Algèbre et Géométrie

CHAPITRE 3

Arithmétique dans $\mathbb{Z}$

Sommaire

1. Les entiers relatifs

1.1. Division euclidienne dans $\mathbb{Z}$

Rappels sur l'ensemble des entiers relatifs $\mathbb{Z}$

La relation d'ordre usuelle sur $\mathbb{Z}$ est compatible avec l'addition et la multiplication:

$$\forall (a,b,c)\in\mathbb{Z}^3,\ a\leq b \Rightarrow a+c\leq b+c$$
$$\forall (a,b,c)\in\mathbb{Z}^3,\ [a\leq b \text{ et } c>0] \Rightarrow ac\leq bc.$$

La valeur absolue sur $\mathbb{Z}$ possède les propriétés classiques :

$$\forall a\in\mathbb{Z},\ |a|>0 \text{ et } |a|=0 \Leftrightarrow a=0$$
$$\forall (a,b)\in\mathbb{Z}^2,\ ||a|-|b||\leq|a+b|\leq|a|+|b|$$

Propriété 1 (Division euclidienne dans $\mathbb{Z}$)

Pour tout couple $(a,b)\in\mathbb{Z}^2$, il existe un unique couple $(q,r)\in\mathbb{Z}^2$ tel que

$$a=bq+r,$$

avec $0\leq r<|b|$.

Exemples

- Division de -56 par 17 : $56=3\times17+5$, d'où $-56=(-3)\times17-5=(-4)\times17+12$. Donc -56 que divise 17 est égal à -4 et il reste 12.
- Division de 32 par -7 : $32=4\times7+4$, d'où $32=(-4)\times(-7)+4$. Donc 32 que divise -7 est égal à -4 et il reste 4.

1.2. Divisibilité dans $\mathbb{Z}$

Soient a et b deux entiers relatifs. On dit que b est un *diviseur* de a, ou encore que a est un *multiple* de b, et on note $b|a$, s'il existe un entier relatif q tel que $a=qb$.

Propriété 2

Soient a, b et c trois entiers relatifs

- $b|a$ et $a|b \Rightarrow a=b$ ou $a=-b$
- $a|b$ et $a|c \Rightarrow a|(b+c)$
- $a|b \Rightarrow a|(cb)$

Pour tout $n\in\mathbb{Z}$, on note $n\mathbb{Z}$ le sous-ensemble des multiples de n, $n\mathbb{Z}=\{nq,\ q\in\mathbb{Z}\}$.

Exemple : $2\mathbb{Z}$ est l'ensemble des entiers relatifs pairs.

Remarque : Les sous-ensembles $n\mathbb{Z}$, $n\in\mathbb{Z}$ sont stables pour l'addition

Soit $n \in \mathbb{N}^*$. La relation de *congruence modulo n* est définie sur $\mathbb{Z}$ par

$$x \equiv y \pmod{n} \Leftrightarrow y\text{-}x \in n\mathbb{Z}.$$

Ce qui peut encore s'écrire $n \mid y\text{-}x$ ou $y=x+kn$ avec $n \in \mathbb{Z}$.

Exemples : $2 \equiv 0 \pmod 2$, $8 \equiv 2 \pmod 6$, $-5 \equiv 1 \pmod 6$.

Propriété 3
La relation de congruence modulo n est une relation d'équivalence qui définit n classes d'équivalence.

Si x est équivalent à y modulo n ($x \equiv y$), cela signifie que x et y ont le même reste dans la division par n. Or à chaque entier relatif x, on peut associer un unique reste $r \in \{0,\ldots,n\text{-}1\}$ par la division par n. Autrement dit la relation de congruence modulo n définie n classes d'équivalence, notée $\mathbb{Z}/n\mathbb{Z}$ ou bien $\mathbb{Z}_n$.

Exemple : $\mathbb{Z}/2\mathbb{Z}$ (ou $\mathbb{Z}_2$) définie deux classes d'équivalence, celle des entiers relatifs pairs, notée $\dot{0}$, et celle des entiers relatifs impairs, notée $\dot{1}$. La table ci-dessous donne les résultats de l'addition dans $\mathbb{Z}/2\mathbb{Z}$. La relation 1+1=0 s'interprète en disant que impair plus impair est pair.

+	0	1
0	0	1
1	1	0

$\mathbb{Z}/3\mathbb{Z}$ (ou $\mathbb{Z}_3$) définie trois classes d'équivalence, celle des entiers relatifs égaux à 0 modulo 3, notée $\dot{0}$, celle des entiers relatifs égaux à 1 modulo 3, notée $\dot{1}$, celle des entiers relatifs égaux à 2 modulo 3, notée $-\dot{1}$ (ou $\dot{2}$). La table ci-dessous donne les résultats de l'addition dans $\mathbb{Z}/3\mathbb{Z}$.

+	0	1	-1
0	0	1	-1
1	1	-1	0
-1	-1	0	1

ou bien

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

2. PGCD et PPCM de deux entiers

2.1. PGCD de deux entiers

2.1.1. Définitions

Propriété 4
Etant donnés deux nombres entiers relatifs a et b, il existe un entier naturel n unique tel que

$$a\mathbb{Z} + b\mathbb{Z} = n\mathbb{Z}.$$

On dit que n est le plus grand diviseur commun, *pgcd*, de a et de b. On le note $a \wedge b$.

Remarques

(i) si n est le pgcd de deux entiers a et b, alors il existe deux entiers u et v tels que au+bv=n.

(ii) s'il existe deux entiers u et v tels que au+bv=m alors m est un multiple de $a \wedge b$.

Propriété 5
$a \wedge b$ est le plus grand entier naturel qui divise à la fois a et b. Tout diviseur de a et de b divise aussi $a \wedge b$.

2.1.2. Théorèmes

On dit que deux nombres entiers relatifs a et b sont *premiers entre eux* si leur pgcd est égal à 1, $a \wedge b = 1$.

Propriété 6 (Théorème de Bezout)
Soient deux entiers relatifs non nuls a et b,

$$a \wedge b = 1 \Leftrightarrow \exists (u,v) \in \mathbb{Z}^2,\ ua + vb = 1.$$

Propriété 7
Etant donné a, b, α, β des entiers non nuls et $d \in \mathbb{N}$. Si $a = \alpha d$ et si $b = \beta d$ alors

$$a \wedge b = d \Leftrightarrow \alpha \wedge \beta = 1.$$

Propriété 8 (Théorème de Gauss)
Soient a, b et c trois entiers relatifs non nuls. Si $a \mid bc$ et si a est premier avec b alors $a \mid c$.

Propriété 9 (Théorème d'Euclide)
Soient a, b, q et r des entiers relatifs non nuls,

$$a = bq + r \Rightarrow a \wedge b = b \wedge r.$$

Ce théorème est à la base de l'algorithme d'Euclide permettant d'obtenir le pgcd de deux nombres entiers relatifs a et b. En effet, on divise a par b, ce qui donne un reste r_1. On divise ensuite b par r_1, obtenant ainsi un deuxième reste r_2. r_1 est alors divisé par r_2 afin d'obtenir un troisième reste r_3. On itère ce procédé jusqu'à obtenir un reste $r_{n+1}=0$. Le dernier reste non nul $r_n \neq 0$ est alors le pgcd de a et b :

Euclide

$$\begin{cases} a = bq_1 + r_1 & (1) & & a \wedge b = b \wedge r_1 \\ b = r_1 q_2 + r_2 & (2) & & b \wedge r_1 = r_1 \wedge r_2 \\ r_1 = r_2 q_3 + r_3 & (3) & \Rightarrow & r_1 \wedge r_2 = r_2 \wedge r_3 \\ \ldots\ldots & & & \ldots \\ r_{n-2} = r_{n-1} q_n + r_n & (n) & & r_{n-2} \wedge r_{n-1} = r_{n-1} \wedge r_n \\ r_{n-1} = r_n q_{n+1} & (n+1) & & r_{n-1} \wedge r_n = r_n \\ \\ 0 < r_n < r_{n-1} < \ldots < r_2 < r_1 < |b| \end{cases}$$

En effet r_n divise r_{n-1} d'après (n+1), or donc d'après (n) r_{n-1} divise r_{n-2}, donc r_n divise r_{n-2}. De proche en proche, on voit que r_n divise b et r_n divise a. donc r_n divise le pgcd de a et b. Inversement, soit d un diviseur de a et de b, d'après (1), d divise r_1. De (2) et de $d \mid b$ et de $d \mid r_1$, on déduit que d divise r_2, etc. D'où d divise r_n. Le pgcd de a et de b divise r_n. Donc r_n est le pgcd de a et b.

Exemple : Cherchons le pgcd de 255 et 95.

$$\begin{array}{lcl} 255 = 2 \times 95 + 65 & \overset{\text{Euclide}}{\Rightarrow} & 255 \wedge 95 = 95 \wedge 65 \\ 95 = 1 \times 65 + 30 & \Rightarrow & 95 \wedge 65 = 65 \wedge 30 \\ 65 = 2 \times 30 + 5 & \Rightarrow & 65 \wedge 30 = 30 \wedge 5 \\ 30 = 6 \times 5 + 0 & \Rightarrow & 30 \wedge 5 = 5 \end{array}$$

Donc $255 \wedge 95 = 5$.

Remarque : Deux entiers relatifs a et b sont premiers entre eux si et seulement si le dernier reste non nul dans l'algorithme d'Euclide est égal à 1.

2.2. PPCM de deux entiers

Propriété 10

Soient a et b deux entiers relatifs, il existe un unique entier naturel m tel que

$$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}.$$

On dit que m est le plus petit commun multiple, *ppcm*, de a et de b. On le note $a \vee b$. On remarque que si m est le ppcm de deux entiers relatifs a et b, alors il existe deux entiers relatifs s et t tels que

$$m = sa = tb.$$

Propriété 11

$a \vee b$ est le plus petit entier naturel non nul multiple commun à a et b. Tout multiple de a et de b est multiple de $a \vee b$.

Propriété 12

Soient a et b deux entiers relatifs, alors

$$(a \wedge b)(a \vee b) = |ab|.$$

2.3. Extension au cas de plusieurs variables

Propriété 13

Les lois $(a,b) \mapsto a \wedge b$ et $(a,b) \mapsto a \vee b$ sont commutatives et associatives dans $\mathbb{Z}$.

Soient $a_1, a_2, \ldots, a_n$ dans $\mathbb{Z}$, $n \geq 2$, les notations

$$\begin{cases} a_1 \wedge a_2 \wedge \ldots \wedge a_n \\ a_1 \vee a_2 \vee \ldots \vee a_n \end{cases}$$

ont alors un sens indépendamment de l'ordre des facteurs a_i et de celui dans lequel on effectue les calculs.
Ces notations correspondent alors respectivement au *pgcd* et au *ppcm de la famille* $(a_1, a_2, \ldots, a_n)$.

Extension des propriétés du pgcd et du ppcm

De la même façon que précédemment, $d = \text{pgcd}(a_1, a_2, \ldots, a_n)$ est l'unique entier naturel tel que

$$a_1\mathbb{Z} + a_2\mathbb{Z} + \ldots + a_n\mathbb{Z} = d\mathbb{Z}.$$

En particulier il existe des entiers relatifs u_k tels que

$$d = u_1a_1 + u_2a_2 + \ldots + u_na_n.$$

d est le plus grand entier naturel qui divise tous les a_i. Ainsi x divise $a_1, \ldots, a_n$ si et seulement si il divise d.

De même, $m = \text{ppcm}(a_1, a_2, \ldots, a_n)$ est l'unique entier naturel tel que

$$a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \ldots \cap a_n\mathbb{Z} = m\mathbb{Z}.$$

Ainsi un entier est un multiple de $a_1, \ldots, a_n$ si et seulement s'il est multiple de m.

Extension des nombres premiers entre eux

On dit que les n entiers relatifs $a_1, a_2, \ldots, a_n$ sont *premiers entre eux dans leur ensemble* si leur pgcd est égal à 1.

Ce qui équivaut à dire que les seuls diviseurs communs sont 1 et –1.

Ce qui équivaut encore d'après le théorème de Bezout, à l'existence de n entiers relatifs $u_1, u_2, \ldots, u_n$ tels que

$$u_1a_1 + u_2a_2 + \ldots + u_na_n = 1.$$

Remarque : Si deux au moins des entiers $a_1,\dots,a_n$ sont premiers entre eux, alors ils le sont dans leur ensemble. En revanche la réciproque est fausse. En effet pgcd(6,10,5)=1 or $6\wedge10=2$, $6\wedge15=3$ et $10\wedge15=5$.

Propriété 14
Soient $\alpha\in Z$ et $(a_1,\dots,a_n)$ une famille dans $\mathbb{Z}$. Soit δ un diviseur de $a_1,\dots,a_n$, alors on a les égalités suivantes :

$$\begin{cases} pgcd(\alpha a_1,\dots,\alpha a_n)=|\alpha|\,pgcd(a_1,\dots,a_n) \\ ppcm(\alpha a_1,\dots,\alpha a_n)=|\alpha|\,ppcm(a_1,\dots,a_n) \end{cases} \text{ et } \begin{cases} pgcd(\frac{a_1}{\delta},\dots,\frac{a_n}{\delta})=\frac{1}{|\delta|}pgcd(a_1,\dots,a_n) \\ ppcm(\frac{a_1}{\delta},\dots,\frac{a_n}{\delta})=\frac{1}{|\delta|}ppcm(a_1,\dots,a_n) \end{cases}$$

3. Nombres premiers

3.1. Définition et propriétés

Soit p un entier naturel. On dit que p est un *nombre premier* si

1. $p\neq0$ et $p\neq1$
2. ses seuls diviseurs dans $\mathbb{N}$ sont 1 et lui-même

L'ensemble des nombre premiers est infini et commence par 2, 3, 5, 7, 11, 13, 17, 19, 23, 29. L'entier 1 n'est pas considéré comme un nombre premier.

Propriété 15
Soient p et q deux nombres premiers. Si $p \mid q$ alors p=q.

Propriété 16

- Soient a un entier relatif et p un nombre premier. Alors ou bien p divise a ou bien p est premier avec a.
- Tout entier naturel $n\geq2$ est divisible par au moins un nombre premier.

Propriété 17
Si un nombre premier p divise un produit $a=b_1b_2\dots b_n$, alors p divise au moins l'un des facteurs b_i.

4.2 Décomposition en produit de facteurs premiers

Propriété 18
Tout entier relatif a non nul et différent de 1 et –1 admet une et une seule décomposition en produit de nombres premiers, *i.e* il existe un unique entier naturel m, une unique suite de nombre premier $(p_1,\dots,p_m)$ et une unique suite d'entiers naturels $(\alpha_1,\dots,\alpha_m)$, tels que

$$a = \varepsilon\, p_1^{\alpha_1} \ldots p_m^{\alpha_m}$$

avec $\varepsilon = \pm 1$ suivant le signe de a.

Cette décomposition s'appelle *décomposition de a en produit de facteurs premiers*.

La décomposition en produit de facteurs premiers permet un calcul simplifier du pgcd et du ppcm. En effet, si on considère deux entiers relatifs

$$a = \varepsilon_a\, p_1^{\alpha_1} \ldots p_m^{\alpha_m} \text{ et } b = \varepsilon_b\, p_1^{\beta_1} \ldots p_m^{\beta_m},$$

où les exposants de la décomposition, α_i et β_i, peuvent être nuls (ce qui permet d'écrire la décomposition en produit des mêmes nombres premiers). On a alors

$$a \wedge b = p_1^{\min\{\alpha_1,\beta_1\}} \ldots p_m^{\min\{\alpha_m,\beta_m\}} \text{ et } a \vee b = p_1^{\max\{\alpha_1,\beta_1\}} \ldots p_m^{\max\{\alpha_m,\beta_m\}}$$

Exemple : pgcd et ppcm de 360 et 21.
On a $21 = 3 \times 7$ et $360 = 2^3 \times 3^2 \times 5$, d'où

$$360 \wedge 21 = 2^0 \times 3^1 \times 5^0 \times 7^0 = 3 \text{ et } 360 \vee 21 = 2^3 \times 3^2 \times 5^1 \times 7^1 = 2520.$$

4. Equation diophancienne

Une équation diophancienne est une équation du type

$$(x,y) \in \mathbb{Z}^2 \quad Ax + By = C, \qquad (1)$$

avec les coefficients $(A,B,C) \in \mathbb{Z}^3$.

Propriété 19
L'équation (1) admet une solution si et seulement si $A \wedge B$ divise C.

Démonstration

a) Condition nécessaire
   Soit $d = A \wedge B$ et les entiers a et b tels que $A = da$ et $B = db$. Si l'équation (1) admet une solution $(x,y) \in \mathbb{Z}^2$, alors en remplaçant dans (1), on obtient $d(ax+by) = C$. Ce qui montre que d est nécessairement un diviseur de C.
b) Condition suffisante
   Supposons maintenant que $A \wedge B$ divise C. En divisant par $d = A \wedge B$ à droite et à gauche dans l'équation (1), on se ramène à une nouvelle équation équivalente à (1)

   $$(x,y) \in \mathbb{Z}^2 \quad ax + by = c,$$

   où a et b sont les entiers précédemment définis et c est l'entier défini par $C = cd$.

On remarque que a et b sont maintenant premiers entre eux, $a \wedge b=1$ (propriété 9). Donc d'après le théorème de Bezout, il existe deux entiers u et v tels que au+bv=1. Il s'ensuit que a(cu)+b(cv)=c, donc (cu,cv) est une solution de l'équation (1). Finalement, en multipliant par d, on obtient a(dcu)+b(dcv)=cd $\Leftrightarrow$ A(cu)+B(cv)=C, donc (cu,cv) est aussi une solution de l'équation (1).

D'après la démonstration précédente, la résolution de l'équation (1) se ramène à la résolution de l'équation

$$(u,v)\in\mathbb{Z}^2 \quad au+bv=1 \qquad (2)$$

On fait appel pour cela à l'algorithme d'Euclide. En appliquant cet algorithme à $a \wedge b=1$, on trouve un couple (u_0,v_0) tel que $au_0+bv_0=1$. Une solution particulière de l'équation (1) est alors donnée par le couple (cu_0,cv_0) et l'ensemble des solutions de l'équation (2) est donné par

$$(cu_0+kb, cv_0-ka),\ k\in\mathbb{Z}.$$

<u>Exemple</u>

Soit l'équation diophancienne

(1) $\qquad (x,y)\in\mathbb{Z}^2, \qquad 300x+126y=12$

On a $A \wedge B=6$. En simplifiant par 6, on obtient l'équation équivalente

$$(x,y)\in\mathbb{Z}^2, \qquad 50x+21y=2,$$

où 50 et 21 sont premiers entre eux. Donc il existe $(u_0,v_0)\in\mathbb{Z}^2$ tel que

(2) $\qquad 50u_0+21v_0=1.$

Pour trouver (u_0,v_0), on utilise l'algorithme d'Euclide :

$50=2\times21+8$	$\Rightarrow 8=50-2\times21$	$\Rightarrow 1=8\times(50-2\times21)-3\times21=\mathbf{8}\times50\mathbf{-19}\times21$
$21=2\times8+5$	$\Rightarrow 5=21-2\times8$	$\Rightarrow 1=2\times8-3\times(21-2\times8)=8\times8-3\times21$
$8=1\times5+3$	$\Rightarrow 3=8-5$	$\Rightarrow 1=2\times(8-5)-5=2\times8-3\times5$
$5=1\times3+2$	$\Rightarrow 2=5-3$	$\Rightarrow 1=3-(5-3)=2\times3-5$
$3=1\times2+1$	$\Rightarrow 1=3-2$	$\Rightarrow 1=3-2$

On a $8\times50+(-19)\times21=1$, donc $u_0=8$ et $v_0=-19$, est une solution particulière de (2).. En multipliant par 2, on obtient une solution particulière de l'équation (1), et on en déduit l'ensemble des solutions de l'équation (1),

$$\{(16+21k,-38-50k), k\in\mathbb{Z}\}.$$