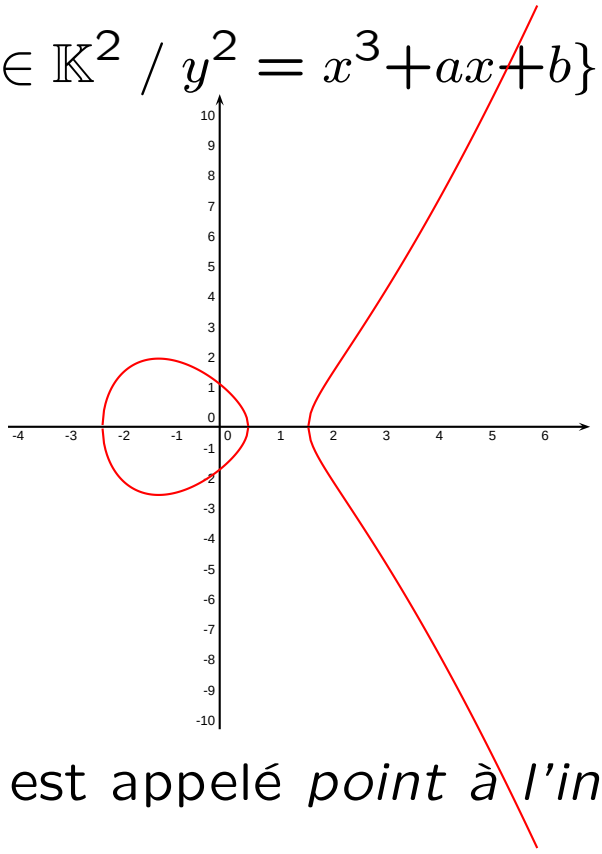
Factorisation de grands entiers à l'aide de courbes elliptiques

Une courbe elliptique $E(\mathbb{K})$ définie sur un corps $\mathbb{K}$ de caractéristique différente de 2 ou 3 est déterminée par son équation réduite de Wierstraß :

$$E = \{(x, y) \in \mathbb{K}^2 \ / \ y^2 = x^3 + ax + b\} \cup \{\mathcal{O} = (0, 1, 0)\}$$



Le point $\mathcal{O}$ est appelé *point à l'infini*.

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 $\mathcal{O}$.

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

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

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

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

On a alors : $N | k = \text{ppcm}(1, 2, \ldots, B)$.

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.