5
Arithmétique

5.1 Objectifs

— Introduction au raisonnement dans $\mathbb{N}$.

— La *division Euclidienne* et la divisibilité

— Le PGCD : définition et propriétés et algorithme d'Euclide

— L'identité de Bézout et Théorème de Bézout.

— Application au théorème de Gauss et aux équations diophantiennes (lineáires)

5.2 Avant propos

L'arithmétique concerne l'étude des entiers naturels $\mathbb{N} = \{0,\ 1,\ 2,\ 3, ...\}$ ou relatifs $\mathbb{Z} = \{...,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3\ ...\}$. Ces ensembles discrets demandent plus d'intuition et de rigueur que le travail dans $\mathbb{R}$. Les trois principes suivant régissent ces ensembles, et on s'y appuiera pour les démonstrations tout au long du chapitre.

Axiome 5.1 — Principe des tiroirs. Si n chaussettes sont rangées dans m tiroirs, et si $m < n$, slors il y a un tiroir qui contient au moins deux chaussettes.

■ **Exemple 5.1**

Vous avez des chausses rouges, vertes et bleues dans un tiroir. Il fait noir. Combien de chaussettes doit-on prendre pour être sûr d'en avoir (au moins) deux de la même couleur ?

Axiome 5.2 — Principe du bon ordre. Toute partie non vide de $\mathbb{N}$ admet un plus petit élément

Corollaire 5.3 Le raisonnement par récurrence résulte du principe du bon ordre.

Démonstration. Si un sous-ensemble $E \subset \mathbb{N}$ vérifie les propriétés :

(i) $0 \in E$

(*ii*) hérédité : $\forall k \in \mathbb{N},\ k \in E \Rightarrow k+1 \in E$.

Pour montrer que $E = \mathbb{N}$, nous allons démontrer que le complémentaire de E est vide.

Raisonnons par l'absurde : Supposons qu'il n'est pas vide. D'après le *principe du bon ordre* le complémentaire de E admet *un plus petit élément* $n \notin E$.

■

Axiome 5.4 — Principe de descente infinie. Toute suite dams $\mathbb{N}$ strictement décroissante est nécessairement finie.

■ **Exemple 5.2** $\sqrt{2}$ est un irrationnel.

R Idée de la démonstration. Supposons que $\dfrac{p}{q} = \sqrt{2}$. Alors $p^2 = 2q^2$, et $p < q = \sqrt{2}p < 2p$

$$\sqrt{2} = \frac{p}{q} = \frac{p(p-q)}{q(p-q)} = \frac{p^2 - pq}{qp - q^2} = \frac{2q^2 - pq}{qp - q^2} = \frac{q(2q-p)}{q(p-q)} = \frac{2q-p}{p-q}.$$

Démonstration.

Raisonnons par l'absurde. Et supposons que $\sqrt{2} = \dfrac{p}{q}$, $p[$ et q entiers naturels.

Alors $\dfrac{p^2}{q^2} = 2$, donc $p^2 - 2q^2 = 0$.

1. On vérifie $q < p < 2q$.
2. On pose $p' = 2q - p$ et $q' = p - q$. p' et $q' \in \mathbb{N}$.
   a) $q' = p - q = q - \underbrace{(2q-p)}_{>0} < q$
   b) $p'^2 - 2q'^2 = (2q-p)^2 - 2(p-q)^2 = 2q^2 - p^2 = 0$
3. On peut donc créer une suite infinie q strictement décroissante tels que $p^2 - 2q^2 = 1$.

Ceci est impossible par le principe de descente infinie. ■

■ **Exemple 5.3** Pour $r \in \mathbb{N}$, il y a deux possiblités :

1. $\sqrt{r} \in \mathbb{N}$, la racine est entière.
2. $\sqrt{r} \notin \mathbb{Q}$, la racine est un irrationnel.

R Si $\sqrt{r} \notin \mathbb{N}$, on pose $a = \lfloor \sqrt{r}$ (la partie entière de $\sqrt{r}$).

Supposons alors que $\dfrac{p}{q} = \sqrt{r}$ alors $p^2 = \ldots\ldots$ et $ap < q = \sqrt{r}p < \ldots\ldots\ldots q$.

$$\sqrt{r} = \frac{p}{q} = \frac{p(p-aq)}{q(p-aq)} =$$

5.3 Division euclidienne

Théorème 5.5 — Division euclidienne dans $\mathbb{Z}$. Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$.

Il existe un *unique* couple d'entier q et r tel que :

$$a = bq + r \qquad \text{avec} \quad 0 \leqslant r < b$$

Cette relation est la *division euclidienne* de a par b.

— q est appelé le *quotient* de la division euclidienne de a par b.

— r est appelé le *reste* de la division euclidienne de a par b.

R Le théorème 5.5 laisse la possibilité que a soit négatif à la condition que le reste r est positif ou nul sinon, plusieurs valeurs peuvent correspondre :

$-14 = 3(-3) + (-5)$ ici $r = -5 < 3$, le quotient est donc -5 et le reste est $r = 1$.

$-14 = 3(-4) + (-2)$ ici $r = -2 < 3$

$-14 = 3(-5) + (1)$ ici $0 \leqslant r = 1 < 3$

■ **Exemple 5.4**

1. La division euclidienne de 412 par 15 est $412 = 15 \times 27 + 7$.
2. La division euclidienne de -412 par 15 est : $-412 = -15 \times 27 - 7 = -16 \times 27 + 8$

Démonstration.

1. **Existence** On pose $E = \{a - bx \mid \quad x \in \mathbb{Z} \quad \text{et} \quad a - bx \geqslant 0\}$.

   a) *Affirmation : « E n'est pas vide »*. Pour $x = -|a|$, on a $a - bx = a + b|a| \geqslant 0$. En effet :

   $\therefore a - bx \in E$.

   b) *Affirmation : « il existe q et r tel que $a = bq + r$ avec $r \geqslant 0$ »*. En effet :

c) *Affirmation :* « $r < b$ ». Démonstration par l'absurde :

Supposons le contraire $r \geqslant b$.

2. **Unicité** Supposons que deux couples (q, r) et (q', r') vérifient :

   (i) $a = bq + r$ avec $0 \leq r < b$.

   (ii) $a = bq' + r'$ avec $0 \leq r' < b$.

$\therefore r = r'$ et $q = q'$. ■

R La démonstration du manuel n'est pas satisfaisante. Elle repose sur l'existence et l'unicité de la partie entière d'un réel x. Ceci se démontre à partir du principe du bon ordre comme précédemment !

■ Exemple 5.5

Le reste de la division de a par b est 8. Le reste de la division de $2a$ par b est 5. Déterminer b.

solution.

$a = bq + 8$ avec $b > 8$, donc $2a = 2bq + 16$.

et $2a = bq' + 5$ avec $b > 5$.

Donc $2bq + 16 = bq' + 5 \iff b(2q - q') = -11 \iff b(q' - 2q = 11)$ et $b > 8$.

b est un diviseur de 11 supérieur à 8, donc $b = 11$. ■

5.4 Divisibilité dans $\mathbb{Z}$

Définition 5.1 — diviseurs et multiples. Soient a et $b \in \mathbb{Z}$.

On dit que « b divise a », noté $b \mid a$ s.s.i $\exists k \in \mathbb{Z}$ tel que $a = kb$.

R Autres formulations possibles « b est un *diviseur* de a » ou « a est un *multiple* de b ».

Proposition 5.6 $b \mid a \iff$ le reste de la division de a par b est nul.

Démonstration. La division Euclidienne de a par b est $a = bq + r$.

■

■ **Exemple 5.6**

1. $3 \mid 24$ car $24 = 3(8)$ mais $3 \nmid 17$.
2. $-6 \mid 54$ car $54 = (-6)(-9)$.
3. Les diviseurs de 6 dans $\mathbb{Z}$ sont 1, 2, 3, 6 ainsi que -1, -2, -3 et -6.
4. $5\mathbb{Z} = \{\ldots; -15; -10; -5; 0; 5; 10; \ldots\}$ est l'ensemble des multiples de 5

■ **Exemple 5.7 — 0 est un multiple universel.** Il est divisible par tout entier relatif n car $0 = 0(n)$

■ **Exemple 5.8 — 1 est un diviseur universel.** Il divise tout entier relatif n car $n = 1(n)$.

R a et $-a$ ont les mêmes diviseurs, en effet :

Si $b \mid a$, alors pour un certain entier c, $a = bc$, donc $-a = b(-c)$ donc $b \mid -a$.

Similairement, si $b \mid -a$, alors $b \mid a$.

Lemme 5.7 Soit $a \neq 0$. Si $b \mid a$ alors $|b| \leqslant |a|$

Démonstration.

■

Propriétés 5.8

(i) Tout diviseur positif d'un entier $a \neq 0$ est inférieur ou égal à $|a|$.

(ii) Le nombre de diviseurs d'un entier $a \neq 0$ est fini.

Propriétés 5.9 Soient a, b et $c \in \mathbb{Z}$.

transitivité Si $a \mid b$ et $b \mid c$, alors $a \mid c$.

combinaison linéaire Si $a \mid b$ et $a \mid c$, alors $a \mid mb + nc$ où m et n sont deux entiers relatifs.

R En particulier, si $a \mid b$ alors $a \mid a+b$ et $a \mid a-b$.

Démonstration. Soient a, b et c trois nombres relatifs.

transitivité

combinaison linéaire

∎

■ **Exemple 5.9** 19 divise 38 et 38 divise 114 donc 19 divise 114.

■ **Exemple 5.10 — un algorithme de collège.**

```
Entrée : a entier positif, liste L vide.
b ← 1
tant que b ⩽ a :
    r ← a (mod b)   # reste de la division de a par b
    si r = 0 :
        ajouter b à L
    fin si
    b ← b + 1
fin tant que
Retourne : liste L des diviseurs de a
```

en langage Python (lien basthon)

```python
def diviseurs( a ) :
    L = []
    b = 1
    while b <= a :
        if a % b == 0 :
            L.append(b)
        b = b + 1
    return L
```

5.5 Le PGCD

Définition 5.2 — définition faible du PGCD. a et $b \in \mathbb{Z}$.

Le *plus grand commun diviseur* de a et b est le plus grand entier d qui divise a et b :

(i) $d \mid a$ et $d \mid b$

(ii) Si $c \mid a$ et $c \mid b$ alors $c \leqslant d$.

Le PGCD de a et b est usuellement noté $\operatorname{pgcd}(a, b) = a \wedge b$.

Démonstration. Si a et b ne sont pas tous les deux nuls

1 est un diviseur commun à a et b (diviseur universel)

L'ensemble des diviseurs de a, et l'ensemble des diviseurs de b sont finis.

L'ensemble des diviseurs communs de a et b est fini, et non vide.

Il existe un unique plus grand élément diviseurs de a et b, de plus $\operatorname{pgcd}(a, b) \geqslant 1$. ∎

Définition 5.3 Deux entiers a et b sont dits premiers entre eux si $\operatorname{pgcd}(a, b) = 1$.

■ **Exemple 5.11**

Les diviseurs de 12 sont : $\{1;\ -1;\ 2;\ -2;\ 3;\ -3;\ 4;\ -4;\ 6;\ -6;\ 12;\ -12\}$.

Les diviseursde 30 sont : $\{1;\ -1;\ 2;\ -2;\ 3;\ -3;\ 5;\ -5;\ 6;\ -6;\ 10;\ -10;\ -15;\ 15;\ 30;\ -30\}$

Les diviseurs communs de 12 et 30 sont $\{1;\ -1;\ 2;\ -2;\ 3;\ -3;\ 6;\ -6;\}$.

Le plus grand commun diviseur de 12 et 30 est $\operatorname{pgcd}(12; 30) = 12 \wedge 30 = 6$.

Propriétés 5.10

(i) $\operatorname{pgcd}(a; b) = \operatorname{pgcd}(|a|; |b|)$.

(ii) $\operatorname{pgcd}(a; 0) = a \wedge 0 = |a|$.

(iii) Si $b \mid a$, alors $\operatorname{pgcd}(a; b) = |b|$.

Démonstration.

∎

Lemme 5.11 — d'Euclide. Si r est le reste de la division de a par b, alors $\text{pgcd}(a;b) = \text{pgcd}(b;r)$.

Démonstration. (*par double inégalité*) La division Euclidienne de a par b est $a = qb + r$.

1. $\text{pgcd}(a;b) \geqslant \text{pgcd}(b;r)$. En effet :

2. $\text{pgcd}(a;b) \leqslant \text{pgcd}(b;r)$. En effet :

■

Définition 5.4 — Algorithme d'Euclide. est un algorithme permettant de calculer le pgcd de deux entiers naturels a et b :

```
Entrée : a, b, entiers positifs
Sortie : le pgcd(a;b)
tant que b > 0 :
    r ← a (mod b)    # reste de la division de a par b
    (a , b ) ← (b , r)
fin tant que
Retourne : a
```

en langage Python (lien basthon)

```python
def pgcd( a , b ) :
    while b > 0 :
        r = a % b
        a , b = b , r
    return a
```

■ **Exemple 5.12** Calcul de proche en proche du $\text{pgcd}(524;148)$

$$\begin{aligned}
\text{pgcd}(524;148) & & 524 = 148 \times 3 + 80 \\
= \text{pgcd}(148;80) & & 148 = 80 \times 1 + 68 \\
= \text{pgcd}(80;68) & & 80 = 68 \times 1 + 12 \\
= \text{pgcd}(68;12) & & 68 = 12 \times 5 + 8 \\
= \text{pgcd}(12;8) & & 12 = 8 \times 1 + 4 \\
= \text{pgcd}(8;4) & & 8 = 4 \times 2 \\
= \text{pgcd}(4;0) = 4 & &
\end{aligned}$$

Démonstration.

La suite des restes (r_n) obtenus par l'algorithme d'Euclide est strictement décroissante dans $\mathbb{N}$. D'après le principe de la descente infinie, il existe un rang n tel que $r_n = 0$. L'algorithme d'Euclide se termine, et de proche en proche le dernier reste non nul est le pgcd. ■

Théorème 5.12 — Identité de Bachet-Bézout. Soit a et b entiers.

Si $d = \text{pgcd}(a, b)$ alors il existe un couple d'entiers relatifs $(u\ ;\ v)$ tels que $au + bv = d$

R Le théorème ne dit pas que le couple u et v est unique. Par exemple pour $a = 2$ et $b = 3$, $d = \text{pgcd}(2; 3) = 1$ et on a : $-1(2) + 1(3) = 1$ et $-4(2) + 3(3) = 1$.

R Le théorème ne dit pas non plus que « s'il existe deux entiers u et v tel que $d = au + bv$ alors d est le $\text{pgcd}(a, b)$ ». Ceci est d'ailleurs faux : $-1(2) + 2(3) = 4$ mais $\text{pgcd}(2; 3) = 1 \neq 4$.

Démonstration. Supposons a et b non tous les deux nuls, $d = \text{pgcd}(a, b) \geqslant 1$

On pose $E = \{ax + by \mid \quad x, y \in \mathbb{Z} \quad \text{et} \quad ax + by > 0\}$:

1. *Affirmation :* « E n'est pas vide et admet un plus petit élément non nul e ». En effet :

   $a^2 + b^2 > 0$ en prenant $x = a$ et $x = b$. E n'est pas vide.

   D'après le principe du bon ordre, il admet un plus petit élément $e = ax_0 + by_0 > 0$.

2. *Affirmation :* « $e \mid a$ et $e \mid b$ ». En effet :

3. *Affirmation :* « tout diviseur commun c de a et b vérifie $c \leqslant e$ ». En effet :

   Les deux dernières affirmations impliquent que $e = \text{pgcd}(a, b)$. ■

Théorème 5.13 — de Bézout. a et b sont premiers entre eux, si et seulement si, il existe deux entiers relatifs u et v tels que $au + bv = 1$:

$$\text{pgcd}(a; b) = 1 \iff \exists u, v \in \mathbb{Z} \quad au + bv = 1$$

Démonstration.

1. Sens direct $(\Rightarrow)$ conséquence de l'identité de Bachet-Bézout.
2. Sens indirect $(\Leftarrow)$. Il existe u et v tel que $au + bv = 1$.

$d = \text{pgcd}(a; b)$, $d \mid a$ et $d \mid b$, donc $d \mid au + bv$ et $d \mid 1$ i.e. $d = 1$. ■

■ **Exemple 5.13 — Méthode de Bézout.** permet de déterminer un tel couple $(u\ ;\ v)$.

Reprenons notre exemple $4 = \text{pgcd}(524; 148)$:

On commence par les deux premières lignes :

$$\begin{aligned}
1(524) + 0(148) &= 524 \\
0(524) + 1(148) &= 148 && 80 = 524 - 148 \times 3 \\
1(524) - 3(148) &= 80 && 68 = 148 - 80 \times 1 \\
-1(524) + 4(148) &= 68 && 12 = 80 - 68 \times 1 \\
2(524) - 7(148) &= 12 && 8 = 68 - 12 \times 5 \\
-11(524) + 39(148) &= 8 && 4 = 12 - 8 \times 1 \\
13(524) - 46(148) &= 4
\end{aligned}$$

■ **Exemple 5.14** Utiliser le théorème de Bézout pour démontrer que $2n+1$ et $9n+4$ sont premiers entre eux.

solution. Par la méthode de Bézout :

$$\begin{aligned}
1(9n+4) + 0(2n+1) &= 9n+4 \\
0(9n+7) + 1(2n+1) &= 2n+1 && n = (9n+4) - (2n+1) \times 4 \\
1(9n+4) - 4(2n+1) &= n && 1 = (2n+1) - n \times 2 \\
-2(9n+4) + 9(2n+1) &= 1
\end{aligned}$$

D'après le théorème de Bézout, $(2n+1)$ et $(9n+4)$ sont premiers entre eux. ■

Définition 5.5 — définition forte du pgcd. a et b deux nombres entiers.

Le plus grand commun diviseur de a et b (au sens de la définition 5.2) est l'entier d tel que :

(i) $d \mid a$ et $d \mid b$ et $d \geqslant 0$.

(ii) Si $c \mid a$ et $c \mid b$ alors $c \mid d$. (tout diviseur commun à a et b divise aussi d)

Démonstration.

1. (caractérisation forte $\Rightarrow$ faible) D'après la caractérisation forte, d est un diviseur et tous les autres diviseurs communs de a et de b le divise aussi, donc lui sont inférieurs.
2. (caractérisation faible $\Rightarrow$ forte) Si d est le pgcd. D'après le théorème de Bézout, il existe u et v entiers tels que $au + bv = d$.

   Si un entier $c \mid a$ et $c \mid b$ alors $c \mid au + bv$ donc divise d

■

Proposition 5.14 — homogénéité du pgcd. $\text{pgcd}(ka; kb) = k\,\text{pgcd}(a; b)$.

Démonstration. laissé en exercice ■

5.6 Applications du théorème de Bézout

Théorème 5.15 — de Gauss. a, b et $c \in \mathbb{Z}$.

Si $a \mid bc$ et $\text{pgcd}(a;b) = 1$ alors $a \mid c$

Corollaire 5.16 a et b entiers. p un nombre premier.

Si $p \mid ab$ alors $p \mid a$ ou $p \mid b$.

Démonstration.

$\text{pgcd}(a;b) = 1$, il existe u et v tel que $au + bv = 1.$

$$\left.\begin{aligned} au + bv &= 1 \\ acu + bcv &= c \end{aligned}\right) c$$

$a \mid bc$ et $a \mid ac$, donc a divise la combinaison $acu + bcv = c$ ■

■ **Exemple 5.15** Déterminer les couples d'entiers solutions de l'équation $(E)\colon 5(x-1) = 7y$

solution.

Si $5(x-1) = 7y$, alors $5 \mid (7y)$, or $\text{pgcd}(5;7) = 1$, donc $5 \mid y$

Il existe $k \in \mathbb{Z}$ tel que $y = 5k$. En remplaçant dans (E) : $5(x-1) = 35k$, $x = 7k + 1$.

Les solutions sont les couples de la forme $(x = 7k + 1; y = 5k)$ ou $k \in \mathbb{Z}$. ■

Une *équation diphantienne* est une équation polynomiale à une ou plusieurs inconnues, à coefficients entiers dont on cherche les solutions parmi les nombres entiers.

Proposition 5.17

L'équation diophantienne $ax + by = c$ d'inconnues x et y, admet des solutions entières si et seulement si c est un multiple du $\text{pgcd}(a,b)$

Démonstration. On pose $d = \text{pgcd}(a,b)$

1. Supposons c est un multiple de d. Il existe $k \in \mathbb{N}$, tel que $c = kd$.

   D'après l'identité de Bézout, il existe u et v tel que $au + bv = d$. Et alors $aku + bkv = kd = c$.

   $x = ku$ et $y = kv$ est un couple solution de l'équaiont $ax + by = c$.
2. Supposons que $ax + by = c$ admet un couple solution x_0 et y_0.

   Le pgcd $d \mid a$ et $d \mid b$, donc d divise la combinaison linéaire $ax + by = c$.

■

■ **Exemple 5.16**

1. $4x + 9y = 2$ admet des solutions car $\text{pgcd}(4; 9) = 1$ et 1 divise 2.
2. $9x - 15y = 2$ n'adment pas de solution car $\text{pgcd}(9; 15) = 3$ et 3 ne divise pas 2.

R Soit une équation diophantienne $ax + by = c$ tel que $d = \text{pgcd}(a; b)$ divise c. En divisant les deux membres par d, on se ramène au cas $a'x + b'y = c'$ avec $\text{pgcd}(a'; b') = 1$.

■ **Exemple 5.17 — résolution d'une équation diophantienne $ax + by = c$ avec $\text{pgcd}(a; b) = 1$.** Résoudre dans $\mathbb{Z}$ l'équation (E): $17x - 33y = 1$.

Démonstration.

1. *Déterminer un couple solution de* (E) *(solution évidente ou par Méthode de Bézout)*

   $17(2) - 33(1) = 1$, le couple $x = 2$ et $y = 1$ est *solution particulière*
2. Soit $(x; y)$ un couple solution quelconque.
   $$\begin{cases} 17x - y = 1 \\ 17(2) - 33(1) = 1 \end{cases} \Rightarrow \quad 17(x-2) - 33(y-1) = 0 \quad \Rightarrow \quad 17(x-2) = 33(y-1)$$
   $33 \mid 17(x - 2)$, or $\text{pgcd}(33; 17) = 1$. D'après le théorème de Gauss, $33 \mid (x - 2)$

   Il existe $k \in \mathbb{Z}$ tel que $x - 2 = 33k$.

   Par substitution, $y - 1 = 17k$. Les solutions de (E) sont nécessairement de la forme $(x = 2 + 33k \; ; \; y = 1 + 17k)$
3. *Vérifier que tous les couples de la forme* $(x = 2 + 33k \; ; \; y = 1 + 17k)$ sont solution de (E) [1] :

   $17(2 + 33k) - 33(1 + 17k) = 34 + 561k - 33 - 561k = 1$.

■

1. En effet, nous avons uniquement établi une condition nécessaire.