Chapitre 6 : Arithmétique des entiers.

On rappelle que $\mathbb{N} = \{0, 1, 2, \dots\}$ et $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$.

On étudie quelques propriétés de la divisibilité dans l'ensemble des entiers relatifs $\mathbb{Z}$. Dans ce chapitre, on entendra "entier relatif" quand on dira "entier".

L'ensemble $\mathbb{Z}$ est muni d'une relation *d'ordre* notée $\leq$ et de deux *opérations internes* $+$ et $*$ vérifiant les propriétés bien connues : associativité, commutativité, distributivité ...

On rappelle trois des axiomes des nombres entiers naturels :

- Tout ensemble non vide d'entiers naturels admet un plus petit élément.
- Tout ensemble non vide et majoré d'entiers naturels admet un plus grand élément.
- $\mathbb{N}$ n'a pas de plus grand élément.

Plan

1 Divisibilité, division euclidienne

On considère a et b des entiers.

On dit que :

- a **divise** b ou ,
- a est un **diviseur** de b ou ,
- b **est un multiple** de a.

quand il existe q un entier relatif tel que

$$b = q \times a = qa$$

On note alors $a \mid b$.

Tout entier divise 0 et est un multiple de lui même et de 1. 1 divise tout entier, 0 aucun sinon lui même. a non nul divise b si et seulement si $\frac{b}{a}$ (à priori un rationnel) est un entier.

a divise b si et seulement si $|a|$ divise $|b|$. Dans ce cas alors : $|a| \leq |b|$.

On a les propriétés élémentaires suivantes :

- Si $a \mid b$ alors $\pm a \mid \pm b$.
- Si $a \mid b$ et $b \mid c$ alors $a \mid c$.
- Si $a \mid b$ et $b \mid a$ alors $a = \pm b$.
- Si $a \mid 1$ alors $a = \pm 1$.
- Si $a \mid b$ et $c \in \mathbb{Z}$ alors $ac \mid bc$.

Ces propriétés, un peu analogues à celles de la relation $\leq$, nous feront dire que la relation $\mid$ est une **relation d'ordre**.

Au delà des cas de divisibilités élémentaires, pour évaluer si un entier divise un autre, on peut utiliser la division euclidienne.

Théorème 1 (Division euclidienne) *Soit a et $b > 0$ des entiers, il existe q et r 2 entiers, uniques, tels que :*

$$a = qb + r \qquad et \qquad 0 \leq r < b$$

- *a est le* ***dividende***
- *b est le* ***diviseur***
- *q est le* ***quotient***
- *r est le* ***reste***

de la ***division euclidienne*** *de a par b.*

En Python 3, le reste est obtenu par a % b, le quotient par a // b.

Première application :

Propriété 1 *Un entier $a > 0$ divise un entier b si et seulement si le reste de la division euclidienne de b par a est nul.*

2 Multiples et diviseurs communs

On considère a et $b > 0$ des entiers naturels.

Définition 1 *Le* PGCD ***: plus grand diviseur commun*** *de a et b est le plus grand entier divisant a et b. On le note $a \wedge b$ ou* $\mathrm{PGCD}(a, b)$.

Remarquons que :

- $1 \mid \mathrm{PGCD}(a, b) \mid a$,
- $1 \mid \mathrm{PGCD}(a, b) \mid b$,
- $1 \leq a \wedge b \leq \min(a, b)$.

,

On convient si a et b sont des entiers relatifs ($b \neq 0$) : $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(|a|, |b|)$ et $\mathrm{PGCD}(b, 0) = |b|$.

L'**algorithme d'Euclide** fournit le PGCD de 2 entiers à l'aide de la relation :

Propriété 2 *Si a et b sont des entiers naturels non nuls et si r est le reste de la division euclidienne de a par b alors :*

$$\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, r)$$

On peut alors considérer l'algorithme :
Si $a > b$ prendre (a, b) et faire la division euclidienne de a par b.

- Si $r = 0$, $\mathrm{PGCD}(a, b) = b$
- Si $r > 0$, reprendre ce qui précède avec le couple $b > r$.

L'algorithme débouche car il construit une suite strictement décroissante d'entiers naturels.

On a même mieux :

Théorème 2 *Soit a et b 2 entiers non nuls et $d = \mathrm{PGCD}(a, b)$ alors il existe des entiers relatifs n et m tels que :*

$$d = na + mb$$

Une telle relation s'appelle une **relation de Bezout**.

En écrivant explicitement les divisions euclidiennes intervenant dans l'algorithme d'Euclide :

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{p-1} &= q_{p+1} r_p + r_{p+1} \\ r_p &= q_{p+2} r_{p+1} + d \\ r_{p+1} &= q_{p+3} d + 0 \end{aligned}$$

avec $a > b > r_1 > r_2 \cdots > r_{p+1} > d > 0$, on fournit une preuve et un algorithme (dit **algorithme d'Euclide étendu**) de calcul des valeurs d'une relation de Bezout.

On obtient ensuite :

Propriété 3 *Un entier d divise a et b si et seulement si $d \mid a \wedge b$.*

On considère toujours des entiers naturels non nuls.

Définition 2 *Le* PPCM ***: plus petit commun multiple*** *de a et b est le plus petit entier naturel non nul qui est un multiple de a et b. On le note $a \vee b$ ou* $\mathrm{PPCM}(a, b)$.

Le lien avec le PGCD est donné par la propriété (conséquence de la décomposition en facteurs premiers , voir plus loin) :

$$a \cdot b = (a \vee b) \cdot (a \wedge b)$$

3 Nombres premiers entres eux

On dit que a et b des entiers naturels non nuls sont **premiers entre eux** quand de manière équivalente :

- $\text{PGCD}(a, b) = a \wedge b = 1$,
- Il existe n et m des entiers relatifs tels que : $an + bm = 1$ (théorème de Bezout).

On peut se ramener à la situation précédente par l'utile :

Propriété 4 *Soit a et b des entiers naturels non nuls, $d = a \wedge b$, il existe des entiers naturels non nuls a' et b' tels que :*

- $a = da'$,
- $b = db'$,
- $a' \wedge b' = 1$.

Propriété 5 (Lemme de Gauss) *a, b, c sont des entiers naturels non nuls.*

$$Si \;\; a \mid b.c \;\; et \;\; a \wedge b = 1 \;\; alors \;\; a \mid c$$

Propriété 6 *a, b, c, $n \geq 1$ sont des entiers naturels non nuls.*

$$Si \begin{cases} a \wedge b = 1 \;\; et \\ a \wedge c = 1 \end{cases} \qquad alors \;\; a \wedge bc = 1$$

$$a \wedge b = 1 \;\; si \;\; et \;\; seulement \;\; si \;\; a \wedge b^n = 1$$

4 Nombres premiers

Un entier naturel $n \geq 2$ est dit **premier** si ses seuls diviseurs entiers naturels sont 1 et lui même.

Le lien avec les nombres "premiers entre eux" est donné par :

Si a est un entier non nul et p est un entier premier alors :

- ou p divise a,
- ou a et p sont premiers entre eux.

Théorème 3 (Euclide) *Il y a un nombre infini d'entiers premiers.*

Si un entier n'est pas premier, on peut le décomposer en facteurs premiers :

Théorème 4 (Théorème fondamental de l'arithmétique) *Si $n > 2$ est un entier naturel, il existe une suite $p_1 < p_2 < \cdots < p_r$ de nombres premiers et des entiers non nuls $v_1, \ldots, v_r$ tels que :*

$$n = p_1^{v_1} p_2^{v_2} \ldots p_r^{v_r}$$

Cette décomposition est de plus unique dans le sens suivant :

Si $p_1 < p_2 < \cdots < p_r$ et $p'_1 < p_2 < \cdots < p'_q$ sont des nombres premiers, $v_1, \ldots, v_r$, $v'_1, \ldots, v'_q$ sont des entiers naturels non nuls et si :

$$p_1^{v_1} p_2^{v_2} \ldots p_r^{v_r} = (p'_1)^{v'_1} (p'_2)^{v'_2} \ldots (p'_q)^{v'_q}$$

alors $r = q$, $p_1 = p'_1$, $p_2 = p'_2$,...,$p_r = p'_r$ et $v_1 = v'_1$, $v_2 = v'_2$,...,$v_r = v'_r$.

Du coup, si un entier premier p divise un entier naturel n (on dit que p est un **facteur premier** de n), on considère la plus grande puissance de p qui divise n (c'est celle qui intervient dans la décomposition en facteurs premier de n). C'est la **valuation p-adique de n**. Elle est notée $v_p(n)$. Si p ne divise par n, on convient $v_p(n) = 0$.

On constate alors que (la multiplication se limitant en fait aux diviseurs premiers de n) :

$$n = \prod_{p \text{ premier}} p^{v_p(n)}$$

et que si n et m sont des entiers naturels non nuls et si p est premier alors :

$$v_p(n \times m) = v_p(n) + v_p(m).$$

Propriété 7 *Un entier a divise un entier b si et seulement si pour tout entier premier p : $v_p(a) \leq v_p(b)$.*

Ce qui permet de montrer :

Propriété 8 *En autorisant les puissances nulles dans l'écriture :*

Si $a = p_1^{v_1} p_2^{v_2} \ldots p_r^{v_r}$ et $b = p_1^{v'_1} p_2^{v'_2} \ldots p_r^{v'_r}$ sont les décompositions en facteurs premiers de a et b alors :

$$a \wedge b = p_1^{\text{Min}(v_1, v'_1)} \cdot p_2^{\text{Min}(v_2, v'_2)} \cdot \ldots \cdot p_r^{\text{Min}(v_r, v'_r)}$$

$$a \vee b = p_1^{\text{Max}(v_1, v'_1)} \cdot p_2^{\text{Max}(v_2, v'_2)} \cdot \ldots \cdot p_r^{\text{Max}(v_r, v'_r)}$$

Pour ce qui est des grands nombres, la question de la primalité est délicate. Signalons le critère le plus basique :

Propriété 9 *Si un entier $n > 2$ n'est pas premier, il existe un diviseur d de n avec : $2 \leq d \leq \sqrt{n}$.*

Tout rationnel r non nul peut s'écrire sous la forme $r = \pm\frac{p}{q}$ (avec p et q des entiers naturels). On dit qu'il est **écrit sous forme irréductible** quand $p \wedge q = 1$. Une telle écriture existe et est unique.

Soit maintenant $a_1, \ldots, a_r$ des entiers naturels non tous nuls.

Définition 3 *Le* PGCD ***: plus grand diviseur commun*** *de $n_1, \ldots, n_r$ est le plus grand entier divisant a_1,a_2, ... et a_r. On le note* PGCD$(a_1, \ldots, a_r)$.

On montre que, dans le cas précédent, si $d = \text{PGCD}(a_1, \ldots, a_r)$ alors il existe des entiers relatifs $n_1, n_2, \ldots, n_r$ tels que :

$$d = n_1 a_1 + n_2 a_2 + \cdots + n_r a_r$$

une telle relation s'appelle **relation de Bezout**.

On dit que $a_1, \ldots, a_r$ sont **premiers entre eux dans leur ensemble** quand $\text{PGCD}(a_1, \ldots, a_r) = 1$, c'est à dire qu'il n'y a pas de facteur premier commun à a_1,a_2, ... et a_r.

Si les nombres $a_1, \ldots, a_r$ sont **premiers entre eux 2 à 2** alors ils sont premiers entre eux dans leur ensemble mais la réciproque est bien sûr fausse ...

5 Congruences

Soit n un entier naturel et a et b 2 entiers.

Définition 4 *S'il existe un entier (relatif) k tel que $a = b + k.n$ alors on dit que a et b sont* ***congrus*** *ou* ***égaux modulo*** *n et on note :*

$$a \equiv b \ [n]$$

Notons :

$$a \equiv b \ [n] \text{ si et seulement si : } n|(b-a)$$

On obtient les règles de calcul élémentaires suivantes (a, b, c, d sont des entiers) :

$$\text{Si } \begin{cases} a \equiv b \ [n] \\ c \equiv d \ [n] \end{cases} \quad \text{alors : } \begin{cases} a + c \equiv b + d \ [n] \\ a.c \equiv b.d \ [n] \end{cases}$$

et si r est un entier naturel :

$$\text{Si : } a \equiv b \ [n] \text{ alors : } a^r \equiv b^r \ [n]$$

On utilise les congruences pour prouver :

Théorème 5 (Petit théorème de Fermat) *Si a est un entier et p est un entier premier alors :*

$$a^p \equiv a \ [p]$$

Si de plus p ne divise pas a :

$$a^{p-1} \equiv 1 \ [p]$$

Savoirs et savoirs faire indispensables

Énoncés et mise en pratique des résultats de base : division euclidienne, calcul d'un pgcd, algorithme d'Euclide, lemme de Gauss, décomposition d'un nombre en facteurs irréductibles ...