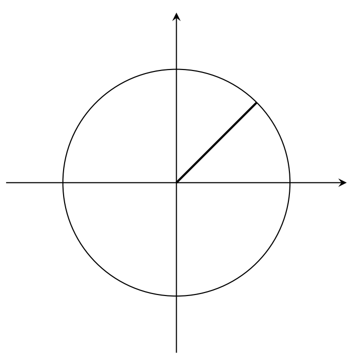
Courbes elliptiques

19 mars 2021

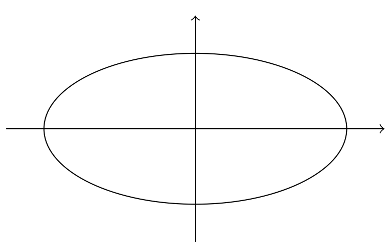
Même niveau de sécurité que RSA & DLP en utilisant des opérandes beaucoup plus petites (160-256 bits versus 1024-3072 bits pour RSA).

Avoir un but d'avoir un groupe cyclique (ensemble d'élements avec operateur et générateur pour être cyclique)

$$x^2 + y^2 = r^2, (x, y) \in \mathbb{R}$$



$$ax^2 + by^2 = c, (x, y) \in \mathbb{R}$$

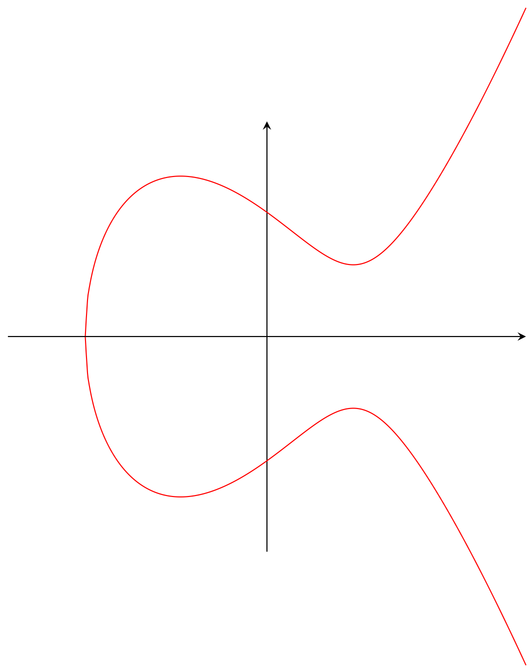


Ellipse

Exemple de courbe qui sont des ensemble de points (x, y) qui sont des solutions à une équation.

Définition : Courbe elliptique sur $\mathbb{Z}_p$ est l'ensemble de tuples $(x, y) \in \mathbb{Z}_p$ tel que $y^2 \equiv x^3 + ax + b \mod p$ muni d'un point abstraite (point à l'infini $\mathcal{O}$) où $a, b \in \mathbb{Z}_p$ et $4a^3 + 27b^2 \neq 0 \mod p$.

Courbe elliptique : courbe non-régulière (lisse), $\emptyset$ intersection, $\emptyset$ sommets ($-16(4a^3 + 27b^2) \neq 0$)



Symmétrie sur x,

$$y_i = \pm\sqrt{x_i^3 + ax_i + b}$$

points $y = 0$? $0 \equiv x^3 + ax + b \mod p$

1 ou 3 racines avec equations cubiques

Circonférence d'un cercle : $2\pi r$ ou πd Pour les courbes elliptiques, c'est plus compliqué…

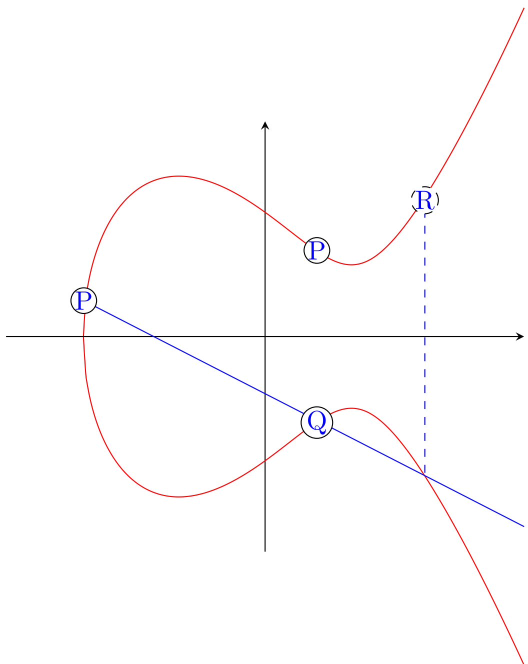
Défini un ensemble d'éléments, définir opération d'addition (+).

$$P(x_1, y_1) + Q(x_2, y_2) = R(x_3, y_3)$$

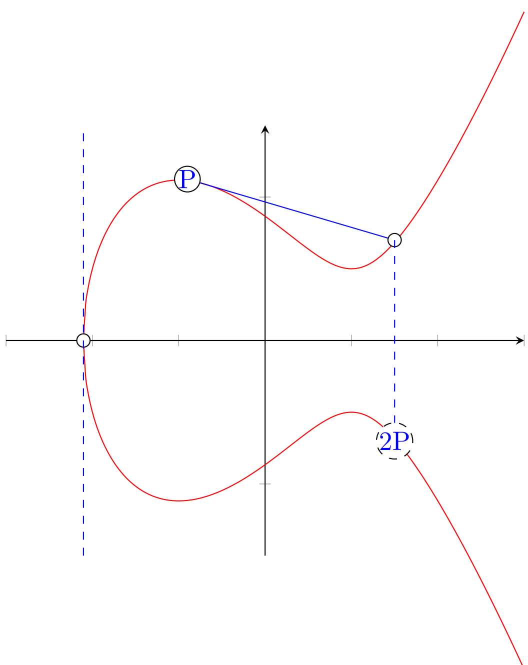
$$x_3 = x_1 + x_2, y_3 = y_1 + y_2$$

ne fonctionne pas (pas de fermeture)

1. Addition de point $P + Q$



2. Doubler le point $P + P = 2P$



Ce qui satisfie les critères d'un groupe :

- ✓ Fermeture
- ✓ Associatif
- ✓ $\exists 1 \in \mathcal{G}$
- ✓ $\exists a^{-1} \in \mathcal{G}$

$$a + a^{-1} = e$$

Les formules

$$\overbrace{(x_1, y_1)}^{P} + \overbrace{(x_2, y_2)}^{Q} = \overbrace{(x_3, y_3)}^{R}$$

$$x_5 = S^2 - x_1 - x_2 \mod p$$

$$S = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \mod p; & P \neq Q, \\ \frac{3x^2 + a}{2y_1} \mod p; & P = Q \end{cases}$$

$$y_3 = S(x_1 - x_3) - y_1 \mod p$$

$$P + \mathcal{G} = P$$

Inverse : $P = (x_p, y_p) \Rightarrow P^{-1} = (x_p, -y_p) = -P$

$$GF(p) \rightarrow -y_p \equiv p - y_p \mod p, -P = (x_p, p - y_p)$$

$$P + -P = \mathcal{O}$$

Ex : $\mathbb{Z}_{17}$, E : $y^2 \equiv x^3 + 2x + 2 \mod 17$ point : $(5, 1)$
Est-ce que point dans eq ? $2P = (5, 1) + (5, 1) \cdot (x_3, y_2)$

$$S = \frac{3x_1^2 + a}{2y_1} = \frac{3 \cdot 5^2 + 2}{2 \cdot 1} \equiv \frac{9}{2} \equiv 9 \cdot 2^{-1} = 9 \cdot 9 \equiv 13 \mod 17$$

Extended Euclidian $1 = 5 \cdot 17 + t \cdot 2, t = 2^{-1}$

$$x_3 = S^2 - x_1 - x_2 = 13^2 - 5 - 5 = 159 \equiv 6 \mod 17$$

$$y_3 = S(x_1 - x_2) - y_1 = 13(5 - 6) - 1 = -14 \equiv 3 \mod 17$$

$$2P = (5, 1) + (5, 1), = (6, 3)$$

$$
\begin{aligned}
y^2 &\equiv x^3 + 2x + 2 \mod 17 \\
3^2 &\equiv 6^3 + 2 \cdot 6 + 2 \mod 17 \\
9 = 230 &\equiv 9 \mod 17 \checkmark
\end{aligned}
$$

Théorème : Les points sur une courbe elliptique muni de $\mathcal{O}$ ont des sous-groupes cycliques. Sous certaines conditions, tout les points sous une courbe elliptique forme un groupe cyclique.

E : $y^2 \equiv x^3 + 2x + 2 \mod 17$

$$\#E = 19$$

Essayons avec $(5, 1)$:

$$
\begin{aligned}
P &= (5,1) \\
2P &= (5,1) + (5,1) = (6,2) \\
3P &= 2P + P = (10,6) \\
4P &= (3,1) \\
5P &= (9,6) \\
6P &= (16,13) \\
7P &= (0,6) \\
8P &= (13,7) \\
9P &= (7,6)
\end{aligned}
$$

$$
\begin{aligned}
10P &= (7,11) \\
11P &= (13,10) \\
12P &= (0,11) \\
13P &= (16,4) \\
14P &= (9,1) \\
15P &= (3,16) \\
16P &= (10,11) \\
17P &= (6,14) \\
18P &= (5,16) \\
19P &= \mathcal{O}
\end{aligned}
$$

Theorème de Hasse (à l'examen) : Étant donné une courbe elliptique E mod p, le nombre de points sur la courbe (#E) est borné par $p + 1 - 2\sqrt{p} \leq \#E \leq p + 1 + 2\sqrt{p}$

$$\alpha^a \mod p = A$$

Pour un cycle 2^{160} éléments, faut que $p \Rightarrow 160$ bits.

Elliptic Curve Discrete Logarithm Problem (ECDLP)

Étant donné une courbe E, nous considérons un élément primitif (génerateur) et un autre élément T. P, T sont des tuples d'entier (points). Le DLP est de trouver un $d \in \mathbb{Z}, 1 \leq d \leq \#E$ tel que :

$$\underbrace{P + P + \ldots + P}_{d \text{ fois}} = dP = T$$

$d \rightarrow$ clef privé $\in \mathbb{Z}$. $T = (x_T, y_T)$ en contraste avec DH $K_{pub} \& K_{pr} \in \mathbb{Z}$

EX E : $y^2 \equiv x^3 + 2x + 2 \mod 17$

$$\underset{\underset{K_{pr}}{\uparrow}}{d} \qquad \overbrace{(5,1)}^{\alpha \to \text{ domain parameter}} \qquad = \underbrace{(16,4)}_{K_{pub}}$$

SQ : Mult. (ou exponentiation rapide)

$$26P = (11010_2)P = (d_4 d_3 d_2 d_1 d_0)P$$

$$\begin{aligned}
&d_4 = 1_2 P \\
&d_3 = \begin{cases} P + P = 2P = 10_2 P & \text{DOUBLE} \\ 2P + P = 3P = 11_2 P & \text{ADD} \end{cases} \\
&d_2 = 3P + 3P = 110_2 P \ \text{DOUBLE} \\
&d_1 = \begin{cases} 6P + 6P = 12P = 1100_2 P & \text{DOUBLE} \\ 12P + P = 3P = 1101_2 P & \text{ADD} \end{cases} \\
&d_0 = 13P + 13P = 26P = 11010_2 \ \text{DOUBLE}
\end{aligned}$$

Exemple ECDHKE (Elliptic curve Diffie-Hellman Key Exchange)

1. E : $y^2 \equiv x^3 + ax + b \mod p$ Domain parameter
2. $P = (x_p, y_p)$ Point de base

Alice	Bob
$K_{pr} = a \in \{2, 3, \ldots, \#E - 1\}$	$K_{pr} = b \in \{2, 3, \ldots, \#E - 1\}$
$K_{pub_A} = A = aP = A = (x_A, y_A)_A$	$K_{pub_B} = B = bP = B = (x_B, y_B)_B$

$$aB = T_{AB} \quad \underset{\xleftarrow[\hspace{4cm}]{\text{B}}}{\xrightarrow[\hspace{4cm}]{\text{A}}} \quad bA = T_{AB}$$

$$y^2 \equiv x^3 + 2x + 2 \mod 17; P = (5,1)$$

Alice	Bob
$a = 3, A = (10,6)$	$b = 10$
$K_{pub_A} = 3(5,1) = 3P$	$B = K_{pub_B} = 10 \cdot P = (7,11)$

$$T_{AB} = aB = 3(7,11) = (13,10) = 10(10,6)$$