Un algorithme déterministe polynomial pour la primalité

Bien que prouvée dès 1976 dans [3] sous l'hypothèse de Riemann étendue (ERH), l'appartenance du problème de la primalité à la classe $\mathcal{P}$ est restée incomplètement résolue jusqu'en 2002. A cette date, les auteurs de [1] répondent positivement à la question à l'aide d'un algorithme assez simple. Cet algorithme est basé sur le résultat suivant.

Le théorème principal

0.1. — Théorème. *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

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

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

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

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

0.2. — Lemme. *Les conditions*

$$q \geqslant 4\lceil\sqrt{r}\log_2 N\rceil \quad \textit{et} \quad s = 2\lceil\sqrt{r}\log_2 N\rceil \tag{3}$$

impliquent la condition (2).

Démonstration — Si les conditions (3) sont satisfaites alors

$$C^s_{s+q-1} = \frac{(s+q-1)\cdots(q+1)q}{s\cdots 2\cdot 1} \geqslant \left(\frac{q}{s}\right)^s \geqslant 2^s \geqslant 2^{2\sqrt{r}\log_2(N)} = N^{2\sqrt{r}} \geqslant N^{2\lfloor\sqrt{r}\rfloor}.$$

Et voilà. □

Un peu de combinatoire

0.3. — Lemme. *Soient $s, q \in \mathbb{N}$. Le nombre de s-uplets d'entiers $(e_1, \ldots, e_s) \in \mathbb{N}^s$ tels que $e_1 + \cdots + e_s \leqslant q$ est C^s_{s+q}. C'est aussi le nombre de $(s+1)$-uplets $(e_0, \ldots, e_s) \in \mathbb{N}^{s+1}$ tels que $e_0 + \cdots + e_{s-1} = q$.*

Démonstration — Il est clair que les deux nombres annoncés sont égaux. Notons-les $A_{s,q}$. On voit que $A_{0,q} = 1 = C^0_q$ pour tout q. L'identité classique

$$C^k_n = \sum_{i=k-1}^{n-1} C^{k-1}_i \qquad \text{pour } n, k \in \mathbb{N}$$

donne ici

$$C^s_{s+q} = \sum_{i=s-1}^{s+q-1} C^{s-1}_i = \sum_{i=0}^{q} C^{s-1}_{s-1+i}$$

Si l'on suppose la propriété vraie pour $s-1$, on obtient $C^s_{s+q} = \sum_{i=0}^q A_{s-1,i}$. Mais il est aussi clair que

$$\sum_{i=0}^{q} A_{s-1,i} = \sum_{i=0}^{q} \#\{s\text{-uplets de somme } i\} = \#\{s\text{-uplets de somme} \leqslant q\} = A^q_s.$$

On obtient donc le résultat par récurrence sur s. □

Démonstration du théorème 0.1

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 (voir par exemple le théorème 13.2 dans [2]). 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 $C^s_{s+q-1} \geqslant N^{2\lfloor\sqrt{r}\rfloor}$ d'après le lemme 0.3.

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 $N = p$. □

L'algorithme

D'après le théorème 0.1 dans le cas particulier du lemme 0.2, l'algorithme ci-dessous fournit une réponse exacte au problème de la primalité.

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

Si N est de la forme a^b avec $b \geqslant 2$ répondre "non".
Pour $r = 3$ initialement et incrémenté par pas de 2 répéter
    Si $\text{pgcd}(r, N) > 1$ 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.
– – Ici, r est un premier vérifiant (1) et $s = 2\lceil\sqrt{r}\log_2 N\rceil$ vérifie (2).
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".

Estimation du coût

Le test critique (en fin d'algorithme) fait intervenir des exponentiations dans l'anneau $\mathbb{Z}[X]/(X^r-1,N)$ où la représentation de chaque élément est de taille $r\log_2 N$ bits. Un multiplication dans cet anneau coûte $\mathcal{O}'(r\ln N)$ opérations binaires si l'on utilise la transformée de Fourier rapide (la notation $\mathcal{O}'(f)$ signifie ici $\mathcal{O}(f^{1+\varepsilon})$). Le test critique coûte alors $\mathcal{O}'(r\ln^2 N)$ opérations et la dernière boucle $\mathcal{O}'(r^{3/2}\ln^3 N)$ opérations.

Un théorème de Fouvry permet d'obtenir une borne en $\mathcal{O}(\ln^6 N)$ sur le nombre premier r fourni par la première boucle. Cela donne un coût en $\mathcal{O}'(\ln^{12} N)$ opérations pour la dernière boucle. Le reste de l'algorithme est de coût inférieur (même en utilisant des méthodes naïves pour la primalité de r et la factorisation de $r-1$). Cela montre un coût total polynomial en $\mathcal{O}'(\ln^{12} N)$ pour la primalité de N. Bien que polynomial, ce coût est trop élevé pour une application pratique. Mais ces travaux ne sont pas à l'abri d'éventuelles améliorations...

Bibliographie

[1] M. Agrawal, N. Kayal, N. Saxena : *PRIMES is in P.* preprint, August 2002.

[2] K. Ireland, M. Rosen : *A Classical Introduction to Modern Number Theory.* Springer-Verlag, New York, 2nd edition 1990.

[3] G.L. Miller : *Riemann's Hypothesis and tests for primality.* Journal of Computer and System Sciences, 13 (1976), 300–317.