Anaël Marit ENS Rennes

CRITÈRE DE PRIMALITÉ DE SOLOVEY-STRASSEN

- 120, 121, 127 –

—

On va dans ce développement étudier un critère de primalité d'usage pratique qui ouvre la voie à des test probabilistes de primalité assez efficaces dans la pratique.

Le critère de Solovey-Strassen repose sur le symbole de Legendre et sa généralisation à $\mathbb{Z}/n\mathbb{Z}$, le symbole de Jacobi. Comme il n'est pas envisageable, en 15 minutes, de développer la théorie qui les entoure en plus du développement, il faut avoir de bonnes bases sur le sujet avant de se lancer dans le dev !

Etant donnés a et n deux entiers, avec n, on notera $a \wedge n$ leur p.g.c.d. positif. Si n est non nul, on notera $[a]_n$ le projeté de a dans $\mathbb{Z}/n\mathbb{Z}$. Si b est un second entier, on écrira :

$$a \equiv b[n] \tag{1}$$

lorsque $[a]_n = [b]_n$. Le groupe des inversible de $\mathbb{Z}/n\mathbb{Z}$ sera noté $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$. On désignera par φ l'indicatrice d'Euler, dont la valeur en n est le cardinal de ce groupe.

Si p est un nombre premier impair et a un entier, on notera $\left(\frac{a}{p}\right)$ le symbole de Legendre de a modulo p, défini par :

$$\left(\frac{a}{p}\right) := \begin{cases} 0 \text{ si } p \mid a \\ 1 \text{ si } a \text{ est un carré modulo } p \\ -1 \text{ sinon} \end{cases} \tag{2}$$

Lorsque n est un entier impair positif admettant la décomposition en produit de nombres premiers $\prod_p p^{\nu_p(n)}$, on notera $\left(\frac{a}{n}\right)$ le symbole de Jacobi de a modulo n, défini par :

$$\left(\frac{a}{n}\right) := \prod_p \left(\frac{a}{p}\right)^{\nu_p(n)} \tag{3}$$

Nombres de Carmichael

Lorsque p est un nombre premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est en fait un corps dont le groupe des inversibles est de cardinal $p-1$. Le théorème de Lagrange indique donc que pour tout a premier avec p, on a :

$$a^{p-1} \equiv 1[p] \tag{4}$$

Nous allons dans cette première partie montrer que la réciproque est fausse, et caractériser les cas pathologiques qui la mettent en défaut.

Contactez-moi en cas de coquille à prénom.nom@ens-rennes.fr !

Définition 1 (Nombre de Carmichael). *Un entier $n > 2$ est dit de Carmichael s'il est composé (c'est-à-dire non premier) et si :*

$$\forall a \in \mathbb{N},\ a \wedge n = 1 \implies a^{n-1} \equiv 1[n] \tag{5}$$

Théorème 2 (Caractérisation des nombres de Carmichael ([1], prop. 3.33)). *Soit n un entier composé. C'est un nombre de Carmichael si, et seulement si :*

1. *Les facteurs premiers de n sont simples.*
2. *Pour tout facteur premier p de n, $p-1 \mid n-1$.*

Démonstration.

Commençons par le sens indirect , qui est plus élémentaire. On suppose donc que les facteurs premiers de n sont simples et que pour tout tel facteur premier p, $p-1 \mid n-1$. Fixons a un entier premier avec n (et donc en particulier premier avec tous les facteurs premiers de n). Si p est un facteur premier de n, a est donc inversible modulo p. Par théorème de Lagrange, et comme $p-1 \mid n-1$, il vient :

$$a^{p-1} \equiv a^{n-1} \equiv 1[p] \tag{6}$$

Ainsi, $a^{n-1}-1$ est divisible par tous les facteurs premiers (simples) de n, donc est divisble par n. On a bien :

$$a^{n-1} \equiv 1[n] \tag{7}$$

Dans le sens direct , on suppose n de Carmichael. Par l'absurde, on suppose que n admet un facteur premier p multiple. Notons $n = p^2 m$ avec $m \in \mathbb{Z}$. On considère alors $a := pm + 1$. On a :

$$a^{n-1} = \sum_{k=0}^{n-1} \binom{n-1}{k} p^k m^k \equiv 1 + pm \equiv a[n] \tag{8}$$

Pourtant, on a une relation de Bézout évidente entre n et a : ces deux entiers sont premiers entre eux. Donc par hypothèse :

$$a^{n-1} \equiv 1[n] \tag{9}$$

Mais comme p est premier, $p \geqslant 2$ et donc :

$$1 < a < n \tag{10}$$

Ce qui entraîne une contradiction, car alors $[a]_n \neq [1]_n$. Les facteurs premiers de n sont donc simples. Fixons un tel facteur premier p. Le groupe $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ est cyclique (car c'est le groupe des inversibles d'un corps fini) d'ordre $p-1$. Il contient donc un élément ω d'ordre $p-1$. D'après le lemme des reste chinois, on a l'isomorphisme d'anneaux :

$$\begin{aligned} \Phi : \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ [a]_n &\mapsto ([a]_p, [a]_m) \end{aligned} \tag{11}$$

où m est tel que $n = pm$. Ainsi, il existe un élément $a \in Z$ tel que $[a]_p = \omega$ et $[a]_m = [1]_m$. Un tel élément a est nécessairement premier avec n, car inversible modulo p et m. On a donc par hypothèse :

$$a^{n-1} \equiv 1[n] \tag{12}$$

Et donc, en appliquant l'isomorphisme Φ :

$$\Phi([a^{n-1}]_n) = \Phi([1]_n) = (\omega^{n-1}, [1]_m^{n-1}) = ([1]_p, [1]_m) \tag{13}$$

Donc $\omega^{n-1} = [1]_p$. Comme ω est d'ordre $p-1$, on a $p-1 \mid n-1$, et ceci vaut pour tous les facteurs premiers de n.

□

Critère de Solovey-Strassen

L'étude des nombres de Carmichael va nous permettre d'établir un critère pratique de primalité reposant sur les symboles de Jacobi.

Lorsque p est un nombre premier, les résultats généraux sur les résidus quadratiques indiquent :

$$\forall a \in \mathbb{Z},\ a \wedge p = 1 \implies a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)[p] \tag{14}$$

Nous allons ici établir la réciproque.

Théorème 3 (Solovey-Strassen, ([1], prop 5.28)). *Soit n un entier impair. n est un nombre premier si, et seulement si :*

$$\forall a \in \mathbb{Z},\ a \wedge n = 1 \implies \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}}[n] \tag{$\star$}$$

Démonstration. On s'intéresse uniquement au sens indirect, l'autre sens étant couvert par la théorie des résidus quadratiques dans les corps $\mathbb{F}_p$. Supposons donc que n est un entier satisfaisant $(\star)$. Par l'absurde, on suppose que n est composé. Montrons que c'est nécessairement un nombre de Carmichael. Si a est un entier premier avec n, on a alors :

$$a^{n-1} = \left(a^{\frac{n-1}{2}}\right)^2 \equiv \left(\frac{a}{n}\right)^2 \equiv 1[n] \tag{15}$$

Ainsi, d'après la caractérisation des nombres de Carmichael, il existe $(p_1, \dots, p_r)$ des nombres premiers distincts tels que $n = \prod p_i$ et tels que pour tout $i \in [\![1, r]\!], p_i - 1 \mid n-1$. Puisqu'on a supposé n composé, $r \geqslant 2$. On considère une famille $(x_i)_{1 \leqslant i \leqslant r}$ telle que :

$$\begin{cases} \forall i \in [\![1, r]\!],\ x_i \in \left(\mathbb{Z}/p_i\mathbb{Z}\right)^\times \\ x_1 \text{ n'est pas un carré modulo } p_1 \\ \forall i \in [\![2, r]\!],\ x_i \text{ est un carré modulo } p_i \end{cases} \tag{16}$$

Mais d'après le lemme chinois, on a un isomorphisme d'anneaux :

$$\begin{aligned} \Phi : \mathbb{Z}/n\mathbb{Z} &\to \prod_{i=1}^{r} \mathbb{Z}/p_i\mathbb{Z} \\ [a]_n &\mapsto ([a]_{p_i})_{1 \leqslant i \leqslant r} \end{aligned} \tag{17}$$

Ainsi, en appliquant Φ^{-1} à la famille $(x_i)_{1\leqslant i\leqslant r}$, on trouve un entier a premier avec n (car inversible modulo tous les (p_i)) tel que :

$$\forall i \in [\![1, r]\!],\ [a]_{p_i} = x_i \tag{18}$$

On trouve donc :

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right) = -1 \tag{19}$$

Mais par réduction modulo p_r, en notant k tel que $k(p_r - 1) = n - 1$:

$$a^{\frac{n-1}{2}} \equiv \left(a^{\frac{p_r-1}{2}}\right)^k \equiv \left(\frac{a}{p_r}\right)^k \equiv 1[p_r] \tag{20}$$

Il reste ne qu'à exploiter le diagramme commutatif :

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\pi_{p_r}} & \mathbb{Z}/p_r\mathbb{Z} \\ \downarrow{\scriptstyle \pi_n} & \nearrow & \\ \mathbb{Z}/n\mathbb{Z} & & \end{array} \tag{21}$$

et l'hypothèse $(\star)$: par projection de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/p_r\mathbb{Z}$, on obtient :

$$-1 \equiv \left(\frac{a}{n}\right) \equiv 1[p_r] \tag{22}$$

ce qui est absurde car p_r est impair, puisqu'on a supposé n impair. Donc n est premier. □

On obtient immédiatement un corollaire pratique :

Corollaire 4. *Soit n une entier impair composé. l'ensemble des entiers a de $[\![1, n-1]\!]$ premiers avec n tels que :*

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}}[n] \tag{23}$$

est de cardinal au plus $\varphi(n)/2$, où φ est l'indicatrice d'Euler.

Démonstration. Il suffit de remarquer que l'ensemble des tels éléments a, une fois projeté dans $\mathbb{Z}/n\mathbb{Z}$, est un sous-groupe strict de $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$. Comme, d'après le théorème de Lagrange, son cardinal doit être un diviseur strict de $\varphi(n)$, il est majoré par $\varphi(n)/2$. Enfin, comme $\varphi(n) \leqslant n$, on trouve le résultat. □

Annexe - Test probabiliste de Solovey-Strassen

Tout le travail précédemment effectué permet de créer un test probabiliste de primalité. Il n'y a pas le temps de le présenter pendant le développement, mais ce serait vraiment dommage de se priver de le mettre dans le plan... Vous trouverez beaucoup de remarques instructives sur l'algorithme sur le document d'Alice M.

```
    Algorithme : Solovey-Strassen
Entrée : un entier n > 1 impair, un entier k
Sortie : Vrai ou Faux
Répéter k fois :
   Choisir a ∈ ⟦2, n⟧ avec probabilité uniforme
   Si a ∧ n ≠ 1 :
      Retourner Faux
   Sinon, si (a/n) ≢ a^((n−1)/2) [n] :
      Retourner Faux
Retourner Vrai
```

Proposition 5. *Si l'algorithme renvoie Faux lorsque testé sur n, alors n est composé. Sinon, la probabilité pour que n soit composé est inférieure à $\dfrac{1}{2^k}$.*

Remarque :

- D'après [1], le coût de calcul du symbole de Jacobi s'effectue en $O(\log_2(n)^2)$.
- Le coût de l'algorithme d'Euclide est en $O(n^3)$ pour le calcul du pgcd, et le calcul de $a^{\frac{n-1}{2}} \pmod n$ peut s'effectuer en utilisant l'algorithme d'exponentiation rapide avec une division euclidienne par n à chaque étape, pour un coup total de $n^2 \log_2(n)$.
- Le coût de l'algorithme est finalement en $O(k \cdot n^3)$, soit bien meilleur que les tests déterministes connus.
- Ce test ne permet pas de savoir avec certitude qu'un entier est premier. Toutefois, en prenant $k = 30$, la probabilité qu'un entier composé passe le test de Solovey-Strassen est inférieure à un sur un milliard.

♦

Références

[1] Michel Demazure. *Cours d'algèbre*. Cassini, 2008. isbn : 978-2-84225-127-7.