INTRODUCTION AUX COURBES ELLIPTIQUES

Abderrahmane NITAJ

Université de Caen, France

Rabat, 29 Octobre 2008

عبدالرحمان نتاج

CONTENU

CONTENU

Equation de Weiersrass

- $\mathbb{K}$ est un corps ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$,...), $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$.
- Une courbe elliptique sur $\mathbb{K}$ est définie par :
  - Une équation de Weiersrass (forme projective)

$$E : \quad Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

  - Un discriminant $\Delta \neq 0$.
  - Le point $\mathcal{O} = [0, 1, 0]$ est appelé point à l'infini.
- Pour $Z \neq 0$, on peut écrire $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, et l'équation de Weiersrass devient (forme affine)

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

- L'ensemble des points $\mathbb{K}$ rationnels est

$$E(K) = \left\{(x, y) \in \mathbb{K}^2, y^2 \cdots = \cdots + a_6\right\} \cup \{\mathcal{O}\}.$$

Equation de Weiersrass

- $\mathbb{K}$ est un corps ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$,...), $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$.
- Une courbe elliptique sur $\mathbb{K}$ est définie par :
  - Une équation de Weiersrass (forme projective)

$$E: \quad Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

  - Un discriminant $\Delta \neq 0$.
  - Le point $\mathcal{O} = [0, 1, 0]$ est appelé point à l'infini.
- Pour $Z \neq 0$, on peut écrire $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, et l'équation de Weiersrass devient (forme affine)

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

- L'ensemble des points $\mathbb{K}$ rationnels est

$$E(K) = \left\{(x, y) \in \mathbb{K}^2, y^2 \cdots = \cdots + a_6\right\} \cup \{\mathcal{O}\}.$$

Equation de Weiersrass

- $\mathbb{K}$ est un corps ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$,...), $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$.
- Une courbe elliptique sur $\mathbb{K}$ est définie par :
  - Une équation de Weiersrass (forme projective)

$$E: \quad Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

  - Un discriminant $\Delta \neq 0$.
  - Le point $\mathcal{O} = [0, 1, 0]$ est appelé point à l'infini.
- Pour $Z \neq 0$, on peut écrire $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, et l'équation de Weiersrass devient (forme affine)

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

- L'ensemble des points $\mathbb{K}$ rationnels est

$$E(K) = \left\{(x, y) \in \mathbb{K}^2, y^2 \cdots = \cdots + a_6\right\} \cup \{\mathcal{O}\}.$$

Equation de Weiersrass

- $\mathbb{K}$ est un corps ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$,...), $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$.
- Une courbe elliptique sur $\mathbb{K}$ est définie par :
  - Une équation de Weiersrass (forme projective)

$$E: \quad Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

  - Un discriminant $\Delta \neq 0$.
  - Le point $\mathcal{O} = [0, 1, 0]$ est appelé point à l'infini.
- Pour $Z \neq 0$, on peut écrire $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, et l'équation de Weiersrass devient (forme affine)

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

- L'ensemble des points $\mathbb{K}$ rationnels est

$$E(K) = \left\{(x, y) \in \mathbb{K}^2, y^2 \cdots = \cdots + a_6\right\} \cup \{\mathcal{O}\}.$$

Charactéristiue > 3

Equation de Weiersrass :

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

- Si la caractéristique de $\mathbb{K}$ est différente de 2, l'équation peut s'écrire :

$$E: \quad y^2 = x^3 + a_2'x^2 + a_4'x + a_6',$$

- Si la caractéristique de $\mathbb{K}$ est différente de 2 et de 3, l'équation peut s'écrire :

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

Le discriminant est $\Delta = -16(4a^3 + 27b^2) \neq 0$.

Charactéristiue > 3

Equation de Weiersrass :

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

- Si la caractéristique de $\mathbb{K}$ est différente de 2, l'équation peut s'écrire :

$$E: \quad y^2 = x^3 + a_2'x^2 + a_4'x + a_6',$$

- Si la caractéristique de $\mathbb{K}$ est différente de 2 et de 3, l'équation peut s'écrire :

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

Le discriminant est $\Delta = -16(4a^3 + 27b^2) \neq 0$.

Charactéristiue > 3

Equation de Weiersrass :

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

- Si la caractéristique de $\mathbb{K}$ est différente de 2, l'équation peut s'écrire :

$$E: \quad y^2 = x^3 + a_2'x^2 + a_4'x + a_6',$$

- Si la caractéristique de $\mathbb{K}$ est différente de 2 et de 3, l'équation peut s'écrire :

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

Le discriminant est $\Delta = -16(4a^3 + 27b^2) \neq 0$.

Charactéristiue $= 2$ ou $= 3$

- Si la caractéristique de $\mathbb{K}$ est 2, l'équation peut s'écrire :

$$E : \quad y^2 + xy = x^3 + ax^2 + b,$$

ou bien

$$E : \quad y^2 + ay = x^3 + bx + c,$$

- Si la caractéristique de $\mathbb{K}$ est 3, l'équation peut s'écrire :

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

ou bien

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

Charactéristiue $= 2$ ou $= 3$

- Si la caractéristique de $\mathbb{K}$ est 2, l'équation peut s'écrire :

$$E : \quad y^2 + xy = x^3 + ax^2 + b,$$

ou bien

$$E : \quad y^2 + ay = x^3 + bx + c,$$

- Si la caractéristique de $\mathbb{K}$ est 3, l'équation peut s'écrire :

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

ou bien

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

Unicité

Soit $E/\mathbb{K}$ définie par $E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$

- Cette équation est unique modulo les changements de varibles :
  - $x = u^2X + r$
  - $y = u^3Y + su^2X + t$ avec $r, s, t, u \in \mathbb{K}$.
- L'équation devient alors

$$E' : \quad Y^2 + a_1'XY + a_3'Y = X^3 + a_2'X^2 + a_4'X + a_6'.$$

Avec

- $ua_1' = a_1 + 2s$
- $u^2a_2' = a_2 - sa_1 + 3r - s^2$
- $u^3a_3' = a_3 + ra_1 + 2t$
- $u^4a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st$
- $u^6a_6' = a_6 + ra_4 + r^2a_2 + r^3 - ta^3 - t^2 - rta_1.$

Unicité

Soit $E/\mathbb{K}$ définie par $E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$

- Cette équation est unique modulo les changements de varibles :
  - $x = u^2X + r$
  - $y = u^3Y + su^2X + t$ avec $r, s, t, u \in \mathbb{K}$.
- L'équation devient alors

$$E': \quad Y^2 + a_1'XY + a_3'Y = X^3 + a_2'X^2 + a_4'X + a_6'.$$

Avec
  - $ua_1' = a_1 + 2s$
  - $u^2a_2' = a_2 - sa_1 + 3r - s^2$
  - $u^3a_3' = a_3 + ra_1 + 2t$
  - $u^4a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st$
  - $u^6a_6' = a_6 + ra_4 + r^2a_2 + r^3 - ta^3 - t^2 - rta_1.$

Unicité

Soit $E/\mathbb{K}$ définie par $E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$

- Cette équation est unique modulo les changements de varibles :
  - $x = u^2X + r$
  - $y = u^3Y + su^2X + t$ avec $r, s, t, u \in \mathbb{K}$.
- L'équation devient alors

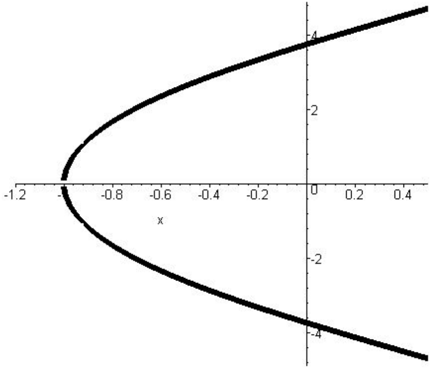
$$E' : \quad Y^2 + a_1'XY + a_3'Y = X^3 + a_2'X^2 + a_4'X + a_6'.$$

Avec
- $ua_1' = a_1 + 2s$
- $u^2a_2' = a_2 - sa_1 + 3r - s^2$
- $u^3a_3' = a_3 + ra_1 + 2t$
- $u^4a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st$
- $u^6a_6' = a_6 + ra_4 + r^2a_2 + r^3 - ta^3 - t^2 - rta_1.$

Représentation graphique

Exemple 1 :

Soit $E/\mathbb{R}$ définie par
$E: \quad y^2 = (x^2+x+14)(x+1) = x^3+2x^2+15x+14.$

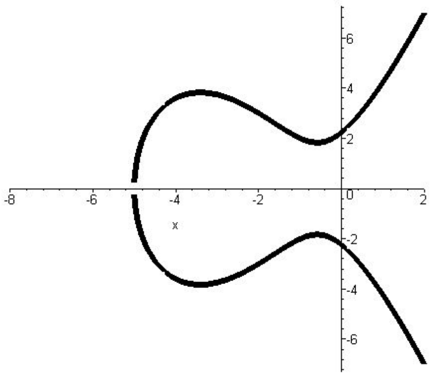


Représentation graphique

Exemple 2 :

Soit $E/\mathbb{R}$ définie par

$E: \quad y^2 = (x^2 + x + 1)(x + 5) = x^3 + 6x^2 + 6x + 5.$

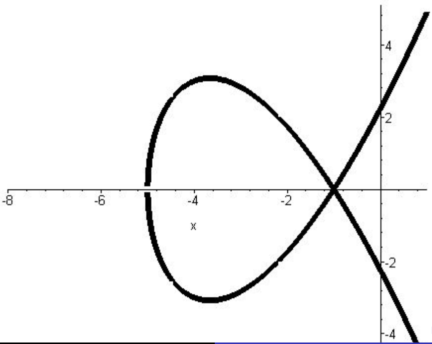


Représentation graphique

Exemple 3 :

Soit $E/\mathbb{R}$ définie par E : $\quad y^2 = (x+1)^2(x+5)$.

Ceci n'est pas une courbe elliptique car $\Delta = 0$.

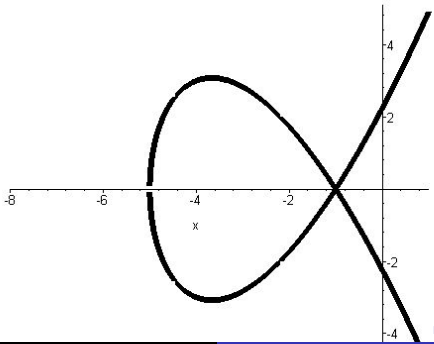


Représentation graphique

Exemple 3 :

Soit $E/\mathbb{R}$ définie par E : $y^2 = (x+1)^2(x+5)$.

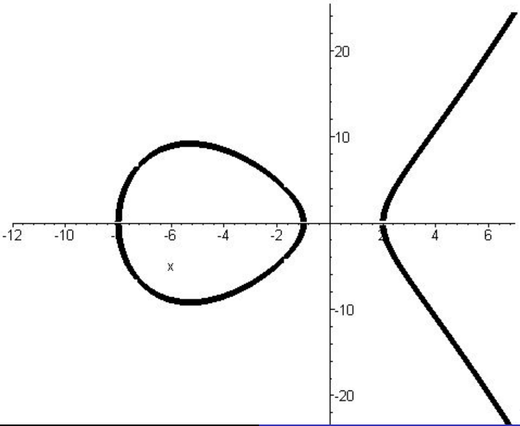
Ceci n'est pas une courbe elliptique car $\Delta = 0$.



Représentation graphique

Exemple 4 :

Soit $E/\mathbb{R}$ définie par E : $\quad y^2 = (x+8)(x+1)(x-2)$.

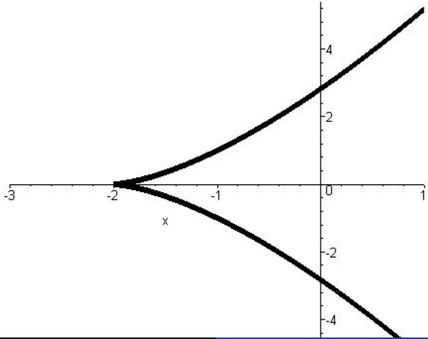


Représentation graphique

Exemple 3 :

Soit $E/\mathbb{R}$ définie par E : $\quad y^2 = (x+2)^3.$

Ceci n'est pas une courbe elliptique car $\Delta = 0$.

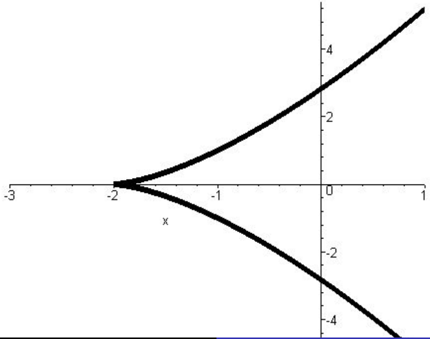


Représentation graphique

Exemple 3 :

Soit $E/\mathbb{R}$ définie par E : $\quad y^2 = (x+2)^3.$

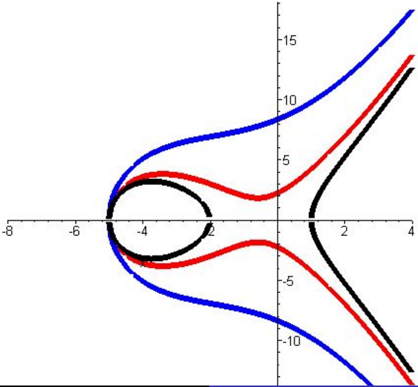
Ceci n'est pas une courbe elliptique car $\Delta = 0$.



Représentation graphique

Exemple 5 :

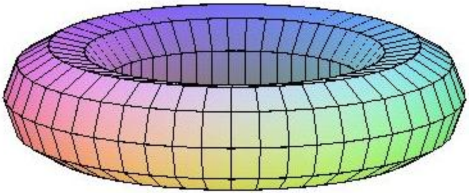
Soit $E/\mathbb{R}$ définie par $E: \quad y^2 = (x-1)(x+2)(x+5)$, $(x^2+x+14)(x+5)$, $(x^2+x+1)(x+5)$.



Représentation graphique

Exemple 4 :

Soit $E/\mathbb{C}$ définie par $E: \quad y^2 = x^3 + ax + b$. La courbe elliptique E est isomorphe à un tore complexe $\mathbb{C}/\mathbb{L}$ où $\mathbb{L}$ est un réseau de dimension 2.
La représentation graphique de E peut être transformée en tore.



Points rationnels d'une courbe elliptique

Définition :

Soit $E/\mathbb{K}$ définie par $E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.
L'ensemble des points $\mathbb{K}$ rationnels de E est

$$E(K) = \left\{(x, y) \in \mathbb{K}^2, y^2 \cdots = \cdots + a_6\right\} \cup \{\mathcal{O}\}.$$

Exemple 1 :

Soit E la courbe elliptique définie sur $\mathbb{Q}$ par $E: \quad y^2 + y = x^3 + x$.
L'ensemble des points $\mathbb{Q}$ rationnels de E contient les points

$$\mathcal{O}, (0,0), (0,-1), (1,1), (3,-6), (1,-2), (3,5), \left(-\frac{2}{9}, -\frac{17}{27}\right), \left(-\frac{2}{9}, -\frac{10}{27}\right), \left(\frac{33}{4}, -\frac{195}{8}\right), \left(\frac{33}{4}, \frac{187}{8}\right), \cdots.$$

Points rationnels d'une courbe elliptique

Définition :

Soit $E/\mathbb{K}$ définie par $E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.
L'ensemble des points $\mathbb{K}$ rationnels de E est

$$E(K) = \left\{(x,y) \in \mathbb{K}^2, y^2 \cdots = \cdots + a_6\right\} \cup \{\mathcal{O}\}.$$

Exemple 1 :

Soit E la courbe elliptique définie sur $\mathbb{Q}$ par $E: \quad y^2 + y = x^3 + x$.
L'ensemble des points $\mathbb{Q}$ rationnels de E contient les points

$$\mathcal{O}, (0,0), (0,-1), (1,1), (3,-6), (1,-2), (3,5), \left(-\frac{2}{9}, -\frac{17}{27}\right),$$
$$\left(-\frac{2}{9}, -\frac{10}{27}\right), \left(\frac{33}{4}, -\frac{195}{8}\right), \left(\frac{33}{4}, \frac{187}{8}\right), \ldots .$$

Points rationnels d'une courbe elliptique

Exemple 2 :

Soit E définie par $E: \quad y^2 + y = x^3 - 6x + 4$. L'ensemble des points $\mathbb{Q}$ rationnels de E est

$$E(K) = \{\mathcal{O}, (-1,3), (-1,-3), (2,-3), (2,0), (1,-1)\}.$$

Exemple 3 :

Soit $E/(\mathbb{Z}/13\mathbb{Z})$ définie par $E: \quad y^2 = x^3 - 5x + 8$. Il y a 20 points sur $\mathbb{Z}/13\mathbb{Z}$:

$$\mathcal{O}, (1,\pm 2), (4,0), (5,\pm 2), (6,\pm 5), (7,\pm 2), (8,\pm 5), (9,\pm 4),$$
$$(10,\pm 3), (11,\pm 6), (12,\pm 5).$$

Points rationnels d'une courbe elliptique

Exemple 2 :

Soit E définie par E : $y^2 + y = x^3 - 6x + 4$. L'ensemple des points $\mathbb{Q}$ rationnels de E est

$$E(K) = \{\mathcal{O}, (-1,3), (-1,-3), (2,-3), (2,0), (1,-1)\}.$$

Exemple 3 :

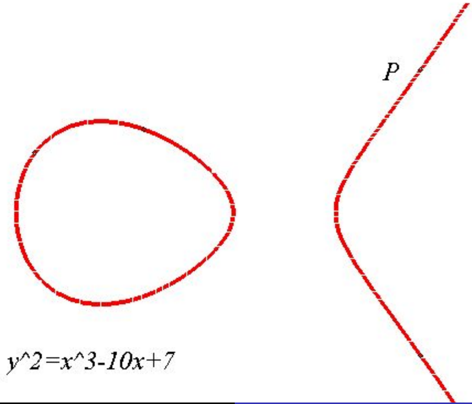
Soit $E/(\mathbb{Z}/13\mathbb{Z})$ définie par E : $y^2 = x^3 - 5x + 8$. Il y a 20 points sur $\mathbb{Z}/13\mathbb{Z}$:

$$\mathcal{O}, (1,\pm 2), (4,0), (5,\pm 2), (6,\pm 5), (7,\pm 2), (8,\pm 5), (9,\pm 4),$$
$$(10,\pm 3), (11,\pm 6), (12,\pm 5).$$

L'oposé d'un point

Soit $E/\mathbb{K}$ une courbe elliptique et $P \in E(\mathbb{K})$.

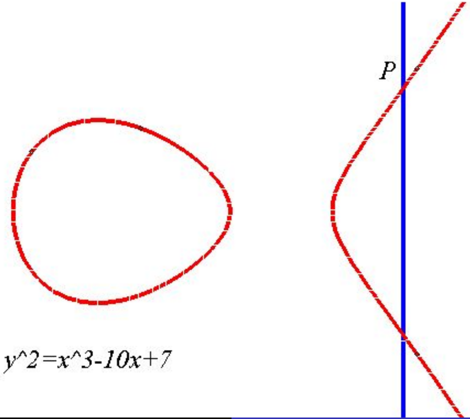
Comment placer le point $-P$?



L'oposé d'un point

Pour placer le point $-P$.

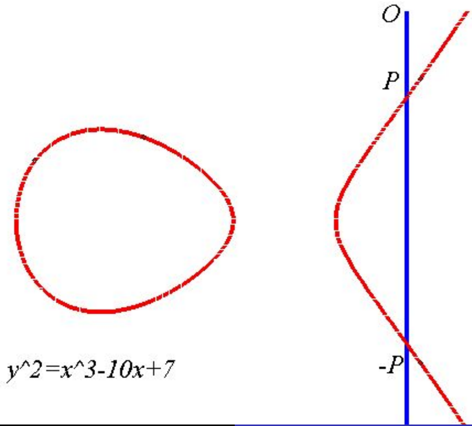
On trace la verticale qui passe par P.



L'oposé d'un point

Pour placer le point $-P$.

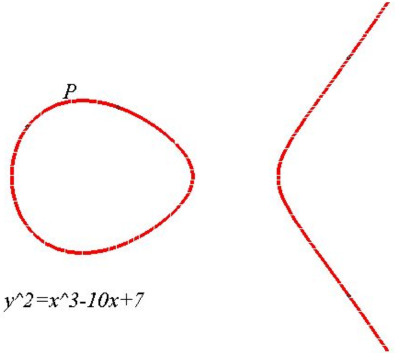
On obtient le point $-P$ à l'intersection avec la courbe.



Doubler un point

Soit $E/\mathbb{K}$ une courbe elliptique et $P \in E(\mathbb{K})$.

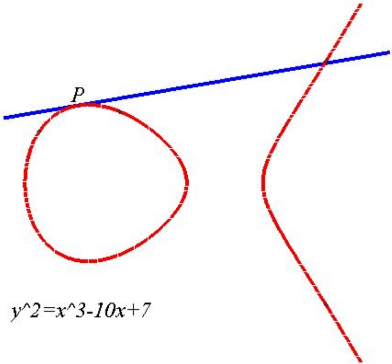
Comment placer le point $2P$ si $x_P \neq 0$?



Doubler un point

Pour placer le point $2P$ si $x_P \neq 0$.

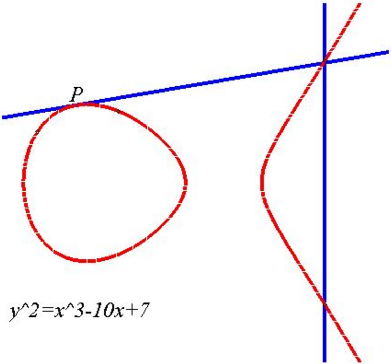
On trace la tangente en P.



Doubler un point

Pour placer le point $2P$ si $x_P \neq 0$.

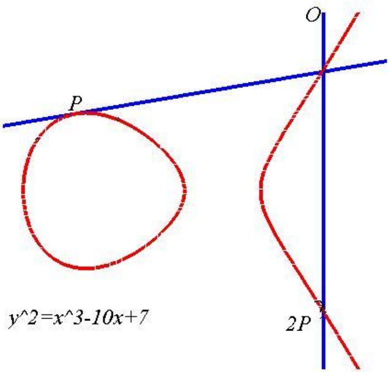
On trace la verticale.



Doubler un point

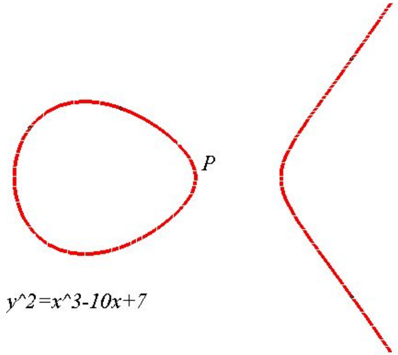
Pour placer le point $2P$ si $x_P \neq 0$.

On obtient le point $2P$.



Doubler un point

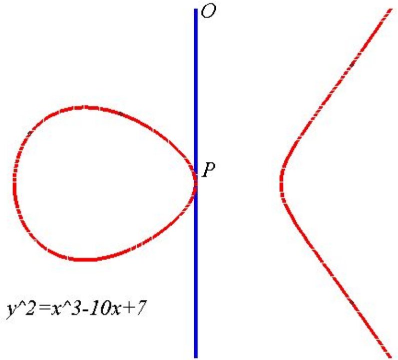
Comment placer le point $2P$ si $x_P = 0$?



Doubler un point

Pour placer le point $2P$ si $x_P = 0$.

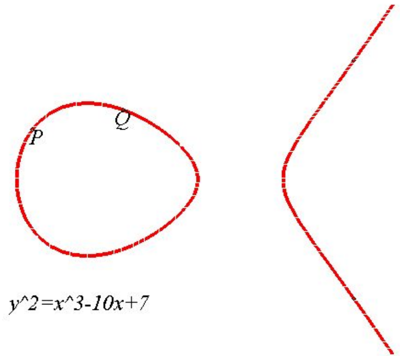
On trace la verticale en P. On obtient $2P = \mathcal{O}$.



Additionner deux points différents

Soit $E/\mathbb{K}$ une courbe elliptique et $P, Q \in E(\mathbb{K})$ avec $P \neq Q$.

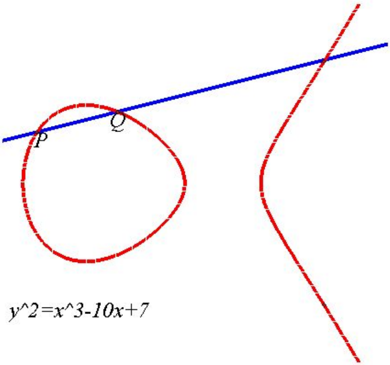
Comment placer le point $P+Q$?



Additionner deux points différents

Pour placer le point $P+Q$.

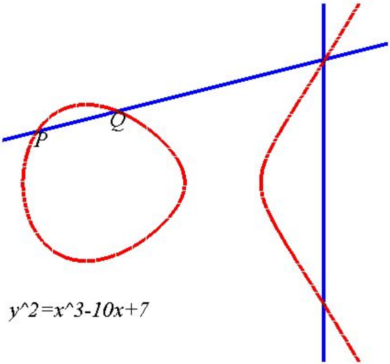
On trace la droite (PQ).



Additionner deux points différents

Pour placer le point $P+Q$.

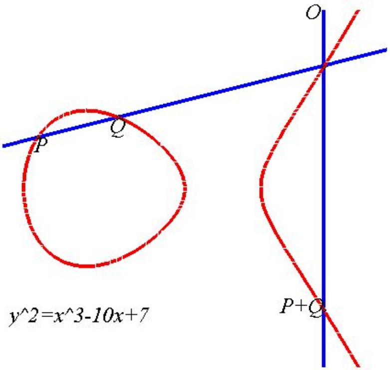
On trace la verticale au 3ème point d'intersection.



Additionner deux points différents

Pour placer le point $P+Q$.

On obtient le point $P+Q$.



Formules explicites d'addition

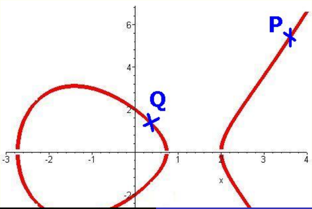
Points différents et non opposés

$P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$ sont deux points de $E(\mathbb{K})$ avec $x_P \neq x_Q$. Alors $P + Q = R = (x_R, y_R)$, avec

$$x_R = \lambda^2 - x_P - x_Q, \qquad y_R = -\lambda x_R - \nu,$$

et

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}, \qquad \nu = y_P - \lambda x_P.$$

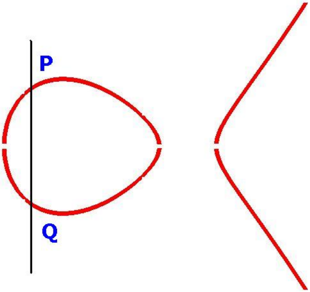


Formules explicites d'addition

Points différents et opposés

$P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$ sont deux points de $E(\mathbb{K})$ avec $x_P = x_Q$ et $y_P \neq y_Q$ alors

$$P + Q = \mathcal{O}.$$

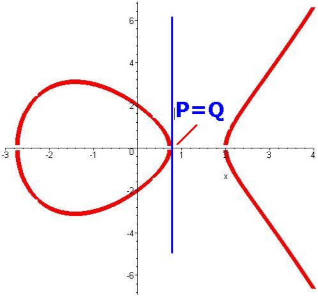


Formules explicites d'addition

Points identiques sur l'axe

$P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$ sont deux points de $E(\mathbb{K})$ avec $x_P = x_Q$ et $y_P = y_Q = 0$ alors

$$P + Q = 2P = \mathcal{O}.$$



Formules explicites d'addition

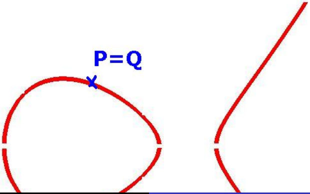
Points identiques

$P = (x_P, y_P)$ et $Q(x_Q, y_Q)$ sont deux points de $E(\mathbb{K})$ avec $x_P = x_Q$ et $y_P = y_Q \neq 0$ alors $P + Q = R = (x_R, y_R)$, avec

$$x_R = \lambda^2 - x_P - x_Q, \qquad y_R = -\lambda x_R - \nu,$$

et

$$\lambda = \frac{3x_P^2 + a}{2y_P}, \qquad \nu = y_P - \lambda x_P.$$



Points de torsion

Définition :

Soit $E/\mathbb{K}$ une courbe elliptique. L'ensemple des points de torsion est

$$E(\mathbb{K})_{\text{tors}} = \{P \in E(\mathbb{K}), \quad \exists m \in \mathbb{N}^* \quad mP = \mathcal{O}\}.$$

Points de torsion

Théorème (Lutz-Nagell, 1935-1937):

Soit $E/\mathbb{Q}$ une courbe elliptique à coefficients entiers. Si $P=(x,y)$ est un point de torsion de E, alors $x,y\in\mathbb{Z}$ et $y=0$ ou $y^2|\Delta$.

Théorème (Mazur, 1975):

Soit $E/\mathbb{Q}$ une courbe elliptique. Alors

$$E(\mathbb{Q})_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/m\mathbb{Z}, \quad m=1,2,3,4,5,6,7,8,9,10,12 \\ \text{ou} \\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2m\mathbb{Z}, \quad m=1,2,3,4. \end{cases}$$

Points de torsion

Théorème (Lutz-Nagell, 1935-1937):

Soit $E/\mathbb{Q}$ une courbe elliptique à coefficients entiers. Si $P = (x, y)$ est un point de torsion de E, alors $x, y \in \mathbb{Z}$ et $y = 0$ ou $y^2 | \Delta$.

Théorème (Mazur, 1975):

Soit $E/\mathbb{Q}$ une courbe elliptique. Alors

$$E(\mathbb{Q})_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/m\mathbb{Z}, \quad m = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12 \\ \text{ou} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, \quad m = 1, 2, 3, 4. \end{cases}$$

Points de torsion

Exemple 1 :

Soit $E/\mathbb{Q}$ définie par E : $y^2 = x^3 + x^2 - x$. Alors

$$E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (0,0), (1,1), (1,-1), (-1,1), (-1,-1)\} \simeq \mathbb{Z}/6\mathbb{Z}.$$

$P = (-1,-1) \in E(\mathbb{Q})$, alors $6P = \mathcal{O}$.

Exemple 2 :

Soit $E/\mathbb{Q}$ définie par E : $y^2 + y = x^3 - 1070x + 7812$. Alors

$$E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}.$$

$P = (34, 88) \in E(\mathbb{Q})$, alors $8P = \mathcal{O}$.

Points de torsion

Exemple 1 :

Soit $E/\mathbb{Q}$ définie par $E: \quad y^2 = x^3 + x^2 - x$. Alors

$$E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (0,0), (1,1), (1,-1), (-1,1), (-1,-1)\} \simeq \mathbb{Z}/6\mathbb{Z}.$$

$P = (-1,-1) \in E(\mathbb{Q})$, alors $6P = \mathcal{O}$.

Exemple 2 :

Soit $E/\mathbb{Q}$ définie par $E: \quad y^2 + y = x^3 - 1070x + 7812$. Alors

$$E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}.$$

$P = (34, 88) \in E(\mathbb{Q})$, alors $8P = \mathcal{O}$.

Structure de E(K)

Théorème (Mordell-Weil (1922-1928):

Soit $E/\mathbb{K}$ une courbe elliptique. Alors il existe un nombre fini de points $P_1, P_2, \cdots, P_n \in E(K)$ tels que tout point P de $E(\mathbb{K})$ s'écrit sous la forme

$$P = m_1P_1 + m_2P_2 + \cdots + m_nP_n \quad \text{avec} \quad m_1, m_2, \cdots, m_n \in \mathbb{Z}.$$

On a donc

$$E(K) \simeq \mathbb{Z}^r \oplus E(\mathbb{K})_{\text{tors}}$$

avec $r \in \mathbb{N}$, appelé rang de E.

Structure de E(K)

Exemple 1 :

Soit $E/\mathbb{K}$ définie par $E: \quad y^2 = x^3 - 2x$. L'ensemple des points $\mathbb{Q}$ rationnels de E est

$$E(\mathbb{Q}) = \langle (0,0), (-1,-1) \rangle,$$

où $(0,0)$ est un point d'ordre 2 et $(-1,-1)$ est un point d'ordre infini. Alors

$$E(\mathbb{Q}) = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

Structure de E(K)

Exemple 2 :

Soit $E/\mathbb{Q}$ définie par E : $\quad y^2 = x^3 + 4x$. L'ensemple des points $\mathbb{Q}$ rationnels de E est

$$E(\mathbb{Q}) = \langle (2,4) \rangle \ ,$$

où $(2,4)$ est un point d'ordre 4. Alors

$$E(\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z}$$

Structure de E(K)

Exemple 3 :

Soit $E/\mathbb{Q}$ définie par $E: \quad y^2 = x^3 - 82x$. L'ensemple des points $\mathbb{Q}$ rationnels de E est

$$E(\mathbb{Q}) = \langle (0,0), (-8,12), (-1,-9), (-9,-3) \rangle,$$

où $(0,0)$ est un point d'ordre 2 et les autres d'ordre infini. Alors

$$E(\mathbb{Q}) = \mathbb{Z}^3 \oplus \mathbb{Z}/2\mathbb{Z},$$

i.e. E est de rang 3.

Le rang d'une courbe elliptique

Conjecture "folklorique"

Il existe des courbes elliptiques $E/\mathbb{Q}$ de n'importe quel rang.

Exemple 1 (N. Elkies, 2006):

Soit $E/\mathbb{Q}$ définie par

$$\begin{aligned} E: \quad y^2+xy+y &= x^3-x^2 \\ &\quad -20067762415575526585033208209338542750930230312178956502x \\ &\quad +34481611795030556467032985690390720374855944359319180361266008296291939448732243429. \end{aligned}$$

Alors $E(\mathbb{Q}) = \mathbb{Z}^r \oplus \{\mathcal{O}\}$, avec $r \geq 28$, i.e. E est de rang ≥ 28.

Le rang d'une courbe elliptique

Conjecture "folklorique"

Il existe des courbes elliptiques $E/\mathbb{Q}$ de n'importe quel rang.

Exemple 1 (N. Elkies, 2006):

Soit $E/\mathbb{Q}$ définie par

$$\begin{aligned} E: \quad y^2 + xy + y \quad = \quad & x^3 - x^2 \\ & -20067762415575526585033208209338542750930230312178956502x \\ & +34481611795030556467032985690390720374855944359319180361266008 \\ & 296291939448732243429. \end{aligned}$$

Alors $E(\mathbb{Q}) = \mathbb{Z}^r \oplus \{\mathcal{O}\}$, avec $r \geq 28$, i.e. E est de rang ≥ 28.

CONTENU

Les corps finis

Les corps premiers $\mathbb{F}_p$

Soit p dun nombre premier. Alors $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z} \pmod{p}$ est un corps fini.

Exemples

- $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \mathbb{Z} \pmod{2} = \{0, 1\}$.
- $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z} = \mathbb{Z} \pmod{3} = \{-1, 0, 1\}$.
- $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z} = \mathbb{Z} \pmod{5} = \{-2, -1, 0, 1, 2\}$.

Les corps finis

Les corps premiers $\mathbb{F}_p$

Soit p dun nombre premier. Alors $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z} \pmod{p}$ est un corps fini.

Exemples

- $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \mathbb{Z} \pmod{2} = \{0, 1\}$.
- $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z} = \mathbb{Z} \pmod{3} = \{-1, 0, 1\}$.
- $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z} = \mathbb{Z} \pmod{5} = \{-2, -1, 0, 1, 2\}$.

Les corps finis

Le corps fini $\mathbb{F}_{2^3}$

On considère le polynôme $P(X) = X^3 + X + 1$ de $\mathbb{F}_2[X]$.
Alors

- P est iréductible car $P(0) = P(1) = 1$.
- $\mathbb{F}_2[X]/(P(X))$ est un corps.
- $\mathbb{F}_2[X]/(P(X)) = \{aX^2 + bX + c, \quad a, b, c \in \mathbb{F}_2\}$.
- $\mathbb{F}_2[X]/(P(X)) = \{0, 1, X, X^2, 1+X, 1+X^2, X+X^2, 1+X+X^2\}$.
- $\#\mathbb{F}_2[X]/(P(X)) = 8 = 2^3$.

$$\mathbb{F}_2[X]/(P(X)) = \mathbb{F}_{2^3}.$$

Les corps finis

Le corps fini $\mathbb{F}_{2^3}$

On considère le polynôme $P(X) = X^3 + X + 1$ de $\mathbb{F}_2[X]$.
Alors

- P est iréductible car $P(0) = P(1) = 1$.
- $\mathbb{F}_2[X]/(P(X))$ est un corps.
- $\mathbb{F}_2[X]/(P(X)) = \{aX^2 + bX + c, \quad a, b, c \in \mathbb{F}_2\}$.
- $\mathbb{F}_2[X]/(P(X)) = \{0, 1, X, X^2, 1 + X, 1 + X^2, X + X^2, 1 + X + X^2\}$.
- $\#\mathbb{F}_2[X]/(P(X)) = 8 = 2^3$.

$$\mathbb{F}_2[X]/(P(X)) = \mathbb{F}_{2^3}.$$

Les corps finis

Le corps fini $\mathbb{F}_{2^3}$

On considère le polynôme $P(X) = X^3 + X + 1$ de $\mathbb{F}_2[X]$.
Alors

- P est iréductible car $P(0) = P(1) = 1$.
- $\mathbb{F}_2[X]/(P(X))$ est un corps.
- $\mathbb{F}_2[X]/(P(X)) = \{aX^2 + bX + c, \quad a, b, c \in \mathbb{F}_2\}$.
- $\mathbb{F}_2[X]/(P(X)) = \{0, 1, X, X^2, 1+X, 1+X^2, X+X^2, 1+X+X^2\}$.
- $\#\mathbb{F}_2[X]/(P(X)) = 8 = 2^3$.

$$\mathbb{F}_2[X]/(P(X)) = \mathbb{F}_{2^3}.$$

Les corps finis

Le corps fini $\mathbb{F}_{2^3}$

On considère le polynôme $P(X) = X^3 + X + 1$ de $\mathbb{F}_2[X]$.
Alors

- P est iréductible car $P(0) = P(1) = 1$.
- $\mathbb{F}_2[X]/(P(X))$ est un corps.
- $\mathbb{F}_2[X]/(P(X)) = \{aX^2 + bX + c, \quad a, b, c \in \mathbb{F}_2\}$.
- $\mathbb{F}_2[X]/(P(X)) = \{0, 1, X, X^2, 1+X, 1+X^2, X+X^2, 1+X+X^2\}$.
- $\#\mathbb{F}_2[X]/(P(X)) = 8 = 2^3$.

$$\mathbb{F}_2[X]/(P(X)) = \mathbb{F}_{2^3}.$$

Les corps finis

Le corps fini $\mathbb{F}_{2^3}$

On considère le polynôme $P(X) = X^3 + X + 1$ de $\mathbb{F}_2[X]$.
Alors

- P est iréductible car $P(0) = P(1) = 1$.
- $\mathbb{F}_2[X]/(P(X))$ est un corps.
- $\mathbb{F}_2[X]/(P(X)) = \{aX^2 + bX + c, \quad a, b, c \in \mathbb{F}_2\}$.
- $\mathbb{F}_2[X]/(P(X)) = \{0, 1, X, X^2, 1+X, 1+X^2, X+X^2, 1+X+X^2\}$.
- $\#\mathbb{F}_2[X]/(P(X)) = 8 = 2^3$.

$$\mathbb{F}_2[X]/(P(X)) = \mathbb{F}_{2^3}.$$

Le corps fini $\mathbb{F}_{2^3}$

Addition

L'addition dans $\mathbb{F}_{2^3}$ se fait modulo 2 avec $1+1=0$. Exemples :

$$(1+X^2)+(X+X^2)=1+X, \qquad (1+X^2)+(1+X^2)=0.$$

Multiplication

La multiplication dans $\mathbb{F}_{2^3}$ se fait modulo 2 et X^3+X+1, avec $X^3=-X-1=X+1$. Exemple :

$$\begin{aligned}(1+X^2)\times(X+X^2) &= X+X^2+X^3+X^4\\ &= X+X^2+(X+1)+(X^2+X)\\ &= 1+X.\end{aligned}$$

L'addition est simple mais la multiplication est plus compliquée.

Le corps fini $\mathbb{F}_{2^3}$

Addition

L'addition dans $\mathbb{F}_{2^3}$ se fait modulo 2 avec $1+1=0$. Exemples :

$$(1+X^2)+(X+X^2)=1+X, \qquad (1+X^2)+(1+X^2)=0.$$

Multiplication

La multiplication dans $\mathbb{F}_{2^3}$ se fait modulo 2 et X^3+X+1, avec $X^3=-X-1=X+1$. Exemple :

$$\begin{aligned}(1+X^2)\times(X+X^2) &= X+X^2+X^3+X^4\\ &= X+X^2+(X+1)+(X^2+X)\\ &= 1+X.\end{aligned}$$

L'addition est simple mais la multiplication est plus compliquée.

Le corps fini $\mathbb{F}_{2^3}$

Addition

L'addition dans $\mathbb{F}_{2^3}$ se fait modulo 2 avec $1+1=0$. Exemples :

$$(1+X^2)+(X+X^2)=1+X, \qquad (1+X^2)+(1+X^2)=0.$$

Multiplication

La multiplication dans $\mathbb{F}_{2^3}$ se fait modulo 2 et X^3+X+1, avec $X^3=-X-1=X+1$. Exemple :

$$\begin{aligned}(1+X^2)\times(X+X^2) &= X+X^2+X^3+X^4\\ &= X+X^2+(X+1)+(X^2+X)\\ &= 1+X.\end{aligned}$$

L'addition est simple mais la multiplication est plus compliquée.

Le corps fini $\mathbb{F}_{2^3}$

Racines de $P(T) = T^3 + T + 1$ dans $\mathbb{F}_{2^3}$

On peut vérifier :

$$(X)^3 + (X) + 1 = 0 \qquad \text{et} \qquad (X^2)^3 + (X^2) + 1 = 0.$$

Ainsi P a deux racines dans $\mathbb{F}_{2^3}$. On note $\omega = X$. Alors

$$\begin{aligned} \omega^1 &= X, \quad \omega^2 = X^2, \quad \omega^3 = X + 1, \quad \omega^4 = X + X^2, \\ \omega^5 &= 1 + X + X^2, \quad \omega^6 = 1 + X^2, \quad \omega^7 = 1, \quad \omega^8 = X. \end{aligned}$$

Ainsi

$$\mathbb{F}_{2^3} = \langle \omega \rangle .$$

Le corps fini $\mathbb{F}_{2^3}$

Addition

L'addition dans $\mathbb{F}_{2^3} = \langle \omega \rangle$.
Exemple :

$$(1+X^2)+(X+X^2) = 1+X \Leftrightarrow \omega^6+\omega^4 = \omega^3.$$

Multiplication

La multiplication dans $\mathbb{F}_{2^3} = \langle \omega \rangle$ se fait modulo 7 pour les exposants. Exemple :

$$(1+X^2)\times(X+X^2) = 1+X \Leftrightarrow \omega^6\times\omega^4 = \omega^{10} = \omega^3.$$

La multiplication est simple mais l'addition est plus compliquée.

Le corps fini $\mathbb{F}_{2^3}$

Addition

L'addition dans $\mathbb{F}_{2^3} = \langle\omega\rangle$.
Exemple :

$$(1 + X^2) + (X + X^2) = 1 + X \Leftrightarrow \omega^6 + \omega^4 = \omega^3.$$

Multiplication

La multiplication dans $\mathbb{F}_{2^3} = \langle\omega\rangle$ se fait modulo 7 pour les exposants. Exemple :

$$(1 + X^2) \times (X + X^2) = 1 + X \Leftrightarrow \omega^6 \times \omega^4 = \omega^{10} = \omega^3.$$

La multiplication est simple mais l'addition est plus compliquée.

Le corps fini $\mathbb{F}_{2^3}$

Addition

L'addition dans $\mathbb{F}_{2^3} = \langle \omega \rangle$.
Exemple :

$$(1 + X^2) + (X + X^2) = 1 + X \Leftrightarrow \omega^6 + \omega^4 = \omega^3.$$

Multiplication

La multiplication dans $\mathbb{F}_{2^3} = \langle \omega \rangle$ se fait modulo 7 pour les exposants. Exemple :

$$(1 + X^2) \times (X + X^2) = 1 + X \Leftrightarrow \omega^6 \times \omega^4 = \omega^{10} = \omega^3.$$

La multiplication est simple mais l'addition est plus compliquée.

Les corps finis : description

Le théorème de Wedderburn

Tout corps fini est commutatif : $xy = yx$.

La caractéristique

Si $\mathbb{F}$ est un corps fini, alors il existe un nombre premier p tel que $p.1 = 0$ dans $\mathbb{F}$.
On dit que p est la caractéristique de $\mathbb{F}$.

$\mathbb{F}$ est un espace vectoriel

Si $\mathbb{F}$ est un corps fini de caractéristique p, alors

- $\mathbb{F}$ est un $\mathbb{F}_p$-espace vectoriel de dimension finie $n \geq 1$.
- $\#\mathbb{F} = p^n$.

Les corps finis : description

Le théorème de Wedderburn

Tout corps fini est commutatif : $xy = yx$.

La caractéristique

Si $\mathbb{F}$ est un corps fini, alors il existe un nombre premier p tel que $p.1 = 0$ dans $\mathbb{F}$.
On dit que p est la caractéristique de $\mathbb{F}$.

$\mathbb{F}$ est un espace vectoriel

Si $\mathbb{F}$ est un corps fini de caractéristique p, alors

- $\mathbb{F}$ est un $\mathbb{F}_p$-espace vectoriel de dimension finie $n \geq 1$.
- $\#\mathbb{F} = p^n$.

Les corps finis : description

Le théorème de Wedderburn

Tout corps fini est commutatif : $xy = yx$.

La caractéristique

Si $\mathbb{F}$ est un corps fini, alors il existe un nombre premier p tel que $p.1 = 0$ dans $\mathbb{F}$.
On dit que p est la caractéristique de $\mathbb{F}$.

$\mathbb{F}$ est un espace vectoriel

Si $\mathbb{F}$ est un corps fini de caractéristique p, alors

- $\mathbb{F}$ est un $\mathbb{F}_p$-espace vectoriel de dimension finie $n \geq 1$.
- $\#\mathbb{F} = p^n$.

Les corps finis : description

L'ordre d'un élément

Soit $\mathbb{F}$ un corps fini avec $\#\mathbb{F} = p^n$ et $a \in \mathbb{F}^*$. Alors il existe un entier $m \geq 1$ tel que

- $a^m = 1$.
- $m | (p^n - 1)$.
- $X^m - 1 = \displaystyle\prod_{i=0}^{m-1} \left(X - a^i\right)$.

Le nombre m s'appelle l'ordre de a.

Les corps finis : description

L'ordre d'un élément

Soit $\mathbb{F}$ un corps fini avec $\#\mathbb{F} = p^n$. Alors

- Si $m|(p^n - 1)$, il existe $a \in \mathbb{F}$ d'ordre m.
- En particulier, il existe $\omega \in \mathbb{F}$ d'ordre $p^n - 1$.
  On dit que ω est un élément primitif.

$\mathbb{F}^*$ est cyclique

Soit $\mathbb{F}$ un corps fini avec $\#\mathbb{F} = p^n$ et ω un élément primitif. Alors

- $\mathbb{F}^* = \langle \omega \rangle$.
- $\mathbb{F}^*$ est un groupe cyclique.

Les corps finis : description

L'ordre d'un élément

Soit $\mathbb{F}$ un corps fini avec $\#\mathbb{F} = p^n$. Alors

- Si $m|(p^n - 1)$, il existe $a \in \mathbb{F}$ d'ordre m.
- En particulier, il existe $\omega \in \mathbb{F}$ d'ordre $p^n - 1$.
  On dit que ω est un élément primitif.

$\mathbb{F}^*$ est cyclique

Soit $\mathbb{F}$ un corps fini avec $\#\mathbb{F} = p^n$ et ω un élément primitif. Alors

- $\mathbb{F}^* = \langle \omega \rangle$.
- $\mathbb{F}^*$ est un groupe cyclique.

Les corps finis

Les corps finis $\mathbb{F}_q$

- Soit $\mathbb{K}$ un corps fini. Alors le cardinal de $\mathbb{K}$ est une puissance d'un nombre premier:

$$\mathbb{K} = \mathbb{F}_q \quad \text{avec} \quad q = p^n, n \geq 1.$$

- Soit $q = p^n$ une puissance d'un nombre premier. Alors il existe un corps fini unique (à isomorphisme près) avec q éléments.

Les corps finis

Les corps finis $\mathbb{F}_q$

- Soit $\mathbb{K}$ un corps fini. Alors le cardinal de $\mathbb{K}$ est une puissance d'un nombre premier:

$$\mathbb{K} = \mathbb{F}_q \quad \text{avec} \quad q = p^n, n \geq 1.$$

- Soit $q = p^n$ une puissance d'un nombre premier. Alors il existe un corps fini unique (à isomorphisme près) avec q éléments.

Les corps finis

Groupes multiplicatifs $(\mathbb{F}_p^*, \times)$

Soit p un nombre premier. Le groupe $(\mathbb{F}_p^*, \times)$ est cyclique. C'est le groupe des racines $(p-1)$-èmes de l'unité :

$$\mathbb{F}_p^* = \left\{\omega, \omega^2, \cdots, \omega^{p-1} = 1\right\}.$$

Exemples

- Pour $\mathbb{F}_2^*$, $\omega = 1$.
- Pour $\mathbb{F}_3^*$, $\omega = 2$.
- Pour $\mathbb{F}_5^*$, $\omega = 2$.
- Pour $\mathbb{F}_{17}^*$, $\omega = 3$.

Les corps finis

Groupes multiplicatifs $(\mathbb{F}_p^*, \times)$

Soit p un nombre premier. Le groupe $(\mathbb{F}_p^*, \times)$ est cyclique. C'est le groupe des racines $(p-1)$-èmes de l'unité :

$$\mathbb{F}_p^* = \left\{\omega, \omega^2, \cdots, \omega^{p-1} = 1\right\}.$$

Exemples

- Pour $\mathbb{F}_2^*$, $\omega = 1$.
- Pour $\mathbb{F}_3^*$, $\omega = 2$.
- Pour $\mathbb{F}_5^*$, $\omega = 2$.
- Pour $\mathbb{F}_{17}^*$, $\omega = 3$.

Les corps finis

Les corps finis $\mathbb{F}_q$

Soit p un nombre premier et $q = p^n$. Le corps finis $\mathbb{F}_q$ est cyclique. C'est l'ensemble des racines du polynôme $X^q - X$ et admet un élément ω d'ordre maximal $q-1$, appelé élément primitif :

$$\mathbb{F}_q = \left\{0, \omega, \omega^2, \cdots, \omega^{q-1} = 1\right\}.$$

Exemples

- Pour $\mathbb{F}_{2^2}^*$, ω est une racine de $X^2 + X + 1$.
- Pour $\mathbb{F}_{2^3}^*$, ω est une racine de $X^3 + X + 1$.
- Pour $\mathbb{F}_{3^2}^*$, ω est une racine de $X^2 + 1$.
- Pour $\mathbb{F}_{2^4}^*$, ω est une racine de $X^4 + X + 1$.

Les corps finis

Les corps finis $\mathbb{F}_q$

Soit p un nombre premier et $q = p^n$. Le corps finis $\mathbb{F}_q$ est cyclique. C'est l'ensemble des racines du polynôme $X^q - X$ et admet un élément ω d'ordre maximal $q - 1$, appelé élément primitif :

$$\mathbb{F}_q = \left\{0, \omega, \omega^2, \cdots, \omega^{q-1} = 1\right\}.$$

Exemples

- Pour $\mathbb{F}^*_{2^2}$, ω est une racine de $X^2 + X + 1$.
- Pour $\mathbb{F}^*_{2^3}$, ω est une racine de $X^3 + X + 1$.
- Pour $\mathbb{F}^*_{3^2}$, ω est une racine de $X^2 + 1$.
- Pour $\mathbb{F}^*_{2^4}$, ω est une racine de $X^4 + X + 1$.

Les corps finis

Construction pratique de $\mathbb{F}_q$

Soit p un nombre premier et $q = p^n$. Le corps finis $\mathbb{F}_q$ est l'ensemble des racines du polynôme $X^q - X$. Pour construire $\mathbb{F}_q$

- On factorise le polynôme $X^q - X$ dans $\mathbb{F}_p[X]$ (algorithme Cantor-Zassenhaus ou de Berlekamp).
- On détermine une racine ω d'un d'un polynôme irréductible P de $\mathbb{F}_p[X]$ de degré n.

En résumé : $q = p^n$

- $\mathbb{F}_q = \langle\omega\rangle \cup \{0\}$.
- $\mathbb{F}_q = \mathbb{F}_p[X]/P(X)$, P est irréductible sur $\mathbb{F}_p$ et de degré n.

Les corps finis

Construction pratique de $\mathbb{F}_q$

Soit p un nombre premier et $q = p^n$. Le corps finis $\mathbb{F}_q$ est l'ensemble des racines du polynôme $X^q - X$. Pour construire $\mathbb{F}_q$

- On factorise le polynôme $X^q - X$ dans $\mathbb{F}_p[X]$ (algorithme Cantor-Zassenhaus ou de Berlekamp).
- On détermine une racine ω d'un d'un polynôme irréductible P de $\mathbb{F}_p[X]$ de degré n.

En résumé : $q = p^n$

- $\mathbb{F}_q = \langle\omega\rangle \cup \{0\}$.
- $\mathbb{F}_q = \mathbb{F}_p[X]/P(X)$, P est irréductible sur $\mathbb{F}_p$ et de degré n.

Retour aux courbes elliptiques. Un exemple sur $\mathbb{F}_{2^4}$

Soit E la courbe elliptique définie sur $\mathbb{F}_{2^4}$ par
$E: \quad y^2 + xy = x^3 + \omega^2 x + \omega^3$ avec $\omega^4 = \omega + 1$.

Propriétés

- $\#E(\mathbb{F}_q) = 12$.
- $E(\mathbb{F}_q) = \{\mathcal{O}, (\omega^{14}, \omega^7), (\omega^{10}, 1), (\omega^{13}, \omega^{10}), (\omega, \omega^{10}), (\omega^{12}, \omega^{10})\} \cup \{(0, \omega^9), (\omega^{12}, \omega^3), (\omega, \omega^8), (\omega^{13}, \omega^9), (\omega^{10}, \omega^5), (\omega^{14}, \omega)\}$
- $P = (\omega^{12}, \omega^{10})$, $Q = (\omega, \omega^8)$. Alors $P + Q = (\omega^{14}, \omega^7)$.

Le nombre de points

$\#E(\mathbb{F}_q)$

Soit p un nombre premier et $q = p^n$. Alors

$$\#E(\mathbb{F}_q) = 1 + q + \sum_{x \in \mathbb{F}_q} \chi\left(x^3 + ax + b\right),$$

où χ est le caractère quadratique :

$$\chi(r) = \begin{cases} +1 & \text{si } r \text{ est un carré dans } \mathbb{F}_q, \\ 0 & \text{si } r = 0, \\ -1 & \text{si } r \text{ n'est pas un carré dans } \mathbb{F}_q. \end{cases}$$

Structure de $E(\mathbb{F}_q)$

Théorème [Deuring (1941)]

Soit p un nombre premier et $q = p^n$. Alors $E(\mathbb{F}_q)$ est un groupe cyclique ou le produit de deux groupes cycliques :

$$E(\mathbb{F}_q) \cong \begin{cases} \mathbb{Z}/M\mathbb{Z}, & \text{avec} \quad M = \#E(\mathbb{F}_q) \\ \text{ou} & \\ \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/L\mathbb{Z}, & \text{avec} \quad M|L, ML = \#E(\mathbb{F}_q). \end{cases}$$

Exemple 1:

Soit E la courbe définie sur $(\mathbb{F}_{7^2})$ par $E: \quad y^2 = x^3 + 2x + 4$. Alors

$$E(\mathbb{F}_q) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} = \langle (1,0), (\omega^{19}, \omega^2) \rangle,$$

où ω est un générateur de $(\mathbb{F}_{7^2})$.

Structure de $E(\mathbb{F}_q)$

Théorème [Deuring (1941)]

Soit p un nombre premier et $q = p^n$. Alors $E(\mathbb{F}_q)$ est un groupe cyclique ou le produit de deux groupes cycliques :

$$E(\mathbb{F}_q) \cong \begin{cases} \mathbb{Z}/M\mathbb{Z}, & \text{avec} \quad M = \#E(\mathbb{F}_q) \\ \text{ou} & \\ \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/L\mathbb{Z}, & \text{avec} \quad M|L, ML = \#E(\mathbb{F}_q). \end{cases}$$

Exemple 1:

Soit E la courbe définie sur $(\mathbb{F}_{7^2})$ par E : $y^2 = x^3 + 2x + 4$. Alors

$$E(\mathbb{F}_q) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} = \langle (1,0), (\omega^{19}, \omega^2) \rangle,$$

où ω est un générateur de $(\mathbb{F}_{7^2})$.

Le théorème de Hasse

Théorème (Hasse, 1933)

Soit p un nombre premier et $q = p^k$. Soit E une courbe elliptique défine par

$$E : \qquad y^2 = x^3 + ax + b, \quad \text{avec} \quad a, b \in \mathbb{F}_q.$$

Alors le nombre $\#E(\mathbb{F}_q)$ de points de $E(\mathbb{F}_q)$ vérifie

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

Exemple :

Soit E définie sur $(\mathbb{Z}/13\mathbb{Z})$ par $E : \quad y^2 = x^3 - 5x + 8$.
Alors $\#E(\mathbb{F}_{13}) = 20$ et on a bien
$|\#E(\mathbb{F}_{13}) - (13+1)| = |20 - 14| = 6 < 2\sqrt{13}$.

Le théorème de Hasse

Théorème (Hasse, 1933)

Soit p un nombre premier et $q = p^k$. Soit E une courbe elliptique défine par

$$E : \qquad y^2 = x^3 + ax + b, \quad \text{avec} \quad a, b \in \mathbb{F}_q.$$

Alors le nombre $\#E(\mathbb{F}_q)$ de points de $E(\mathbb{F}_q)$ vérifie

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

Exemple :

Soit E définie sur $(\mathbb{Z}/13\mathbb{Z})$ par $E : \quad y^2 = x^3 - 5x + 8.$
Alors $\#E(\mathbb{F}_{13}) = 20$ et on a bien
$|\#E(\mathbb{F}_{13}) - (13+1)| = |20 - 14| = 6 < 2\sqrt{13}.$

Calcul de $\#E(\mathbb{F}_p)$

Recherche exhaustive

Soit E défine sur $E(\mathbb{F}_p)$ par $E: \ y^2 = x^3 + ax + b$.
Pour chaque $x = 1, 2, \cdots, p-1$, on peut tester si $x^3 + ax + b$ est un carré dans $\mathbb{F}_p$ par le critère d'Euler :

$$d \quad \text{est un carré modulo } p \quad \Longleftrightarrow d^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Cette méthode a une complexité de $\mathcal{O}(p \log p) = \mathcal{O}(p^{1+\varepsilon})$.

Faisabilité

Cette méthode est assez efficace pour de très petites valeurs $p < 200$.

Calcul de $\#E(\mathbb{F}_p)$

La méthode de Shanks (1971)

Cette méthode a une complexité de $\mathcal{O}(p^{\frac{1}{4}+\varepsilon})$.

Faisabilité

Assez efficace pour des petites valeurs $p < 10^{20}$.

La méthode de Schoof (1985) [+Atkin (1988)+Elkies (1991) $\Longleftrightarrow$ Méthode SEA.

Cette méthode a une complexité de $\mathcal{O}((\log p)^6)$.

Faisabilité

Assez efficace pour les grandes valeurs $10^{20} < p < 10^{??}$.

Calcul de $\#E(\mathbb{F}_p)$

La méthode de Shanks (1971)

Cette méthode a une complexité de $\mathcal{O}(p^{\frac{1}{4}+\varepsilon})$.

Faisabilité

Assez efficace pour des petites valeurs $p < 10^{20}$.

La méthode de Schoof (1985) [+Atkin (1988)+Elkies (1991) $\Longleftrightarrow$ Méthode SEA.

Cette méthode a une complexité de $\mathcal{O}((\log p)^6)$.

Faisabilité

Assez efficace pour les grandes valeurs $10^{20} < p < 10^{??}$.

Calcul de $\#E(\mathbb{F}_p)$

La méthode de Shanks (1971)

Cette méthode a une complexité de $\mathcal{O}(p^{\frac{1}{4}+\varepsilon})$.

Faisabilité

Assez efficace pour des petites valeurs $p < 10^{20}$.

La méthode de Schoof (1985) [+Atkin (1988)+Elkies (1991) $\Longleftrightarrow$ Méthode SEA.

Cette méthode a une complexité de $\mathcal{O}((\log p)^6)$.

Faisabilité

Assez efficace pour les grandes valeurs $10^{20} < p < 10^{??}$.

Calcul de $\#E(\mathbb{F}_p)$

La méthode de Shanks (1971)

Cette méthode a une complexité de $\mathcal{O}(p^{\frac{1}{4}+\varepsilon})$.

Faisabilité

Assez efficace pour des petites valeurs $p < 10^{20}$.

La méthode de Schoof (1985) [+Atkin (1988)+Elkies (1991) $\Longleftrightarrow$ Méthode SEA.

Cette méthode a une complexité de $\mathcal{O}((\log p)^6)$.

Faisabilité

Assez efficace pour les grandes valeurs $10^{20} < p < 10^{??}$.

Points de torsion de $\mathbb{F}_q$

Définition

Soit E une courbe elliptique défine sur $E(\mathbb{F}_q)$. Soit $n \in \mathbb{Z}$. L'ensemble des points de n torsion est

$$E[n] = \{P \in E(\mathbb{F}_q), \quad nP = \mathcal{O}\}.$$

Théorème

- Pour chaque $n \in \mathbb{Z}$, $E[n]$ est fini.
- Si $\gcd(q, n) = 1$, alors $\#E[n] = n^2$.
- $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Points de torsion de $\mathbb{F}_q$

Définition

Soit E une courbe elliptique défine sur $E(\mathbb{F}_q)$. Soit $n \in \mathbb{Z}$.
L'ensemble des points de n torsion est

$$E[n] = \{P \in E(\mathbb{F}_q), \quad nP = \mathcal{O}\}.$$

Théorème

- Pour chaque $n \in \mathbb{Z}$, $E[n]$ est fini.
- Si $\gcd(q, n) = 1$, alors $\#E[n] = n^2$.
- $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

CONTENU

Test de primalité

Théorème [Goldwasser-Kilian, (1986)]

Soit N un nombre entier premier avec 6. S'il existe un entier m et un point P de la courbe elliptique définie par le point $\mathcal{O}$ et par l'équation

$$Y^2 = x^3 + ax + b \pmod N,$$

vérifiant

- m a un facteur premier $d > \left(N^{\frac{1}{4}} + 1\right)^2$,
- $mP = \mathcal{O}$,
- $\frac{m}{d}P \neq \mathcal{O}$,

alors N est un nombre premier.

Test de primalité

ECPP [Atkin-Morain, (1990)]

Le test de primalité ECPP (Elliptic Curve Primality Proving) est basé sur le critère de Goldwasser-Kilian et est très efficace et sa complexité est polynômiale:

$$\mathcal{O}\left((\log N)^4\right).$$

Un bel exemple de nombre premier avec ECPP (2004)

Le nombre suivant est premier ($\approx 10^{15071}$) :

$$2638^{4405} + 4405^{2638}.$$

Test de primalité

ECPP [Atkin-Morain, (1990)]

Le test de primalité ECPP (Elliptic Curve Primality Proving) est basé sur le critère de Goldwasser-Kilian et est très efficace et sa complexité est polynômiale:

$$\mathcal{O}\left((\log N)^4\right).$$

Un bel exemple de nombre premier avec ECPP (2004)

Le nombre suivant est premier ($\approx 10^{15071}$) :

$$2638^{4405} + 4405^{2638}.$$

Factorisation

La méthode ECM [H.W. Lenstra, (1986)]

La méthode ECM (Elliptic Curve Method) est une généralisation de la méthode $p-1$ de Polard. Le domaine de calcul est $E(\mathbb{Z}/N\mathbb{Z})$ où E est une courbe elliptique aléatoirement choisie. Pour $P \in E(\mathbb{Z}/N\mathbb{Z})$, la méthode consiste à calculer des points mP jusqu'à ce que un dénominateur contienne un facteur de N . Elle permet de trouver les petits facteurs d'un entier N.

Un record avec ECM

Avec ECMNET project de l'INRIA-Loria, un grand facteur premier a été déterminé par B. Dodson en 2006:

$$p \approx 10^{67}, \qquad p | 10^{381} + 1.$$

Factorisation

La méthode ECM [H.W. Lenstra, (1986)]

La méthode ECM (Elliptic Curve Method) est une généralisation de la méthode $p-1$ de Polard. Le domaine de calcul est $E(\mathbb{Z}/N\mathbb{Z})$ où E est une courbe elliptique aléatoirement choisie. Pour $P \in E(\mathbb{Z}/N\mathbb{Z})$, la méthode consiste à calculer des points mP jusqu'à ce que un dénominateur contienne un facteur de N . Elle permet de trouver les petits facteurs d'un entier N.

Un record avec ECM

Avec ECMNET project de l'INRIA-Loria, un grand facteur premier a été déterminé par B. Dodson en 2006:

$$p \approx 10^{67}, \qquad p|10^{381}+1.$$

Le problème du logarithme discret

Soit E une courbe elliptique définie sur $\mathbb{F}_p$. Soit P et Q deux points de $E(\mathbb{F}_p)$ tels que $Q \in \langle P \rangle$.

DLP.

Déterminer un entier n tel que $Q = nP$.

- Si $\#E(\mathbb{F}_p) \approx 10^{60}$ est premier, ce problème est difficile.
- La cryptograhie des téléphones cellulaires est basée sur ce problème.

Le cryptosystème El Gamal

Principe [Taher El Gamal (1985)]

Ali veut envoyer un message secret à Baba, en utilisant le cryptosystème El Gamal.

Préparation de Baba

- Baba choisit une courbe elliptique $E: \quad y^2 = x^3 + Ax + B$ sur corps fini $\mathbb{F}_q$ et un point P de $E(\mathbb{F}_q)$.
- Baba choisit un entier b et calcule bP.
- Baba publie q, E, P et bP et garde secret la clé b.

Le cryptosystème El Gamal

Principe [Taher El Gamal (1985)]

Ali veut envoyer un message secret à Baba, en utilisant le cryptosystème El Gamal.

Préparation de Baba

- Baba choisit une courbe elliptique $E : \quad y^2 = x^3 + Ax + B$ sur corps fini $\mathbb{F}_q$ et un point P de $E(\mathbb{F}_q)$.
- Baba choisit un entier b et calcule bP.
- Baba publie q, E, P et bP et garde secret la clé b.

Le cryptosystème El Gamal

Principe [Taher El Gamal (1985)]

Ali veut envoyer un message secret à Baba, en utilisant le cryptosystème El Gamal.

Cryptage de Ali

- Ali transforme son message secret M en un entier m.
- Ali calcule une valeur y à l'aide de la courbe elliptiuqe de Baba : $y^2 = m^3 + Am + B$.
- Ali choisit un entier k et calcule kP, kbP et $m + kbP$.
- Ali envoie à Baba les quantités kP et $(m, y) + kbP$ et garde secret la clé k (et son mesage secret clair m).

Le cryptosystème El Gamal

Principe [Taher El Gamal (1985)]

Ali veut envoyer un message secret à Baba, en utilisant le cryptosystème El Gamal.

Décryptage de Baba

- Baba reçoit kP et $(m, y) + kbP$.
- Baba calcule bkP, $-bkP$ puis retrouve $(m, y) = (-bkP) + ((m, y) + kbP)$.

Sécurité du cryptosystème El Gamal

La sécurité de ce système est basée sur le problème du logarithme discrer. En effet, les quantités bP et kP peuvent être interceptées, mais il est très difficile de calculer k, b ou même kbP (Problème de Diffie-Hellman).

Le cryptosystème El Gamal

Principe [Taher El Gamal (1985)]

Ali veut envoyer un message secret à Baba, en utilisant le cryptosystème El Gamal.

Décryptage de Baba

- Baba reçoit kP et $(m, y) + kbP$.
- Baba calcule bkP, $-bkP$ puis retrouve $(m, y) = (-bkP) + ((m, y) + kbP)$.

Sécurité du cryptosystème El Gamal

La sécurité de ce système est basée sur le problème du logarithme discrer. En effet, les quantités bP et kP peuvent être interceptées, mais il est très difficile de calculer k, b ou même kbP (Problème de Diffie-Hellman).

Le cryptosystème ECES

Principe [Menezes-Qu-Vanstone (1995)]

ECES=Elliptic Curve Encryption System

Ali veut envoyer un message secret à Baba, en utilisant le cryptosystème ECES.

Préparation de Baba

- Baba choisit une courbe elliptique $E: \quad y^2 = x^3 + Ax + B$ sur corps fini $\mathbb{F}_q$ et un point P de $E(\mathbb{F}_q)$.
- Baba choisit un entier b et calcule bP.
- Baba publie q, E, P et bP et garde secret la clé b.

Le cryptosystème ECES

Principe [Menezes-Qu-Vanstone (1995)]

ECES=Elliptic Curve Encryption System

Ali veut envoyer un message secret à Baba, en utilisant le cryptosystème ECES.

Préparation de Baba

- Baba choisit une courbe elliptique $E: \quad y^2 = x^3 + Ax + B$ sur corps fini $\mathbb{F}_q$ et un point P de $E(\mathbb{F}_q)$.
- Baba choisit un entier b et calcule bP.
- Baba publie q, E, P et bP et garde secret la clé b.

Le cryptosystème ECES

Principe [Menezes-Qu-vanstone (1995)]

Ali veut envoyer un message secret à Baba, en utilisant le cryptosystème ECES.

Cryptage de Ali

- Ali transforme son message secret M en un entier m avec $1 \leq m < q$.
- Ali choisit un entier k et calcule kP, $kbP = (x_A, y_A)$.
- Ali calcule $c = mx_A \pmod{q}$.
- Ali envoie à Baba les quantités kP et c et garde secret la clé k (et son mesage secret clair m).

Le cryptosystème ECES

Principe [Menezes-Qu-vanstone (1995)]

Ali veut envoyer un message secret à Baba, en utilisant le cryptosystème ECES.

Décyptage de Baba

- Baba reçoit kP et c.
- Baba calcule $bkP = (x_A, y_A)$.
- Baba calcule $m = cx_A^{-1} \pmod q$.

Sécurité du cryptosystème ECES

Sa sécurité est basé sur le problème du logarithme discrer. En effet, les quantités bP, kP et $mx_A \pmod q$ peuvent être interceptées, mais il est très difficile de calculer k, b, m ou x_A.

Le cryptosystème ECES

Principe [Menezes-Qu-vanstone (1995)]

Ali veut envoyer un message secret à Baba, en utilisant le cryptosystème ECES.

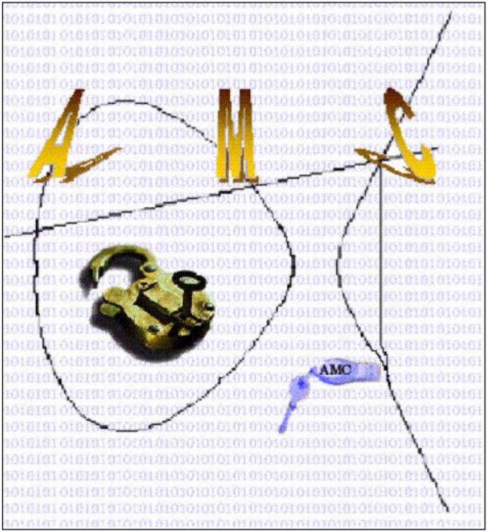
Décyptage de Baba

- Baba reçoit kP et c.
- Baba calcule $bkP = (x_A, y_A)$.
- Baba calcule $m = cx_A^{-1} \pmod q$.

Sécurité du cryptosystème ECES

Sa sécurité est basé sur le problème du logarithme discrer. En effet, les quantités bP, kP et $mx_A \pmod q$ peuvent être interceptées, mais il est très difficile de calculer k, b, m ou x_A.

Merci



شكرا