Factorisation de grands entiers à l'aide de courbes elliptiques

Plan projectif $\mathbb{P}^2(\mathbb{K}) = (\mathbb{K}^3 \backslash \{(0,0,0)\})/\mathcal{R}$ où :

$(x,y,z)\mathcal{R}(x',y',z') \Leftrightarrow [\exists t \in \mathbb{K}\backslash\{0\}, (x,y,z) = t(x',y',z'$

Courbe elliptique $E(\mathbb{K})$ définie sur le corps $\mathbb{K}$:
courbe cubique dans le plan projectif $\mathbb{P}^2(\mathbb{K})$
et munie d'une origine $\mathcal{O} \in E(\mathbb{K})$:

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

Équation de Weierstraß :

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

Équation réduite de Weierstraß (si $\mathbb{K}$ est de caractéristique différente de 2 ou 3) :

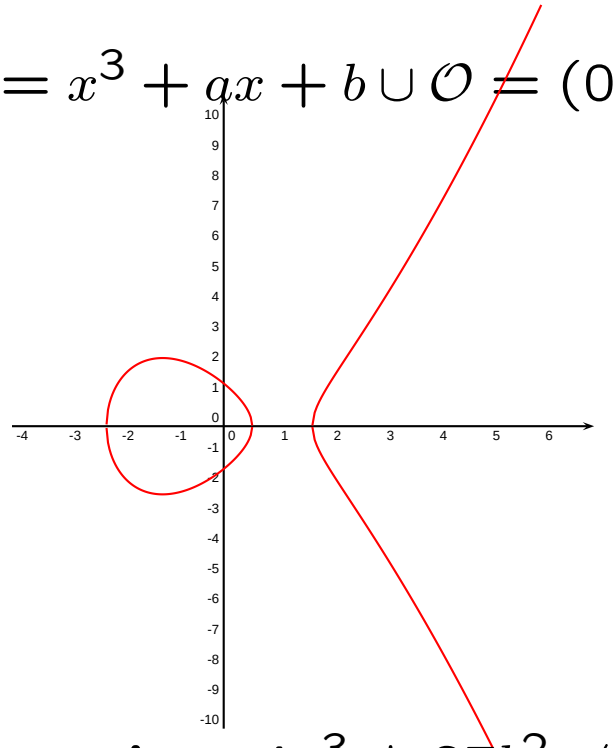
$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

Changements de var : $Y \leftarrow (Y - \frac{1}{2}(a_1X + a_3))$ et $X \leftarrow (X - \frac{a_1^2+4a_2}{12}Z)$.

On remarque : $Z = 0 \Rightarrow X = 0$ donc $\mathcal{O} = (0, 1, 0)$ seul *point à l'infini* $(Z = 0)$

En coordonnées non homogènes ($x = \frac{X}{Z}$ et $y = \frac{Y}{Z}$) :

$$E : y^2 = x^3 + qx + b \cup \mathcal{O} = (0, 1, 0)$$



La condition : $\Delta = 4a^3 + 27b^2 \neq 0$ permet d'imposer la courbe non singulière (admet une tangente en tout point).

Théorème : si E a au moins deux points d'intersection (avec leur multiplicité) avec une droite D, alors E a exactement trois points d'intersection avec la droite D.

L. c. i. $*$: "$P * Q = (PQ) \cap E$" .

Loi de groupe $+$: $P + Q = \mathcal{O} * (P * Q)$.

Expression analytique de $+$:
– si $x_1 = x_2$ et $y_2 = -y_1$ alors $P_1 + P_2 = \mathcal{O}$
– si $P_3 = P_1 + P_2$, alors

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

où

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{si } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{si } P = Q \end{cases}$$

– $\forall P \in E, P + \mathcal{O} = \mathcal{O} + P = P$
$(E, +)$ est un groupe abélien de neutre $\mathcal{O}$.

Méthode $p-1$ de Pollard

Soit $N = \prod_{i=1}^{m} p_i^{\alpha_i} \in \mathbb{N}$. N est dit *B-superlisse* si et seulement si :

$$\forall i \in [\![1, m]\!], p_i^{\alpha_i} \leq B$$

Soit $N \in \mathbb{N}$; on suppose que p est un facteur premier de N tel que $p-1$ soit B-superlisse. On a : $(p-1)|k = \text{ppcm}(1, \ldots, B)$ d'où (petit th. de Fermat) :

$$\forall a \in \mathbb{N}, a \wedge N = 1 \Rightarrow a^k \equiv 1 \pmod{p}$$

donc

$$l = [(a^k - 1) \wedge N] > 1$$

– si $l \neq N$: facteur de N
– si $l = N$, on prend une autre valeur de a
– si $l = 1$, on incrémente B

Théorème de Hasse : la cardinalité $\#E(\mathbb{F}_p)$ de E définie sur le corps fini $\mathbb{F}_p$ de cardinalité p vérifie :

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

Méthode de Lenstra pour la factorisation

On espère factoriser $N = pq$ (supposé *non premier*) à l'aide de la courbe elliptique

$$E_{a,b} : y^2 = x^3 + ax + b \cup \mathcal{O} = (0, 1, 0)$$

- on vérifie $\mathbf{N \wedge 6 = 1} \rightarrow$ caractéristique de $\mathbb{Z}/p\mathbb{Z}$ différente de 2 et 3 $\rightarrow$ le groupe $(E_{a,b}(\mathbb{Z}/p\mathbb{Z}),$ - est bien défini
- on impose $\mathbf{b = -a} \rightarrow P = (1, 1) \in E_{a,b}$
- on vérifie $\mathbf{\Delta \wedge N = 4a^3 + 27b^2 \wedge N = 1} \rightarrow$ $E_{a,b}(\mathbb{Z}/N\mathbb{Z})$ non singulière
- on a : $p \leq \sqrt{N}$ donc (th. de Hasse) :

  $$\#E_{a,b}(\mathbb{F}_p) \leq B = \lceil (N^{1/4} + 1)^2 \rceil$$

  donc $\#E_{a,b}(\mathbb{F}_p) | k = \text{ppcm}(1, \ldots, B)$ donc (th. de Lagrange) : $kP = \mathcal{O}$.
  Dans la pratique : $k = \text{ppcm}(B, B - 1)$.

Dans $E_{a,b}(\mathbb{Z}/p\mathbb{Z})$: $kP = \mathcal{O}$.
Donc $\underbrace{P + P + \ldots + P}_{Q} + P = \mathcal{O}$: on est amené à calculer $Q + P = \mathcal{O}$
(dans la pratique, on utilise l'exponentiation rapide : le principe reste valable).

Formules d'addition :
– $P + Q = \mathcal{O} \Leftrightarrow p_x = q_x$ et $p_y = -q_y$
– sinon : $R = P+Q$ avec : $\begin{cases} r_x = \lambda^2 - p_x - q_x \\ r_y = \lambda(p_y - q_y) - p_y \end{cases}$
où $\lambda = (q_y - p_y)(q_x - p_x)^{-1}$ (pour $P \neq Q$)
Donc $p_x \equiv q_x \pmod{p}$.

Mais il se peut que $p_x \not\equiv q_x \pmod{N}$! Dans ce cas $p|(q_x - p_x) < N$ et $(q_x - p_x) \wedge N \neq 1$ (non inversible dans $\mathbb{Z}/N\mathbb{Z}$).

On fait donc le calcul de kP dans $E_{a,b}(\mathbb{Z}/N\mathbb{Z})$ en espérant qu'on ne pourra pas toujours calculer λ (car $\mathbb{Z}/N\mathbb{Z}$ n'est pas un corps !).

Si les calculs aboutissent on recommence avec d'autres valeurs de a et B.

Critère de Goldwasser-Kilian

Soit $N \in \mathbb{N}$. S'il existe $m \in \mathbb{N}$ et $P \in E_{a,b}(\mathbb{Z}/N\mathbb{Z})$ tels que :

- il existe q facteur premier de m tel que : $q > (N^{1/4}+1)^2$
- $mP = \mathcal{O}$
- $\frac{m}{q}P \neq \mathcal{O}$

alors N est premier.

Démonstration. On note :

$E : E_{a,b}(\mathbb{Z}/N\mathbb{Z})$	$E' : E_{a,b}(\mathbb{Z}/p\mathbb{Z})$
$m = \#E$	$m' = \#E'$
P	P'

On a $mP = \mathcal{O}$ et $\frac{m}{q}P \neq \mathcal{O}$ donc $mP' = \mathcal{O}$ et $\frac{m}{q}P' \neq \mathcal{O}$ donc (th. de Lagrange) : $q|m'$. D'où (th. de Hasse) :

$$q \leq m' \leq (\sqrt{p}+1)^2 \leq (N^{1/4}+1)^2$$

Contradiction.

Algorithme “Baby steps, giant steps”

D’après le th. de Hasse : $\#E = p+1-c$ avec $c \in [\![-2\sqrt{p}, 2\sqrt{p}]\!]$. Énumération naïve : $O(\sqrt{p})$ (cherchant c tel que $\forall P \in E, (p+1-c)P = \mathcal{O}$).

Permet de calculer la cardinalité de $E(\mathbb{F}_p)$ en $O(p^{1/4} \ln^2 p)$ en moyenne.

Idée : le calcul de l’opposé d’un point est immédiat.

Soit $P \in E$. On cherche $c_0 \in [\![0, 2p^{1/4}]\!]$ et $c_1 \in [\![-\frac{p^{1/4}}{2}, \frac{p^{1/4}}{2}]\!]$ tels que :

$$(p + 1 - c_1 4\lceil p^{1/4} \rceil)P = \pm c_0 P$$

(on aura $c = \pm c_0 + c_1 4\lceil p^{1/4} \rceil$).

Deux phases :

- “giant steps” : on stocke les $\lceil p^{1/4} \rceil + 1$ points $(p + 1 - c_1 4\lceil p^{1/4} \rceil)P$;
- “baby steps” : on calcule $c_0 P$ pour $c_0 \in [\![0, 2\lceil p^{1/4} \rceil]\!]$ et on compare $\pm c_0 P$ avec les éléments de la table précédente.