Quelques tests de primalité

J.-M. Couveignes (merci à T. Ezome et R. Lercier)

Institut de Mathématiques de Bordeaux & INRIA Bordeaux Sud-Ouest

Jean-Marc.Couveignes@u-bordeaux.fr

École de printemps C2

Mars 2014

Plan

Définition et résultats classiques

- Euclide, livre sept des Élément, vers -300 : définition, existence d'un diviseur premier, algorithme pour pgcd et ppcm, infinité, $p_{k+1} \leq \prod_{l \leq k} p_l + 1$,
- crible d'Eratosthène,
- théorème fondamental de l'arithmétique (preuve par Gauss),
- complexité linéaire pour $+$, quadratique pour $\times$, exponentielle pour primalité et factorisation : $T = n^{1/2+o(1)}$.

Distribution des nombres premiers

A	10	100	1000	10000	100000
$\pi(A)$	4	25	168	1229	9592
$A/\pi(A)$	2.5	4	5.95	8.14	10.4
$\log A$	2.3	4.6	6.9	9.2	11.5

Théorème des nombres premiers : $\pi(A) = \frac{A}{\log A} \times (1 + o(1))$ et $p_n = (1 + o(1)) \times n \log n$.
Assez nombreux !

Exponentiation

Étant donné g dans G et e entier naturel, calculer g^e.

Maladroit g, g^2, g^3, $\ldots$, g^{e-1}, g^e.

$$T = (e - 1).$$

L'algorithme d'*exponentiation rapide* permet de calculer efficacement g^e. Méthode inventée par Piṅgala dans son Chandah-sûtra (entre -450 et -250).

$e = \sum_{0 \leq k \leq K} \epsilon_k 2^k$ et $b_0 = g$, $b_k = b_{k-1}^2$ pour $1 \leq k \leq K$.
Puis

$$g^e \equiv \prod_{0 \leq k \leq K} b_k^{\epsilon_k}.$$

$$T = O(\log e).$$

Ordre d'un élément dans un groupe

$$0 \longrightarrow o\mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow G$$

$$a \longmapsto g^a.$$

Trouver o ? Prouver o ?
Si $f = \prod_i p_i^{m_i}$ et $q_i = f/p_i$ et $g^f = 1$ et $g^{q_i} \neq 1$ alors $f = o$.
Si l'on a des *preuves courtes* de primalité, on a des preuves courtes pour l'ordre d'un élément dans un groupe.

Un peu d'arithmétique

Les propriétés de l'anneau $\mathbb{Z}/n\mathbb{Z}$ reflètent la factorisation de n.
Si $n = \prod_i p_i^{m_i}$ alors $\mathbb{Z}/n\mathbb{Z} \equiv \prod_i (\mathbb{Z}/p_i^{m_i}\mathbb{Z})$.

Bijection effective : $r_i = n/p_i^{m_i}$ et s_i inverse de r_i modulo $p_i^{m_i}$

$$(u_i)_i \mapsto \sum_i u_i r_i s_i \bmod n.$$

En particulier $(\mathbb{Z}/n\mathbb{Z})^*$ est d'ordre $\prod_i p_i^{m_i-1}(p_i - 1)$ donc
$\#(\mathbb{Z}/n\mathbb{Z})^* = n - 1 \iff n$ est premier.

Une preuve que g mod n est d'ordre $n-1$ est une preuve de primalité.

Preuves courtes de primalité

Exhiber un générateur g de $(\mathbb{Z}/n\mathbb{Z})^*$
et une preuve que g est d'ordre $n-1$.

Exhiber la factorisation $n-1 = \prod_i p_i^{m_i}$ et une preuve que les p_i sont premiers.

Vérifier que $g^{n-1} = 1$ et $g^{\frac{n-1}{p_i}} \neq 1$.

PRIMES est dans **NP** $\cap$ **co-NP**.

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.

Des premiers pour quoi faire ?

On va voir que PRIMES est dans **P**.

Le problème de la factorisation ne semble pas être dans **P**.

Fonctions asymétriques et fonctions trappes.

Pour construire des groupes multiplicatifs et utiliser des logarithmes discrets. On connaît $\#(\mathbb{Z}/p\mathbb{Z})^*$.

Pour construire des corps finis et faire de la géométrie :
$(3x + 2y)^p = 3x^p + 2y^p \in \mathbb{F}_p[x, y]$. Si V est une variété algébrique sur $\mathbb{F}_p$ on a une application $F : V \to V$. On peut calculer $\#E(\mathbb{F}_p)$.

Critère de Fermat

Si n est premier alors $x^n = x \bmod n$ pour tout entier x et $x^{n-1} = 1 \bmod n$ si $(x, n) = 1$.
Preuve 1 : on vérifie pour $x = 1$ et on utilise $(x + y)^p = x^p + y^p$.
Preuve 2 : théorème de Lagrange.
Critère de composition : $W_n = (\mathbb{Z}/n\mathbb{Z})^*$, F_n associée est définie par :

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

$$x \longmapsto \begin{cases} \text{prime si } x^{n-1} = 1 \bmod n \\ \text{composite si } x^{n-1} \neq 1 \bmod n \end{cases}$$

On choisit x au hasard (comment ?) et on calcule $F_n(x)$.
Si $F_n(x) = \text{composite}$ alors n est composé. Critère de composition.
Si $F_n(x) = \text{prime}$ que faire ?

Critère de Fermat

Combien de faux témoins ? Pas trop en général.

100% pour les nombres de Carmichael

exemple $n = 561 = 3 \times 11 \times 17$. Que se passe-t-il ?

Il y a une infinité de nombres de Carmichael d'après Alford, Granville, Pomerance.

Le test de Fermat n'a pas de faux témoins si n est premier, mais peut avoir 100% de faux témoins pour certains nombres composés.

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.

Critère de composition : $W_n = (\mathbb{Z}/n\mathbb{Z})^*$, M_n associée est définie par :

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

$$x \longmapsto \begin{cases} \text{prime si (1) est vraie} \\ \text{composite sinon} \end{cases}$$

On choisit x au hasard et on calcule $M_n(x)$.
Comment ? Complexité ?
Si $M_n(x) = \text{composite}$ alors n est composé. Critère de composition.
Si $M_n(x) = \text{prime}$ que dire ?

Le test de Miller-Rabin

Théorème

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

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

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

Remarque 1 : 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

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

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

Si $x^m = 1 \bmod n$ alors $x \in B'$. Si $x^{m2^i} = -1 \bmod n$ avec $1 \leq i < k$ alors 2^{i+1} divise $p-1$ pour tout $p|n$. Donc $l \geq i+1$. Donc $x^{2^{l-1}m} = (-1)^{2^{l-i-1}}$.

Preuve II

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

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

Donc,

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

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

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

Preuve III

- Comme $2^{l-1}\mathrm{pgcd}(p-1,m)$ divise $(p-1)/2$, on a

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

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

Complexité et fiabilité

Si n est premier, pas de faux temoin.
Si n est composé, la densité de faux témoins est $\leq 1/4$ et $\leq 1/2^{t-1}$.

$T = (\log n)^{2+\epsilon(n)}$ avec exponentiation et arithmétique rapides.

Avec $\lambda/2$ tests de Miller-Rabin, pour $n \geq 15$ 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 $\lambda \leq \log n$.

Symbole de Legendre

Soit $n \geq 3$ un entier premier. Pour a entier $\left(\frac{a}{n}\right)$ est défini par

$$\left(\frac{a}{n}\right) = \begin{cases} 0 & \text{si } a = 0 \bmod n. \\ 1 & \text{si l'équation } X^2 = a \text{ a deux solutions dans } \mathbb{Z}/n\mathbb{Z}. \\ -1 & \text{si l'équation } X^2 = a \text{ n'a aucune solution dans } \mathbb{Z}/n\mathbb{Z}. \end{cases}$$

On a $\left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \bmod n$. En effet si $a = b^2$ alors $a^{\frac{n-1}{2}} = b^{n-1} = 1$ et le polynôme $x^{\frac{n-1}{2}} - 1$ n'a pas plus de $(n-1)/2$ solutions.
Cela donne une première méthode pour calculer efficacement ce symbole.
Notons que $a \mapsto \left(\frac{a}{n}\right)$ est un morphisme de groupes.

Loi de réciprocité quadratique

Théorème

Si p et q sont des premiers impairs positifs et distincts, alors

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}},$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}, \text{ et } \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Démonstration.

Soit $\Phi_q(x) = 1 + x + \cdots + x^{q-1}$ et $A(x) \in \mathbb{F}_p[x]$ un facteur irréductible de $\Phi_q(x)$ modulo p. Soit $\mathbb{L} = \mathbb{F}_p[x]/A$ et $\zeta = x \bmod A(x) \in \mathbb{L}$. C'est une racine q-ième primitive de l'unité dans $\mathbb{L}$. La *somme de Gauss*

$$\tau = \sum_{x \in \mathbb{F}_q^*} \left(\frac{x}{q}\right) \zeta^x$$

est dans $\mathbb{L}$. On montre que $\tau^2 = \left(\frac{-1}{q}\right) q \in \mathbb{L}$. Donc τ est une racine carrée de $\left(\frac{-1}{q}\right) q$. Cette racine est dans $\mathbb{F}_p$ si et seulement si $\tau^p = \tau$. On vérifie que $\tau^p = \left(\frac{p}{q}\right) \tau$. Donc $\left(\frac{-1}{q}\right) q$ est un carré modulo p si et seulement si $\left(\frac{p}{q}\right) = 1$. □

Symbole de Jacobi

Soit $N \geq 3$ entier impair et $N = \prod_i p_i^{e_i}$ sa factorisation. Le symbole de Jacobi est

$$\left(\frac{x}{N}\right) = \prod_i \left(\frac{x}{p_i}\right)^{e_i}.$$

Dépend de x mod N. Et $\left(\frac{a}{b}\right) \neq 0$ ssi $\mathrm{pgcd}(a, b) = 1$.

Théorème (Gauss)

Pour $M \geq 3$ et $N \geq 3$ impairs $\left(\frac{-1}{M}\right) = (-1)^{\frac{M-1}{2}}$, $\left(\frac{2}{M}\right) = (-1)^{\frac{M^2-1}{8}}$,

et

$$\left(\frac{M}{N}\right)\left(\frac{N}{M}\right) = (-1)^{\frac{(M-1)(N-1)}{4}}.$$

Calcul du symbole de Jacobi

Pour calculer $\left(\frac{M}{N}\right)$ on utilise alternativement trois idées

- remplacer M par $M\%N$,
- si M est pair, sortir 2,
- si M est impair et $< N$ basculer.

$$T = (\log \max(M, N))^{2+o(1)}.$$

Et même mieux.

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 donc $W_n = (\mathbb{Z}/n\mathbb{Z})^*$ et l'application associée

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

est définie par : $S_n(x) = \text{prime}$ ssi $x^{\frac{n-1}{2}} = \left(\frac{x}{n}\right) \bmod n$.

Densité de faux témoins

Si n est premier impair, pas de faux témoins.

Théorème

Si n est un entier impair composé, la densité de faux témoins vérifie

$$\frac{\{x \in (\mathbb{Z}/n\mathbb{Z})^* |\ x^{\frac{n-1}{2}} = \left(\frac{x}{n}\right) \bmod n\}}{\varphi(n)} \leq \frac{1}{2},$$

où $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$.

Complexité ? Densité ? Comparaison avec Miller-Rabin ?

Bilan

On a montré que PRIME est dans $\mathbf{co}-\mathbf{RP}$.

Montrer que PRIME est dans **RP** a pris beaucoup de temps.
Adleman et Huang l'ont montré en 1992.

Rappel : $\mathbf{RP} \cap \mathbf{co}-\mathbf{RP}$ est noté **ZPP**.

Quantités pertinentes pour un test de composition : densité $\mu(n)$, complexité $T(n)$. Le quotient

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

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

Résumé

- 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 $\mathbf{NP} \cap \mathbf{co} - \mathbf{NP}$
- Ordre exact
- Test de Pocklington-Lehmer
- Tests de composition (Miller-Rabin, Solovay-Strassen)
- PRIME est dans $\mathbf{co} - \mathbf{RP}$