

Factorisation et corps finis

Louis Coumau, Axel Durbet, Fivos Reyre, Sid Ali Zitouni Terki

Université de Bordeaux

15 mai 2020

Table des matières

- 1 Introduction
- 2 Test de primalité
- 3 2 Méthodes de factorisations
- 4 Courbe elliptique
- 5 Complexité
- 6 Conclusion



oooo

ooooo

oooooo

ooooo

o

Introduction

Introduction

Test de primalité

Test de primalité

Test de primalité

Théorème (Petit théorème de Fermat)

Soit p un nombre premier.

Alors, $\forall a \in \mathbb{N}^$, $a^{p-1} \equiv 1 \pmod{p}$.*

Théorème (Miller-Rabin)

Soit n un nombre premier impair. On pose $n - 1 = 2^e m$ avec m un entier impair. Pour tout entier a premier à n ,

$$\begin{cases} \text{soit } a^m \equiv 1 \pmod{n} \\ \text{soit il existe } i \in [0, e-1] \text{ tel que } a^{2^i} \equiv -1 \pmod{n} \end{cases}$$

Probabilité d'erreur

Théorème

Si $n \geq 9$ est un nombre composé impair, alors

$$\text{card}(M_n) \leq \frac{n-1}{4}$$

Ainsi, $p_n \leq \frac{1}{4}$.

Comparaison

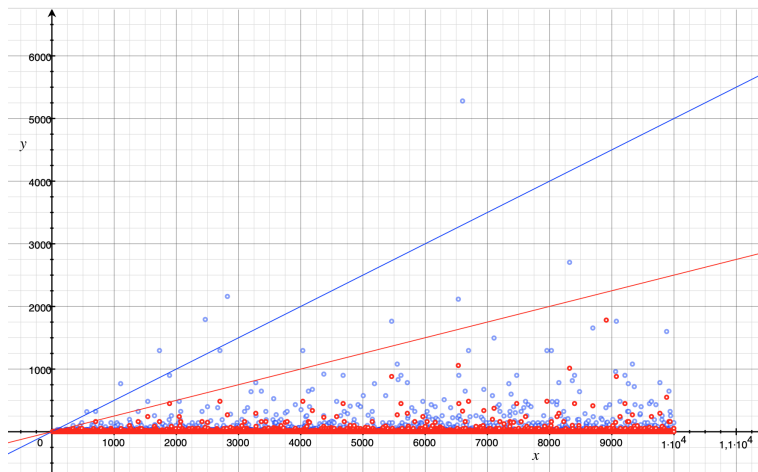


Figure – Comparaison

2 Méthodes de factorisations

B -friable

Définition (B -friable ou B -lisse)

On dit qu'un entier n est B -friable si $\forall i, p_i \leq B$ i.e. si B est supérieur ou égal au plus grand diviseur premier de n .

Exemple : $126 = 2 \times 3^2 \times 7 \Rightarrow 126$ est 7-friable.

B -ultra-friable

Définition (B -ultra-friable ou B -super-lisse)

On dit qu'un entier n est B -ultra-friable si $\forall i, p_i^{\alpha_i} \leq B$ i.e. si B est supérieur ou égal à l'entier étant la plus grande puissance de premier divisant n .

Exemple : $126 = 2 \times 3^2 \times 7 \Rightarrow 126$ est 9-ultra-friable

Algorithme

Proposition

Si $p - 1$ est B -ultra-friable, alors $\text{PGCD}(a^{B!} - 1, n) = d$ tel que $d > 1$.

$P - 1$ Pollard

Algorithme

[p-1 Pollard]

Entrée : n un entier et B une borne

Sortie : d un diviseur de n

- ① *on tire a aléatoirement sur $[2, n - 1]$*
- ② *$d \leftarrow \text{pgcd}(a, n)$*
- ③ *si $d \neq 1$:*
- ④ *retourner d*
- ⑤ *pour q allant de 2 à B*
- ⑥ *$a \leftarrow a^q \bmod n$*
- ⑦ *retourner $\text{pgcd}(a - 1, n)$*

Courbes elliptiques

Courbes elliptiques

Définition d'une Courbe elliptique

Définition (Courbe elliptique)

Soit A un anneau dans lequel 6 est inversible. Soient a et b deux éléments inversibles de A .

On définit une courbe elliptique sur A par l'équation (dite de Weierstrass) suivante :

$$E : \{(x, y, z) \in \mathbb{P}^2(A) \mid y^2 z = x^3 + axz^2 + bz^3\}$$

Exemple

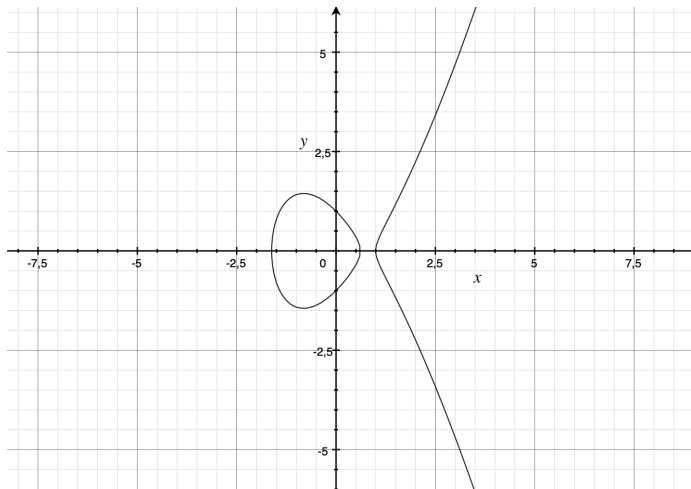


Figure – Graphe en 2D avec $a = -2$, $b = 1$ et $z = 1$

Addition sur la courbe

Soit P, Q, R trois points de la courbe E tels que $P + Q = R$.

- Si $P = Q = O$ alors $R = O$ ou si $Q = O$ alors $P = R$
- Si $x_P = x_Q$ et $y_Q = -y_P$ alors $R = O$
- Si $x_P \neq x_Q$ alors
$$\begin{cases} x_R = \lambda^2 - x_P - x_Q \bmod p \\ y_R = \lambda \times (x_P - x_Q) - y_P \bmod p \\ \lambda = (y_Q - y_P) \times (x_Q - x_P)^{-1} \bmod p \end{cases}$$
- Si $P = Q$ et $y_P \neq 0$ alors
$$\begin{cases} x_R = \lambda^2 - 2 \times x_P \bmod p \\ y_R = \lambda \times (x_P - x_R) - y_P \bmod p \\ \lambda = (3x_P^2 + a) \times (2 \times y_P)^{-1} \bmod p \end{cases}$$

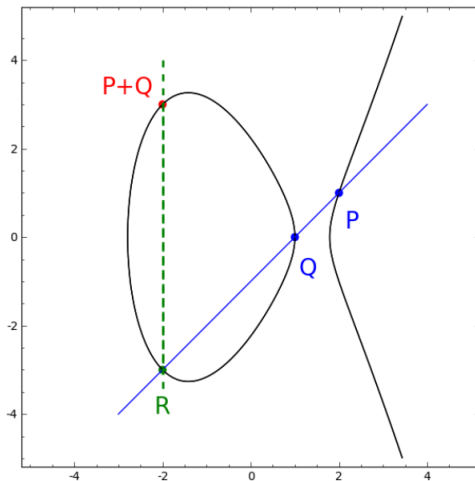


Figure – Addition sur les courbes elliptiques

Algorithme

- ❶ On choisit aléatoirement a, x_P, y_P puis, on calcule $b = y_P^2 - x_P^3 - a \times x_P$.
- ❷ On vérifie que le discriminant $4a^3 + 27b^2$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$
- ❸ On construit la courbe E avec a, b
- ❹ On choisit k un entier.
- ❺ Si le cardinal de E divise k , $kP = 0 \bmod p$, et nous aurons trouvé un facteur de n .
- ❻ Sinon, On recommence avec une nouvelle courbe elliptique E' avec un cardinal différent de celui de E

Complexité

Complexité

Théorème

Théorème

La complexité de $P - 1$ est $O(B \times \log(B) \times (\log(N))^{1+\epsilon})$ avec B la borne choisie et N l'entier à factoriser.

La fonction L

Définition

On définit, pour toute constante $c > 0$ et pour tout $\alpha \in [0, 1]$ la fonction suivante :

$$L_x(\alpha, c) = e^{((c+o(1))(\ln x)^\alpha (\ln \ln x)^{1-\alpha})}$$

La fonction L

Théorème

Un entier aléatoire de taille $L_x(\alpha, c)$ est $L_x(\beta, c')$ -friable avec une probabilité $L_x(\alpha - \beta, -\frac{\varepsilon}{c'}(\alpha - \beta) + o(1))$ quand x tend vers l'infini.

Optimisation de la borne

Théorème

$B = L_n(\frac{1}{2}, \frac{1}{2}) = \exp(\frac{1}{2} \times \sqrt{\ln(n)} \times \sqrt{\ln(\ln(n))})$ est la meilleur borne possible. Elle donne le plus petit temps d'exécution

$$T = e^{\sqrt{\ln(n) \times \ln(\ln(n))}}$$

La complexité de l'algorithme dépend de la taille du facteur à trouver.

Elle peut être exprimée par $O(e^{(\sqrt{2}+o(1))\sqrt{\ln(p) \times \ln(\ln(p))}})$ où p est le plus petit facteur de n .

Conclusion

Conclusion