LEÇON N° 5

Multiples et diviseurs dans $\mathbb{N}$, nombres premiers

Clément BOULONNE

Session 2020

Préambule

Niveau de la leçon

Collège, Terminale S Spé

Prérequis

Notions d'arithmétique : division, nombres entiers, construction de $\mathbb{N}$ et $\mathbb{Z}$

Références

— Contributeurs de WIKIPÉDIA, *Liste des critères de divisibilité*. Wikipédia.
— C. PARFENOFF, *Division euclidienne, division décimale*. Classe de Sixième. URL : `http://parfenoff.org`.
— J. ONILLON, *Vestiges d'une terminale S — Résolution générale des équations diophantiennes*. URL : `http://tanopah.com`.
— ZAUCTORE, *Équations diophantiennes du premier degré*. 3 octobre 2007. `http://www.mathforu.com/pdf/equation-diophantienne-premier-degre.pdf`.
— D.-J. MERCIER, *CAPES/AGREG Maths, Préparation intensive à l'entretien*. `http://megamaths.perso.neuf.fr/exgeo/preparationintensive.html`.
— F. HERBAUT, *Souvenirs d'oraux du CAPES 2011*. Académie de Nice. `http://fabien.herbault.free.fr/oraux/oraux_2011_v1.pdf`.
— Contributeurs de WIKIPÉDIA, *Équation diophantienne* $ax + by = c$. Wikipédia.
— X. DELAHAYE, *Conjectures*. Terminale S. URL : `xmaths.free.fr`.
— J.-P. QUELEN, *Petit théorème de Fermat et codage RSA*. 15 juillet 2011.
— M. LEZEN, *Leçon n° 14 : Congruences dans* $\mathbb{Z}$*. Anneau* $\mathbb{Z}/n\mathbb{Z}$. 2011. `www.cappes-de-maths.com/lecons/lecon14.pdf`.

Table des matières

1 Multiples et diviseurs

1.1 Définition

Définition 1.1. Soient a et b deux entiers relatifs. a est un multiple de b, si et seulement si, il existe un entier relatif k tel que : $a = kb$.

On dit aussi que :
— a est divisible par b ;
— b est un diviseur de a ;
— b divise a.

Exemples 1.2.
1. 54 est un multiple de 3 car $54 = 18 \times 3$.
2. -5 divise 45 car $45 = (-9) \times (-5)$.

1.2 Propriétés

PROPRIÉTÉS 1.3.
1. 0 est un multiple de tout entier.
2. 1 divise tout entier.
3. Si a est un multiple de b et si $a \neq 0$ alors $|a| \geq |b|$.
4. Si a divise b et si b divise a alors $a = b$ ou $a = -b$ avec a et b non nuls.

1.3 Règles de divisibilité

Toutes les règles de divisibilité peuvent être démontrées par la congruence.

PROPRIÉTÉS 1.4.
1. Un entier est divisible par 2 s'il se termine par 0, 2, 4, 6, 8.
2. Un entier est divisible par 5 s'il se termine par 0 ou 5.
3. Un entier est divisible par 10 s'il se termine par 0.

4. Un entier est divisible par 25 s'il se termine par 00, 25, 50, 75.
5. Un entier est divisible par 4 si le nombre formé par les deux derniers chiffres est divisible par 4.

Démonstration du critère de divisibilité par 2. $\Diamond$ Soit N un nombre entier. Il existe donc un B et a_0 tel que

$$N = 10B + a_0$$

avec $0 \leq a_0 \leq 9$. Or $10B$ est toujours multiple de 2 donc N est multiple de 2 si et seulement si a_0 est multiple de 2. □

Exemples 1.5.
1. 1932 est divisible par 4 car 32 est divisible par 4.
2. Par contre, 1714 n'est pas divisible par 4 car 14 n'est pas divisible par 4.

PROPRIÉTÉS 1.6.
1. Un entier est divisible par 3 si la somme des chiffres est divisible par 3.
2. Un entier est divisible par 9 si la somme des chiffres est divisible par 9.

Démonstration du critère de divisibilité par 3. $\Diamond$ Soit N un entier naturel divisible par 3. On a alors :

$$3 \mid N \Leftrightarrow N \equiv 0 \pmod 3.$$

On pose

$$N = a_0 + a_1 \times 10 + a_2 \times 10^2 + \cdots + a_n \times 10^n.$$

Or $10 \equiv 1 \pmod 3$ donc

$$N \equiv 0 \pmod 3 \Leftrightarrow a_0 + a_1 + \cdots + a_n \equiv 0 \pmod 3.$$

Ainsi, lorsqu'un nombre est divisible par 3, la somme des chiffres de ce nombre est divisible par 3. □

Exemples 1.7.
1. 8232 est divisible par 3 car $8 + 2 + 3 + 5 = 15$ et 15 est divisible par 3.
2. 4365 est divisible par 9 car $4 + 3 + 6 + 5 = 18$ et 18 est divisible par 9.

PROPRIÉTÉ 1.8. D'une façon générale un entier est divisible par 11 si la différence entre la somme des chiffres de rangs pairs et la somme des chiffres de rangs impairs est divisible par 11.

Exemples 1.9.
1. 6457 est divisible par 11 car :

$$(7 + 4) - (5 + 6) = 11 - 11 = 0$$

et 0 est divisible par 11.

2. 4939 est divisible par 11 car :

$$(9 + 9) - (3 + 4) = 18 - 7 = 11$$

et 11 est divisible par 11.

PROPRIÉTÉ 1.10 (CRITÈRE DE DIVISIBILITÉ PAR 7). Un nombre est *divisible par* 7 si et seulement si le résultat de la soustraction du *nombre de dizaines* par le double du chiffre des unités est multiple de 7.

La démonstration nécessite la connaissance du théorème de Gauss (voir théorème **??**).

Démonstration du critère de divisibilité par 7. $\Diamond$ Soit N un nombre entier divisible par 7. On pose

$$N = a_0 + a_1 \times 10 + \cdots + a_n \times 10^n.$$

On a :

$$7 \mid 10(a_1 + a_2 \times 10 + \cdots + a_n \times 10^{n-1} - 2a_0).$$

Or 7 et 10 sont premiers entre eux, donc d'après le théorème de Gauss :

$$7 \mid a_1 + a_2 \times 10 + \cdots + a_n \times 10^{n-1} - 2a_0.$$

Réciproquement si

$$7 \mid a_1 + a_2 \times 10 + \cdots + a_n \times 10^{n-1} - 2a_0$$

alors

$$7 \mid 10(a_1 + a_2 \times 10 + \cdots + a_n \times 10^{n-1} - 2a_0)$$

Or, $7 \mid 21$ donc

$$7 \mid a_1 \times 10 + a_2 \times 10^2 + \cdots + a_n \times 10^n - 20a_0 + 21a_0.$$

On obtient ainsi $7 \mid N$. □

Exemple 1.11. 252 est divisible par 7 car son nombre de dizaine est 25, son chiffre des unités est 2 et

$$25 - 2 \times 2 = 25 - 4 = 21 \quad \text{(divisible par 7)}.$$

Exemple 1.12. Grâce aux règles de divisibilité, on montre facilement que :

1. Les diviseurs de 20 sont : 1, 2, 4, 5, 10, 20
2. Les diviseurs de 36 sont : 1, 2, 3, 4, 6, 9, 12, 18, 36
3. Les diviseurs de 120 sont : 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120

1.4 Décompositions en facteurs premiers

THÉORÈME 1.13. Soient a et b deux entiers naturels tels que :

$$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \quad \text{et} \quad b = p_1^{\beta_1} \cdots p_k^{\beta_k}.$$

Alors :

$$\mathrm{PGCD}(a, b) = p_1^{\delta_1} \cdots p_k^{\delta_k}$$

avec $\delta_i = \min(\{\alpha_i, \beta_i\})$.

Démonstration du théorème 1.13. $\Diamond$ Soit $d = p_1^{\delta_1} \cdots p_k^{\delta_k}$. On vérifie que d est bien un diviseur commun de a et de b. Réciproquement, soit d' un diviseur commun de a et de b. Tout facteur premier p de d est aussi un facteur premier de a et de b. Si p_i^{δ} divise a et b alors $\delta \leq \alpha_i$ et $\delta \leq \beta_i$ onc :

$$\delta \leq \delta_i = \min(\{\alpha_i, \beta_i\}).$$

Cela entraîne que d' est un diviseur de d. Donc d est le PGCD de a et de b. □

1.5 Un exercice d'application

Exercice 1.14. 1. Déterminer tous les couples d'entiers naturels tels que :

$$x^2 - 2xy = 15.$$

2. Déterminer tous les entiers relatifs n tels que $(n-3)$ divise $n+5$.

Solution. $\Diamond$

1. On cherche à mettre le terme de droite en facteur de façon à faire apparaître des diviseurs de 15. En factorisant, on trouve :
$$x(x-2y) = 15.$$
Comme x et y sont des entiers naturels, on a la relation suivante : $x \geq x - 2y$. De plus, les diviseurs de 15 sont :
$$D_{15} = \{1, 3, 5, 15\}.$$
Les décompositions possible sont donc :
$$\begin{cases} x = 15 \\ x - 2y = 1 \end{cases} \quad \text{ou} \quad \begin{cases} x = 5 \\ x - 2y = 3 \end{cases}$$
soit
$$\begin{cases} x = 15 \\ y = \frac{15-1}{2} = 7 \end{cases} \quad \text{ou} \quad \begin{cases} x = 5 \\ y = \frac{5-3}{2} = 1 \end{cases}.$$
On obtient alors les couples solutions : $(15, 7)$ et $(5, 1)$.
2. Si $(n-3)$ divise $(n+5)$ alors il existe un entier k tel que :
$$n + 5 = k(n-3)$$
On cherche à factoriser par $(n-3)$ en faisant ressortir ce terme à gauche :
$$\begin{aligned} (n-3) + 8 &= k(n-3) \\ k(n-3) - (n-3) &= 8 \\ (n-3)(k-1) &= 8 \end{aligned}$$
donc $(n-3)$ est un diviseur de 8. L'ensemble des diviseurs de 8 dans $\mathbb{Z}$ est :
$$D_8 = \{-8, -4, -2, -1, 1, 2, 4, 8\}.$$
On a donc le tableau suivant correspond aux valeurs possibles de n :

$n-3$	-8	-4	-2	-1	1	2	4	8
n	-5	-1	1	2	4	5	7	11

$\square$

1.6 Opérations sur les multiples

THÉORÈME 1.15. Soit trois entiers relatifs a, b et c.
Si a divise b et c alors a divise $a+b$, $a-b$ ou toutes combinaison linéaire de b et de c.

Démonstration. $\Diamond$ On sait que a divise b et c, donc il existe deux entiers relatifs k et k' tels que :

$$b = ka \quad \text{et} \quad c = k'a.$$

On a alors :

$$b + c = (k + k')a, \quad b - c = (k - k')a \quad \text{et} \quad \alpha b + \beta c = (\alpha k + \beta k')a.$$

Donc a divise $b + c$, $b - c$ et $\alpha b + \beta c$. □

Exemple 1.16. Soit k un entier naturel, on pose $a = 9k + 2$ et $b = 12k + 1$. On cherche les diviseurs positifs communs à a et b.

Soit d un diviseur commun à a et b. Comme d divise a et b, il divise $c = 4a - 3b$, soit :

$$c = 4(9k + 2) - 3(12k + 1) = 36k + 8 - 36k - 3 = 5$$

donc d divise 5. Comme 5 n'a que 2 diviseurs positifs, 1 et 5, on a alors $d = 1$ et $d = 5$.

Les diviseurs positifs possibles communs à a et b sont 1 et 5.

1.7 Division euclidienne

Définition 1.17. Soit a un entier relatif et b un entier naturel non nul.
On appelle division euclidienne de a par b, l'opération qui au couple (a, b) associe le couple (q, r) tels que :

$$a = bq + r \quad \text{avec } 0 \leq r < b.$$

a s'appelle le dividende, b le diviseur, q le quotient et r le reste.

Exemples 1.18.
1. La division euclidienne de 114 par 8 : $114 = 8 \times 14 + 2$
2. La division de -17 par 3 : $17 = 3 \times (-6) + 1$.

Exercice 1.19.
1. Trouver tous les entiers qui divisés par 5 donne un quotient égal à 3 fois le reste.
2. Lorsqu'on divise a par b, le reste est 8 et lorsqu'on divise $2a$ par b, le reste est 5. Déterminer le diviseur b.

Solution. $\Diamond$

1. Soit a l'entier cherché. On divise a par 5, on a alors :

   $$a = 5q + r \quad \text{avec } 0 \leq r < 5$$

   Comme $q = 3r$, on a :

   $$a = 15r + r = 16r \quad \text{avec } 0 \leq r < 5$$

   On trouve toutes les valeurs de a en faisant varier r de 0 à 4 compris, on a alors l'ensemble solution suivant :

   $$S = \{0, 16, 32, 48, 64\}.$$

2. Écrivons les deux divisions, en notant q et q' les restes respectifs :

   $$\begin{aligned} 2bq + 16 &= bq' + 5 \quad \text{avec } b > 8 \\ b(2q - q') &= -11 \\ b(q' - 2q) &= 11 \end{aligned}$$

   On en déduit que p est un multiple positif non nul de 11, supérieur à 8, donc : $b = 11$.

□

Algorithme. On propose un algorithme sur Xcas qui effectue une division euclidienne par soustraction successives :

```
diveucl(a,b) fonction
  local r,q;
  si b < 0 alors
    b := -b;
    a := -a;
  fsi
  q := 0;
  r := a;
  si a >= 0 alors
    tantque r>=b faire
      r := r-b;
      q := q+1;
    ftantque
   sinon
     tantque r<0 faire
      r := r+b;
      q := q-1;
     ftantque
  fsi
    afficher(q);
    afficher(r);
ffonction:;
```

2 Nombres premiers

2.1 Définition

Définition 2.1. Soit $p \geq 2$ un nombre entier naturel. On dit que p est un nombre *premier* si p admet exactement deux diviseurs distincts : 1 et lui-même.

Exemples 2.2.
1. 7 est un nombre premier car il admet comme diviseurs 1 et 7.
2. 13 est un nombre premier car il admet comme diviseurs 1 et 13.
3. 9 n'est pas un nombre premier car il admet trois diviseurs : 1, 3 et 9.

Remarques 2.3.
1. La définition exclut 1 comme potentiel nombre premier. il n'a qu'un seul diviseur distinct, lui-même.
2. Attention : ne pas confondre nombre premier avec nombres premiers entre eux. On dit que deux nombres a et b sont premiers entre eux si $\mathrm{PGCD}(a, b) = 1$, ou ils n'ont comme plus grand diviseur commun 1.

2.2 Quelques propriétés sur les nombres premiers

PROPRIÉTÉ 2.4. L'ensemble des nombres premiers est un ensemble infini.

Démonstration. $\Diamond$ On suppose que l'ensemble $\mathcal{P}$ des nombres premiers est un ensemble non vide ayant un nombre fini d'éléments (2 est un nombre premier car 2 a pour diviseurs 1 et 2).

Ainsi :

$$P = \{p_1, \ldots, p_n\}$$

où n est un nombre entier naturel non nul et p_1, ..., p_n sont des nombres premiers. Á partir des éléments de $\mathcal{P}$, on peut construire $N := p_1 \times \cdots \times p_n$. On a alors : $N + 1 := (p_1 \times \cdots \times p_n) + 1$ et quand on fait la division euclidienne de $N + 1$ avec p_i ($1 \leq i \leq n$), on trouve comme reste 1. On peut donc affirmer que $N + 1$ est donc un nombre premier. Il y a donc une contradiction avec l'hypothèse de départ car on peut donc, à partir de n nombres premiers, fabriquer un nouveau nombre premier. L'ensemble des nombres premiers est donc un ensemble infini. □

PROPRIÉTÉ 2.5. Soit n un entier supérieur ou égal à 2 ; n est premier si, et seulement si, n n'a pas de diviseur premier inférieur ou égal à $\sqrt{n}$.

Démonstration. ◊ Soit n un entier supérieur ou égal à 2.

— On suppose que n est premier, n admet alors exactement deux diviseurs 1 et n. 1 est donc le seul diviseur de n inférieur ou égal à $\sqrt{n}$.

— Réciproquement, on suppose que n n'a pas de diviseur premier inférieur ou égal à $\sqrt{n}$ et on montre (par un raisonnement par l'absurde) que n est premier.
Supposons que n n'est pas premier. L'ensemble des diviseurs de n (dans $\mathbb{N}$) autres que 1 et n étant non vide, il admet un plus petit élément m. On peut montrer que m est un nombre premier par un raisonnement par l'absurde.
Supposons que m ne soit pas premier alors il aurait comme diviseur k avec $1 \leq k \leq m$. Or comme $m \mid n$ et que $k \mid m$, on aurait $k \mid n$. Ce qui est absurde car le plus petit diviseur de n est m. m n'a donc comme diviseurs 1 et m, m est donc premier.
m divise n et m premier donc il existe un k tel que $1 < m \leq k < n$ et $n = mk$. Comme $n = mk$ et $1 < m \leq k < n$, on en déduit donc :

$$1 < m \times m \leq mk \Leftrightarrow 1 < m^2 \leq n.$$

Comme $m > 0$ et $n > 0$, on peut appliquer la racine carrée dans les deux membres de l'inégalité $m \leq \sqrt{n}$. Ce qui est absurde car n n'a pas de diviseur premier inférieur ou égal à $\sqrt{n}$.
Donc : n est premier.

□

THÉORÈME 2.6 (LEMME D'EUCLIDE). Si un nombre premier p divise le produit de deux nombres entiers b et c, alors p divise b ou c.

Démonstration. ◊ Si p ne divise pas a alors p et a sont premiers entre eux. En utilisant le lemme de Gauss (voir remarque), on en déduit que $p \mid b$. □

Remarque 2.7. Le lemme de Gauss (ou théorème de Gauss en Terminale S) est une généralisation du lemme d'Euclide : « Soient a, b et c des entiers relatifs non nuls. Si p divise le produit bc, et si a et b sont premiers entre eux, alors a divise c. »

Démonstration du lemme de Gauss. ◊ Comme a divise bc, il existe un entier k tel que $bc = ka$. Comme a et b sont premeirs entre eux, d'après le théorème de Bézout, il existe des entiers relatifs u et v tels que $au + bv = 1$.

En multipliant par c cette dernière égalité, on obtient :

$$c = acu + bcv = acu + kav = a(cu + kv).$$

Comme $(cu + kv)$ est un entier, cette égalité prouve que a divise c. □

3 Congruences dans $\mathbb{Z}$

3.1 Définitions et propriétés

Définition 3.1 (Congruence). Soient $n \in \mathbb{N}$ et $a, b \in \mathbb{Z}$. On dit que a est *congru* à b *modulo* n si $n \mid a - b$. On note alors $a \equiv b \pmod{n}$.

Exemples 3.2.
1. $11 \equiv 1 \pmod{5}$ car $5 \mid 11 - 1$.
2. $25 \equiv 4 \pmod{7}$ car $7 \mid 25 - 4$.

Définition 3.3. Soient $n \in \mathbb{N}$ et $a, b \in \mathbb{Z}$. On dit que a est *congru* à b *modulo* p, si a et b ont le même reste dans la division euclidienne par p.

Nous avons donné deux définitions de congruence. On montre qu'elles sont équivalentes.

Démonstration. $\Diamond$
— Supposons que a et b ont le même reste r dans la division euclidienne par p. On peut donc écrire

$$a = p \times k + r \quad \text{et} \quad b = p \times k' + r \quad \text{avec } k, k' \in \mathbb{Z}, r \in \mathbb{N} \text{ et } 0 \leq r \leq p.$$

donc

$$b - a = p \times k' + r - (p \times k) + r = p \times k' - p \times k = p(k' - k).$$

$k' - k$ étant un entier relatif, on en déduit que $b - a$ est multiple de p.
— Supposons que $b - a$ est multiple de p, on peut écrire $b - a = k \times p$ avec $k \in \mathbb{Z}$. On note q et r le quotient et le reste de la division euclidienne de b par p. On a donc $b = p \times q + r$. Alors, en remplaçant dans l'égalité $b - a = k \times p$, on obtient

$$p \times q + r = a = kp.$$

Donc

$$A = p \times q + r - kp = p(q - k) + r$$

$q - k$ est un entier relatif et r est un entier naturel tel que $0 \leq r < p$. On en déduit que r est le reste de la division euclidienne de a par p. Donc a et b ont le même reste dans la division euclidienne par p.

□

PROPRIÉTÉS 3.4.
1. Si $a \equiv b \pmod{p}$ et $b \equiv c \pmod{p}$ alors $a \equiv c \pmod{p}$.
2. Si $a \equiv b \pmod{p}$ et si $a' \equiv b' \pmod{p}$ alors
   — $a + a' \equiv b + b' \pmod{p}$,
   — $aa' \equiv bb' \pmod{p}$,
   — $a^n \equiv b^n \pmod{p}$, $n \in \mathbb{N}^*$.
3. Si $a \equiv b \pmod{p}$ alors, pour tout $c \in \mathbb{Z}$,
   — $a + c \equiv b + c \pmod{p}$,
   — $a - c \equiv b - c \pmod{p}$,
   — $ac \equiv bc \pmod{p}$.

Démonstration des propriétés 3.4. $\Diamond$
1. Si $a \equiv b \pmod{p}$ et $b \equiv c \pmod{p}$ alors a et b ont le même reste dans la division euclidienne par p et b et c ont le même reste dans la division euclidienne par p donc a et c ont le même reste dans la division euclidienne par p et par conséquent $a \equiv c \pmod{p}$.

2. Si $a \equiv b \pmod{p}$ et si $a' \equiv b' \pmod{p}$ alors $b-a$ est un multiple de p et $b'-a'$ est un multiple de p. On en déduit, d'après les propriétés des multiples que $(b-a)+(b'-a')$ et $(b-a)-(b'-a')$ sont des multiples de p, c'est-à-dire $(b+b')-(a+a')$ et $(b-b')-(a-a')$ sont des multiples de p donc :

$$a+a' \equiv b+b' \pmod{p} \quad \text{et} \quad a-a' \equiv b-b' \pmod{p}.$$

D'autre part, puisque $b-a$ est un multiple de p, $a'(b-a)$ est un multiple p et puisque $b'-a'$ est un multiple de p, $b(b'-a')$ est un multiple de p et par conséquent $a'(b-a)+b(b'-a')$ est un multiple de p, c'est-à-dire $a'b-a'a+bb'-ba'$ est un multiple de p donc $bb'-aa'$ est un multiple de p donc

$$aa' \equiv bb' \pmod{p}.$$

Enfin considérons, pour $n \in \mathbb{N}^*$, la proposition $P(n)$: « $a^n \equiv b^n \pmod{p}$. Pour $n=1$, on a $a^1 = 1$et $b^1 = b$ et on sait que $a \equiv b \pmod{p}$ donc $P(1)$ est vraie. Supposons la proposition $P(n)$ vraie pour un entier $n \geq 1$ alors $a^n \equiv b^n \pmod{p}$ et comme on a aussi $a \equiv b \pmod{p}$, on peut en utilisant la propriété précédente justifier que $a^n \times a \equiv b^n \times b \pmod{p}$ soit $a^{n+1} \equiv b^{n+1} \pmod{p}$, c'est-à-dire la proposition $P(n+1)$ est vraie. On a donc démontré par récurrence que $P(n)$ est vraie pour tout entier $n \geq 1$.

3. Si $a \equiv b \pmod{p}$ alors $b-a$ est un multiple de p mais on peut écrire :

$$b-a = (b+c)-(a+c)$$

donc $(b+c)-(a+c)$ est un multiple de p, donc

$$a+c \equiv b+c \pmod{p} \quad \text{pour tout } c \in \mathbb{Z}$$

De même, on peut écrire $b-a = (b-c)-(a-c)$ donc

$$a-c \equiv b-c \pmod{p} \quad \text{pour tout } c \in \mathbb{Z}.$$

D'autre part, puisque $b-a$ est un multiple de p alors, pour tout $c \in \mathbb{Z}$, $c(b-a)$ est un multiple de p, c'est-à-dire $bc-ac$ est un multiple de p donc

$$ac \equiv bc \pmod{p} \quad \text{pour tout } c \in \mathbb{Z}.$$

□

Exemples 3.5. 1. On démontre que, pour tout $n \in \mathbb{N}$, $10^n-(-1)^n$ est divisible par 11. On peut écrire $10 \equiv -1 \pmod{11}$ donc pour tout $n \in \mathbb{N}$, $10^n \equiv (-1)^n \pmod{11}$ et ainsi, $10^n-(-1)^n$ est divisible par 11.

3.2 Compléments : l'anneau $\mathbb{Z}/n\mathbb{Z}$

PROPOSITION 3.6. La relation de congruence modulo n est une relation d'équivalence

Démonstration. ◊ Les propriétés de reflexivité, symétricité et transitivité sont démontrées dans la section précédente. □

Remarque 3.7. Soit $a \in \mathbb{Z}$. On note $\overline{a}$ la classe d'équivalence de a pour cette relation, c'est-à-dire :

$$\overline{a} = \{b \in \mathbb{Z},\ a \equiv b \pmod{n}\}.$$

Définition 3.8 ($\mathbb{Z}/n\mathbb{Z}$). L'ensemble des classes d'équivalence de $\mathbb{Z}$ par cette relation est l'ensemble quotient noté $\mathbb{Z}/n\mathbb{Z}$.

Conséquence 3.9. Pour tout $a \in \mathbb{Z}$, il existe un unique $r \in \mathbb{Z}$ tel que :

$$\begin{cases} 0 \leq r < n \\ \overline{a} = \overline{r} \end{cases}$$

Démonstration. $\Diamond$

Existence Soit $a \in \mathbb{Z}$, il existe $(q, r) \in \mathbb{Z}^2$ tel que :

$$\begin{cases} a = qn + r \\ 0 \leq r \leq n \end{cases}$$

Or, $a \equiv r \pmod{n}$ car $r = 0n + r$ et $0 \leq r < n$, donc $\overline{a} = \overline{r}$. En effet,

$$\overline{a} = \{b \in \mathbb{Z},\ b \equiv a \pmod{n}\} = \{b \in \mathbb{Z},\ b \equiv r \pmod{n}\} = \overline{r}.$$

Unicité Supposons qu'il existe un autre $r' \in \mathbb{Z}$ tel que $0 \leq r' < n$ et $\overline{r'} = \overline{a}$ donc $|r - r'| < n$ et $\overline{r} = \overline{r'}$, c'est-à-dire $r \equiv r' \pmod{n}$ ou il existe $k \in \mathbb{Z}$ tel que $r - r' = nk$. D'où : $|r - r'| = n\,|k| < n$ donc $|k| < 1$ car $n > 0$, donc $k = 0$ c'est-à-dire $r = r'$.

□

PROPOSITION 3.10.

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \ldots, \overline{n-1}\right\}$$

et $\operatorname{card}(\mathbb{Z}/n\mathbb{Z}) = n$.

Démonstration. $\Diamond$ D'après ce qui précède, $\mathbb{Z}/n\mathbb{Z} \subset \left\{\overline{0}, \ldots, \overline{n-1}\right\}$. En effet, soit $a \in \mathbb{Z}$, $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ alors il existe $r \in \mathbb{Z}$ tel que $0 \leq r < n$ et $\overline{r} = \overline{a}$, donc $\overline{a} = \overline{r} \in \left\{\overline{0}, \ldots, \overline{n-1}\right\}$ donc :

$$\left\{\overline{0}, \ldots, \overline{n-1},\ \subset\right\} \mathbb{Z}/n\mathbb{Z},$$

c'est-à-dire $\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \ldots, \overline{n-1}\right\}$.

De plus, soit $a \in \{0, \ldots, n-1\}$. Il existe $r \in \mathbb{Z}$ tel que $0 \leq r < n$ et $\overline{r} = \overline{a}$ et ce r est unique donc $a = r$.

Ainsi :

$$\begin{cases} a \equiv a \pmod{n} \\ a \not\equiv i \pmod{n} \end{cases} \quad \text{pour tout } i \in \{0, \ldots, n-1\} \text{ tel que } i \neq a$$

c'est-à-dire :

$$\begin{cases} a \in \overline{a} \\ a \in \overline{i} \end{cases} \quad \text{pour tout } i \in \{0, \ldots, n-1\} \text{ tel que } i \neq a$$

donc les éléments de $\left\{\overline{0}, \ldots, \overline{n-1}\right\}$ sont deux à deux distincts. □

THÉORÈME 3.11. On définit deux lois de composition interne sur $\mathbb{Z}/n\mathbb{Z}$ tel que pour tout $(a, b) \in \mathbb{Z}^2$:

$$\begin{cases} \overline{a} + \overline{b} = \overline{a + b} \\ \overline{a} \times \overline{b} = \overline{a \times b} \end{cases}$$

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif unifère.

Démonstration. ◊ La loi :

$$\begin{array}{rccc} + & : & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & & (a \times b) & \mapsto & \overline{a} + \overline{b} = \overline{a+b} \end{array}$$

est une loi de composition interne, car c'est une application $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ (cela provient du fait que la relation de congruence est compatible avec l'addition). De plus, cette application est indépendante du représentant choisi.

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif unifère provient du fait que $(\mathbb{Z}, +, \times)$ est un anneau commutatif unifère. □

Remarques 3.12.
1. $\mathbb{Z}/1\mathbb{Z} = \left\{\overline{0}\right\}$ n'est pas unitaire.
2. $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre. $\overline{3}$ et $\overline{2} \in \mathbb{Z}/6\mathbb{Z}$ donc $\overline{3} \times \overline{2} = \overline{6} = \overline{0}$ mais $\overline{3} \neq \overline{0}$ et $\overline{2} \neq \overline{0}$.

THÉORÈME 3.13. Soit $m \in \mathbb{N} \setminus \{0\}$. $\mathrm{PGCD}(m, n) = 1$ si et seulement si $\overline{m}$ est un élément inversible de $\mathbb{Z}/n\mathbb{Z}$.

Démonstration. ◊
($\Rightarrow$) $\mathrm{PGCD}(m, n) = 1$, donc d'après le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $un + vm = 1$, donc :

$$\overline{u} \times \overline{n} + \overline{v} \times \overline{m} = \overline{1} \Leftrightarrow \overline{v} \times \overline{m} = 1$$

car $\overline{n} = \overline{0}$ donc $\overline{m}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.
($\Leftarrow$) Soit $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ tel que il existe $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ et $\overline{a} \times \overline{m} = \overline{1}$ donc $\overline{am} = \overline{1}$ et ainsi $am \equiv 1 \pmod{n}$. Il existe docn $k \in \mathbb{Z}$ tel que $a \times m - kn = 1$, c'est-à-dire $\mathrm{PGCD}(n, m) = 1$.

□

Corollaire 3.14. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si n est premier.

Démonstration. ◊

$$\begin{aligned} (\mathbb{Z}/n\mathbb{Z}, +, \times) \text{ est un corps} &\Leftrightarrow \forall \overline{m} \in \mathbb{Z}/n\mathbb{Z}, \quad \overline{m} \text{ est inversible et } \overline{m} \neq \overline{0} \\ &\Leftrightarrow \forall m \in \mathbb{Z},\ \mathrm{PGCD}(m, n) = 1 \text{ et } n \text{ ne divise pas } m \\ &\Leftrightarrow n \text{ est premier.} \end{aligned}$$

□

Remarque 3.15. L'ensemble des éléments de $(\mathbb{Z}/n\mathbb{Z}, \times)$ est un groupe.

THÉORÈME 3.16. Soit $m \in \mathbb{N}\setminus\{0\}$. $\mathrm{PGCD}(m, n) = 1$ si et seulement si $\overline{m}$ engendre $(\mathbb{Z}/m\mathbb{Z}, +)$.

Démonstration. ◊
($\Rightarrow$) $\overline{m}$ engendre $(\mathbb{Z}/n\mathbb{Z}, +)$ signifie que

$$G(\overline{m}) = \{k\overline{m},\ \forall k \in \mathbb{Z}\} =$$

Il suffit de démontrer que $\overline{1} \in G(\overline{m})$ afin d'avoir $(\mathbb{Z}/n\mathbb{Z}, +) \subset G(\overline{m})$. En effet,si $\overline{1} \in G(\overline{m})$, alors soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$.
$\overline{x} = \overline{1} \times \overline{x} \in G(\overline{m})$ car $\overline{1}G(\overline{m})$ et $\overline{x} \in \mathbb{Z}/n\mathbb{Z} \subset \mathbb{Z}$.
Par hypothèse, $\mathrm{PGCD}(n, m) = 1$, donc d'après le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $nu+mv = 1$, donc $\overline{nu}+\overline{mv} = \overline{1}$. Or $\overline{n} = 0$ donc $\overline{1} = \overline{vm} \in G(\overline{m})$ car $\overline{v} \in \mathbb{Z}/n\mathbb{Z} \subset \mathbb{Z}$.
Montrons que $(\mathbb{Z}/n\mathbb{Z}, + \supset G(\overline{m})$. Soit $\overline{x} \in G(\overline{m})$. Il existe $k \in \mathbb{Z}$ tel que $\overline{x} = k\overline{m}$ donc

$$\overline{x} = \underbrace{\overline{m} + \cdots + \overline{m}}_{k \text{ fois}} \in \mathbb{Z}/n\mathbb{Z}$$

car $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe.

($\Leftarrow$) Comme $\overline{m}$ engendre $(\mathbb{Z}/n\mathbb{Z}, +)$, on a donc $G(\overline{m}) = (\mathbb{Z}/n\mathbb{Z}, +)$. Or $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$, donc il existe $k \in \mathbb{Z}$ tel que $\overline{1} = k\overline{m}$ donc $km \equiv 1 \pmod{n}$ donc il existe $k' \in \mathbb{Z}$ tel que $km - k'n = 1$, c'est-à-dire $\mathrm{PGCD}(m, n) = 1$.

□

Corollaire 3.17. $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique d'ordre n. Ce groupe est engendré par la classe de tout entier p premier avec n.

Démonstration. $\Diamond$ $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe fini d'ordre n et monogène car $\overline{1}$ est générateur.
D'après ce qui précède, si $\mathrm{PGCD}(p, n) = 1$ alors $\overline{p}$ engendre $(\mathbb{Z}/n\mathbb{Z}, +)$. □

4 Applications

4.1 Reste

On souhaite déterminer les restes successifs dans la division par 7 des nombres suivants :

$$50^{100},\ 100,\ 100^3,\ 50^{100} + 100^{100}.$$

1. On détermine le reste de 50^{100} par la division par 7. On a $50 \equiv 1 \pmod{7}$ car $50 = 7 \times 7 + 1$. D'après la compatibilité avec les puissances, on a :
$$50^{100} \equiv 1^{100} \equiv 1 \pmod{7}.$$
Le reste est 1.
2. On détermine le reste de 100 par la division par 7. $100 = 50 \times 2$, comme $50 \equiv 1 \pmod{7}$, d'après la compatibilité avec la multiplication, on a :
$$100 \equiv 2 \pmod{7}.$$
Le reste est 2.
3. Pour déterminer le reste de 100^3 par la division par 7, on utilise la question précédente et la compatibilité avec les puissances. On a :
$$100^3 \equiv 2^3 \equiv 8 \equiv 1 \pmod{7}.$$
Le reste est 1.
4. On détermine le reste de $50^{100} + 100^{100}$ par la division par 7. On a : $100^{100} = 100^{3\times 33+1} = (100^3)^{33} \times 100$, donc d'après la compatibilité avec les puissances et la multiplication, on a :
$$100^{100} \equiv 1^{33} \times 2 \equiv 2 \pmod{7}.$$
Par compatibilité avec l'addition, on a alors :
$$50^{100} + 100^{100} \equiv 1 + 2 \equiv 3 \pmod{7}.$$

4.2 Divisibilité

On va montrer que, pour tout $n \in \mathbb{N}$, $3^{n+3} - 4^{4n+2}$ est divisible par 11.
On a : $3^{n+3} = 3^n \times 3^3 = 27 \times 3^n$, or $27 \equiv 5 \pmod{11}$, donc d'après la compatibilité avec la multiplication, on a :

$$3^{n+3} \equiv 5 \times 3^n \pmod{11}.$$

On a : $4^{4n+2} = (4^4)^n \times 4^2$, or $4^2 \equiv 5 \pmod{11}$ donc $4^4 \equiv 5^2 \equiv 3 \pmod{11}$, donc :

$$4^{4n+2} \equiv 3^n \times 5 \pmod{11}.$$

On en déduit donc :

$$3^{n+3} - 4^{4n+2} \equiv 0 \pmod{11}.$$

La proposition est donc vérifiée, pour tout $n \in \mathbb{N}$.

4.3 Petit théorème de Fermat

THÉORÈME 4.1 (PETIT THÉORÈME DE FERMAT). Soit p un nombre premier et a un entier naturel premier avec p alors $a^{p-1}-1$ est divisible par p. En d'autres termes $a^{p-1} \equiv 1 \pmod{p}$.

Démonstration du théorème 4.1. $\Diamond$ p ne divise aucun nombre de la suite a, $2a$, ..., $(p-1)a$. En effet, d'après le théorème de Gauss, si p divisait un de ces produits ka, p diviserait k puisque a et p sont premiers entre eux. Ceci est impossible puisque $1 < k < p$.

De plus, les restes des divisions de a, $2a$, ..., $(p-1)a$ par p sont tous différents. Si on trouvait des restes identiques pour ka et $k'a$ ($k > k'$) alors le reste de $(k-k')a$ par p serait nul, ce qui est impossible d'après ce qui précède. Donc, à l'ordre près des facteurs les restes de a, $2a$, ..., $(p-1)a$ par p sont $1, 2, \ldots, p-1$.

Par conséquent la division du produit $a \times 2a \times \cdots \times (p-1)a$ par p a pour reste le produit $1 \times 2 \times \cdots \times (p-1)$ et donc $a \times 2a \times \cdots \times (p-1)a$ qui s'écrit encore

$$a^{p-1} \times 2 \times \cdots (p-1) \equiv 2 \times 3 \times \cdots \times (p-1) \pmod{p}.$$

Il existe donc un entier relatif k tel que

$$(a^{p-1}-1)(1 \times 2 \times 3 \times \cdots \times (p-1)) = kp.$$

Comme p est premier avec $1 \times 2 \times \cdots \times (p-1)$ d'après le théorème de Gauss, p divise $a^{p-1}-1$. a^{p-1} est donc congru à 1 modulo p. □

Corollaire 4.2. Soit p un nombre premier et a un entier quelconque alors $a^p \equiv a \pmod{p}$.

Démonstration du corollaire 4.2. $\Diamond$ D'après ce qui précède, si a et p sont premiers entre eux, $a^{p-1}-1$ est congru à 0 modulo p. Sinon, p étant premier, a est congru à 0 modulo p. On a donc soit $a^{p-1} \equiv 1 \pmod{p}$ soit $a^P \equiv a \equiv 0 \pmod{p}$ et par conséquent dans les deux cas $a^p \equiv a \pmod{p}$. □

4.4 Le cryptage RSA

Le cryptage RSA (du nom des inventeurs, Ronald Rivest, Adi Shamir et Leonard Adleman) est intéressant car la clé de cryptage est publique et il n'a donc pas de risques liés à l'envoi de la clé et au procédé de codage des données. Bob, comme tout le monde, peut crypter et envoyer un message. Par contre, seul la destinataire, Alice, qui connaît la clé privée correspondante pourra reconstituer le message initial.

Alice, la destinataire rend publique deux nombres n et c où n est le produit de deux grands nombres premiers p et q qu'elle est seule à connaître, où c est un entier premier avec le produit $(p-1)(q-1)$ compris entre 2 et $(p-1)(q-1)$.

Pour coder le message « Bonjour », par exemple, on commence par remplacer les lettres par leurs positions dans l'ordre alphabétique, ce qui donne

$$02\ 15\ 14\ 10\ 15\ 21\ 18.$$

Si on utilise $n = 10573 = 97 \times 109$, on peut regrouper les chiffres par 4 sans risquer de dépasser n. Ce qui donne 0215 1410 1521 0018. Pour chaque nombre a de la série, on détermine alors b, reste de la division de a^c par n. On obtient alors dans ce cas avec $c = 5$ la série :

$$9131\ 7391\ 0690\ 7574.$$

C'est cette série de nombres qu'envoie Bob à Alice.

Alice qui connaît les deux facteurs premiers de n (ici $p = 97$ et $q = 109$) détermine alors facilement le nombre entier d vérifiant $1 < d < (p-1)(q-1)$ et tel que

$$cd \equiv 1 \pmod{(p-1)(q-1)}.$$

Ici $d = 6221$.

Alice peut alors retrouver la série initiale de nombres car, pour chaque entier b de cette série, on démontre de b^d est congru à a modulo n.

L'intérêt pour Alice est bien sûr d'avoir un nombre n produit de deux nombres premiers très grands de façon à ce que les calculateurs même les plus rapides ne puissent pas trouver en un temps suffisammment court les deux facteurs premiers nécessaires pour calculer d.

On note d'autre part que c et d jouent le même et sont interchangeables. Ainsi Alice peut décider de coder elle-même un message en utiliser sa clé privée $d = 6621$. Bob décryptera alors aisément ce message avec la clé publique c. Le message envoyé à Bob constitue en fait une signature du message d'Alice. En effet, si Bob réussit à décrypter sans problème le message à l'aide de la clé c, c'est que ce message a été codé avec la clé privée d connue d'Alice seule et cela suffit pour en garantir l'authenticité.

On donne quelques propriétés permettant de justifier la robustesse de la méthode RSA.

PROPRIÉTÉ 4.3. Soient p et q deux nombres premiers. Si c, tel que $1 < c < (p-1)(q-1)$, est premier avec le produit $(p-1)(q-1)$ alors il existe un unique d tel que $1 < d < (p-1)(q-1)$ et vérifiant

$$cd \equiv 1 \pmod{(p-1)(q-1).)}$$

Démonstration de la propriété 4.3. $\Diamond$ Si c et $(p-1)(q-1)$ sont premiers entre eux, il existe, d'après le théorème de Bézout, deux entiers relatifs u_0 et v_0 tels que $u_0 c + v_0(p-1)(q-1) = 1$. Par suite (u, v) est solution de

$$uc + v(p-1)(q-1) = 1$$

si et seulement si il existe un entier relatif k tel que

$$u = u_0 - k(p-1)(q-1) \quad \text{et} \quad v = v_0 + kc.$$

Soit donc k tel que u soit le plus petit des entiers positifs. Dans ces conditions

$$uc = 1 - v(p-1)(q-1) \equiv 1 \pmod{(p-1)(q-1)}$$

et le nombre d recherché est par conséquent égal à u.

Il est unique car s'il en existait un autre, d', alors on aurait

$$c(d - d') \equiv 0 \pmod{(p-1)(q-1)}.$$

Comme c est premier avec $(p-1)(q-1)$, alors, d'après le théorème de Gauss,

$$d - d' \equiv 0 \pmod{(p-1)(q-1)}.$$

Mais comme on a $1 < d < (p-1)(q-1)$ et $1 < d' < (p-1)(q-1)$ et bien, on peut avoir que $d = d'$. □

PROPRIÉTÉ 4.4. Dans les conditions précédentes, si p et q sont différents et si $b \equiv a^c \pmod{pq}$ alors $b^d \equiv a \pmod{pq}$.

Démonstration de la propriété 4.4. $\Diamond$ Si $b \equiv a^c \pmod{pq}$ alors $b^d \equiv a^{cd} \pmod{pq}$ et $cd \equiv 1 \pmod{(p-1)(q-1)}$. Il existe donc un entier $k \geq 0$ tel que $cd = 1 + k(p-1)(q-1)$. On obtient donc

$$a^{cd} = a\left((a^{p-1})^{q-1}\right)^k.$$

Si a est divisible par p alors de façon évidente, $a^{cd} \equiv a \equiv 0 \pmod{p}$, sinon, d'après le petit théorème de Fermat, $a^{p-1} \equiv 1 \pmod{p}$ d'où $a^{cd} \equiv a \pmod{p}$. De même $a^{cd} \equiv a \pmod{q}$. Il existe donc deux entiers k et k' tels que $a^{cd} = a + kp$ et $a^{cd} = a + k'q$. Ainsi $kp = k'q$, entier qui se trouve donc être multiple de pq puisque p et q sont des nombres premiers différents. On obtient donc dans ces conditions $a^{cd} \equiv a \pmod{pq}$. □

4.5 Le numéro INSEE

Le numéro INSEE ou numéro de Sécurité Sociale est formé de 15 chiffres déterminés, pour chaque individu de la façon suivante :

- 1 chiffre pour le sexe : Homme (1) et Femme (2)
- 2 chiffres correspondants aux deux derniers chiffres de l'année de naissance
- 2 chiffres correspondant au mois de naissance
- 2 chiffres correspondant au département de naissance
- 3 chiffres correspondant à la commune de naissance
- 3 chiffres correspondant au numéro d'inscription sur le registre des naissances
- 2 chiffres correspondant à une clé de contrôle. La clé de contrôle est ainsi déterminée de la manière suivante : « *On prend le nombre formé par les 13 premiers chiffres, on cherche son reste r dans la division par 97, la clé est alors égale au nombre $97 - r$ écrit avec deux chiffres (le premier étant éventuellement un 0.*

Exemple 4.5.

1. Vérifier la clé de contrôle associée au numéro $2\ 85\ 05\ 33\ 565\ 001\ 89$
2. On change le dixième chiffre « 5 » par le chiffre « 9 ». Montrer qu'alors la clé de contrôle permet de détecter l'erreur.

4.6 Théorème chinois

THÉORÈME 4.6. Soit $(n, m) \in (\mathbb{Z} \setminus \{0, 1\})^2$ tel que $\mathrm{PGCD}(m, n) = 1$. Soit $(a, b) \in \mathbb{Z}^2$. Alors

$$\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases} \qquad (\Sigma)$$

admet au moins une solution dans $\mathbb{Z}$.

Si, de plus, $x_0 \in \mathbb{Z}$ est une solution particulière de Σ, alors l'ensemble des solutions $\mathcal{S}$ est $\{x_0 + knm,\ k \in \mathbb{Z}\}$.

Démonstration. $\Diamond$ Soit $x \in (\Sigma)$. Si $x_0 \in \mathbb{Z}$ tel que :

$$\begin{cases} x_0 \equiv a \pmod{n} \\ x_0 \equiv b \pmod{m} \end{cases}$$

alors

$$\begin{cases} x_0 \equiv x \pmod{n} \\ x_0 \equiv x \pmod{m} \end{cases}$$

Il existe $(k, k') \in \mathbb{Z}^2$ tel que $nk = x_0 - x$ et $mk' = x_0 - x$. D'après le théorème de Gauss, $n \mid k'$ car $\mathrm{PGCD}(n, m) = 1$. Il existe $l \in \mathbb{Z}$ tel que $k' = ln$, donc $x_0 - x = lmn$, c'est-à-dire

$$\mathcal{S} \subset \{x_0 + lmn,\ l \in \mathbb{Z}\}.$$

Soit $x = x_0 + lmn$, où $l \in \mathbb{Z}$. On a $x \equiv x_0 \pmod{n}$ et $x \equiv x_0 \pmod{m}$. Ainsi on obtient l'égalité.

Montrons que $\mathcal{S} \neq \emptyset$.

$$(\Sigma) \Leftrightarrow \begin{cases} xm \equiv am \pmod{mn} \\ xn \equiv bn \pmod{nm} \end{cases}$$

donc $x(m-n) \equiv am - bn \pmod{nm}$. Dans $\mathbb{Z}/n\mathbb{Z}$, on a :

$$\overline{x} \times \overline{m-n} = \overline{am - bn}.$$

Si $\overline{m-n}$ est inversible dans $\mathbb{Z}/mn\mathbb{Z} \setminus \{0\}$, alors on a une solution :

$$\overline{x} = \overline{am - bn}\,\overline{m-n}^{-1}$$

puisqu'il existe $k \in \mathbb{Z}$ tel que $x(m-n) = am - bn + lmn$ donc $m(x-a) = n(-b+km+x)$ donc n divise $x - a$ (car $\mathrm{PGCD}(n,m) = 1$ et $-b + km + x \in \mathbb{Z}$). De façon analogue, $x \equiv b \pmod{m}$.

Montrons que $\overline{m-n}$ est inversible dans $\mathbb{Z}/mn\mathbb{Z}$, c'est-à-dire $\mathrm{PGCD}(m-n, mn) = 1$. Comme $\mathrm{PGCD}(m,n) = 1$, on a $\mathrm{PGCD}(m-n,n) = 1 = \mathrm{PGCD}(m-n,m)$, d'après le théorème de Bezout. En effet, il existe $(u,v) \in \mathbb{Z}^2$ tel que $nu + mv = 1$ donc :

$$(m-n)v + (u+v)n = 1$$

donc $\mathrm{PGCD}(m-n,n) = 1$ car $u + v \in \mathbb{Z}$.

Par suite, $\mathrm{PGCD}(m-n, mn) = 1$ car si $d = \mathrm{PGCD}(m-n, mn)$. Soit d' tel que $d' \mid mn$ et $d' \mid m - n$, d est un diiviseur premier de d. Comme $\mathrm{PGCD}(m,n) = 1$, d' divise m ou n (par ex., $d' \mid n$. Or $d' \mid m - n$, donc $d' \mid m$. Ainsi $d' \mid \mathrm{PGCD}(m,n)$ et $d' = 1$ (ce qui est absurde. Comme d n'a pas de diviseur premier, $d = 1$. □

Exemple 4.7. Résoudre dans $\mathbb{Z}$:

1. $\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 1 \pmod{6} \end{cases}$
2. $\begin{cases} x \equiv 2 \pmod{8} \\ x \equiv 3 \pmod{6} \end{cases}$

Solution. ♢

1. On multiple la première ligne par 6 et la deuxième par 5 :

$$\begin{cases} 6x \equiv 18 \pmod{30} \\ 5x \equiv 5 \pmod{30} \end{cases}$$

donc $6x - 5x = x \equiv 13 \pmod{30}$.

Réciproquement, si $x \equiv 13 \pmod{30}$ alors il existe $k \in \mathbb{Z}$ tel que $x - 13 = 5 \times 6k$ donc $x \equiv 13 \pmod{5}$. Or $13 \equiv 3 \pmod{5}$, donc $x \equiv 3 \pmod{5}$. De plus,

$$x \equiv 13 \equiv 1 \pmod{6}.$$

Ainsi, l'ensemble des solutions est : $\{x \in \mathbb{Z},\ x \equiv 13 \pmod{5}\}$.

2. On arriverait à $x \equiv 6 \pmod{24}$. Réciproquement, il existe $k \in \mathbb{Z}$ tel que $x - 6 = 24k = 8 \times 3k$, donc $x \equiv 6 \pmod{8}$ mais $6 \not\equiv 2 \pmod{8}$ ou $x \equiv 6 \equiv 0 \pmod{6}$ mais $3 \not\equiv 0 \pmod{6}$. Il n'y a donc pas de solution.

□

4.7 Applications de la vie de tous les jours

Problème 4.8. Un jardinier doit planter une haie autour d'une passerelle rectangulaire de longueur $10{,}2$ m et de largeur $7{,}8$ m. Il doit mettre un plant à chaque sommet d'un rectangle et espacer les plants régulièrement d'un nombre entier de centimètres.

Combien de plants au minimum peut-il planter ?

Solution du problème 4.8. $\Diamond$ On calcule $\mathrm{PGCD}(102, 78)$ par l'algorithme d'Euclide :

$$\begin{aligned} 102 &= 78 \times 1 + 24 \\ 78 &= 24 \times 3 + 6 \\ 24 &= 6 \times 4 + 0 \end{aligned}$$

On a de plus :

$$102 = 6 \times 17 \quad \text{et} \quad 78 = 6 \times 13.$$

Les plants devront être plantés à 6 cm d'espacement chacun. Sur une longueur, on peut planter 17 plants et sur la largeur, 13 plants. Donc, on peut planter $(13 + 17) \times 2 = 60$ plants. □

Problème 4.9. Une fleuriste dispose de 244 lys, 366 roses et 183 œillets roses. En utilisant le tout, quel nombre maximal de bouquets identiques peut-elle composer ?

Préciser la composition d'un bouquet.

Solution du problème 4.9. $\Diamond$ On a :

$$\mathrm{PGCD}(244, 366, 183) = \mathrm{PGCD}(\mathrm{PGCD}(244, 366), 183) = \mathrm{PGCD}(122, 183) = 61.$$

On peut donc composer au maximum 61 bouquets. La composition du bouquet est :

— 4 lys ;
— 6 roses ;
— 3 oeillets roses.

□

4.8 Équation de droite

L'ensemble des points $M(x, y)$ vérifiant l'équation $ax + by = c$ forme une droite. Les couples d'entiers relatifs vérifiant cette équation correspond aux points M de la droite dont les coordonnées sont entières. La résolution de l'équation dans l'ensemble des entiers relatifs permet de donner les coordonnées de ces points. Selon la valeur de c, la droite D peut ne jamais passer par des points de coordonnées entières ou bien posséder une infinité de points de coordonnées régulièrement répartis.

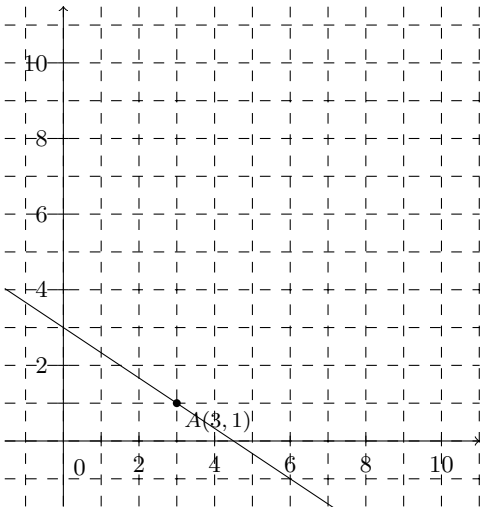

FIGURE 1 – Résolution graphique de l'équation $9x + 6y = 27$. Existence de solutions car la droite a un point à coordonnées entières.

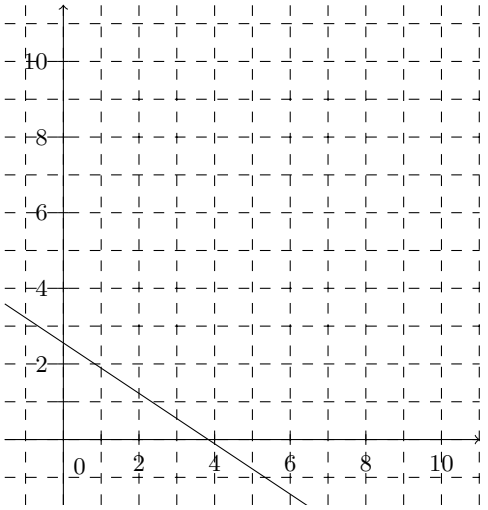

FIGURE 2 – Résolution graphique de l'équation $9x + 6y = 23$. Non-existence de solutions car la droite n'a aucun point à coordonnées entières.