Chapitre 4 : Arithmétique dans $\mathbb{Z}$

Dans ce chapitre, « entier » signifie « élément de $\mathbb{Z}$ », et « entier naturel » ou « entier positif » « élément de $\mathbb{N}$ ».

Rappel : la relation de divisibilité est une relation d'ordre sur $\mathbb{N}$ (mais pas sur $\mathbb{Z}$).

I Diviseurs communs à deux entiers

Pour tous entiers a et b, notons $\mathcal{D}(a,b)$ l'ensemble des diviseurs communs de a et b dans $\mathbb{Z}$. On remarque tout de suite que $\mathcal{D}(0,0) = \mathbb{Z}$, et en dehors de ce cas, c'est-à-dire lorsque $(a,b) \neq (0,0)$, l'ensemble $\mathcal{D}(a,b)$ ne contient pas 0, est symétrique par rapport à 0, est fini et est aussi égal à $\mathcal{D}(|a|,|b|)$. C'est la raison pour laquelle, en pratique, on ne recherche que les diviseurs communs positifs de deux entiers positifs non tous deux nuls. Mais, afin de conserver la généralité des énoncés, nous n'allons pas, pour le cours, nous limiter aux entiers positifs.

A) PGCD et algorithme d'Euclide

Étant donnés deux entiers a et b, avec $(a,b) \neq (0,0)$, on cherche à déterminer l'ensemble $\mathcal{D}(a,b)$ des diviseurs communs de a et b.

Pour tout entier q, on a l'égalité : $\mathcal{D}(a,b) = \mathcal{D}(b, a-bq)$.

En particulier, si on suppose $b \neq 0$, la division euclidienne de a par b donne : $a = bq + r$ avec $0 \leqslant r < |b|$, et on a alors $\mathcal{D}(a,b) = \mathcal{D}(b,r)$. D'où l'algorithme suivant :

- On note $r_0 = |a|, r_1 = |b|$.
- Si $r_1 \neq 0$, la division euclidienne de r_0 par r_1 donne $r_0 = r_1 q_1 + r_2$ avec $0 \leqslant r_2 < r_1$
- Si $r_2 \neq 0$, la division euclidienne de r_1 par r_2 donne $r_1 = r_2 q_2 + r_3$ avec $0 \leqslant r_3 < r_2$
- Si $r_3 \neq 0$, la division euclidienne de r_2 par r_3 donne $r_2 = r_3 q_3 + r_4$ avec $0 \leqslant r_4 < r_3$
- Si $r_3 \neq 0$, la division euclidienne de r_2 par
- ...Si $r_k \neq 0$, la division euclidienne de r_{k-1} par r_k donne $r_{k-1} = r_k q_k + r_{k+1}$ avec $0 \leqslant r_{k+1} < r_k$

On s'arrête quand on obtient un reste nul, ce qui se produit nécessairement, sinon la suite $(r_k)_{k\in\mathbb{N}}$ formerait une suite strictement décroissante d'entiers naturels, ce qu'on sait impossible. Il existe donc $n \in \mathbb{N}$ tel que r_n est défini et non nul, mais le reste suivant, c'est-à-dire r_{n+1} est nul. Alors, compte tenu de la remarque précédente :

$$\mathcal{D}(a,b) = \mathcal{D}(r_0,r_1) = \mathcal{D}(r_1,r_2) = \ldots = \mathcal{D}(r_n, r_{n+1}) = \mathcal{D}(r_n, 0). \tag{4.1}$$

Or, $\mathcal{D}(r_n,0)$ est évidemment l'ensemble des diviseurs de r_n. Ainsi, l'ensemble des diviseurs communs à a et b est égal à l'ensemble des diviseurs de r_n. Donc r_n est un diviseur commun positif à a et b, et tout diviseur commun à a et b divise r_n. Donc r_n est le plus grand, au sens de la relation de divisibilité, des diviseurs communs positifs de a et b.

Théorème, définition :
Soient a, b deux entiers non tous deux nuls. L'ensemble des diviseurs communs positifs de a et b admet un plus grand élément, au sens de la divisibilité (qui l'est aussi au sens de $\leqslant$). On l'appelle le plus grand diviseur commun (PGCD) de a et b, noté $\text{pgcd}(a,b)$ ou $a \wedge b$.

Le PGCD de a et b est par conséquent l'unique entier δ tel que δ est un diviseur commun positif à a et b, et tout diviseur commun à a et b divise δ.

Avec l'algorithme d'Euclide, le PGCD de a et b est le dernier reste non nul.

Exemple :
L'algorithme d'Euclide appliqué à $a = 1236$ et $b = 96$ donne :

$$1236 = 96 \times 12 + 84, \quad 96 = 84 \times 1 + 12, \quad 84 = 12 \times 7 + 0, \tag{4.2}$$

donc $1236 \wedge 96 = 12$.

Définition :
Soient a, b deux entiers. On dit que a et b sont premiers entre eux lorsque les seuls diviseurs communs de a et b sont -1 et 1. Autrement dit, lorsque $(a,b) \neq (0,0)$ et $a \wedge b = 1$.

Proposition :
Soient a et b deux entiers non nuls, et soit $\delta = a \wedge b$. Si on pose $a = \delta a'$ et $b = \delta b'$, alors a' et b' sont premiers entre eux.

Démonstration :
Si a' et b' avaient un diviseur commun $d > 1$, alors $d\delta$ serait un diviseur commun à a et b strictement supérieur à δ.

II Égalité de Bézout

Théorème :
Soient a et b deux entiers non tous deux nuls. On a alors l'équivalence :

$$a \wedge b = 1 \iff \exists (u,v) \in \mathbb{Z}^2, au + bv = 1 \tag{4.3}$$

Démonstration :
Le sens $\implies$ est immédiat, puisque si d divise a et b, il divise $au + bv$ pour tous u, v de $\mathbb{Z}$, et donc divise 1.

Pour l'autre implication, on reprend ici les notations de l'algorithme d'Euclide : en particulier, n est l'élément de $\mathbb{N}$ tel que $r_n = a \wedge b$. Montrons par récurrence (sur k) que pour tout k entre 0 et $n+1$, il existe x_k et y_k dans $\mathbb{Z}$ tels que $ax_k + by_k = r_k$.

- Déjà, le résultat est vrai pour $k = 0$ et $k = 1$: $a.(\pm 1) + b.0 = r_0$ et $a.0 + b.(\pm 1) = r_1$ (selon les signes).
- Soit $k \in [\![1, n]\!]$, supposons que le résultat est vrai pour $k-1$ et k. On a alors $ax_{k-1} + by_{k-1} = r_{k-1}$, et $ax_k + by_k = r_k$. Si on retranche q_k fois la deuxième égalité de la première, on obtient $a(x_{k-1} -$

$q_k x_k) + b(y_{k-1} - q_k y_k) = r_{k-1} - q_k r_k$, c'est-à-dire $ax_{k+1} + by_{k+1} = r_{k+1}$, avec $x_{k+1} = x_{k-1} - q_k x_k$ et $y_{k+1} = y_{k-1} - q_k y_k$, ce qui achève la récurrence.

Ainsi, avec $k = n$, on a x_n et y_n dans $\mathbb{Z}$ tels que $ax_n + by_n = r_n$. Si $a \wedge b = 1$, on a donc bien l'existence de u et v comme voulus, puisque $r_n = a \wedge b = 1$.

Exemple :

Avec $a = 61$ et $b = 27$: on a $1.a + 0.b = 61$, $0.a + 1.b = 27$. Or, $61 = 27.2 + 7$, donc $1.a - 2.b = 7$. Et comme $27 = 7.3 + 6$, on a $-3.a + 7.b = 6$. Puis comme $7 = 6.1 + 1$, on a $4.a - 9.b = 1$.

Remarque :

La récurrence précédente est valable quelle que soit la valeur de $a \wedge b$, et cela montre que si $\delta = a \wedge b$, alors il existe u, v dans $\mathbb{Z}$ tels que $au + bv = \delta$. (La réciproque est fausse). Mais ce dernier résultat est aussi clair en multipliant par δ les deux membres de l'égalité de Bézout appliquée aux entiers a' et b' tels que $a' = \delta a$ et $b' = \delta b$, puisque ceux-ci sont premiers entre eux.

A) Le théorème de Gauss et autres propriétés

Proposition :

Pour tous entiers a, b non tous deux nuls, $a \wedge b = b \wedge a$. (Évident, puisque l'ensemble des diviseurs communs à a et b est évidemment celui des diviseurs communs à b et a !)

Proposition :

Pour tous entiers a, b non tous deux nuls, et tout entier c non nul, on a $ca \wedge cb = |c|(a \wedge b)$

Démonstration :

Notons $\delta = a \wedge b$. On a vu qu'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = \delta$. Donc $c\delta = cau + cbv$, et donc tout diviseur commun à ca et cb divise $c\delta$. De plus, $c\delta$ est évidemment un diviseur commun à ca et cb, donc $|c\delta| = |c|\delta$ est bien le PGCD de ca et cb.

Corollaire :

Soient a et b deux entiers non tous deux nuls, et soit d un diviseur commun à a et b. Si on pose $a = da'$ et $b = db'$, alors $|d|$ est le PGCD de a et b si et seulement si $a' \wedge b' = 1$.

Démonstration :

On a $a \wedge b = da' \wedge db' = |d|(a' \wedge b')$ d'où on tire immédiatement l'équivalence.

Théorème (Gauss) :

Soient trois entiers a, b, c. Si c divise le produit ab, et si c est premier avec b, alors c divise a.

Démonstration :

Si $a = 0$, le résultat est évident, sinon on peut écrire $ab \wedge ac = |a|(b \wedge c) = |a|$. Mais comme c divise ab et ac, il divise leur PGCD, c'est-à-dire a.

Théorème :
Soient trois entiers a, b et c. Si a est premier avec b et avec c, alors a est premier avec bc.

Démonstration :
Selon l'une des implications du théorème de Bézout, il existe des entiers relatifs u, u', v, v' tels que $au + bv = 1$ et $au' + cv' = 1$. En multipliant, on a alors :

$$a(auu' + cuv' + bu'v) + cbvv' = 1, \tag{4.4}$$

d'où le résultat par l'autre implication du théorème de Bézout.
On en déduit alors la proposition suivante par récurrence :

Proposition :
Si a est premier avec n nombres ($n \geqslant 2$) $b_1, b_2, \dots b_n$, alors a est premier avec leur produit.

Démonstration :
Pour $n = 2$, c'est le résultat précédent, et si c'est vrai pour $n - 1$, alors a est premier avec le produit $b_1 b_2 \dots b_n - 1$ et avec b_n, donc est premier avec $(b_1 b_2 \dots b_{n-1})b_n$ selon le résultat précédent.

Proposition :
Si a et b sont premiers entre eux, alors, pour tous entiers naturels m et p, a^m et b^p sont premiers entre eux.

Démonstration :
En effet, en supposant m et p non nuls (sinon c'est évident), et en appliquant le résultat précédent avec a et $b, b, \dots b$, on obtient $a \wedge b^p = 1$, puis en appliquant encore ce résultat avec b^p et $a, a, \dots a$, on obtient $a^m \wedge b^p = 1$.

Théorème :
Soient trois entiers a, b, c. Si b et c sont premiers entre eux et divisent a, alors bc divise a.

Démonstration :
a s'écrit ba', c divise ba' et est premier avec b donc, selon le théorème de Gauss, c divise a', et finalement bc divise a.
On en déduit par récurrence la proposition :

Proposition :
Si a est divisible par $b_1, b_2, \dots b_n$, et si les b_i sont premiers entre eux deux à deux, alors a est divisible par le produit des b_i.

Démonstration :
En effet, pour $n = 2$, c'est le résultat précédent, et si c'est vrai pour $n - 1$, alors a est divisible par $b_1 b_2 \dots b_{n-1}$ et par b_n, mais comme b_n est premier avec chaque b_i pour $1 \leqslant i \leqslant n - 1$, il est premier avec leur produit, donc a est divisible par $(b_1 b_2 \dots b_{n-1})b_n$ selon le résultat précédent.

Exemple :

Si 20 et 9 divisent a, alors 180 divise a, mais si 10 et 18 divisent a, cela ne prouve pas que 180 divise a (a pourrait être 90).

Donnons pour finir la résolution classique de l'équation $ax + by = c$.

a, b et c sont trois entiers (a et b sont supposés non nuls), et on cherche les solutions (x, y) dans $\mathbb{Z}^2$.

Notons δ le PGCD de a et b. Si c n'est pas un multiple de δ, il n'y a pas de solutions (car δ divise $ax + by$ pour tous x, y de $\mathbb{Z}$).

Supposons maintenant que $c = \delta c'$ avec $c' \in \mathbb{Z}$. Notre équation équivaut donc à l'équation $a'x + b'y = c'$, où a' et b' sont les nombres premiers entre eux tels que $a = \delta a'$ et $b = \delta b'$. Selon le théorème de Bézout, on peut trouver (et on connaît une méthode pour le faire) u et v dans $\mathbb{Z}$ tels que $a'u + b'v = 1$. On a donc une solution $(x_0, y_0) = (cu, cv)$ à notre équation. On doit maintenant trouver les autres.

Soit (x, y) une autre solution. On a : $a'x + b'y = c' = a'x_0 + b'y_0$, donc $a'(x - x_0) = -b'(y - y_0)$. Or, b' est premier avec a'. Donc selon le théorème de Gauss, il divise $x - x_0$. Il existe donc $k \in \mathbb{Z}$ tel que $x = x_0 + kb'$, et par remplacement on obtient $y = y_0 - ka'$.

Réciproquement, on remarque aisément que les couples $(x_0 + kb', y_0 - ka')$ avec $k \in \mathbb{Z}$ sont bien solutions. Ils constituent donc l'ensemble des solutions.

III PPCM

Proposition, définition :

Soient a, b deux entiers non nuls. L'ensemble des multiples communs strictement positifs de a et b admet un plus petit élément au sens de la divisibilité (donc aussi au sens de $\leqslant$). On l'appelle le plus petit multiple commun (PPCM) de a et b.

Démonstration :

L'ensemble des multiples communs à a et b (dans $\mathbb{Z}$) est $a\mathbb{Z} \cap b\mathbb{Z}$ qui est un sous-groupe de $(\mathbb{Z}, +)$, donc du type $\mu\mathbb{Z}$, avec $\mu \in \mathbb{N}$. μ n'est pas nul car ab, qui est non nul, appartient à ce sous-groupe. Le générateur positif μ est donc bien le plus petit multiple commun strictement positif, le sens « plus petit » étant pris pour la relation de divisibilité.

Proposition :

Soient a et b deux entiers positif non nuls. Alors $ab = \mu\delta$, où δ est le PGCD de a et b et μ le PPCM.

Démonstration :

Posons $a = \delta a'$, et $b = \delta b'$ avec $a' \wedge b' = 1$. Alors $\delta a'b'$ est un multiple commun à a et à b. Soit maintenant m un multiple commun de a et b. Alors $m = ax = by$, donc $m = \delta a'x = \delta b'y$. Donc $a'x = b'y$. Ainsi, b' divise $a'x$. Or, b' est premier avec a', donc b' divise x. Ainsi, $x = b'q$, donc $a'x = a'b'q$, donc $m = \delta a'b'q$. Donc tout multiple de a et b est multiple de $\delta a'b'$. Donc le plus petit multiple commun à a et b est $\mu = \delta a'b'$, d'où l'égalité $ab = \delta^2 a'b' = \mu\delta$.

On notera que si a et b sont premiers entre eux, alors le PGCD vaut 1 et le PPCM vaut ab.

IV Les nombres premiers

On appelle nombre premier tout entier naturel, strictement supérieur à 1, dont les seuls diviseurs positifs sont 1 et lui-même.

Les premiers nombres premiers sont 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41...Le crible d'Eratosthène permet de prolonger cette liste. Les résultats suivant s'obtiennent aisément :

- Si p est premier, alors p est premier avec tout nombre qu'il ne divise pas.
  En effet, pour tout entier a, le PGCD de a et p est un diviseur positif de p, donc vaut 1 ou p. Si ce n'est pas p, c'est 1. Il en résulte que deux nombres premiers distincts sont toujours premiers entre eux.
- Si $p_1, p_2, \dots p_n$ sont des nombres premiers distincts, et si pour tout i, $p_i^{k_i}$ divise a, alors a est divisible par les produit des $p_i^{k_i}$.
  C'est en effet une application directe d'un résultat déjà vu, en remarquant que les $p_i^{k_i}$ sont premiers entre eux deux à deux.
- Si p est premier et divise un produit de facteurs, alors p divise l'un des facteurs.
  En effet, sinon p serait premier avec chacun des facteurs, donc avec le produit. (Le résultat est faux si p n'est pas premier, par exemple 4 divise 2×6 mais 4 ne divise ni 2 ni 6).

Théorème :
Tout entier naturel strictement plus grand que 1 se décompose de manière unique (à commutativité près) en produit (éventuellement réduit à un seul terme) de nombres premiers.

Démonstration :
Existence : supposons que l'ensemble A des entiers strictement supérieurs à 1 n'admettant pas de décomposition en facteurs premiers soit non vide : il admet donc un plus petit élément a. Cet élément a n'est pas premier car sinon $a = a$ est une décomposition de a en facteurs premiers. Donc a s'écrit $a = bc$, avec $1 < b < a$ et $1 < c < a$. Mais comme a est le minimum de A, b et c ne sont pas éléments de A, et se décomposent donc en produit de facteurs premiers. Il en est donc de même pour a, ce qui mène donc à une contradiction.

Unicité : soit un entier naturel strictement plus grand que 1. Supposons qu'on ait deux décompositions. Après avoir éventuellement complété avec des p_i^0, on obtient $p_1^{r_1} p_2^{r_2} \dots p_n^{r_n} = p_1^{s_1} p_2^{s_2} \dots p_n^{s_n}$, où les r_i et les s_i sont des entiers naturels (dont certains sont éventuellement nuls). Ainsi, d'après le théorème de Gauss, $p_1^{r_1}$ divise le membre de droite, mais est premier avec $p_2, \dots p_n$, donc divise $p_1^{s_1}$, donc $r_1 \leqslant s_1$. De façon symétrique, $s_1 \leqslant r_1$. Donc $s_1 = r_1$, et on fait de même avec les autres puissances.

Théorème :
L'ensemble des nombres premiers est infini (démonstration connue depuis Euclide)

Démonstration :
Soient $p_1, p_2 \dots, p_n$ n nombres premiers. Montrons qu'il en existe nécessairement un autre. Soit q un diviseur premier du nombre $p_1 p_2 \dots p_n + 1$ (il en existe un car ce nombre se décompose en facteurs premiers). Alors q est nécessairement différent de chaque p_i, car p_i, qui divise $p_1 p_2 \dots p_n$, ne peut évidemment pas

diviser $p_1 p_2 \dots p_n + 1$ (car sinon il diviserait 1). Ainsi, q est un nombre premier différent de chaque p_i, d'où le résultat. (Remarque : il se peut que $q = p_1 p_2 \dots p_n + 1$)

Proposition :
Si $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ et $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$, où les p_i sont des nombres premiers distincts (et les α_i, β_i sont éventuellement nuls), alors le PGCD de a et b est égal à $p_1^{s_1} p_2^{s_2} \dots p_n^{s_n}$ où $s_i = \min(\alpha_i, \beta_i)$ et le PPCM de a et b est égal à $p_1^{t_1} p_2^{t_2} \dots p_n^{t_n}$, où $t_i = \max(\alpha_i, \beta_i)$.

Exemple :
$156 = 2^2 \times 3 \times 13$ et $24 = 2^3 \times 3$. Donc le PGCD vaut $2^2 \times 3 = 12$ et le PPCM vaut $2^3 \times 3 \times 13 = 312$. Cependant, rechercher le PGCD ou le PPCM en passant par la décomposition en facteurs premiers est inefficace pour des grands nombres, qu'on ne peut pas factoriser en temps raisonnable. Il est nettement préférable de déterminer le PGCD par l'algorithme d'Euclide.

Quelques repères historiques :

Euclide III^e^ siècle av. J-C .

Eratosthène III^e^ siècle av. J-C.

Bézout XVIII^e^ siècle.

Gauss début du XIX^e^ siècle.