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 $\mathbf{co} - \mathbf{RP}$,

Résumé

- Ordre exact,
- Test de Pocklington-Lehmer,
- Group replacement,
- Extensions galoisiennes d'anneaux : propriétés, contruction,
- Adleman, Pomerance, Rumely,
- Théorème de Pomerance-Odlyzko, $T = (\log n)^{\Theta \log\log\log n}$,
- Critère galoisien de composition,
- Densité

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

remplacée par

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

Encore un critère galoisien

Théorème (Agrawal, Kayal, Saxena)

Soient $n \geq 2$, $R = \mathbb{Z}/n\mathbb{Z}$ *et* $(R, S, <\sigma>)$ *une extension cyclique de degré* d. *Soient* $a \in S^*$ *et* $\sigma_n \in <\sigma>$ *tels que* $\sigma_n(a) = a^n$. *Soient* $p|n$, $K = \mathbb{Z}/p\mathbb{Z}$, $L = S/pS$ *et* $b = a \bmod p$. *Soit* $\Gamma = <\sigma_n, \mathrm{Frob}_p>$. *Si l'ordre de* $b \in L^*$ *est* $\geq n^{\lfloor\sqrt{\#\Gamma}\rfloor}$ *alors* n *est une puissance de* p.

Théorème (Adleman, Pomerance, Rumely)

Soient $n \geq 2$, $R = \mathbb{Z}/n\mathbb{Z}$ *et* $(R, S, <\sigma>)$ *une extension cyclique de degré* d. *Soit* $a \in S^*$ *d'ordre exact* $s \geq \sqrt{n} + 1$ *tel que* $\sigma(a) = a^n$.
Si n *est composé il admet un diviseur premier* p *égal à* $n^i \,\%\, s$ *pour un* $1 \leq i \leq d - 1$.

Critère AKS

Dans L on vérifie que

$$b^n = \sigma_n(b) = \sigma^t(b) \text{ et } b^p = \mathrm{Frob}_p(b) = \sigma^z(b).$$

Soit $q = n/p$. On a

$$b^q = b^{\frac{n}{p}} = \sigma^{t-z}(b).$$

Donc

$$b^{q^k p^l} = \sigma^{k(t-z)+lz}(b).$$

Il existe deux couples distincts (k_1, l_1) et (k_2, l_2) dans $\{0, 1, 2, \ldots, \lfloor \sqrt{\#\Gamma} \rfloor\}$ tels que

$$k_1(t-z) + l_1 z = k_2(t-z) + l_2 z \bmod \#\Gamma,$$

donc

$$q^{k_1} p^{l_1} = q^{k_2} p^{l_2} \bmod \text{ ordre de } b \text{ qui est } \geq n^{\sqrt{\#\Gamma}}.$$

Extension cyclotomique

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

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

Pour tout $k \in (\mathbb{Z}/r\mathbb{Z})^*$ on définit $\sigma_k : S \to S$ par $\sigma_k(x) = x^k$ et $G = \{\sigma_k | k \in (\mathbb{Z}/r\mathbb{Z})^*\}$.

- σ_k est un morphisme de R-algèbres,
- $\sigma_k(\sum u_i x^i) = u_0 - u_{-k^{-1}} + \sum_{1 \leq i \leq r-2} v_i x^i$ si $k \neq 1 \bmod r$,
- $\sigma_k(x) - x = x(x^{k-1} - 1)$ est une unité si $k \neq 1 \mod r$.

Les trois conditions d'Agrawal, Kayal et Saxena

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

1. Pour tout $0 \leq j \leq r-2$, on a $(x+j)^n = x^n + j$, dans S.
2. Pour tout $1 \leq i < (\log n/\log 2)^2$, r ne divise pas $n^i - 1$;
3. Aucun des nombres premiers $\leq r$ ne divise n ;

Si les trois conditions sont satisfaites, il existe un $p|n$ et un a dans S tel que $a^n = \sigma_n(a)$ et $b = a \bmod p$ est d'ordre $\geq n^{\lfloor\sqrt{\#\Gamma}\rfloor}$ dans L^*. Ici

$$\Gamma =< n, p > \in (\mathbb{Z}/r\mathbb{Z})^* = G.$$

Donc n est une puissance de p.

Le théorème des nombres premiers permet de garantir les conditions 2 et 3 pour un $r = O((\log n)^5)$ si n est premier. Le temps pour trouver r est polynomial. Pour vérifier la condition 1 aussi.

Existence d'un élément de grand ordre

2 implique $n \neq 1 \bmod r$ donc il existe $p|n$ tel que $p \neq 1 \bmod r$.

$K = \mathbb{Z}/p\mathbb{Z}$, $L = S/pS$, $H \subset L^*$ l'ensemble de u tels que $u^n = \sigma_n(u)$.

H contient les $x + j$ pour $0 \leq j \leq r - 2$. Ils sont distincts car $p > r$ d'après la condition 3. Leurs combinaisons multiplicatives sont deux à deux distinctes. Si $E_1, E_2 \subset \{0, 1, \ldots, r - 2\}$ distincts alors

$$\prod_{j \in E_1} (x + j) \neq \prod_{j \in E_2} (x + j) \bmod (\Phi_r, p).$$

Donc $\#H \geq 2^{r-1}$. Or $pS = \mathfrak{p}_1 \times \mathfrak{p}_2 \times \cdots \times \mathfrak{p}_m$ avec $mf = r - 1$ et $\#(S/\mathfrak{p}_i) = p^f$ et f est l'ordre de Frob_p dans $G = (\mathbb{Z}/r\mathbb{Z})^*$.
Montrons que l'image K (cyclique) de H dans $S/\mathfrak{p}_1$ est assez grande.

Action de Galois

Soit Γ le sous-groupe de $G \sim (\mathbb{Z}/r\mathbb{Z})^* \subset \mathrm{Aut}(L/K)$ engendré par σ_p et σ_n. On a $\#\Gamma \geq (\log n/\log 2)^2$ d'après 2.

$$H \longrightarrow \prod_{\sigma \in G/\Gamma} S/\mathfrak{p}_1 S$$

$$u \longmapsto (\sigma(u) \bmod \mathfrak{p}_1)_{\sigma \in G/\Gamma}$$

est une injection car

$$\sigma_i(u) = 1 \bmod \mathfrak{p}_1 \implies \sigma_i(u^n) = 1 \implies \sigma_i(\sigma_n(u)) = 1 \implies \sigma_{in}(u) = 1,$$

$$\sigma_i(u) = 1 \bmod \mathfrak{p}_1 \implies \sigma_i(u^p) = 1 \implies \sigma_i(\sigma_p(u)) = 1 \implies \sigma_{ip}(u) = 1.$$

Donc $\#H \leq (\#K)^{\frac{\#G}{\#\Gamma}}$ et

$$\#K \geq (\#H)^{\frac{\#\Gamma}{\#G}} \geq (2^{r-1})^{\frac{\#\Gamma}{\#G}} = 2^{\#\Gamma} = (2^{\sqrt{\#\Gamma}})^{\sqrt{\#\Gamma}} \geq n^{\sqrt{\#\Gamma}}.$$

Algorithme d'Agrawal, Kayal et Saxena

Soit $n \geq 3$ un entier naturel, on pose $R = \mathbb{Z}/n\mathbb{Z}$.

1. Vérifier que n n'est pas une puissance propre d'un entier.
2. a. Déterminer le plus petit nombre premier r ne divisant pas n ni aucun des $n^i - 1$ pour $0 \leq i < (\log n / \log 2)^2$.
   b. Puis vérifier que n n'est divisible par aucun des premiers $\leq r$.
3. Vérifier que $(x + j)^n = x^n + j$ dans $S = R[x]/\Phi_r(x)$, pour $0 \leq j \leq r - 2$.

Si n ne passe pas les tests, il est composé. Et s'il les passe tous, il est premier.

$r = O((\log(n))^5)$ donc $T = (\log n)^{12+o(1)}$.

Choix de r

On cherche le plus petit premier r ne divisant pas

$$A = n \prod_{i<(\log_2(n))^2} (n^i - 1).$$

Or $\log A \leq \log n + \log n \sum_{i<(\log_2(n))^2} i = O((\log n)^5)$.

On peut montrer qu'il existe une constante Θ telle que

$$\sum_{l \leq L} \log l \geq \Theta L.$$

Donc le plus petit nombre premier qui ne divise pas A est $O((\log n)^5)$.

Algorithme d'Agrawal, Kayal et Saxena

Donc PRIME est dans **PTIME**.

Pas efficace. Lenstra et Pomerance proposent une variante déterministe de complexité $T = (\log n)^{6+o(1)}$.

Les meilleures versions de Adleman, Pomerance, Rumely, sont plus efficaces en pratique.

Autre ressource : le *group replacement*.

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).

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.

On a déjà remplacé $\mathbb{Z}/n\mathbb{Z}$ par une extension galoisienne.

Courbe elliptique

C'est un groupe algébrique : l'ensemble et la loi sont définis par des équations polynomiales.
Si E est défini sur R on note $E(R)$ l'ensemble des sections (solutions).
Si E est une courbe elliptique sur R et $\mathfrak{u}$ un ideal de R alors

$$\rho_{\mathfrak{u}} : E(R) \to E(R/\mathfrak{u})$$

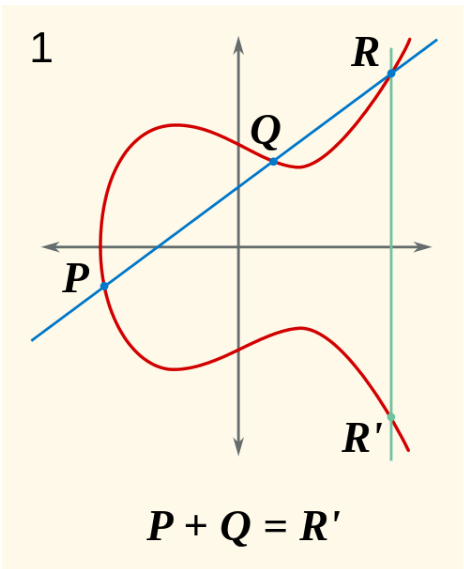
est un morphisme de groupes.
Si R est un anneau fini alors le temps pour une opération dans $E(R)$ est $\log(\#R)^{1+o(1)}$.
Intervalle de Hasse : si R est un corps fini d'ordre q alors

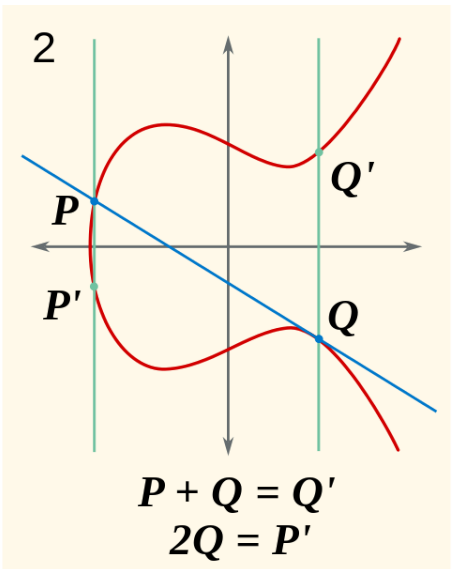
$$\#E(R) \in [q+1-2\sqrt{q}, q+1+2\sqrt{q}].$$

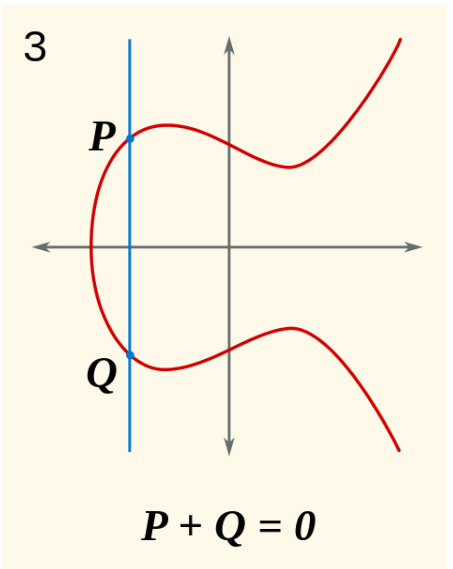
Cet ordre se calcule en temps deterministe $(\log q)^{5+o(1)}$ avec l'algorithme de Schoof.
Si $\mathrm{pgcd}(a,b) = 1$ alors
$E_{\mathbb{Z}/ab\mathbb{Z}}(\mathbb{Z}/ab\mathbb{Z}) = E_{\mathbb{Z}/a\mathbb{Z}}(\mathbb{Z}/a\mathbb{Z}) \times E_{\mathbb{Z}/b\mathbb{Z}}(\mathbb{Z}/b\mathbb{Z})$.

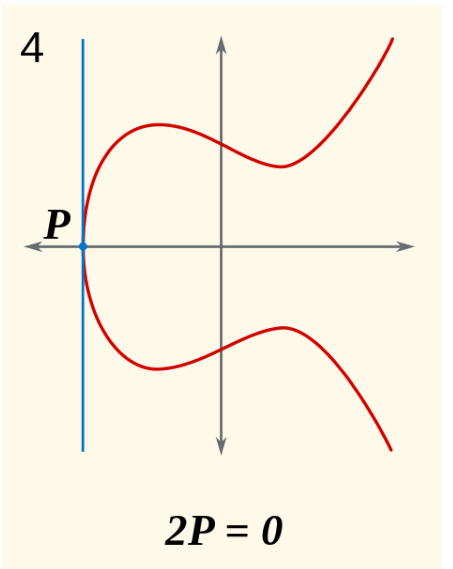
Le dessin que tout le monde attendait

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$









Ordre exact d'un point

Soient E une courbe sur $\mathbb{Z}/n\mathbb{Z}$ et $\mathrm{pgcd}(o, n) = 1$. Un point A est d'ordre exact o ssi $oA = 0$ 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 $\frac{o}{q}A \neq 0 \bmod p$.

Théorème (Goldwasser, Kilian)

Soient N un entier naturel et E une courbe elliptique sur $\mathbb{Z}/N\mathbb{Z}$. On suppose qu'il existe un point $A \in E(\mathbb{Z}/N\mathbb{Z})$ d'ordre exact s avec $s > (\sqrt[4]{N} + 1)^2$. Alors N est premier.

ECPP

Théorème (Goldwasser, Kilian)

Soient N un entier naturel et E une courbe elliptique sur $\mathbb{Z}/N\mathbb{Z}$. On suppose qu'il existe un point $A \in E(\mathbb{Z}/N\mathbb{Z})$ d'ordre exact s avec $s > (\sqrt[4]{N}+1)^2$. Alors N est premier.

Démonstration.

Soit p un diviseur premier de n. L'ordre de $A \in E(\mathbb{Z}/p\mathbb{Z})$ est égal à s. Donc $\#E(\mathbb{Z}/p\mathbb{Z}) > (\sqrt[4]{N}+1)^2$. Or d'après la borne de Hasse $\#E(\mathbb{Z}/p\mathbb{Z}) \leq (\sqrt{p}+1)^2$.
Ainsi

$$(\sqrt{p}+1)^2 > (\sqrt[4]{N}+1)^2.$$

Par conséquent tout diviseur p de N vérifie $p > \sqrt{N}$. Donc N est un nombre premier. □

Première idée

On choisit une courbe au hasard E modulo N.

Si N est premier, le cardinal $\#E(\mathbb{Z}/N\mathbb{Z})$ est un nombre dans $[N+1-2\sqrt{N}, N+1+2\sqrt{N}]$ avec répartition presque uniforme.

On le calcule avec l'algorithme de Schoof comme si N était premier.

Avec un peu de chance, $c = \#E(\mathbb{Z}/N\mathbb{Z})$ admet un facteur s facile à factoriser et $> (\sqrt[4]{N}+1)^2$.

Soient $B \in E(\mathbb{Z}/N\mathbb{Z})$ aléatoire et $A = \frac{c}{s}B$. C'est probablement un point d'ordre exact s.

On le vérifie. Reste à prouver la factorisation de s récursivement.

Améliorations

On ne choisit pas E au hasard mais *à multiplication complexe*.
Plus facile de calculer le cardinal. Mais moins aléatoire ...

Algorithme efficace mais non prouvé.
Complexité heuristique $T = (\log n)^{4+o(1)}$.
Très efficace en pratique. Preuves courtes.

Principale difficulté théorique : randomisation trop faible.

Adleman et Huang : variétés abéliennes. Bonne randomisation.
Prouvent que PRIME est dans **RP**. Inefficace.

Bilan mitigé

Mais si les matières qu'il traite ne sont pas nouvelles, la disposition en est nouvelle. Quand on joue à la paume, c'est une même balle dont joue l'un et l'autre ; mais l'un la place mieux.

J'aimerais autant qu'on l'accusât de se servir des mots anciens : comme si les mêmes pensées ne formaient pas un autre corps de discours par une disposition différente ; aussi bien que les mêmes mots forment d'autres pensées par les différentes dispositions.

Blaise Pascal

État de l'art

- Algorithme déterministe prouvé $T = (\log n)^{6+o(1)}$,
- Algorithme Las Vegas prouvé $T = (\log n)^{4+o(1)}$, $S = (\log n)^{3+o(1)}$,
- Algorithme Las Vegas non-prouvé $T = (\log n)^{4+o(1)}$, $S = (\log n)^{2+o(1)}$,
- Un bit de sécurité Monte-Carlo $T = (\log n)^{2+o(1)}$, $S = (\log n)^{1+o(1)}$.

Bibliographie

Manindra Agrawal, Neeraj Kayal, and Nitin Saxena.
PRIMES is in P.
Annals of Mathematics, 160(2) :781–793, 2004.

Daniel J. Bernstein.
Proving primality in essentially quartic random time.
Mathematics of Computation, 76(257) :389–403, January 2007.

F. Morain.
Implementing the asymptotically fast version of the elliptic curve primality proving algorithm.
Mathematics of Computation, 76(257) :493–505, January 2007.

R. Schoof.
Four primality testing algorithms.
In *Algorithmic number theory*, volume 44 of *Math. Sci. Res. Inst. Publ., Surveys in Number Theory*, pages 101–126. Cambridge Univ. Press, Cambridge, 2008.