Théorie des nombres algorithmique

(Aspects classiques)

2023-2024

Table des matières

Chapitre 1

Premier point : factorisation

1.1 Méthode de Fermat

Une idée, calcul successif des :

$$issquare(n + k^2)?$$

si oui, alors

$$n = (\sqrt{n + k^2} - k)(\sqrt{n + k^2} + k)$$

et on a une factorisation :

Avancée(s) 1. On a un algorithme en prenant k petit, l'algo est naif et marche que si k petit.

Remarque 1. *L'ordre de l'autre carré est de $\sqrt{n}$.*

En fait, si on obtient un multiple de n comme différence de deux carrés, i.e. :

$$x^2 \equiv y^2 \mod n$$

alors faut calculer en plus $n \wedge x - y$. Grande probabilité que y'ai un facteur commun.

Avancée(s) 2. On peut faire la méthode d'avant, en travaillant $\mod n$. Marche toujours que si k est petit.

1.2 Méthode de Dixon

Maintenant, on peut utiliser la technique d'avant de la manière suivante :

Choisir une base de premiers $P_B := \{p \in \mathbb{P} | p \leq B\}$ et ajouter -1.

Ensuite on choisit aléatoirement $a \mod n$ et on calcule

$$a^2 \equiv b \mod n$$

puis on regarde si il est B-lisse. Si oui on stocke

$$a^2 = \prod_i p_i^{e_i} \mod n$$

On obtient un ensemble de congruences C, on peut en chopper $\#P_B$ et on forme

1.3 Crible quadratique