
LE PROBLÈME DE FERMAT

ET LA THÉORIE DES NOMBRES PREMIERS

LE THÉORÈME D'ADLEMAN, FOUVRY ET HEATH-BROWN

Michel BALAZARD

Chargé de recherches au CNRS

Université de Bordeaux 1

On a assez tôt divisé l'étude de l'équation de Fermat

$$x^p + y^p = z^p \quad (1)$$

où x , y et z sont des nombres entiers et p un nombre premier impair, en deux cas :

- le premier cas, où p ne divise aucun des nombres x , y , z ;
- le deuxième cas, où p divise le produit xyz .

On dit que le premier cas du théorème de Fermat est vrai pour l'exposant p si l'équation (1) entraîne que p divise xyz .

En 1837, deux siècles après l'assertion de Fermat, Dirichlet fondait la théorie analytique des nombres qui, après un siècle et demi de développement, allait donner l'un de plus beaux résultats sur l'équation de Fermat.

Théorème (Adleman, Fouvry et Heath-Brown, 1985)

Le premier cas du théorème de Fermat est vrai pour une infinité de nombres premiers p .

Dans cet article, nous allons donner quelques éléments d'approche de la démonstration de ce théorème. Pour commencer, il nous faut quelques notions sur la répartition des nombres premiers.

Nombres premiers et progressions arithmétiques

On sait depuis Euclide que la suite 2, 3, 5, 7, ... des nombres premiers est infinie. Autrement dit

$$\pi(x) \rightarrow +\infty \quad \text{quand} \quad x \rightarrow +\infty$$

où $\pi(x)$ désigne le nombre de nombres premiers inférieurs ou égaux à x .

Maintenant, qu'en est-il des nombres premiers appartenant à une progression arithmétique donnée :

$$a, a + b, a + 2b, \dots ?$$

Bien entendu, si le $\text{pgcd}(a, b)$ est supérieur à 1, cette suite comporte au plus un nombre premier. En revanche, si a et b sont premiers entre eux, elle en contient une infinité. Notons $\pi(x; b, a)$ le nombre de nombres premiers inférieurs ou égaux à x et congrus à a modulo b . On a donc

$$\pi(x, b, a) \rightarrow +\infty \quad \text{quand } x \rightarrow +\infty, \quad \text{si } (a, b) = 1$$

Ce résultat de 1837 est dû à Dirichlet. Dans sa démonstration il utilise pour la première fois les séries qui portent son nom, et crée une nouvelle branche de l'arithmétique : la théorie analytique des nombres.

En 1896, Hadamard et de la Vallée-Poussin démontrent indépendamment le théorème des nombres premiers

$$\pi(x) \sim \text{li}(x) \quad \text{quand } x \rightarrow +\infty \quad (2)$$

où $\text{li}(x)$ est la fonction "logarithme intégral" définie par

$$\text{li}(x) = \lim_{\varepsilon \rightarrow 0^+} \left\{ \int_0^{1-\varepsilon} \frac{dt}{\log t} + \int_{1+\varepsilon}^x \frac{dt}{\log t} \right\}$$

On a l'équivalence asymptotique $\text{li}(x) \sim \frac{x}{\log x}$ quand x tend vers $+\infty$, mais $\pi(x)/\text{li}(x)$ tend vers 1 beaucoup plus vite que $\pi(x) \log x/x$: c'est pourquoi nous avons écrit (2) sous cette forme.

Le théorème des nombres premiers est fondamental. Il permet notamment d'évaluer des sommes portant sur les nombres premiers. Ainsi, on a pour une grande classe de fonctions f :

$$\sum_{y < p \leq x} f(p) \sim \int_y^x f(t) \frac{dt}{\log t} \quad \text{quand } x \rightarrow +\infty \quad (3)$$

A la même époque, de la Vallée-Poussin met en évidence l'équirépartition des nombres premiers dans les $\varphi(b)$ progressions arithmétiques

$$\{n; n \equiv a \pmod{b}\}, \quad (a, b) = 1$$

en démontrant

$$\pi(x; b, a) \sim \frac{\text{li}(x)}{\varphi(b)} \quad \text{quand } x \rightarrow +\infty, \quad \text{si } (a, b) = 1 \quad (4)$$

Ici, $\varphi(b)$ désigne l'indicateur d'Euler de b . On a

$$\varphi(b) = b \prod_{p|b} \left(1 - \frac{1}{p}\right).$$

Au vingtième siècle, la recherche sur les nombres premiers a porté essentiellement sur cette dernière équivalence asymptotique et notamment sur les difficiles problèmes d'uniformité qu'elle pose. Contentons-nous de citer deux des principaux résultats de la théorie.

Théorème (Brun-Titchmarsh)

Pour tous nombres entiers a, b et tout x tel que $x > b \geq 1, (a, b) = 1$, on a

$$\pi(x, b, a) < 2 \frac{x}{\varphi(b) \log\left(\frac{x}{b}\right)}$$

Théorème (Bombieri-Vinogradov)

Pour tout $\varepsilon > 0$, tout $A > 0$ on a

$$\sum_{b \leq x^{\frac{1}{2}-\varepsilon}} \max_{\substack{a \\ (a,b)=1}} \left| \pi(x; b, a) - \frac{li(x)}{\varphi(b)} \right| \ll_{A,\varepsilon} x(\log x)^{-A}$$

où la notation $\ll_{A,\varepsilon}$ signifie $\leq C(A,\varepsilon)$, $C(A,\varepsilon)$ étant un nombre positif ne dépendant que de A et de ε .

Ce dernier théorème nous dit que la différence entre les deux termes de (4) est majorée "en moyenne" pour $b \leq x^{\frac{1}{2}-\varepsilon}$ par $C(A,\varepsilon)x^{\frac{1}{2}+\varepsilon}(\log x)^{-A}$. Cette différence est donc petite en moyenne. On conjecture qu'elle est en fait petite tout le temps : ce serait une conséquence de l'hypothèse de Riemann généralisée.

Quant au théorème de Brun-Titchmarsh, on peut le réécrire

$$\pi(x; b, a) < C(r) \frac{x}{\varphi(b) \log x} \quad (5)$$

où $r = \frac{\log b}{\log x}$ et $C(r) = \frac{2}{1-r}$. Par conséquent, si r n'est pas trop proche de 1, le quotient des deux termes de (4) est borné.

L'hypothèse d'Adleman et Heath-Brown

En 1832, Sophie Germain donna le critère suivant :

Théorème 1 :

Si p et $2p + 1$ sont des nombres premiers, le premier cas du théorème de Fermat est vrai pour l'exposant p .

En cette époque reculée les préjugés sexistes étaient encore très vivaces dans le milieu mathématique et Sophie Germain avançait masquée sous le pseudonyme de monsieur Leblanc, notamment dans sa correspondance avec Gauss et Legendre, qui admiraient ses travaux.

Le théorème de Sophie Germain s'applique par exemple pour $p = 3, 5, 11, 23$. Malheureusement, nos connaissances sur la suite des nombres premiers sont toujours insuffisantes pour en déduire la validité du premier cas pour une infinité de nombres premiers p . La difficulté est essentiellement la même que dans le problème des nombres premiers jumeaux (existe-t-il une infinité

de nombres premiers p tels que $p + 2$ soit aussi premier?) Il s'agit là de questions extrêmement difficiles.

Cependant, la voie tracée par Sophie Germain a été suivie par de nombreux chercheurs et en 1984, Léonard Adleman et Roger Heath-Brown découvrirent indépendamment le :

Théorème 2 :

Il existe une constante absolue $A > 0$ telle que, pour tout nombre entier $k \geq 1$, non multiple de 3, on ait la propriété suivante; si p est un nombre premier tel que $2kp + 1$ est premier, alors le premier cas du théorème de Fermat est vrai pour l'exposant p , sauf éventuellement pour au plus Ck^2 nombres premiers p .

Les démonstrations des théorèmes 1 et 2 s'appuient sur des lois de réciprocité : quadratique dans le cas du théorème 1, et pour des puissances supérieures dans le cas du théorème 2. Nous n'en dirons pas plus dans cet exposé.

Adleman et Heath-Brown montrèrent alors que le premier cas du théorème de Fermat était vrai pour une infinité de nombres premiers p , à condition d'admettre une certaine hypothèse sur la répartition des nombres premiers dans les progressions arithmétique. Pour formuler cette hypothèse nous définissons $\pi^*(x; b, a)$ comme le nombre de premiers q inférieurs ou égaux à x , congrus à a modulo b et à 2 modulo 3.

Hypothèse :

Il existe un nombre réel θ , $\frac{2}{3} < \theta < 1$ tel que :

$$\sum_{x^\theta < p \leq x} \pi^*(x; p, 1) \gg \frac{x}{\log x} \quad \text{quand } x \rightarrow +\infty$$

Rappelons que cette dernière formulation signifie : il existe une constante absolue $B > 0$ et un nombre réel $x_0 > 0$ tels que

$$\sum_{x^\theta < p \leq x} \pi^*(x; p, 1) \geq B \frac{x}{\log x} \quad \text{pour } x \geq x_0$$

Dans ce qui suit nous allons expliquer comment le théorème sur le premier cas de l'équation de Fermat découle du théorème 2 et de l'hypothèse, puis nous donnerons quelques idées sur cette hypothèse et sa démonstration par Etienne Fouvry.

L'hypothèse et le théorème 2 entraînent le premier cas

Soit S l'ensemble des nombres premiers pour lesquels le premier cas du théorème de Fermat est vrai. Nous voulons montrer que la somme

$$\sum_{\substack{p \leq x \\ p \in S}} 1 \text{ tend vers l'infini avec } x$$

Pour cela, nous allons minorer cette somme par une autre, où le poids constant 1 est remplacé $\pi^*(x; p, 1)$, puis nous étudierons la somme obtenue à l'aide du théorème 2 et de l'hypothèse.

Soit θ et φ deux nombres réels, $0 < \theta < 1$, $0 < \varphi < 1$. Nous avons, si

$$x^{\theta\varphi} < p \leq x^\varphi, \quad 1 \geq \frac{x^{\theta\varphi}}{2(p-1)} \frac{(1-\varphi) \log x}{\log(x/p)}$$

Par conséquent

$$\sum_{\substack{p \leq x \\ p \in S}} 1 \geq \frac{1-\varphi}{2} x^{\theta\varphi-1} \log x \sum_{\substack{y^\theta < p \leq y \\ p \in S}} \frac{x}{(p-1) \log(x/p)}$$

où $y = x^\varphi$. Le théorème de Brun-Titchmarsh nous permet d'en déduire :

$$\begin{aligned} \sum_{\substack{p \leq x \\ p \in S}} 1 &\geq \frac{1-\varphi}{4} x^{\theta\varphi-1} \log x \sum_{\substack{y^\theta < p \leq y \\ p \in S}} \pi^*(x; p, 1) \geq \\ &\geq \frac{1-\varphi}{4} x^{\theta\varphi-1} \log x \sum_{\substack{y^\theta < p \leq y \\ p \in S}} \pi^*(y; p, 1) \end{aligned}$$

Maintenant

$$\sum_{\substack{y^\theta < p \leq y \\ p \in S}} \pi^*(y; p, 1) = \sum_{\substack{y^\theta < p \leq y}} \pi^*(y; p, 1) - \sum_{\substack{y^\theta < p \leq y \\ p \in S}} \pi^*(y; p, 1) \quad (6)$$

D'après l'hypothèse, on peut trouver $\theta > \frac{2}{3}$ tel que la première somme du second membre de (6) soit $\gg y/\log y$. Quant à la deuxième somme, elle se réécrit

$$\sum_{\substack{y^\theta < p \leq y \\ p \in S}} \sum_{\substack{k \\ 3 \nmid k \\ 2kp+1 \text{ premier} \\ 2kp+1 \leq y}} 1 \leq \sum_{\substack{k \leq x^{1-\theta} \\ 3 \nmid k}} \sum_{\substack{p \\ 2kp+1 \text{ premier} \\ p \in S}} 1 \ll \sum_{k \leq y^{1-\theta}} k^2 \ll y^{3-3\theta}$$

l'avant dernière inégalité découlant du théorème 2.

Comme $\theta > \frac{2}{3}$, cette somme est négligeable par rapport à $y/\log y$ et

$$\sum_{\substack{y^\theta < p \leq y \\ p \in S}} \pi^*(y; p, 1) \gg \frac{y}{\log y} \gg_\varphi \frac{x^\varphi}{\log x}$$

d'où

$$\sum_{\substack{y^\theta < p \leq y \\ p \in S}} 1 \gg_\varphi x^{\theta\varphi-1+\varphi}$$

Il suffit donc de choisir pour φ une constante supérieure à $\frac{1}{1+\theta}$ (et inférieure à 1) pour conclure.

Quelques idées sur la démonstration de l'hypothèse

Ici nous nous contenterons d'indiquer le contexte dans lequel s'insèrent les travaux de Fouvry, qui sont d'une extrême sophistication technique. Pour simplifier, nous traiterons de $\pi(x; p, 1)$ ou lieu de $\pi^*(x; p, 1)$; cela ne change presque rien.

On part de l'idée de Tchebycheff qui, vers 1850, avait utilisé l'identité

$$\log n = \sum_{p^\nu \parallel n} \log p^\nu$$

(où $p^\nu \parallel n$ signifie que n est divisible par p^ν mais pas par $p^{\nu+1}$) pour donner des majorations et des minoration de $\pi(x)$. Ici, nous écrivons

$$T(x) := \sum_{p \leq x} \log(p-1) = \sum_{p \leq x} \sum_{q^\nu \parallel p-1} \log(q^\nu) = \sum_{q^\nu \leq x} \pi(x; q^\nu, 1) \log(q^\nu)$$

Dans cette somme, la contribution des puissances q^ν avec $\nu \geq 2$ est $\ll \frac{x}{\log x}$, et d'autre part :

$$T(x) \sim \int_2^x \frac{\log(t-1)}{\log t} dt \sim x, \quad \text{d'après (3), donc}$$

$$\sum_{q \leq x} \pi(x; q, 1) \log q \sim x \tag{7}$$

Supposons maintenant qu'il existe θ, η et x_0 tels que $0 < \theta < 1$, $0 < \eta < 1$, $x_0 \geq 2$ et

$$\sum_{q \leq x^\theta} \pi(x; q, 1) \log q \leq (1-\eta)x \quad \text{pour } x \geq x_0 \tag{8}$$

On en déduit :

$$\sum_{x^\theta < q \leq x} \pi(x; q, 1) \geq \frac{1}{\log x} \sum_{x^\theta < q \leq x} \pi(x; q, 1) \log q \gg \frac{x}{\log x}$$

comme souhaité. Il nous reste à établir (8) pour une valeur de $\theta > \frac{2}{3}$.

On observe premièrement que le théorème de Bombieri-Vinogradov nous fournit un équivalent de

$$\sum_{q \leq x^{\frac{1}{2}-\epsilon}} \pi(x; q, 1) \log q$$

pour tout $\epsilon > 0$:

$$\begin{aligned} \sum_{q \leq x^{\frac{1}{2}-\epsilon}} \pi(x; q, 1) \log q &= li(x) \sum_{q \leq x^{\frac{1}{2}-\epsilon}} \frac{\log q}{\varphi(q)} + O\left(\frac{x}{(\log x)^A}\right) \\ &\sim \frac{x}{\log x} \int_{\frac{3}{2}}^{x^{\frac{1}{2}-\epsilon}} \frac{dt}{t-1} \sim \left(\frac{1}{2} - \epsilon\right) x \end{aligned}$$

où l'on a utilisé le théorème des nombres premiers sous la forme (3).

Tout revient donc à montrer que

$$\sum_{x^{\frac{1}{2}-\epsilon} < q \leq x^\theta} \pi(x; q, 1) \log q \leq \left(\frac{1}{2} + \epsilon - \eta\right) x \quad (9)$$

pour un certain $\theta > \frac{2}{3}$, $\eta > 0$ et $x \geq x_0$.

Voyons déjà ce que nous donne l'inégalité de Brun-Titchmarsh :

$$\begin{aligned} \sum_{x^{\frac{1}{2}-\epsilon} < q \leq x^\theta} \pi(x; q, 1) \log q &\leq 2 \sum_{x^{\frac{1}{2}-\epsilon} < q \leq x^\theta} \frac{\log q}{\log(x/q)} \frac{x}{\varphi(q)} \\ &\sim 2 \int_{x^{\frac{1}{2}-\epsilon}}^{x^\theta} \frac{\frac{x}{t}}{\log\left(\frac{x}{t}\right)} dt = 2x \int_{x^{1-\theta}}^{x^{\frac{1}{2}+\epsilon}} \frac{du}{u \log u} = 2x \log \left(\frac{\frac{1}{2} + \epsilon}{1 - \theta}\right) \end{aligned}$$

On voit donc que si $2 \log \left(\frac{1}{2(1-\theta)} \right) < \frac{1}{2}$, on peut choisir ε et η positif assez petits pour que (9) soit vérifiée. Ainsi, on a l'inégalité (8) pour tout $\theta < 0,6105996085\dots$

Pour aller plus loin, observons d'abord que le théorème de Brun-Titchmarsh s'écrit

$$\pi(x; q, 1) \leq \frac{x}{(q-1) \log x} C(r), \quad r = \frac{\log q}{\log x} \quad \text{et} \quad C(r) = \frac{2}{1-r} \quad (10)$$

La majoration qu'on en déduit est

$$\sum_{x^{\frac{1}{2}-\varepsilon} < q \leq x^\theta} \pi(x; q, 1) \log q < x \sum_{x^{\frac{1}{2}-\varepsilon} < q \leq x^\theta} \frac{1}{q-1} \frac{\log q}{\log x} C\left(\frac{\log q}{\log x}\right) \sim x \int_{\frac{1}{2}-\varepsilon}^{\theta} C(r) dr$$

On a bien sûr intérêt à trouver une fonction $C(r)$ aussi petite que possible. Cela étant, nous n'avons pas besoin de toute la force de la majoration individuelle (10) pour majorer la somme étudiée, dans laquelle on peut espérer un effet de moyenne. On a ainsi cherché à obtenir des majorations du type (10) valables non plus pour tout q mais pour "presque tout q ", et l'affaiblissement de cette exigence permet de prendre des fonctions $C(r)$ plus petites que $2/(1-r)$.

Nous en resterons là, et terminerons en citant Heath-Brown : "Pendant les 15 dernières années les améliorations successives du théorème de Brun-Titchmarsh ont donné lieu à beaucoup de versions différentes de l'estimation

$$\sum_{x^\theta < p \leq x} \pi^*(x; p, 1) \gg \frac{x}{\log x}$$

dont nous n'avons mentionné que quelques unes. En particulier, les valeurs 0.58, 0.611, 0.619, 0.625, 0.638, 0.6563, 0.6578, 0.6587 et 0.6687 ont paru dans la littérature ou dans des correspondances privées. La valeur finale, celle due à Fouvry, incorpore cinq nouvelles estimations de $C(r)$, pour différents domaines de valeurs de r . Il arrive souvent, dans certaines parties de la théorie analytique des nombres, que beaucoup d'énergie soit dépensée pour améliorer un exposant ou un autre, comme les chiffres ci-dessus le montrent. Pour qui est extérieur à la théorie, cela peut paraître un refuge pour de faibles chercheurs, comme si les améliorations pouvaient être obtenues simplement avec plus de soin, plus de pages de travail, et plus d'itérations d'une technique bien connue. Au contraire, il est un fait que chacune de ces améliorations, aussi petite soit-elle, nécessite une nouvelle idée. L'amélioration de Fouvry de 0.6587 à 0.6687 a requis cinq nouvelles idées pour obtenir une augmentation de 1.5%. Il faut dire, cependant, que cet exemple est le premier en date où ce processus d'amélioration par petits

pas a permis de passer un seuil critique (à savoir $\theta = 2/3$ dans ce cas) pour produire un résultat *qualitativement* nouveau.”

Bibliographie

L. M. Adleman, D. R. Heath-Brown, *The first case of Fermat's last theorem*. Invent. Math., **79** (1985) 409-416

E. Fouvry, *Théorème de Brun–Titchmarsh. Application au Théorème de Fermat*. Invent. Math., **79** (1985) 383-407

J. M. Deshouillers, *Théorème de Fermat : la contribution de Fouvry*. Séminaire Bourbaki (1984-85), 648

D. R. Heath-Brown, *The first case of Fermat's Last Theorem*. The Mathematical Intelligencer **7**, n°4 (1985) 40-55

