Arithmétique

Définition 1 (Divisibilité dans $\mathbb{N}$) : Soient a et b des entiers naturels.

On dit que a *divise* b, noté $a|b$, s'il existe un entier naturel k tel que $b = ka$.

On dit alors que :

- a est *un diviseur* de b. On note $\mathscr{D}(b)$ leur ensemble.

Proposition 1 (Compatibilité) :

$\boxed{1}$ $\begin{array}{l}\forall a, b, c \in \mathbb{N} \\ \forall m, n \in \mathbb{N}\end{array}$, $\begin{cases} a|b \\ a|c \end{cases} \implies a|mb + nc$ $\left(\begin{array}{l}\text{« } a|b \text{ » est compatible avec les} \\ \text{combinaisons linéaires entières}\end{array}\right)$

Proposition 2 : Soient a et b deux entiers naturels avec b non nul.

$b|a \iff$ le reste dans la division euclidienne de a par b est nul.

Théorème 3 (Critère d'arrêt) :

- Tout entier naturel n, $n \geqslant 2$, admet un diviseur premier.
- Si n n'est pas premier, alors il admet un diviseur premier p tel que :

$$2 \leqslant p \leqslant \sqrt{n}.$$

Théorème 4 : L'ensemble des nombres premiers est infini .

Preuve : Supposons le contraire i.e. qu'il existe un nombre fini de nombres premiers que l'on va noter p_1, p_2, ..., P_n et posons

$$N = p_1 \times p_2 \times \ldots \times p_n + 1.$$

L'objectif de la cette démonstration est de prouver que N est premier . Comme il est strictement plus grand que les p_i , on aura notre contradiction.

Si N est premier , la contradiction est déjà toute trouvée. Sinon, d'après le critère d'arrêt, N admet un diviseur premier . Soit p_i ce diviseur premier.

Par définition p_i divise donc $p_1 \times p_2 \times \ldots \times p_n$ et N donc divise aussi $N - p_1 \times p_2 \times \ldots \times p_n = 1$.

Ceci est impossible, donc l'hypothèse qu'il existe un nombre fini de nombres premiers est absurde.

Corollaire 4.1 : $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ admet $\displaystyle\prod_{i=1}^{k} (1+\alpha_i)$ diviseurs.

En particulier, $60 = 2^2 \times 3^1 \times 5^1$ admet 12 diviseurs.

Théorème 5 : Soient a et b deux entiers non nuls.

- Les multiples communs de a et b sont **exactement** les multiples de $\text{ppcm}\,(a\,;b)$:

$$\text{ppcm}\,(a\,;b)\,|m \iff \begin{cases} a|m \\ b|m \end{cases}$$

De manière équivalente : $(a \vee b)\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$.

Proposition 6 : Soient a et b deux entiers supérieurs à 2 dont les décompositions primaires s'écrivent $a = \displaystyle\prod_{p\in\mathbb{P}} p^{\alpha_p}$ et $b = \displaystyle\prod_{p\in\mathbb{P}} p^{\beta_p}$.

Alors,

$$a \wedge b = \prod_{p\in\mathbb{P}} p^{\min(\alpha_p,\beta_p)}.$$

Exercice 1 : Calculer :

1. $\text{pgcd}\,(36\,;24) = 12 \times \text{pgcd}\,(3\,;2) = 12$.

2. $\text{pgcd}\,(231\,;299) = 1$.

   Commentaires : *La méthode la plus jolie étant, une fois n'est pas coutume, de voir que $231 = 11 \times 21$ et de vérifier que 299 n'est divisible ni par 11, 7, ou 3.*

Arithmétique

Définition 2 (Divisibilité dans $\mathbb{N}$) : Soient a et b des entiers naturels.

On dit que a *divise* b, noté $a|b$, s'il existe un entier naturel k tel que $b = ka$.

On dit alors que :

- b est *un multiple* de a. On note $a\mathbb{N}$ leur ensemble.

Proposition 7 (Compatibilité) :

1. $\forall a, b, c \in \mathbb{N}, \quad \begin{cases} a|b \\ b|c \end{cases} \implies a|c$ $\quad\big($ « $a|b$ » est transitive $\big)$

Proposition 8 : Soient a et b deux entiers naturels avec b non nul.

$b|a \iff$ le reste dans la division euclidienne de a par b est nul.

Théorème 9 (Théorème fondamental de l'arithmétique) : Tout entier n supérieur à 2 admet une et une seule (à l'ordre des facteurs près) décomposition en facteurs premiers .

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \text{ avec } p_i \in \mathbb{P} \text{ deux à deux distincts et } \alpha_i \in \mathbb{N}^*.$$

Preuve : Pour tout entier $n \geqslant 2$, posons :

$\mathrm{H}(n)$: « L'entier n peut s'écrire sous la forme d'un produit de nombres premiers. »

On va démontrer cette propriété par une récurrence forte .

Comme 2 est premier , il peut s'écrire comme le produit de lui-même et $\mathrm{H}(2)$ est vérifiée.

Supposons alors que $\mathrm{H}(k)$ soit vérifiée pour tout entier k tel que $2 \leqslant k \leqslant n$ et considérons l'entier $n+1$:

- Si $n+1$ est premier , alors $\mathrm{H}(n+1)$ est vraie .
- Si $n+1$ n'est pas premier alors il admet un diviseur premier p et on a $n = p \times m$ où m est un entier tel que $2 \leqslant m \leqslant n$.

  Il suffit alors d'appliquer l'hypothèse de récurrence à m pour avoir l'existence de la décomposition et la propriété $\mathrm{H}(n+1)$.

  En conclusion, la propriété $\mathrm{H}(n)$ est donc héréditaire .

  Étant initialisée pour $n = 2$, elle est vraie pour tout entier $n \geqslant 2$.

Corollaire 9.1 : $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ admet $\displaystyle\prod_{i=1}^{k} (1+\alpha_i)$ diviseurs.

En particulier, $450 = 2^1 \times 3^2 \times 5^2$ admet 18 diviseurs.

Théorème 10 : Soient a et b deux entiers non nuls.

- Les diviseurs communs de a et b sont **exactement** les diviseurs de $\operatorname{pgcd}(a\,;b)$:

$$d|\operatorname{pgcd}(a\,;b) \iff \begin{cases} d|a \\ d|b \end{cases}$$

De manière équivalente : $\mathscr{D}(a \wedge b) = \mathscr{D}(a) \cap \mathscr{D}(b)$.

Proposition 11 : Soient a et b deux entiers supérieurs à 2 dont les décompositions primaires s'écrivent $a = \displaystyle\prod_{p \in \mathbb{P}} p^{\alpha_p}$ et $b = \displaystyle\prod_{p \in \mathbb{P}} p^{\beta_p}$.

Alors,

$$a \vee b = \prod_{p \in \mathbb{P}} p^{\max(\alpha_p, \beta_p)}.$$

Exercice 1 : Calculer :

1. $\operatorname{pgcd}(15\,;45) = 5 \times \operatorname{pgcd}(3\,;9) = 5 \times 3 = 15.$

2. $\operatorname{pgcd}(201\,;289) = 1.$

   Commentaires : *La méthode la plus jolie étant, une fois n'est pas coutume, de reconnaître $289 = 17^2$ et de vérifier que 201 n'est pas divisible par 17.*