Au sujet des courbes elliptiques

Approche géométrique et intérêts cryptologiques

Samuel Debray
- 5156 -

Travaux d'Initiative Personnelle Encadrés

juin - juillet 2019

Sommaire

Plan projectif

Soit K un corps. Pour $(a,b,c),(a',b',c') \in K^3 \backslash \{(0,0,0)\}$, on note $(a,b,c) \sim (a',b',c')$ ssi il existe $t \in K^*$ tel que $(a,b,c) = t(a',b',c')$.

Définition 1

Le *plan projectif* $\mathbb{P}_2(K)$ est l'ensemble quotient de $K^3 \setminus \{(0,0,0)\}$ par la relation $\sim$.

Définition 2

Les nombres a, b, c sont des *coordonnées homogènes* du point P.

Plan projectif

Soit K un corps. Pour $(a,b,c),(a',b',c') \in K^3\backslash\{(0,0,0)\}$, on note $(a,b,c) \sim (a',b',c')$ ssi il existe $t \in K^*$ tel que $(a,b,c) = t(a',b',c')$.

Définition 1

Le *plan projectif* $\mathbb{P}_2(K)$ est l'ensemble quotient de $K^3 \setminus \{(0,0,0)\}$ par la relation $\sim$.

Définition 2

Les nombres a,b,c sont des *coordonnées homogènes* du point P.

On peut considérer $\mathbb{P}_2(K)$ comme une « extension »de K^2 dans la mesure où à tout point $(a,b) \in K^2$, on peut faire correspondre un unique point $(a,b,1) \in \mathbb{P}_2(K)$. Les points ajoutés sont les points de la forme $(x,y,0)$, qui correspondent à des points à l'infini.

Représentation du plan projectif

Notons $\mathbb{A}_2$ le plan affine usuel. On peut voir $\mathbb{P}_2(\mathbb{R})$ comme la réunion de $\mathbb{A}_2$ et d'une droite, qui représente les points à l'infini, un par direction.

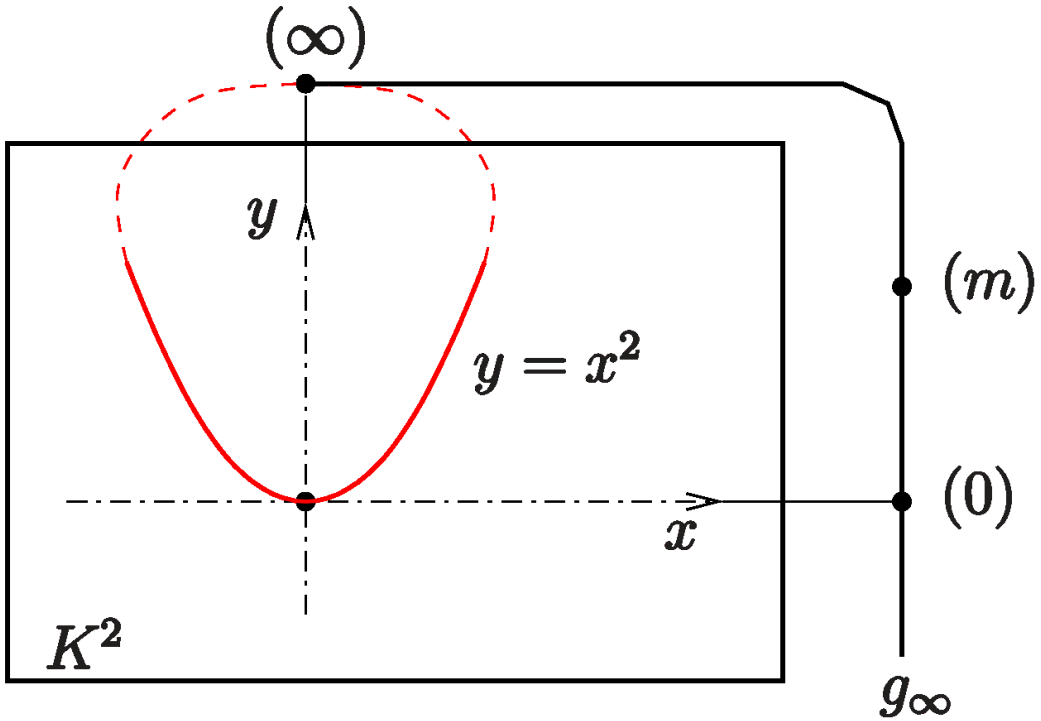


FIGURE – Plan projectif.

Source de l'image : `https://www.freepng.fr/png-nokxu9/`.

Courbes projectives (1)

Définition 3

Une *courbe* C de $\mathbb{P}_2(K)$ de degré d est l'ensemble des points vérifiant

$$F(X, Y, Z) = 0$$

où $F \in K[X, Y, Z]_d$ est un polynôme homogène de degré $d \geqslant 1$. Si $d = 1$, on parle de *droite*, et si $d = 3$ de *cubique*.

Courbes projectives (1)

Définition 3

Une *courbe* C de $\mathbb{P}_2(K)$ de degré d est l'ensemble des points vérifiant

$$F(X, Y, Z) = 0$$

où $F \in K[X, Y, Z]_d$ est un polynôme homogène de degré $d \geqslant 1$. Si $d = 1$, on parle de *droite*, et si $d = 3$ de *cubique*.

Définition 4

Un point P d'une courbe $C : F(X, Y, Z) = 0$ est dit *singulier* ssi

$$\left.\frac{\partial F}{\partial X}\right|_P = \left.\frac{\partial F}{\partial Y}\right|_P = \left.\frac{\partial F}{\partial Z}\right|_P = 0.$$

P est dit *simple* dans le cas contraire.

Courbes projectives (2)

Définition 5

Une courbe est *lisse* si tous les points sont simples.

Courbes projectives (2)

Définition 5

Une courbe est *lisse* si tous les points sont simples.

Définition 6

Une courbe est dite *irréductible* ssi elle ne peut pas s'écrire comme le produit non trivial de deux polynômes.

Représentations homogène et non-homogène (1)

Soit une courbe projective $C : F(X, Y, Z) = 0$ sur un corps K de degré d. Comme F est homogène, on peut diviser F par Z^d pour obtenir un nouveau polynôme f en les variables réduites $x := \frac{X}{Z}$ et $y := \frac{Y}{Z}$ pour se ramener au plan affine. Les points $P = (a, b, c)$ de C sont alors de deux types :

Représentations homogène et non-homogène (1)

Soit une courbe projective $C : F(X, Y, Z) = 0$ sur un corps K de degré d. Comme F est homogène, on peut diviser F par Z^d pour obtenir un nouveau polynôme f en les variables réduites $x := \frac{X}{Z}$ et $y := \frac{Y}{Z}$ pour se ramener au plan affine. Les points $P = (a, b, c)$ de C sont alors de deux types :

- Si $c \neq 0$, vue la définition du plan projectif, on peut supposer $c = 1$, si bien que le point P' du plan affine de coordonnées (a, b) appartient à la projection de C sur $\mathbb{A}_2$.

Représentations homogène et non-homogène (1)

Soit une courbe projective $C\colon F(X,Y,Z)=0$ sur un corps K de degré d. Comme F est homogène, on peut diviser F par Z^d pour obtenir un nouveau polynôme f en les variables réduites $x := \frac{X}{Z}$ et $y := \frac{Y}{Z}$ pour se ramener au plan affine. Les points $P=(a,b,c)$ de C sont alors de deux types :

- Si $c \neq 0$, vue la définition du plan projectif, on peut supposer $c=1$, si bien que le point P' du plan affine de coordonnées (a,b) appartient à la projection de C sur $\mathbb{A}_2$.
- Si $c=0$, il est alors impossible de diviser F par Z en P,si bien que P n'a pas de coordonnées non-homogènes : c'est un point de C situé *à l'infini*, dans la direction (a,b).

Représentations homogène et non-homogène (1)

Soit une courbe projective $C\colon F(X,Y,Z)=0$ sur un corps K de degré d. Comme F est homogène, on peut diviser F par Z^d pour obtenir un nouveau polynôme f en les variables réduites $x := \frac{X}{Z}$ et $y := \frac{Y}{Z}$ pour se ramener au plan affine. Les points $P=(a,b,c)$ de C sont alors de deux types :

- Si $c \neq 0$, vue la définition du plan projectif, on peut supposer $c=1$, si bien que le point P' du plan affine de coordonnées (a,b) appartient à la projection de C sur $\mathbb{A}_2$.
- Si $c=0$, il est alors impossible de diviser F par Z en P,si bien que P n'a pas de coordonnées non-homogènes : c'est un point de C situé *à l'infini*, dans la direction (a,b).

Ainsi C peut être représentée dans $\mathbb{A}_2$, moyennant l'ajout de points à l'infini au plan.

Représentations homogène et non-homogène (2)

On s'intéresse à la cubique C : $P(X, Y, Z) = 0$ où $P = YZ - X^2$. Elle contient des points à l'infini : $(0, 1, 0)$ par exemple, et des points représentables dans $\mathbb{A}_2$: $(2, 4, 1)$ par exemple.
L'équation non-homogène de C est alors $y = x^2$, et C peut être représentée dans le plan auquel on ajoute les points de C à l'infini.

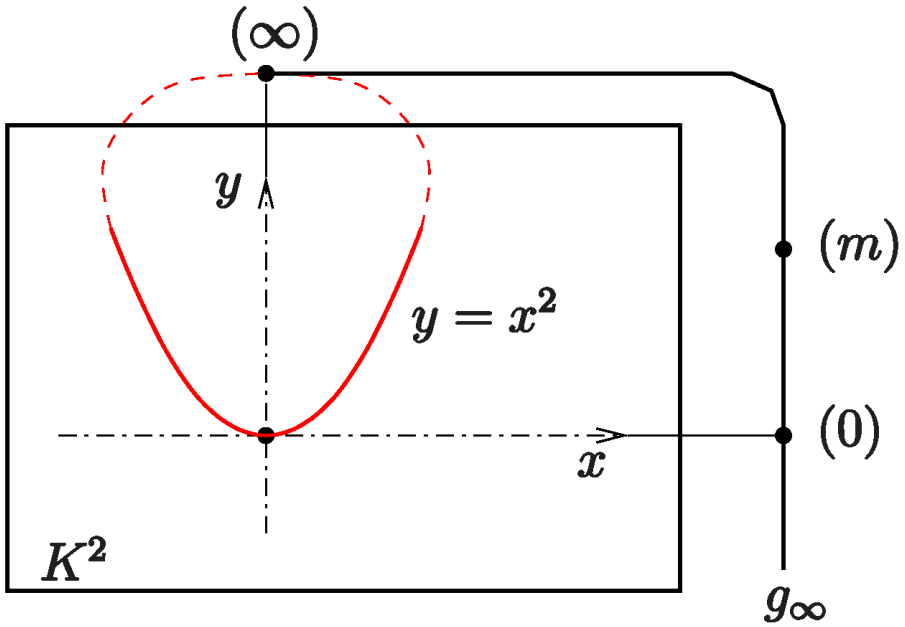


FIGURE – P en représentation non-homogène.

Théorème de Bézout

Définition 7

Soient $L : aX + bY + cZ = 0$ une droite et $C : F(X, Y, Z) = 0$ une courbe projectives, soit P un point de $L \cap C$. On appelle *ordre d'intersection* de L et C en P (et on note $I(P, L, C)$) la multiplicité de P en tant que racine du polynôme associé à la courbe $L \cap C$: $F\left(x, \frac{by+c}{a}\right)$ [a]. Si $P \notin L \cap C$, on note $I(P, L, C) = 0$.

a. qui est un polynôme d'une seule variable en coordonnées non homogènes.

Théorème de Bézout

Définition 7

Soient $L : aX + bY + cZ = 0$ une droite et $C : F(X, Y, Z) = 0$ une courbe projectives, soit P un point de $L \cap C$. On appelle *ordre d'intersection* de L et C en P (et on note $I(P, L, C)$) la multiplicité de P en tant que racine du polynôme associé à la courbe $L \cap C$: $F\left(x, \frac{by+c}{a}\right)$ [a]. Si $P \notin L \cap C$, on note $I(P, L, C) = 0$.

a. qui est un polynôme d'une seule variable en coordonnées non homogènes.

On admet le théorème suivant :

Théorème 1 [de Bézout, version affaiblie]

Soient L une droite et C une courbe projectives sans facteur commun. Alors

$$\sum_{P \in L \cap C} I(P, L, C) = \deg C.$$

Définition

Définition 8

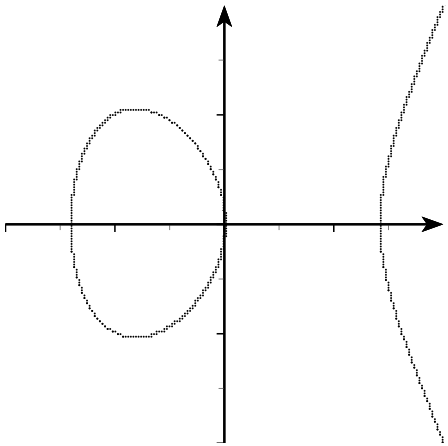
Une *courbe elliptique* sur K est la donnée d'une cubique lisse $E\colon F(X,Y,Z)=0$ de $\mathbb{P}_2(K)$ et d'un point $\mathcal{O}\in E(K)$, où $E(K)=\{(x,y,z)\in\mathbb{P}_2(K)\,|\,F(x,y,z)=0\}$. $\mathcal{O}$ est appelée *origine* de la courbe elliptique.

Définition 9

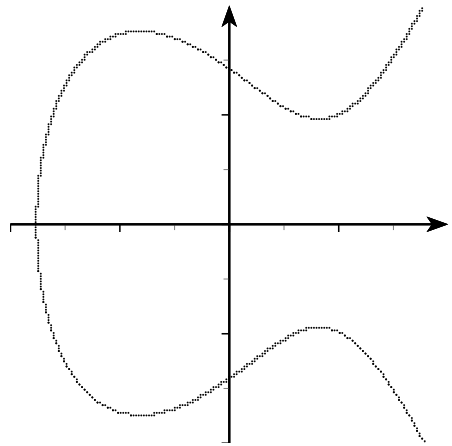
L'ensemble $E(K)$ s'appelle ensemble des *points rationnels* de E sur K.

Lorsqu'il n'y a pas d'ambiguïté sur K, on confondra la courbe E et l'ensemble de ses points rationnels $E(K)$.

Équation réduite



(a) $y^2 = x^3 - 2x$



(b) $y^2 = x^3 - 2x + 2$

FIGURE – Points rationnels de courbes elliptiques.

Le recours aux formes de Weierstrass permet d'établir que toute courbe elliptique sur un corps de caractéristique différente de 2 et 3 a pour équation affine

$$y^2 = x^3 + ax + b \quad \text{avec} \quad 4a^3 + 27b^2 \neq 0 \tag{1}$$

et alors le point $\mathcal{O} = (0, 1, 0)$ s'appelle *point à l'infini*, il représente l'intersection des droites verticales du plan.

Lien avec le théorème de Bézout

Proposition 1

Toute courbe elliptique est irréductible.

⏩ Démonstration

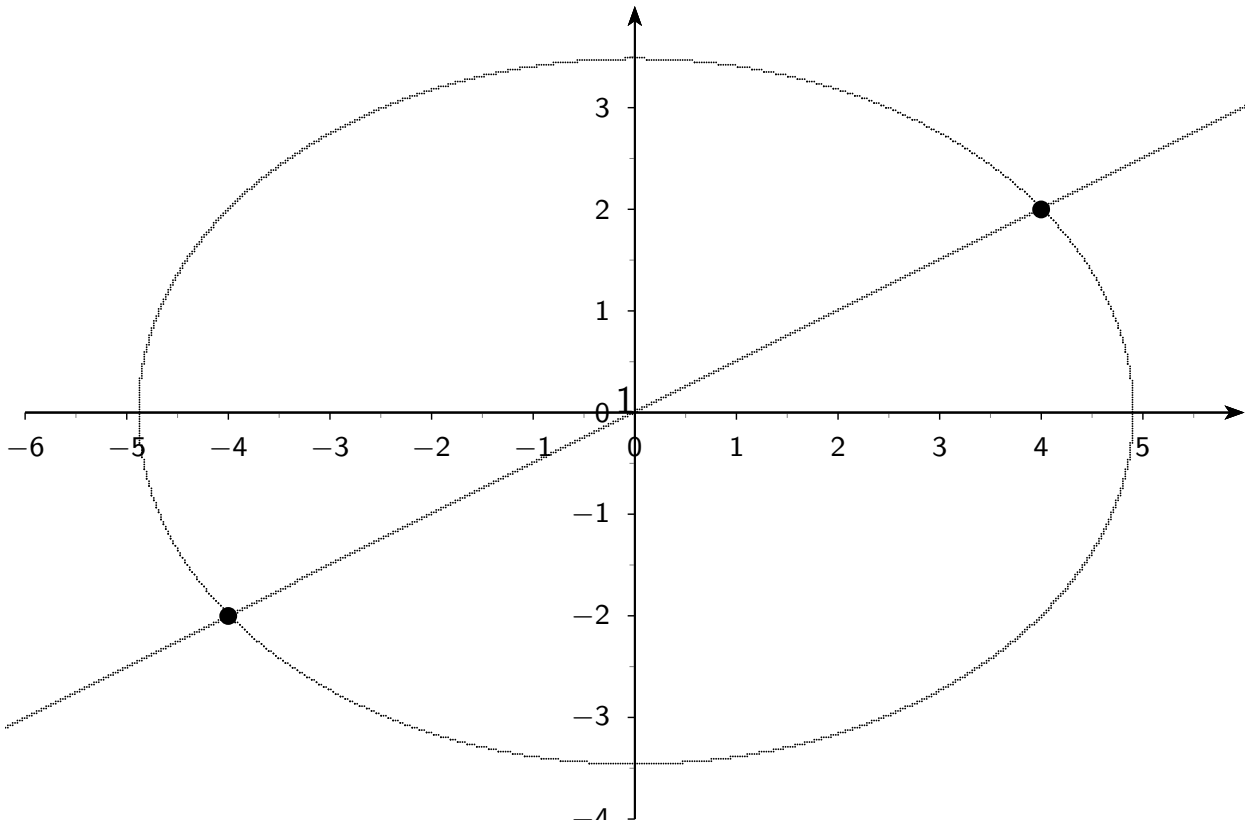


FIGURE – Non lissité d'une cubique factorisable par une droite.

Méthode de la sécante-tangente (1)

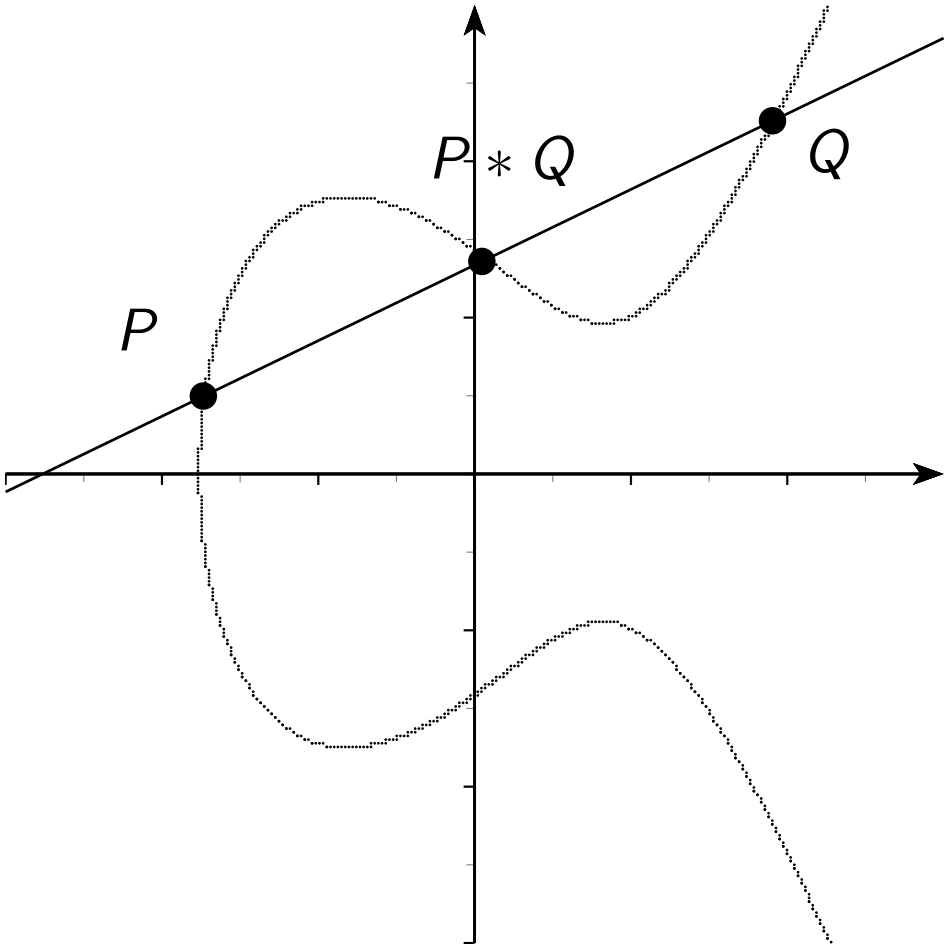


FIGURE – $*$ de deux points.

Méthode de la sécante-tangente (1)

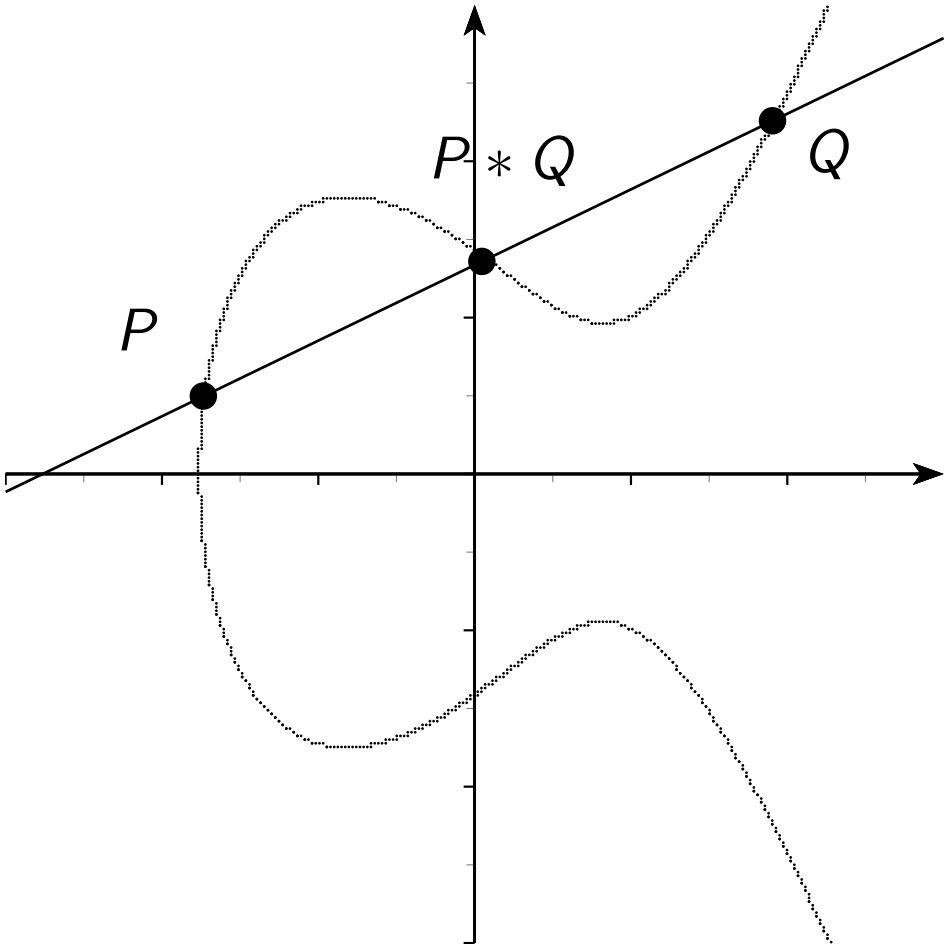


FIGURE – $*$ de deux points.

Soient P et Q deux points de E, alors $P + Q := \mathcal{O} * (P * Q)$.

Méthode de la sécante-tangente (2)

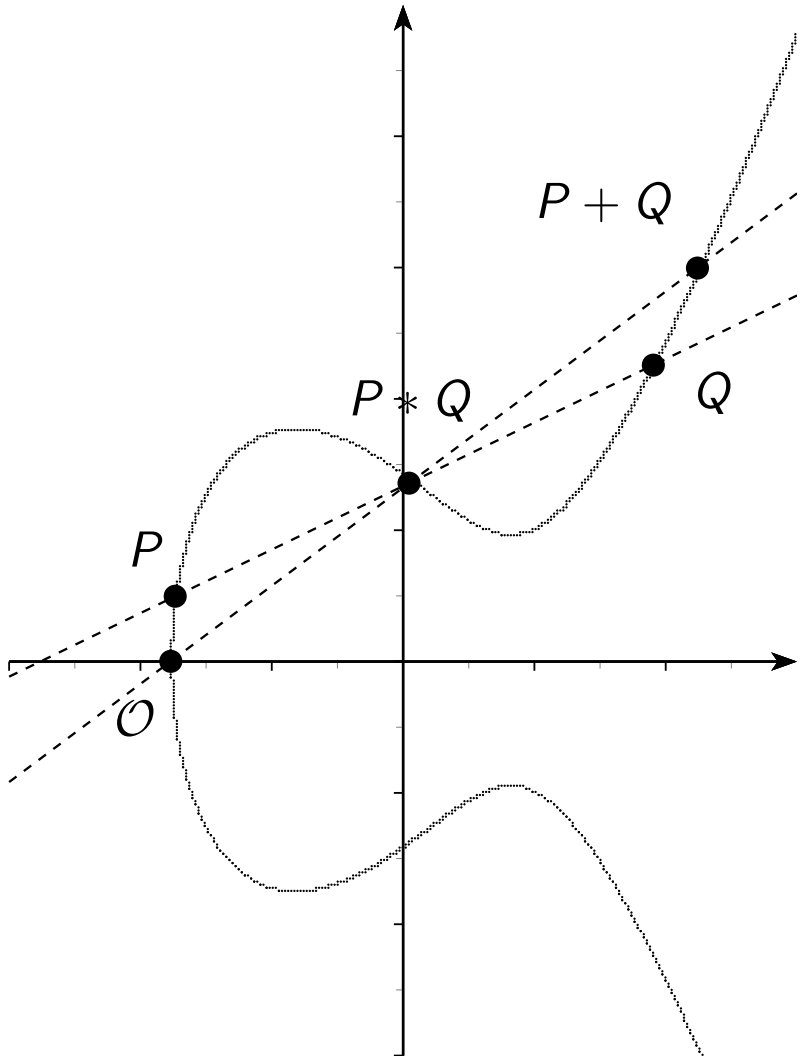


FIGURE – Somme de deux points.

Méthode de la sécante-tangente (3)

On remarque alors sur la figure 6 que :

1. pour tout point P de E, $P + \mathcal{O} = \mathcal{O} + P = P$,
2. $+$ est commutative.
3. $+$ est une loi interne.

Méthode de la sécante-tangente (3)

On remarque alors sur la figure 6 que :

1. pour tout point P de E, $P + \mathcal{O} = \mathcal{O} + P = P$,
2. $+$ est commutative.
3. $+$ est une loi interne.

Théorème 2

$((E, \mathcal{O}), +)$ est un groupe abélien.

Le point délicat dans la démonstration de ce théorème repose sur l'associativité de $+$.

Méthode de la sécante-tangente (3)

On remarque alors sur la figure 6 que :

1. pour tout point P de E, $P + \mathcal{O} = \mathcal{O} + P = P$,
2. $+$ est commutative.
3. $+$ est une loi interne.

Théorème 2

$((E, \mathcal{O}), +)$ est un groupe abélien.

Le point délicat dans la démonstration de ce théorème repose sur l'associativité de $+$.

Théorème 3 [de Mordell-Weil]

Soit E une courbe elliptique définie sur une extension finie[a] K de $\mathbb{Q}$. Alors le groupe $E(K)$ est de type fini.

a. i.e. une extension K telle que le $\mathbb{Q}$-espace vectoriel K est de dimension finie.

Loi de groupe explicite (1)

On s'intéresse ici à la sommation analytique de deux points d'une courbe elliptique, ou au doublement d'un point. Soient donc

$$E : f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0 \qquad (2)$$

une courbe elliptique dont l'origine est $\mathcal{O} = (0, 1, 0)$ et P, Q deux points distincts de E. $\mathcal{O}$ étant l'unique point de E situé à l'infini, on travaille en coordonnées non homogènes.

Loi de groupe explicite (1)

On s'intéresse ici à la sommation analytique de deux points d'une courbe elliptique, ou au doublement d'un point. Soient donc

$$E : f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0 \qquad (2)$$

une courbe elliptique dont l'origine est $\mathcal{O} = (0,1,0)$ et P, Q deux points distincts de E. $\mathcal{O}$ étant l'unique point de E situé à l'infini, on travaille en coordonnées non homogènes.
Notons alors $P = (p_1, p_2)$ et $Q = (q_1, q_2)$ les coordonnées réduites de P et Q, avec $p_1 - q_1$ et $p_2 - q_2$ non simultanément nuls.

Loi de groupe explicite (2)

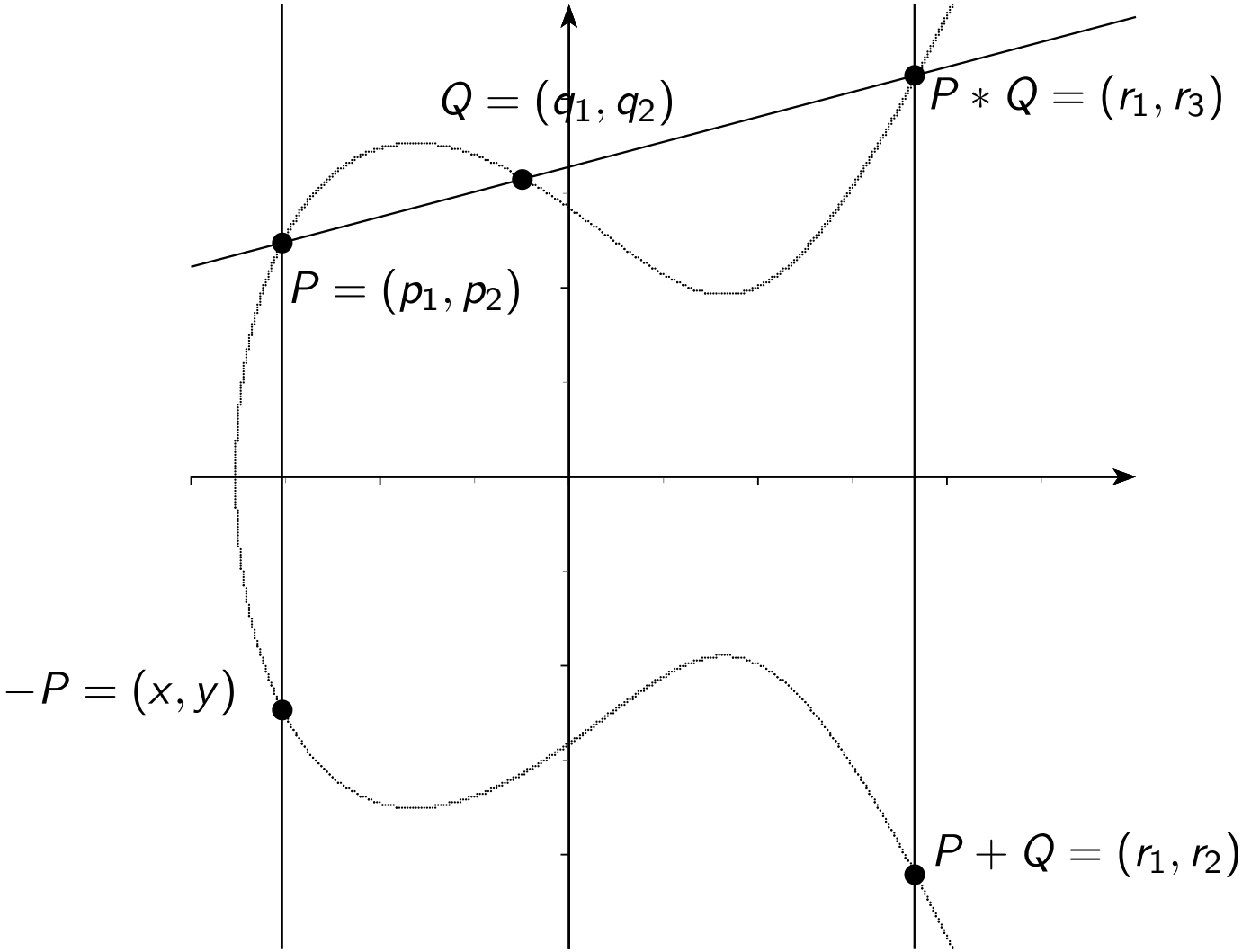


FIGURE – Loi de groupe d'une courbe elliptique avec l'origine à l'infini.

Loi de groupe explicite (3)

On peut montrer que :

- $-P = (p_1, -p_2 - a_1 p_1 - a_3)$.
- $P + Q = (\underbrace{-a_2 + \lambda^2 + a_1\lambda - p_1 - q_1}_{r_1}, -(\lambda r_1 + \gamma) - a_1 r_1 - a_3)$ où

$$\lambda := \frac{q_2 - p_2}{q_1 - p_1} \quad \text{et} \quad \gamma := p_2 - \lambda p_1.$$

- $2P = (\underbrace{-a_2 + \lambda^2 + a_1\lambda - 2p_1}_{r_1}, -(\lambda r_1 + \gamma) - a_1 r_1 - a_3)$ où

$$\lambda := \frac{3p_1^2 + 2a_2 p_1 + a_4 - a_1 p_2}{2p_2 + a_1 p_1 + a_3}.$$

One-time pad

Définition 10

Un chiffrement est dit *parfait* ssi, même avec une puissance de calcul infinie, la connaissance du message chiffré ne donne aucune information sur le message clair.

One-time pad

Définition 10

Un chiffrement est dit *parfait* ssi, même avec une puissance de calcul infinie, la connaissance du message chiffré ne donne aucune information sur le message clair.

Théorème 4 [one-time pad]

Il existe un unique chiffrement parfait. La clé de chiffrement vérifie les conditions suivantes :

- elle est aussi longue que le message à chiffrer,
- elle est aléatoire,
- elle est à usage unique.

⏩ Démonstration partielle

Chiffre de Vernam

Algorithme 4 [chiffre de Vernam]

1. On transforme le message clair en une suite de bits $v = v_1 \dots v_n$.
2. On choisit une clé aléatoire de même taille $k = k_1 \dots k_n$.
3. On calcule le message chiffré bit par bit par une opération XOR : $u = u_1 \dots u_n$ où $\forall i \in [\![1, n]\!], u_i = v_i \oplus k_i$.

Le déchiffrement du message se fait en calculant $u \oplus k$.

Définition

Définition 11

Soient G un groupe noté additivement et $g \in G$. Le *problème du logarithme discret sur G en base g* est, pour $y \in G$ fixé, de trouver un entier x tel que $xg = y$.

Remarquons déjà que l'existence d'un tel entier n'est pas garantie, car G n'est pas engendré par chacun de ses éléments (il se peut même que G ne soit pas monogène).

1. ce qui revient à supposer qu'il existe une solution au problème du logarithme discret sur $E(K)$ en base A pour P.

Définition

Définition 11

Soient G un groupe noté additivement et $g \in G$. Le *problème du logarithme discret sur G en base g* est, pour $y \in G$ fixé, de trouver un entier x tel que $xg = y$.

Remarquons déjà que l'existence d'un tel entier n'est pas garantie, car G n'est pas engendré par chacun de ses éléments (il se peut même que G ne soit pas monogène).

Prenons E une courbe elliptique sur un corps K et notons $N := \operatorname{card} E(K)$. Soient P et A deux points de $E(K)$ et supposons qu'il existe $n \in [\![0, N]\!]$ tel que $nA = P$ [1].

1. ce qui revient à supposer qu'il existe une solution au problème du logarithme discret sur $E(K)$ en base A pour P.

Algorithme Baby step - Giant step

Algorithme 4 [Baby step - Giant step]

1. On fixe un entier $m > \sqrt{N}$ et on calcule mA.
2. On établit la liste des points jA pour $j \in [\![0, m-1]\!]$.
3. On détermine les points $P - k(mA)$ pour $k \in [\![0, m-1]\!]$ jusqu'à en trouver un qui soit égal à l'un des jA précédemment calculés.

n est alors donné par $n = km + j$ où j et k sont tels que $jA = P - k(mA)$.

Algorithme Baby step - Giant step

Algorithme 4 [Baby step - Giant step]

1. On fixe un entier $m > \sqrt{N}$ et on calcule mA.
2. On établit la liste des points jA pour $j \in [\![0, m-1]\!]$.
3. On détermine les points $P - k(mA)$ pour $k \in [\![0, m-1]\!]$ jusqu'à en trouver un qui soit égal à l'un des jA précédemment calculés.

n est alors donné par $n = km + j$ où j et k sont tels que $jA = P - k(mA)$.

Théorème 5

L'algorithme Baby step - Giant step permet de résoudre le problème du logarithme discret en $O(\sqrt{N})$ opérations.

⏩ Démonstration

Algorithme Baby step - Giant step

Algorithme 4 [Baby step - Giant step]

1. On fixe un entier $m > \sqrt{N}$ et on calcule mA.
2. On établit la liste des points jA pour $j \in [\![0, m-1]\!]$.
3. On détermine les points $P - k(mA)$ pour $k \in [\![0, m-1]\!]$ jusqu'à en trouver un qui soit égal à l'un des jA précédemment calculés.

n est alors donné par $n = km + j$ où j et k sont tels que $jA = P - k(mA)$.

Théorème 5

L'algorithme Baby step - Giant step permet de résoudre le problème du logarithme discret en $O(\sqrt{N})$ opérations.

Démonstration

S'il est vrai que l'algorithme a une complexité $O(\sqrt{N})$, il n'en demeure pas moins exponentiel en l'ordre de $E(K)$ car $O(\sqrt{N}) = O\left(\mathrm{e}^{\frac{1}{2}\log_2(N)}\right)$ et N est stocké sur $\log_2(N) + 1$ bits, en tant qu'entier non signé.

Illustration

On prend $K = \mathbb{F}_{53}$ et $E : y^2 = x^3 - 2x + 2$. Un programme `Python` permet de vérifier que $E(K)$ est d'ordre 56 et que $A = (43, 20)$ engendre $E(K)$. Par ailleurs, on obtient aussi que $P = (38, 7) \in E(K)$. Calculons son logarithme discret en base A. On cherche le plus petit $n < 56$ tel que $nA = P$.

Illustration

On prend $K = \mathbb{F}_{53}$ et $E : y^2 = x^3 - 2x + 2$. Un programme `Python` permet de vérifier que $E(K)$ est d'ordre 56 et que $A = (43, 20)$ engendre $E(K)$. Par ailleurs, on obtient aussi que $P = (38, 7) \in E(K)$. Calculons son logarithme discret en base A. On cherche le plus petit $n < 56$ tel que $nA = P$.

▶ Prenons $m = 8$, les points jA donnés par nos programmes `Python` pour j allant de 0 à m sont, dans l'ordre :

$$\mathcal{O}, \quad (43, 20), \quad \boxed{(7, 15)}, \quad (46, 37), \quad (2, 18), \quad (36, 23), \quad (38, 46), \quad (16, 41), \quad (9, 36).$$

Illustration

On prend $K = \mathbb{F}_{53}$ et $E : y^2 = x^3 - 2x + 2$. Un programme `Python` permet de vérifier que $E(K)$ est d'ordre 56 et que $A = (43, 20)$ engendre $E(K)$. Par ailleurs, on obtient aussi que $P = (38, 7) \in E(K)$. Calculons son logarithme discret en base A. On cherche le plus petit $n < 56$ tel que $nA = P$.

▶ Prenons $m = 8$, les points jA donnés par nos programmes `Python` pour j allant de 0 à m sont, dans l'ordre :

$$\mathcal{O}, \quad (43, 20), \quad \boxed{(7, 15)}, \quad (46, 37), \quad (2, 18), \quad (36, 23), \quad (38, 46), \quad (16, 41), \quad (9, 36).$$

▶ Par ailleurs, les points $P - k(mA)$ pour k allant de 0 à $m - 1$ sont, dans l'ordre :

$$(38, 7), \quad (22, 35), \quad (12, 40), \quad (26, 47), \quad (29, 35), \quad (28, 3), \quad \boxed{(7, 15)}, \quad (38, 7).$$

Illustration

On prend $K = \mathbb{F}_{53}$ et $E : y^2 = x^3 - 2x + 2$. Un programme `Python` permet de vérifier que $E(K)$ est d'ordre 56 et que $A = (43, 20)$ engendre $E(K)$. Par ailleurs, on obtient aussi que $P = (38, 7) \in E(K)$. Calculons son logarithme discret en base A. On cherche le plus petit $n < 56$ tel que $nA = P$.

▶ Prenons $m = 8$, les points jA donnés par nos programmes `Python` pour j allant de 0 à m sont, dans l'ordre :

$$\mathcal{O}, \quad (43, 20), \quad \boxed{(7, 15)}, \quad (46, 37), \quad (2, 18), \quad (36, 23), \quad (38, 46), \quad (16, 41), \quad (9, 36).$$

▶ Par ailleurs, les points $P - k(mA)$ pour k allant de 0 à $m - 1$ sont, dans l'ordre :

$$(38, 7), \quad (22, 35), \quad (12, 40), \quad (26, 47), \quad (29, 35), \quad (28, 3), \quad \boxed{(7, 15)}, \quad (38, 7).$$

La correspondance a lieu pour $j = 2$ et $k = 6$, ce qui donne

$$n = km + j = 50.$$

Protocole Diffie-Hellman

Algorithme 5 [protocole Diffie-Hellman elliptique]

1. Alice et Bob choisissent un corps fini K et une courbe elliptique E définie sur K, de telle sorte que le problème du logarithme discret soit difficile à résoudre dans le groupe $E(K)$. Ils choisissent de plus un point $P \in E(K)$ tel que l'ordre du sous-groupe engendré par P soit grand. En pratique, l'ordre de ce groupe est un grand nombre premier. Le triplet (K, E, P) est public.
2. Alice choisit secrètement $a \in \mathbb{N}$ et calcule le point $P_a = aP$ puis le transmet publiquement à Bob.
3. Bob choisit secrètement $b \in \mathbb{N}$ et calcule le point $P_b = bP$ puis le transmet publiquement à Alice.
4. Alice et Bob déterminent $aP_b = abP$.

La clé secrète commune est alors le point abP. Alice et Bob peuvent aussi fabriquer une clé secrète à partir de abP en utilisant un procédé convenu, typiquement en utilisant les derniers chiffres de l'abscisse de abP comme clé secrète.

Problème de Diffie-Hellman

L'apport des courbes elliptiques sur les corps finis réside dans le fait qu'il est plus délicat de résoudre le problème du logarithme discret dans le groupe des points rationnels d'une courbe elliptique sur un corps fini K que sur le groupe K^*, qui est le groupe sur lequel on travaille généralement.

Problème de Diffie-Hellman

L'apport des courbes elliptiques sur les corps finis réside dans le fait qu'il est plus délicat de résoudre le problème du logarithme discret dans le groupe des points rationnels d'une courbe elliptique sur un corps fini K que sur le groupe K^*, qui est le groupe sur lequel on travaille généralement.

Problème de Diffie-Hellman Connaissant P, aP et bP dans $E(K)$, peut-on trouver abP ?

À l'heure actuelle, on ne sait pas résoudre le problème de Diffie-Hellman sans avoir à résoudre celui du logarithme discret au préalable.

Utilisation du programme proposé

On teste par exemple le programme sur le texte « samuel », que l'on encode en binaire (via un convertisseur en ligne quelconque puis en transformant la chaine de caractères obtenue grâce à une fonction ad hoc) par la liste :

$$l = [0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0].$$

On veut chiffrer ce message à l'aide d'une clé prise dans $E(\mathbb{F}_{21347})$ où $E\colon y^2 = -2x + 2$ à partir du point rationnel $(23, 2372)$ à la puissance 57.

Utilisation du programme proposé

On teste par exemple le programme sur le texte « samuel », que l'on encode en binaire (via un convertisseur en ligne quelconque puis en transformant la chaine de caractères obtenue grâce à une fonction ad hoc) par la liste :

l = [0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0].

On veut chiffrer ce message à l'aide d'une clé prise dans $E(\mathbb{F}_{21347})$ où $E\colon y^2 = -2x + 2$ à partir du point rationnel $(23, 2372)$ à la puissance 57.

`vernam(l, cle(21347, [0,0,0,-2,2], (23, 2372), 57, len(l)))` donne alors le cryptage :

[0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1].

Toute courbe elliptique est irréductible (1)

Soit E une courbe elliptique donnée par son équation homogène la plus générale[2]

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

Supposons que $F := Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6$ se décompose sous la forme d'un produit de polynômes non triviaux $F(X, Y) = P(X, Y)Q(X, Y)$. Alors, comme F n'est factorisable par aucune puissance de X ou de Y, P et Q dépendent à la fois de X et de Y, donc le degré partiel en Y de P et Q est 1 car $\deg_Y F = 2$.
Écrivons donc

$$P(X, Y) = P_1(X)Y + P_2(X) \quad \text{et} \quad Q(X, Y) = Q_1(X)Y + Q_2(X)$$

de sorte que

$$PQ(X, Y) = P_1Q_1(X)Y^2 + (P_1Q_2(X) + P_2Q_1(X))Y + P_2Q_2(X).$$

2. i.e. valable dans un corps de caractéristique quelconque.

Toute courbe elliptique est irréductible (2)

On déduit alors que $P_1 Q_1$ est un polynôme constant puisque $PQ = F$ et $\deg P_2 Q_2 = 3$. Or $\deg P_2 Q_2 = \deg P_2 + \deg Q_2$ d'où $\deg P_2 \neq \deg Q_2$, ce qui justifie que $\deg(P_2 + Q_2) = \max(\deg P_2, \deg Q_2) > 1$.
Ainsi, puisque P_1 et Q_1 sont constants et non nuls, $\deg(P_1 Q_2 + P_2 Q_1) > 1$, ce qui n'est pas car $PQ = F$ donc $P_1 Q_2 + P_2 Q_1 = a_1 X + a_3$.

Existence d'un chiffre parfait

Soient $u = u_1 \dots u_n$ un message chiffré avec un telle clé et $v = v_1 \dots v_n$ le message clair associé. Soit ϕ l'injection canonique de $\{a, b, \dots, z\}$ dans $[\![1, 26]\!]$. Alors les conditions ci-dessus permettent de considérer que pour tout $k \in [\![1, n]\!]$, la probabilité que $v_1 = \phi(m)$ pour $m \in [\![1, 26]\!]$ est uniforme, i.e. qu'elle ne dépend pas de u_k. En d'autres termes, la donnée du message chiffré n'aide en rien son déchiffrement vu le caractère aléatoire de la clé, ce qui justifie le caractère parfait du chiffrement.

Terminaison de l'algorithme Baby step - Giant step

Prouvons la correction et la terminaison de l'algorithme, la complexité annoncée étant évidente si l'on considère que m est de l'ordre de grandeur de $\sqrt{N}$. Il s'agit donc de montrer l'existence de $j, k \in [\![0, m-1]\!]$ tels que $jA = P - kmA$. La division euclidienne de n par m donne :

$$n = mq + r \quad \text{avec} \quad 0 \leqslant r < m.$$

Or on a $0 \leqslant n < m^2$ par hypothèse, d'où $q = \frac{n-r}{m} \leqslant \frac{n}{m} < m$ et

$$P - q(mA) = nA - q(mA) = (n - qm)A = rA.$$

Ainsi, $j = r$ et $k = q$ conviennent et l'on a $n = km + j$.

Analyse de la complexité du programme proposé

En supposant qu'on ne travaille qu'avec des entiers standards (i.e. des entiers représentables sur 64 bits), la complexité temporelle du programme proposé est de l'ordre de :

- $O(c \times b)$ pour `cle(p,e,ap,b,n)`, si l'on note c la complexité de `somme`, car l'exponentiation rapide ne demande guère plus de $O(n)$ opérations. Or `somme(p,e,point1,point2)` a la même complexité que `inv(a,p)`, i.e. $O(\log(p)^2)$ d'où la complexité $O(b\log(p)^2)$ pour `cle`.
- $O(|\texttt{mot}|)$ pour `vernam` car `decompose(n,t)` s'exécute en temps linéaire en `t`.