NOMBRES PREMIERS

ALEXANDRA BRUASSE-BAC

Table des matières

Voir également les chapitres sur les corps finis, sur la factorisation ainsi que sur le calcul du logarithme discret.

En cas de problème, voici la liste des notations utilisées.

Dans ce chapitre, nous allons nous intéresser à la question de savoir si un entier donné est premier ou non. Nous allons pour cela étudier plusieurs algorithmes (déterministes ou non) permettant de répondre à la question. Une remarque importante que tous ces algorithmes fournissent une réponse à la question : p est-il premier, cependant si ce n'est pas le cas, *aucun d'eux de produit un facteur de* p, d'où la nécessité des algorithmes de factorisation.

Presque tous les algorithmes présentés dans ce chapitre sont implémentés dans la librarie LiDIA.

Nous commencerons en fait par revoir un outil de base : le théorème des restes chinois.

1. Quelques visions du théorème des restes chinois

(i) Version arithmétique

(ii) Version iso de groupes

(iii) Question des inversibles

2. Les tests de primalité

Il est couteux de prouver qu'un entier donné est premier, en revanche, il existe des algorithmes très performants pour prouver qu'un entier est premier avec une forte probabilité. De tels algorithmes sont appelés *tests de primalité*.

Date: Année 2002-2003.

2.1. **Le test de Fermat.**

Le test de primalité de Fermat est basé sur la version suivante du petit théorème de Fermat :

Théorème 2.1 (Petit théorème de Fermat)**.** *Si n est un nombre premier, alors pour tout $a \in \mathbb{Z}$ tel que* $\text{pgcd}(a, n) = 1$*, on a :*

$$a^{n-1} \equiv 1 \ [n]$$

Ce théorème peut être utilisé pour montrer qu'un entier n donné est composite (c'est-à-dire non premier). Soit $a \in \{1, 2, \dots n-1\}$. On calcule $y = a^{n-1}[n]$. Si $y \neq 1$, alors n est composite.

On notera que si $y = 1$, on ne peut conclure si y est premier ou composite.

Remarque 2.2. Si le test de Fermat prouve que n est composite, il ne donne par pour autant un facteur de n. Ce test ne peut donc pas être utilisé comme algorithme de factorisation.

2.2. **Les nombres de Carmichael.**

Le test de Fermat permet de montrer que n est composite. Or si n a échoué au test pour de nombreuses bases a, il parait naturel de penser que n a une forte probabiltié d'être premier. Malheureusement, il existe des entiers non premiers dont aucune base a ne permet de montrer qu'ils sont composites. Ces entiers sont appelés nombres de Carmichael.

Pour présenter ces phénomènes zoologiques, nous aurons tout d'abord besoin de la définition suivante.

Définition 2.3. Si n est un nombre composite impair et si a est un entier tel que

$$a^{n-1} \equiv 1 \ [n]$$

alors n est appelé un pseudo-premier par rapport à la base a.

Définition 2.4. Si n est un pseudo-premier par rapport à la base a pour tout entier a tel que $\text{pgcd}(a, n) = 1$, alors n est appelé un nombre de Carmichael.

Le plus petit nombre de Carmichael connu est $561 = 3 \cdot 11 \cdot 17$. A cause de l'existence de tels nombres, le test de Fermat n'est pas très efficace dans la pratique. Un meilleur choix est celui du test de Miller-Rabin que nous décrirons plus loin. Mais avant de la présenter, nous aurons besoin de la caractérisation suivante des nombres de Carmichael :

Théorème 2.5. *Un nombre composite impair $n \geq 3$ est un nombre de Carmichael si et seulement si :*

(i) *il est sans carrés (c'est-à-dire qu'il n'a pas de diviseurs premiers multiples),*

(ii) *pour tout diviseur premier p de n, $p - 1$ divise $n - 1$.*

Voir [Buchmann] p.131 pour une démonstration de ce résultat (qui est lourdement basée sur le théorème des restes chinois).

2.3. **Le test de Miller-Rabin.**

Dans cette partie, nous allons décrire le test de Miller-Rabin. Son avantage (par rapport au test de Fermat) est qu'il peut déterminer, pour tout entier n si n est premier ou composite.

Le test de Miller-Rabin est en fait une modification du test de Fermat. Soit n un entier impair et positif, on définit :

$$s = \max\{r \in \mathbb{N} \,;\, 2^r \mid n - 1\}$$

i.e. 2^s est la plus grande puissance de 2 qui divise $n-1$. On pose alors :

$$d = \frac{n-1}{2^s}$$

d est impair.

Théorème 2.6. *Si n est un nombre premier et si a est un entier tel que* $\text{pgcd}(a,n) = 1$*, alors soit :*

$$a^d \equiv 1 \ [n]$$

soit il existe $r \in \{0, 1, \ldots, s-1\}$ tel que :

$$a^{2^r d} \equiv -1 \ [n]$$

Pour démontrer ce théorème, nous aurons besoin du lemme suivant :

Lemme 2.7. *Soit n un entier premier avec $n \geq 3$, le seul élément d'ordre 2 de $(\mathbb{Z}/n\mathbb{Z})^*$ est -1.*

Démonstration. Le nombre -1 est clairement d'ordre 2 puisque $(-1)^2 \equiv 1 \ [n]$. Réciproquement, si $a^2 \equiv 1 \ [n]$, alors $a^2 - 1 \equiv 0 \ [n]$, c'est-à-dire $(a-1)(a+1) \equiv 0 \ [n]$. Or, comme n est premier (en termes savants, on dit que $\mathbb{Z}/n\mathbb{Z}$ est intègre), on en déduit que $a-1 \equiv 0 \ [n]$ ou $a+1 \equiv 0 \ [n]$, puis comme 1 est d'ordre 1, le seul élément d'ordre 2 est $a = -1$. □

Démonstration du théorème 2.6. Soit a un entier tel que $\text{pgcd}(a,n) = 1$. Comme n est premier, l'ordre de $(\mathbb{Z}/n\mathbb{Z})^*$ (le groupe des inversibles) est $n-1 = 2^s d$. Comme a est premier avec n, a est inversible (ie. $a \in (\mathbb{Z}/n\mathbb{Z})^*$), donc l'ordre de a divise $2^s d$. Par conséquent, $(a^d)^{2^s} = a^{2^s d} \equiv 1 \ [n]$, puis l'ordre de a^d divise 2^s (c'est donc une puissance de 2). On aboutit donc aux deux cas suivants :

(i) si cet ordre est $k = 2^0 = 1$, alors $a^d \equiv 1 \ [n]$.

(ii) si cet ordre est $k = 2^l$ avec $1 \leq l \leq s$, alors avec le même raisonnement que précédemment, on montre que l'ordre de $a^{2^{l-1} d}$ divise 2, puis qu'il est égal à 2. Or, d'après le lemme 2.7, le seul élément d'ordre 2 de $(\mathbb{Z}/n\mathbb{Z})^*$ est -1, d'où $a^{2^r d} \equiv -1 \ [n]$ pour $r = l-1$.

□

Si n est un nombre premier, l'une des conditions du théorème 2.6 est vérifiée. Par conséquent, si l'on trouve un entier a avec $\text{pgcd}(a,n) = 1$ qui ne satisfait aucune des conditions du théorème 2.6, alors n est composite. Un tel entier a est appelé un témoin de la non-primalité de n.

Pour l'efficacité du test de Miller-Rabin, il est important qu'il y ait suffisamment de tels témoins. Le théorème suivant assure cette "densité de témoins" :

Théorème 2.8. *Si $n \geq 3$ est un nombre impair composite, alors l'ensemble $\{1, \ldots, n-1\}$ contient au plus $\frac{n-1}{4}$ nombres premiers avec n qui ne sont pas des témoins de non-primalité pour n.*

Voir [Buchmann] p.133 pour une preuve de ce résultat.

Dans la pratique, pour tester un nombre n impair, on choisit au hasard un entier $a \in \{2, 3, \ldots, n-1\}$. Si $\text{pgcd}(a,n) > 1$, alors on vient de trouver un facteur de n qui est donc composite. Sinon, on calcule $a^d, a^{2d}, \ldots, a^{2^{n-1} d}$ modulo n et on vérifie les conditions du théorème 2.6. Si l'on a trouvé un témoin de non-primalité pour n, alors n est composite, sinon, on recommence avec un autre entier a. D'après le théorème 2.8, la probabilité que n soit composite et que a choisi au hasard ne soit pas un témoin est d'au plus $\frac{1}{4}$.

2.4. **Le test de Solovay-Strassen.**

Le test de Solovay-Strassen est basé sur une propriété différente des nombres premiers :

Proposition 2.9. *Soit $p \in \mathbb{N}$ premier et soit a tel que* $\text{pgcd}(a,p) = 1$*, alors a est un carré modulo p si et seulement si* $a^{\frac{p-1}{2}} \equiv 1\ [p]$.

Par ailleurs, on sait tester d'une autre manière si un entier est ou non un carré dans $\mathbb{Z}/n\mathbb{Z}$, et ce grâce au symbole de Jacobi :

Définition 2.10. Soient a et n deux entiers. Le symbole de Jacobi de a par rapport à n est défini par :

$$\left(\frac{a}{n}\right) = \begin{cases} 0 & \text{si } a \equiv 0\ [n] \\ 1 & \text{si } a \text{ est un carré dans } \mathbb{Z}/n\mathbb{Z} \\ -1 & \text{si } a \text{ n'est pas un carré dans } \mathbb{Z}/n\mathbb{Z} \end{cases}$$

Ce symbole peut être calculé à partir des propriété suivantes :

Proposition 2.11.

(i) *le symbole de Jacobi est multiplicatif :*

$$\left(\frac{a_1 a_2}{n}\right) = \left(\frac{a_1}{n}\right)\left(\frac{a_2}{n}\right) \qquad \left(\frac{a}{n_1 n_2}\right) = \left(\frac{a}{n_1}\right)\left(\frac{a}{n_2}\right)$$

(ii) *si $a = b + qn$, alors*

$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$$

(iii) *si $n \equiv \pm 1\ [8]$, alors*

$$\left(\frac{2}{n}\right) = 1$$

si $n \equiv \pm 3\ [8]$, alors

$$\left(\frac{2}{n}\right) = -1$$

(iv) *si $a \equiv n \equiv 3\ [4]$, alors*

$$\left(\frac{a}{n}\right) = -\left(\frac{n}{a}\right)$$

sinon

$$\left(\frac{a}{n}\right) = \left(\frac{n}{a}\right)$$

(v) *on a*

$$\left(\frac{1}{n}\right) = 1 \qquad \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$$

Exemple 2.12. On se demande si $n = 253$ est premier. Soit $a = 12$, on calcule :

$$\begin{aligned} \left(\frac{12}{253}\right) = \left(\frac{2^2 \cdot 3}{253}\right) &= \left(\frac{2}{253}\right)^2 \left(\frac{3}{253}\right) \\ &= 1^2 \left(\frac{3}{253}\right) && 253 \equiv 1\ [4] \\ &= \left(\frac{253}{3}\right) && 253 = 83 \cdot 3 + 1 \\ &= \left(\frac{1}{3}\right) = 1 \end{aligned}$$

Par ailleurs, on calcule que :

$$a^{\frac{n-1}{2}} = 12^{126} \ [253] = 133 \ [253]$$

Donc 253 n'est pas premier.

Comme pour le test de Miller-Rabin, il est intéressant de savoir dans quelle mesure on détectera un entier non-premier. *On peut montrer que la probabilité que n un nombre impaire ne soit pas premier et que $a < n$ ne soit pas un témoin de non-primalité est de* $\frac{1}{2}$ (ce qui est moins bon que pour le test de Miller-Rabin).

3. Un algorithme déterministe de primalité

Dans la partie précédente, nous avons vu des tests de primalité permettant de savoir avec une certaine probabilité si n est premier. Nous allons ici présenter une esquisse d'algorithme permettant de dire avec certitude si p est premier ou non.

Si un tel algorithme existe, on peut se demander quel est l'interêt d'avoir recours à des tests de primalité (rendant seulement des résultats partiels). L'interêt est bien-sûr une question de coût : le présent algorithme déterministe est bien plus complexe que le test de Miller-Rabin.

On notera également que l'algorithme proposé ici est le coeur de l'algorithme proposé dans [AKS,02] montrant que le problème de décider si n est premier est dans P. L'idée centrale de cette méthode repose sur le théorème suivant :

Théorème 3.1. *Soit p un entier dont on veut tester la primalité et soit a tel que* $\text{pgcd}(a,p) = 1$. *Alors p est premier si et seulement si*

$$(X-a)^p \equiv (X^p - a) \ [p]$$

Démonstration. Supposons que p est premier. Pour tout $0 < i < p$, d'après le binôme de Newton, le coefficient d'ordre X^i de $(X-a)^p$ est $(-1)^{p-i}\text{C}_p^i a^{p-i}$. Or, comme on l'a vu dans le cours sur les corps finis, pour $0 < i < p$, on a $p \mid \text{C}_p^i$. Par conséquent, $(X-a)^p \equiv (X^p - a^p) \ [p]$. De plus, comme $\text{pgcd}(a,p) = 1$, on a $a \in (\mathbb{Z}/p\mathbb{Z})^*$, donc son ordre divise $p-1$. Par conséquent, $a^{p-1} \equiv 1 \ [p]$, puis $a^p \equiv a \ [p]$. D'où $(X-a)^p \equiv (X^p - a) \ [p]$.

Réciproquement, supposons que p soit composite. Soit q un nombre premier facteur de p dont l'exposant maximal dans p est k ($p = q^k m$ avec $\text{pgcd}(q,m) = 1$). Montrons que dans ce cas, q^k ne divise pas C_p^q. On a :

$$\text{C}_p^q = \frac{p \cdot (p-1) \cdots (p-q+1)}{q!} = \frac{q^k m \cdot (p-1) \cdots (p-q+1)}{q!}$$

Par l'absurde, si $q^k \mid \text{C}_p^q$, alors

$$\frac{m \cdot (p-1) \cdots (p-q+1)}{q!} = \frac{m \cdot (p-1) \cdots (p-q+1)}{q \cdot (q-1) \cdots 1} \in \mathbb{N}$$

Or, comme q est premier, on en déduit que $q \mid m \cdot (p-1) \cdots (p-q+1)$, puis qu'il existe $i \in \{1 \dots q-1\}$ tel que $q \mid p - i = q^k m - i$. Par conséquent, on devrait avoir $q \mid i$, ce qui est impossible.

Ainsi, q^k ne divise pas C_p^q. Par ailleurs, comme a et p sont premiers entre eux, on a également $\text{pgcd}(a^{p-q}, q^k) = 1$, puis $q^k \nmid \text{C}_p^q a^{p-q}$. On en déduit donc que le coefficient d'ordre q de $(X-a)^p$ est non nul modulo p, puis $(X-a)^p \not\equiv (X^p - a) \ [p]$. □

Par conséquent, dans la pratique, pour savoir si p est premier, il suffit de choisir un élément $a \in \{1 \dots p\}$ tel que $\text{pgcd}(a,p) = 1$ et de calculer $(X-a)^p \ [p]$. Si $(X-a)^p \equiv (X^p - a) \ [p]$, alors p est premier, sinon p est composite. On notera cependant que cet algorithme étudie une propriété qui doit être vérifiée par tous

les nombres premiers et ne fournit donc pas un facteur explicite de p au cas où ce dernier serait composite.

Bibliographie

[AKS,02] M. Agrawal, N. Kayal, and N. Saxena. Primes is in p. Technical report, Indian Institute of Technology Kanpur, `manindra@cse.iitk.ac.in , kayaln@iitk.ac.in, nitinsa@cse.iitk.ac.in`, 2002.

[Buchmann] J.A. Buchmann. *Introduction to cryptography*. Springer, 2001.

[LN,86] R. Lidl and H. Niederreiter. *Introduction to finite fields and their applications*. Cambridge University Press, 1986.