Extensions d'anneaux et (pseudo)-primalité

(avec R. Lercier et T. Ezome)

J.-M. Couveignes

Institut de Mathématiques de Bordeaux & INRIA Bordeaux Sud-Ouest

Jean-Marc.Couveignes@math.u-bordeaux1.fr

Journées C2

Octobre 2012

Plan

Trois types de tests

- algorithmes déterministes (Agrawal, Kayal, Saxena),
- algorithmes probabilistes Las Vegas (Adleman, Rumely, Pomerance),
- tests de composition (de pseudo-primalité) (Miller, Rabin).

Tests de pseudo-primalité

- Un test de pseudo-primalité repose sur un critère de composition et donne un avis ("premier" ou "composé") sur un entier n.
- Le critère de composition permet de définir une application

$$\mathrm{P}_n : W_n \to \{\mathrm{composite}, \mathrm{prime}\}$$

qui donne une information sur n pour tout x dans W_n.

  - Si n est premier, $\mathrm{P}_n(x) = \mathrm{prime}$ pour tout témoin x dans W_n (tous les x sont de bons témoins)
  - Si n est composé et si $\mathrm{P}_n(x) = \mathrm{prime}$, on dit que x est un faux témoin.

- Deux caractéristiques importantes :
  - le temps de calcul $n \mapsto T(n)$,
  - la densité $n \mapsto \mu(n)$ de faux témoins.

Outline

Le critère de Miller-Rabin

Théorème

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

$$x^m = 1 \text{ ou } x^{2^i m} = -1 \text{ pour un } 0 \leqslant i < k\,. \tag{1}$$

Démonstration.

D'après le théorème de Fermat, $x^{n-1} - 1 = 0$. Mais

$$x^{n-1} - 1 = (x^{\frac{n-1}{2}})^2 - 1 = (x^{\frac{n-1}{2}} - 1)(x^{\frac{n-1}{2}} + 1) = \\ (x^m - 1)(x^m + 1)(x^{2m} + 1) \cdots (x^{2^{k-1} m} + 1)$$

$(\mathbb{Z}/n\mathbb{Z})^*$ est un corps, donc au moins un des facteurs est nul. □

Le test de Miller-Rabin

Corollaire : Si l'on trouve un x tel que Eq. (1) est fausse, alors n est composé.

Théorème (Schoof)

Si n est composé et impair, et s'il a t facteurs premiers, alors

$$\frac{\#\{x \text{ in } (\mathbb{Z}/n\mathbb{Z})^* \ : \ \text{Eq. (1) est vraie}\}}{\varphi(n)} \leqslant \min(\frac{1}{2}, \frac{1}{2^{t-1}}) .$$

Remarque 1 : On peut remplacer $1/2$ par $1/4$ si $n \geq 15$. Après λ tests, la probabilité de manquer un composé est majorée par $1/4^{\lambda}$.

Remarque 2 : Cette majoration est presque optimale. Pour $n = p\,q$ avec $p = 2\,a + 1$, $q = 4\,a - 1$ deux premiers et a impair, $n - 1 = 2\,a\,(4a + 3)$ et il y a beaucoup d'entiers x d'ordre a modulo n.

Preuve I

- Soit l le plus grand entier tel que 2^l divise $p-1$ pour tout diviseur premier p de n. Alors

$$B = \{x \text{ in } (\mathbb{Z}/n\mathbb{Z})^* \ : \ \text{Eq. (1) est vraie}\}$$

$$\text{est contenu dans} \quad B' = \{x \text{ in } (\mathbb{Z}/n\mathbb{Z})^* \ : \ x^{2^{l-1}m} = \pm 1\}$$

- Le nombre de x tels que $x^{2^{l-1}m} = 1$ est le produit sur p du nombre de solutions de $x^{2^{l-1}m} = 1 \bmod p^{a_p}$,

$$\gcd((p-1)p^{a_p-1}, m\,2^{l-1}) \qquad (= \ \gcd(p-1,m)\,2^{l-1})\,.$$

Donc,

$$\#\{x \text{ in } (\mathbb{Z}/n\mathbb{Z})^* \ : \ x^{2^{l-1}m} = 1\} = \prod_{p|n} \gcd(p-1,m)\,2^{l-1}\,.$$

Preuve II

- De même, le nombre de x tels que $x^{2^l m} = 1 \bmod p^{a_p}$ est $\gcd(p-1, m)\, 2^l$, donc le nombre de x tels que $x^{2^{l-1} m} = -1 \bmod p^{a_p}$ est aussi $\gcd(p-1, m)\, 2^{l-1}$. Donc, $\#B' = 2 \prod_{p|n} \gcd(p-1, m)\, 2^{l-1}$, et

$$\frac{\#B'}{\varphi(n)} = 2 \prod_{p|n} \frac{\gcd(p-1, m)\, 2^{l-1}}{(p-1)\, p^{a_p - 1}}.$$

- Comme $\gcd(p-1, m)$ divise $(p-1)/2^l$, on a

$$\frac{\#B'}{\varphi(n)} \leqslant \frac{1}{2^{t-1}}.$$

- Enfin si $t = 1$, $\#B'/\varphi(n) \leq 1/3$.

Complexité

Avec $\lambda/2$ tests de Miller-Rabin, pour n impair, l'algorithme répond prime avec probabilité $\leqslant 2^{-\lambda}$ si n est composé.

Le temps de calcul est

$$(\lambda/2)\,(\log n)^{2+\epsilon(n)}\,.$$

Nous verrons qu'il existe un algorithme qui atteint la même sécurité en temps

$$\lambda^{\frac{1}{2}+\epsilon(\lambda)}\,(\log n)^{2+\epsilon(n)}$$

si $\lambda \leq \log n$.

Outline

Test de Pocklington-Lehmer

Théorème (Pocklington)

Soit $n \geqslant 2$ un entier. Soit $a \in (\mathbb{Z}/n\mathbb{Z})^*$ d'ordre exact $s \geqslant \sqrt{n}$. Alors n est premier.

"a est d'ordre exact s" signifie $a^s = 1$ et $a^i - 1$ est inversible pour $1 \leqslant i < s$ (de façon équivalente $a^{s/q} - 1$ est inversible pour tout diviseur premier q de s).

Démonstration.

Soit p un diviseur premier de n. Le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ contient a mod p. Donc s divise $p-1$. Donc $p \geqslant 1+s > \sqrt{n}$. Donc tout diviseur premier de n est plus grand que $\sqrt{n}$, et n est premier. □

Ce qui est difficile en pratique, c'est de trouver un facteur s assez grand de $n-1$ qui soit produit de petits premiers. Souvent on écrit $n-1 = 2m$ et on est bloqué.

Outline

Extensions galoisiennes d'un anneau

On se donne un anneau R unitaire et commutatif. Et $S \supset R$ une R-algèbre commutative fidèle. Et $G \subset \mathrm{Aut}_R(S)$ un sous-groupe fini. On dit que (R, S, G) est une extension galoisienne si

(i) $S^G = R$,

(ii) Pour tout idéal maximal M de S, et tout $\sigma \neq 1$ dans G, il existe un x dans S tel que $\sigma(x) - x \notin M$.

Variante : on considère le carré tensoriel $S \otimes_R S$ et l'application $S \to S \otimes 1$ qui en fait une S-algèbre. Soit

$$\iota : \qquad S \otimes_R S \longrightarrow S^G$$

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

Alors, on peut remplacer la condition (ii) par

(ii)' L'application $\iota : S \otimes_R S \to S^G$ est un isomorphisme de S-algèbres.

Exemple

Soit $n \geq 2$ un entier. Soit $R = \mathbb{Z}/n\mathbb{Z}$. Soit d un diviseur de $\varphi(n)$. Soit $\zeta \in R^*$ un élément d'ordre exact d. Soit a dans R^* et posons

$$S = R[x]/(x^d - a),$$

et $\sigma : S \to S$ tel que $\sigma(x) = \zeta x$ et $G =< \sigma >$.

- σ est un morphisme de R-algèbres,
- $\sigma(\sum u_i x^i) - \sum u_i x^i = \sum_i (\zeta^i - 1) u_i x^i$,
- $\sigma^i(x) - x = (\zeta^i - 1)x$ est une unité si $i \neq 1 \bmod d$.

Exemple

Soit $n \geq 2$ un entier. Soit $R = \mathbb{Z}/n\mathbb{Z}$. Soit $d \geq 2$ un entier premier et premier à n. Soit $\Phi_d(x) = x^{d-1} + \cdots + x + 1$ le polynôme cyclotomique et posons

$$S = R[x]/\Phi_d(x),$$

et pour tout $a \in (\mathbb{Z}/d\mathbb{Z})^*$ on définit $\sigma_a : S \to S$ par $\sigma(x) = x^a$ et $G = \{\sigma_a | a \in (\mathbb{Z}/d\mathbb{Z})^*\}$.

- σ_a est un morphisme de R-algèbres,
- $\sigma_a(\sum u_i x^i) = u_0 - u_{-a^{-1}} + \sum_{1 \leq i \leq d-2} v_i x^i$ si $a \neq 1 \bmod d$,
- $\sigma_a(x) - x = x(x^{a-1} - 1)$ est une unité si $a \neq 1 \bmod d$.

Extensions cycliques de $\mathbb{Z}/n\mathbb{Z}$

Soit $n \geq 2$ un entier. Soit $R = \mathbb{Z}/n\mathbb{Z}$. Soit (R, S, G) une extension Galoisienne avec $G = \langle \sigma \rangle$ cyclique. On note d la dimension de S sur R. Pour tout premier p divisant n il existe un diviseur f de d tel que

$$pS = \mathfrak{p}_1 \cdots \mathfrak{p}_m$$

avec $m = d/f$. Il existe un entier z premier à f tel que

$$x^p = \sigma^{zm}(x) \bmod p$$

pour tout x dans S. On dit que σ^m est le Frobenius Frob_p.

Outline

Adleman, Pomerance, Rumely test

Soit $R = \mathbb{Z}/n\mathbb{Z}$ et $(R, S, \langle\sigma\rangle)$ une extension galoisienne de degré d.
Soit $a \in S^*$ d'ordre exact s avec $s \geq \sqrt{n}+1$ un diviseur de $n^d - 1$.
Supposons aussi que $\sigma(a) = a^n$. Si p est un diviseur premier de n, alors a est d'ordre s dans $(S/pS)^*$ et il existe $u = zm$ tel que

$$\mathrm{Frob}_p(a) = a^p = \sigma^u(a) = a^{n^u} \in (S/pS)^*.$$

Comme a mod p est d'ordre s on déduit que

$$p = n^u \bmod s. \tag{2}$$

Donc $p \in < n > \subset (\mathbb{Z}/s\mathbb{Z})^*$. L'ordre de ce groupe divise d. Si n n'est pas premier, il existe un premier $p \leq \sqrt{n} < s$ divisant n. Donc (2) implique $p = n_i$ pour un $1 \leq i \leq d-1$ avec $n_i = n^i \pmod s$.
On calcule les n_i et on vérifie qu'aucun ne divise n. Cela prouve que n est premier.

Adleman, Pomerance, Rumely test

Soit $R = \mathbb{Z}/n\mathbb{Z}$ et $(R, S, \langle\sigma\rangle)$ galoisienne de degré d. Soit $a \in S^*$ d'ordre exact s avec $s \geq \sqrt{n}+1$ un diviseur de $n^d - 1$. Supposons $\sigma(a) = a^n$. Alors p est dans le groupe engendré par n dans $(\mathbb{Z}/s\mathbb{Z})^*$. L'ordre de ce groupe divise d. Si n n'est pas premier, il existe un premier $p \leq \sqrt{n} < s$ divisant n. Donc (2) implique $p = n_i$ pour un $1 \leq i \leq d-1$ avec $n_i = n^i \pmod{s}$.
Utile si on peut construire S et $a \in S^*$ d'ordre prouvable grand.
Possible si on connaît un entier petit d tel que $n^d - 1$ a beaucoup de petits diviseurs premiers.

Théorème (Pommerance-Odlyzko)

Il existe une constant positive Θ telle que pour tout $n \geqslant \Theta$ il existe $d \leqslant (\log n)^{\Theta \log\log\log n}$ tel que $n^d - 1$ a un facteur $s > \sqrt{n}$ dont tous les diviseurs premiers sont $\leqslant d+1$.

Construction d'une extension cyclique de $\mathbb{Z}/n\mathbb{Z}$ de degré d

1. Algorithme de Berlekamp pour trouver $f(x) \in (\mathbb{Z}/n\mathbb{Z})[x]$ de degré d qui est irreducible si n est premier, *i.e.*

   $x^{n^i} - x \bmod f(x)$ est une unité dans $(\mathbb{Z}/n\mathbb{Z})[x]/(f(x))$ pour $0 < i \leqslant d/2$

2. On pose $S = (\mathbb{Z}/n\mathbb{Z})[x]/f(x)$, et $\sigma : S \to S$ l'endomorphisme de $(\mathbb{Z}/n\mathbb{Z})$-module tel que $x^i \mapsto x^{in} \bmod f(x)$ pour $0 \leqslant i < d$,
   on calcule sa matrice dans la base $(1, x, ..., x^{d-1})$.
3. Vérifier que σ est multiplicative i.e. $\sigma(x^i) = x^{in} \bmod f(x)$ pour $d \leqslant i < 2d - 1$.
4. Vérifier $\sigma^d = 1$, i.e. $x^{n^d} - x = 0 \bmod f(x)$.
5. Vérifier $S^\sigma = \mathbb{Z}/n\mathbb{Z}$ avec la matrice de σ.
6. Choisir $u \in S$ et vérifier que $\sigma^i(u) - u \in S^*$ pour $0 < i < d$.

Outline

Critère galoisien de primalité

Théorème (Couveignes-Ezome-Lercier)

Soit $n \geqslant 2$ un entier et $S \supset (\mathbb{Z}/n\mathbb{Z})$ une algèbre finie, associative, commutative, fidèle (unitaire). Soit σ un $(\mathbb{Z}/n\mathbb{Z})$-endomorphisme de S. Soit $\Omega \subset S$ un sous-ensemble de S tel que la plus petite sous $(\mathbb{Z}/n\mathbb{Z})$-algèbre de S contenant Ω et stable par σ soit S. On suppose que $\omega^n = \sigma(\omega)$ pour tout ω dans Ω.

Si n est premier, alors pour tout x dans S on a $x^n = \sigma(x)$.

Démonstration.

Soit T le sous-ensemble de S formé des x tels que $x^n = \sigma(x)$. On a $T \supset \Omega$. Si n est premier alors T contient $\mathbb{Z}/n\mathbb{Z}$ et il est stable par addition, multiplication, et action de σ. Donc $T = S$ et $x^n = \sigma(x)$ pour tout x dans S. □

Le test de Galois

Si n est composé, alors les unités $x \in S$ telles que $x^n = \sigma(x)$ sont les faux témoins. Leur densité est

$$\mu = \frac{\#\{x \in S^* | \sigma(x) = x^n\}}{\#S^*}.$$

Si S est une R-algèbre cyclique et $n \geqslant 3$ impair et composé, alors l'étude de la structure Galoisienne de $S*$ montre que soit

$$\mu \leqslant n^{-0.9}$$

soit pour tout diviseur premier p de n on a

$$p^{a_p} < n^{4/d}$$

Soit la densité de faux témoins est faible soit n n'a que de petits (et nombreux) diviseurs premiers.

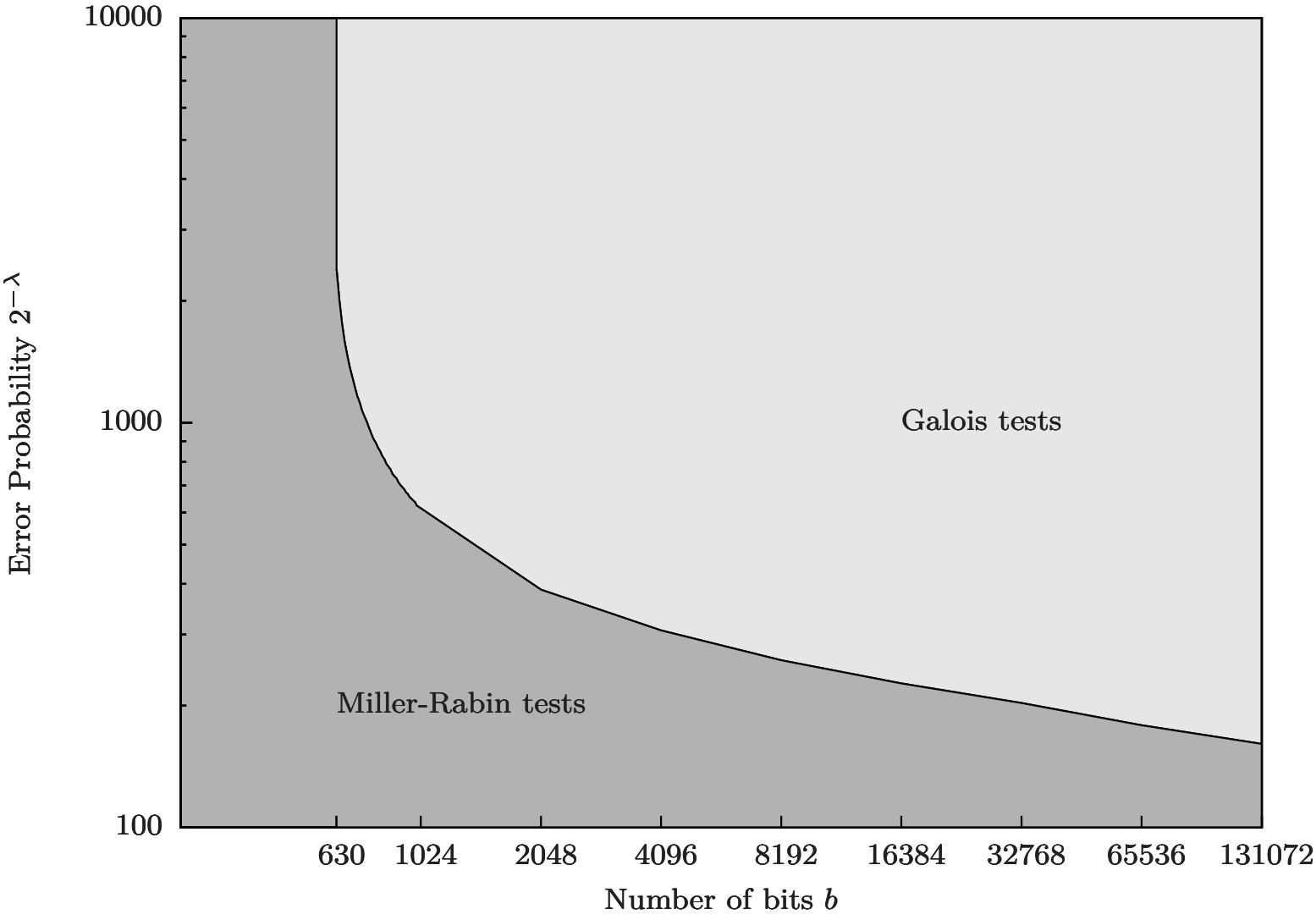
Test composé

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 $(\mathbb{Z}/n\mathbb{Z})$-algèbre S de degré d tel que $k \leqslant d \leqslant k^{1+\epsilon(k)}$ où $k = \max(16, \lfloor\sqrt{\lambda}\rfloor)$.
4. Enchaîner r tests de Miller-Rabin avec $r = \lceil \lambda/(0.18 \times d)\rceil$. Si l'un d'eux échoue on sait que n est composé.
5. Choisir au hasard z non-nul dans S et vérifier qu'il est inversible. Sinon on sait que n est composé.
6. Vérifier que $\sigma(z) = z^n$ et retourner prime si c'est vrai et $\mathrm{composite}$ sinon.

Le temps de calcul est $(\log n)^{2+\epsilon(n)}\lambda^{\frac{1}{2}+\epsilon(\lambda)}$ car d et r sont $\leqslant \lambda^{\frac{1}{2}+\epsilon(\lambda)}$.

Ranges of efficiency



Compared timings for b-bit integers, and prob. up to $2^{-b/2}$ (in seconds)

Based on a Intel Core i7 M620 2.67GHz processor.

Parameters					Galois							Miller–Rabin
b	λ	r	d_{cyc}	d_{kum}	2	4	5	9	$\sigma(x)$	x^n	Tot.	
1024	512	129	1	15	0.0	0.3	–	0.0	0.0	0.2	0.5	0.5
		171	2	6	0.0	0.4	0.0	0.0	0.0	0.3	0.7	
2048	1024	181	1	20	0.0	2.1	–	0.0	0.2	1.5	3.8	6.2
		237	2	8	0.0	2.9	0.0	0.1	0.2	2.0	5.2	
4096	2048	246	1	28	0.0	18.7	–	0.0	1.3	11.6	31.6	75.1
		293	2	12	0.0	22.6	0.0	1.0	1.9	19.8	45.3	
8192	4096	333	1	40	0.4	176.9	–	0.7	1.3	122.5	314.8	1215.0
		424	2	16	0.4	251.6	0.2	5.3	18.8	198.3	474.6	
		316	3	14	0.4	169.7	1.9	7.8	25.6	266.7	472.1	

A reasonably optimized implementation in Magma V2.18-2 is available on the authors' web pages for independent checks.