Multiple, nombres premiers

Définition

Un entier $n \geqslant 2$ est un nombre premier ssi n admet exactement deux diviseurs 1 et lui-même.

Remarque : un nombre non premier est dit composé.

Les premiers nombres premiers sont :

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, ...

Il n'existe pas de machine à générer des nombres premiers. Par contre, on dispose de résultats concernant la densité des nombres premiers (hors programme)

Le plus grand nombre premier connu à ce jour (2016) est le nombre de Mersenne suivant :

$2^{74\,207\,281} - 1$ qui comporte 22 338 618 chiffres !

Test de primalité ou critère d'arrêt

Théorème : Soit $n \geqslant 2$:

- n admet un diviseur premier.
- Si n n'est pas premier alors il admet un diviseur premier p tel que : $2 \leqslant p \leqslant \sqrt{n}$.

Pour montrer qu'un nombre n est premier, on utilise la contraposée de ce théorème. Si n n'admet pas de diviseur premier $p \leqslant \sqrt{n}$ alors n est premier.

Exemple : montrons que 109 est premier.

- On calcule $\sqrt{109} \approx 10,4$.
- On teste tous les nombres premiers inférieur à 10 : 2, 3, 5 et 7
- Ces nombres ne divisent pas 109. Donc 109 est premier.

À la recherche des nombres premiers

- Pour obtenir une liste de nombres premiers inférieurs à un entier n donné, on peut utiliser le **crible d'Ératosthène**.

  On procède par élimination des multiples stricts des nombres premiers p_i inférieur ou égal à $\sqrt{n}$ sur la liste des entiers de 2 à n.

- **Les nombres de Mersenne** : On pose $M_n = 2^n - 1$.

  Proposition (exos bac) : Si M_n est premier alors n est premier.

  ⚠ La réciproque est fausse malheureusement. Contre-exemple : Si $n = 11$ alors n est premier, mais $M_{11} = 2047 = 23 \times 89$ n'est pas premier.

Infinité des nombres premier

ROC : Il existe une infinité de nombres premiers.

Démonstration par l'absurde, proche de celle d'Euclide en son temps. On suppose qu'il existe un nombre fini n de nombres premiers, on établit alors que le nombre $N = p_1 p_2 \dots p_n + 1$ est aussi premier ce qui est contradictoire avec l'hypothèse de départ.

Opération sur les multiples - ROC

Théorème : Si a divise b et c, alors a divise toute combinaison linéaire de b et de c soit $\alpha b + \beta c$, avec $\alpha, \beta \in \mathbb{Z}$.

Soit $k \in \mathbb{Z}$, on donne $a = 9k - 4$ et $b = 5k - 3$.

Si d divise a et b, alors d divise 7 car :

$$5a - 9b = 45k - 20 - 45k + 27 = 7$$

Les valeurs possibles pour d sont alors 1 et 7.

Théorème fondamental de l'arithmétique

Tout entier naturel $n \geqslant 2$ peut se décomposer en produits de puissances de nombres premiers (à l'ordre des facteurs près).

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_m^{\alpha_m}$$

Exemple : $120 = 2^3 \times 3 \times 5$.

Remarque : Les nombres premiers apparaissent comme des briques élémentaires de l'arithmétique.

Diviseurs et nombres de diviseurs

- Tout diviseur d de n admet comme décomposition :

  $$d = p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_m^{\beta_m} \quad \text{avec} \quad 0 \leqslant \beta_i \leqslant \alpha_i$$

- Le nombre N de diviseurs de n est égal à :

  $$N = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_m + 1)$$

Exemple : 120 a $N = (3+1)(1+1)(1+1) = 16$ diviseurs.

Multiple, diviseur

- Soit a et b deux entiers relatifs.
  L'entier a est un multiple de l'entier b ssi il existe un entier relatif k tel que $a = kb$.
  On dit aussi que b divise a que l'on peut écrire $b|a$.
- **Conséquence** : comme un entier ne possède qu'un nombre restreint de diviseurs, on cherchera à factoriser une équation ou un problème de divisibilité.
- Déterminer $n \in \mathbb{N}$ tel que $(n-2)$ divise $(2n+3)$.

  $2n + 3 = k(n-2) \Leftrightarrow 2(n-2) + 7 = k(n-2) \Leftrightarrow$

  $(n-2)(k-2) = 7$ donc $(n-2)$ divise 7

  $n - 2 = 1$ ou $n - 2 = 7$ soit $n = 3$ ou $n = 9$