Factorisation des entiers

Vincent Dalsheimer Gaëtan Pradel

Année 2016 - Semestre 10

Table des matières

1 Introduction

Théorème 1 (Théorème fondamental de l'arithmétique)**.** *Tout entier strictement positif peut être écrit comme un produit de nombres premiers d'une unique façon, à l'ordre près des facteurs.*

Théorème 2. *Il existe une infinité de nombres premiers.*

2 Rappels sur l'utilité des nombres premiers en cryptographie

En cryptographie, les nombres premiers sont très utilisés et très utiles car ils apportent, grâce à leurs propriétés, de la sécurité.

2.1 Chiffrement RSA

En effet, présentons l'algorithme RSA qui les utilise.

Tout d'abord, le chiffrement RSA est un chiffrement asymétrique, c'est-à-dire qu'il utilise une paire de clés, qui sont des nombres entiers, composée d'une clé publique pour chiffrer et d'une clé privée pour déchiffrer. La clé privée peut être aussi utilisée pour signer un message.

2.1.1 Création des clés

- Choisir p et q, deux nombres premiers entiers distincts ;
- calculer leur produit $n = p * q$
- calculer $\phi(n) = (p-1)(q-1)$ qui est la valeur de l'indicatrice d'Euler en n ;
- choisir un entier naturel e premier avec $\phi(n)$ et strictement inférieur à $\phi(n)$;
- calculer l'entier naturel d, inverse de e modulo $\phi(n)$, et strictement inférieur à $\phi(n)$; d peut se calculer efficacement par l'algorithme d'Euclide étendu.

Le couple (n, e) est la clé publique et d est la clé privée.

La sécurité de cet algorithme repose sur le fait que la factorisation (de grands nombres) est un problème difficile, c'est-à-dire qu'on ne peut pas le résoudre en temps polynomial.

2.1.2 Chiffrement

Soit m un message à chiffrer. Le message chiffré c de m sera :

$$c \equiv m^e \pmod{n}.$$

2.1.3 Déchiffrement

Soit le message chiffré c comme ci-dessus. Pour retrouver le message m on fait :

$$c^d \equiv m^{e*d} \equiv m \pmod{n}.$$

2.1.4 Justification

La démonstration repose sur le petit théorème de Fermat, à savoir que comme p et q sont deux nombres premiers, si m n'est pas un multiple de p on a la première égalité ci-dessous, et la seconde s'il n'est pas un multiple de q :

$$m^{p-1} \equiv 1 \pmod{p}\ ,\quad m^{q-1} \equiv 1 \pmod{q}.$$

En effet

$$c^d \equiv (m^e)^d \equiv m^{ed} \pmod{n}.$$

Or

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

ce qui signifie que pour un entier k

$$ed = 1 + k(p-1)(q-1),$$

donc, si m n'est pas multiple de p d'après le petit théorème de Fermat

$$m^{ed} \equiv m^{1+k(p-1)(q-1)} \equiv m \cdot \left(m^{p-1}\right)^{k(q-1)} \equiv m \pmod{p}$$

et de même, si m n'est pas multiple de q

$$m^{ed} \equiv m \pmod{q}.$$

3 Méthode naïve de la factorisation

Pour factoriser un nombre n, la méthode la plus naïve et la plus naturelle consiste à faire les divisions euclidiennes successives de n par 2 (autant de fois que l'on peut), puis 3, etc ... jusqu'à la partie entière de $\sqrt[2]{n}$.

4 L'algorithme $p-1$ de Pollard

L'algorithme $p-1$ de Pollard est un algorithme de décomposition en produit de facteurs premiers. Cette méthode fonctionne seulement avec des nombres qui ont une forme particulière. Il trouve les facteurs p dont $p-1$ est ultrafriable.

Définition 1 (Entier friable)**.** *Un entier strictement positif est dit B-friable ou B-lisse si tous ses facteurs premiers sont inférieurs ou égaux à B.*

Exemple 1. $90 = 2 \times 3^2 \times 5$ *est* 5*-friable car aucun de ses facteurs premiers ne dépasse 5. Cette définition inclut les nombres qui ne figurent pas parmi les facteurs premier : par exemple, 12 est* 5*-friable.*

Définition 2 (Entier ultrafriable)**.** *Un nombre est dit B-superlisse our B-ultrafriable si tous ses diviseurs sont de la forme p^r, avec p premier et r entier, satisfont :*

$$p^r \leqslant B.$$

Exemple 2. $720 = 2^4 \times 3^2 \times 5$ *est* 5*-friable mais pas* 5*-ultrafriable (*$3^2 = 9 > 5$*). Par contre il est* 16*-ultrafriable puisque sa plus grande puissance de facteur premier est* $2^4 = 16$.

4.1 Principe de l'algorithme

Soit n un entier divisible par un nombre premier p, avec $n \neq p$.

Théorème 3 (Petit Théorème de Fermat)**.** *Si p est un nombre premier et si a est un entier non divisible par p, alors $a^{p-1} - 1$ est un multiple de p. C'est-à-dire :*

$$a^{p-1} = 1 \pmod{p}.$$

Par le petit théorème de Fermat, nous savons que

$$a^{p-1} = 1 \pmod{p}$$

pour a premier avec p.

Cela implique que pour tout multiple M de $p-1$ on a :

$$a^M - 1 \equiv 0 \pmod{p} \text{ car } a^{k(p-1)} - 1 = (a^{p-1} - 1) \sum_{i=0}^{k-1} a^{i(p-1)}.$$

Si $p-1$ est B-ultrafriable pour un certain seuil B, alors $p-1$ divise le pgcd des entiers de 1 à B. Donc, si l'on pose $M = ppcm(1, ..., M)$, on a :

$$a^M \equiv 1 \pmod{p} \text{ pour tout } a \text{ premier avec } p.$$

Autrement dit, p divise $a^M - 1$ et donc le pgcd de n et $a^M - 1$ est supérieur ou égal à p. En revanche, il est possible que le pgcd soit égal à n lui-même auquel cas, on n'obtient pas de facteur non trivial.

4.2 Pseudo-code

Algorithme 1 : Factorisation de n par $p-1$ de Pollard

Entrées : Un entier n
Sorties : Un facteur premier p de n ou n lui-même

Choisir un résidu $x \pmod{n}$ au hasard et initialier p à 1 et un compteur cmp à 0;
Définir une suite en posant $x_1 = x$, $x_2 = x_1^2 \pmod{n}$, $x_3 = x_2^3 \pmod{n}$, ... Ainsi x_{k+1} est obtenu en élevant x_k à la puissance $k+1$ modulo n. Autrement dit $x_k = x^{k!}$.;
Répéter
    $x_k = x^{k!} \pmod{n}$;
    $p = pgcd(x_k - 1, n)$;
    $k = k + 1$;
    $cmp = cmp + 1$;
jusqu'à $p \neq 1$ *ou que* $cmp =$ *une certaine limite choisie*;
if *Le compteur est égal à la limite et* p *est toujours égal à* 1 **then**
    Retourner n
end
Retourner p

4.3 Exemple

Nous factorisons le nombre 172189 avec notre algorithme $p-1$ de Pollard. On a $172189 = 409 \times 421$ et

$$409 - 1 = 408 = 2^3 \times 3 \times 17$$

puis

$$421 - 1 = 420 = 2^2 \times 3 \times 5 \times 7.$$

Voici ce que l'on obtient avec cet exemple :

k	1	2	3	4	5	6	7
$x_k = x^{k!} \pmod n$	2	4	64	74883	27019	147176	45890
$pgcd(x_k - 1, n)$	1	1	1	1	1	1	421

Au premier tour on trouve donc 421. On le fait ensuite sur $172189 \div 421 = 409$.

k	1	2	3	4	5	6	...
$x_k = x^{k!} \pmod n$	2	4	64	36	25	345	...
$pgcd(x_k - 1, n)$	1	1	1	1	1	1	...

L'algorithme nous renvoie 409 car il ne trouve pas de facteur, c'est normal car il est premier.

4.4 Les limites

Dans certains cas, l'algorithme nous renvoie le même nombre mis en entrée ou une factorisation imcomplète de celui-ci, en effet, cela correspond aux cas où les $p - 1$ ne sont pas ultrafriables.

Par exemple, avec le nombre 7345461, l'algorithme nous renvoies une factorisation imcomplète. La factorisation naïve nous renvoies $7345461 = 3 \times 563 \times 4349$ tandis que $p-1$ de Pollard nous renvoie $7345461 = 3 \times 2448487$. A priori, on suppose donc que 562 et 4348 ne sont pas ultrafriables, et en effet : $562 = 2 \times 281$ et $4348 = 2 \times 1087$.

5 Crible de Dixon

Le crible de Dixon se base sur la recherche de congruences de carrés. Son fonctionnement s'inspire de celui de l'algorithme de factorisation de Fermat qui consistait à écrire n comme la différence de deux carrés. On avait alors :

$$n = a^2 - b^2 = (a - b)(a + b).$$

5.1 Principe de l'algorithme

On cherche deux entiers u et v tels que $u^2 = v^2 \pmod n$ et $u \neq v \pmod n$. Un facteur de n pourra alors être trouvé en calculant $\text{pgcd}(u-v, n)$.

Pour cela, on choisit une borne B et on note k le nombre de premiers inférieurs à B.

On prend ensuite un x aléatoirement dans $[\sqrt{n}, n-1]$ et on calcule $y = x^2 \pmod n$. Si y est B-friable, on garde le couple (x, y) appelé *relation*. Appelons R l'ensemble des relations et m son cardinal. On recommence l'opération jusqu'à avoir $m > k$.

On construit ensuite la matrice $M = (v_{i,p} \pmod 2)a_{p\in P, 1\leqslant i\leqslant m}$, puis on trouve un vecteur non nul $(e_1, ..., e_m)$ annulant M. On a alors :

$$\prod_{i=1}^{m} x_i^{2e_i} = \prod_{i=1}^{m} \prod_{p\in P} p_{i,p}^{v} e_i^{e} = \prod_{p\in P} p^{\sum_{i=1}^{m} v_{i,p}e_i} \pmod n.$$

Or $(e_1, ..., e_m)$ annule M, donc :

$$\sum_{i=1}^{m} v_{i,p}e_i = 0 \pmod 2.$$

On a donc une congruence de carrés $u^2 = v^2 \pmod n$ avec $u = \prod_{i=1}^{m} x_i^{e_i} \text{et} v = \prod_{p\in P} p^{\frac{1}{2}\sum_{i=1}^{m} v_{i,p}e_i}$ qui nous donnera un facteur de n en calculant $\text{pgcd}(u - v, n)$.