LES NOMBRES PREMIERS

par

Pierre Colmez

Un *nombre premier* est un nombre entier supérieur ou égal à 2 qui n'est divisible que par 1 et par lui-même. Jusqu'à 100, les nombres premiers sont 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 et 97. L'importance de cette notion vient de ce que tout nombre entier strictement positif peut s'écrire comme un produit de nombres premiers et cette écriture est unique à permutation près des facteurs (par convention, 1 est le produit de 0 nombres premiers), résultat connu sous le nom de *théorème fondamental de l'arithmétique*.

Chaque nombre premier p donne naissance à un nouveau monde (le monde *p-adique*), parallèle au monde réel, et beaucoup d'objets mathématiques ont des composantes réelle et p-adique, ce qui donne plusieurs voies d'approche pour les étudier. Ce principe a des applications à des questions variées, notamment en théorie des nombres.

Un ensemble infini— Les grecs savaient déjà que *l'ensemble des nombres premiers est infini* : si on dispose de k nombres premiers

distincts $p_1, \dots, p_k$, on en construit un $(k+1)$-ième en prenant n'importe quel diviseur premier de $p_1 \cdots p_k + 1$ (produit des p_i augmenté de 1). La répartition des nombres premiers n'a cessé depuis de fasciner les mathématiciens et a joué un rôle moteur dans le développement de plusieurs branches des mathématiques, mais on ne sait toujours pas répondre à certaines questions anciennes comme :

— Existe-t-il une infinité de nombres premiers p tels que $p+2$ soit premier (problème des *nombres premiers jumeaux*) ?

— Existe-t-il une infinité de nombres premiers de la forme n^2+1 ?

— Y a-t-il toujours un nombre premier entre n^2 et $(n+1)^2$?

— Existe-t-il une infinité de nombres premiers p tels que $2^{p-1}-1$ soit (resp. ne soit pas) divisible par p^2 ?

— Existe-t-il une infinité de nombres premiers de la forme 2^n+1 (*premiers de Fermat*) ou 2^n-1 (*premiers de Mersenne*) ?

Des considérations probabilistes couplées avec le *théorème des nombres premiers* dont il sera question plus loin permettent de se faire une idée assez précise de ce à quoi on peut s'attendre. Par exemple, on s'attend à ce qu'il y ait une infinité de premiers de Mersenne, ce que l'expérience semble confirmer puisqu'on en trouve régulièrement : le plus grand connu[(1)] est $2^{43\,112\,609}-1$, découvert en août 2008 ; il a plus de 10^7 chiffres en écriture décimale et c'est aussi le plus grand nombre premier connu à ce jour (juin 2012).

Les nombres premiers ont trouvé une utilisation industrielle assez récemment : les techniques modernes de cryptographie ou de systèmes de sécurité à clef publique comme le système RSA (1977) en font une grande consommation. De nombreux algorithmes ont été inventés pour décider si un grand nombre est premier ou pas (et

[(1)] Détrôné en janvier 2013 par $2^{57\,885\,161}-1$.

pour factoriser effectivement des grands nombres, ce qui est nettement plus délicat). On pouvait décider de la primalité de nombres de 200 chiffres en 1980 ; en 2010 on en était à 26000 chiffres. Les recherches portant sur ces questions intéressent au plus haut point les services secrets des différents pays, et on peut penser que certains algorithmes performants sont soigneusement tenus secrets.

Une formule pour les nombres premiers ?— Beaucoup de gens ont cherché, sans succès, des formules simples fournissant des nombres premiers. Par exemple Fermat a affirmé que $F_n = 2^{2^n} + 1$ est premier pour tout entier n ce qu'il a effectivement vérifié pour $n = 0, 1, 2, 3, 4$, mais Euler a montré que F_5 est divisible par 641 et on ne connaît pas d'autre premier de Fermat.

Un résultat de logique mathématique (Matiyasevich, 1970) implique l'existence de polynômes en plusieurs variables $x_1, \ldots, x_k$, à coefficients entiers, énumérant l'ensemble des nombres premiers au sens que $n > 0$ est premier si et seulement si il existe $x_1, \ldots, x_k$, entiers ≥ 0, tels que $n = P(x_1, \ldots, x_k)$. Jones, Sato, Wada et Wiens (1976) ont construit explicitement un tel polynôme (en 26 variables). Ce polynôme n'est d'aucune utilité pour fabriquer des nombres premiers car il est très rare que $P(x_1, \ldots, x_{26}) > 0$.

Le crible d'Eratosthène.— Si $n = pq$, alors p ou q est $\leq \sqrt{n}$. Il s'ensuit que pour prouver qu'un nombre est premier, il suffit de vérifier qu'il n'est divisible par aucun nombre $\leq \sqrt{n}$, ce qui fournit un algorithme (naïf) permettant de décider si un petit nombre est premier ou pas. On peut améliorer cet algorithme en ne testant que la divisibilité par les nombres premiers $\leq \sqrt{n}$.

Le crible d'Eratosthène (antiquité) fournit, en partant de ce principe, une méthode permettant de faire la liste des nombres premiers : on écrit les nombres de 2 à n ; à chaque étape on prend le

plus petit nombre ni entouré ni barré que l'on entoure et on barre tous ses multiples (le processus commence avec 2) ; on s'arrête dès que le plus petit nombre non barré est $> \sqrt{n}$ et on entoure tous les nombres non barrés qui restent ; les nombres premiers compris entre 2 et n sont alors tous les nombres entourés.

Par exemple, si $n = 100$, la première étape entoure 2 et barre tous les nombres autres que 2 qui se terminent par 0, 2, 4, 6 ou 8 ; la seconde étape entoure 3 et barre 9, 15, 21, 27, 33, 39, 45, 51, 57, 63, 69, 75, 81, 87, 93 et 99 ; la troisième entoure 5 et barre 25, 35, 55, 65, 85 et 95 ; la quatrième entoure 7 et barre 49, 77 et 91, et comme le premier nombre non barré, à savoir 11, est $> \sqrt{100} = 10$, on entoure les nombres non barrés et obtient la liste des nombres premiers ≤ 100 en énumérant les nombres entourés.

Le théorème des nombres premiers.— En l'absence d'une formule explicite « simple » donnant le n-ième nombre premier, on peut essayer de donner une valeur approchée du n-ième nombre premier p_n ou, de manière équivalente, du nombre $\pi(x)$ de nombres premiers $\leq x$. Le résultat, connu sous le nom de *théorème des nombres premiers*, est que[(2)]

$$\pi(x) \sim \tfrac{x}{\log x} \quad \text{et} \quad p_n \sim n \log n.$$

De manière imagée, un nombre entier n pris au hasard a une probabilité de $\frac{1}{\log n}$ d'être premier. Ce résultat, démontré en 1896 indépendamment par Hadamard et de la Vallée Poussin, a une longue histoire :

Euler (1737) a établi que $\sum_{p \leq x} \frac{1}{p} \sim \log \log x$, et donc obtenu une démonstration de l'existence d'une infinité de nombres premiers qui va plus loin que celle des grecs : elle suggère que la densité des

[(2)]La notation $f(x) \sim g(x)$ signifie que $\frac{f(x)}{g(x)}$ tend vers 1 quand x tend vers $+\infty$.

nombres premiers autour de x est de l'ordre de $\frac{1}{\log x}$, et donc que $\pi(x) \sim \mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$. (La fonction Li est *le logarithme intégral*; on a $\mathrm{Li}(x) \sim \frac{x}{\log x}$, mais $\mathrm{Li}(x)$ est une meilleure approximation de $\pi(x)$ que $\frac{x}{\log x}$.) C'est aussi la conclusion à laquelle ont abouti Legendre et Gauss au début du dix-neuvième siècle, en examinant des tables de nombres premiers.

Le résultat d'Euler repose sur l'étude, au voisinage de $s = 1$, de la fonction ζ de Riemann, définie par $\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}$ si $s > 1$. Le théorème fondamental de l'arithmétique permet de factoriser $\zeta(s)$ sous la forme

$$\zeta(s) = \prod_p \left(1 + \tfrac{1}{p^s} + \tfrac{1}{p^{2s}} + \cdots\right) = \prod_p \tfrac{1}{1-p^{-s}},$$

(le produit porte sur les nombres premiers) ce qui fait le lien entre cette fonction et les nombres premiers. L'étape suivante est due à Riemann (1858) qui a étendu le domaine de définition de ζ à tout le plan complexe, et prouvé que, sous *l'hypothèse de Riemann* selon laquelle ζ ne s'annule pas sur le demi-plan $\mathrm{Re}(s) > \frac{1}{2}$, l'on a[3] $\pi(x) = \mathrm{Li}(x) + O(x^{1/2}\log x)$, ce qui renforce grandement le théorème des nombres premiers.

L'hypothèse de Riemann n'est toujours pas démontrée malgré 150 ans d'efforts, mais Hadamard et de la Vallée Poussin ont réalisé qu'il suffisait de montrer que ζ ne s'annule pas sur le demi-plan $\mathrm{Re}(s) \geq 1$ (seule la droite $\mathrm{Re}(s) = 1$ pose problème) pour en déduire le résultat. De la Vallée Poussin a exhibé une région contenant ce demi-plan, sur laquelle ζ ne s'annule pas, ce qui lui a permis de

[3] La notation $f = O(g)$ signifie qu'il existe $C > 0$ tel que $|f(x)| \leq Cg(x)$ pour tout x assez grand.

renforcer le théorème des nombres premiers sous la forme

$$\pi(x) = \mathrm{Li}(x) + O\big(x \exp(-\tfrac{1}{15}\sqrt{\log x})\big).$$

Ce résultat n'a pas franchement été amélioré depuis.

La première démonstration « élémentaire » (i.e. n'utilisant pas la variable complexe) du théorème des nombres premiers remonte à 1948 (Erdös et Selberg).

Le théorème de la progression arithmétique.— Si on utilise le crible d'Erathostène pour faire la liste des nombres premiers, on peut difficilement ne pas remarquer que le chiffre des unités des nombres premiers est 1, 3, 7 ou 9, et qu'il y en a peu près autant de chaque. On est donc naturellement amené à penser que les nombres premiers s'équirépartissent dans les progressions arithmétiques de la forme $Dn+a$ dans lesquelles il peut y en avoir plusieurs (i.e. a et D n'ont pas de facteur premier en commun, ce que nous supposons dans ce qui suit) ; le nombre de telles progressions est $C_D^{-1}D$, où C_D est le produit des $(1-\frac{1}{p})^{-1}$, pour p premier divisant D (e.g. $C_{10} = \frac{5}{2}$). On note $\pi(D, a, x)$ le nombre de $n \leq x$ tels que $Dn+a$ soit premier, et la discussion précédente suggère que $\pi(D, a, x) \sim C_D \frac{x}{\log x}$.

Une première version de ce résultat a été obtenue par Dirichlet (1837) en adaptant la preuve d'Euler de l'existence d'une infinité de nombres premiers. Il a, pour ce faire, introduit une nouvelle classe de fonctions, les *fonctions L de Dirichlet*, qui jouent le rôle de la fonction ζ dans la preuve d'Euler. Une fonction L de Dirichlet de niveau D est une fonction de la forme $L(\chi, s) = \sum_{n\geq 1} \chi(n)n^{-s}$, où χ est un *caractère de Dirichet modulo* D, c'est-à-dire une fonction $\chi : \mathbf{N} \to \mathbf{C}^*$ vérifiant $\chi(n + D) = \chi(n)$ pour tout $n \in \mathbf{N}$, $\chi(nm) = \chi(n)\chi(m)$ pour tous n, m, et $\chi(n) = 0$ si n a un facteur premier commun avec D. Ces fonctions admettent une factorisation

$L(\chi, s) = \prod_p \frac{1}{1-\chi(p)p^{-s}}$ analogue à celle de la fonction ζ. En combinant les techniques de Dirichlet et les siennes, de la Vallée Poussin a renforcé le résultat de Dirichlet sous la forme :

$$\pi(D, a, x) = C_D \mathrm{Li}(x) + O\big(x \exp(-\alpha_D \sqrt{\log x})\big),$$

où $\alpha_D > 0$ dépend de D. On pourrait remplacer $x \exp(-\alpha_D \sqrt{\log x})$ par $x^{1/2} \log x$, si on savait que les fonctions L ne s'annulent pas dans le demi-plan $\mathrm{Re}(s) > \frac{1}{2}$, *hypothèse de Riemann généralisée* (GRH en abréviation anglaise) ; cela aurait des applications pratiques.

Nombres premiers de la forme $x^2 + ny^2$.— Fermat (1640) a montré qu'un nombre premier impair est une somme de deux carrés si et seulement si il est de la forme $4n+1$: par exemple $17 = 4{\cdot}4{+}1 = 4^2 + 1^2$ ou $97 = 4 \cdot 24 + 1 = 9^2 + 4^2$. Il y a donc une infinité de nombres premiers de la forme $x^2 + y^2$ d'après le théorème de la progression arithmétique.

La situation générale est plus compliquée : par exemple, p est de la forme $x^2 + 27y^2$ si et seulement si il est de la forme $3k + 1$ et il existe un entier a tel que p divise $a^3 - 2$ (résultat conjecturé par Euler (1750) et démontré par Gauss (1805)). Mais il reste vrai que l'ensemble des nombres premiers de la forme $x^2 + ny^2$ est infini, si n est un entier > 0. La démonstration utilise le théorème de Tchebotarev (1926) qui est une vaste généralisation[(4)] du théorème de la progression arithmétique et l'outil le plus puissant dont on dispose pour produire des nombres premiers.

[(4)] Via la théorie de Galois, le théorème de la progression arithmétique devient : les nombres premiers s'équirépartissent dans le groupe de Galois du polynôme $X^D - 1$ (ce groupe est égal à $(\mathbf{Z}/D\mathbf{Z})^*$). Le théorème de Tchebotarev dit que les nombres premiers s'équirépartissent dans le groupe de Galois de n'importe quel polynôme, énoncé qui demanderait à être précisé.

Polynômes et nombres premiers.— Soient $P_1, \cdots, P_k$ des éléments distincts de l'anneau $\mathbf{Z}[X]$ des polynômes à coefficients entiers. On s'intéresse àux entiers $n \geq 0$ tels que $P_1(n), \ldots, P_k(n)$ soient simultanément premiers (le problème des nombres premiers jumeaux correspond à $k = 2$, $P_1 = X$ et $P_2 = X + 2$, celui de la progression arithmétique à $k = 1$ et $P_1 = DX + a$). On note $\pi(P_1, \ldots, P_k, x)$ le nombre de tels n jusqu'à x.

Si $P_i(n)$ était pris au hasard, la probabilité qu'il soit premier serait $\frac{1}{\log P_i(n)} \sim \frac{1}{\deg P_i} \cdot \frac{1}{\log n}$. Comme les $P_i(n)$ ne sont pas complètement pris au hasard, il faut un petit peu modifier cette probabilité. Si p est premier, on note $N(p)$ le nombre de $a \in \{0, 1, \ldots, p-1\}$ tels que l'un des $P_i(a)$ soit divisible par p, et on pose $C_p = \big(1-\frac{1}{p}\big)^{-k}\big(1-\frac{N(p)}{p}\big)$ (c'est le quotient de la probabilité qu'aucun des $P_i(n)$ ne soit divisible par p par la probabilité qu'on obtiendrait si les $P_i(n)$ étaient des nombres pris au hasard). On note $C(P_1, \ldots, P_k)$ le produit des C_p (on a $C(P_1, \ldots, P_k) \neq 0$ sauf s'il existe p tel que, pour tout n, l'un des $P_i(n)$ est divisible par p). Alors Bateman et Horn (1962) ont conjecturé que :

$$\pi(P_1, \ldots, P_k, x) \sim \frac{C(P_1, \ldots, P_k)}{\deg P_1 \cdots \deg P_k} \cdot \frac{x}{(\log x)^k}.$$

Le seul cas où l'on sache démontrer la conjecture, même sous une forme faible, est celui où $k = 1$ et P est de degré 1 qui correspond au théorème de la progression arithmétique. Par exemple, on ne sait pas démontrer qu'il existe une infinité de nombres premiers jumeaux ou de nombres premiers de la forme $n^2 + 1$. On a quand même des résultats récents allant dans ce sens :

• Pour tout $\varepsilon > 0$, il existe des couples de nombres premiers $p < q$ vérifiant[5] $q - p < \varepsilon \log p$ (Goldston et Yildirim, 2005).

• Il existe une infinité de nombres premiers de la forme $n^2 + m^4$ (Friedlander et Iwaniec, 1998).

• Si P est un polynôme à coefficients entiers, il existe $r \geq 1$ et une infinité de n tels que $P(n)$ ait au plus r facteurs premiers (Bourgain, Gamburd et Sarnak, 2009). Pour $P(X) = X(X+2)$, on peut prendre $r = 3$ (Chen, 1975) ; le problème des nombres premiers jumeaux équivaut à $r = 2$. Pour $P = X^2 + 1$, on peut prendre $r = 2$ (Iwaniec, 1978).

La situation s'améliore si on rajoute une variable :

• Green et Tao (2004) ont prouvé l'existence de progressions arithmétiques de longueur arbitraire formées de nombres premiers : si $k \in \mathbf{N}$, il existe une infinité de $(n_1, n_2) \in \mathbf{N}^2$, avec $n_2 \geq 1$, tels que $n_1, n_1 + n_2, \ldots, n_1 + kn_2$ soient des nombres premiers, résultat que Green, Tao et Ziegler ont précisé en 2010 en montrant qu'il existe une constante $C > 0$, obtenue par la recette de Bateman et Horn ci-dessus, telle que le nombre de tels $(n_1, n_2) \in \mathbf{N}^2$, avec $n_1 \leq x$ et $n_2 \leq x$, est équivalent à $C \frac{x^2}{(\log x)^{k+1}}$.

• Tao et Ziegler (2006) ont démontré que si $P_1, \ldots, P_k \in \mathbf{Z}[X]$ vérifient la condition $P_1(0) = \cdots = P_k(0) = 0$, il existe une infinité de $(n_1, n_2) \in \mathbf{N}^2$, avec $n_2 \geq 1$, tels que $n_2 + P_1(n_1), \ldots, n_2 + P_k(n_1)$ soient des nombres premiers.

[5] Ce résultat a été amélioré de manière spectaculaire par Zhang en 2013 : il existe une constante C et une infinité de couples de nombres premiers $p < q$ vérifiant $q - p \leq C$. Zhang montre que l'on peut prendre $C = 7 \cdot 10^7$, mais il n'a pas cherché à optimiser la constante fournie par sa méthode. D'autres s'en sont chargés mais on n'est pas encore descendu à $C = 2$ et le problème des nombres premiers jumeaux n'est donc toujours pas résolu.

La conjecture de Goldbach.— Un autre problème célèbre est la *conjecture de Goldbach* (1742) selon laquelle *tout nombre pair* ≥ 2 *est somme d'au plus 2 nombres premiers et tout nombre impair* ≥ 3 *est somme d'au plus 3 nombres premiers.*

Vinogradov (1937) a montré que tout nombre impair assez grand est somme de 3 nombres premiers, mais la borne fournie par sa méthode reste, malgré des améliorations successives, trop grande pour permettre une vérification des cas manquants. Tao (2012) a prouvé que tout nombre impair ≥ 3 est somme d'au plus 5 nombres premiers [(6)].

On ne dispose pas de résultat analogue à celui de Vinogradov pour les sommes de 2 nombres premiers, mais Chen (1966) a prouvé que tout nombre pair assez grand est somme d'un nombre premier et d'un nombre ayant au plus deux facteurs premiers. Le même genre d'heuristique que précédemment suggère que le nombre de manières d'écrire un entier n pair sous la forme $p_1 + p_2$, avec p_1, p_2 premiers, devrait être de l'ordre de $C \prod_{p|n} \frac{p-1}{p-2} \frac{n}{(\log n)^2}$ (le produit porte sur les nombres premiers divisant n), avec $C = 2 \prod_{p \geq 3} \left(1 - \frac{1}{p}\right)^{-2} \left(1 - \frac{2}{p}\right)$ (Hardy-Littlewood, 1923).

Tests de primalité.— L'algorithme naïf est totalement impraticable pour décider si un nombre N de 30 chiffres est premier ou pas car le nombre d'opérations à faire est exponentiel en le nombre de chiffres (qui est de l'ordre de $\log N$). Comme on a besoin de nombres encore plus grands pour les applications aux transactions

[(6)] Helfgott a réussi, en 2013, à faire descendre la borne de Vinogradov à un niveau raisonnable (cela a demandé, entre autres, l'aide de Platt et 400 000 heures de calculs sur machine pour vérifier GRH suffisamment loin pour suffisamment de caractères de Dirichlet), et donc à prouver que *tout nombre impair* ≥ 3 *est somme d'au plus 3 nombres premiers.*

sécurisées, il faut trouver d'autres méthodes (si possible polynomiales en $\log N$, avec un degré du polynôme le plus petit possible). Remarquons tout de même que les nombres premiers sont relativement denses (si on prend un nombre de mille chiffres au hasard et qu'on s'assure qu'il n'est pas divisible par 2, 3 ou 5, alors il a plus d'une chance sur mille d'être premier), et donc que si on peut décider rapidement si un nombre est premier ou pas, on n'a pas de mal à en trouver explicitement.

L'existence d'un test de primalité aboutissant en temps polynomial en $\log N$ est restée en suspens jusqu'à ce qu'Agrawal, Kayal et Saxena en construisent un en 2002 (et démontrent qu'il est effectivement polynomial). Il s'agit d'une avancée théorique très importante, mais en pratique on utilise d'autres tests dont on ne sait pas prouver qu'ils sont polynomiaux sauf en admettant des conjectures classiques sur la répartition des nombres premiers comme GRH ou l'existence de $\frac{\sqrt{x}}{(\log x)^c}$ nombres premiers dans l'intervalle $[x, x+\sqrt{x}]$, où $c > 0$ ne dépend pas de x.

La plupart des calculs à faire pour décider qu'un nombre N est premier se font dans l'anneau $\mathbf{Z}/N\mathbf{Z}$ obtenu en rajoutant à $\mathbf{Z}$ la relation $N = 0$. On obtient de la sorte un anneau fini, de cardinal N, et l'addition et la multiplication dans $\mathbf{Z}/N\mathbf{Z}$ ne demandent pas beaucoup plus que $\log N$ opérations. Une propriété fondamentale des nombres premiers est que $\mathbf{Z}/N\mathbf{Z}$ *est un corps si et seulement si* N *est premier*, et que *le groupe* $(\mathbf{Z}/N\mathbf{Z})^*$ *des éléments inversibles de* $\mathbf{Z}/N\mathbf{Z}$ *est cyclique, de cardinal* $N-1$*, si et seulement si* N *est premier*. Ceci est à la base de beaucoup des tests qui suivent.

Un premier test de non-primalité est fourni par le petit théorème de Fermat (1640) : *si* p *est premier, alors* $a^p - a$ *est divisible par* p *pour tout entier* a. Il n'y a pas de réciproque au petit théorème de Fermat : il existe des entiers N dit *de Carmichael* tels que $a^N - a$

soit divisible par N pour tout a, et qui ne sont pas premiers (le plus petit est $561 = 3 \cdot 11 \cdot 17$). Le résultat le plus proche est le test de primalité de Lucas (1876) généralisé par Lehmer (1927) : *s'il existe* $a \in \{2, \dots, n-1\}$ *tel que* $a^{N-1} \equiv 1$ *mod* n *et* $a^{(N-1)/p} \not\equiv 1$ *mod* N *pour tout diviseur premier* p *de* $N-1$*, alors* N *est premier*. Prendre $a = 5$ suffit à prouver que $2^{1001}3^{1600}+1$ est premier (on dit que 5 est un *certificat de primalité* pour $2^{1001}3^{1600} + 1$ pour le test d'Atkin-Lehmer). Pour un entier N quelconque, il faut d'abord factoriser $N - 1$, ce qui est plus dur que de prouver que N est premier par d'autres méthodes.

La vérification de la primalité d'un nombre de Mersenne repose sur un autre test de Lucas-Lehmer : on pose $s_0 = 4$ et $s_i = s_{i-1}^2 - 2$ si $i \geq 1$; alors $M_n = 2^n - 1$ est premier si et seulement si n est premier et s_{n-2} est divisible par M_n. Ce test est particulièrement efficace, ce qui explique pourquoi les plus gros nombres premiers connus sont des nombres de Mersenne.

La primalité des nombres de Fermat se vérifie grâce au test de primalité de Pépin : $F_n = 2^{2^n} + 1$ est premier si et seulement si $3^{2^{n-1}} + 1$ est divisible par F_n (les nombres de Fermat sont énormes et on ne peut pas aller très loin).

Pour un entier quelconque, on dispose du test *probabiliste* de Rabin-Miller (1980), amélioration d'un test de Solovay-Strassen (1977) : soit $N = 2^s m + 1$ avec $s \geq 1$ et m impair. Alors N *est premier si et seulement si, pour tout* $a \in \{1, 2, \dots, N-1\}$*, ou bien* $a^m - 1$ *est divisible par* N *ou bien il existe* $r \in \{0, 1, \dots, s-1\}$ *tel que* $a^{2^r m} + 1$ *soit divisible par* N *; de plus, si* N *n'est pas premier, la proportion des* a *vérifiant la propriété est* $\leq 1/4$. Cela permet, en prenant k valeurs de a distinctes, d'affirmer que N n'est pas premier ou bien qu'il est premier avec une probabilité $\geq 1 - \frac{1}{4^k}$: c'est suffisant pour les applications industrielles, et si on est prêt à

admettre GRH, alors il suffit de tester tous les $a \leq 2(\log N)^2$ pour certifier que N est premier (Bach, 1990).

Tous les tests décrits ci-dessus utilisent le groupe $(\mathbf{Z}/N\mathbf{Z})^*$. Un des tests les plus employés, connu sous le nom de ECPP (Atkin-Morain, 1993), repose sur l'utilisation de groupes associés à des courbes elliptiques (d'équation $y^2 = x^3 + ax + b$, avec $a, b \in \mathbf{Z}/N\mathbf{Z}$) bien choisies. Il aboutit conjecturalement en temps polynomial et fournit en outre un certificat de primalité.

Bibliographie

H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, volume 138, Springer-Verlag, Berlin, 1993.

P. Colmez, *Éléments d'analyse et d'algèbre*, seconde édition augmentée, Éditions de l'École Polytechnique, Palaiseau 2011.

D. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication*, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1989.

W. Ellison, *Les nombres premiers*, En collaboration avec M. Mendès France, Publications de l'Institut de Mathématique de l'Université de Nancago, No. IX, Actualités Scientifiques et Industrielles, No. 1366. Hermann, Paris, 1975.

M. Hindry, *Arithmétique*, Calvage et Mounet, Paris, 2008.

F. Morain, La primalité en temps polynomial, Séminaire Bourbaki 2002-2003, in Astérisque, vol. 294, p. 205, Société Mathématique de France, Paris, 2004.

G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, 3-ième édition, Belin, Paris, 2008.

Pierre Colmez, C.N.R.S., Institut de mathématiques de Jussieu, Université Pierre et Marie Curie, 4 place Jussieu, 75005 Paris, France
E-mail : colmez@math.jussieu.fr