texte. Il doit contenir des illustrations informatiques réalisées sur ordinateur, ou, à défaut, des propositions de telles illustrations. Des pistes de réflexion, indicatives et largement indépendantes les unes des autres, vous sont proposées en fin de texte.

1 Introduction

Soit $(G, \cdot)$ un groupe fini et $g \in G$ un élément d'ordre n. Le *protocole d'échange de clés de Diffie-Hellman* repose sur le schéma suivant : deux participants A et B souhaitent s'accorder sur un secret commun sans communication préalable. A choisit secrètement $a \in \{1, \dots, n-1\}$, calcule g^a et l'envoie à B ; B choisit secrètement b, calcule g^b et l'envoie à A. Chacun peut alors calculer g^{ab}, qui devient leur secret partagé. La sécurité du protocole repose sur la difficulté du *problème du logarithme discret* (DLP) dans G : étant donnés g et $h = g^a$, trouver a.

Le choix du groupe G est crucial. Le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$, où p est un nombre premier, est le candidat classique, mais il est vulnérable aux meilleures attaques connues, notamment le crible algébrique des corps de nombres, dont la complexité est sous-exponentielle en $\log p$. Cela impose des tailles de clés très importantes. En revanche, le groupe $E(\mathbb{F}_q)$ des points d'une courbe elliptique sur un corps fini $\mathbb{F}_q$ présente un avantage majeur : aucune attaque sous-exponentielle n'est connue pour le DLP elliptique (ECDLP) en général, ce qui permet d'obtenir un niveau de sécurité comparable avec des clés significativement plus courtes.

Dès lors, l'efficacité du calcul de la *multiplication scalaire* devient un enjeu central : c'est l'opération fondamentale de tout protocole basé sur les courbes elliptiques. Or, ce coût dépend fortement du *modèle* choisi pour représenter la courbe. L'objet de ce texte est de comparer, du point de vue du calcul formel, plusieurs modèles de courbes elliptiques et les formules de groupe qui leur sont associées.

2 Equation de Weierstrass et loi de groupe

2.1 Définition

Soit $\mathbb{K}$ un corps de caractéristique différente de 2 et de 3.

Définition 2.1. Une *courbe elliptique* sur $\mathbb{K}$ en forme de Weierstrass courte est définie par une équation de la forme

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{K},$$

avec la condition de non-singularité $\Delta = -16(4a^3 + 27b^2) \neq 0$. On note

$$E(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

l'ensemble des points de la courbe définis sur $\mathbb{K}$, où $\mathcal{O}$ est le *point à l'infini*.

2.2 Loi de groupe

La loi de groupe repose sur la règle corde-et-tangente : $P + Q + R = \mathcal{O}$ si et seulement si P, Q, R sont les trois points d'intersection d'une droite avec E, comptés avec multiplicité. Plus précisément, pour $P, Q \in E(\mathbb{K})$:

- $\mathcal{O}$ est l'élément neutre : $P + \mathcal{O} = P$ pour tout P.
- Si $P = (x, y)$, alors $-P = (x, -y)$. En particulier, $P + (-P) = \mathcal{O}$.
- Si $P \neq -Q$, on trace la droite D passant par P et Q (tangente en P si $P = Q$). Notons λ sa pente, x_1, y_1 (resp. x_2, y_2) les coordonnées de P (resp. Q). En substituant l'équation de D dans celle de E, on obtient un polynôme de degré 3 en x admettant x_1 et x_2 comme racines. Les formules de Vieta donnent la troisième racine $x_3 = \lambda^2 - x_1 - x_2$, et on pose $P + Q = -(x_3, \lambda(x_1 - x_3) - y_1)$.

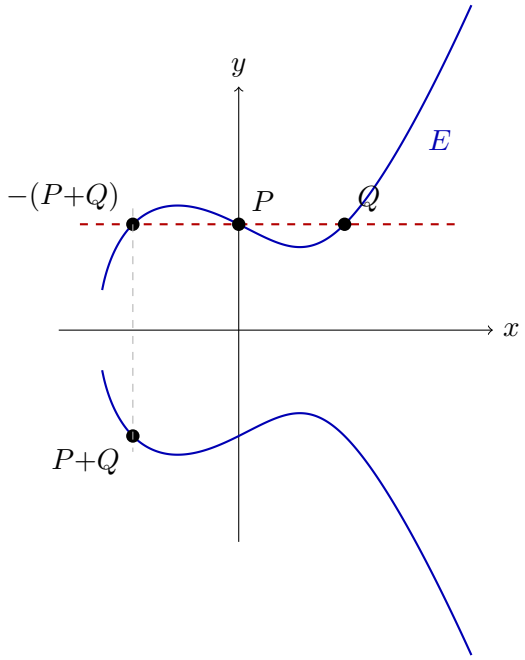

FIGURE 1 – Construction de $P + Q$ sur $E : y^2 = x^3 - x + 1$, avec $P = (0, 1)$, $Q = (1, 1)$, $P + Q = (-1, -1)$.

Proposition 2.2. *Muni de cette loi, $E(\mathbb{K})$ est un groupe abélien.*

La commutativité est immédiate par symétrie de la construction. La vérification de l'associativité est en revanche bien plus délicate, et peut être effectuée via un calcul formel.

2.3 Formules explicites en coordonnées affines

Soient $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ deux points de $E(\mathbb{K})$ distincts de $\mathcal{O}$. On pose

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{si } P_1 \neq P_2, \\ \dfrac{3x_1^2 + a}{2y_1} & \text{si } P_1 = P_2 \text{ (doublement).} \end{cases}$$

Dans les deux cas, le résultat $P_3 = (x_3, y_3) = P_1 + P_2$ est donné par :

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = \lambda(x_1 - x_3) - y_1.$$

Exemple 2.3. Sur la courbe $y^2 = x^3 - x + 1$ avec $P = (0, 1)$ et $Q = (1, 1)$: $\lambda = 0$, $x_3 = -1$, $y_3 = -1$, soit $P + Q = (-1, -1)$.

Le coût d'une addition est $1\mathrm{I} + 2\mathrm{M} + 1\mathrm{S}$ et celui d'un doublement est $1\mathrm{I} + 2\mathrm{M} + 2\mathrm{S}$, où I, M et S désignent respectivement le coût d'une inversion, d'une multiplication et d'un carré dans $\mathbb{F}_q$. Or l'inversion dans $\mathbb{F}_q$ est significativement plus coûteuse qu'une multiplication, ce qui rend ces formules peu adaptées à un usage intensif.

Dans la suite, on se place sur un corps fini $\mathbb{K} = \mathbb{F}_q$ où $q = p^r$ est une puissance d'un nombre premier $p > 3$.

3 Coordonnées jacobiennes

3.1 Motivation

Définition 3.1. Pour $P \in E(\mathbb{K})$ et $k \in \mathbb{Z}$, on définit la *multiplication scalaire* $[k]P$ par $[0]P = \mathcal{O}$, $[1]P = P$, $[k]P = P + [k-1]P$ pour $k \geq 2$, et $[k]P = [-k](-P)$ pour $k < 0$.

Pour calculer $[k]P$ avec k un entier de 256 bits, l'algorithme classique de multiplication scalaire effectue environ 384 opérations de groupe. En coordonnées affines, chacune requiert une inversion dans $\mathbb{F}_q$, soit au total plusieurs centaines d'inversions — un coût prohibitif en pratique. Les *coordonnées jacobiennes* permettent d'éviter les inversions au prix de quelques multiplications supplémentaires, en ne réalisant qu'une seule inversion à la toute fin du calcul.

3.2 Définition et formules

On représente un point affine $(x, y) \in E(\mathbb{K})$ par un triplet $(X : Y : Z)$ avec $Z \neq 0$ via $x = X/Z^2$ et $y = Y/Z^3$. Ainsi, deux triplets $(X : Y : Z)$ et $(X' : Y' : Z')$ représentent le même point si et seulement si $(X', Y', Z') = (\lambda^2 X, \lambda^3 Y, \lambda Z)$ pour un certain $\lambda \neq 0$: le représentant d'un point affine (x, y) n'est donc pas unique. Le représentant canonique $(x : y : 1)$ permet de retrouver les coordonnées affines. Le point à l'infini $\mathcal{O}$ est représenté par les triplets de la forme $(\lambda^2 : \lambda^3 : 0)$, dont le représentant canonique est $(1 : 1 : 0)$. En substituant $x = X/Z^2$, $y = Y/Z^3$ dans l'équation de E, on obtient l'équation de E en coordonnées jacobiennes :

$$Y^2 = X^3 + aXZ^4 + bZ^6.$$

Les formules de **doublement** $(X_1 : Y_1 : Z_1) \mapsto (X_3 : Y_3 : Z_3)$, valables pour $Y_1 \neq 0$, sont :

$$\begin{aligned} A &= 4X_1Y_1^2, \quad B = 3X_1^2 + aZ_1^4, \\ X_3 &= B^2 - 2A, \quad Y_3 = B(A - X_3) - 8Y_1^4, \quad Z_3 = 2Y_1Z_1. \end{aligned}$$

Coût : $4\mathrm{M} + 6\mathrm{S}$.

Les formules d'**addition** $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = (X_3 : Y_3 : Z_3)$, pour $P_1 \neq \pm P_2$, sont :

$$U_1 = X_1 Z_2^2, \quad U_2 = X_2 Z_1^2, \quad S_1 = Y_1 Z_2^3, \quad S_2 = Y_2 Z_1^3, H = U_2 - U_1, \quad R = S_2 - S_1,$$
$$X_3 = R^2 - H^3 - 2U_1 H^2, \quad Y_3 = R(U_1 H^2 - X_3) - S_1 H^3, \quad Z_3 = H Z_1 Z_2.$$

Coût : 12M + 4S.

À l'issue du calcul de $[k]P$, une unique inversion permet de revenir en coordonnées affines.

4 Equation de Montgomery

4.1 Définition et condition d'existence

Définition 4.1. Une *équation de Montgomery* sur $\mathbb{F}_q$ est une équation de la forme

$$M_{A,B} : Bv^2 = u^3 + Au^2 + u, \quad A, B \in \mathbb{F}_q, \quad B(A^2 - 4) \neq 0.$$

Une courbe elliptique E définie sur $\mathbb{F}_q$ admet une équation de Montgomery si et seulement si $E(\mathbb{F}_q)$ contient un point d'ordre 4.

Proposition 4.2. *Soit $E : y^2 = x^3 + ax + b$ avec un point d'ordre 2, $(\alpha, 0) \in E(\mathbb{F}_q)$. Notons $\beta = 3\alpha^2 + a$. Si β est un carré non nul dans $\mathbb{F}_q$, disons $\beta = s^2$, alors le changement de variables*

$$x = sU + \alpha, \qquad y = sV$$

transforme l'équation de E en une équation de Montgomery $M_{A,B}$ avec

$$A = \frac{3\alpha}{s}, \qquad B = \frac{1}{s}.$$

Remarque 4.3. On peut vérifier que l'équation obtenue satisfait bien la condition de non-singularité $B(A^2 - 4) \neq 0$.

La condition $\beta = s^2$ est équivalente à l'existence d'un point d'ordre 4 dont la carré est $(\alpha, 0)$ dans $E(\mathbb{F}_q)$.

4.2 Arithmétique sur la coordonnée x

Une courbe elliptique donnée par une équation de Montgomery $M_{A,B}$ admet une propriété remarquable : pour calculer la coordonnée x du point $[k]P$, il n'est pas nécessaire de connaître les coordonnées y. En coordonnées jacobiennes $(X : * : Z)$ avec $x = X/Z$, si l'on connaît $x(P) = X_P/Z_P$, $x([n]P) = X_n/Z_n$ et $x([n+1]P) = X_{n+1}/Z_{n+1}$, on calcule $x([2n]P)$ et $x([2n+1]P)$ par les formules suivantes.

Doublement (xDBL) :

$$c = (A+2)/4, \quad u = (X_n + Z_n)^2, \quad v = (X_n - Z_n)^2, \quad w = u - v$$
$$X_{2n} = uv, \quad Z_{2n} = w(v + c\,w)\,.$$

Coût : 3M + 2S.

Addition différentielle (xADD) :

$$u = (X_n - Z_n)(X_{n+1} + Z_{n+1}), \quad v = (X_n + Z_n)(X_{n+1} - Z_{n+1})$$
$$X_{2n+1} = Z_P\,(u+v)^2, \qquad Z_{2n+1} = X_P\,(u-v)^2.$$

Coût : 4M + 2S.

Ces formules ne requièrent ni inversion ni coordonnée y.

5 Equation d'Edwards tordue

5.1 Définition et loi d'addition complète

Définition 5.1. Une *équation d'Edwards tordue* sur $\mathbb{F}_q$ est une équation de la forme

$$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2,$$

avec $a \in (\mathbb{F}_q^*)^2$ et $d \in \mathbb{F}_q^* \setminus (\mathbb{F}_q^*)^2$.

Remarque 5.2. Puisque a est un carré, il existe $s \in \mathbb{F}_q^*$ tel que $s^2 = a$ et le point $(s^{-1}, 0)$ appartient à $E_{a,d}$; on vérifie que $[2](s^{-1}, 0) = (0, -1)$ et donc que ce point est d'ordre 4. Réciproquement, une courbe elliptique sur $\mathbb{F}_q$ admet une équation d'Edwards tordue si et seulement si elle possède un point d'ordre 4 dans $E(\mathbb{F}_q)$.

L'intérêt majeur de ce modèle est que la loi d'addition est *complète*, c'est-à-dire valable sans exception pour tous les points de $E_{a,d}(\mathbb{F}_q)$.

Théorème 5.3. *Pour $P_i = (x_i, y_i) \in E_{a,d}(\mathbb{F}_q)$, la loi*

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

définit une structure de groupe abélien sur $E_{a,d}(\mathbb{F}_q)$. L'élément neutre est $(0, 1)$ et l'opposé de (x, y) est $(-x, y)$.

Remarque 5.4. La preuve de ce théorème est technique : elle nécessite notamment le fait que les dénominateurs $1 \pm dx_1x_2y_1y_2$ ne s'annulent jamais sur $E_{a,d}(\mathbb{F}_q)$.

L'absence de cas particuliers est une propriété précieuse en implémentation : elle simplifie le code et évite les vulnérabilités liées à la gestion de cas dégénérés.

Exemple 5.5. Sur $\mathbb{F}_{101}$, on prend $a = 1$ et $d = 2$. Le point $P = (1, 0)$ appartient à $E_{1,2}(\mathbb{F}_{101})$, vérifie $[2]P = (0, -1)$ et est d'ordre 4.

5.2 Correspondance birationnelle avec Montgomery

Théorème 5.6. *La courbe elliptique définie par l'équation de Montgomery $M_{A,B}$ est birationnellement équivalente sur $\mathbb{F}_q$ à la courbe elliptique définie par l'équation d'Edwards tordue $E_{a,d}$ avec*

$$a = \frac{A + 2}{B}, \qquad d = \frac{A - 2}{B}.$$

La correspondance est donnée par les applications rationnelles réciproques :

$$\varphi : M_{A,B} \to E_{a,d}, \qquad (u, v) \mapsto \left(\frac{u}{v}, \frac{u - 1}{u + 1} \right),$$

$$\psi : E_{a,d} \to M_{A,B}, \qquad (x, y) \mapsto \left(\frac{1 + y}{1 - y}, \frac{1 + y}{(1 - y)x} \right).$$

De plus, φ est un isomorphisme de groupes là où elle est définie.

Exemple 5.7. Sur $\mathbb{F}_{1009}$, considérons la courbe d'équation $M_{13,1}$. La condition $B(A^2 - 4) = 165 \neq 0$ est bien vérifiée. La correspondance donne

$$a = \frac{A + 2}{B} = 15, \qquad d = \frac{A - 2}{B} = 11.$$

On vérifie que $a = 15 = 32^2$ est un carré dans $\mathbb{F}_{1009}$, et que $d = 11$ est un non-carré dans $\mathbb{F}_{1009}$. La courbe définie par $M_{13,1}$ est donc birationnellement équivalente à la courbe définie par $E_{15,11}$ sur $\mathbb{F}_{1009}$.

6 Algorithme de l'échelle de Montgomery

Les formules de la section 4.2 permettent de calculer $x([k]P)$ à partir de $x(P)$ sans jamais avoir recours à la coordonnée y ni à une inversion dans $\mathbb{F}_q$. L'algorithme de l'échelle de Montgomery exploite cette propriété pour calculer $x([k]P)$ de façon efficace et résistante aux attaques par canaux auxiliaires.

Soit $k \geq 1$ un entier. On note $k = \sum_{i=0}^{m} k_i 2^i$ son écriture binaire avec $k_m = 1$. L'algorithme suivant calcule $x([k]P)$ en maintenant un invariant de boucle : on a toujours

$$(R_0, R_1) = (x([j]P),\, x([j{+}1]P))$$

où $j = \lfloor k/2^{i+1} \rfloor$.

`Algorithme de l'échelle de Montgomery`

`1.` $R_0 \leftarrow x(P)$; $R_1 \leftarrow \mathrm{xDBL}(x(P))$

`2. pour` i `de` $m{-}1$ `à` 0 `:`

`(a) si` $k_i = 0$ `:`

$R_1 \leftarrow \mathrm{xADD}(R_0, R_1, x(P))$; $R_0 \leftarrow \mathrm{xDBL}(R_0)$

`sinon :`

$R_0 \leftarrow \mathrm{xADD}(R_0, R_1, x(P))$; $R_1 \leftarrow \mathrm{xDBL}(R_1)$

`3. renvoyer` R_0

À chaque itération, on effectue exactement une addition différentielle et un doublement, quel que soit le bit k_i. La séquence d'opérations est donc *uniforme* : elle ne dépend pas de la valeur de k. Cela confère à l'algorithme une résistance naturelle aux *attaques par canaux auxiliaires* (timing attacks, simple power analysis), qui exploitent les variations du temps d'exécution ou de la consommation électrique pour en déduire les valeurs secrètes.

Proposition 6.1. *L'algorithme de l'échelle de Montgomery calcule $x([k]P)$ en utilisant m doublements et m additions différentielles, soit $m(7\mathrm{M} + 4\mathrm{S})$ opérations dans $\mathbb{F}_q$, plus une inversion finale.*

Suggestions et pistes de réflexion

Les pistes de réflexion suivantes ne sont qu'indicatives et il n'est pas obligatoire de les suivre. Vous pouvez choisir d'étudier, ou non, certains des points proposés, de façon plus ou moins approfondie, mais aussi toute autre question à votre initiative. Vos investigations comporteront une partie traitée sur ordinateur et, si possible, des représentations graphiques de vos résultats. À défaut, si vos illustrations informatiques n'ont pas abouti, il est conseillé d'expliquer ce que vous auriez souhaité mettre en œuvre.

- On pourra compléter les preuves des diverses assertions du texte.
- Vérifier symboliquement l'associativité de la loi de groupe sur une courbe donné par une équation de Weierstrass courte.
- Écrire des fonctions permettant de convertir un point entre différents modèles : de Weierstrass affine vers coordonnées jacobiennes, de Weierstrass vers Montgomery via la transformation de la section 4.1 (sous réserve d'un point d'ordre 4), de Montgomery vers Edwards via la correspondance φ de la section 5.2.
- Implémenter et comparer expérimentalement le coût du calcul de $[k]P$ pour différents modèles.
- Vérifier la correspondance birationnelle entre $M_{A,B}$ et $E_{a,d}$, en vérifiant que φ est un morphisme de groupes.
- Prouver la proposition 6.1 : établir l'invariant de boucle de l'algorithme de l'échelle de Montgomery et en déduire que $R_0 = x([k]P)$ à la fin de l'algorithme.
- Implémenter l'échelle de Montgomery et comparer son efficacité de manière expérimentale avec une multiplication scalaire naïve.