Arithmétique dans $\mathbb{Z}$

I – Divisibilité dans $\mathbb{Z}$

1) Diviseurs, multiples

Définition 1 (diviseur, multiple) Soient $a, b \in \mathbb{Z}$.

- ⋆ On dit que a est un *diviseur* de b (ou que b est un *multiple* de a), noté $a \mid b$, s'il existe $k \in \mathbb{Z}$ tel que $b = ak$
- ⋆ On note $\mathscr{D}(a)$ l'ensemble des diviseurs de a, c'est-à-dire :

$$\mathscr{D}(a) = \left\{k \in \mathbb{Z} \,\middle|\, k \mid a\right\}$$

Exemple 1 ⋆ L'entier 3 divise 9 mais 3 ne divise pas 5 (car $\frac{5}{3} \notin \mathbb{Z}$).

- ⋆ Les entiers 1 et -1 divisent tous les entiers.
- ⋆ L'entier 0 est un multiple de tous les entiers (*i.e.* $\mathscr{D}(0) = \mathbb{Z}$), mais il ne divise que lui-même.
- ⋆ L'ensemble des diviseurs de 6 est $\mathscr{D}(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$.
- ⋆ On a l'égalité $\mathscr{D}(a) = \mathscr{D}(|a|)$.

Remarques :

- ⋆ Soit $a \in \mathbb{Z}$. L'ensemble des multiples de a est $a\mathbb{Z} = \left\{ak \,\middle|\, k \in \mathbb{Z}\right\}$.
- ⋆ La relation « divise » est réflexive et transitive mais elle n'est pas antisymétrique. En effet, $2 \mid -2$ et $-2 \mid 2$ (pourtant $2 \neq -2$).
- ⋆ La divisibilité sur $\mathbb{N}^*$ est liée à l'ordre naturel sur $\mathbb{N}^*$ par la relation :

$$a \mid b \Longrightarrow a \leqslant b$$

  En effet, si $a \mid b$, alors il existe $k \in \mathbb{Z}$ tel que $b = ka$ et, puisque a et b sont strictement positifs, on a $k \in \mathbb{N}^*$ et donc $b \geqslant a$.

Proposition 1 (caractérisation des couples d'entiers associés) Soient $a, b \in \mathbb{Z}$. Alors :

$$a \mid b \text{ et } b \mid a \iff |a| = |b|$$

Démonstration Soient $a, b \in \mathbb{Z}$.

- ⋆ Supposons que $a \mid b$ et $b \mid a$. Il existe alors des entiers relatifs k et ℓ tels que $a = kb$ et $b = \ell a$ et donc $a = k\ell a$.
  - — Si $a = 0$, alors $b = 0$.
  - — Sinon, $k\ell = 1$ et donc $|k| = |\ell| = 1$ (puisque k et ℓ sont des entiers) et $|a| = |b|$.
- ⋆ Si $|a| = |b|$, alors $a = b$ ou $a = -b$ donc $a \mid b$ et $b \mid a$. ■

Remarque : la relation « divise » est donc une relation d'ordre dans $\mathbb{N}$.

Proposition 2 Soient $a, b \in \mathbb{Z}$.

- ⋆ Soient $u, v, d \in \mathbb{Z}$. Alors :
$$d \mid a \text{ et } d \mid b \Longrightarrow d \mid (au + bv)$$
- ⋆ Soit $x \in \mathbb{Z}^*$. Alors :
$$a \mid b \iff ax \mid bx$$

Démonstration Soient $a, b \in \mathbb{Z}$.

- ⋆ Soient $u, v, d \in \mathbb{Z}$. Si $d \mid a$ et $d \mid b$, alors il existe $k, \ell \in \mathbb{Z}$ tels que $a = kd$ et $b = \ell d$. Par conséquent :
$$au + bv = kdu + \ell dv = (ku + \ell v)d$$
Comme $ku + \ell v$ est un entier, on peut conclure que d divise $au + bv$.
- ⋆ Soit $x \in \mathbb{Z}^*$. Alors :
$$a \mid d \iff \exists\, k \in \mathbb{Z},\ d = ka \iff \exists\, k \in \mathbb{Z},\ dx = k(ax) \qquad (\text{car } x \neq 0)$$
$$\iff ax \mid dx$$
■

✎✎✎ **Exercice 1** Déterminer les entiers naturels n tels que $n + 1$ divise $n + 8$.

Solution. On raisonne par analyse-synthèse.

- ⋆ Supposons que $n \in \mathbb{N}$ soit tel que $n + 1 \mid n + 8$. On a aussi $n + 1 \mid n + 1$ donc $n + 1$ divise $n + 8 - (n + 1) = 7$. Par conséquent, $n + 1 \in \{1, 7\}$ d'où l'on tire que $n = 0$ ou $n = 6$.
- ⋆ Réciproquement, les entiers 0 et 6 sont solutions.

Les entiers cherchés sont donc 0 et 6.

2) Division euclidienne

Théorème 1 (de la division euclidienne) Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. Il existe un unique couple d'entiers relatifs (q, r) tel que :
$$a = bq + r \qquad \text{avec} \qquad 0 \leqslant r < b \tag{1}$$
On dit qu'on a effectué la division euclidienne de a par b. Dans cette division, le quotient est q, le reste est r.

Démonstration Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. On raisonne par analyse synthèse.

- ⋆ **Analyse :** supposons qu'il existe $q, r \in \mathbb{Z}$ tels que $a = bq + r$ et $0 \leqslant r < b$. Alors $0 \leqslant a - bq < b$, c'est-à-dire $\frac{a}{b} - 1 < q \leqslant \frac{a}{b}$. On a donc $q = \left\lfloor \frac{a}{b} \right\rfloor$. Le couple (q, r) est donc uniquement déterminé.
- ⋆ **Synthèse :** posons $q = \left\lfloor \frac{a}{b} \right\rfloor$ et $r = a - bq$. On a alors bien $a = bq + r$ et $\frac{a}{b} - 1 < q \leqslant \frac{a}{b}$ donc $0 \leqslant r < b$. ■

Remarque : avec ces notations, on a $a \equiv r\ [b]$.

Exemple 2 La division euclidienne de 151 par 7 est $151 = 21 \times 7 + 4$ (le quotient vaut 21, le reste vaut 4).

Corollaire 1 (sous-groupes de $\mathbb{Z}$) Soit G un sous-groupe de $(\mathbb{Z}, +)$. Alors il existe un unique entier naturel n tel que $G = n\mathbb{Z}$.

Démonstration On commence par démontrer l'existence d'un tel entier. Considérons l'ensemble $E = G \cap \mathbb{N}^*$.

- ⋆ **Premier cas :** si $E = \varnothing$, alors $G \cap \mathbb{Z}^* = \varnothing$ (car G est un groupe), et comme $0 \in G$, on a $G = \{0\} = 0\mathbb{Z}$.
- ⋆ **Deuxième cas :** sinon, E est une partie de $\mathbb{N}$ non vide et minorée par 0 donc elle admet un plus petit élément que l'on note n_0. En particulier, $n_0 \in G$. Montrons alors que $G = n_0\mathbb{Z}$.
  - — Soit $g \in n_0\mathbb{Z}$. Il existe alors $k \in \mathbb{Z}$ tel que $g = n_0 k$. Alors $g \in G$ (puisque $n_0 \in G$ et car G est un groupe).
  - — Soit $g \in G$. D'après le théorème de la division euclidienne, il existe des entiers relatifs q et r tels que :

$$g = n_0 q + r \qquad \text{avec} \qquad 0 \leqslant r < n_0$$

Comme g et n_0 appartiennent à G, on a $r \in G$ (puisque G est un groupe). Par ailleurs, $0 \leqslant r < n_0$ donc $r \notin E$. On en déduit que $r = 0$ et donc $g \in n_0\mathbb{Z}$.

Finalement, on a bien l'égalité $G = n_0\mathbb{Z}$.

Démontrons maintenant l'unicité. Supposons qu'il existe deux entiers naturels m et n tels que $m\mathbb{Z} = n\mathbb{Z}$. Alors $m \mid n$ et $n \mid m$. Donc $|m| = |n|$, c'est-à-dire $m = n$ puisque m et n sont positifs. ■

II – Plus grand commun diviseur (PGCD), plus petit commun multiple (PPCM)

1) Définitions

Soient $a, b \in \mathbb{Z}$. Si $(a, b) \neq (0, 0)$, alors $\mathscr{D}(a) \cap \mathscr{D}(b)$ (ensemble des diviseurs communs à a et à b) est une partie de $\mathbb{N}$ non vide (elle contient 1) et qui est majorée (par $\max(|a|, |b|)$). Elle possède donc un plus grand élément (qui est supérieur ou égal à 1). Ceci nous permet de définir le PGCD de a et b.

Définition 2 (PGCD) Soit $a, b \in \mathbb{Z}$.

- ⋆ Si $a \neq 0$ ou $b \neq 0$, on appelle PGCD de a et b, noté $a \wedge b$, le plus grand élément (pour la relation $\leqslant$) de l'ensemble des diviseurs communs et à b, c'est-à-dire :

$$a \wedge b = \max(\mathscr{D}(a) \cap \mathscr{D}(b)) = \max\left\{d \in \mathbb{N}^* \,\middle|\, d \mid a \text{ et } d \mid b\right\}$$

- ⋆ Si $a = b = 0$, on pose $a \wedge b = 0$.

Remarques :

- ⋆ Le PGCD de deux entiers naturels est donc un entier positif.
- ⋆ Pour tous $a, b \in \mathbb{Z}$, on a $a \wedge b = |a| \wedge |b|$.*Dans la suite, on pourra donc travailler avec des entiers naturels.*
- ⋆ Par définition du PGCD :

$$\forall a \in \mathbb{Z}, \qquad a \wedge 0 = |a|$$

Exemple 3 $2 \wedge 3 = 1$, $-2 \wedge 4 = -2$ et $6 \wedge 8 = 2$

2) Algorithme d'Euclide

Nous allons présenter un algorithme qui permet de calculer facilement le PGCD de deux entiers.

Lemme 1 Soit $u = (u_n)_{n\in\mathbb{N}}$ une suite décroissante d'entiers naturels. Alors u est stationnaire, *i.e.* :

$$\exists\, N \in \mathbb{N},\ \forall n \geqslant N,\ u_n = u_N$$

Démonstration L'ensemble $\mathscr{E} = \{u_n \mid n \in \mathbb{N}\}$ est une partie de $\mathbb{N}$, non vide (elle contient u_0) et minorée par 0. Donc $\mathscr{E}$ possède un minimum m. On a donc :

- ⋆ $\forall n \in \mathbb{N},\ u_n \geqslant m$;
- ⋆ il existe $N \in \mathbb{N}$ tel que $m = u_N$ (puisque $m \in \mathscr{E}$).

La suite u est décroissante donc pour tout $n \geqslant N$, on a $u_n \leqslant u_N$. Le premier point ci-dessus nous donne l'inégalité dans l'autre sens donc, pour tout $n \geqslant N$, on a $u_n = u_N$, ce qu'il fallait démontrer. ■

Fixons $(a, b) \in \mathbb{N} \times \mathbb{N}^*$. On sait qu'il existe $q, r \in \mathbb{N}$ tels que $a = bq + r$ et $0 \leqslant q < b$.

Proposition 3 (algorithme d'Euclide) Alors :

$$\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(b) \cap \mathscr{D}(r)$$

Par conséquent, $a \wedge b = b \wedge r$.

Démonstration On raisonne par double inclusion.

- ⋆ Montrons que $\mathscr{D}(a) \cap \mathscr{D}(b) \subset \mathscr{D}(b) \cap \mathscr{D}(r)$. Soit $d \in \mathscr{D}(a) \cap \mathscr{D}(b)$. Alors $d \mid bq$ et $d \mid a$ donc $d \mid (a - bq)$, c'est-à-dire $d \mid r$. Par suite, $d \in \mathscr{D}(b) \cap \mathscr{D}(r)$.
- ⋆ L'inclusion réciproque s'obtient de manière analogue.

On a donc l'égalité :

$$\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(b) \cap \mathscr{D}(r)$$

Les plus grands éléments de $\mathscr{D}(a) \cap \mathscr{D}(b)$ et $\mathscr{D}(b) \cap \mathscr{D}(r)$ sont égaux donc $a \wedge b = b \wedge r$. ■

Explicitons maintenant l'algorithme d'Euclide « étendu » qui va nous permettre de déterminer, en pratique, le PGCD de deux entiers. Avec les mêmes notations, posons :

- ⋆ $r_0 = a$
- ⋆ $r_1 = b$
- ⋆ On effectue la division euclidienne de r_0 par r_1. Le reste r est noté r_2.
- ⋆ Pour $n \in \mathbb{N}$, si $r_{n+1} \neq 0$, alors on fait la division euclidienne de r_n par r_{n+1} et on note r_{n+2} le reste. Si $r_{n+1} = 0$, alors on pose $r_{n+2} = 0$.

Proposition 4 Avec les mêmes notations :

- ⋆ il existe $N \in \mathbb{N}^*$ tel que $r_N = 0$;
- ⋆ $a \wedge b = r_{N-1}$ (autrement dit, le PGCD de a et b est le dernier reste non nul dans l'algorithme d'Euclide étendu) et $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(a \wedge b)$.

Démonstration

- ⋆ Par construction, la suite $(r_n)_{n \geqslant 1}$ est décroissante. C'est une suite d'entiers naturels donc elle est stationnaire d'après le lemme ; il existe donc $N \in \mathbb{N}^*$ tel que pour tout $n \geqslant N$, on ait $r_n = r_N$. Supposons que $r_N \neq 0$. Alors $r_N = 1 \times r_{N+1} + 0$ donc $r_{N+2} = 0$ (par unicité du reste). Ceci est absurde car $r_{N+2} = r_N \neq 0$. Ceci prouve le premier point.
- ⋆ D'après la proposition précédente, on a :

$$a \wedge b = r_0 \wedge r_1 = r_1 \wedge r_2 = \cdots = r_{N-1} \wedge \underbrace{r_N}_{=0} = r_{N-1}$$

De plus (toujours d'après la proposition précédente) :

$$\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(r_0) \cap \mathscr{D}(r_1) = \mathscr{D}(r_1) \cap \mathscr{D}(r_2) = \cdots = \mathscr{D}_{r_{N-1}} \cap \underbrace{\mathscr{D}(r_N)}_{=\mathbb{Z}} = \mathscr{D}(a \wedge b),$$

ce qui termine la démonstration. ■

Remarque : l'égalité $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(a \wedge b)$ nous dit que

- ⋆ tout diviseur commun à a et à b divise $a \wedge b$
- ⋆ le PGCD de a et b est aussi le plus grand élément, au sens de la divisibilité, de l'ensemble des diviseurs positifs communs à a et à b.

Exemple 4 Déterminons le PGCD de 137 et 12. On a successivement :

- ⋆ $137 = 12 \times 11 + 5$;
- ⋆ $12 = 5 \times 2 + 2$;
- ⋆ $5 = 2 \times 2 + 1$;
- ⋆ $2 = 1 \times 2 + 0$.

Donc $137 \wedge 12 = 1$ (on dit que 137 et 12 sont premiers entre eux).

Proposition 5 ($(ka) \wedge (kb)$) Soient $a, b \in \mathbb{Z}$ et $k \in \mathbb{N}^*$. Alors :

$$(ka) \wedge (kb) = k(a \wedge b)$$

Démonstration

⋆ On commence par traiter le cas où $a, b \in \mathbb{N}$. Posons $d = a \wedge b$ et $\delta = (ka) \wedge (kb)$. On veut montrer que $\delta = kd$.

- Par définition, d divise a et b donc kd divise ka et kb. On en déduit que kd divise $(ka) \wedge (kb)$, c'est-à-dire $kd \mid \delta$.
- Comme k divise ka et kb, l'entier k divise $(ka) \wedge (kb) = \delta$. Donc il existe $\ell \in \mathbb{N}$ tel que $\delta = k\ell$. Comme $k\ell$ divise ka et kb, l'entier ℓ divise a et b donc ℓ divise $a \wedge b = d$. Ainsi, $\delta = k\ell$ divise kd.

Ainsi, $|kd| = |\delta|$, c'est-à-dire $kd = \delta$ puisque les deux entiers sont positifs.

⋆ Si $a, b \in \mathbb{Z}$, alors :

$$\begin{aligned}(ka) \wedge (kb) = |ka| \wedge |kb| = (k|a|) \wedge (k|b|) &= k(|a| \wedge |b|) \qquad \text{(d'après le premier point)} \\ &= k(a \wedge b)\end{aligned}$$

■

3) Relation de Bézout

Proposition 6 (relation et coefficients de Bézout) Soient $a, b \in \mathbb{Z}$. Alors :

$$\exists\, u, v \in \mathbb{Z}, \qquad au + bv = a \wedge b$$

Un tel couple (u, v) est appelé un *couple de coefficients de Bézout* de a et b.

Démonstration On se place d'abord dans le cas où $a, b \in \mathbb{N}$. Démontrons par récurrence (forte) sur $b \in \mathbb{N}$ la propriété $\mathscr{P}_b$: « pour tout entier $a \in \mathbb{N}$, il existe $u, v \in \mathbb{Z}$ tel que $au + bv = a \wedge b$ ».

⋆ Pour tout $a \in \mathbb{N}$, on a :

$$a \times 1 + 0 \times 0 = 0 = a \wedge 0$$

donc la proposition $\mathscr{P}_0$ est vraie.

⋆ Soit $b \in \mathbb{N}$ tel que les propositions $\mathscr{P}_0, \ldots, \mathscr{P}_b$ soient vraies. Montrons que $\mathscr{P}_{b+1}$ est vraie. Soit $a \in \mathbb{N}$ et posons $d = a \wedge (b+1)$. On effectue la division euclidienne de a par $b + 1 \in \mathbb{N}^*$. Il existe $q, r \in \mathbb{Z}$ tels que :

$$a = (b+1)q + r \qquad \text{avec} \qquad 0 \leqslant r \leqslant b$$

On sait que $d = a \wedge (b+1) = (b+1) \wedge r$ (algorithme d'Euclide). La proposition $\mathscr{P}_r$ est vraie donc il existe $u', v' \in \mathbb{Z}$ tels que :

$$(b+1)u' + rv' = d$$

On a donc :

$$(b+1)u' + (a - (b+1)q)v' = d$$

et donc, en posant $u = v' \in \mathbb{Z}$ et $v = u' - qv' \in \mathbb{Z}$, on a l'égalité $au + (b+1)v = d$. La proposition $\mathscr{P}_{b+1}$ est donc vraie.

Si maintenant $a, b \in \mathbb{Z}$, alors, d'après ce qui précède, il existe $u, v \in \mathbb{Z}$ tel que :

$$a \wedge b = |a| \wedge |b| = |a|u + |b|v$$

Si $|a| = -a$, *i.e.* si $a < 0$, alors $|a|u = a(-u)$. ■

Remarque : on utilise l'algorithme d'Euclide étendu pour déterminer un couple de coefficients de Bézout.

Exemple 5 Déterminons un couple de coefficients de Bézout de 33 et 21. D'après l'algorithme d'Euclide, on a :

- ⋆ $33 = 21 \times 1 + 12$;
- ⋆ $21 = 12 \times 1 + 9$;
- ⋆ $12 = 9 \times 1 + 3$;
- ⋆ $9 = 3 \times 3 + 0$

En « remontant » ces égalités, on obtient :

$$\begin{aligned} 33 \wedge 21 = 3 = 12 - 9 \times 1 = (33 - 21) - (21 - 12) &= (33 - 21) - (21 - (33 - 21)) \\ &= 33 \times 2 + (-3) \times 21 \end{aligned}$$

Un couple de coefficients de Bézout est donc $(2, -3)$.

III – Entiers premiers entre eux

1) Définition

Définition 3 Soient $a, b \in \mathbb{Z}$. On dit que a et b sont *premiers entre eux* si $a \wedge b = 1$.

Remarque : les entiers a et b sont donc premiers entre eux si leurs seuls diviseurs communs sont -1 et 1.

Exemple 6
- ⋆ Les entiers 3 et 7 sont premiers entre eux.
- ⋆ Soit $n \in \mathbb{Z}$. Les entiers n et $n+1$ sont premiers entre eux. En effet, en posant $d = n \wedge (n+1)$, on a d divise n et d divise $n+1$ donc d divise $(n+1) - n = 1$. Ainsi, $d = 1$ car $d \geqslant 0$.

2) Théorème de Bézout

Le théorème suivant donne un critère de primalité pour deux entiers.

Théorème 2 (de Bézout) Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. Alors a et b sont premiers entre eux si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

Démonstration On raisonne par double implication.

- ⋆ Supposons qu'il existe deux entiers u et v tels que $au + bv = 1$. Posons $d = a \wedge b$. Alors $d \mid a$ et $d \mid b$ donc $d \mid (au + bv)$, c'est-à-dire $d \mid 1$. Comme $d \in \mathbb{N}^*$, on a nécessairement $d = 1$, ce qui prouve que les entiers a et b sont premiers entre eux.
- ⋆ La réciproque est une application directe de la relation de Bézout. ■

Remarque : pour tout entier relatif n, on a :

$$(n+1) \times 1 + n \times (-1) = 1$$

donc on retrouve le fait que n et $n+1$ sont premiers entre eux.

Proposition 7 Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$. Alors les entiers $\dfrac{a}{a \wedge b}$ et $\dfrac{b}{a \wedge b}$ sont premiers entre eux.

Démonstration Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$. Comme $b \neq 0$, on a $a \wedge b \in \mathbb{N}^*$ donc les entiers $\alpha = \dfrac{a}{a \wedge b}$ et $\beta = \dfrac{b}{a \wedge b}$ sont bien définis. De plus, d'après la relation de Bézout, il existe $u, v \in \mathbb{Z}$ tels que :

$$a \wedge b = au + bv = a \wedge b(\alpha u + \beta v) \qquad \text{c'est-à-dire tel que} \qquad \alpha u + \beta v = 1$$

en simplifiant par $a \wedge b \neq 0$. Les entiers α et β sont donc premiers entre eux d'après le théorème de Bézout. ■

Corollaire 2 (existence de la forme irréductible pour un rationnel) Tout nombre rationnel s'écrit sous forme *irréductible*, c'est-à-dire sous la forme $\dfrac{a}{b}$ où a et b sont des entiers relatifs premiers entre eux, le nombre b étant non nul.

Démonstration Soit $r \in \mathbb{Q}$. Il existe $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$ tel que $r = \dfrac{a}{b}$, ce que l'on peut réécrire $r = \dfrac{\frac{a}{a \wedge b}}{\frac{b}{a \wedge b}}$. On sait que les entiers $\dfrac{a}{a \wedge b}$ et $\dfrac{b}{a \wedge b}$ sont premiers entre eux. ■

Corollaire 3 Soient $a, b, n \in \mathbb{Z}$. Si $a \wedge n = b \wedge n = 1$, alors $(ab) \wedge n = 1$.

Démonstration Supposons que $a \wedge n = b \wedge n = 1$. D'après le théorème de Bézout, il existe $u, v, w, x \in \mathbb{Z}$ tels que :

$$au + nv = 1 \qquad \text{et} \qquad bw + nx = 1$$

En multipliant membre à membre, on obtient :

$$1 = (au + nv)(bw + nx) = abuw + n(aux + bvw + nvx)$$

Comme $uw, aux + bvw + nvx \in \mathbb{Z}$, le théorème de Bézout nous dit que ab et n sont premiers entre eux. ■

Remarque : par récurrence, on peut montrer que

$$\forall p \in \mathbb{N} \setminus \{0,1\},\ \forall a_1, \ldots, a_p, n \in \mathbb{Z},\ \begin{cases} a_1 \wedge n = 1 \\ a_2 \wedge n = 1 \\ \quad \vdots \\ a_p \wedge n = 1 \end{cases} \implies (a_1 a_2 \ldots a_p) \wedge n = 1$$

3) Lemme de Gauss

Théorème 3 (lemme de Gauss) Soient $a, b, c \in \mathbb{Z}$. Alors :

$$(a \wedge b = 1 \quad \text{et} \quad a \mid bc) \implies a \mid c$$

Démonstration Supposons que $a \wedge b = 1$ et $a \mid bc$. D'après le théorème de Bézout, il existe des entiers relatifs u et v tels que $au + bv = 1$, ce qui implique $acu + bcv = c$. Comme a divise bc, la relation précédente entraîne que a divise c. ■

Corollaire 4 Tout nombre rationnel s'écrit de manière unique sous la forme $\frac{a}{b}$ où $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$ et $a \wedge b = 1$.

Démonstration L'existence a déjà été établie. Montrons maintenant l'unicité. Soient $(a_1,b_1),(a_2,b_2) \in \mathbb{Z} \times \mathbb{N}^*$ tels que $a_1 \wedge b_1 = a_2 \wedge b_2 = 1$ et $\frac{a_1}{b_1} = \frac{a_2}{b_2}$. Alors $a_1 b_2 = a_2 b_1$. Donc b_2 divise $a_2 b_1$. Or $a_2 \wedge b_2 = 1$ donc, d'après le lemme de Gauss, on a $b_2 \mid b_1$. En faisant le même raisonnement avec b_1, on a aussi $b_1 \mid b_2$. Comme b_1 et b_2, on obtient $b_1 = b_2$. Par suite, $a_1 = a_2$ d'où l'unicité. ■

Corollaire 5 Soient $a, b, n \in \mathbb{Z}$. On suppose que $a \mid n$, $b \mid n$ et que $a \wedge b = 1$. Alors $ab \mid n$.

Démonstration Comme a divise n, il existe $k \in \mathbb{Z}$ tel que $n = ak$. Or b divise $n = ak$ et $a \wedge b = 1$ donc (lemme de Gauss) $b \mid k$. Ainsi, $ab \mid ak$ *i.e.* $ab \mid n$. ■

Exemple 7 Si $n \in \mathbb{Z}$ est tel que $3 \mid n$ et $5 \mid n$, alors $15 \mid n$.

Application du lemme de Gauss : résolution d'équations diophantiennes

Soient $a, b, c \in \mathbb{Z}$ avec a et b non nuls. On considère l'équation (dite diophantienne) suivante :

$$ax + by = c \tag{E}$$

dont on cherche les solutions $(x,y) \in \mathbb{Z}^2$.

Voir la fiche méthode

✎✎✎ **Exercice 2** Résoudre l'équation diophantienne $131x + 28y = 2$.

Solution. On note $\mathscr{S}$ l'ensemble des solutions de l'équation diophantienne proposée.

- ⋆ Commençons par déterminer une solution particulière de celle-ci en utilisant l'algorithme d'Euclide étendu. On a :

  $$131 = 4 \times 28 + 19 \qquad \text{puis} \qquad 28 = 19 + 9 \qquad \text{et} \qquad 19 = 9 \times 2 + 1$$

  Ainsi, 131 et 28 sont premiers entre eux et :

  $$\begin{aligned} 1 = 19 - 2 \times 9 = 19 - 2 \times (28 - 19) = 3 \times 19 - 2 \times 28 = 3 \times (131 - 4 \times 28) - 2 \times 28 \\ = 3 \times 131 - 14 \times 28 \end{aligned}$$

  En multipliant par 2, on a donc $6 \times 131 + (-28) \times 28 = 2$. Ainsi, le couple $(x_0, y_0) = (6, -28)$ est solution de l'équation.
- ⋆ Soit $(x,y) \in \mathscr{S}$. On a :

  $$131x + 28y = 2 \qquad \text{et} \qquad 131x_0 + 28y_0 = 2$$

  En soustrayant la deuxième équation à la première, il vient :

  $$131(x - x_0) + 28(y - y_0) = 0 \qquad \text{soit encore} \qquad 131(x - x_0) = 28(y_0 - y) \tag{$*$}$$

  donc 131 divise $28(y_0 - y)$. Or $131 \wedge 28 = 1$ donc (d'après le lemme de Gauss) 131 divise $y_0 - y$. Il existe donc $k \in \mathbb{Z}$ tel que $y_0 - y = 131k$, c'est-à-dire tel que $y = y_0 - 131k$. En remplaçant dans $(*)$, on obtient :

  $$131(x - x_0) = 28 \times 131k \qquad \text{c'est-à-dire} \qquad x - x_0 = 28k,$$

  soit encore $x = x_0 + 28k$. Ceci démontre l'inclusion :

  $$\mathscr{S} \subset \left\{(6 + 28k, -28 - 131k) \,\middle|\, k \in \mathbb{Z}\right\}$$
- ⋆ Par ailleurs, pour tout $k \in \mathbb{Z}$, on a :

  $$131(6 + 28k) + 28(-28 - 131k) = 131 \times 6 - 28^2 = 2$$

  donc $(6 + 28k, -28 - 131k) \in \mathscr{S}$. Ainsi :

  $$\left\{(6 + 28k, -28 - 131k) \,\middle|\, k \in \mathbb{Z}\right\} \subset \mathscr{S}$$

On peut donc conclure que l'ensemble des solutions de l'équation diophantienne proposée est :

$$\boxed{\mathscr{S} = \left\{(6 + 28k, -28 - 131k) \,\middle|\, k \in \mathbb{Z}\right\}}$$

4) Plus petit multiple commun (PPCM)

Soient $a, b \in \mathbb{Z}$ tels que $ab \neq 0$ (*i.e.* $a \neq 0$ et $b \neq 0$), alors l'ensemble des multiples strictement positifs communs à a et à b, *i.e.* $a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*$, est une partie de $\mathbb{N}$ non vide (car elle contient $|ab|$). Elle possède donc un plus petit élément.

Définition 4 (PPCM) Soit $(a, b) \in \mathbb{Z}^2$.

- ⋆ Si $ab \neq 0$, on appelle PPCM de a et b, noté $a \vee b$, le plus petit élément (pour la relation $\leqslant$) de l'ensemble des multiples (positifs) de a et b, c'est-à-dire :

$$a \vee b = \min(a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*)$$

- ⋆ Si $ab = 0$, alors on pose $a \vee b = 0$.

Remarques :

- ⋆ Le PPCM est donc un entier positif.
- ⋆ Pour tous $a, b \in \mathbb{Z}$, on a $a \vee b = |a| \vee |b|$.

Proposition 8 Soient $a, b \in \mathbb{Z}$ tels que $a \wedge b = 1$. Alors $a \vee b = |ab|$.

Démonstration Soient $a, b \in \mathbb{Z}$ tels que $a \wedge b = 1$.

- ⋆ On sait que $a \vee b$ est le plus petit multiple commun positif à a et à b et que $|ab|$ en est un. On a donc $a \vee b \leqslant |ab|$.
- ⋆ Par ailleurs $a \mid a \vee b$ et $b \mid a \vee b$. Comme $a \wedge b = 1$, on a aussi $ab \mid a \vee b$. Ceci implique que $|ab| \leqslant a \vee b$.

On a donc bien l'égalité annoncée. ■

Proposition 9 (relation entre PGCD et PPCM) Pour tous $a, b \in \mathbb{Z}$, on a :

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

Démonstration L'égalité est claire si a ou b est nul (dans ce cas $ab = 0$ et $a \vee b = 0$). Supposons que $a, b \in \mathbb{N}^*$. Les entiers $\alpha = \dfrac{a}{a \wedge b}$ et $\beta = \dfrac{b}{a \wedge b}$ sont bien définis et sont premiers entre eux et on a, en posant $d = a \wedge b$,, les égalités $a = \alpha d$ et $b = \beta d$. Posons encore $m = a \vee b$. On veut montrer que $m = d\alpha\beta$.

- ⋆ On a $d \mid a$ et $a \mid m$ donc, par transitivité de la relation $|$, on a $d \mid m$. Il existe donc $x \in \mathbb{N}$ tel que $m = dx$. Comme $a = \alpha d \mid dx$, on a aussi $\alpha \mid x$. De même, β divise x. Or α et β sont premiers entre eux donc $\alpha\beta$ divise x. Ainsi, $d\alpha\beta$ divise m. En particulier, $d\alpha\beta \leqslant m$.
- ⋆ Réciproquement, $d\alpha\beta = a\beta = b\alpha$ est un multiple de a et de b. Par définition du PPCM, on a $m \leqslant d|\alpha\beta|$.

On a donc démontré l'égalité $a \vee b = d\alpha\beta$. Ainsi :

$$(a \vee b)(a \wedge b) = d|\alpha\beta| \times d = |ab|$$

Si $a, b \in \mathbb{Z}$, alors :

$$(a \vee b)(a \wedge b) = (|a| \vee |b|)(|a| \wedge |b|) = \big||a|\,|b|\big| = |ab|$$

La proposition est donc démontrée. ■

5) Généralisation du PGCD à plusieurs entiers

Définition 5 Soient $n \in \mathbb{N} \setminus \{0,1\}$ et $a_1, \dots, a_n \in \mathbb{Z}$.

- ⋆ Si $a_1 = \cdots = a_n = 0$, alors on pose $a_1 \wedge \cdots \wedge a_n = 0$.
- ⋆ Si l'un des entiers $a_1, \dots, a_n$ est non nul, alors on pose :

$$a_1 \wedge \cdots \wedge a_n = \max(\mathscr{D}(a_1) \cap \cdots \cap \mathscr{D}(a_n))$$

On dit que les entiers $a_1, \dots, a_n$ sont *premiers entre eux dans leur ensemble* si $a_1 \wedge \cdots \wedge a_n = 1$.

Exemple 8 ⋆ $2 \wedge 4 \wedge 6 = 2$

⋆ $2 \wedge 4 \wedge -3 = 1$

Remarque : si les entiers $a_1, \dots, a_n$ sont deux à deux premiers entre eux, alors ils sont premiers entre eux dans leur ensemble (et la réciproque est fausse).

Exemple 9 $2 \wedge 4 \wedge 5 = 1$ et $2 \wedge 4 \neq 1$

Proposition 10 (relation de Bézout) Soient $n \in \mathbb{N} \setminus \{0,1\}$ et $a_1, \dots, a_n \in \mathbb{Z}$. Il existe $u_1, \dots, u_n \in \mathbb{Z}$ tels que :

$$\sum_{i=1}^{n} u_i a_i = a_1 \wedge \cdots \wedge a_n$$

Démonstration On utilise un raisonnement par récurrence. Pour tout entier $n \geqslant 2$, on considère la proposition $\mathscr{P}_n$: « pour tout $(a_1, \dots, a_n) \in \mathbb{Z}^n$, il existe $(u_1, \dots, u_n) \in \mathbb{Z}^n$ tel que $\sum_{i=1}^{n} u_i a_i = a_1 \wedge \cdots \wedge a_n$ ».

- ⋆ La proposition $\mathscr{P}_2$ est vraie d'après la relation de Bézout.
- ⋆ Soit $n \in \mathbb{N} \setminus \{0,1\}$ tel que $\mathscr{P}_n$ soit vraie et soit $(a_1, \dots, a_n, a_{n+1}) \in \mathbb{Z}^{n+1}$. Remarquons que :

$$a_1 \wedge \cdots \wedge a_n \wedge a_{n+1} = (a_1 \wedge \cdots \wedge a_n) \wedge a_{n+1}$$

D'après la relation de Bézout, il existe $(u, u_{n+1}) \in \mathbb{Z}^2$ tel que :

$$(a_1 \wedge \cdots \wedge a_n)u + a_{n+1}u_{n+1} = a_1 \wedge \cdots \wedge a_n \wedge a_{n+1}$$

On applique ensuite l'hypothèse de récurrence à la famille $(a_1, \dots, a_n)$. Il existe $(u_1, \dots, u_n) \in \mathbb{Z}^n$ tel que :

$$\sum_{i=1}^{n} u_i a_i = a_1 \wedge \cdots \wedge a_n$$

On a alors :

$$\sum_{i=1}^{n} u u_i a_i + a_{n+1}u_{n+1} = a_1 \wedge \cdots \wedge a_n \wedge a_{n+1}$$

La proposition $\mathscr{P}_{n+1}$ est donc vraie. ■

IV – Nombres premiers

Dans ce paragraphe, nous ne considèrerons que des entiers naturels.

1) Définition

Définition 6 Un entier $p \in \mathbb{N}$ est appelé un *nombre premier* s'il est différent de 1 et si ses seuls diviseurs positifs sont 1 et p *i.e.* si :

$$p \geqslant 2 \qquad \text{et} \qquad \mathscr{D}(p) = \{1, p\}$$

Un entier qui n'est pas premier est dit *composé*.

Exemple 10 1 n'est pas premier, $2, 3, 5$ et 13 sont premiers, 24 ne l'est pas.

Dans la suite, on note $\mathscr{P}$ l'ensemble des nombres premiers.
Le crible d'Eratosthène permet de construire une table des premiers nombres premiers. Il s'agit de supprimer de la table des entiers tous les multiples d'un entier. En supprimant tous ces multiples, il ne restera que les entiers qui ne sont multiples d'aucun entier supérieur ou égal à 2, et qui sont donc les nombres premiers.

2) Premières propriétés

Proposition 11
- ⋆ Deux nombres premiers distincts sont premiers entre eux.
- ⋆ Soient $p \in \mathscr{P}$ et $a, b \in \mathbb{Z}$. Si p divise ab, alors p divise a ou p divise b.
- ⋆ Tout entier naturel supérieur ou égal à 2 admet au moins un diviseur premier.
- ⋆ L'ensemble $\mathscr{P}$ des nombres premiers est infini.

Démonstration

⋆ Si p et q sont deux nombres premiers distincts, alors :

$$\mathscr{D}(p) \cap \mathscr{D}(q) \cap \mathbb{N}^* = \{1, p\} \cap \{1, q\} = 1$$

⋆ Par l'absurde, supposons que p ne divise ni a ni b. Alors $a \wedge p = 1$ et $b \wedge p = 1$. On sait alors que $ab \wedge p = 1$.

⋆ Soit $n \in \mathbb{N} \setminus \{0, 1\}$. L'ensemble $\mathscr{D}(n) \cap (\mathbb{N} \setminus \{0, 1\})$ est une partie de $\mathbb{N}$ non vide puisqu'elle contient n. Son plus petit élément p est un entier supérieur ou égal à 2. Si p n'est pas un nombre premier, alors il existe $k \in [\![2, p-1]\!]$ tel que $k \mid p$. Mais alors $k \mid n$ et donc, par minimalité de p, on a $k \geqslant p$, ce qui est absurde. Donc $p \in \mathscr{P}$.

⋆ Raisonnons par l'absurde. Supposons qu'il existe un nombre fini $n \in \mathbb{N}^*$ de nombres premiers que l'on note $p_1, \ldots, p_n$. Posons alors :

$$P = 1 + \prod_{i=1}^{n} p_i$$

Alors P est un entier supérieur ou égal à 2 donc il admet un diviseur premier (d'après le point précédent). Il existe donc $i_0 \in [\![1, n]\!]$ tel que $p_{i_0} \mid P$. Or on a aussi $p_{i_0} \mid \prod_{i=1}^{n} p_i$ donc $p_{i_0} \mid 1$, ce qui est absurde. Ainsi, $\mathscr{P}$ est infini. ■

Remarque : plus généralement, on peut montrer par récurrence que :

$$\forall n \in \mathbb{N} \setminus \{0, 1\},\ \forall p \in \mathscr{P},\ \forall a_1, \ldots, a_n \in \mathbb{Z},\ p \mid a_1 \ldots a_n \implies (\exists\, k \in [\![1, n]\!],\ p \mid a_k)$$

3) Décomposition en produit de facteurs premiers

Théorème 4 (fondamental de l'arithmétique) Soit $n \in \mathbb{N} \setminus \{0, 1\}$. Il existe un unique entier $r \in \mathbb{N}^*$ un unique $(p_1, \ldots, p_r) \in \mathscr{P}^r$ vérifiant $p_1 < \cdots < p_r$ et un unique $(\alpha_1, \ldots, \alpha_r) \in (\mathbb{N}^*)^r$ tels que :

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

Démonstration ⋆ **Existence :** on utilise une récurrence (forte). Pour tout entier n supérieur ou égal à 2, on considère la proposition $\mathscr{P}_n$: « tout entier compris entre 2 et n admet une décomposition en produit de facteurs premiers ».

— La proposition $\mathscr{P}_2$ est vraie car 2 est un nombre premier.

— Soit $n \in \mathbb{N} \setminus \{0,1\}$ tel que $\mathscr{P}_2, \dots, \mathscr{P}_n$ soient vraies. Montrons alors que $n+1$ admet une décomposition en produit de facteurs premiers. C'est évident si $n+1$ est premier. Sinon, on sait qu'il admet un diviseur premier $p \in [\![2, n]\!]$. Il existe alors $q \in \mathbb{N}^*$ tel que $n+1 = pq$. Comme $p \in [\![2, n]\!]$, on a $2 \leqslant q \leqslant n$. On peut donc appliquer l'hypothèse de récurrence à l'entier q, d'où le résultat pour $n+1$.

⋆ **Unicité :** supposons que l'on dispose de deux décompositions de n. Quitte à rajouter des exposants α_i ou β_i égaux à 0, ceci peut s'écrire :

$$n = \prod_{i=1}^{r} p_i^{\alpha_i} = \prod_{i=1}^{r} p_i^{\beta_i} \qquad \text{(les } p_i \text{ étant deux à deux distincts)}$$

Supposons qu'il existe un entier $k \in [\![1, r]\!]$ pour lequel $\alpha_k \neq \beta_k$. Par exemple, on peut supposer que $\alpha_k < \beta_k$. On a alors :

$$\prod_{\substack{1 \leqslant i \leqslant r \\ i \neq k}} p_i^{\alpha_i} = p_k^{\beta_k - \alpha_k} \prod_{\substack{1 \leqslant i \leqslant r \\ i \neq k}} p_i^{\beta_i}$$

Ainsi, p_k divise $\displaystyle\prod_{\substack{1 \leqslant i \leqslant r \\ i \neq k}} p_i^{\alpha_i}$ ce qui est impossible car pour tout les nombres premiers $p_1, \dots, p_{k-1}, p_{k+1}, \dots, p_r$ sont tous distincts de p_k (voir la dernière remarque). ■

Exemple 11 $12 = 2^2 \times 3$, $15 = 3 \times 5$, $32 = 2^5$

4) Valuation p-adique

Soient $n \in \mathbb{N}^*$ et $p \in \mathscr{P}$. L'ensemble $\left\{k \in \mathbb{N} \,\middle|\, p^k \mid n\right\}$ est non vide (il contient 0 puisque $1 \mid n$) et il est majoré (par $\ln(n)/\ln(p)$) donc il admet un maximum.

Définition 7 (valuation p-adique) Soient $n \in \mathbb{N}^*$ et $p \in \mathscr{P}$. On appelle *valuation p-adique* de n l'entier :

$$v_p(n) = \max\left\{k \in \mathbb{N} \,\middle|\, p^k \mid n\right\}$$

Exemple 12 $v_5(250) = 3$, $v_3(8) = 0$

Remarques :

⋆ Ainsi, $v_p(n)$ est la plus grande puissance de p qui divise n.

⋆ D'après le théorème fondamental de l'arithmétique, on a l'égalité suivante :

$$\forall n \in \mathbb{N} \setminus \{0,1\}, \qquad n = \prod_{p \in \mathscr{P}} p^{v_p(n)},$$

le produit étant fini car seul un nombre fini de valuation p-adiques sont non nulles (ainsi, seul un nombre fini de facteurs dans le produit sont différents de 1).

⋆ Cette égalité est vraie aussi pour $n = 1$ (toutes les valuations p-adiques sont nulles).

Proposition 12 (propriétés de la valuation p-adique) Soient $a, b \in \mathbb{N}^*$ Alors :

⋆ pour tout $p \in \mathscr{P}$, on a $v_p(ab) = v_p(a) + v_p(b)$;

⋆ $a \mid b \iff (\forall p \in \mathscr{P},\ v_p(a) \leqslant v_p(b))$;

⋆ $a \wedge b = \prod_{p \in \mathscr{P}} p^{\min(v_p(a), v_p(b))}$;

⋆ $a \vee b = \prod_{p \in \mathscr{P}} p^{\max(v_p(a), v_p(b))}$.

Démonstration ⋆ D'après le théorème fondamental de l'arithmétique, on a :

$$ab = \left(\prod_{p \in \mathscr{P}} p^{v_p(a)} \right) \left(\prod_{p \in \mathscr{P}} p^{v_p(b)} \right) = \prod_{p \in \mathscr{P}} p^{v_p(a) + v_p(b)}$$

D'autre part, on a $ab = \prod_{p \in \mathscr{P}} p^{v_p(ab)}$. Par unicité de la décomposition en produit de facteurs premiers de ab, on a :

$$\forall p \in \mathscr{P}, \qquad v_p(ab) = v_p(a) + v_p(b)$$

⋆ On raisonne par double implication.

$\boxed{\Longrightarrow}$ On suppose que $a \mid b$. Soit $p \in \mathscr{P}$. Alors $p^{v_p(a)} \mid a$ donc (par transitivité de la relation $\mid$) on a aussi $p^{v_p(a)} \mid b$, *i.e.* :

$$p^{v_p(a)} \mid p^{v_p(b)} \prod_{q \in \mathscr{P} \setminus \{p\}} q^{v_q(b)}$$

Mais $p^{v_p(a)}$ et $\prod_{q \in \mathscr{P} \setminus \{p\}} q^{v_q(b)}$ sont premiers entre eux donc $p^{v_p(a)}$ divise $p^{v_p(b)}$ d'après le lemme de Gauss. Ceci implique que $p^{v_p(a)} \leqslant p^{v_p(b)}$ soit encore que $v_p(a) \leqslant v_p(b)$.

$\boxed{\Longleftarrow}$

⋆ Soit $p \in \mathscr{P}$. On a $a \wedge b \mid a$ donc $v_p(a \wedge b) \leqslant v_p(a)$. De même, $v_p(a \wedge b) \leqslant v_p(a)$. On en déduit que :

$$v_p(a \wedge b) \leqslant \min(v_p(a), v_p(b))$$

De plus, par définition de $v_p(a)$ et $v_p(b)$, on a $p^{\min(v_p(a), v_p(b))}$ divise a et b donc divise $a \wedge b$. Par définition de $v_p(a \wedge b)$, on a donc $\min(v_p(a), v_p(b)) \leqslant v_p(a \wedge b)$. Ainsi, $v_p(a \wedge b) = \min(v_p(a), v_p(b))$.

⋆ La démonstration est analogue. ■

✎✎✎ **Exercice 3** Déterminer le PGCD et le PPCM de 124 et de 342.

V – Congruences

Dans tout ce paragraphe, n désigne un entier naturel. On rappelle que :

$$\forall a, b \in \mathbb{Z}, \qquad a \equiv b \ [n] \iff \exists\, k \in \mathbb{Z},\ a = b + kn$$

1) Opérations sur les congruences

Proposition 13 La relation de congruence modulo n est compatible avec l'addition et la multiplication. Autrement dit, pour tous $a, b, c, d \in \mathbb{Z}$, on a :

⋆ $(a \equiv b \ [n] \text{ et } c \equiv d \ [n]) \Longrightarrow a + c \equiv b + d \ [n]$

⋆ $(a \equiv b \ [n] \text{ et } c \equiv d \ [n]) \Longrightarrow ac \equiv bd \ [n]$

⋆ $a \equiv b \ [n] \implies (\forall k \in \mathbb{N},\ a^k \equiv b^k \ [n])$

Démonstration Soient $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b\ [n]$ et $c \equiv d\ [n]$. Alors il existe des entiers relatifs k et ℓ tels que :

$$a = b + kn \qquad \text{et} \qquad c = d + \ell n$$

Ainsi :

$$a + c = b + d + (k + \ell)n \equiv b + d\ [n]$$

et :

$$ac = (b + kn)(d + \ell n) = bd + n(b\ell + dk + k\ell n) \equiv bd\ [n],$$

ce qu'il fallait démontrer.

⋆ Il s'agit de faire une récurrence à partir du point précédent. ■

✎✎✎ **Exercice 4** Calculer le reste dans la division euclidienne de $x = 24^{35}$ par 5.

Solution. On a :

$$x = (2^3)^{35}3^{35} = 2^{105}3^{35}$$

Or $2 \equiv -3\ [5]$ donc $2^{105} \equiv -3^{105}\ [5]$. Par conséquent, $x \equiv -3^{140}\ [5]$. Or $3^{140} = 9^{70}$ et $9 \equiv -1\ [5]$ donc $9^{70} \equiv 1\ [5]$. Finalement, $x \equiv -1 \equiv 4\ [5]$ donc le reste cherché vaut 4.

Définition 8 (inverse modulo n) Soit $a \in \mathbb{Z}$. On dit que a est inversible modulo n s'il existe $b \in \mathbb{Z}$ tel que $ab \equiv 1\ [n]$.

On dispose du résultat suivant :

Proposition 14 Soit $a \in \mathbb{Z}$.

- ⋆ Alors a est inversible modulo n si et seulement si $a \wedge n = 1$.
- ⋆ Si a est inversible modulo n, alors il existe un unique entier $k \in [\![1, n-1]\!]$ tel que $ak \equiv 1[n]$.

Démonstration Soit $a \in \mathbb{Z}$.

- ⋆ On a :

  $$a \text{ est inversible modulo } n \iff \exists b, v \in \mathbb{Z},\ ab = nv + 1 \iff a \wedge n = 1$$

  d'après le théorème de Bézout.
- ⋆ Si $k, \ell \in [\![1, n-1]\!]$ sont tels que $ak \equiv 1\ [n]$ et $a\ell \equiv 1\ [n]$, alors on a $ak \equiv a\ell\ [n]$ (par transitivité de la relation de congruence). On en déduit que n divise $a(k - \ell)$. Or $n \wedge a = 1$ (d'après le premier point) donc $n \mid k - \ell$. Mais $|k - \ell| < n$ donc $k = \ell$, ce qu'il fallait démontrer. ■

Exemple 13 On veut résoudre l'équation modulaire $5x \equiv 2\ [3]$. On remarque que $5 \times 2 \equiv 1\ [3]$ donc 5 est inversible modulo 3 et :

$$\forall x \in \mathbb{Z}, \qquad 5x \equiv 2\ [3] \iff 2 \times (5x) \equiv 2 \times 2\ [3] \iff x \equiv 4 \equiv 1\ [3]$$

L'ensemble des solutions cherché est donc :

$$\mathscr{S} = \left\{3k + 1 \,\middle|\, k \in \mathbb{Z}\right\}$$

2) Le petit théorème de Fermat

Lemme 2 Soient $p \in \mathscr{P}$ et $a, b \in \mathbb{Z}$. Alors :

- ⋆ $\forall k \in [\![1, p-1]\!]$, $p \mid \binom{p}{k}$;
- ⋆ $(a+b)^p \equiv a^p + b^p \ [p]$.

Démonstration Soient $p \in \mathscr{P}$ et $a, b \in \mathbb{Z}$.

(*i*) Soit $k \in [\![1, p-1]\!]$. Alors :

$$k\binom{p}{k} = p\binom{p-1}{k-1}$$

Donc $p \mid k\binom{p}{k}$ et comme $1 \leqslant k \leqslant p-1$, on a $p \wedge k = 1$ (puisque p est premier). Donc (lemme de Gauss) $p \mid \binom{p}{k}$.

(*ii*) D'après la formule du binôme de Newton :

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k}$$

d'où le résultat en utilisant le premier point. ■

Théorème 5 (petit théorème de Fermat) Soit p un nombre premier. Alors :

$$\forall a \in \mathbb{Z}, \qquad a^p \equiv a \ [p]$$

et :

$$\forall a \in \mathbb{Z} \setminus (p\mathbb{Z}), \qquad a^{p-1} \equiv 1 \ [p]$$

Démonstration On raisonne par récurrence sur l'entier a. Commençons par traiter le cas a positif. L'égalité est claire si $a = 0$. Supposons la relation de congruence vraie au rang $a \in \mathbb{N}$. Alors (d'après le lemme) :

$$(a+1) \equiv a^p + 1^p \equiv a + 1 \ [p]$$

en utilisant l'hypothèse de récurrence. On en déduit le résultat pour $a < 0$ par imparité si p est impair. Si $p = 2$, alors tout entier est congru à 0 ou 1 modulo 2 et le résultat est évident. Soit maintenant $a \in \mathbb{Z} \setminus (p\mathbb{Z})$. On sait que p divise $a^p - a = a(a^{p-1} - 1)$. Comme $p \wedge a = 1$ (puisque $a \notin p\mathbb{Z}$), on conclut du lemme de Gauss que $p \mid a^{p-1} - 1$. ■