Chapitre 12

Arithmétique dans $\mathbb{Z}$

12.1 Introduction historique

Les nombres entiers ont été faits par le bon Dieu, tout le reste est l'œuvre de l'homme.

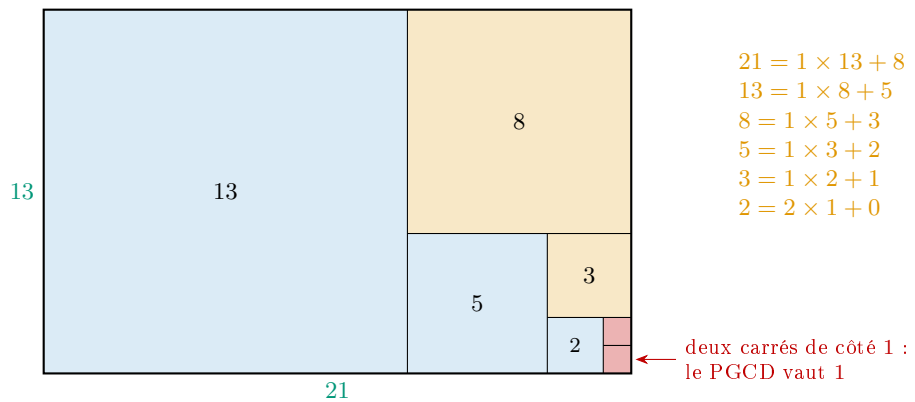
Leopold Kronecker, cité par Heinrich Weber - *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 1893

12.1.1 Vingt-trois siècles d'arithmétique

Vers 300 avant notre ère, les livres VII à IX des *Éléments* d'**Euclide** contiennent l'essentiel de ce chapitre : pour trouver la plus grande mesure commune de deux nombres, on retranche sans cesse le plus petit du plus grand (livre VII, propositions 1 et 2) ; un nombre premier qui divise un produit divise l'un des facteurs ; les nombres premiers sont en nombre infini. En 1624, dans la seconde édition de ses *Problèmes plaisants et délectables*, **Claude-Gaspard Bachet de Méziriac** résout l'équation $ax-by=1$ en remontant l'algorithme d'Euclide, cent cinquante ans avant que **Bézout** n'adapte la méthode aux polynômes. En 1640, **Pierre de Fermat** annonce à Frénicle de Bessy que $a^{p-1}-1$ est divisible par p ; **Euler** en publie la première démonstration en 1736. En 1801, les *Disquisitiones arithmeticae* de **Gauss** introduisent la notation des congruences et donnent la première démonstration complète de l'unicité de la décomposition en facteurs premiers. Enfin, en 1844, **Gabriel Lamé** montre que l'algorithme d'Euclide est rapide : son nombre d'étapes ne dépasse pas cinq fois le nombre de chiffres du plus petit des deux entiers.

12.1.2 Un rectangle découpé en carrés

La méthode d'Euclide se voit sur un rectangle de côtés 21 et 13. On en retire le plus grand carré possible, de côté 13 ; dans le rectangle restant, de côtés 13 et 8, on recommence, et ainsi de suite. Les côtés successifs, 13, 8, 5, 3, 2, 1, 1, sont les restes de l'algorithme d'Euclide, et le dernier carré, de côté 1, donne le PGCD : 21 et 13 sont premiers entre eux. Ce sont des nombres de Fibonacci, et Lamé a montré qu'ils constituent le cas le plus lent de l'algorithme. La section 12.3 en donnera la justification algébrique : le PGCD ne change pas lorsqu'on remplace le plus grand nombre par le reste de sa division par le plus petit.



12.2 Divisibilité et division euclidienne

Les entiers relatifs et leurs opérations sont supposés connus ; l'ensemble $\mathbb{Z}$ est un anneau intègre au sens du chapitre 11. Ce chapitre en étudie la divisibilité, en s'appuyant sur les sous-groupes de $(\mathbb{Z}, +)$.

12.2.1 Divisibilité

Définition : Soit a et b deux entiers relatifs. On dit que a **divise** b, et l'on note $a \mid b$, s'il existe $k \in \mathbb{Z}$ tel que $b = ka$. On dit aussi que a est un **diviseur** de b, ou que b est un **multiple** de a. Pour $n \in \mathbb{Z}$, on note $\mathcal{D}(n)$ l'ensemble des diviseurs de n.

Avec les notations du chapitre 11, $a \mid b$ si et seulement si $b \in a\mathbb{Z}$, ou encore si et seulement si $b\mathbb{Z} \subset a\mathbb{Z}$: « diviser », c'est « contenir » pour les ensembles de multiples. Tout entier divise 0, puisque $0 = 0 \times a$; en revanche, 0 ne divise que 0. L'erreur la plus répandue est d'écrire $a \mid b$ comme une fraction : $a \mid b$ est une *affirmation*, vraie ou fausse, alors que $\frac{b}{a}$ est un *nombre*.

Proposition 1 : Soit a, b, c des entiers relatifs.

(i) On a $a \mid a$, et si $a \mid b$ et $b \mid c$, alors $a \mid c$.

(ii) Si $a \mid b$ et $a \mid c$, alors $a \mid bu + cv$ pour tous entiers u et v.

(iii) Si $a \mid b$ et $b \neq 0$, alors $|a| \leqslant |b|$.

∘ Démonstration :

▷ *(i)* On a $a = 1 \times a$, et si $b = ka$ et $c = \ell b$, alors $c = (\ell k)a$.

▷ *(ii)* Si $b = ka$ et $c = \ell a$, alors $bu + cv = (ku + \ell v)a$.

▷ *(iii)* Si $b = ka$ avec $b \neq 0$, alors $k \neq 0$, donc $|k| \geqslant 1$ et $|b| = |k|\,|a| \geqslant |a|$. □

La divisibilité est donc réflexive et transitive. Elle n'est pas antisymétrique sur $\mathbb{Z}$, puisque $2 \mid -2$ et $-2 \mid 2$; la proposition suivante mesure exactement ce défaut.

Proposition 2 : *(Entiers associés.)* Soit a et b deux entiers. On a $a \mid b$ et $b \mid a$ si et seulement si $|a| = |b|$, c'est-à-dire $b = \pm a$. On dit alors que a et b sont **associés**.

∘ Démonstration : Si $b = \pm a$, chacun divise l'autre. Réciproquement, si $a = 0$, alors b, multiple de a, est nul. Sinon $b \neq 0$, et le point (iii) de la proposition 1 donne $|a| \leqslant |b|$ et $|b| \leqslant |a|$. □

Sur $\mathbb{N}$, la divisibilité est donc une relation d'ordre, partiel au sens du chapitre 2 : ni $2 \mid 3$ ni $3 \mid 2$. Dans le langage du chapitre 11, les associés de a sont les ua, où u parcourt le groupe $\mathbb{Z}^\times = \{-1, 1\}$ des inversibles de $\mathbb{Z}$.

12.2.2 Division euclidienne

Théorème 1 : Division euclidienne :
Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que

$$a = bq + r \qquad \text{et} \qquad 0 \leqslant r < b.$$

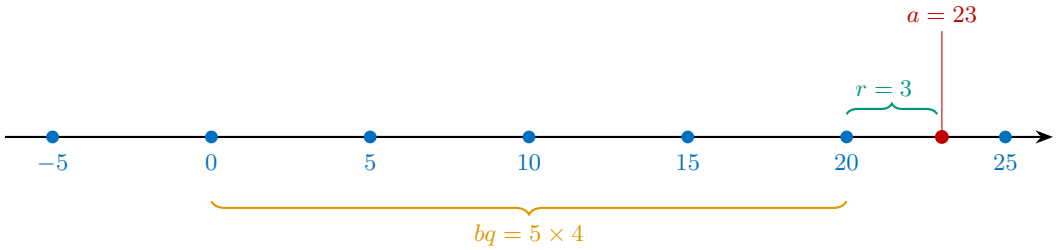
L'entier q est le **quotient**, et r le **reste**, de la division euclidienne de a par b.

∘ Démonstration :

▷ *Existence.* On pose $q = \lfloor \frac{a}{b} \rfloor$, partie entière du réel $\frac{a}{b}$ (chapitre 7), de sorte que $q \leqslant \frac{a}{b} < q + 1$. En multipliant par $b > 0$, on obtient $bq \leqslant a < bq + b$, donc $r = a - bq$ vérifie $0 \leqslant r < b$.

▷ *Unicité.* Si $a = bq + r = bq' + r'$ avec $0 \leqslant r, r' < b$, alors $b(q - q') = r' - r$, et $|r' - r| < b$. Ainsi b divise un entier de valeur absolue strictement inférieure à b : par le point (iii) de la proposition 1, cet entier est nul. Donc $r = r'$, puis $q = q'$. □

La figure place a entre deux multiples consécutifs de b : bq est le plus grand multiple de b inférieur ou égal à a, et le reste r mesure l'écart.



Les points bleus sont les éléments de $5\mathbb{Z}$; le reste est la distance de a au multiple de 5 situé immédiatement à sa gauche, ce qui explique la condition $0 \leqslant r < b$.

Remarques :

- Pour a négatif, le reste reste positif : $-23 = 5 \times (-5) + 2$. L'erreur la plus répandue est d'écrire $-23 = 5 \times (-4) - 3$, qui n'est pas une division euclidienne, puisque $-3 < 0$. C'est la même erreur que pour la partie entière d'un négatif (chapitre 7).
- Le reste de la division par b est le représentant de la classe de a modulo b dans $[\![0\,, b-1]\!]$ (chapitre 2, proposition 9) : $a \equiv r\ [b]$, et $b \mid a$ si et seulement si $r = 0$.

12.2.3 Les sous-groupes de $\mathbb{Z}$

Le chapitre 11 a montré que les $n\mathbb{Z}$ sont des sous-groupes de $(\mathbb{Z}, +)$; la division euclidienne montre que ce sont les seuls.

Théorème 2 : Sous-groupes de $\mathbb{Z}$:
Pour tout sous-groupe H de $(\mathbb{Z}, +)$, il existe un unique entier naturel n tel que $H = n\mathbb{Z}$.

∘ Démonstration :

▷ *Existence.* Si $H = \{0\}$, alors $H = 0\mathbb{Z}$. Sinon, H contient un entier non nul x, et aussi $-x$: la partie $H \cap \mathbb{N}^*$ est non vide, et elle a un plus petit élément n. Comme $n \in H$, tous ses multiples sont dans H, d'où $n\mathbb{Z} \subset H$. Réciproquement, soit $x \in H$, et $x = nq + r$ sa division euclidienne par n. Alors $r = x - nq$ appartient à H, et $0 \leqslant r < n$; par minimalité de n, on a $r = 0$, donc $x \in n\mathbb{Z}$.

▷ *Unicité.* Si $n\mathbb{Z} = m\mathbb{Z}$ avec n et m dans $\mathbb{N}$, alors $n \mid m$ et $m \mid n$, donc $n = m$ par la proposition 2. □

Remarque : La démonstration est celle de l'exercice 49 de la feuille du chapitre 11, pour les sous-groupes de $\mathbb{R}$: on prend le plus petit élément strictement positif. Dans $\mathbb{Z}$, ce plus petit élément existe toujours, parce que toute partie non vide de $\mathbb{N}$ a un plus petit élément ; c'est pourquoi le cas « dense » ne se présente pas.

12.3 PGCD, PPCM et relation de Bézout

On pourrait définir le PGCD de deux entiers comme le plus grand de leurs diviseurs communs, puis établir ses propriétés une à une. On choisit ici de l'obtenir directement à partir du théorème 2, ce qui donne la relation de Bézout sans effort ; la proposition 3 montrera que l'on retrouve bien le plus grand diviseur commun.

12.3.1 Définitions

Soit a et b deux entiers. L'ensemble $a\mathbb{Z} + b\mathbb{Z} = \{au + bv \mid (u, v) \in \mathbb{Z}^2\}$ est un sous-groupe de $\mathbb{Z}$, puisqu'il contient 0 et la différence de deux de ses éléments ; l'intersection $a\mathbb{Z} \cap b\mathbb{Z}$ en est un aussi (chapitre 11, proposition 8). Le théorème 2 permet de poser la définition suivante.

Définition : Soit a et b deux entiers relatifs.

- Le **PGCD** de a et b est l'unique entier naturel d tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. On le note $a \wedge b$.
- Le **PPCM** de a et b est l'unique entier naturel m tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. On le note $a \vee b$.

Les deux notations rappellent l'intersection et la réunion, et ce n'est pas un hasard : dans l'ensemble ordonné $(\mathbb{N}, |)$, $a \wedge b$ est la borne inférieure et $a \vee b$ la borne supérieure de $\{a, b\}$, comme le montre la proposition 3. Par exemple, $0 \wedge 0 = 0$, $a \wedge 0 = |a|$, $a \wedge 1 = 1$, et $a \wedge b = |a| \wedge |b|$, puisque $a\mathbb{Z} = (-a)\mathbb{Z}$.

Proposition 3 : Soit a et b deux entiers, $d = a \wedge b$ et $m = a \vee b$.

(i) Les diviseurs communs à a et b sont exactement les diviseurs de d : $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(d)$.

(ii) Si $(a, b) \neq (0, 0)$, alors $d \geqslant 1$, et d est le plus grand élément de $\mathcal{D}(a) \cap \mathcal{D}(b)$, pour l'ordre usuel comme pour la divisibilité.

(iii) Les multiples communs à a et b sont exactement les multiples de m. Si a et b sont non nuls, m est le plus petit multiple commun strictement positif.

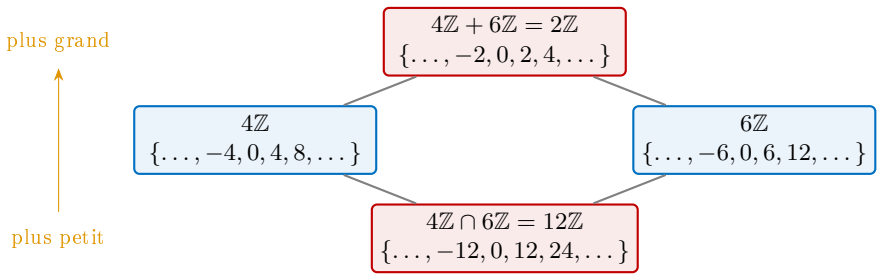
∘ Démonstration :

▷ *(i)* Comme $a = a \times 1 + b \times 0$, l'entier a appartient à $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$: $d \mid a$, et de même $d \mid b$. Tout diviseur de d divise donc a et b. Réciproquement, $d \in a\mathbb{Z} + b\mathbb{Z}$ s'écrit $d = au + bv$, et un diviseur commun à a et b divise $au + bv = d$ (proposition 1).

▷ *(ii)* Si $d = 0$, alors $a\mathbb{Z} + b\mathbb{Z} = \{0\}$, donc $a = b = 0$. Sinon, tout diviseur commun c divise $d \neq 0$, donc $c \leqslant |c| \leqslant d$ (proposition 1), et d lui-même est un diviseur commun.

▷ *(iii)* Un entier est multiple de a et de b si et seulement s'il appartient à $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. Si a et b sont non nuls, $ab \in a\mathbb{Z} \cap b\mathbb{Z}$ est non nul, donc $m \neq 0$, et tout multiple commun strictement positif est un multiple strictement positif de m, donc supérieur ou égal à m. □

On retrouve ainsi la définition usuelle : pour $(a, b) \neq (0, 0)$, $a \wedge b$ est le plus grand diviseur commun à a et b. La figure représente les quatre sous-groupes en jeu pour $a = 4$ et $b = 6$, rangés par inclusion : la somme $4\mathbb{Z} + 6\mathbb{Z}$ est le plus petit sous-groupe contenant les deux, l'intersection le plus grand contenu dans les deux.



Plus un sous-groupe est grand, plus son générateur est petit : le sommet $2\mathbb{Z}$ correspond au PGCD $4 \wedge 6 = 2$, et la base $12\mathbb{Z}$ au PPCM $4 \vee 6 = 12$. On retrouve le résultat annoncé au chapitre 2.

12.3.2 Relation de Bézout et algorithme d'Euclide

Théorème 3 : Relation de Bézout :
Soit a et b deux entiers. Il existe des entiers u et v tels que

$$au + bv = a \wedge b.$$

∘ Démonstration : Par définition, $a \wedge b$ appartient à $a\mathbb{Z} + b\mathbb{Z}$. □

Le couple (u, v) n'est pas unique : $(u + kb', v - ka')$ convient aussi, si $a = da'$ et $b = db'$. Il reste à calculer $a \wedge b$ et un tel couple, ce que fait l'algorithme d'Euclide.

Proposition 4 : Soit a, b, q des entiers. Alors $a \wedge b = b \wedge (a - bq)$. En particulier, si r est le reste de la division euclidienne de a par b, alors $a \wedge b = b \wedge r$.

∘ Démonstration : Les sous-groupes $a\mathbb{Z} + b\mathbb{Z}$ et $b\mathbb{Z} + (a - bq)\mathbb{Z}$ sont égaux. En effet, b et $a - bq$ sont dans le premier, donc le second est contenu dans le premier ; et $a = (a - bq) + bq$ est dans le second, donc le premier est contenu dans le second. Leurs générateurs positifs sont égaux. □

♡ **Méthode : Algorithme d'Euclide étendu, pour calculer $a \wedge b$ et un couple de Bézout** $(a > b > 0)$:

- On effectue les divisions euclidiennes successives : a par b, puis b par le premier reste, puis chaque reste par le suivant, en numérotant les lignes (L_1), (L_2), etc. Le dernier reste non nul est $a \wedge b$, puisque le PGCD est le même à chaque ligne (proposition 4) et que $r \wedge 0 = r$.
- On isole ce dernier reste non nul dans l'avant-dernière ligne : il s'écrit comme combinaison des deux restes qui le précèdent.
- On remonte l'algorithme : à chaque étape, on remplace le plus petit des deux restes présents par son expression tirée de la ligne au-dessus, puis on développe et on regroupe. Après la ligne (L_1), il ne reste que a et b, et l'on lit u et v.

On termine en vérifiant numériquement l'égalité $au + bv = a \wedge b$.

Exemple : Pour $a = 1071$ et $b = 462$, l'algorithme d'Euclide s'écrit

$$1071 = 2 \times 462 + 147 \quad (L_1), \qquad 462 = 3 \times 147 + 21 \quad (L_2), \qquad 147 = 7 \times 21 + 0 \quad (L_3).$$

Le dernier reste non nul est 21, donc $1071 \wedge 462 = 21$. On isole 21 dans (L_2), puis on remplace 147 grâce à (L_1) :

$$21 = 462 - 3 \times 147 = 462 - 3 \times (1071 - 2 \times 462) = 7 \times 462 - 3 \times 1071.$$

Le couple $(u, v) = (-3, 7)$ convient : $1071 \times (-3) + 462 \times 7 = -3213 + 3234 = 21$. Trois divisions ont suffi, là où la recherche de tous les diviseurs de 462 en demanderait bien davantage.

Remarque : La remontée oblige à conserver toutes les lignes, et elle devient laborieuse lorsque l'algorithme compte beaucoup d'étapes. On peut l'éviter en écrivant chaque reste, au fur et à mesure qu'on le calcule, sous la forme $r_k = au_k + bv_k$: on part de $a = a \times 1 + b \times 0$ et $b = a \times 0 + b \times 1$, et si $r_{k+1} = r_{k-1} - q_k r_k$, alors $u_{k+1} = u_{k-1} - q_k u_k$ et $v_{k+1} = v_{k-1} - q_k v_k$. Le couple de Bézout apparaît en même temps que le PGCD, sans retour en arrière. Pour $a = 1071$ et $b = 462$, on dispose les calculs dans un tableau, une ligne par reste :

reste r_k	quotient q_k	u_k	v_k
1071		1	0
462	2	0	1
147	3	1	-2
21	7	-3	7
0			

La ligne de 147 se lit $147 = 1071 \times 1 + 462 \times (-2)$, c'est-à-dire (L_1) réécrite ; celle de 21 s'obtient en retranchant 3 fois la ligne de 147 à celle de 462, et redonne le couple $(-3, 7)$ trouvé par la remontée. C'est cette version que l'on programme, et c'est elle qui servira au chapitre 13 pour les polynômes, où la remontée deviendrait très lourde.

Proposition 5 : Pour tous entiers a, b et k, $(ka) \wedge (kb) = |k|\,(a \wedge b)$.

∘ Démonstration : On a $ka\mathbb{Z} + kb\mathbb{Z} = k(a\mathbb{Z} + b\mathbb{Z}) = k(a \wedge b)\mathbb{Z} = |k|(a \wedge b)\mathbb{Z}$, en multipliant par k chaque élément. □

Remarque : L'erreur la plus répandue est de croire que l'algorithme d'Euclide consiste à chercher les diviseurs communs. Il n'en cherche aucun : il remplace le couple (a, b) par un couple plus petit qui a le même PGCD, et c'est ce qui le rend si rapide. Le théorème de Lamé, cité dans l'introduction, en borne le nombre d'étapes.

12.4 Entiers premiers entre eux

12.4.1 Le théorème de Bézout

Définition : Deux entiers a et b sont **premiers entre eux** si $a \wedge b = 1$, c'est-à-dire si leurs seuls diviseurs communs sont 1 et -1.

Théorème 4 : Théorème de Bézout :
Deux entiers a et b sont premiers entre eux si et seulement s'il existe des entiers u et v tels que

$$au + bv = 1.$$

∘ Démonstration : Si $a \wedge b = 1$, la relation de Bézout fournit u et v. Réciproquement, si $au + bv = 1$, alors $1 \in a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$, donc $a \wedge b$ divise 1, et $a \wedge b = 1$. □

Remarque : Le sens réciproque est propre à la valeur 1. L'égalité $au + bv = d$ ne prouve pas que $a \wedge b = d$: elle prouve seulement que $a \wedge b$ divise d. Par exemple, $4 \times 2 + 6 \times (-1) = 2$ et $4 \wedge 6 = 2$, mais aussi $4 \times 1 + 6 \times 1 = 10$, alors que $4 \wedge 6 \neq 10$. C'est l'erreur la plus répandue sur la relation de Bézout. On retrouve l'exemple du chapitre 1 : $2 \times (-1) + 3 \times 1 = 1$ montre que 2 et 3 sont premiers entre eux.

Théorème 5 : Lemme de Gauss :
Soit a, b, c trois entiers. Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.

∘ Démonstration : Par le théorème de Bézout, il existe u et v tels que $au + bv = 1$. En multipliant par c, on obtient $c = acu + bcv$. Or a divise acu et bc, donc il divise c (proposition 1). □

L'hypothèse $a \wedge b = 1$ est indispensable : 6 divise 4×3 sans diviser 4 ni 3.

Proposition 6 : *(Forme irréductible.)* Soit a et b deux entiers non tous deux nuls, $d = a \wedge b$, et $a = da'$, $b = db'$. Alors $a' \wedge b' = 1$. En conséquence, tout rationnel s'écrit de façon unique $\frac{p}{q}$ avec $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$ et $p \wedge q = 1$: c'est sa **forme irréductible**.

∘ Démonstration :

▷ *Simplification par le PGCD.* Par la proposition 5, $d = (da') \wedge (db') = d\,(a' \wedge b')$, et $d \neq 0$, donc $a' \wedge b' = 1$.

▷ *Existence de la forme irréductible.* Soit $x = \frac{a}{b}$ avec $b \in \mathbb{N}^*$. On divise a et b par leur PGCD d : $x = \frac{a'}{b'}$ avec $b' \in \mathbb{N}^*$ et $a' \wedge b' = 1$.

▷ *Unicité.* Si $\frac{p}{q} = \frac{p'}{q'}$ sont deux formes irréductibles, alors $pq' = p'q$. Ainsi q divise pq' et est premier avec p ; par le lemme de Gauss, q divise q', et de même q' divise q. Les deux étant positifs, $q = q'$, puis $p = p'$. □

Proposition 7 : Soit a, b, n trois entiers.

(i) Si $a \mid n$, $b \mid n$ et $a \wedge b = 1$, alors $ab \mid n$.

(ii) Si $a \wedge n = 1$ et $b \wedge n = 1$, alors $ab \wedge n = 1$.

(iii) Si a et b sont des entiers naturels, $(a \wedge b)(a \vee b) = ab$.

∘ Démonstration :

▷ *(i)* On écrit $n = ak$. Comme b divise ak et est premier avec a, il divise k (lemme de Gauss) : $k = b\ell$, et $n = ab\ell$.

▷ *(ii)* On écrit $au + nv = 1$ et $bu' + nv' = 1$. En multipliant ces égalités, $ab\,(uu') + n\,(auv' + bu'v + nvv') = 1$, et le théorème de Bézout conclut.

▷ *(iii)* Si a ou b est nul, les deux membres sont nuls. Sinon, soit $d = a \wedge b$, $a = da'$ et $b = db'$, avec $a' \wedge b' = 1$ (proposition 6), et $M = da'b'$. Cet entier est un multiple commun de $a = da'$ et de $b = db'$. Réciproquement, si n est un multiple commun, $n = ak = da'k$ est divisible par db', donc $a'k$ est divisible par b', et b' divise k par le lemme de Gauss : n est un multiple de $da'b' = M$. Ainsi $a\mathbb{Z} \cap b\mathbb{Z} = M\mathbb{Z}$, donc $a \vee b = M$, et $(a \wedge b)(a \vee b) = d \cdot da'b' = ab$. □

Exemple : Pour $a = 1071$ et $b = 462$, on obtient $1071 \vee 462 = \frac{1071 \times 462}{21} = 23\,562$. On calcule ainsi le PPCM sans chercher de multiples, à partir du PGCD donné par l'algorithme d'Euclide.

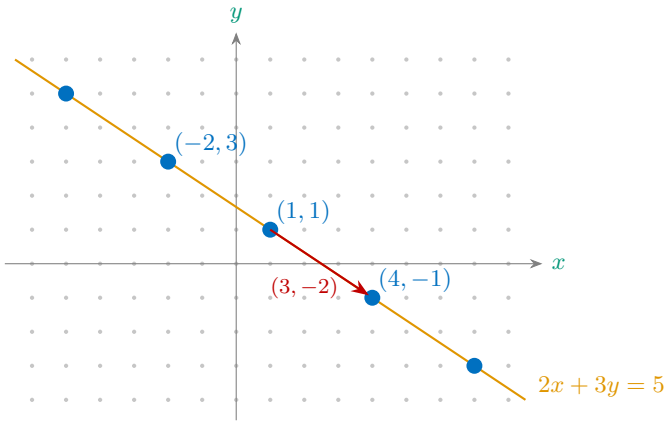
12.4.2 Équations $ax + by = c$

♡ **Méthode : Pour résoudre dans $\mathbb{Z}^2$ l'équation $ax + by = c$** (a et b non nuls) :

- On calcule $d = a \wedge b$. Si d ne divise pas c, l'équation n'a pas de solution, puisque d divise $ax + by$ pour tous x et y.
- Si $d \mid c$, on divise tout par d pour se ramener au cas $a \wedge b = 1$, puis on trouve une solution particulière (x_0, y_0) à partir d'un couple de Bézout, multiplié par c.
- Si (x, y) est une autre solution, alors $a(x - x_0) = -b(y - y_0)$, et le lemme de Gauss donne $b \mid x - x_0$: les solutions sont les couples $(x_0 + kb,\ y_0 - ka)$, pour $k \in \mathbb{Z}$.

Exemple : Résolvons $4x + 6y = 10$. On a $4 \wedge 6 = 2$, qui divise 10, et l'équation équivaut à $2x + 3y = 5$. Le couple $(1, 1)$ en est une solution évidente ; les solutions sont donc les couples $(1 + 3k,\ 1 - 2k)$, pour $k \in \mathbb{Z}$. L'équation $4x + 6y = 7$, au contraire, n'a pas de solution entière : le membre de gauche est pair.

La figure représente la droite d'équation $2x + 3y = 5$ et ses points à coordonnées entières : ils sont régulièrement espacés, le passage de l'un au suivant se faisant par le vecteur $(3, -2)$.



La droite passe par des points à coordonnées entières parce que $2 \wedge 3$ divise 5 ; pour la droite $2x + 4y = 5$, il n'y en aurait aucun.

12.4.3 Famille finie d'entiers

Les définitions s'étendent à un nombre fini d'entiers $a_1, \ldots, a_n$. Le sous-groupe $a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$ s'écrit $d\mathbb{Z}$, avec un unique $d \in \mathbb{N}$ appelé PGCD de la famille, et noté $a_1 \wedge \cdots \wedge a_n$. Le raisonnement de la proposition 3 montre que les diviseurs communs aux a_i sont les diviseurs de d, et l'on a une relation de Bézout $a_1u_1 + \cdots + a_nu_n = d$. On vérifie aussi que $a_1 \wedge a_2 \wedge a_3 = (a_1 \wedge a_2) \wedge a_3$, puisque $a_1\mathbb{Z} + a_2\mathbb{Z} + a_3\mathbb{Z} = (a_1 \wedge a_2)\mathbb{Z} + a_3\mathbb{Z}$.

Définition : Les entiers $a_1, \ldots, a_n$ sont **premiers entre eux dans leur ensemble** si $a_1 \wedge \cdots \wedge a_n = 1$, et **premiers entre eux deux à deux** si $a_i \wedge a_j = 1$ pour tous $i \neq j$.

Exemple : Les entiers 6, 10 et 15 sont premiers entre eux dans leur ensemble, puisque $6 \wedge 10 = 2$ et $2 \wedge 15 = 1$; une relation de Bézout est $6 + 10 - 15 = 1$. Ils ne sont pas premiers entre eux deux à deux : $6 \wedge 10 = 2$, $10 \wedge 15 = 5$ et $6 \wedge 15 = 3$. Deux à deux entraîne dans leur ensemble, mais la réciproque est fausse dès qu'il y a trois entiers.

12.5 Nombres premiers

12.5.1 Définition et crible d'Ératosthène

Définition : Un entier naturel p est **premier** si $p \geqslant 2$ et si ses seuls diviseurs positifs sont 1 et p. On note $\mathcal{P}$ l'ensemble des nombres premiers.

Le chapitre 1 a établi deux résultats, par récurrence forte et par l'absurde : tout entier $n \geqslant 2$ est un produit de nombres premiers, et $\mathcal{P}$ est infini. L'entier 1 n'est pas premier ; ce choix rendra unique la décomposition du théorème 6.

Proposition 8 : Si $n \geqslant 2$ n'est pas premier, il admet un diviseur premier p tel que $p \leqslant \sqrt{n}$.

∘ Démonstration : On écrit $n = ab$ avec $2 \leqslant a \leqslant b$, ce qui est possible puisque n n'est pas premier. Alors $a^2 \leqslant ab = n$, donc $a \leqslant \sqrt{n}$, et un facteur premier p de a, qui existe d'après le chapitre 1, vérifie $p \leqslant a \leqslant \sqrt{n}$ et divise n. □

♡ **Méthode : Crible d'Ératosthène, pour obtenir les nombres premiers jusqu'à N :**

- On écrit les entiers de 2 à N, puis on entoure 2 et l'on barre tous ses autres multiples.
- Le premier entier non barré qui suit est premier : on l'entoure, et l'on barre ses multiples, en commençant à son carré.
- On s'arrête dès que l'entier entouré dépasse $\sqrt{N}$: par la proposition 8, tous les entiers non barrés sont alors premiers.

La figure montre le crible pour $N = 100$, avec $\sqrt{100} = 10$: il suffit de barrer les multiples de 2, 3, 5 et 7. Chaque case barrée est colorée selon son plus petit facteur premier.

1	(2)	(3)	4	(5)	6	(7)	8	9	10
(11)	12	(13)	14	15	16	(17)	18	(19)	20
21	22	(23)	24	25	26	27	28	(29)	30
(31)	32	33	34	35	36	(37)	38	39	40
(41)	42	(43)	44	45	46	(47)	48	49	50
51	52	(53)	54	55	56	57	58	(59)	60
(61)	62	63	64	65	66	(67)	68	69	70
(71)	72	(73)	74	75	76	77	78	(79)	80
81	82	(83)	84	85	86	87	88	(89)	90
91	92	93	94	95	96	(97)	98	99	100

Les vingt-cinq entiers entourés en violet sont les nombres premiers inférieurs à 100 ; les cases bleues, orange, vertes et rouges sont les entiers barrés dont le plus petit facteur premier est 2, 3, 5 ou 7. La colonne des multiples de 10 est toute bleue, et les nombres premiers autres que 2 et 5 se trouvent tous dans les colonnes 1, 3, 7 et 9.

12.5.2 Le lemme d'Euclide et la décomposition en facteurs premiers

Proposition 9 : Soit p un nombre premier et a un entier.

(i) Si p ne divise pas a, alors $p \wedge a = 1$.

(ii) *(Lemme d'Euclide.)* Si p divise un produit ab, alors $p \mid a$ ou $p \mid b$. Plus généralement, si p divise un produit de k facteurs, il divise l'un des facteurs.

∘ Démonstration :

▷ *(i)* Le PGCD $p \wedge a$ est un diviseur positif de p, donc vaut 1 ou p ; il ne vaut pas p, puisque $p \nmid a$.

▷ *(ii)* Si $p \nmid a$, alors $p \wedge a = 1$, et le lemme de Gauss donne $p \mid b$. Le cas de k facteurs s'en déduit par récurrence sur k. □

Théorème 6 : Décomposition en facteurs premiers :
Tout entier $n \geqslant 2$ s'écrit

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

où $p_1 < p_2 < \cdots < p_r$ sont des nombres premiers et α_1, …, α_r des entiers naturels non nuls. Cette écriture est unique.

De plus, les diviseurs positifs de n sont exactement les entiers $p_1^{\beta_1} \cdots p_r^{\beta_r}$, avec $0 \leqslant \beta_i \leqslant \alpha_i$ pour tout i, et leur nombre est

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1).$$

∘ Démonstration :

▷ *Existence.* C'est le résultat du chapitre 1, en regroupant les facteurs égaux et en les rangeant par ordre croissant.

▷ *Unicité.* On montre, par récurrence forte sur n, que deux décompositions de n en produit de nombres premiers ont les mêmes facteurs, répétés le même nombre de fois. C'est clair pour $n = 2$. Soit

$$n = p_1 \cdots p_k = q_1 \cdots q_\ell$$

deux écritures en produits de nombres premiers, non nécessairement distincts. Le premier p_1 divise $q_1 \cdots q_\ell$, donc, par le lemme d'Euclide, il divise l'un des q_j, et lui est égal puisque q_j est premier. On simplifie par $p_1 = q_j$: l'entier $\frac{n}{p_1}$ vaut 1, ce qui impose $k = \ell = 1$, ou bien il est compris entre 2 et $n-1$, et l'hypothèse de récurrence s'applique aux deux produits restants.

▷ *Diviseurs.* Soit $d \geqslant 1$ un diviseur de n, et $k = \frac{n}{d}$. Tout nombre premier qui divise d ou k divise n, donc l'un des p_i d'après le lemme d'Euclide, et lui est égal. En décomposant d et k, on peut donc écrire $d = p_1^{\beta_1} \cdots p_r^{\beta_r}$ et $k = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$ avec des exposants entiers naturels, éventuellement nuls. Alors $n = dk = p_1^{\beta_1+\gamma_1} \cdots p_r^{\beta_r+\gamma_r}$, et l'unicité donne $\beta_i + \gamma_i = \alpha_i$, donc $\beta_i \leqslant \alpha_i$. Réciproquement, si $0 \leqslant \beta_i \leqslant \alpha_i$ pour tout i, l'entier $p_1^{\beta_1} \cdots p_r^{\beta_r}$ divise n, le quotient étant $p_1^{\alpha_1-\beta_1} \cdots p_r^{\alpha_r-\beta_r}$. L'application

$$(\beta_1, \ldots, \beta_r) \longmapsto p_1^{\beta_1} \cdots p_r^{\beta_r}, \qquad [\![0, \alpha_1]\!] \times \cdots \times [\![0, \alpha_r]\!] \longrightarrow \mathcal{D}(n) \cap \mathbb{N}^*,$$

est donc surjective, et elle est injective par unicité de la décomposition. Le lemme 6 du chapitre 2, appliqué $r-1$ fois, donne le nombre d'éléments du produit cartésien, soit $(\alpha_1 + 1) \cdots (\alpha_r + 1)$. □

Exemple : Comme $1071 = 3^2 \times 7 \times 17$, l'entier 1071 a $(2+1)(1+1)(1+1) = 12$ diviseurs positifs : 1, 3, 7, 9, 17, 21, 51, 63, 119, 153, 357 et 1071. On les obtient tous en choisissant l'exposant de 3 parmi 0, 1, 2, et ceux de 7 et de 17 parmi 0, 1 ; l'ensemble $\mathcal{D}(1071)$, qui contient aussi les opposés, a donc 24 éléments. L'erreur la plus répandue est d'oublier le $+1$, c'est-à-dire l'exposant nul : le diviseur 1 et tous ceux qui ne font pas intervenir l'un des facteurs disparaîtraient alors du compte.

Remarque : Gauss est le premier à avoir explicitement démontré l'unicité, en 1801. Elle n'a rien d'évident : dans l'anneau $\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} \mid (a, b) \in \mathbb{Z}^2\}$, qui ressemble aux entiers de Gauss du chapitre 11, on a $6 = 2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$, et l'on peut montrer que ces quatre facteurs ne se décomposent pas davantage. C'est le lemme d'Euclide, donc la relation de Bézout, qui fait la différence.

12.5.3 Valuations p-adiques

Définition : Soit p un nombre premier et $n \in \mathbb{Z}^*$. La **valuation p-adique** de n, notée $v_p(n)$, est le plus grand entier naturel k tel que p^k divise n.

Elle existe, puisque $p^k \mid n$ impose $2^k \leqslant p^k \leqslant |n|$, et elle vaut 0 si $p \nmid n$. Le théorème 6 s'écrit alors, pour $n \geqslant 1$,

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)},$$

le produit ne comportant qu'un nombre fini de facteurs différents de 1. Par exemple, $1071 = 3^2 \times 7 \times 17$, donc $v_3(1071) = 2$, $v_7(1071) = v_{17}(1071) = 1$, et $v_p(1071) = 0$ pour tout autre premier p. Le chapitre 1 a déjà rencontré la valuation 2-adique, avec l'écriture $n = 2^k(2m + 1)$.

Proposition 10 : Soit p un nombre premier, et a, b deux entiers non nuls.

(i) $v_p(ab) = v_p(a) + v_p(b)$.

(ii) $a \mid b$ si et seulement si $v_p(a) \leqslant v_p(b)$ pour tout nombre premier p.

(iii) $v_p(a \wedge b) = \min\big(v_p(a), v_p(b)\big)$ et $v_p(a \vee b) = \max\big(v_p(a), v_p(b)\big)$.

∘ Démonstration :

▷ *(i)* On écrit $a = p^\alpha a'$ et $b = p^\beta b'$ avec $\alpha = v_p(a)$, $\beta = v_p(b)$, et $p \nmid a'$, $p \nmid b'$. Alors $ab = p^{\alpha+\beta} a'b'$, et $p \nmid a'b'$ par le lemme d'Euclide, donc $v_p(ab) = \alpha + \beta$.

▷ *(ii)* Si $b = ak$, le point (i) donne $v_p(b) = v_p(a) + v_p(k) \geqslant v_p(a)$. Réciproquement, si $v_p(a) \leqslant v_p(b)$ pour tout p, l'entier $k = \prod_p p^{v_p(b)-v_p(a)}$ vérifie $|b| = |a|\,k$ par le théorème 6, donc $a \mid b$.

▷ *(iii)* Par le point (ii), un entier positif c divise a et b si et seulement si $v_p(c) \leqslant \min(v_p(a), v_p(b))$ pour tout p. Le plus grand d'entre eux, qui est $a \wedge b$ par la proposition 3, est donc $\prod_p p^{\min(v_p(a),v_p(b))}$. Le cas du PPCM est symétrique. □

Exemple : Avec $1071 = 3^2 \times 7 \times 17$ et $462 = 2 \times 3 \times 7 \times 11$, on retrouve $1071 \wedge 462 = 3 \times 7 = 21$ et $1071 \vee 462 = 2 \times 3^2 \times 7 \times 11 \times 17 = 23\,562$. Cette méthode suppose les décompositions connues ; pour de grands entiers, elles sont très difficiles à obtenir, alors que l'algorithme d'Euclide reste rapide. C'est sur cette différence que repose la sécurité du chiffrement RSA.

12.6 Congruences

12.6.1 Rappels et premières applications

Le chapitre 2 a défini la congruence modulo un entier $n \in \mathbb{N}^*$: $a \equiv b\ [n]$ si n divise $b - a$. C'est une relation d'équivalence, dont les n classes sont celles de 0, 1, …, $n-1$ (proposition 9 du chapitre 2), et elle est compatible avec l'addition, la multiplication et les puissances (proposition 10 du chapitre 2). D'après le théorème 1, la classe de a est celle de son reste dans la division par n.

Exemple : Comme $10 \equiv 1\ [9]$, on a $10^k \equiv 1\ [9]$ pour tout k, donc un entier est congru modulo 9 à la somme de ses chiffres : $\sum c_k 10^k \equiv \sum c_k\ [9]$. En particulier, $10^n + 1 \equiv 2\ [9]$ pour tout n, ce qu'annonçait le chapitre 1 à propos d'une récurrence sans initialisation. De même, $10 \equiv -1\ [11]$ donne $\sum c_k 10^k \equiv \sum (-1)^k c_k\ [11]$: 2026 est congru à $6 - 2 + 0 - 2 = 2$ modulo 11.

Remarque : On ne divise pas une congruence. L'erreur la plus répandue est de simplifier $2x \equiv 2y\ [6]$ en $x \equiv y\ [6]$: on a $2 \times 4 \equiv 2 \times 1\ [6]$, puisque $8 - 2 = 6$, mais $4 \not\equiv 1\ [6]$. La proposition suivante dit quand la simplification est permise.

12.6.2 Inverse modulo n

Proposition 11 : Soit $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. Il existe un entier u tel que $au \equiv 1\ [n]$ si et seulement si $a \wedge n = 1$. Un tel u est appelé un **inverse** de a modulo n. Dans ce cas, pour tous entiers x et y, $ax \equiv ay\ [n]$ entraîne $x \equiv y\ [n]$.

∘ Démonstration : On a $au \equiv 1\ [n]$ si et seulement s'il existe v tel que $au + nv = 1$, ce qui équivaut à $a \wedge n = 1$ par le théorème de Bézout. Si $ax \equiv ay\ [n]$, on multiplie par u : $x \equiv uax \equiv uay \equiv y\ [n]$. □

♡ **Méthode : Pour résoudre la congruence $ax \equiv b\ [n]$, lorsque $a \wedge n = 1$:**

- On cherche un inverse u de a modulo n, par l'algorithme d'Euclide étendu appliqué à a et n, ou à vue si n est petit.
- On multiplie la congruence par u : elle équivaut à $x \equiv ub\ [n]$, puisque l'on peut revenir en arrière en multipliant par a.
- On donne les solutions sous la forme $x = x_0 + kn$, $k \in \mathbb{Z}$, avec x_0 le reste de ub modulo n.

Si $d = a \wedge n > 1$, la congruence n'a de solution que si $d \mid b$, et l'on se ramène au cas précédent en divisant a, b et n par d, comme pour l'équation $ax + by = c$.

Exemple : Résolvons $7x \equiv 3\ [12]$. Comme $7 \times 7 = 49 = 4 \times 12 + 1$, l'entier 7 est son propre inverse modulo 12. La congruence équivaut à $x \equiv 21 \equiv 9\ [12]$: les solutions sont les entiers $9 + 12k$. Vérification : $7 \times 9 = 63 = 5 \times 12 + 3$. ✓

12.6.3 Modulo un nombre premier

Proposition 12 : Soit p un nombre premier, et a, b deux entiers. Si $ab \equiv 0\ [p]$, alors $a \equiv 0\ [p]$ ou $b \equiv 0\ [p]$. Tout entier non divisible par p a un inverse modulo p.

∘ Démonstration : La première affirmation est le lemme d'Euclide (proposition 9). Si $p \nmid a$, alors $a \wedge p = 1$, et la proposition 11 fournit un inverse. □

C'est ce qu'annonçait le chapitre 11 : modulo 6, on a $2 \times 3 \equiv 0$ sans qu'aucun facteur soit nul, ce qui ne peut pas se produire modulo un nombre premier. Modulo p, on calcule donc comme dans un corps : on peut simplifier par tout entier non divisible par p.

Proposition 13 : Soit p un nombre premier. Pour tout $k \in [\![1\,, p-1]\!]$, p divise $\binom{p}{k}$.

∘ Démonstration : La formule $k\binom{p}{k} = p\binom{p-1}{k-1}$ (chapitre 3) montre que p divise $k\binom{p}{k}$. Comme $1 \leqslant k \leqslant p-1$, p ne divise pas k, donc $p \wedge k = 1$ (proposition 9), et le lemme de Gauss conclut. □

Pour $p = 5$, la ligne $1, 5, 10, 10, 5, 1$ du triangle de Pascal le vérifie ; pour $p = 6$, qui n'est pas premier, $\binom{6}{2} = 15$ n'est pas divisible par 6.

Théorème 7 : Petit théorème de Fermat :
Soit p un nombre premier. Pour tout entier a,

$$a^p \equiv a\ [p], \qquad \text{et, si } p \nmid a, \qquad a^{p-1} \equiv 1\ [p].$$

∘ Démonstration :

▷ *Pour $a \in \mathbb{N}$, par récurrence.* L'égalité est vraie pour $a = 0$. Si $a^p \equiv a\ [p]$, la formule du binôme et la proposition 13 donnent

$$(a+1)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k + 1 \equiv a^p + 1 \equiv a + 1\ [p].$$

▷ *Pour $a < 0$.* L'entier a est congru à un entier naturel r modulo p, son reste, et $a^p \equiv r^p \equiv r \equiv a\ [p]$.

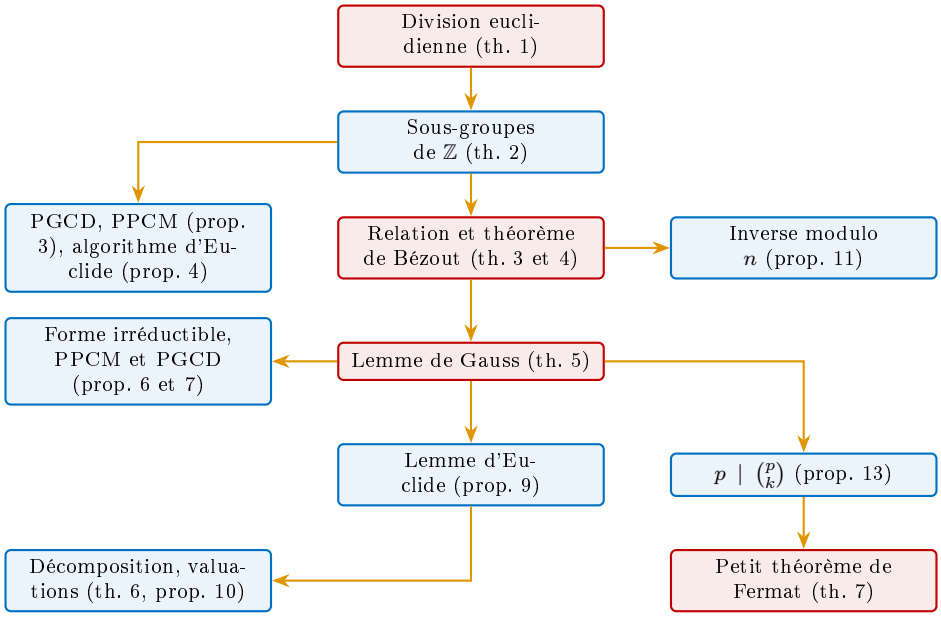
▷ *Seconde forme.* Si $p \nmid a$, la relation $a \cdot a^{p-1} \equiv a \cdot 1\ [p]$ se simplifie par a, inversible modulo p (proposition 12). □

Exemples :

- Pour calculer 3^{2026} modulo 7, on utilise $3^6 \equiv 1\ [7]$ et $2026 = 6{\times}337{+}4$, d'où $3^{2026} \equiv 3^4 \equiv 4\ [7]$, puisque $81 = 11 \times 7 + 4$. Le petit théorème de Fermat réduit l'exposant modulo $p-1$, et non modulo p : c'est l'erreur la plus répandue.
- La réciproque est fausse. L'entier $341 = 11 \times 31$ n'est pas premier, et pourtant $2^{340} \equiv 1\ [341]$, comme l'a remarqué Sarrus en 1820. En revanche, si $a^{n-1} \not\equiv 1\ [n]$ pour un a premier avec n, l'entier n n'est certainement pas premier : c'est le principe des tests de primalité utilisés en cryptographie.

12.7 Bilan

Tout le chapitre découle de la division euclidienne, à travers les sous-groupes de $\mathbb{Z}$. Le schéma montre l'enchaînement des résultats ; une flèche signifie « sert à démontrer ».



Les boîtes rouges sont les quatre résultats clés : la division euclidienne fonde tout, la relation de Bézout et le lemme de Gauss portent la théorie de la divisibilité, et le petit théorème de Fermat en est la première application aux congruences.

Question	Outil	Référence
calculer $a \wedge b$	algorithme d'Euclide	proposition 4
trouver u, v avec $au + bv = a \wedge b$	algorithme d'Euclide étendu	méthode, section 12.3
montrer que $a \wedge b = 1$	exhiber $au + bv = 1$	théorème 4
déduire $a \mid c$ de $a \mid bc$	vérifier $a \wedge b = 1$	théorème 5
résoudre $ax + by = c$	solution particulière, puis Gauss	méthode, section 12.4
résoudre $ax \equiv b\ [n]$	inverse de a modulo n	proposition 11
calculer a^k modulo p premier	réduire k modulo $p - 1$	théorème 7

Le chapitre 13 reprendra ce plan presque mot pour mot pour les polynômes : division euclidienne, PGCD, relation de Bézout, lemme de Gauss et décomposition en facteurs irréductibles. Seul le rôle des nombres premiers y sera tenu par les polynômes irréductibles.