Un test de pseudo-primalité efficace

Tony EZOME

Université des Sciences et Techniques de Masuku (USTM)
Franceville - Gabon

19 février 2013

Contexte

Dans cet exposé, je vais présenter un travail qui est le fruit d'une collaboration avec J.-M. Couveignes et R. Lercier

Étant donné un entier naturel n, on peut se demander si n est premier ou composé.

Il existe plusieurs méthodes pour étudier la primalité des entiers (article de R. Schoof 2008) :
les tests de Miller-Rabin, AKS, APR-CL, ECPP.

Deux types d'algorithmes :
tests de composition (pseudo-primalité) et tests de primalité.

Objectif

L'objectif de cet exposé est de présenter un nouveau test de pseudo-primalité efficace qui mêle test de Miller-Rabin et extensions galoisiennes

Plan

Un critère de composition est un énoncé concernant les propriétés des inversibles d'un anneau S, qui peut-être $\mathbb{Z}/n\mathbb{Z}$ ou une extension.

À partir du critère de composition, on construit un ensemble de *témoins* W_n et une application

$$P_n : W_n \to \{\text{composite}, \text{prime}\}$$

qui à tout témoin $x \in W_n$ associe une affirmation concernant la primalité de n.

Un *test de composition* est la donnée d'un critère de composition, de l'ensemble des témoins W_n associé à ce critère, et de l'application $P_n : W_n \to \{\text{composite}, \text{prime}\}$.

Lorsque n est premier, l'image de P_n est $P_n(W_n) = \{\text{premier}\}$. Dans ce cas, il n'y a que de *bons témoins*.

Si n est composé, alors les éléments x de W_n tels que $P_n(x) = \text{premier}$ sont appelés *faux témoins*.

On dit que n a *validé un test* P_n, si après avoir choisi uniformément un témoin x dans W_n, on a obtenu $P_n(x) = \text{prime}$.

Deux caractéristiques importantes :

- Le temps de Calcul $n \mapsto T(n)$ de $P_n(x)$,
- La densité de faux témoins $n \mapsto \mu_n$ dans W_n qui mesure la fiabilité du test.

Plan

C'est un test de composition qui repose sur le résultat suivant :

Théorème (Critère Miller-Rabin)

Soit $n \geq 3$ un entier impair. On pose $n-1 = 2^k m$, où m est un entier impair. Si n est premier alors pour tout x dans $(\mathbb{Z}/n\mathbb{Z})^*$

$$x^m = 1, \text{ ou bien } \exists i \in \{0, 1, 2, \ldots, k-1\} \text{ tel que } x^{m2^i} = -1. \quad (1)$$

L'ensemble des témoins pour le test de Miller-Rabin est $W_n = (\mathbb{Z}/n\mathbb{Z})^*$, et l'application associée $\mathrm{MR}_n : (\mathbb{Z}/n\mathbb{Z})^* \to \{\mathrm{composite}, \mathrm{prime}\}$ est définie par :

$$\mathrm{MR}_n(x) = \mathrm{prime} \iff \begin{cases} x^m = 1 \\ \text{ ou} \\ \exists i \in \{0, 1, 2, \ldots, k-1\}, x^{m2^i} = -1. \end{cases}$$

La fiabilité de ce test est donnée par le théorème suivant.

Théorème (R. Schoof)

Soit n un entier impair composé. Alors la densité de faux témoins pour le test Miller-Rabin vérifie

$$\mu_{\mathrm{MR}} = \frac{\#\{x \in (\mathbb{Z}/n\mathbb{Z})^* | \text{ la condition (1) est vérifiée}\}}{\varphi(n)} \leq \frac{1}{2^{t-1}}$$

où $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$ et t est le nombre de diviseurs premiers distincts de n.
De plus si $n \geq 11$, alors $\mu_{\mathrm{MR}} \leq \frac{1}{4}$.

Le test de Miller-Rabin est donc particulièrement efficace lorsque n a beaucoup de diviseurs premiers.

On a au moins une chance sur quatre de détecter un nombre composé $n \geq 11$. La probabilité qu'un entier composé valide k tests de Miller-Rabin indépendants est au plus égale à $(1/4)^k$. le temps de calcul des k tests est $k(\log n)^{2+\epsilon(n)}$.

Ce test ne prouve pas qu'un entier est premier, mais apporte une forte conviction. C'est pourquoi on dit aussi que c'est un test de *pseudo-primalité*.

Plan

Un critère de pseudo-primalité

Le test de Galois est un test de pseudo-primalité qui repose sur le résultat suivant :

Théorème (Couveignes-Ezome-Lercier)

Soit $n \geq 2$ un entier, on pose $R = \mathbb{Z}/n\mathbb{Z}$. Soit $S \supset R$ une R-algèbre commutative fidèle libre de rang fini. Soit σ un R-endomorphisme de S. Soit $\Omega \subset S$ un sous-ensemble de S tel que la plus petite sous R-algèbre de S contenant Ω et stable par σ est encore S. Supposons que $\sigma(\omega) = \omega^n$ pour tout $\omega \in \Omega$. Si n est premier, alors pour tout x dans S on a : $\sigma(x) = x^n$.

En pratique l'algèbre S est telle que $(S, \langle\sigma\rangle)$ est une extension galoisienne de l'anneau $R = \mathbb{Z}/n\mathbb{Z}$.

Le livre de Demeyer et Ingraham et l'article de Chase, Harrison et Rosenberg décrivent les extensions galoisiennes d'anneaux.

Nous insistons sur les éléments suivants :

Definition (F. DeMeyer, E. Ingraham)

Soit R un anneau commutatif unitaire. Soient $S \supset R$ une R-algèbre commutative fidèle et $\mathcal{G}$ un sous-groupe fini de l'ensemble $\mathrm{Aut}_R(S)$ des R-automorphismes de S. On dit que $(S, \mathcal{G})$ est une extension galoisienne de R de degré $\#\mathcal{G}$ si :

1. La sous-algèbre $S^{\mathcal{G}}$ des éléments de S fixés par $\mathcal{G}$ est égale à R.
2. Pout tout idéal maximal M de S et pour tout σ dans $\mathcal{G} - \{\mathrm{Id}_S\}$, il existe un élément x dans S tel que $\sigma(x) - x \notin M$.

Lorsque $\mathcal{G} = \langle\sigma\rangle$, on dit que $(S, \mathcal{G})$ est une extension cyclique de R.

On montre que l'anneau S est une R-algèbre libre de rang $\#\mathcal{G}$.

Il existe plusieurs définitions de la notion d'extension d'anneaux. Nous en donnons encore une autre :

Le produit tensoriel $S \otimes_R S$ a une structure de S-algèbre induite par la relation $s(a \otimes b) = (sa) \otimes b$, pour tous $a, b, s \in S$. Soit

$$i : \quad S \otimes_R S \longrightarrow S^{\#\mathcal{G}}$$

$$x \otimes y \longmapsto (x\sigma(y))_{\sigma \in \mathcal{G}}.$$

Alors on peut remplacer l'assertion (2) de la définiton ci-dessus par : (2)′ L'application $i : S \otimes_R S \to S^{\#\mathcal{G}}$ est un isomorphisme de S-algèbres.

Illustration

Soit $n \geq 2$ un entier, on pose $R = \mathbb{Z}/n\mathbb{Z}$. Soit d un diviseur de $\varphi(n)$. Soit $\zeta \in R^*$ un élément d'ordre exact d (cela signifie que $\zeta^d = 1$ et $\zeta^i - 1$ est inversible pour tout $1 \leq i < d$).

Soit $a \in R^*$ un inversible, on pose $S = R[x]/(x^d - a)$.
On note $\sigma : S \to S$ l'endomorphisme du R-module S défini par $\sigma(x) = \zeta x$. Alors :

- σ est un automorphisme de R-algèbres,
- $\sigma(\sum_i u_i x^i) - \sum_i u_i x^i = \sum_i (\zeta^i - 1) u_i x^i$ (donc $S^{\mathcal{G}} = R$),
- $\sigma^i(x) - x = (\zeta^i - 1)x$ est une unité si $i \neq 0 \bmod d$.

Illustration

Donc $(R[x]/(x^d - a), \langle\sigma\rangle)$ est une extension cyclique de $R = \mathbb{Z}/n\mathbb{Z}$.

Par ailleurs si R est un corps, S une extension de R et $\mathcal{G}$ un groupe fini alors le couple $(S, \mathcal{G})$ est une extension galoisienne de R au sens de la définition ci-dessus

si et seulement si

$(S, \mathcal{G})$ est une extension galoisienne de R au sens de la théorie de Galois classique sur les corps.

Proposition (S. CHase, D. Harrison, A. Rosenberg)

Soient $n > 1$ un entier naturel, on pose $R = \mathbb{Z}/n\mathbb{Z}$. Si $(S, \mathcal{G})$ est une extension galoisienne de R, il existe un élément ω dans S tel que $(\sigma(\omega))_{\sigma \in \mathcal{G}}$ est une R-base de S, autrement dit S possède une base normale sur R.

On peut donc utiliser le critère de pseudo-primalité de tout à l'heure avec les extensions galoisiennes de $\mathbb{Z}/n\mathbb{Z}$.

Construction d'une extension cyclique de degré d

- Algorithme de Berlekamp pour trouver $f(x) \in (\mathbb{Z}/n\mathbb{Z})[x]$ de degré d qui est irréductible si n est premier, $i.e$ $x^{n^i} - x$ est une unité de $R[x]/f(x)$ pour $1 \leq i \leq \frac{d}{2}$.
- On pose $S = R[x]/f(x)$, et $\sigma : S \to S$ l'endomorphisme de R-modules défini par $\sigma(x^i) = x^{ni} \bmod f(x)$ pour $0 \leq i \leq d-1$.
- Vérifier que σ est multiplicative, $i.e$ $\sigma(x^i \bmod f(x)) = x^{ni} \bmod f(x)$ pour $d \leq i \leq 2d-2$.
- Vérifie que σ est d'ordre d, $i.e$ $x^{n^d} - x = 0 \bmod f(x)$.
- Vérifier que $S^\sigma = R$, en utilisant la matrice de σ dans la base $(1, x, \ldots, x^{d-1})$.
- Choisir $u \in S$ et vérifier que $\sigma^i(u) - u \in S^*$ pour $1 \leq i \leq d-1$.

Plan

L'ensemble des témoins pour le test de Galois est égal au groupe S^* des unités de la $\mathbb{Z}/n\mathbb{Z}$-algèbre S, où n est l'entier dont on veut étudier la primalité.

Soit $n = \prod_p p^{v_p}$ la décomposition en facteurs premiers de n. Si p et q sont deux diviseurs premiers de n, alors $p^{v_p} S + q^{v_q} S = S$.

De plus l'intersection des $p^{v_p} S$ est nulle. Donc $S \cong \prod_{p|n} S/(p^{v_p} S) = \prod_{p|n} S_p$.

Ainsi $S^* = \prod_{p|n} S_p^*$. On va donc compter les faux témoins dans chacun des S_p^*.

Cela donne lieu à une étude simple des extensions de l'anneau et/ou de ses quotients $\mathbb{Z}/p\mathbb{Z}$ où p est un diviseur de n.

On obtient des résultats intéressants.

Par exemple si $(S, \langle\sigma\rangle)$ est une extension galoisienne de $\mathbb{Z}/n\mathbb{Z}$ de degré d, alors pour tout nombre premier p divisant n :

- $(S/pS, \langle\sigma\rangle)$ est une extension galoisienne de $\mathbb{Z}/p\mathbb{Z}$.
- il existe un diviseur f de d tel que $pS = \mathfrak{p}_1 \cdots \mathfrak{p}_m$, où $m = d/f$.
- il existe un entier z premier à f tel que

$$x^p = \sigma^{zm}(x) \bmod p, \text{ pour tout } x \in S,$$

C'est-à-dire que l'automorphisme de Frobenius du quotient S/pS est une puissance de σ.

Théorème (Couveignes-Ezome-Lercier)

Soient $A > 2$ et $B \geq 3$ deux nombres réels. Soit $n \geq 3$ un entier, on pose $R = \mathbb{Z}/n\mathbb{Z}$. Supposons que tout diviseur premier de n est plus grand ou égal à B et que n n'est pas une puissance d'un nombre premier. Soit $(S, \langle\sigma\rangle)$ une extension galoisienne de R de rang d. Supposons que p est un nombre premier tel que p^v divise n et $v \log p > \frac{A \log n}{d}$.
Alors la densité $\mu_S = \frac{\#\{x \in S^* | \sigma(x) = x^n\}}{\#S^*}$ de faux témoins dans S^* est telle que

$$\mu_S \leq p^{-\frac{vd}{2}(1-\frac{2}{A}-\frac{4}{B})} \leq n^{-\frac{A}{2}(1-\frac{2}{A}-\frac{4}{B})}.$$

Définition du Test produit

On définit la loi de composition associative

$$\vee : \{\text{composite}, \text{prime}\} \times \{\text{composite}, \text{prime}\} \to \{\text{composite}, \text{prime}\}$$

munie de la table

$\vee$	composite	prime
composite	composite	composite
prime	composite	prime

Test produit

Si pour $1 \leq i \leq r$ les applications $\mathrm{P}_n^i : W_n^i \to \{\mathrm{composite}, \mathrm{prime}\}$ sont r tests de pseudo-primalité.

Le test produit $\mathrm{P}_n = \vee_{1 \leq i \leq r} \mathrm{P}_n^i$ est tel que

$$\mathrm{P}_n \quad : \quad W_n = W_n^1 \times W_n^2 \times \cdots \times W_n^r \longrightarrow \{\mathrm{composite}, \mathrm{prime}\}$$

$$(w_1, \ldots, w_r) \longmapsto \vee_{1 \leq i \leq r} \mathrm{P}_n^i(w_i).$$

Test produit

Un témoin pour P_n est un r-uplet $w = (w_1, \ldots, w_r)$ de témoins w_i des r tests P_n^i. Si n est composé, alors w est un mauvais témoin si et seulement si tous les w_i sont de mauvais témoins.

Donc la densité de mauvais témoins est égale au produit de toutes les densités. Et le temps de calcul du test produit est égal à la somme des complexités multipliée par $\lceil \log_2 r \rceil + 1$.

le test de Galois est efficace lorsque n a est un grand diviseur p^v.

D'autre part, si n a beaucoup de diviseurs premiers il est rapidement détecté par une serie raisonnable de tests de Miller-Rabin.

On a construit (avec Couveignes et Lercier) un test de pseudo-primalité efficace (le test de Miller-Rabin-Galois) qui est le produit d'un test de Galois et de r tests de Miller-Rabin.

Algorithme (Test de Miller-Rabin-Galois)

Pour une densité de faux témoins $\leq 2^{-\lambda}$.

1. *Vérifier que n n'a pas de diviseur premier* < 1000.
2. *Vérifier que n n'est pas une puissance exacte.*
3. *Construire une extension galoisienne* $(S, \langle\sigma\rangle)$ *de* $\mathbb{Z}/n\mathbb{Z}$ *de degré d telle que* $k \leq d \leq k^{1+\epsilon(k)}$ *où* $k = max(16, \lfloor\sqrt{\lambda}\rfloor)$.
4. *Enchaîner r tests Miller-Rabin avec* $r = \lceil\lambda/(0.18 \times d)\rceil$. *Si l'un des tests échoue n est composé.*
5. *Choisir au hasard dans S un élement non nul x et vérifier que x est inversible. Sinon n est composé.*
6. *Vérifier que* $\sigma(x) = x^n$. *Si c'est vraie retouner* prime, *sinon* composite.

Une implémentation de ce test, sur MAGMA V2.18-2, est disponible sur la page internet de Reynald Lercier.

Merci de votre attention !