Étude de $\mathbb{N}$ et $\mathbb{Z}$

(Spécialité Maths) Terminale S

Dernière mise à jour : Jeudi 22 Novembre 2007

Vincent OBATON, Enseignant au lycée Stendhal de Grenoble (Année 2007-2008)

J'aimais et j'aime encore les mathématiques pour elles-mêmes comme n'admettant pas l'hypocrisie et le vague, mes deux bêtes d'aversion.

Stendhal

Table des matières

1 Quelques rappels

1.1 L'ensemble des entiers naturels ($\mathbb{N}$)

1.1.1 Définition

Définition :

$$\mathbb{N} = \{0; 1; 2; 3; 4; 5; 6; \ldots\}$$

C'est l'ensemble de tous les entiers positifs auquel on ajoute 0.

1.1.2 Propriétés

(P_1) : $\mathbb{N}$ est stable pour l'addition et la multiplication seulement.

$$\forall x \in \mathbb{N}, \forall y \in \mathbb{N}, \ , \ x + y \in \mathbb{N} \text{ et } x \times y \in \mathbb{N}$$

Par contre $\mathbb{N}$ n'est pas stable pour la soustraction et la division.
Exemples :
- $(+1) - (+3)$ n'existe pas dans $\mathbb{N}$
- $\dfrac{+1}{+3}$ n'existe pas dans $\mathbb{N}$

1.1.3 Quelques axiomes

Le mot axiome vient du grec $\alpha\xi\iota\omega\mu\alpha$ (axioma), qui signifie "qui est considéré comme digne ou convenable" ou "**qui est considéré comme évident en soi**". Pour certains philosophes grecs de l'antiquité cela représentait une affirmation qu'ils considéraient comme évidente et qui n'avait nul besoin de preuve.

$\boxed{A_1}$: Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

$\boxed{A_2}$: Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.

$\boxed{A_3}$: Toute suite d'entiers naturels strictement décroissante est finie.

$\boxed{A_4}$: Toute suite d'entiers relatifs négatifs strictement croissante est finie.

1.2 L'ensemble des entiers relatifs ($\mathbb{Z}$)

1.2.1 Définition

Définition :

$$\mathbb{Z} = \{\ldots; -6; -5; -4; -3; -2; -1; 0; 1; 2; 3; 4; 5; 6; \ldots\}$$

C'est l'ensemble de tous les entiers positifs et négatifs auquel on ajoute 0.

1.2.2 Propriétés

(P_1) : $\mathbb{Z}$ est stable pour l'addition, la soustraction et la multiplication seulement.

$$\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z},\ , x+y \in \mathbb{Z}\ , x-y \in \mathbb{Z}\ , x \times y \in \mathbb{Z}$$

Par contre $\mathbb{Z}$ n'est pas stable pour la division.
Exemple :
- $\dfrac{+1}{+3}$ n'existe pas dans $\mathbb{Z}$

(P_2) : Tout nombre de $\mathbb{Z}$ admet un opposé dans $\mathbb{Z}$

$$\forall x \in \mathbb{Z}, -(x) \in \mathbb{Z}$$

(P_3) : $\mathbb{N} \subset \mathbb{Z}$

$$\forall x \in \mathbb{N}, x \in \mathbb{Z}$$

1.2.3 Quelques axiomes

Le mot axiome vient du grec $\alpha\xi\iota\omega\mu\alpha$ (axioma), qui signifie "qui est considéré comme digne ou convenable" ou "**qui est considéré comme évident en soi**". Pour certains philosophes grecs de l'antiquité cela représentait une affirmation qu'ils considéraient comme évidente et qui n'avait nul besoin de preuve.

Attention, les axiomes précédents $\boxed{A_1}$ et $\boxed{A_3}$ sont faux dans $\mathbb{Z}$.

$\boxed{A_2}$: Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.

2 Divisibilité dans $\mathbb{Z}$

2.1 Multiples d'un entier relatif

On note n et m deux entiers relatifs.
Définition :

On dit que m **est un multiple de** n si, et seulement si, il existe un nombre entier relatif quelconque k tel que $m = k \times n$.

Exemples :

1. Les multiples de 7 sont : $\{\ldots; -21; -14; -7; 0; 7; 14; 21; \ldots\}$
2. Les multiples de -2 sont : $\{\ldots; -6; -4; -2; 0; 2; 4; 6; \ldots\}$

2.2 Diviseurs d'un entier relatif

On note n et m deux entiers relatifs.
Définition :

On dit que n **divise** m (que n **est un diviseur de** m) si, et seulement si , il existe $k \in \mathbb{Z}$ tel que $m = k \times n$. (m est un multiple de n)

On note $n|m$ pour dire que n **divise** m.
Remarques :
– $\forall a \in \mathbb{Z}$, $1|n$ et $-1|n$.
– $\forall a \in \mathbb{Z}$, $a|0$
– $\forall a \in \mathbb{Z}$, a admet au moins 4 diviseurs $\{1; -1; a; -a\}$

2.3 Propriétés sur la divisibilité

Dans toute cette partie, $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $c \in \mathbb{Z}$.

$$(P_1) : b|a \Rightarrow -b|a.$$

Démonstration : (A faire par les élèves)
Si $b|a$ alors il existe $k \in \mathbb{Z}$ tel que a=k$\times b$ alors a=(-k)$\times(-b)$ avec $-k \in \mathbb{Z}$ donc $-b|a$

$$(P_2) : b|a \text{ et } a \neq 0 \Rightarrow |b| \leq |a|.$$

Démonstration : (A faire par les élèves)
Si $b|a$ alors il existe $k \in \mathbb{Z}$ tel que $a = kb$ donc $|a| = |kb| = |k||b|$
or $k \in \mathbb{Z}$ donc $|k| \in \mathbb{N}$
comme $a \neq 0$ alors $k \neq 0$ et donc $|k| \geq 0$
donc $|a| = |k||b| \geq |1||b|$ donc $|a| \geq |b|$

$$(P_3) : b|a \text{ et } a|c \Rightarrow b|c.$$

Démonstration : (A faire par les élèves)
Si $b|a$ alors il existe $k_1 \in \mathbb{Z}$ tel que $a = k_1 \times b$
Si $a|c$ alors il existe $k_2 \in \mathbb{Z}$ tel que $c = k_2 \times a$
donc
$c = k_2 \times a = k_2 k_1 \times b$ avec $k_1 k_2 \in \mathbb{Z}$ donc $b|c$

$$(P_4) : b|a \text{ et } a|b \Rightarrow a = b \text{ ou } a = -b.$$

Démonstration : (A faire par les élèves)
Si $b|a$ alors $|b| \leq |a|$
Si $a|b$ alors $|a| \leq |b|$
donc on a $|a| = |b|$ et donc $a = b$ ou $a = -b$

$$(P_5) : b|a \text{ et } b|c \Rightarrow \forall (u,v) \in \mathbb{Z}^2 \ b|(ua+vc).$$

On dit que si $b|a$ et $b|c$ alors b divise toute **combinaison linéaire** de a et c.
Démonstration : (A faire par les élèves)
Si $b|a$ alors il existe $k_1 \in \mathbb{Z}$ tel que $a = k_1 \times b$
Si $b|c$ alors il existe $k_2 \in \mathbb{Z}$ tel que $c = k_2 \times b$
alors pour tout $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ on a :
$ua + vc = u(k_1 \times b) + v(k_2 \times b) = uk_1b + vk_2b = (uk_1 + vk_2)b$
Or $uk_1 + vk_2 \in \mathbb{Z}$ donc $b|(ua + vc)$

$$(P_6) : b|a \Rightarrow \forall c \in \mathbb{Z} \ b|ac.$$

Démonstration : (A faire par les élèves)
Si $b|a$ alors il existe $k \in \mathbb{Z}$ tel que $a = kb$
donc pour tout $c \in \mathbb{Z}$ $ac = kbc = (kc)b$ avec $kc \in \mathbb{Z}$ donc $b|ac$

$$(P_7) : b|a \Rightarrow \forall c \in \mathbb{Z} \ bc|ac.$$

Démonstration : (A faire par les élèves)
Si $b|a$ alors il existe $k \in \mathbb{Z}$ tel que $a = kb$
donc pour tout $c \in \mathbb{Z}$ on a $ac = kbc$ donc $bc|ac$

3 La division Euclidienne

3.1 La division Euclidienne dans $\mathbb{N}$

On note $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$

3.1.1 Théorème

Il existe un couple unique (q, r) d'entiers naturels tels que :
$a = bq + r$ et $0 \leq r < b$

3.1.2 Définition

Dans ce cas on dira que q est **le quotient** et r est **le reste** de **la division Euclidienn**e de a par b.

Exemple : $17 = 5 \times 3 + 2$ donc 3 est le quotient et 2 est le reste de la division Euclidienne de 17 par 5.

3.1.3 Démonstration

1. Existence du couple (q, r) :
   La démonstration repose sur le fait que $\mathbb{N}$ est **archimédien**.

> $\mathbb{N}$ est archimédien :
> On note $b \in \mathbb{N}^*$
> Pour tout $a \in \mathbb{N}$, $\exists n \in \mathbb{N}$ tel que $a < nb$
> **Traduction** : On peut rendre le produit nb aussi grand que l'on veut pourvu que n soit suffisamment grand

   Soit a un entier naturel et b un entier naturel non nul.
   Comme $\mathbb{N}$ est archimédien, l'ensemble des entiers naturels n tels que $a < nb$ n'est pas vide.
   D'après l'axiome $\boxed{A_1}$, cet ensemble admet un plus petit élément qu'on nomme k avec $k \neq 0$
   On a donc $k - 1 \in \mathbb{N}$ et $(k-1)b \leq a < kb$
   On pose $q = k - 1$ et on en déduit que $qb \leq a < (q+1)b$ et donc que
   $qb - qb \leq a - qb < qb + b - qb$ et donc $0 \leq a - qb < b$
   On pose donc $r = a - qb$ et on a bien $a = qb + r$ avec $0 \leq r < b$
2. Unicité du couple (q, r) :
   On suppose qu'il existe deux couples (q_1, r_1) et (q_2, r_2) tels que
   $a = bq_1 + r_1$ avec $0 \leq r_1 < b$
   et
   $a = bq_2 + r_1 2$ avec $0 \leq r_2 < b$
   alors $\mathrm{r}_2 - r_1 = b(q_1 - q_2) et$-$\mathrm{b}<\mathrm{r}_2 - r_1 < b$.
   On a donc $r_2 - r_1$ est un multiple de b strictement compris entre $-b$ et b.
   Donc $r_2 - r_1 = 0$ et donc $r_2 = r_1$.
   Si $r_2 = r_1$ alors $q_1 = q_2$ et donc les couples sont identiques.

3.2 La division Euclidienne dans $\mathbb{Z}$

On note $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$

3.2.1 Théorème

> Il existe un couple unique (q, r) d'entiers relatifs tels que :
> $a = bq + r$ et $0 \leq r < |b|$
> Remarque : r est toujours positif.

3.2.2 Définition

> Dans ce cas on dira que q est **le quotient** et r est **le reste** de **la division Euclidienn**e de a par b.

3.2.3 Démonstration

1. Existence du couple (q, r) :
   Soit a un entier relatif et b un entier relatif non nul.
   L'ensemble des entiers naturels n tels que $a + |b|n \geq 0$ n'est pas vide.
   Dans le cas contraire la suite $(a + |b|k)_{k \in \mathbb{N}}$ serait strictement croissante et

incluse dans $\mathbb{Z}^-$ (Voir axiome $\boxed{A_4}$).
Le nombre $a+|b|n$ est dans $\mathbb{N}$ donc d'après le paragraphe précédent, il existe un unique couple (q',r') tel que :
$a+|b|n = |b|q'+r'$ avec $0 \leq r' < |b|$
donc $a = |b|(q'-n)+r' = b\dfrac{|b|}{b}(q'-n)+r' = bq+r$ avec $q = \dfrac{|b|}{b}(q'-n)$ et $r = r'$

2. Unicité du couple (q,r) :
On suppose qu'il existe deux couples (q_1,r_1) et (q_2,r_2) tels que
$a = bq_1+r_1$ avec $0 \leq r_1 < |b|$
et
$a = bq_2+r_12$ avec $0 \leq r_2 < |b|$
alors $r_2-r_1 = b(q_1-q_2)$ et $-|b| < r_2-r_1 < |b|$.
On a donc r_2-r_1 est un multiple de b strictement compris entre $-|b|$ et $|b|$.
Donc $r_2-r_1 = 0$ et donc $r_2 = r_1$.
Si $r_2 = r_1$ alors $q_1 = q_2$ et donc les couples sont identiques.

3.3 Exemples

1. Division Euclidienne de -38 par 5
$-38 = 5\times(-8)+2$
2. Division Euclidienne de -126 par -7
$-126 = -7\times 19+7$

3.4 Application au changement de système de numération

En base 10 les nombres peuvent s'écrire à l'aide des puissances de 10 :

$$x = a_n.10^n + a_{n-1}.10^{n-1} + \ldots + a_1.10 + a_0$$

On peut écrire le même nombre en base 2 ou 3 ou 16 etc ... Par exemple, en base 2 les nombres s'écrivent à l'aide des puissances de 2.

$$x = b_n.2^n + b_{n-1}.2^{n-1} + \ldots + b_1.2 + b_0$$

Le système binaire (base 2) est fondamental pour l'éléctronique ou en informatique car il se compose que de deux caractères 0 et 1.(Le courant passe ou ne passe pas)
Pour passer du système décimal (base 10) au système binaire (base 2) on utilise la division euclidienne par 2.

Exemple : On souhaite convertir 234 en base 2.
$234 = 117\times 2+\mathbf{0}$
$117 = 58\times 2+\mathbf{1}$
$58 = 29\times 2+\mathbf{0}$
$29 = 14\times 2+\mathbf{1}$
$14 = 7\times 2+\mathbf{0}$
$7 = 3\times 2+\mathbf{1}$
$3 = 1\times 2+\mathbf{1}$
$1 = 0\times 2+\mathbf{1}$
donc en écriture binaire 234 est 11101010.
et $234 = 1\times 2^7+1\times 2^6+1\times 2^5+0\times 2^4+1\times 2^3+0\times 2^2+1\times 2^1+0\times 2^0$

Exemple : On souhaite convertir 234 en base 5.
$234 = 46\times 5+4$
$46 = 9\times 5+1$
$9 = 1\times 5+4$

$1 = 0 \times 5 + 1$
donc en base cinq 234 est 1414
et $234 = 1 \times 5^3 + 4 \times 5^2 + 1 \times 5^1 + 4 \times 5^0$

Exemple : On souhaite convertir 234 en base 16 (hexadécimale).
On dispose dans cette base de 16 symboles :$0; 1; 2; 3; 4; 5; 6; 7; 8; 9; A; B; C; D; E; F$
$234 = 14 \times 16 + 10$
$14 = 0 \times 16 + 14$
donc en base hexadécimale 234 est EA et donc prend beaucoup moins de mémoire que 234 ou 1414 ou 11101010 La base hexadécimale est utilisée en informatique.

4 Congruence dans $\mathbb{Z}$

4.1 Définition

On note $n \geq 2$ un entier naturel et a et b deux entiers relatifs
On dit que a et b sont **congrus modulo** n et on note $a \equiv b[n]$
si les divisions euclidiennes de a et de b par n ont le même reste.

Exemples : $33 \equiv 13(5)$ $29 \equiv -121(5)$ $-623 \equiv 17(10)$

4.2 Propriétés

On note n et n' deux entiers naturels tels que $n \geq 2$ et $n' \geq 2$
On note a et b deux entiers relatifs

$$(P_1) : a \equiv b[n] \Leftrightarrow n|(a-b)$$

Démonstration :
⇝ Si $a \equiv b[n]$ alors il existe un unique couple (q, r) d'entiers tel que $a = qn + r$ avec $0 \leq r < n$ et un unique couple (q', r) d'entiers tel que $b = q'n + r$ avec $0 \leq r < n$
donc $a - b = qn + r - q'n - r = n(q - q')$ donc $n|(a - b)$
⇝ Si $n|(a - b)$ alors il existe $k \in \mathbb{N}$ tel que $a - b = kn$.
D'après la division euclidienne, il existe un couple unique (q, r) d'entiers tel que $a = qn + r$ avec $0 \leq r < n$ et un couple (q', r') d'entiers tel que $b = q'n + r'$ avec $0 \leq r' < n$.
Donc $a - b = n(q - q') + (r - r')$ avec $-n < r - r' < n$
Comme $a - b$ est un multiple de n alors $r - r'$ est un multiple de n.
Or $r - r' \in \mathbb{N}$ et le seul entier multiple de n dans $]-n, n[$ est 0
donc $r - r' = 0$ donc $r = r'$ et donc $a \equiv b[n]$

$$(P_2) : a \equiv 0[n] \Leftrightarrow n|a$$

Démonstration :
C'est un cas particulier de la propriété précédente (P_1) pour $b = 0$.

(P_3) : Si $n'|n$ alors $a \equiv b[n] \Rightarrow a \equiv b(n')$

Démonstration :
Si $n'|n$ alors il existe $k \in \mathbb{N}$ tel que $n = k \times n'$ alors :
➳ Si $a \equiv b[n]$ alors il existe $p \in \mathbb{N}$ tel que $a = b + pn$ donc $a = b + p(kn') = b + (pk)n'$
or $pk' \in \mathbb{N}$ donc $a \equiv b(n')$

4.3 Congruence et opérations

Théorème 1 :

On note a, a', b et b' quatre entiers relatifs quelconques
$a \equiv a'[n]$ et $b \equiv b'[n]$
$\Rightarrow$
$a + b \equiv a' + b'[n]$
et
$a - b \equiv a' - b'[n]$
et
$\forall k \in \mathbb{Z}$, $ka \equiv ka'[n]$
et
$a \times b \equiv a' \times b'[n]$
et
pour tout $p \in \mathbb{N}$, $a^p \equiv a'^p[n]$

Démonstration :
Si $a \equiv a'[n]$ alors il existe $k_1 \in \mathbb{N}$ tel que $a = a' + k_1 n$

Si $b \equiv b'[n]$ alors il existe $k_2 \in \mathbb{N}$ tel que $b = b' + k_2 n$

➳ $a + b = a' + k_1 n + b' + k_2 n = (a' + b') + (k_1 + k_2)n$ donc $a + b \equiv a' + b'[n]$

➳ $a - b = a' + k_1 n - b' - k_2 n = (a' - b') + (k_1 - k_2)n$ donc $a - b \equiv a' - b'[n]$

➳ $\forall k \in \mathbb{Z}$, $ka = ka' + (kk_1)n$ donc $ka \equiv ka'[n]$

➳ $ab = (a' + k_1 n)(+b' + k_2 n) = a'b' + a'k_2 n + b'k_1 n + k_1 k_2 n^2 = a'b' + (a'k_2 + b'k_1 + k_1 k_2 n)n$
donc $ab \equiv a'b'[n]$

➳ On démontre cette partie par récurrence :
On note $\mathcal{P}_k$ la propriété : $\ll a^k \equiv a'^k[n] \gg$
Initialisation :
On a $a^1 \equiv a'^1[n]$ donc $\mathcal{P}_1$ est vraie.
Hérédité :
On suppose que $\mathcal{P}_k$ est vraie au rang k et donc que $a^k \equiv a'^k[n]$
$a^{k+1} = a^k \times a \equiv a'^k \times a'[n]$ donc $a^{k+1} \equiv a'^{k+1}[n]$
Conclusion :
$\forall k \in \mathbb{N}$, on a $a^k \equiv a'^k[n]$

5 PGCD et PPCM de deux entiers

5.1 Définition

5.1.1 Plus Grand Diviseur Commun

On note a et b deux entiers relatifs non nuls.
$PGCD(a;b)$ est le **P**lus **G**rand **D**iviseur **C**ommun de a et b.

Exemples : $PGCD(6;4) = 2$ $PGCD(12;13) = 1$ $PGCD(21;35) = 7$

5.1.2 Plus Petit Multiple Commun

On note a et b deux entiers relatifs non nuls.
$PPCM(a;b)$ est le **P**lus **P**retit **M**ultiple **C**ommun de a et b.

Exemples : $PGCD(6;4) = 12$ $PGCD(12;13) = 156$ $PGCD(21;35) = 105$

5.1.3 Les nombres étrangers

On note a et b deux entiers relatifs non nuls.
On dit que a et b sont des **étranger**s si et seulement si $PGCD(a;b) = 1$.
On dit aussi que a et b sont **premiers entre eux**.

Exemples : $PGCD(3;2) = 1$ $PGCD(10;21) = 1$ $PGCD(51;143) = 1$

5.2 Méthodes de calcul

5.2.1 Plus Grand Diviseur Commun

1. Liste des diviseurs
2. Algorithme des soustractions
3. Algorithme d'Euclide
4. Décomposition en produits de facteurs premiers.

5.2.2 Plus Petit Multiple Commun

1. Lste des multiples
2. Décomposition en produits de facteurs premiers.
3. Formule reliant PGCD et PPCM

6 Théorème de Bézout et de Gauss

6.1 Théorème de Bézout

Soient a et b deux entiers relatifs non nuls.
Il existe deux entiers relatifs a et v tels que $au + bv = PGCD(a, b)$

Démmonstration :
On note $D = \{au + bv \in \mathbb{N} \text{ avec } u \in \mathbb{Z} \text{ et } v \in \mathbb{Z}\}$
➠ D est une partie de $\mathbb{N}^*$ non vide car $|a| \in D$.
D'après l'axiome A_1 l'ensemble D admet un plus petit élément que l'on note d.
Il existe donc $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tels que $au + bv = d$.
➠ $PGCD(a, b)$ est un diviseur de a et b donc

$$\boxed{PGCD(a, b) \leq d}$$

➠ Démontrons que $PGCD(a, b) \in D$
On utilise l'algorithme d'Euclide pour trouver le PGCD(a,b) :
Par division successive, on obtient :

$$\begin{gathered} a = bq_1 + r1 \text{ avec } 0 \leq r_1 < b \\ b = r_1q_2 + r_2 \text{ avec } 0 \leq r_2 < r_1 \\ r_1 = r_2q_3 + r_3 \text{ avec } 0 \leq r_3 < r_2 \\ \vdots \\ r_{n-2} = r_{n-1}q_n + r_n \text{ avec } 0 \leq r_n < r_{n-1} \end{gathered}$$

D'après l'algorthme d'Euclide il existe $k \in \mathbb{N}$ tel que $PGCD(a, b) = r_k$
Montrons par récurrence que $\forall k \in \mathbb{N}$, $r_k \in D$
On note $(\mathcal{P}_k)$ la propriété $\ll r_k \in D \gg$
Initialisation :
$r_1 = a - bq_1$ donc $r_1 \in D$ donc $(\mathcal{P}_1)$ est vraie.
$r_2 = b - r_1q_2 = b - (a - bq_1)q_2 = aq_2 + (1 + q_1q_2)b$ donc $r_2 \in D$ donc $(\mathcal{P}_2)$ est vraie.
Hérédité :
On suppose que pour tout $l \in [|1, k|]$, $(\mathcal{P}_l)$ est vraie.
On a donc
$r_{k+1} = r_{k-1} - r_kq_{k+1}$
or il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tels que $r_{k-1} = au + bv$
et il existe $u' \in \mathbb{Z}$ et $v' \in \mathbb{Z}$ tels que $r_k = au' + bv'$
donc
$r_{k+1} = au + bv - (au' + bv')q_{k+1} = (u - u'q_{k+1})a + (v - v'q_{k+1})b$ avec $(u - u'q_{k+1}) \in \mathbb{Z}$ et $(v - v'q_{k+1}) \in \mathbb{Z}$
donc pour tout $k \in \mathbb{N}$, $(\mathcal{P}_k)$ est vraie et donc $r_k \in D$
Donc $PGCD(a, b) \in D$ or d est le plus petit élément de D

$$\boxed{PGCD(a, b) \geq d}$$

Conclusion : $PGCD(a, b) = d$

Exemple :
Montrer que pour tout $n \in \mathbb{Z}$, $2n + 1$ et $3n + 1$ sont premiers entre eux.

Conséquence :

$$\boxed{\begin{gathered} a \text{ et } b \text{ sont premiers entre eux} \\ \Leftrightarrow \\ \text{il existe deux entiers relatifs } u \text{ et } v \text{ tels que : } au + bv = 1 \end{gathered}}$$

Démonstration :

- Sens direct :
  Montrons que a et b sont premiers entre eux $\Rightarrow$ il existe deux entiers relatifs u et v tels que : $au + bv = 1$
  Si a et b sont premiers entre eux alors $PGCD(a, b) = 1$ donc d'après le théorème de Bézout, il existe u et v de $\mathbb{Z}$ tels que $au + bv = 1$.
- Réciproque :
  Montrons que si il existe deux entiers relatifs u et v tels que : $au + bv = 1 \Rightarrow$ a et b sont premiers entre eux.
  Il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tels que $au + bv = 1$
  Si d est un diviseur commun de a et de b alors il divise $au + bv$ donc il divise 1. On a donc $d = 1$ et donc le seul diviseur commun de ae t b est 1 donc $PGCD(a, b) = 1$. a et b sont premiers entre eux.

Conséquences :

1. Démontrer que tout diviseur de a et b est un diviseur de $PGCD(a, b)$
2. Démontrer que l'équation $ax + by = c$ ($d \in \mathbb{Z}^*$) admet des solutions entières si et seulement si $PDGC(a, b)$ divise c.

6.2 Théorème de Gauss

Soient a, b et c deux entiers relatifs non nuls.
Si a divise bc et si a et b sont premiers entre eux, alors a divise c.

Démmonstration :
a divise bc donc il existe $k \in \mathbb{Z}$ tel que $bc = ka$.
a et b sont premiers entre eux donc d'après le théorème de Bézout, il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tels que $au + bv = 1$
donc $c = cau + cbv$ donc $c = acu + kav = a(cu + kv)$
donc a divise c.

Conséquences :

1. Démontrer que si a et b divisent un entier c et si a et b sont étrangers alors ab divise c.
2. Démontrer que si un entier a est premier avec chacun des entiers $b_1, b_2, \ldots, b_k$, alors a est premier avec leur produit $b_1 \times b_2 \times \ldots \times b_k$.

6.3 Applications

1. **LES CODES BARRES**
   Le code barre (Code UPC : Universal Product Code) utilise des nombres de treize chiffres pour désigner un produit de consommation.

   (a) Les 2 premiers chiffres : Code de la zone d'origine.
   (b) Les 4 chiffres suivants : Le code du fabriquant.
   (c) Les 6 chiffres suivants : Le code de l'article.
   (d) : Le dernier chiffre est un code de contrôle.

   Le code de contrôle est destinée à détecter une erreur dans l'un des douze premiers chiffres. Le code de contrôle est calculé de telle sorte que , si le nombre s'écrit $a_1, a_2, \ldots, a_{13}$ alors :

$$3\left(\sum_{i=1}^{6} a_{2i}\right) + \sum_{i=0}^{6} a_{2i+1} \equiv 0\ [10].$$

   (a) Vérifier que la clé de contrôle du code barre ci-dessus est 0.
   (b) Calculer la clé associée au nombre de douze chiffres : 325039017681.
   (c) La clé de contrôle du code barre 3130630555094 est-il bon ?
   (d) La clé de contrôle du code barre 3130630355094 est-il bon ?
   (e) Montrer que, si un seul chiffre est erroné, alors l'erreur st détectée.

2. **Numéro INSEE**
   En France, chaque personne est identifiée dès sa naissance par un numéro composé de quinze chiffres.

   (a) 1er chiffre : 1 pour un homme et 2 pour une femme.
   (b) 2ème et 3ème chiffre : Deux derniers chiffres de l'année de naissance.
   (c) 4ème et 5ème chiffre : Le mois de naissance.
   (d) 6ème et 7ème chiffre : Le département de naissance. (2A et 2B pour la Corse)
   (e) 8ème et 9ème et 10ème chiffre : Numéro d'ordre de la commune de naissance dans le département
   (f) 11ème et 12ème et 13ème chiffre : Numéro d'ordre de l'acte de naissance.
   (g) 14ème et 15ème chiffre : La clé de contrôle.

   Le code de contrôle est calculé de telle sorte que , si le nombre s'écrit $a_1, a_2, \ldots, a_{15}$ alors :

$$\sum_{i=1}^{15} a_i \equiv 0\ [97].$$

   (a) Calculer la clé associée au numéro : 1561113055376. On pourra décomposer sous la forme : $a \times 10^6 + b$ avec $b < 10^6$
   (b) Vérifier la clé de contrôle suivante : 168039117421232
   (c) Vérifier la clé de contrôle suivante : 168039117411232
   (d) Montrer que, si un seul des chiffres de A est erroné, l'erreur est détectée.

3. **Numéro ISBN**
   LISBN (International Standard Book Number) ou numéro international normalisé du livre est un numéro international qui permet d'identifier, de manière unique, chaque livre publié. Il est destiné à simplifier la gestion informatique du livre : bibliothèques, libraires, distributeurs, etc...
   Il utilise des nombres de longueur 10 chiffres.

   (a) 1er chiffre : Désigne le pays.
   (b) 2ème,3ème,4ème et 5ème chiffre : Désigne l'éditeur.
   (c) 6ème, 7ème, 8ème et 9ème chiffre : Numéro donné par l'éditeur.
   (d) 10ème chiffre : Le code contrôle.

   Si $a_1a_2\dots a_{10}$ est le numéro I.S.B.N complet, alors $\sum_{i=1}^{10} i \times a_{11-i} \equiv 0\ [11]$.

   (a) Vérifier que 2.0113.5294.0 est un numéro ISBN correct.
   (b) Calculer la clé des numéros suivants :
      i. $2.7298.5868.X$
      ii. $0.1685.2059.Y$
      iii. $2.5960.2369.Z$
   (c) Montrer que, si un seul des chiffres est erroné, l'erreur est détectée.
   (d) Montrer que si deux chiffres consécutifs sont permutés, l'erreur est détectée.
   (e) Trouver toutes les valeurs possibles de a et b telles que $2.8422.50ab.1$ soit un code ISBN valide.

4. **Racines rationnelle d'un polynôme à coefficents entiers**
   Un résultat très important pour la recherche des racines d'un polynôme :
   On note P le polynôme :

   $$P(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_2x^2 + a_1x + a_0$$

   avec pour tout $k \in [|0; n|]$, $a_k \in \mathbb{Z}$
   On note $x = \dfrac{p}{q}$ avec p et q des entiers relatifs premiers entre eux.

   (a) Démontrer que si x est une racine de P alors : $p|a_0$ et $q|a_n$.
   (b) Appliquer ce théorème pour trouver les racines de $P_1(x) = 3x^2 + 7x - 6$
   (c) Appliquer ce théorème pour trouver les racines de $P_2(x) = 2x^3 + 5x^2 + x - 2$
   (d) Appliquer ce théorème pour trouver les racines de $P_3(x) = 3x^4 + 14x^3 + 12x^2 - 14x - 15$

7 Les équation diophantienne

7.1 définition

7.2 Méthodes de résolutions

7.3 La Cryptographie à clé cachée