1 Courbes elliptiques

Dans la suite K désignera un corps commutatif.

1.1 Définition

Définition 1 (Courbe elliptique)**.**

On appelle équation de Weierstrass sur K une équation du type

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

avec $a_i \in K$. Une courbe donnée par une telle équation est dite lisse si le système suivant n'admet pas de solution

$$\begin{cases} a_1y = 3x^2 + 2a_2x + a_4 \\ 2y + a_1x + a_3 = 0 \end{cases}$$

autrement dit si les dérivées partielles en x et en y de

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

ne s'annulent pas en même temps. Une courbe elliptique E définie sur K est une courbe lisse donnée par une équation de Weierstrass définie sur K à laquelle on a ajouté un point noté $\mathcal{O}$, qu'on appelle « point à l'inifini » ;

$$E = \left\{(x, y) \in \bar{K}^2 \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\right\} \cup \{\mathcal{O}\}$$

Définition 2 (Ensemble de points K-rationnels)**.**

Les points de la courbe sur un corps K' (contenant K) ont pour coordonnées les solutions (x, y) dans K' de l'équation E ; on y joint un point à l'infini. On note cet ensemble de points $E(K')$, et on les appelle les points K-rationnels.

Remarque 1.

Lorsque K est un corps, $\bar{K}$ désigne une clôture algébrique de K. Une clôture algébrique d'un corps commutatif K est une extension algébrique L de K qui est algébriquement close, c'est-à-dire telle que tout polynôme de degré supérieur ou égal à un, à coefficients dans L, admet au moins une racine dans L.

Proposition 1 (Équation réduite)**.**

Si la caractéristique de K, $\text{char}(K))$ n'est pas 2 ni 3, alors en faisant les deux changements de variables successifs $y \to 1/2\,(y - a_1x - a_3)$ et ensuite $(x, y) \to ((x - 3b_2)/36, y/216)$ dans E, où $b_2 = a_1^2 + 4a_2$, nous obtenons

$$E : y^2 = x^3 - 27c_4x - 54c_6$$

avec $b_4 = 2a_4 + a_1a_3, b_6 = a_3^2 + 4a_6, c_4 = b_2^2 - 24b_4, c_6 = -b_2^3 + 36b_2b_4 - 216b_6$. Ainsi si $\text{char}(K) \notin \{2, 3\}$, nous pouvons toujours travailler avec des courbes elliptiques de la forme :

$$E : y^2 = x^3 + ax + b$$

Dans ce cas la courbe est lisse si et seulement si :

$$4a^3 + 27b^2 \neq 0$$

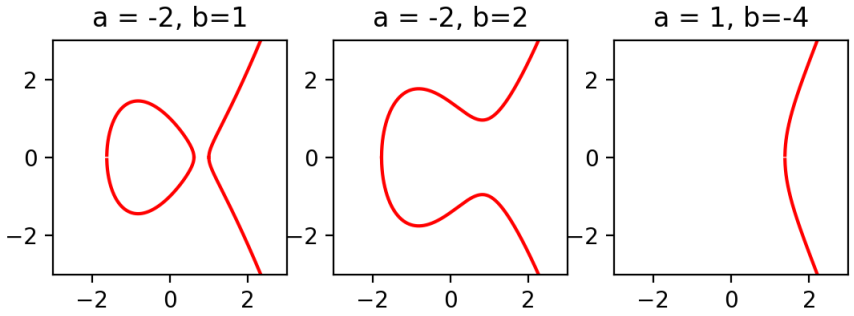


FIGURE 1 – $E(\mathbb{R})$ avec $y^2 = x^3 + ax + b$.

1.2 Loi de groupe

Proposition 2 (Structure de groupe des points rationnels)**.**

Soient E une courbe elliptique définie sur un corps K, et deux points $P, Q \in E(K)$, L la droite reliant P à Q (la tangente à E si $P = Q$) et R le troisième point d'intersection de L avec E. Soit L' la droite verticale passant par R. On définit $P + Q \in E(K)$ comme étant le deuxième point d'intersection de L' avec E.
Muni de cette loi de composition $(E(K), +)$ est un groupe abélien dont l'élément neutre est le point à l'infini $\mathcal{O}$.

Remarque 2.

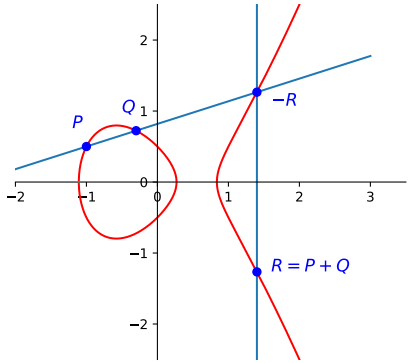
Nous allons donner les formules d'additions effectives dans le groupe $(E(K), +)$ dans le cas de coordonnées affines. Dans la pratiques on préfère utiliser les coordonnées projectives qui permettent de « cumuler » les inversions pour n'en opérer qu'une à la fin du calcul, car l'inversion est très coûteuse.

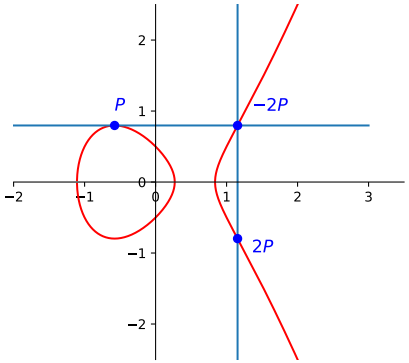
Proposition 3 (Calcul de la somme de deux points d'une courbe elliptique.)**.**

Soient $E : y^2 = x^3 + ax + b$ une courbe elliptique et $P = (x_1, y_1), Q = (x_2, y_2)$ des points de E, avec P, Q différent de $\mathcal{O}$. On a $P+Q = R = (x_3, y_3)$ avec :

1. Si $x_1 \neq x_2$, alors
$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{avec } m = \frac{y_2 - y_1}{x_2 - x_1}$$
2. Si $x_1 = x_2$ mais $y_1 \neq y_2$, alors $R = \mathcal{O}$.
3. Si $P = Q$ et $y_1 \neq 0$, alors
$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{avec } m = \frac{3x_1^2 + a}{2y_1}.$$
4. Si $P = Q$ et $y_1 = 0$, alors $R = \mathcal{O}$.

De plus, on a
$$P + \mathcal{O} = P$$
pour tout P sur E.

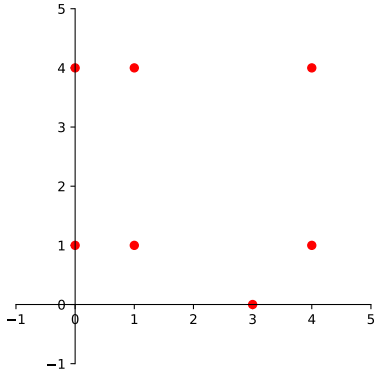




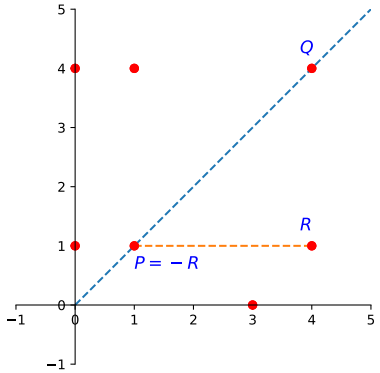
2 Courbe elliptique sur un corps fini

2.1 Un exemple

Sur $\mathbb{F}_5$ la courbe elliptique d'équation $y^2 = x^3 + 4x + 1$, on a l'ensemble de point :



Ca ne ressemble plus vraiment à une courbe et pourtant. La loi de groupe est la même :



2.2 Points rationnels sur un corps fini

Théorème 1 (Structure du groupe$E(\mathbb{F}_q)$)**.**

Le groupe $E(\mathbb{F}_q)$ est :

- soit un groupe cyclique, $E(\mathbb{F}_q) \cong \mathbb{Z}/d_2\mathbb{Z}$ où $d_2 = |E(\mathbb{F}_q)|$.
- soit le produit de deux groupes cycliques :

$$E(\mathbb{F}_q) \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z},$$

où $d_1|d_2$ et $d_1|q-1$.

Théorème 2 (Hasse)**.**

Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$. Alors

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

Le Bitcoin utilise une courbe elliptique avec $a = 0$ et $b = 7$ [1] :

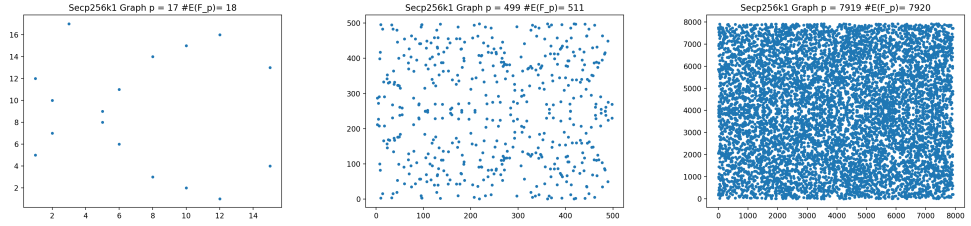


FIGURE 2 – Courbes Secp256k1 pour différentes valeurs de p

On peut affiner ce résultat :

1. Ici se trouve tous les détails : https ://safecurves.cr.yp.to/www.secg.org/SEC2-Ver-1.0.pdf

Théorème 3.

Soit $\#E(\mathbb{F}_q) = q + 1 - a$. Posons $X^2 - aX + q = (X - \alpha)(X - \beta)$, où $\alpha, \beta \in \overline{\mathbb{F}}_q$. Alors

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

pour tout $n \geq 1$.

Exemple 1.

Considérons la courbe elliptique $E : y^2 = x^3 + 2$ définie sur $\mathbb{F}_7$,

$$E(\mathbb{F}_7) = \{\mathcal{O}, (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)\}.$$

Ainsi $\#E(\mathbb{F}_7) = 9$ et $a = 7+1-9 = -1$ et nous avons le polynôme suivant

$$X^2 + X + 7 = \left(X - \frac{-1+\sqrt{-27}}{2}\right)\left(X - \frac{-1-\sqrt{-27}}{2}\right)$$

Nous pouvons donc calculer la cardinalité de tout groupe $E(\mathbb{F}_{7^n})$. Par exemple

$$\left(\frac{-1+\sqrt{-27}}{2}\right)^{60} + \left(\frac{-1-\sqrt{-27}}{2}\right)^{60} = 180498585261198848060064 98$$

et donc

$$\begin{aligned}\#E(\mathbb{F}_{7^{60}}) &= 7^{60} + 1 - 180498585261198848060064 98 \\ &= 508021860739623365322188179602357975652549718829504\end{aligned}$$

Grâce à ce théorème nous pouvons très vite calculer la cardinalité d'un groupe $E(\mathbb{F}_{q^n})$ du moment que nous connaissons $\#E(\mathbb{F}_q)$.

Remarque 3.

Plus la courbe elliptique est grande, plus la sécurité des algorithmes de chiffrement présentés plus loin est élevée.

2.3 Problème du logarithme discret

Soit K un corps et E une courbe elliptique définie sur K. Les points K-rationnels formant un groupe abélien, celui-ci donne un cadre pour le problème du logarithme discret.

Définition 3.

Soit E une courbe elliptique définie sur K et G un point K-rationnel. Si $P \in E(K)$ est donné, le problème du logarithme discret consiste à trouver $n \in \mathbb{N}$, s'il existe, tel que $P = nG$.

Sur un corps fini, ce problème est réputé « difficile » en principe. À ce jour il n'y a pas d'algorithme sous-exponentiel pour résoudre ce problème, à condition de bien choisir E.

Le calcul réciproque de $P = nG$ se fait facilement via un algorithme d'exponentiation rapide.

3 Cryptosystèmes basés sur les courbes elliptiques

3.1 Protocole d'échange de clés de Diffie-Hellmann

Alice et Bob veulent avoir une clé en commun pour schanger des données en toute sécurité. Supposons que leur seul moyen de communication soit public. Un des moyens de sécuriser leurs données est qu'ils établissent une clé privée entre eux.

1. Alice et Bob choisissent une courbe elliptique E définie sur un corps fini $\mathbb{F}_q$ tel que le logarithme discret (voir juste après) soit difficile à résoudre. Il choisissent aussi un point $P \in E(\mathbb{F}_q)$ tel que le sous-groupe généré par P ait un ordre de grande taille. (En général, la courbe E et le point P sont choisis de manière à ce que l'ordre soit un grand nombre premier.)
2. Alice choisit un nombre entier secret $a \in$, calcule aP et l'envoie à Bob.
3. Bob choisit un nombre entier secret $b \in \mathbb{N}$, calcule bP et l'envoie à Alice.
4. Alice calcule abP.
5. Bob calcule baP.
6. Alice et Bob utilisent une méthode quelconque connue pour extraire une clé secrète de abP. Par exemple, ils peuvent utiliser les derniers 256 bits de la première coordonnée de abP comme clé, ou ils peuvent hâcher une des coordonnées de abP avec une fonction de hâchage pour laquelle ils se sont mis d'accord.

3.2 ElGamal sur courbe elliptique

3.2.1 Génération des clefs

On suppose cette fois qu'Alice veut envoyer à Bob un message en utilisant un algorithme de chiffrement par courbes elliptiques.

Bob commence par fabriquer une clé publique de la façon suivante :

1. il choisit une courbe elliptique $E(\mathbb{F}_q)$, de telle manière que le problème du logarithme discret soit plus difficile à résoudre sur $E(\mathbb{F}_q)$ que sur $\mathbb{F}_q$,
2. un point P de la courbe, tel que l'ordre de P soit un grand nombre premier,
3. Il choisit un nombre entier secret s et calcule $B = sP$.

Sa clé publique est constituée par la courbe elliptique $E(\mathbb{F}_q)$ et par les points P et sP de cette courbe elliptique. Sa clé privée est l'entier s, qu'on ne peut pas retrouver même connaissant P et sP, par la difficulté de résoudre le problème du logarithme discret sur une courbe elliptique.

Donc $pk = (E(\mathbb{F}_q), \mathbb{F}_q, P, B)$ et $sk = s$.

L'ensemble des messages clairs est la courbe $\mathcal{M} = E(\mathbb{F}_q)$ et celui des chiffrés est $\mathcal{C} = E(\mathbb{F}_q) \times E(\mathbb{F}_q)$

3.2.2 Chiffrement et déchiffrement

Pour chiffrer un message Alice choisit un entier k et applique :

$$\begin{array}{rccc} \mathcal{E} & : & \mathcal{K} \times \mathcal{M} & \to & \mathcal{C} \\ & & (pk = (E(\mathbb{F}_q), \mathbb{F}_q, P, B), M) & \mapsto & (M_1 = kP,\ M_2 = M + kB) \end{array}$$

Pour déchiffrer un message Bob calcule simplement $M = M_2 - sM_1$:

$$\begin{array}{rccc} \mathcal{D} & : & \mathcal{C} & \to & \mathcal{M} \\ & & (sk = s, C = (M_1, M_2)) & \mapsto & M_2 - sM_1 \end{array}$$

Il y a bien égalité parce que : $M_2 - sM_1 = (M + kB) - s(kP) = M + k(sP) - skP = M$.

Remarque 4.

Remarque. Il est important qu'Alice utilise, à chaque fois qu'elle envoie un message crypté à Bob avec la même clé, un k différent. En effet, si elle utilise le même k pour deux messages différents M et M', alors $M_1 = M_1'$ Éve ayant intercepté les deux messages codés s'en apercevra et pourra calculer

$$M_2' - M_2 = M' - kB - (M - kB) = M' - M$$

Supposons que pour une raison quelconque le message M soit rendu public dès que l'information n'est plus d'actualité, alors Éve calculera sans peine M' qui vaut $M - M_2 + M_2'$

3.3 Avantages

Il a été démontré que la sécurité offerte par le chiffrement sur les courbes elliptiques était tout aussi bonne que RSA pour des clefs bien plus petites. Comme les clefs sont plus petites les calculs demandent moins de ressource.

D'autre part la cryptographie sur les courbes elliptiques utilise un algorithme plus petit pour générer des clés qui sont exponentiellement plus fortes que les clés RSA.

Key Size(in bit)			
Symmetric	Asymmetric		
AES	RSA	Diffie-Hellman	Elliptic Curve
80	1024	1024	160
112	2048	2048	224
128	3072	3072	256
192	7680	7680	384
256	15360	15360	521

FIGURE 3 – NIST recommendation on key size

3.4 Difficultés techniques

Les diffcultés techniques majeures sont au nombre de deux :

1. Il n'y a aucun moyen évident d'attacher des messages texte en points dans $E(\mathbb{F}_p)$.
2. Le cryptosystème elliptique ElGamal a une expansion de message de 4 à 1, par rapport au rapport d'expansion de 2 à 1 d'ElGamal dans $\mathbb{F}_p$.

Différentes méthodes ont été proposées pour résoudre ces deux problèmes :

- La difficulté d'associer les textes en clairs aux points peut être contournée en choisissant M de façon aléatoire et en l'utilisant comme un masque pour le texte en clair réel.
- Pour améliorer l'expansion des messages on peut utiliser la compression des points.

La compression de point sur une courbe elliptique consiste à ne pas envoyer les deux coordonnées d'un point mais seulement la première ainsi qu'un bit qui permet de déterminer de quel point il s'agit :

$$\begin{array}{rccc} \mathcal{CP} & : & E(\mathbb{F}_p) & \to & \mathbb{F}_p \times \mathbb{Z}/2\mathbb{Z} \\ & & (M=(x,y)) & \mapsto & (x, i = y\,[2]) \end{array}$$

Pour décompresser on utilise l'équation de la courbe :

$$\begin{array}{rccc} \mathcal{DP} & : & \mathbb{F}_p \times \mathbb{Z}/2\mathbb{Z} & \to & E(\mathbb{F}_p) \\ & & (x,i) & \mapsto & \begin{cases} (x,\ y) & \text{si} \quad y = i\,[2] \\ (x, p-y) & \text{sinon.} \end{cases} \end{array}$$

avec $y = \sqrt{x^3 + ax + b}\,[p]$.