CORRIGÉ

Terminale · maths expertes · CORRIGÉ

Prouver l'infinité des nombres premiers : forcer de nouveaux facteurs

CHAPITRES

Arithmétique · Divisibilité et PGCD · Congruences · Nombres premiers · Récurrence

I Sortir d'une liste finie

1

Supposons qu'il n'existe qu'un nombre fini de nombres premiers $p_1, p_2, \dots, p_r$ et posons

$$N = p_1 p_2 \cdots p_r + 1.$$

(a) On a clairement $N > 1$. Pour tout $i \in \{1, \dots, r\}$, l'entier p_i divise le produit $p_1 p_2 \cdots p_r$. Ainsi

$$N = p_1 p_2 \cdots p_r + 1 \equiv 1 \pmod{p_i}.$$

Le reste de la division de N par p_i est donc 1. En particulier, aucun des p_i ne divise N.

(b) Puisque $N > 1$, le résultat rappelé dans l'énoncé assure que N possède au moins un diviseur premier ; notons-le q. Si q appartenait à la liste $p_1, \dots, p_r$, on aurait $q = p_i$ pour un certain i, donc $p_i \mid N$, ce qui contredit la question précédente. Ainsi, q n'appartient pas à la liste.

(c) Or cette liste était supposée contenir tous les nombres premiers. L'existence du nombre premier q fournit donc une contradiction. Il existe ainsi une infinité de nombres premiers.

La preuve ne nécessite jamais que N soit lui-même premier. L'exemple donné dans l'énoncé le confirme :

$$30031 = 59 \times 509.$$

Ce qui importe est seulement l'existence d'au moins un diviseur premier de N absent de la liste initiale.

II Des nombres qui ne partagent pas leurs facteurs premiers

2

Par définition, $F_n = 2^{2^n} + 1$. On obtient successivement

$$F_0 = 3, \qquad F_1 = 5, \qquad F_2 = 17, \qquad F_3 = 257, \qquad F_4 = 65537.$$

Calculons ensuite les premiers produits :

$$P_1 = 3, \qquad P_2 = 15, \qquad P_3 = 255, \qquad P_4 = 65535.$$

Or

$$F_1 - 2 = 3, \quad F_2 - 2 = 15, \quad F_3 - 2 = 255, \quad F_4 - 2 = 65535.$$

Ces calculs conduisent à conjecturer que, pour tout $n \geq 1$,

$$\boxed{F_0F_1 \cdots F_{n-1} = F_n - 2.}$$

3

Démontrons cette identité par récurrence. Pour $n = 1$,

$$F_0 = 3 = 5 - 2 = F_1 - 2.$$

La propriété est donc vraie au rang 1.

Supposons maintenant que, pour un certain entier $n \geq 1$,

$$F_0F_1 \cdots F_{n-1} = F_n - 2.$$

Alors

$$F_0F_1 \cdots F_n = (F_n - 2)F_n.$$

À partir de $F_n = 2^{2^n} + 1$, on a $F_n - 2 = 2^{2^n} - 1$. Ainsi,

$$(F_n - 2)F_n = \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) = 2^{2 \cdot 2^n} - 1 = 2^{2^{n+1}} - 1 = F_{n+1} - 2.$$

Donc $F_0F_1 \cdots F_n = F_{n+1} - 2$. Par récurrence,

$$\boxed{F_0F_1 \cdots F_{n-1} = F_n - 2}$$

pour tout entier $n \geq 1$.

4

Soient $m, n \in \mathbb{N}$ avec $m < n$.

(a) D'après la question précédente,

$$F_n - 2 = F_0F_1 \cdots F_{n-1}.$$

Comme $m < n$, le nombre F_m figure parmi les facteurs du membre de droite. Ainsi,

$$\boxed{F_m \mid F_n - 2.}$$

(b) Posons $d = \text{PGCD}(F_m, F_n)$. Comme $d \mid F_m$ et $F_m \mid F_n - 2$, on a $d \mid F_n - 2$. De plus, $d \mid F_n$. Par conséquent,

$$d \mid F_n - (F_n - 2) = 2.$$

Or tous les nombres de Fermat sont impairs ; leur PGCD est donc impair. Comme d est positif et divise 2, on obtient nécessairement $d = 1$. Ainsi,

$$\boxed{\text{PGCD}(F_m, F_n) = 1.}$$

Les nombres de Fermat sont donc deux à deux premiers entre eux.

5

L'objectif est de faire apparaître un diviseur non trivial de F_5. De $641 = 5 \times 2^7 + 1$, on déduit

$$5 \times 2^7 \equiv -1 \pmod{641}.$$

En élevant cette congruence à la puissance 4,

$$5^4\, 2^{28} \equiv 1 \pmod{641}.$$

D'autre part, $641 = 5^4 + 2^4$ donne

$$5^4 \equiv -2^4 \pmod{641}.$$

En remplaçant 5^4 dans la congruence précédente,

$$(-2^4)2^{28} \equiv 1 \pmod{641},$$

donc $-2^{32} \equiv 1 \pmod{641}$, soit

$$2^{32} \equiv -1 \pmod{641}.$$

Or $F_5 = 2^{2^5} + 1 = 2^{32} + 1$. Par conséquent,

$$\boxed{641 \mid F_5.}$$

Comme $1 < 641 < F_5$, ce diviseur est non trivial : F_5 n'est donc pas premier. En fait,

$$F_5 = 4294967297 = 641 \times 6700417.$$

Ce calcul confirme que la suite des nombres de Fermat n'est pas une suite de nombres premiers ; seule leur coprimalité deux à deux sera utilisée dans la suite.

III Le mécanisme général

6

Soient $a_0, a_1, \ldots, a_n$ des entiers strictement supérieurs à 1, deux à deux premiers entre eux. Pour chaque $k \in \{0, \ldots, n\}$, l'entier $a_k > 1$ possède au moins un diviseur premier. Choisissons-en un, noté q_k. Alors $q_k \mid a_k$.

Montrons que les nombres $q_0, q_1, \ldots, q_n$ sont tous distincts. Supposons que, pour deux indices distincts i et j, on ait $q_i = q_j$. Ce nombre premier diviserait alors à la fois a_i et a_j, ce qui contredirait

$$\mathrm{PGCD}(a_i, a_j) = 1.$$

Ainsi $q_i \neq q_j$ dès que $i \neq j$. Nous avons donc obtenu $n+1$ nombres premiers distincts, chacun divisant $a_0 a_1 \cdots a_n$. Ce produit possède donc au moins $n+1$ diviseurs premiers distincts.

7

Considérons une suite infinie $(a_n)_{n \geq 0}$ d'entiers strictement supérieurs à 1, deux à deux premiers entre eux. Pour tout entier $n \geq 0$, les $n+1$ entiers

$$a_0, a_1, \ldots, a_n$$

satisfont les hypothèses de la question précédente. Il existe donc au moins $n+1$ nombres premiers distincts.

Comme cette affirmation est vraie pour tout entier n, le nombre de nombres premiers ne peut être fini. Il existe donc une infinité de nombres premiers.

Appliquons maintenant ce résultat aux nombres de Fermat. Pour tout $n \geq 0$, $F_n > 1$, et la question 4 a montré que les F_n sont deux à deux premiers entre eux. La suite $(F_n)_{n\geq 0}$ satisfait donc les hypothèses du résultat précédent. On en déduit à nouveau qu'il existe une infinité de nombres premiers.

Plus précisément, pour chaque entier n, les nombres $F_0, F_1, \ldots, F_n$ font nécessairement intervenir au moins $n+1$ facteurs premiers distincts.

Bilan

La preuve d'Euclide et celle fondée sur les nombres de Fermat ont donc un même ressort : construire des entiers dont les contraintes de divisibilité interdisent de réutiliser indéfiniment les mêmes facteurs premiers.

SOURCES

Euclide, *Éléments*, livre IX, proposition 20. La preuve distingue explicitement le cas où l'entier auxiliaire est premier de celui où il est composé. Lien direct

Leonhard Euler à Christian Goldbach, 25 juin 1730, correspondance Euler–Goldbach. Euler indique notamment qu'un terme de la suite de Fermat ne peut être divisible par un terme précédent et qu'un diviseur d'un terme ne peut diviser les suivants. Lien direct

Christian Goldbach à Leonhard Euler, 20 juillet 1730, même correspondance. Goldbach explicite l'argument du reste 2 qui conduit à la coprimalité deux à deux des nombres de Fermat. Lien direct

Leonhard Euler, *Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus*, rédigé en 1732 et publié en 1738. Euler y établit notamment la divisibilité de F_5 par 641. Lien direct