Primalité :

Quoi de neuf ?

Journées “Codes & Cryptographie”, Luminy, 12 novembre 2002

François Arnault

PRIMES is in P

Agrawal, Kayal, Saxena

`http://www.cse.iitk.ac.in/primality.pdf`

$2^{13466917} - 1$ est premier

(4 053 946 chiffres décimaux, nombre de Mersenne)

45 jours, 800 MHz

Test de Lucas-Lehmer :

$$L_0 = 4, \qquad L_{k+1} = L_k^2 - 2 \bmod p \quad \text{pour } k \geqslant 1.$$

$$M_p = 2^p - 1 \text{ est premier } \iff \begin{cases} p \text{ est premier} \\ L_{p-2} = 0. \end{cases}$$

$$\mathbf{10^{5019} + 3^2 \cdot 7^5 \cdot 11^{11} \text{ est premier}}$$

$$= \mathbf{10000000000000000000 \ldots 00000000000431570992316316 93}$$

(5020 chiffres décimaux)

13 semaines, 1300 MHz, ECPP

Certification de nombres premiers cryptographiques

Preuve de primalité par ECPP

— en $\simeq$ seconde(s) pour 512 bits

— en $\simeq$ minute(s) pour 1024 bits

algorithme probabiliste, coût estimé en $\mathcal{O}'(\ln^6 N)$

Algorithme APRCL (Sommes de Jacobi)

algorithme déterministe, mais non polynomial

Génération de premiers sains

1024 bits en peu de secondes

Génération de clés DSA par GnuPG

p, q premiers tels que $q \mid p-1$
avec $|p| = 1024$ bits et $|q| = 160$ bits
et $p-1$ non friable

$$k = \lceil (|p| - |q| - 1)/|q| \rceil$$

• Choisir m nombres premiers q_i de taille $l \simeq (|p| - |q| - 1)/k$ (donc $l \geqslant |q|$), avec m assez grand pour que $C_m^k \gg \ln(p)$.

• Choisir k des q_i tels que $p = 2qq_1 \dots q_k + 1$ soit premier.

Théorème trivial

N est premier

$\Updownarrow$

Il existe un entier g d'ordre $N-1$ modulo N

traduction :

N est premier

$\Updownarrow$

$$\begin{cases} g^{N-1} \equiv 1 & \\ g^{(N-1)/q} \not\equiv 1 & \forall \text{ diviseur premier } q \text{ de } N-1 \end{cases}$$

Et si on ne sait pas factoriser $N-1$?

On utilise une courbe elliptique E sur le corps (?) $\mathbb{F}_N$

Théorème. Soient $(\sqrt[4]{N}+1)^2 < s \mid m$ deux entiers et $P \in E$. Si

$$\begin{cases} mP = 0 \\ \text{pgcd}(Z\{(m/q)P\}, N) = 1 \quad \text{pour tout } q \text{ facteur premier de } s \end{cases}$$

Alors N est premier.

Nécessite une factorisation (partielle) de l'ordre de E

Encore plus rapides :

Tests polynomiaux de primalité

Rabin-Miller : en $\mathcal{O}(\ln^3 N)$

Vérifier

$$a^q \equiv 1 \quad \text{ou} \quad \exists i \ (0 \leqslant i < k) \text{ tq } a^{2^i q} \equiv -1 \pmod{p}.$$

avec $p - 1 = 2^k q$ avec q impair et $\text{pgcd}(a, p) = 1$.

Lucas : en $\mathcal{O}(\ln^3 N)$

Rapides : 1 ou 2 secondes pour 20 tests RM en 1024 bits

Probabilité de fausse alarme non nulle

Résolu en pratique

(à peu près)

En est-il autant en théorie ?

La primalité est de classe NP (Pratt '75)

preuve vérifiée en $\mathcal{O}(\ln^5 N)$

$$p = 162259276829213363391578010288127$$

$$p - 1 = 2 \times 3 \times 107 \times 6361 \times 69431 \times q_1 \times q_2$$

$$q_1 = 20394401 \qquad q_2 = 28059810762433$$

g d'ordre $p-1$ modulo p

$$q_1 - 1 = 2^5 \times 5^2 \times 13 \times 37 \times 53$$

$$q_2 - 1 = 2^6 \times 3 \times 41 \times 53 \times q_3$$

$$q_3 = 67254877$$

$$q_3 - 1 = 2^2 \times 3^2 \times 13 \times 131 \times 1097$$

Coût de la vérification :

$$C(p) = C(q_1) + \cdots + C(q_k) + \mathcal{O}(\ln^4 p) = \mathcal{O}(\ln^5 p).$$

Si ERH est vraie

La primalité est de classe P (Miller '75)

Tout N composé admet un témoin $\leqslant c \ln^2 N$.

En fait, $c = 2$ convient (Bach'90).

Algorithme en $\mathcal{O}(\ln^5 N)$

La primalité est de classe RP (Adleman/Huang '92)

Utilisation de courbes de genre 2

Théorème AKS

Soit $N \in \mathbb{N}^*$. Soient r et q deux premiers impair avec $q \mid r-1$ et

$$N^{(r-1)/q} \not\equiv 0, 1 \pmod{r}. \tag{1}$$

Soit $s \in \mathbb{N}^*$ tel que

$$C_{s+q-1}^{s} \geqslant N^{2\lfloor\sqrt{r}\rfloor} \tag{2}$$

et tel que N n'ait pas de diviseur dans l'intervalle $[2, s]$. Si l'identité

$$(X-a)^N \equiv X^N - a \pmod{X^r - 1, N} \tag{3}$$

est vérifiée pour tout entier a contenu dans $[1, s]$, alors N est la puissance d'un nombre premier.

Démonstration

Il existe un diviseur premier p de N tel que

$$p^{(r-1)/q} \not\equiv 0, 1 \pmod{r}.$$

Soit d l'ordre de p modulo r. D'après l'équation précédente, c'est un multiple de q, donc $d \geqslant q$. Le polynôme cyclotomique $X^{r-1} + \cdots + X + 1$ se factorise sur $\mathbb{F}_p$ en produit d'irréductibles de degré d. Soit h l'un d'entre eux et désignons par K une extension du corps $\mathbb{F}_p$ définie par le polynôme h.

Soit G le sous-groupe (cyclique) de K^* engendré par les $X - a$ pour $1 \leqslant a \leqslant s$. Comme les $X - a$, pour $1 \leqslant a \leqslant s$, sont des irréductibles distincts dans $\mathbb{F}_p[X]$ et comme $\deg h \geqslant q$, les produits $(X-1)^{e_1} \cdots (X-s)^{e_s}$ avec $e_1 + \cdots + e_s < q$ sont tous distincts modulo h. Donc l'ordre de G est au moins $C_{s+q-1}^{s} \geqslant N^{2\lfloor\sqrt{r}\rfloor}$.

Considérons dans $\mathbb{F}_p[X]$ un polynôme g qui, modulo h, engendre G. Par hypothèse, pour $1 \leqslant a \leqslant s$, on a l'identité $(X-a)^N \equiv X^N - a$ modulo

$(X^r - 1, p)$. On a aussi $(X - a)^p \equiv X^p - a$ modulo $(X^r - 1, p)$. Donc, pour tout couple (i, j) d'entiers on a, pour $1 \leqslant a \leqslant s$,

$$(X - a)^{N^i p^j} \equiv (X^{N^i p^j} - a) \pmod{X^r - 1, p}$$

et donc

$$g(X)^{N^i p^j} \equiv g(X^{N^i p^j}) \pmod{X^r - 1, p}.$$

Parmi les couples (i, j) tels que $0 \leqslant i, j \leqslant \sqrt{r}$, il y en a deux tels que $N^{i_1} p^{j_1} \equiv N^{i_2} p^{j_2}$ modulo r (car il y a plus de r tels couples au total). On a alors

$$g(X^{N^{i_1} p^{j_1}}) \equiv g(X^{N^{i_2} p^{j_2}}) \pmod{h}$$

et donc

$$g(X)^{N^{i_1} p^{j_1}} \equiv g(X)^{N^{i_2} p^{j_2}} \pmod{h}.$$

Cela implique $N^{i_1} p^{j_1} \equiv N^{i_2} p^{j_2}$ modulo l'ordre de G.

Mais $0 \leqslant N^{i_1} p^{j_1}, N^{i_2} p^{j_2} \leqslant N^{2\lfloor\sqrt{r}\rfloor}$ donc $N^{i_1} p^{j_1} = N^{i_2} p^{j_2}$. Comme les couples (i_1, j_1) et (i_2, j_2) sont différents. Cela implique $N = p^k$. □

Coûts

Taille des éléments de $\mathbb{Z}[X]/(X^r - 1, N)$

$r \log_2 N$

Tests de la condition principale

$\mathcal{O}(sr^2 \ln^3 N)$ sans FFT

$\mathcal{O}'(sr \ln^2 N)$ avec FFT

Fouvry : r en $\mathcal{O}(\ln^6 N)$, s en $\mathcal{O}(\ln^4 N)$

$\mathcal{O}(\ln^{19} N)$ sans FFT

$\mathcal{O}'(\ln^{12} N)$ avec FFT

Choix des paramètres

Les conditions

$$q \geqslant 4\left\lceil \sqrt{r}\log_2 N \right\rceil \quad \text{et} \quad s = 2\left\lceil \sqrt{r}\log_2 N \right\rceil \tag{4}$$

impliquent la condition

$$C_{s+q-1}^{s} \geqslant N^{2\lfloor\sqrt{r}\rfloor} \tag{2}$$

Algorithme AKS

Entrée : un entier $N > 1$.
Sortie : la réponse à la question "N est-il premier ?".

Si N est de la forme a^b avec $b \geqslant 2$ **alors** répondre "non".
Pour $r = 3$ initialement et incrémenté par **pas** de 2 **répéter**
    Si $\mathrm{pgcd}(r, N) > 1$ **alors** répondre "non".
    Si r n'est pas premier **alors** itérer.
    $q :=$ le plus grand facteur premier de $r - 1$.
    Si $q < 4\sqrt{r}\log_2 N$ **alors** itérer.
    Si $N^{(r-1)/q} \equiv 1$ modulo r **alors** itérer.
    Sortir de la boucle.
Pour a de 1 à $\lceil 2\sqrt{r}\log_2 N \rceil$ **répéter**
    Si $a \mid N$ et $a \neq 1$ **alors** répondre "non".
    Si $(X - a)^N \not\equiv X^N - a$ modulo $(X^r - 1, N)$ **alors** répondre "non".
Répondre "oui".

Enfin résolu en théorie

Coût en $\mathcal{O}'(\ln^{12} N)$ avec FFT

Coût en $\mathcal{O}'(\ln^{19} N)$ sans FFT

La primalité est de classe P

Retombées sur la pratique ?

Choix des paramètres

Les conditions

$$q \geqslant 4\lceil \sqrt{r} \log_2 N \rceil \quad \text{et} \quad s = 2\lceil \sqrt{r} \log_2 N \rceil \tag{5}$$

impliquent la condition

$$C^s_{s+q-1} \geqslant N^{2\lfloor \sqrt{r} \rfloor} \tag{2}$$

Mais aussi (puisque $r \geqslant 2q + 1$) :

$$r \geqslant 64 \log_2^2 N.$$

En particulier, la taille $(r \log_2 N)$ des éléments de l'anneau est au moins

$$2^{33} \text{ bits} = 1 \text{ Goctet} \quad \text{pour } N \simeq 2^{512}.$$

Améliorer le coût

Conjecture : r, s en $\mathcal{O}(\ln^2 N)$ et $q = (r-1)/2$

Coût en $\mathcal{O}(\ln^9)$ sans FFT

Coût en $\mathcal{O}'(\ln^6)$ avec FFT

Le degré reste(ra ?) assez élevé

Le facteur constant aussi (taille des données)

Conclusion

Un résultat théorique **majeur**

Un algorithme simple, une démonstration élégante

Intérêt pratique peu probable

Pas à l'abri d'éventuelles améliorations...

(Autres identités polynomiales ?)