Arithmétique : nombres premiers

Prélude - Historique et contexte

Euclide démontre vers 300 av. J.-C. qu'il existe une infinité de nombres premiers. Ératosthène invente un crible pour les lister. En 1640, Pierre de Fermat énonce son « petit théorème », démontré plus tard par Euler. Aujourd'hui, la difficulté à décomposer de très grands nombres en facteurs premiers garantit la sécurité du chiffrement RSA (1977), utilisé chaque jour pour les paiements en ligne.

I Nombres premiers

Définition

Un entier naturel p est **premier** s'il admet exactement deux diviseurs positifs : 1 et p.
Les premiers nombres premiers sont 2, 3, 5, 7, 11, 13, 17, 19, 23, 29… (1 n'est pas premier.)

Propriété

Tout entier $n \geqslant 2$ admet au moins un diviseur premier. Si n n'est pas premier, il admet un diviseur premier p tel que $p \leqslant \sqrt{n}$.

Méthode - Tester si un nombre est premier

On teste la divisibilité de n par les nombres premiers $p \leqslant \sqrt{n}$.
Exemple : $\sqrt{211} \approx 14{,}5$; 211 n'est divisible ni par 2, 3, 5, 7, 11, 13 : 211 est premier.

Propriété - Infinité des nombres premiers

Il existe une infinité de nombres premiers.
Démonstration (Euclide) : si p_1, …, p_k étaient les seuls, $N = p_1 \times \cdots \times p_k + 1$ aurait un diviseur premier p_i, qui diviserait $N - p_1 \cdots p_k = 1$: absurde.

Méthode - Crible d'Ératosthène

Pour lister les nombres premiers inférieurs à N : on écrit les entiers de 2 à N, puis on barre les multiples stricts de 2, de 3, de 5… jusqu'à $\sqrt{N}$. Les nombres non barrés sont premiers.

II Décomposition en facteurs premiers

Propriété - Théorème fondamental de l'arithmétique (admis)

Tout entier $n \geqslant 2$ se décompose en produit de facteurs premiers, de manière unique à l'ordre près : $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_k^{\alpha_k}$.
Exemple : $360 = 2^3 \times 3^2 \times 5$.

Propriété - Diviseurs

Les diviseurs positifs de $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ sont les nombres $p_1^{\beta_1} \cdots p_k^{\beta_k}$ avec $0 \leqslant \beta_i \leqslant \alpha_i$. Il y en a $(\alpha_1 + 1) \cdots (\alpha_k + 1)$.
Exemple : 360 a $4 \times 3 \times 2 = 24$ diviseurs positifs.

Méthode - PGCD à l'aide des décompositions

On prend les facteurs premiers communs, chacun avec le plus petit exposant.
$360 = 2^3 \times 3^2 \times 5$ et $84 = 2^2 \times 3 \times 7$: PGCD$(360\ ;\ 84) = 2^2 \times 3 = 12$.

Propriété

Si un nombre premier p divise un produit ab, alors p divise a ou p divise b (conséquence du théorème de Gauss).

III Petit théorème de Fermat

Propriété - Petit théorème de Fermat

Si p est premier et a un entier non divisible par p, alors $a^{p-1} \equiv 1\ [p]$.
Forme équivalente : pour tout entier a, $a^p \equiv a\ [p]$.

Méthode - Calculer une puissance modulo p

Reste de 3^{2026} dans la division par 7 : 7 est premier et ne divise pas 3, donc $3^6 \equiv 1\ [7]$.
$2026 = 6 \times 337 + 4$, donc $3^{2026} = (3^6)^{337} \times 3^4 \equiv 81 \equiv 4\ [7]$.

Exemple - Application

Pour tout entier n, $n^5 - n$ est divisible par 5 (car $n^5 \equiv n\ [5]$).