Projet de calcul formel : Algorithme ECM de factorisation d'entiers

Christophe Vuillot et Yannick Zakowski

L'algorithme $p-1$ de Pollard

N un entier à décomposer

- Ne serait-il pas premier ? Non : on voudrait donc un bon candidat diviseur, par exemple un élément g non inversible sur $\mathbb{Z}/N\mathbb{Z}$
- Pour cela, tirons aléatoirement un a majoré par une borne de lissage bien choisie.
- Cherchons une puissance de a dont le *pgcd* avec N est différent de 1.
- C'est gagné !

Un algorithme efficace...

L'efficacité de l'algorithme $p-1$ de Pollard repose sur la relativement forte densité d'éléments non inversibles sur $\mathbb{Z}/N\mathbb{Z}$.

Un algorithme efficace...

L'efficacité de l'algorithme $p-1$ de Pollard repose sur la relativement forte densité d'éléments non inversibles sur $\mathbb{Z}/N\mathbb{Z}$.
On peut démontrer qu'il possède une complexité en $O(n^{1/4})$.

L'algorithme ECM

- Conserver cette idée de candidat diviseur en tant qu'élément non-inversible sur $\mathbb{Z}/N\mathbb{Z}$
- mais augmenter nos chances de le trouver.

L'algorithme ECM

- Conserver cette idée de candidat diviseur en tant qu'élément non-inversible sur $\mathbb{Z}/N\mathbb{Z}$
- mais augmenter nos chances de le trouver.
- L'idée va être de calculer à présent sur une courbe elliptique !

La formule de la somme de deux points

Considérons la courbe elliptique $\mathcal{E}$ d'équation $y^2 = x^3 + ax + 1$.
Soit $P = (x_P,\ y_P)$ et $Q = (x_Q,\ y_Q)$ deux points de $\mathcal{E}$.

Montrons que $\begin{cases} x_{P+Q} = \lambda^2 - x_p - x_Q \\ y_{P+Q} = \lambda(x_P + x_Q - x_{P+Q}) - y_P \end{cases}$ $avec \lambda = \frac{y_P - y_Q}{x_P - x_Q}$

La droite (PQ) a pour équation :

$$y = \lambda x + y_P - \lambda x_P \text{ avec } \lambda = \frac{y_Q - y_P}{x_Q - x_P}$$

La formule de la somme de deux points

Cherchons les coordonnées du troisième point d'intersection de cette droite avec $\mathcal{E}$:

$$\begin{cases} y = \lambda x + y_P - \lambda x_P \\ y^2 = x^3 + ax + 1 \end{cases}$$

Son abscisse vérifie donc :

$$(\lambda x + y_P - \lambda x_P)^2 = x^3 + ax + 1$$
$$x^3 - \lambda^2 x^2 + (a + 2\lambda^2 x_P - 2\lambda y_P)x + 1 = 0$$

x_P étant solution

$$(x - x_P)(x^2 + (x_P - \lambda^2)x + (a + 2\lambda^2 x_P - 2\lambda y_P + x_P(x_P - \lambda^2)) = 0$$

x_Q étant solution

$$(x - x_P)(x - x_Q)(x + x_P + x_Q - \lambda^2) = 0$$

La formule de la somme de deux points

$$\text{D'où } \begin{cases} x_{P+Q} = \lambda^2 - x_p - x_Q \\ y_{P+Q} = -(\lambda(\lambda^2 - x_P - x_Q) + y_P - \lambda x_P) \end{cases}$$

$$\begin{cases} x = \lambda^2 - x_p - x_Q \\ y = -\lambda(\lambda^2 - 2x_P - x_Q) - y_P \end{cases}$$

$$\text{Soit } \begin{cases} x = \lambda^2 - x_p - x_Q \\ y = \lambda(x_P + x_Q - x_{P+Q}) - y_P \end{cases}$$

L'idée

- Soit P un point sur notre courbe.
- Calculons ses multiples sur $E(\mathbb{F}_N)$.
- Ce n'est pas une véritable courbe elliptique, on est amené à trouver un élément non-inversible de $\mathbb{Z}/N\mathbb{Z}$
- Nous retombons dans le cadre de Pollard

Complexité

On peut montrer que la complexité ne dépend que de p et non de n, selon : $O\left(e^{(\sqrt{(2)}+o(1))\sqrt{\log p \log\log p}}\right)$