Chapitre 4

La division dans $\mathbb{Z}$

4.1 Les entiers premiers

4.1.1 Définition

Soient $(a, b) \in \mathbb{Z} \times \mathbb{Z}$

1. **On dit que** a **divise** b**, ou que** b **est divisible par** a **ou encore que** a **est un diviseur de** b**, s'il existe** $c \in \mathbb{Z}$ **tel que** $b = ac$**; on écrit aussi** $a \mid b$
2. **On dit que** a **et** b **sont associés si** $a \mid b$ **et si** $b \mid a$
3. **Si** a **divise** b**, ou que** b **est divisible par** a**, on dit que** b **est un multiple de** a

Remarque 1 :

1. La division dans $\mathbb{N}$ a évidemment un sens. Il suffit de ré-écrire la définition 4.1.1

   Soient $(a, b) \in \mathbb{N} \times \mathbb{N}$
   On dit que a **divise** b**, ou que** b **est divisible par** a**, s'il existe** $c \in \mathbb{N}$ **tel que** $b = ac$**; on écrit aussi** $a \mid b$
2. Pour tout $n \in \mathbb{Z}$, $n \mid 0$ car $0 = n \times 0$
3. On montre que a et b sont associés, si et seulement si, $a = bu$, où u est un élément inversible, c'est à dire, dans $\mathbb{Z}$, $u = 1$ ou $u = -1$; ainsi a et b sont associés si et seulement si $a = b$ ou $a = -b$
4. 1 et -1 sont les diviseurs impropres de n

Exercice 1 :

Démontrer que a et b sont associés, si et seulement si, $a = bu$, où u est un élément inversible, c'est à dire, dans $\mathbb{Z}$, $u = 1$ ou $u = -1$

4.1.2 Proposition

1. **Pour tout** $x \in \mathbb{Z}$ **et tout** $y \in \mathbb{Z}$**, si** $x \mid y$**, alors, pour tout** $z \in \mathbb{Z}$, $x \mid yz$ **et** $xz \mid yz$
2. **Pour tout** $x \in \mathbb{Z}$**, tout** $y \in \mathbb{Z}$ **et tout** $z \in \mathbb{Z}$**, si** $x \mid y$ **et si** $x \mid z$**, alors,** $x \mid y + z$ **et** $x \mid y - z$

Démonstration

Dans la démonstration qui suit, x, y et z désignent des entiers relatifs.

1. **Supposons $x \mid y$**
   Alors, il existe $k \in \mathbb{Z}$ tel que $y = kx$.
   Soit $z \in \mathbb{Z}$; en multipliant l'égalité $y = kx$ par z, nous obtenons $yz = kxz$, qui peut donc être écrit de 2 manières différentes :
   — $yz = (kz) \times x$, ce qui montre que $x \mid yz$
   — $yz = k \times (xz)$, ce qui montre bien que $xz \mid yz$
2. **Supposons $x \mid y$ et $x \mid z$**
   Alors, il existe $k \in \mathbb{Z}$ tel que $y = kx$ et il existe $k' \in \mathbb{Z}$ tel que $z = k'x$
   Donc, $y + z = kx + k'x = x\,(k + k')$; ce qui montre bien que x divise $y + z$; on démontrerait de même que x divise $y - z$

4.1.3 Théorème

La divisibilité sur $\mathbb{N}^\star$ est une relation d'ordre partiel

Démonstration

1. **C'est une relation d'ordre**
   ▷ Elle est réflexive
   Soit $x \in \mathbb{N}$, évidemment, $x \mid x$ car $x = x \times 1$
   ▷ Elle est antisymétrique
   Supposons $x \mid y$ et $y \mid x$; il existe alors il existe $k \in \mathbb{N}$ tel que $y = kx$ et $k' \in \mathbb{N}$ tel que $x = k'y$; dès lors $y = kk'y$, et donc $kk' = 1$; la seule possibilité dans $\mathbb{N}$ est que $k = k' = 1$, c'est à dire $x = y$
   ▷ Elle est transitive
   Soient $x \in \mathbb{N}$, $y \in \mathbb{N}$ et $z \in \mathbb{N}$ tels que $x \mid y$ et $y \mid z$.
   Il existe alors $k \in \mathbb{N}$ tel que $y = kx$ et $k' \in \mathbb{N}$ tel que $z = k'y$, et alors, $z = kk'x$, et nous avons donc $x \mid z$, d'où la transitivité.
2. **C'est une relation d'ordre partiel**
   C'est une relation d'ordre partiel parce qu'il existe des nombres que l'on ne peut pas comparer, au sens de la division. Exemple :

$$3 \nmid 4 \text{ et } 4 \nmid 3$$

Remarque 2 :

1. Dans $\mathbb{N}$, si $m \mid n$ et si $n \neq 0$, alors $m \neq 0$ et $m \leqslant n$
   En effet, si $m \mid n$, alors, il existe $k \in \mathbb{N}$ tel que $n = mk$; donc, si $n \neq 0$ alors $m \neq 0$ et $k \neq 0$ et donc $k \geqslant 1$, c'est à dire, $n \geqslant m$
2. Ceci veut dire que **le nombre de diviseurs d'un entier n est fini dans $\mathbb{N}$**, et à un signe près, c'est la même chose dans $\mathbb{Z}$

4.1.4 Définition de nombre premier

1. **Un entier $n \in \mathbb{Z}$ est dit premier s'il n'a pas de diviseur propre, et s'il n'est pas inversible.**
2. **Un entier non premier autre que 0, -1 et $+1$ est dit composé**

Remarque 3 :

1. On répond enfin à la grande question : **1 n'est pas un nombre premier !** *(parce qu'il est inversible)*
2. Les diviseurs non propres d'un entier relatif sont $-n$, $+n$, -1 et $+1$, car $-n$, $+n$ sont associés à n et -1 et $+1$ sont les seuls éléments inversibles de $\mathbb{Z}$

4.1.5 Théorème

Soit $a \in \mathbb{Z}$; alors, a admet au moins un diviseur premier.

Démonstration

Soit D_a, l'ensemble des diviseurs de a ; comme $a \in D_a$, nous pouvons dire que $D_a \neq \emptyset$
Soit b le plus petit élément positif de D_a, c'est à dire le plus petit élément de $D_a \cap \mathbb{N}$; d'après la remarque 2 page 120, cet élément existe. C'est donc le plus petit élément positif de D_a
Montrons que b est premier
Supposons que b ne le soit pas ; soit donc $c > 0$ tel que $c \mid b$ et $c \neq b$, et donc, $c < b$. Comme $b \mid a$, que $c \mid b$, alors, $c \mid a$; b ne serait donc pas le plus petit diviseur de a ; il y a donc contradiction.
b est donc premier.

Remarque 4 :

On vient de montrer que tout nombre admet un diviseur premier, et que le plus petit diviseur positif d'un nombre est forcément premier.

Exercice 2 :

Soit $a \in \mathbb{N}$, non premier. Montrer que son plus petit diviseur positif b est tel que $b \leqslant \sqrt{a}$

4.1.6 Théorème de décomposition en un produit de facteurs premiers

Tout élément de $\mathbb{Z}$ est un produit $p_1 \times p_2 \times \cdots \times p_n$ de facteurs premiers.
Cette décomposition est unique.

Remarque 5 :

Les nombres premiers $p_1, p_2, \ldots p_n$ peuvent se retrouver plusieurs fois dans la décomposition ; en fait, c'est un produit $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_n^{\alpha_n}$

Démonstration

1. Nous admettrons, pour le moment, l'unicité ; la démonstration utilise le lemme de Gauss qui sera prouvé un peu plus loin.
2. La démonstration de la décomposition se fait en deux temps : on le démontre pour $\mathbb{N}$, puis on le généralise à $\mathbb{Z}$
   (a) Pour $\mathbb{N}$, la démonstration se fait par récurrence sur $n \in \mathbb{N}$, avec $n > 1$.
   — C'est vrai pour $n = 2$, puisque 2 étant premier, est déjà une décomposition de lui-même
   — Supposons que jusqu'au rang n, tous les nombres peuvent être décomposés en un produit de nombres premiers
   — Montrons que $n + 1$ peut l'être aussi.
   • Si $n + 1$ est premier, alors, $n + 1$ est déjà une décomposition de lui même
   • Si $n + 1$ n'est pas premier, $n + 1$ admet des diviseurs propres et donc $n + 1 = ku$ avec $k < n + 1$ et $u < n + 1$
   Or, $\begin{cases} k = p_1 \times p_2 \times \cdots \times p_m \text{ car } k \leqslant n \\ u = q_{m+1} \times q_{m+2} \times \cdots \times q_n \text{ car } u \leqslant n \end{cases}$
   Donc, $n + 1 = p_1 \times p_2 \times \cdots \times p_m \times q_{m+1} \times q_{m+2} \times \cdots \times q_n$; ce qui montre que $n + 1$ peut se décomposer en un produit de facteurs premiers.
   (b) La généralisation à $\mathbb{Z}$ est simple : tout entier relatif est le produit d'un entier positif par une unité -1.

4.1.7 Théorème

Il y a, dans $\mathbb{Z}$, une infinité de nombres premiers

Démonstration

On suppose le contraire, c'est à dire que nous supposons que les entiers premiers sont en nombre fini, et nous appelons q le dernier d'entre eux ou le plus grand d'entre eux *(ce qui, pour nos considérations, revient au même)*.
Posons $n = q\,! + 1$
Divisons n par n'importe quel entier premier $p \leqslant q$. Nous avons donc :

$$n = \left(\frac{q\,!}{p}\right) \times p + 1$$

Ce qui exprime que n n'est divisible par aucun des quelconques entiers premiers. Ce qui contredit de le théorème 4.1.6 précédent, lequel affirmait que tout nombre entier admet des diviseurs premiers. Il y a donc contradiction
L'ensemble des nombres premiers est infini

Remarque 6 :

Si on sait que la suite des nombres premiers est infinie, un autre et important problème se pose : celui de **la répartition des nombres premiers** dans $\mathbb{N}$. C'est une vaste question qui dépasse ce cours de L_0. Par contre, il y a une inégalité qu'il est possible d'établir.

On appelle $(p_n)_{n\in\mathbb{N}^*}$ la suite des nombres premiers. Nous avons donc :

$$p_1 = 2\ p_2 = 3\ p_3 = 5\ p_4 = 7\ p_5 = 11$$

Pour tout $n \in \mathbb{N}^*$, nous avons $p_n \geqslant n + 1$

Démonstration

Nous allons le démontrer par récurrence :
- ▷ C'est manifestement vrai pour $n = 1$, $n = 2$, $n = 3$, $n = 4$, $n = 5$; ce sont même ces exemples qui nous ont conduit à cette inégalité
- ▷ Supposons maintenant qu'à l'ordre $n \geqslant 1$,$p_n \geqslant n + 1$
- ▷ Démontrons maintenant, à l'ordre $n + 1$.
  Clairement, p_n est impair, et de même p_{n+1} et donc $p_{n+1} \geqslant p_n + 2$; donc

$$p_{n+1} \geqslant p_n + 2 \geqslant n + 1 + 2 > n + 2 = (n + 1) + 1$$

Nous en déduisons donc que, pour $n \in \mathbb{N}^*$, nous avons $p_n \geqslant n + 1$.
On peut aussi en déduire $\lim\limits_{n\to+\infty} p_n = +\infty$

4.1.8 Exercices résolus

1. *Cet exercice résolu propose de démontrer un cas particulier du théorème de Dirichlet*
   Montrez qu'il existe une infinité de nombres premiers de la forme $4p + 3$

   Résolution
   Supposons le contraire, c'est à dire qu'il existe un nombre fini d'entiers premiers de la forme $4p + 3$, et soit $4n + 3$ le dernier d'entre eux.
   Les nombres premiers ne peuvent être que de 2 formes : $4p + 1$ ou $4p + 3$, lesquels sont des nombres impairs. $4p + 2$ et $4p$ sont des nombres pairs, donc, sûrement pas premiers.
   Soit $a = \prod_{p=0}^{n} (4p + 3)$, c'est à dire que a est le produit de tous les nombres entiers de la forme $4p + 3$ jusqu'au dernier nombre premier $4n + 3$ et nous considérons $b = 4a + 3$.
   Ce nombre b est congru à 3 modulo 4 ; d'autre part, il n'est divisible par aucun des nombres premiers de la forme $4p + 3$.

En effet, si p_a est un nombre premier de ce type, $b = \left(\frac{4a}{p_a}\right) \times p_a + 3$.

Ainsi, les seuls nombres premiers qui divisent b sont de la forme $4p+1$, c'est à dire que nous avons $b = q_1^{\alpha_1} \times q_2^{\alpha_2} \times q_3^{\alpha_3} \times \ldots q_b^{\alpha_b}$, où $q_i \equiv 1\,[4]$ pour tout $i = 1, \ldots, b$, et nous avons, par conséquent, $b \equiv 1\,[4]$; ce qui est faux.

Il y a donc contradiction avec l'hypothèse où le nombre d'entiers premiers du type $4p+3$ est fini. Il existe donc une infinité de nombres premiers de la forme $4p+3$

2. **Soit $(p_n)_{n\in\mathbb{N}}$ la suite des nombres premiers, c'est à dire :**

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7, \cdots$$

p_n est donc le n-ième nombre premier. Il faut montrer que $p_n < 2^{2^n}$

Résolution

Nous allons démontrer cette inégalité par une récurrence sur n.

— Nous avons $p_1 = 2 < 2^{2^1} = 2^2 = 4$; l'inégalité est donc vraie pour $n = 1$

— Supposons $p_n < 2^{2^n}$

— Démontrons l'inégalité à l'ordre $n+1$

Soit $a = p_1 \times p_2 \times \cdots \times p_n + 1$

Alors, clairement, a n'est divisible par aucun des nombres premiers $p_1, \cdots, p_n$. Comme a est décomposable en un produit de facteurs premiers, a admet donc comme diviseur un facteur premier q tel que $q > p_n$, c'est à dire $q \geqslant p_{n+1}$. Nous avons donc :

$$p_{n+1} \leqslant q \leqslant a < 2^{2^1} \times 2^{2^2} \times \cdots \times 2^{2^n} + 1$$

Or, $2^{2^1} \times 2^{2^2} \times \cdots \times 2^{2^n} = 2^{2^1+2^2+2^3+\cdots+2^n}$ et $2^1 + 2^2 + 2^3 + \cdots + 2^n = \sum_{k=1}^{n} 2^k = 2^{n+1} - 2$

Donc, nous avons $a < 2^{2^{n+1}-2} + 1$, à fortiori

$$a < 4 \times 2^{2^{n+1}-2} = 2^2 \times 2^{2^{n+1}-2} = 2^{2^{n+1}-2+2} = 2^{2^{n+1}}$$

C'est à dire $p_{n+1} < 2^{2^{n+1}}$ Ce que nous voulions

4.1.9 Quelques exercices

Exercice 3 :

Soit $A = 315$. Trouver le plus petit entier naturel k tel que $k \times A$ soit le carré d'un nombre entier.

Exercice 4 :

Montrer que les nombres suivants sont composés :

1. $n^4 - 20n^2 + 4$ pour $n \in \mathbb{Z}$
2. $a^4 + 4b^4$ pour $a \in \mathbb{N}$, $b \in \mathbb{N}$ et $a \geqslant 2$ et $b \geqslant 2$

Exercice 5 :

Cet exercice s'intéresse à la répartition des nombres premiers et complète la remarque de 4.1.7

Soit n un entier naturel tel que $n \geqslant 2$

1. On considère les $(n-1)$ nombres :

$$n! + 2,\ n! + 3,\ \cdots, n! + (n-1),\ n! + n$$

Démontrer que ces nombres ne sont pas premiers

2. En déduire que l'on peut trouver une suite de k nombres consécutifs non premiers

Exercice 6 :

1. Déterminer les couples $(x, y) \in \mathbb{Z}^2$ tels que $x^2 - y^2 = 1969$
2. Déterminer les couples $(x, y) \in \mathbb{Z}^2$ tels que $9y^2 - (x+1)^2 = 32$

Exercice 7 :

Soient $p_1, p_2, \ldots, p_k$ des nombres entiers premiers distincts rangés par ordre croissant, c'est à dire : $p_1 < p_2 < \ldots < p_k$.

Montrer que le nombre $1 + p_1 p_2 \ldots p_k = 1 + \prod_{j=1}^{k} p_j$ n'est divisible par aucun des nombres $p_1, p_2, \ldots, p_k$

Exercice 8 :

Montrer qu'il existe une infinité de nombres premiers de la forme $6p + 5$

Exercice 9 :

Montrer que si p est un nombre premier supérieur à 4, alors $p^2 \equiv 1\,[6]$

Exercice 10 :

Etude de la somme des diviseurs d'un nombre entier positif Soit $x = a^m b^n c^p$, où a, b et c sont 3 nombres premiers

1. De quelle forme sont les diviseurs de x ?
2. Soient $n_0 \leqslant n$ et $p_0 \leqslant p$ fixés ; calculez $\sum_{k=0}^{m} a^k b^{n_0} c^{p_0}$
3. En déduire la somme des diviseurs de x

Exercice 11 :

En étudiant les congruences modulo 3, montrer que si p et $2p-1$ sont premiers, alors, $2p+1$ est composé