CORRIGÉ

Terminale · spécialité maths · CORRIGÉ

Trop d'entiers pour trop peu de nombres premiers

CHAPITRES

Dénombrement · Raisonnement par l'absurde · Nombres premiers

Le cœur de la preuve consiste à séparer, dans les exposants des facteurs premiers, ce qui peut entrer dans un carré et ce qui reste. L'hypothèse d'un nombre fini de nombres premiers transforme ensuite ces restes en un nombre fini de choix binaires. Le dénombrement obtenu devient incompatible avec l'existence de tous les entiers $1, \dots, N$ dès que N est choisi assez grand.

Résultat fourni dans le sujet. Tout entier $n \geq 2$ peut s'écrire comme un produit de nombres premiers. L'unicité de cette décomposition n'est pas nécessaire à la preuve présentée ici.

I Mettre de côté les carrés

1

(a) Pour 72, on écrit

$$72 = 2^3 \times 3^2 = 2\,(2^2 \times 3^2) = 2\,(2 \times 3)^2.$$

Ainsi, on peut prendre

$$a = 2, \qquad b = 6.$$

Le facteur $a = 2$ est bien un produit de nombres premiers distincts.

Pour 540,

$$540 = 2^2 \times 3^3 \times 5 = (3 \times 5)\,(2^2 \times 3^2) = 15\,(2 \times 3)^2.$$

On peut donc prendre

$$a = 15 = 3 \times 5, \qquad b = 6.$$

Là encore, les facteurs premiers de a sont distincts.

(b) Dans $72 = 2^3 \times 3^2$, l'exposant de 2 est impair et celui de 3 est pair. Le seul nombre premier qui reste dans a est donc 2. Dans $540 = 2^2 \times 3^3 \times 5^1$, les exposants impairs sont ceux de 3 et de 5 ; ce sont précisément les deux facteurs premiers présents dans $a = 3 \times 5$.

IDÉE Chaque paire de facteurs identiques peut être absorbée dans un carré. Pour un nombre premier donné, il ne peut donc rester hors du carré que zéro ou un exemplaire. C'est cette alternative binaire qui sera comptée dans la partie II.

2

Prenons une écriture de $n \geq 2$ sous la forme

$$n = q_1^{e_1} q_2^{e_2} \cdots q_s^{e_s},$$

où les q_i sont des nombres premiers distincts et les e_i sont des entiers strictement positifs.

Tout entier e_i est soit pair, soit impair. On peut donc écrire

$$e_i = 2k_i + \varepsilon_i, \qquad \varepsilon_i \in \{0, 1\},$$

avec $k_i \in \mathbb{N}$. Alors

$$q_i^{e_i} = q_i^{2k_i+\varepsilon_i} = q_i^{\varepsilon_i}\left(q_i^{k_i}\right)^2.$$

En multipliant ces égalités pour $i = 1, \dots, s$, on obtient

$$n = \left(q_1^{\varepsilon_1} \cdots q_s^{\varepsilon_s}\right)\left(q_1^{k_1} \cdots q_s^{k_s}\right)^2.$$

On pose donc

$$a = q_1^{\varepsilon_1} \cdots q_s^{\varepsilon_s}, \qquad b = q_1^{k_1} \cdots q_s^{k_s}.$$

Comme chaque ε_i vaut 0 ou 1, chaque nombre premier q_i apparaît au plus une fois dans a. Ainsi a est un produit de nombres premiers distincts et

$$\boxed{n = ab^2}.$$

Pour $n = 1$, il suffit de prendre

$$a = 1, \qquad b = 1,$$

ce qui donne bien $1 = 1 \times 1^2$.

IDÉE Nous avons utilisé la parité des exposants, mais pas l'unicité de la factorisation. Une seule écriture en produit de nombres premiers suffit pour construire un couple (a, b).

II Un choix binaire par nombre premier

On suppose maintenant, par l'absurde, que les seuls nombres premiers sont

$$p_1, p_2, \dots, p_r.$$

3

(a) Pour un mot binaire $(\varepsilon_1, \dots, \varepsilon_r)$, la quantité

$$A(\varepsilon_1, \dots, \varepsilon_r) = p_1^{\varepsilon_1} \cdots p_r^{\varepsilon_r}$$

contient exactement les nombres premiers p_i pour lesquels $\varepsilon_i = 1$.

Or, dans la construction de la partie I, a est un produit de nombres premiers distincts. Sous l'hypothèse que $p_1, \dots, p_r$ sont tous les nombres premiers, chacun des facteurs de a appartient donc à cette liste. Il existe ainsi au moins un mot binaire qui produit cette valeur de a.

Le mot $(0, \dots, 0)$ donne

$$A(0, \dots, 0) = p_1^0 \cdots p_r^0 = 1.$$

Il correspond au cas où aucun nombre premier ne reste hors du carré.

(b) Pour chacune des r positions du mot, deux choix sont possibles : 0 ou 1. Par le principe multiplicatif, le nombre de mots est donc

$$\underbrace{2 \times 2 \times \cdots \times 2}_{r \text{ facteurs}} = 2^r.$$

Chaque mot produit une valeur de A. Il peut éventuellement arriver que deux descriptions conduisent à la même valeur numérique ; nous n'avons pas besoin de l'exclure. Une telle coïncidence ne ferait que diminuer le nombre de valeurs distinctes obtenues.

Par conséquent,

$$\boxed{\text{il existe au plus } 2^r \text{ valeurs possibles pour } a.}$$

IDÉE C'est ici que le problème devient réellement combinatoire : le choix de a est codé par un mot binaire de longueur r, exactement comme une partie d'un ensemble à r éléments peut être codée par ses indicatrices 0 ou 1.

III Combien d'entiers peut-on alors fabriquer ?

On fixe $N \geq 1$ et on considère un entier n vérifiant $1 \leq n \leq N$. D'après la partie I, il possède une représentation $n = ab^2$ avec $a \geq 1$ et $b \geq 1$.

4

(a) Comme $a \geq 1$, on a

$$b^2 \leq ab^2 = n \leq N.$$

Les deux membres étant positifs, on peut prendre les racines carrées :

$$\boxed{b \leq \sqrt{N}}.$$

(b) b est un entier strictement positif. Les valeurs possibles de b sont donc parmi

$$1, 2, \ldots, \lfloor \sqrt{N} \rfloor.$$

Il y en a au plus

$$\boxed{\lfloor \sqrt{N} \rfloor}.$$

5

(a) Nous disposons de deux majorations indépendantes :

- au plus 2^r choix pour a ;
- au plus $\lfloor \sqrt{N} \rfloor$ choix pour b.

Par le principe multiplicatif, le nombre de couples possibles (a, b) est donc au plus

$$\boxed{2^r \lfloor \sqrt{N} \rfloor}.$$

(b) À chaque couple (a, b) correspond un seul entier, à savoir ab^2. En revanche, pour obtenir une majoration, nous n'avons pas besoin que deux couples différents donnent nécessairement deux entiers différents.

En effet, s'il y a des coïncidences, par exemple si deux couples différents produisaient la même valeur, ces deux couples ne fourniraient qu'un seul entier distinct au lieu de deux. Les coïncidences peuvent donc seulement faire diminuer le nombre d'entiers distincts représentés.

Ainsi,

$$\boxed{\#\{\text{entiers distincts représentés}\} \leq \#\{\text{couples } (a, b)\}.}$$

IDÉE Pour majorer un nombre d'objets, une représentation non injective ne pose aucun problème : plusieurs descriptions d'un même objet font seulement surestimer le nombre d'objets.

(c) Sous notre hypothèse, tous les entiers

$$1, 2, \ldots, N$$

doivent être représentés. Il y a exactement N entiers dans cette liste. D'après les questions précédentes, leur nombre ne peut pourtant pas dépasser le nombre de couples disponibles. On doit donc avoir

$$N \leq 2^r \lfloor \sqrt{N} \rfloor.$$

Comme

$$\lfloor \sqrt{N} \rfloor \leq \sqrt{N},$$

on obtient la condition nécessaire

$$\boxed{N \leq 2^r \lfloor \sqrt{N} \rfloor \leq 2^r \sqrt{N}.}$$

Cette inégalité devrait donc être vraie pour *tout* entier $N \geq 1$ si l'hypothèse « il n'existe que r nombres premiers » était correcte.

IV Choisir une borne qui fait craquer l'hypothèse

6

Nous voulons rendre impossible la condition obtenue à la question 5, c'est-à-dire chercher un entier N tel que

$$N > 2^r \sqrt{N}.$$

On cherche N sous la forme d'un carré parfait :

$$N = M^2, \qquad M \in \mathbb{N}^*.$$

Alors $\sqrt{N} = M$, donc l'inégalité souhaitée devient

$$M^2 > 2^r M.$$

Puisque $M > 0$, on peut diviser par M :

$$M > 2^r.$$

Il suffit donc de choisir un entier strictement supérieur à 2^r. Le choix le plus simple est

$$\boxed{M = 2^r + 1}.$$

On prend alors

$$\boxed{N = (2^r + 1)^2}.$$

Pour ce choix,

$$\sqrt{N} = 2^r + 1$$

et

$$2^r\sqrt{N} = 2^r(2^r + 1) < (2^r + 1)(2^r + 1) = N,$$

car $2^r < 2^r + 1$.

IDÉE Le carré parfait n'est pas une valeur magique. Il est choisi parce qu'il transforme la comparaison avec $\sqrt{N}$ en une simple comparaison entre M et 2^r.

V Trop d'entiers

7

Pour

$$N = (2^r + 1)^2,$$

on a exactement

$$\lfloor\sqrt{N}\rfloor = 2^r + 1.$$

Le nombre maximal de couples (a, b) disponibles est donc

$$2^r\lfloor\sqrt{N}\rfloor = 2^r(2^r + 1).$$

Mais

$$N = (2^r + 1)^2.$$

Comparons les deux nombres :

$$N - 2^r(2^r + 1) = (2^r + 1)^2 - 2^r(2^r + 1).$$

On factorise par $2^r + 1$:

$$N - 2^r(2^r + 1) = (2^r + 1)\big((2^r + 1) - 2^r\big) = 2^r + 1 > 0.$$

Ainsi,

$$\boxed{2^r\lfloor\sqrt{N}\rfloor < N.}$$

Nous arrivons à deux affirmations incompatibles :

- il existe N entiers distincts $1, 2, \dots, N$, et chacun doit posséder une représentation $n = ab^2$;
- il existe strictement moins de N couples (a, b) disponibles pour produire ces entiers.

Même en autorisant qu'un même entier possède plusieurs représentations, moins de N couples ne peuvent pas produire N valeurs distinctes.

La contradiction provient uniquement de l'hypothèse selon laquelle il n'existerait que les r nombres premiers $p_1, \dots, p_r$. Cette hypothèse est donc fausse.

L'ensemble des nombres premiers est infini.

IDÉE La stratégie est très différente d'une preuve qui construit un entier obligeant à faire apparaître un nouveau facteur premier. Ici, on ne cherche aucun nouveau premier : on montre qu'un nombre fini de premiers offrirait trop peu de configurations pour représenter tous les entiers.

Repère historique

En 1938, Paul Erdős publie un article consacré à un résultat plus fort que la seule infinité des nombres premiers : la divergence de la somme de leurs inverses. Son premier argument utilise explicitement l'idée centrale de ce DM : écrire un entier comme le produit d'un carré et d'un entier sans facteur carré, puis compter les possibilités.

Ce même comptage fournit déjà une information quantitative. Si $\pi(N)$ désigne le nombre de nombres premiers inférieurs ou égaux à N, on obtient $N \leq 2^{\pi(N)}\sqrt{N}$, donc

$$\pi(N) \geq \frac{\ln N}{2 \ln 2}.$$

La borne est très grossière, mais elle montre que l'argument force déjà le nombre de nombres premiers à croître avec N.

SOURCES

Paul Erdős, *Über die Reihe* $\sum 1/p$, *Mathematica (Zutphen) B* **7** (1938), p. 1-2. L'article original contient la décomposition « carré × partie sans facteur carré » et le comptage qui inspire directement le mécanisme du DM. Lien direct

Martin Aigner et Günter M. Ziegler, *Proofs from THE BOOK*, chapitre « Six proofs of the infinity of primes », 6e édition, Springer, 2018. L'ouvrage replace les arguments de dénombrement parmi plusieurs stratégies réellement différentes pour démontrer l'infinité des nombres premiers. Lien direct