Lycée du Parc
842.

Arithmétique

1 Divisibilité

Définition 1. Soit a et b deux entiers relatifs. On dit que b divise a et on note $b|a$ s'il existe $q \in \mathbb{Z}$, $a = bq$.
On dit que b est un diviseur de a et a et un multiple de b.

Exemple 1. *Les diviseurs positifs de* 24 *sont : 1,2,3,4,6,8,12 et 24.*

Remarques. *1.* 1 *divise tous les entiers.*

2. 0 *ne divise aucun entier à part lui-même.*

3. Tous les entiers $b \in \mathbb{Z}$ *divisent* 0.

Proposition 1.
Soit $a, b \in \mathbb{N}^*$. Si b divise a alors $b \leqslant a$.

2 Division euclidienne

Théorème 2.
Soit $a \in \mathbb{N}$ et $b \in \mathbb{N}^\star$. Il existe un unique couple $(q, r) \in \mathbb{N}^2$ tel que :

$$\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}$$

On appelle q le quotient de la division euclidienne de a par b et r le reste.

Remarque : Si $a \in \mathbb{N}$, $b \in \mathbb{N}^\star$

(b divise a) $\Leftrightarrow$ (le reste de la division euclidienne de a par b est 0)

3 Nombre premier

Définition 2. Un entier $p \geqslant 2$ est dit premier si ses seuls diviseurs positifs sont 1 et lui-même.

Théorème 3 (admis). *Tout entier $n \geqslant 2$ se décompose de manière unique, à l'ordre des facteurs près, sous la forme*

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$

où

- *$p_1, \dots, p_k$ sont des nombres premiers distincts.*
- *$\alpha_1, \dots, \alpha_k$ sont des entiers naturels non nuls.*

Proposition 4.
Il existe une infinité de nombres premiers.

Exemple 2. *Montrer qu'il existe une infinité de nombres premiers de la forme $4q - 1$.*

4 PGCD et PPCM

Définition 3. Soient $a, b \in \mathbb{N}$ tels que au moins l'un des deux est non nuls.

- Le PGCD (plus grand commun diviseur) de a et b est le plus grand des entiers qui sont à la fois diviseurs de a et de b. Cet entier est bien défini puisque l'ensemble des diviseurs communs à a et à b est non vide (il contient 1) et il est majoré (par a ou b si $a = 0$). On le note $\text{pgcd}(a, b)$ ou $a \wedge b$.
- Le PPCM (plus petit commun multiple) de a et b est le plus petit des entiers positifs qui est 'a la fois un multiple de a et un multiple de b. Cet entier est bien défini puisque a et b admettent toujours des multiples communs positifs (par exemple ab), et est minoré par 0. Il est noté $a \vee b$, ppcm(a, b) ou PPCM(a, b).
- Lorsque deux entiers ont un PGCD égal à 1, ce qui signifie qu'ils n'ont aucun diviseur commun (et donc aucun nombre premier en commun dans leurs décomposition respectives), on dit qu'ils sont premiers entre eux.

Théorème 5 (théorème de Gauss). *Soit a, b deux entiers naturels. Si n divise ab et qu'il est premier avec a, alors n divise b.*

Proposition 6.
$a \times b = \text{pgcd}(a,b) \times \text{ppcm}(a,b)$. De manière générale, si

$$a = p_1^{\alpha_1} \times \dots p_n^{\alpha_n} \text{ et } b = p_1^{\beta_1} \times \dots p_n^{\beta_n},$$

alors

$$\text{pgcd}(a,b) = p_1^{\gamma_1} \times \dots \times p_n^{\gamma_n} \text{ avec } \gamma_i = \min(\alpha_i, \beta_i)$$

et

$$\text{ppcm}(a,b) = p_1^{\lambda_1} \times \dots \times p_n^{\lambda_n} \text{ avec } \lambda_i = \max(\alpha_i, \beta_i)$$

Il y a deux méthodes classiques pour calculer le PGCD de deux entiers $a, b \in \mathbb{N}^\star$.
Méthode 1: utiliser la décomposition en facteurs premiers

Exemple 3. *pour le calcul du PGCD de 66 et 24, on les décompose en facteurs premiers.*

Méthode 2: l'algorithme d'Euclide

Lemme. Si $a, b \in \mathbb{N}$ sont deux entiers dont un au moins est non nul, alors $\text{pgcd}(a,b) = \text{pgcd}(b,r)$, où r est le reste de la division euclidienne de a par b.

L'algorithme d'Euclide consiste à effectuer des divisions euclidiennes successives, jusqu'à obtenir 0.
Remarque: La suite d'entiers définie par restes successifs finira toujours par valoir 0 puisqu'il s'agit d'une suite d'entiers positifs strictement décroissante.

Exemple 4. *Pour $n \in \mathbb{N}^\star$, on note $\sigma(n)$ la somme des diviseurs positifs de n.*

1. *Montrer que si m et n sont premiers entre eux, alors $\sigma(mn) = \sigma(m)\sigma(n)$.*
2. *Soit p un nombre premier, calculer $\sigma(p^k)$ pour $k \in \mathbb{N}^\star$.*
3. *En déduire le calcul de $\sigma(n)$ pour un entier $n \in \mathbb{N}^\star$ quelconque, en fonction de sa décomposition en nombres premiers.*
4. *Calculer $\sigma(360)$.*

On appelle nombre parfait un entier n tel que $\sigma(n) = 2n$, c'est-à-dire que n est égal à la somme des ses diviseurs autres que lui-même.

5. *Montrer que si $n = 2^{k-1}\left(2^k - 1\right)$, où $2^k - 1$ est premier, alors n est parfait.*
6. *Réciproquement, soit n un nombre parfait pair. On pose $n = 2^a b$ avec $a > 0$ et b impair.*
   (a) *Montrer que $(2^{a+1} - 1)\,\sigma(b) = 2^{a+1} b$.*
   (b) *Montrer que $\sigma(b) - b$ divise b.*
   (c) *En déduire que b est premier et que n est de la forme donnée en a.*