ARITHMÉTIQUE MODULAIRE

ALEXANDRE GIROUARD

9. Division Euclidienne et plus grand commun diviseur de deux entiers

Soient a et b deux entiers avec $b > 0$. Il existe des entiers q et r tels que $a = bq + r$ avec $0 \leq r < a$. Ces entiers sont uniques. Le nombre r est le *reste* de la division de a par b. Si ce reste est zéro, on dit que b *divise* a. On note ceci $b|a$.

Le *plus grand commun diviseur* de deux entiers non-nuls a et b est le plus grand entier positif divisant à la fois a et b. On le note $PGDC(a, b)$ ou encore plus simplement (a, b).

La proposition suivante montre qu'on peut écrire le PGDC de deux nombres comme une combinaison linéaire entière de ces deux nombres.

Lemme 9.1 (Lemme de Bézout)**.** *Soient $a, b \in \mathbb{Z}$. Alors il existe $x, y \in \mathbb{Z}$ tels que*

$$(a, b) = ax + by.$$

Démonstration. Considérons l'ensemble

$$E = \{ax + by \, : \, x, y \in \mathbb{Z} \text{ et } ax + by > 0\} \subset \mathbb{N}.$$

Cet ensemble est non-vide. Soit $m = ax_0 + by_0$ le minimum de cet ensemble[1]. Montrons que m divise a et b : Il existe q et $0 \leq r < m$ tel que

$$a = mq + r.$$

Si $r \neq 0$ on a :

$$r = a - mq = a - (ax_0 + by_0)q = a(1 - x_0q) + b(-y_0q) \in E.$$

Comme $r < m$, ceci contredit la minimalité de m. Donc, $r = 0$ et m divise a. On déduit de la même manière que m divise b.

Montrons maintenant que m est maximal. Soit m' un diviseur commun de a et b. Il existe donc des entiers p et q tels que $a = pm'$ et $b = qm'$. On déduit

$$m = ax_0 + by_0 = m'(px_0 + qy_0).$$

[1]le fait que chaque sous-ensemble non-vide de $\mathbb{N}$ admette un minimum est appelé *principe du bon ordre*

Le nombre m' est donc un diviseur de m. □

Exercice 9.2. *Est-ce que les entiers x, y obtenues dans le lemme précédent sont uniques ?*

Exercice 9.3. *Quel est le PGDC de 34 et 21 ? Exprimez le comme une combinaison linéaire entière de ces deux nombres.*

Deux entiers a et b sont dits *relativement premiers* si $(a, b) = 1$. Un nombre $1 < p \in \mathbb{N}$ est dit *premier* si ses seuls diviseurs sont 1 et p.

Exercice 9.4. *Soient $a, b \in \mathbb{Z}$ des entiers. Soit p un nombre premier. Montrez que si $p|ab$ alors $p|a$ ou $p|b$.*

10. Multiplication sur $\mathbb{Z}_n$

Rappelons que $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$. Sur $\mathbb{Z}$, on a défini une relation d'équivalence de la manière suivante :

$$a \sim b \iff a - b \in n\mathbb{Z}.$$

En mots, a est égal (ou congru) à b modulo n. On note aussi

$$a \equiv b \bmod n.$$

On a vu que l'ensemble des classes d'équivalence

$$\mathbb{Z}_n = \{[0], [1], \cdots, [n-1]\}$$

muni de l'opération d'addition $[a] + [b] = [a + b]$ est un groupe. C'est le *groupe des entiers modulo n.*

On peut aussi multiplier les éléments de $\mathbb{Z}_n$: si $a' \equiv a \bmod n$ et $b' \equiv b \bmod n$ alors il existe $k, l \in \mathbb{Z}$ tels que $a' = a + kn$ et $b' = b + ln$. On a donc :

$$a'b' = (a + kn)(b + ln) = ab + (al + bk)n + kln^2 \equiv ab \bmod n.$$

On peut donc définir le produit de deux classes d'équivalences $[a]$ et $[b]$ de la manière naturelle :

$$[a] \cdot [b] = [ab].$$

Exemple 10.1. *Voici la table de multiplication de* $\mathbb{Z}_6$ *:*

	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

L'ensemble $A = \mathbb{Z}_n$ muni des opérations d'addition et de multiplication définies par $[a] + [b] = [a + b]$ et $[a] \cdot [b] = [ab]$ est un *anneau*. C'est-à-dire que les propriétés suivantes sont vérifiées :

(1) A muni de l'opération $+$ est un groupe abélien.
(2) Le produit est associatif.
(3) Le produit se distribut sur l'addition:

$$\forall a, b, c \in A, \quad a(b + c) = ab + ac.$$

L'anneau $\mathbb{Z}_n$ a deux propriétés particulièrement remarquables :

(1) Son produit est commutatif.
(2) Il existe un élément neutre pour la multiplication. En effet, pour chaque $[a] \in \mathbb{Z}_n$,

$$[1][a] = [a][1] = [a].$$

On remarque aussi que :

– Le produits de certains éléments non-nuls peut être nul. Par exemple dans $\mathbb{Z}_6$,

$$[2][3] = [6] = [0].$$

De tels éléments sont appelés des *diviseurs de zéro*.
– Certains éléments sont inversibles pour la multiplication. Par exemple, toujours dans $\mathbb{Z}_6$, l'élément [5] est son propre inverse :

$$[5][5] = [1].$$

Proposition 10.2. *Soit* $[a] \in \mathbb{Z}_n$*. Alors* $[a]$ *admet un inverse multiplicatif si et seulement si* a *et* n *sont copremiers.*

Démonstration. Les nombrs a et n sont copremiers si et seulement si leur PGDC est 1. Par le lemme de Bézout, ceci est equivalent à l'existence de deux nombres $x, y \in \mathbb{Z}$ tels que

$$ax + ny = 1.$$

Or, cette dernière équation s'exprime aussi sous la forme : $ax = 1 \bmod n$. C'est-à-dire $[1] = [ax] = [a][x]$. □

Les éléments de $\mathbb{Z}_n$ admettant un inverse sont appelés les *unités* de $\mathbb{Z}_n$. La proposition que nous venons de montrer peut donc être reformulé comme ceci :

Proposition 10.3. *Soit $n \in \mathbb{N}$ un entier positif. L'ensemble $U(n)$ des unités de $\mathbb{Z}_n$ est donné par*

$$U(n) = \{[a] \in \mathbb{Z}_n \, : \, (a, n) = 1\}.$$

Exercice 10.4. *Écrire la table de multiplication de $\mathbb{Z}_{12}$. Quelles sont les unités de $\mathbb{Z}_{12}$?*

Proposition 10.5. *L'ensemble $U(n)$ des unités de $\mathbb{Z}_n$, muni de l'opération de multiplication, est un groupe. Son élément neutre est* $[1]$.

Démonstration.

(1) Comme $[1]$ est une unité, $U(n)$ n'est pas vide.

(2) La multiplication étant associative dans $\mathbb{Z}$, elle l'est aussi dans $\mathbb{Z}_n$, et a posteriori aussi dans $U(n)$.

(3) Étant donnés $[a], [b] \in U(n)$, il existe $[a'], [b'] \in \mathbb{Z}_n$ tels que
$$[a][a'] = [1] \text{ et } [b][b'] = [1].$$
On a donc
$$[a][b][b'][a'] = [a][1][a'] = [a][a'] = [1].$$
Donc, $[a][b] \in U(n)$.

(4) Soit $[a] \in U(n)$. Par définition, il existe $[b] \in \mathbb{Z}_n$ tel que $[a][b] = [1]$. En d'autres mots, $[b]$ est aussi une unité. C'est l'inverse de $[a]$. Pour être plus précis :
$$[a][b] = [ab] = [ba] = [b][a] = 1.$$

□

Exemple 10.6. *Les unités de* $\mathbb{Z}_6$ *sont*

$$U(6) = \{[1], [5]\}.$$

On peut le voir directement à partir de la table de multiplication donnée plus haut. On peut aussi constater que comme $6 = 2 \cdot 3$*, parmis les nombres 1,2,3,4,5,6, seuls* 1 *et* 5 *sont copremiers à 6.*

Exercice 10.7. *Soit* p *un nombre premier.*

(1) *Montrez que chaque* $0 \neq [a] \in \mathbb{Z}_p$ *admet un inverse multiplicatif.*
(2) *En déduire que* $U(p) = \{[1], [2], \cdots, [p-1]\}$.