Terminale · maths expertes · DM

CHAPITRES

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

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

> *On sait depuis l'Antiquité qu'il existe une infinité de nombres premiers. Pourtant, les démonstrations ne consistent pas nécessairement à savoir produire explicitement le « nombre premier suivant ». Ce problème étudie deux mécanismes permettant de forcer l'apparition de facteurs premiers qui n'avaient encore jamais été rencontrés.*

On pourra utiliser sans démonstration le résultat suivant : **tout entier strictement supérieur à** 1 **possède au moins un diviseur premier.**

I Sortir d'une liste finie

1 Supposons, par l'absurde, qu'il n'existe qu'un nombre fini de nombres premiers, que l'on note $p_1, p_2, \dots, p_r$. On pose

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

Attention : N n'est pas nécessairement premier.

(a) Montrer que $N > 1$ et, pour tout $i \in \{1, \dots, r\}$, déterminer le reste de la division de N par p_i.

(b) Justifier que N possède un diviseur premier q. Montrer que q n'appartient pas à la liste $p_1, \dots, p_r$.

(c) Conclure.

La construction précédente ne fabrique donc pas nécessairement un nombre premier : elle fabrique un entier dont au moins un facteur premier ne peut appartenir à la liste de départ. Par exemple,

$$2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509.$$

Nous allons maintenant chercher à répéter ce phénomène au sein d'une même famille d'entiers.

II Des nombres qui ne partagent pas leurs facteurs premiers

Pour tout entier $n \geq 0$, on définit le n-ième **nombre de Fermat** par

$$F_n = 2^{2^n} + 1.$$

2 Calculer F_0, F_1, F_2, F_3, F_4. Pour $n \geq 1$, on pose

$$P_n = F_0 F_1 \cdots F_{n-1}.$$

Calculer P_1, P_2, P_3, P_4, puis conjecturer une relation générale entre P_n et F_n.

3 Démontrer la relation conjecturée à la question précédente pour tout entier $n \geq 1$.

4 Soient m et n deux entiers tels que $0 \leq m < n$.

(a) À l'aide de la question précédente, montrer que $F_m \mid F_n - 2$.

(b) En déduire que F_m et F_n sont premiers entre eux.

La propriété précédente ne signifie absolument pas que tous les nombres de Fermat sont premiers. Le premier contre-exemple apparaît déjà pour F_5.

5 On remarque que

$$641 = 5 \times 2^7 + 1 \qquad \text{et} \qquad 641 = 5^4 + 2^4.$$

En exploitant ces deux égalités et en travaillant modulo 641, montrer que F_5 n'est pas premier.

Ainsi, ce ne sont pas les nombres F_n eux-mêmes qui doivent être premiers. Ce qui compte est que leurs facteurs premiers ne puissent pas se retrouver dans deux termes différents.

III Le mécanisme général

6 Soit $n \in \mathbb{N}$, et soient $a_0, a_1, \ldots, a_n$ des entiers strictement supérieurs à 1, deux à deux premiers entre eux. Démontrer que le produit

$$a_0 a_1 \cdots a_n$$

possède au moins $n+1$ diviseurs premiers distincts.

7 On considère maintenant une suite infinie d'entiers $(a_n)_{n\geq 0}$ tels que $a_n > 1$ pour tout n, et dont les termes sont deux à deux premiers entre eux. Démontrer qu'il existe nécessairement une infinité de nombres premiers. Appliquer ce résultat à la suite des nombres de Fermat.

Bilan

La preuve d'Euclide et la construction fondée sur les nombres de Fermat ne cherchent pas à énumérer les nombres premiers. Dans la première, un entier auxiliaire force l'apparition d'un facteur premier absent d'une liste finie donnée. Dans la seconde, une famille entière d'entiers est construite de façon que deux termes distincts ne puissent partager aucun facteur premier. Dans les deux cas, c'est une contrainte de divisibilité qui oblige sans cesse de nouveaux nombres premiers à apparaître.