Quelques tests de primalité

J.-M. Couveignes

Institut de Mathématiques de Bordeaux & INRIA Bordeaux Sud-Ouest

Jean-Marc.Couveignes@u-bordeaux.fr

École de printemps C2

Mars 2014

Plan

Résultats élémentaires

- Complexité des algorithmes antiques
- Distribution des nombres premiers
- Exponentiation rapide
- Preuves courtes de l'ordre d'un élément
- Preuves courtes de primalité et de composition
- PRIME est dans $\mathbf{NP} \cap \mathbf{co} - \mathbf{NP}$
- Tests de composition
- PRIME est dans $\mathbf{co} - \mathbf{RP}$

Critères et tests de composition

Critère de Solovay-Strassen : Si $n \geq 3$ est premier alors pour tout x dans $(\mathbb{Z}/n\mathbb{Z})^*$ on a

$$x^{\frac{n-1}{2}} = \left(\frac{x}{n}\right) \bmod n.$$

L'ensemble des témoins pour ce test est $W_n = (\mathbb{Z}/n\mathbb{Z})^*$ et l'application associée

$$S_n \quad : \qquad (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \{\text{prime}, \text{composite}\}$$

est définie par : $S_n(x) = \text{prime}$ ssi $x^{\frac{n-1}{2}} = \left(\frac{x}{n}\right) \bmod n$.
Si n est premier impair, pas de faux témoins.
Si n est impair composé, la densité de faux témoins est $\leq 1/2$.
Quantités pertinentes : densité $\mu(n)$, complexité $T(n)$. Le quotient

$$\frac{T(n)}{-\log_2 \mu(n)}$$

est le prix d'un bit de sécurité.
On obtient $(\log n)^{2+o(1)}$.

Ordre ou ordre exact

On se donne un groupe *algébrique* G, e.g. groupe multiplicatif ou courbe elliptique sur $\mathbb{Z}/n\mathbb{Z}$.
Soit $G(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^*$ ou $E(\mathbb{Z}/n\mathbb{Z})$ par exemple.

On a un morphisme $\rho_p : G(\mathbb{Z}/n\mathbb{Z}) \to G_p(\mathbb{Z}/p\mathbb{Z})$ pour tout $p|n$.

Soit o premier à n. On dit que $A \in G(\mathbb{Z}/n\mathbb{Z})$ est d'ordre exact o si $oA = 0$ et pour tout $p|n$ l'image $\rho_p(A)$ est d'ordre o dans $G_p(\mathbb{Z}/p\mathbb{Z})$.

Autrement dit pour tout $q|o$ et $p|n$ on a $\frac{o}{q}A \neq 0 \bmod p$.

Ordre ou ordre exact

Soit $n = 7 \times 13 = 91$ et G le groupe multiplicatif.

-1 est d'ordre 2 modulo 7 et 3 est d'ordre 3 modulo 13, donc $3 \times 2 \times 7 + (-1) \times 6 \times 13 = -36 = 55$ est d'ordre 6 modulo n mais pas d'ordre exact 6.

En revanche 3 est d'ordre 6 modulo 7 et 10 est d'ordre 6 modulo 13, donc $10 \times 2 \times 7 + 3 \times 6 \times 13 = 374 = 10$ est d'ordre exact 6.

En particulier $10^2 - 1$ et $10^3 - 1$ sont inversibles modulo n.

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.

Group replacement

On est à l'étroit dans $(\mathbb{Z}/n\mathbb{Z})^*$ car il peut être difficile de factoriser son ordre.
Une idée : changer de groupe

- construire un pseudo-corps à n^d éléments,
- construire une pseudo-courbe elliptique sur $\mathbb{Z}/n\mathbb{Z}$,
- un autre groupe algébrique commutatif sur $\mathbb{Z}/n\mathbb{Z}$, soit un tore, soit une variété abélienne.

Idée utile pour la primalité, la factorisation, la construction de bases de corps finis, etc.

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) $\mathrm{Fix}(G, S) = S^G = R$,

(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

$$\iota : \qquad S \otimes_R S \longrightarrow \mathrm{Map}(G, S) = S^G$$

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

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.

Premières propriétés

• S est un R-module projectif de type fini.
Toute suite courte exacte de R-modules

$$0 \longrightarrow M' \longrightarrow M'' \longrightarrow S \longrightarrow 0$$

est scindée, c'est-à-dire que M'' est isomorphe à $M' \oplus S$.

• Pour tout idéal premier $\mathfrak{p}$ de R, le $R_{\mathfrak{p}}$-module $S \otimes_R R_{\mathfrak{p}}$ est libre de rang $\#G$.
On dit que (R, S, G) est une extension galoisienne de degré $d = \#G$.

Exemple

Soit R un anneau commutatif et $d \geq 3$ et $S = R^d$ et

$$R \longrightarrow S$$

$$r \longmapsto (r, r, \ldots, r).$$

Soit α permutation de $\{1, 2, \ldots, d\}$. Posons

$$\alpha(x_1, \ldots, x_d) = (x_{\alpha(1)}, \ldots, x_{\alpha(d)}),$$

le R-automorphisme de S associé. Soit σ le R-automorphisme d'ordre d de S défini par

$$\sigma(x_1, \ldots, x_d) = (x_2, x_3, \ldots, x_d, x_1).$$

Alors $S^\sigma = R$. Et le morphisme de S-algèbres $\phi : S \otimes_R S \to S^d$ défini par $\phi(a \otimes b) = (a\sigma^k(b))_{k \in \mathbb{Z}/d\mathbb{Z}}$ est un isomorphisme.
Donc $(S, \langle\sigma\rangle)$ est galoisienne de R de degré d.

Exemple

Mais (S, S_d) n'est pas une extension galoisienne de R.

Bien que la sous-algèbre des éléments de S fixés par le groupe symétrique soit $S^{\mathrm{S}_d} = R$.

En effet, notons τ le R-automorphisme de S induit par la transposition $\tau = (1\ 2)$, et soit M un idéal maximal de R. Alors $\mathfrak{M} = R \times R \times M \times R \times \cdots \times R$ est un idéal maximal de S. Et pour tout x dans S, $\tau(x) - x$ appartient à $\mathfrak{M}$. Cela est contraire à la condition (ii) de la définition.

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

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

Pour tout $a \in (\mathbb{Z}/d\mathbb{Z})^*$ on définit $\sigma_a : S \to S$ par $\sigma_a(x) = x^a$ 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 $a \neq 1 \mod d$.

Réduction d'une extension galoisienne

Soient (S, G) une extension galoisienne de R, et $\mathfrak{p}$ un idéal premier de R.

1. L'application
$$R/\mathfrak{p} \times S \longrightarrow S/\mathfrak{p}S$$
$$(r \bmod \mathfrak{p}, s) \longmapsto rs \bmod \mathfrak{p}S$$
est R-bilinéaire et induit un isomorphisme $R/\mathfrak{p} \otimes_R S \cong S/\mathfrak{p}S$.
2. De plus, $(S/\mathfrak{p}S, G)$ est une extension galoisienne de $R/\mathfrak{p}$.

Bases normales

Soient R un anneau commutatif et (S, G) une extension galoisienne de R.

Soit ω un élément de S. Si $(\sigma(\omega))_{\sigma \in G}$ est une R-base de S, alors on dit que c'est une R-base normale de S.

Alors S est isomorphe à $R[G]$, pour la structure de $R[G]$-module sur S induite par $(r\sigma)s = r\sigma(s)$, où $(r, \sigma) \in R \times G$.

Si R est semi-local alors S est un R-module libre de rang $\#G$ et admet une R-base normale.

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

Soit $n \geq 2$ entier. Soit $R = \mathbb{Z}/n\mathbb{Z}$. Soit (R, S, G) une extension Galoisienne. On suppose que $G =< \sigma >$ est cyclique. On note g le degré. Pour tout diviseur premier p de n il existe deux entiers m et f tels que $mf = d$,

$$pS = \mathfrak{p}_1 \times \mathfrak{p}_2 \times \cdots \times \mathfrak{p}_m \text{ et } \sigma(\mathfrak{p}_i) = \mathfrak{p}_{i+1}$$

et

$$\#(S/\mathfrak{p}_i) = p^f,$$

Il existe un entier z premier à f tel que

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

pour tout $x \in S$. On dit que σ^{zm} est le Frobenius Frob_p. Si $zt = 1 \bmod f$ on a

$$\sigma(x) = x^{p^t} = (\mathrm{Frob}_p)^t(x) \bmod p.$$

Adleman, Pomerance, Rumely

Soit $R = \mathbb{Z}/n\mathbb{Z}$ et $(R, S, <\sigma>)$ une extension cyclique 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

$$p = n^u \bmod s. \tag{1}$$

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

Adleman, Pomerance, Rumely

Soit $R = \mathbb{Z}/n\mathbb{Z}$ et $(R, S, <\sigma>)$ une extension cyclique 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 $\sigma(a) = a^n$.
On calcule les $n_i = n^i \,\%\, s$ et on vérifie qu'aucun n'est un diviseur non-trivial de n. Cela prouve que n est premier.

Théorème (Pommerance-Odlyzko)

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

PRIME est presque dans **RP**.

Mise en pratique

- Chercher d tel que $n^d - 1$ ait assez de petits diviseurs pour former un produit $s > \sqrt{n}$.
- Construire une extension cyclique S de degré d de $\mathbb{Z}/n\mathbb{Z}$.
- Trouver une unité a dans S d'ordre exact s. On choisit $b \in S^*$ et on pose $a = b^{(n^d-1)/s}$.
- Vérifier que $\sigma(a) = a^n$ quitte à changer σ.
- Pour i de 1 à $d-1$ calculer $n_i = n^i \,\%\, s$ et vérifier que $\mathrm{pgcd}(n_i, n) = 1$ ou n.

Algorithme probabiliste (Monte Carlo).

Construire une extension cyclique de $\mathbb{Z}/n\mathbb{Z}$

Ici n est probablement premier. Choisir $f(x) \in (\mathbb{Z}/n\mathbb{Z})[x]$ unitaire de degré d. Appliquer l'algorithme de Berlekamp adapté. Vérifier que

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

Si n est premier, on trouve $f(x)$ facilement. On pose

$$S = (\mathbb{Z}/n\mathbb{Z})[x]/f(x) \text{ et } \sigma : S \to S$$

l'application $(\mathbb{Z}/n\mathbb{Z})$-linéaire telle que $x^i \mapsto x^{in} \bmod f(x)$ pour $0 \leqslant i < d$. Calculer la matrice M de σ dans la base $(1, x, ..., x^{d-1})$.

Vérifier que σ est multiplicative : $\sigma(x^i) = x^{in} \bmod f(x)$ pour $d \leqslant i < 2d - 1$.
Vérifier que $\sigma^d = 1$, soit $x^{n^d} - x = 0 \bmod f(x)$.
Vérifier que $S^\sigma = \mathbb{Z}/n\mathbb{Z}$, à l'aide de M.
Choisir $u \in S$ et vérifier que $\sigma^i(u) - u$ est une unité pour $0 < i < d$.

Un exemple (Tony Ezome)

Montrons que $n = 1801$ est premier.
Pour $d = 4$ on a $n^4 - 1 = 2^4 \times 3 \times 5 \times 43837281030$.
On pose $s = 2^4 \times 3 \times 5$.
On trouve $f(x) = x^4 + x + 1$ tel que $x^{n^i} - x$ soit une unité modulo $f(x)$ pour $1 \leq i \leq 3$.
On pose $S = (\mathbb{Z}/n\mathbb{Z})[x]/f(x)$.
Soit $\sigma : S \to S$ l'endomorphisme de R-modules défini par

$$\sigma(x^i) = x^{ni} \bmod f(x) \text{ pour } i \in \{0, 1, 2, 3\}.$$

On trouve

$$M = \begin{pmatrix} 1 & 428 & 893 & 1385 \\ 0 & 623 & 986 & 1664 \\ 0 & 1396 & 530 & 1558 \\ 0 & 1171 & 1791 & 647 \end{pmatrix}$$

Un exemple

On vérifie que

$$\sigma(x^i) = x^{ni} \bmod f(x) \text{ pour } i \in \{4, 5, 6\}$$

et $x^{n^d} = x$.

La matrice $M - \mathrm{Id}$ admet un mineur 3×3 inversible. Donc $S^\sigma = R$.

L'élément $a = (7 + x)^{\frac{n^d - 1}{s}} \in S$ est d'ordre exact s, car $a^s = 1$,
$a^{\frac{s}{2}} - 1 = -2$, $a^{\frac{s}{3}} - 1 = 1726$, $a^{\frac{s}{5}} - 1 = 349$ qui sont inversibles.
On calcule les $r_i = n^i \,\%\, s$

$$r_1 = 121 \bmod s, \;\; r_2 = 1 \bmod s, \quad \text{et} \quad r_3 = 121 \bmod s.$$

On vérifie que $\gcd(r_i, n) = 1$ pour tout i.

Critère galoisien de composition

Théorème (C.-Ezome-Lercier)

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

Si n est premier, alors tout x de S vérifie $x^n = \sigma(x)$.

Démonstration.

Soit T l'ensemble des $x \in S$ tels que $x^n = \sigma(x)$. Par hypothèse $T \supset \Omega$. 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 $x \in S$. □

Test de Galois

On construit une extension cyclique $(\mathbb{Z}/n\mathbb{Z}, S, <\sigma>)$ comme ci-dessus. Par exemple

$$S = (\mathbb{Z}/n\mathbb{Z})[x]/f(x) \text{ et } \sigma(x^i) = x^{in} \text{ pour } 0 \leq i \leq d-1.$$

Notons que $\Omega = \{x\}$ convient.

On choisit $y \in S^*$ aléatoire uniformément distribué.

On vérifie que $\sigma(y) = y^n$.

Ici $W_n = S^*$. Et $T = (\log n)^{2+o(1)} \times d^{1+o(1)}$.

Quelle est la densité de faux témoins ?

Densité de faux témoins

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 un extension cyclique de $R = \mathbb{Z}/n\mathbb{Z}$ et si $n \geqslant 3$ est composé et impair, on peut prouver à l'aide de la structure galoisienne de S^* que ou bien

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

ou bien pour tout diviseur premier p de n

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

Soit la densité de mauvais témoins est très faible,
soit n a beaucoup de diviseurs premier ...
Densité typique : $\prod_{p|n} \mathrm{pgcd}(p^d - 1, p - n)/(p^d - 1)$.

Combinaison avec Miller-Rabin

Théorème

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

$$\frac{\#\{x \text{ in } (\mathbb{Z}/n\mathbb{Z})^* \ : \ \text{condition de M.-R. est vraie}\}}{\varphi(n)} \leqslant \frac{1}{2^{t-1}}.$$

Si de plus $n \geq 15$ alors $\leqslant 1/4$.

On veut composer des tests de Miller-Rabin et un test de Galois pour tirer parti des deux situations.

Composition de tests

Soit $r \geqslant 2$ un entier et $P_n^i : W_n^i \to \{\text{composite}, \text{prime}\}$ des tests de pseudo-primalité. Le test produit

$$P_n = \vee_{1 \leqslant i \leqslant r} P_n^i$$

est défini comme

$$P_n : \qquad W_n = W_n^1 \times W_n^2 \times \cdots \times W_n^r \longrightarrow \{\text{composite}, \text{prime}\}$$

$$(x_1, \ldots, x_r) \longmapsto \vee_{1 \leqslant i \leqslant r} P_n^i(x_i).$$

Un témoins de P est un vecteur de r témoins.
Il suffit d'avoir un bon témoin pour détecter un composé.

Composition de tests

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

Si n est composé, un témoins est faux si ses r coordonnées sont des faux témoins pour chacun des r tests.

La densité de faux témoins est le produit des densités de chaque test.

Et la complexité est la somme des complexités.

On combine d tests de Miller-Rabin et un Galois de degré d.

Si $d \leq \sqrt{\log n}$ on obtient une densité de $\exp(-d^2)$ et une complexité

$$T = d^{1+o(1)} \times (\log n)^{2+o(1)}.$$

Résumé

- Test de Pocklington-Lehmer
- Group replacement
- Extensions galoisiennes d'anneaux : propriétés, contruction.
- Adleman, Pomerance, Rumely
- Théorème de Pomerance-Odlyzko
- Critère galoisien de composition
- Densité

$$\prod_{p|n} \mathrm{pgcd}((p-1), m\,2^{l-1})/(p-1)$$

remplacée par

$$\prod_{p|n} \mathrm{pgcd}(p^d-1, p-n)/(p^d-1).$$