Chapitre 6 : Eléments d'arithmétique de $\mathbb{Z}$

Introduction

L'arithmétique des entiers est un champ singulier des mathématiques. Il est étudié depuis l'Antiquité, enseigné dès les petites classes, a des applications très importantes et recèle encore de nombreux problèmes dont la résolution pourrait avoir des conséquences cruciales (en sécurité des données numériques notamment).
Sa place dans le programme de PCSI est aussi singulière : son objet principal est de préparer l'arithmétique des polynômes. La plupart des notions qu'il faudra retenir de ce chapitre sont déjà connues : divisibilité, division euclidienne, nombres premiers et leur utilisation pour décomposer un entier naturel en produit de nombres premiers.
La plupart des démonstrations qui sont proposées se transposeront de façon similaire dans le champ des polynômes, il est donc judicieux de les comprendre. Certaines, hors programme, sont néanmoins présentes dans ce cours : elles ont vocation à stimuler les étudiants les plus à l'aise.

1 Divisibilité et nombres premiers

Définition
Soit $(a, b) \in \mathbb{N}^2$. On dit que a divise b lorsqu'il existe $c \in \mathbb{N}$ tel que $b = ac$.
On note alors $a|b$ et on dit que a est un diviseur de b ou que b est un multiple de a.

Exemples :

a) $7|28$ car $28 = 7 \times 4$.

b) $\forall n \in \mathbb{N},\ 1|n$ et $n|n$.

c) L'ensemble des diviseurs de 12 est $\{1; 2; 3; 4; 6; 12\}$.

Remarque : la divisiblité est une relation d'ordre partielle dans $\mathbb{N}$ car elle est réflexive, antisymétrique et transitive.

Définition
Soit $n \in \mathbb{N}$. On dit de n qu'il est premier lorsqu'il admet exactement deux diviseurs, qui sont alors 1 et n lui-même.

Exemples :

a) 2, 3, 5 sont des exemples de nombres premiers.

b) 6 n'est pas premier car il est divisible par 2.

c) 1 n'est pas premier car il n'a qu'un diviseur.

Méthode (Crible d'Eratosthène pour trouver les nombres premiers inférieurs à n)
1. On écrit la liste des entiers de 1 à n, par ordre croissant.
2. **Tant que** tous les entiers ne sont ni barrés, ni entourés :
   — on entoure le premier nombre ni barré ni entouré ;
   — on barre tous ses multiples.
3. La liste des nombres entourés est la liste des nombres premiers de $[\![2; n]\!]$

Remarque : on ne dispose pas d'algorithme qui soit beaucoup plus performant que le Crible d'Eratosthène pour décider si un nombre est premier ou non. Il existe néanmoins des résultats théoriques qui donnent le « rythme » d'appartition des nombres premiers inférieurs à n quand n tend vers $+\infty$.

Théorème
Il existe une infinité de nombres premiers.

Démonstration
Raisonnons par l'absurde et supposons qu'il existe un nombre fini N de nombres premiers, on les note alors $p_1, \dots, p_N$.
Le nombre $\prod_{i=1}^{N} p_i + 1$ n'est divisible par aucun des p_i *(voyez-vous bien pourquoi ?)* il est donc soit premier, soit divisible par un nombre premier qui n'est pas l'un des p_i.
Dans les deux cas, c'est en contradiction avec notre hypothèse. ■

2 Division euclidienne

Proposition
Soit a, b deux entiers avec $b \neq 0$.

- Il existe un unique couple $(q, r) \in \mathbb{N} \times [\![0; b-1]\!]$ tel que $a = bq + r$.
- L'écriture $a = bq + r$ est appelée la division euclidienne de a par b, q en est le quotient et r le reste.

Exemples :

a) $13 = 5 \times 2 + 3$ est la division de 13 par 5, mais pas celle de 13 par 2 car $3 \notin [\![0; 1]\!]$.

b) Si $a < b$ alors $a = 0 \times b + a$ est la division euclidienne de a par b.

Démonstration

— **Existence de la division euclidienne :** soit Ω l'ensemble des multiples de b inférieurs à a. On a :

$$\Omega = \{n \in [\![0; a]\!] \ / \ b|n\} = \{0; 1b; 2b; \dots; \underbrace{mb}_{\leq a}\}$$

Ω n'est pas vide puisqu'il contient 0, il est fini puisqu'il est majoré par a, il admet donc un plus grand élément qu'on note mb.
$(m+1)b \notin \Omega$ donc $mb \leq a < (m+1)b$ ce qui entraîne $a - mb \in [\![0; b-1]\!]$.
$a = mb + (a - mb)$ est donc une division euclidienne de a par b.

— **Unicité de la division euclidienne :** supposons que $a = bq_1 + r_1$ et $a = bq_2 + r_2$ soient deux divisions euclidiennes de a par b.
On a r_1 et r_2 qui sont dans $[\![0; b-1]\!]$ et donc $-b < r_1 - r_2 < b$.
On a également $r_1 - r_2 = b(q_2 - q_1)$ donc $b|r_1 - r_2$ ce qui entraîne que $r_1 - r_2 = 0$ car c'est le seul entier de $]-b; b[$ qui soit divisible par b.
Il suit que $q_1 = q_2$. Finalement, la division euclidienne de a par b est unique.

Proposition
Soit a, b deux entiers.
b divise a si, et seulement si, le reste dans la division euclidienne de a par b est nul.

Démonstration
On procède par double implication.

$\Longrightarrow$: si b divise a alors il existe un entier c tel que $a = bc$. C'est la division euclidienne de a par b, son reste est nul.

$\Longleftarrow$: si $a = bq + 0$ avec $q \in \mathbb{N}$ alors $a = bq$ et donc b divise a.

3 Congruences modulo n

Notation : dans cette partie, n désigne un entier non nul.

Définition
On dit de deux entiers a et b qu'ils sont congrus modulo n lorsqu'ils ont le même reste dans la division euclidienne par n. On note alors $a \equiv b\ [n]$ ou $a \equiv b \bmod n$.

Théorème
La congruence modulo n est une relation d'équivalence dans $\mathbb{N}$, c'est-à-dire qu'elle est réflexive, symétrique et transitive.

Remarque : lorsqu'on dispose d'une relation d'équivalence sur un ensemble E, on peut regrouper les éléments de E dans des sous-ensembles au sein desquels tous les éléments sont équivalents entre eux, on les appelle classes d'équivalence.

Exemples :

1. Il y a deux restes possibles dans la division euclidienne par 2 : 0 et 1. Il y a donc deux classes d'équivalence modulo 2 : la classe des nombres pairs et la classe des nombres impairs. Dire de deux nombres entiers qu'ils sont congrus modulo 2 c'est dire qu'ils ont la même parité.
2. Il y a trois restes possibles dans la division euclidienne par 3 : 0, 1 et 2. Il y a donc trois classes d'équivalence modulo 3 :
   — la classe de 0 qui regroupe tous les nombres divisibles par 3 ;
   — la classe de 1 qui regroupe tous les nombres de la forme $3k+1$;
   — la classe de 2 qui regroupe tous les nombres de la forme $3k+2$;

Remarque : pour les mesures des angles en radians, représenter le même angle orienté (c'est-à-dire le même point sur le cercle trigonométrique) est une relation d'équivalence pour les réels.
Pour des réels x et y, écrire $x \equiv y\ [2\pi]$ signifie qu'il existe $k \in \mathbb{Z}$ tel que $y - x = k2\pi$. Il y a donc autant de classes d'équivalence que de réels dans un intervalle de la forme $[\theta; \theta + 2\pi[$. La notion de mesure principale revient à choisir un représentant de la classe d'équivalence.

Théorème
La relation de congruence modulo n est compatible avec l'addition et la multiplication des entiers.

Remarque : le théorème précédent est crucial, la proposition ci-dessous illustre le type de résultats qu'il permet de prouver.

Proposition (Critère de divisiblité par 3)
Un entier est divisible par 3 si, et seulement si, la somme de ses chiffres est divisible par 3.

Démonstration
Soit a un entier, notons $c_0, \ldots, c_p$ ses chiffres dans le système décimal.
Autrement dit : $a = c_p c_{p-1} \ldots c_0$ avec $\forall i,\ c_i \in [\![0; 9]\!]$. Notons que $10 \equiv 1 \bmod 3$. On a :

$$a = \sum_{i=0}^{p} c_i 10^i \equiv \sum_{i=1}^{p} c_i 1^i \bmod 3 \equiv \sum_{i=1}^{p} c_i \bmod 3$$

a et $\sum_{i=1}^{p} c_i$ sont congrus modulo 3, c'est-à-dire qu'ils ont même reste dans la division euclidienne par 3.
Il suit que a est divisible par 3 si, et seulement si, $\sum_{i=1}^{p} c_i$ est divisible par 3. ■

4 Décomposition en produit de facteurs premiers

Théorème (Lemme d'Euclide)
Soit a, b deux entiers et p un nombre premier.
Si p divise ab alors p divise a ou b.

Démonstration
Raisonnons par l'absurde. Supposons que p ne divise ni a ni b.
Soit $\Lambda = \{n \in \mathbb{N} \ / \ p \mid an \text{ et } p \nmid n\}$. Λ contient b, il n'est donc pas vide. Il admet donc un plus petit élément, notons-le c. $c \in [\![1; p-1]\!]$ car, sinon, le reste dans la division de c par p serait un élément de Λ plus petit que c.
La division euclidienne de p par c donne $p = qc + r$: $(\star)$ avec $r < c$ ce qui entraîne $r < p$ et donc $p \nmid r$.
Or, $(\star) \iff ar = ap - aqc$ et donc p divise ar puisqu'on sait que p divise ac. Il suit que $r \in \Lambda$ ce qui est contradictoire avec le fait que c soit le plus petit élément de Λ.
Finalement, p divise a ou b. ■

Théorème
Tout nombre entier $n \geq 2$ admet une décomposition en produit de facteurs premiers.
De plus, cette décomposition est unique, à l'ordre des facteurs près.

Remarque : la démonstration qui suit est hors-programme.

Démonstration

— **Existence :** on procède par récurrence forte. C'est vrai pour $n = 2$, si c'est vrai pour tous les entiers de $[\![2; n]\!]$ (avec $n \geq 2$) alors soit $n+1$ est premier (et alors il est le produit d'un nombre premier : lui-même), soit il ne l'est pas et il existe deux entiers $(a, b) \in [\![2; n]\!]^2$ tels que $n + 1 = ab$. a et b ont une décomposition en produits de facteurs premiers, donc $n+1$ aussi. Finalement, tous les entiers ≥ 2 ont une décomposition en produit de facteurs premiers.

— **Unicité :** Soit $n \geq 2$, on note $p_1, \dots p_r$ les nombres premiers de $[\![2; n]\!]$. Supposons que n ait deux décompositions en produits de facteurs premiers :

$$n = \prod_{i=1}^{r} p_i^{\alpha_i} = \prod_{i=1}^{r} p_i^{\beta_i} \qquad \text{avec } \forall i \in [\![1; r]\!],\ \alpha_i \in \mathbb{N} \text{ et } \beta_i \in \mathbb{N}.$$

Supposons $\alpha_1 \neq \beta_1$, mettons $\alpha_1 > \beta_1$. On a alors, en divisant par $p_1^{\beta_1}$:

$$p_1^{\alpha_1 - \beta_1} \prod_{i=2}^{r} p_i^{\alpha_i} = \prod_{i=2}^{r} p_i^{\beta_i}$$

$\alpha_1 - \beta_1 > 0$ donc p_1 divise le membre de gauche de l'égalité précédente ; on en déduit qu'il divise le membre de droite, ce qui est absurde d'après le Lemme d'Euclide.
On procède de la sorte pour tous les indices $i \in [\![1; r]\!]$ et on obtient l'unicité de la décomposition en produits de facteurs premiers.

Remarque : un Lemme est un résultat intermédiaire qui sert à démontrer un résultat plus important.

Méthode
Pour simplifier une fraction d'entiers ou une racine carrée d'entiers, on écrit la décomposition des entiers en produits de facteurs premiers et les simplifications sont immédiates avec les règles $\sqrt{A^2B} = A\sqrt{B}$ et $\frac{AB}{AC} = \frac{B}{C}$ (où A, B et C désignent des entiers non nuls).

Exemples : $\sqrt{540} = \sqrt{3^3 \times 5 \times 2^2} = \sqrt{3^2 \times 2^2} \times \sqrt{3 \times 5} = 6\sqrt{15}$.

$$\frac{1400}{490} = \frac{2^3 \times 5^2 \times 7}{2 \times 5 \times 7^2} = \frac{2^2 \times 5}{7}.$$

Remarque : il n'existe pas d'algorithme performant pour trouver la décomposition d'un entier en produit de facteurs premiers.

5 PGCD, PPCM

Proposition
Soit a et b deux entiers naturels.
L'ensemble des diviseurs communs de a et de b est non vide (car il contient 1) et majoré (par $a+b$), il admet donc un plus grand élément qu'on appelle Plus Grand Diviseur Commun de a et b, qu'on note $\mathrm{PGCD}(a,b)$ ou $a \wedge b$.

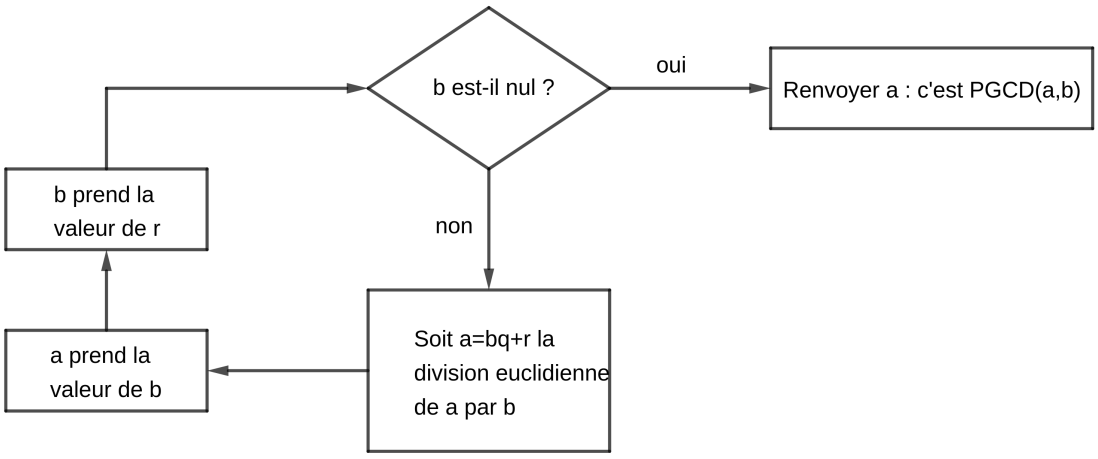
Exemple : $9 \wedge 12 = 3$; pour tout n, $0 \wedge n = n$; que vaut $708 \wedge 210$?

Méthode
$a \wedge b$ se déduit facilement des décompositions en produits de facteurs premiers de a et b.

Exemple : $708 \wedge 210 = 2^2 \times 3 \times 59 \wedge 2 \times 3 \times 5 \times 7 = 2 \times 3$.

Remarque : puisque la décomposition en produit de facteurs premiers est difficile à trouver, la méthode précédente n'est utile que pour des « petits » entiers.

Méthode (Algorithme d'Euclide pour calculer $a \wedge b$)
Entrée : a, b deux entiers naturels.
Sortie : $a \wedge b$.



Exemple : mise en œuvre pour calculer $72 \wedge 15$. On exécute l'algorithme et on indique l'état des variables au fur et à mesure de son exécution ; sur le côté on détaille ce qui s'est passé :

a	b	c
72	15	12
15	12	3
12	3	0
$\boxed{3}$	0	

$$\begin{aligned} 72 \wedge 15 &= (15 \times 4 + 12) \wedge 15 = 12 \wedge 15 \\ &= 15 \wedge 12 \\ &= (12 \times 1 + 3) \wedge 12 = 3 \wedge 12 \\ &= 12 \wedge 3 \\ &= (3 \times 4 + 0) \wedge 3 \\ &= \boxed{3} \end{aligned}$$

Définition
On dit que les entiers a et b sont premiers entre eux lorsque $a \wedge b = 1$.

Remarque : le théorème de Bézout assure que a et b sont premiers entre eux si, et seulement si, il existe des entiers u et v tels que $au + bv = 1$. De façon plus générale (et c'est également un théorème de Bézout), il existe toujours u et v tels que $au + bv = a \wedge b$.
Dans ce type d'égalités, u et v sont appelés *coefficients de Bézout*. Pour les trouver, on « remonte » l'algorithme d'Euclide. Sur l'exemple précédent, cela donne :

$$3 = 15 - 12 = 15 - (72 - 4 \times 15) = 5 \times 15 - 72 = 15 \times 5 + 72 \times (-1)$$

Définition
Soit a et b deux entiers naturels. On appelle Plus Petit Commun Multiple de a et b le plus petit élément de $\{n \in \mathbb{N} \ / \ a|n \text{ et } b|n\}$. On le note $\text{PPCM}(a, b)$ ou $a \vee b$.

Proposition
On a : $ab = (a \wedge b) \times (a \vee b)$.

Méthode (Pour déterminer le PPCM de a et b)
- On peut le déduire simplement des décompositions de a et b en produit de facteurs premiers ;
- A l'aide de la propriété précédente, en commençant par déterminer le PGCD à l'aide de l'algorithme d'Euclide.