13 | Arithmétique dans l'anneau $\mathbb{Z}$

1 Divisibilité dans $\mathbb{Z}$

1.1 Diviseurs, multiples

Définition 1 – Diviseur, multiple, entiers associés

Soit a et b deux entiers relatifs.

- On dit que a est un *diviseur de* b, ou que b est un *multiple de* a, ce que l'on note $a \mid b$, lorsqu'il existe $k \in \mathbb{Z}$ tel que $b = ka$. L'ensemble des multiples de a est $a\mathbb{Z}$ et on note $\mathcal{D}(a)$ l'ensemble des diviseurs de a.
- Les entiers a et b sont dits *associés* lorsque $a \mid b$ et $b \mid a$.

Exemple 2

- 1 et -1 divisent tous les entiers, mais ne sont divisibles que par 1 et -1, autrement dit $\mathcal{D}(1) = \mathcal{D}(-1) = \{\pm 1\}$.
- 0 est multiple de tous les entiers, autrement dit $\mathcal{D}(0) = \mathbb{Z}$, mais n'est diviseur que de lui-même.
- $\mathcal{D}(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$.

Théorème 3 – Propriétés de la relation de divisibilité

Soit a, b, c et d des entiers relatifs.

(i) Caractérisation des entiers associés. On a l'équivalence $(a \mid b \text{ et } b \mid a) \iff |a| = |b|$.

(ii) Relation d'ordre. La relation de divisibilité $\mid$ est une relation d'ordre sur $\mathbb{N}$, mais elle est seulement réflexive et transitive sur $\mathbb{Z}$.

(iii) Combinaison linéaire. Pour tous $u, v \in \mathbb{Z}$, on a l'implication $(d \mid a \text{ et } d \mid b) \implies d \mid au + bv$.

(iv) Produit. On dispose des deux implications suivantes

$$(a \mid b \text{ et } c \mid d) \implies ac \mid bd \qquad \text{et, en particulier,} \qquad a \mid b \implies \big(\forall k \in \mathbb{N},\ a^k \mid b^k\big).$$

Démonstration. ... ∎

Remarque 4

- Pour l'ordre $\mid$ sur $\mathbb{N}$, le plus petit élément de $\mathbb{N}$ est 1, et le plus grand 0.
- La divisibilité sur $\mathbb{N}^*$ est liée à l'ordre naturel de $\mathbb{N}^*$ par l'implication : $\forall a, b \in \mathbb{N}^*,\ a \mid b \implies a \leqslant b$. Ce résultat est toutefois faux dans $\mathbb{N}$, *e.g.* $1 \mid 0$.
- Pour tout $a \in \mathbb{Z}^*$, $\mathcal{D}(a) = \mathcal{D}(|a|)$ et $\max \mathcal{D}(a) = |a|$ (pour l'ordre usuel $\leqslant$).

1.2 Relation de congruence modulo un entier

Définition 5 – Relation de congruence modulo un entier

Soit $a, b, n \in \mathbb{Z}$. L'entier a est dit *congru à* b *modulo* n, ce que l'on note $a \equiv b\,[n]$, lorsque $n \mid b - a$, *i.e.* lorsqu'il existe $k \in \mathbb{Z}$ tel que $a = b + kn$.

La relation de congruence généralise celle de divisibilité, via l'équivalence

$$n \mid a \iff a \equiv 0\,[n].$$

Cette équivalence fondamentale permet de passer du langage de la divisibilité à celui des congruences et vice versa.

Théorème 6 – Propriétés de la relation de congruence modulo un entier

Soit $a, a', b, b', m, n \in \mathbb{Z}$.

(i) Relation d'équivalence. La relation de congruence $\equiv [n]$ est une relation d'équivalence sur $\mathbb{Z}$.

(ii) Somme. Si $a \equiv b\,[n]$ et $a' \equiv b'\,[n]$, alors $a + a' \equiv b + b'\,[n]$.

(iii) Produit. Si $a \equiv b\,[n]$ et $a' \equiv b'\,[n]$, alors $aa' \equiv bb'\,[n]$ et, pour tout $k \in \mathbb{N}$, $a^k \equiv b^k\,[n]$.

(iv) Multiplication/division par un entier non nul. Si m est non nul, $a \equiv b\,[n] \iff ma \equiv mb\,[mn]$.

Démonstration. ... ■

Exemple 7 $2^{345} + 5^{432}$ est divisible par 3. **En effet**, $2^{345} + 5^{432} \equiv (-1)^{345} + (-1)^{432} \equiv -1 + 1 \equiv 0\,[3]$.

Exemple 8 Pour tout $n \in \mathbb{Z}$ impair, $n^2 \equiv 1\,[8]$.

Exemple 9 Soit $n \in \mathbb{N}^*$. Un entier a est pair (resp. impair) si et seulement si a^n est pair (resp. impair).

1.3 Division euclidienne

Théorème 10 – Division euclidienne

Si a est un entier relatif et b un entier naturel non nul, alors il existe un unique couple d'entiers relatifs (q, r) tel que

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

On a notamment $q = \lfloor a/b \rfloor$ et $r \equiv a\,[b]$. Les entiers a, b, q et r sont respectivement appelés le *dividende*, le *diviseur*, le *quotient* et le *reste de la division euclidienne de a par b*.

Démonstration. ... ■

Corollaire 11

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. L'entier b divise a si et seulement si le reste de la division euclidienne de a par b est nul.

Remarque 12 – Anneau $\mathbb{Z}/n\mathbb{Z}$ (programme de MP) Soit $n \in \mathbb{N}^*$. Le théorème de la division euclidienne se reformule en termes de congruence :

$$\forall a \in \mathbb{Z}, \quad \exists! r \in [\![0, n-1]\!], \quad a \equiv r\,[n].$$

Ainsi, tout entier relatif a est congru modulo n à un unique entier r compris entre 0 et $n-1$. L'ensemble quotient de $\mathbb{Z}$ par la relation d'équivalence $\equiv [n]$ est donc $\mathbb{Z}/\equiv [n] = \{n\mathbb{Z}, n\mathbb{Z}+1, \dots, n\mathbb{Z}+n-1\}$ (on le note aussi $\mathbb{Z}/n\mathbb{Z}$) et il est de cardinal n. La compatibilité de la relation de congruence avec l'addition et le produit (théorème 6 points **(ii)** et **(iii)**) permet alors de munir l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ d'une structure d'anneau héritée de celle de $\mathbb{Z}$. Précisément, en notant $\overline{x}$ la classe d'équivalence d'un entier, l'addition et la multiplication sur $\mathbb{Z}/n\mathbb{Z}$ sont définies par

$$\forall x, y \in \mathbb{Z}, \quad \overline{x} + \overline{y} = \overline{x+y} \quad \text{et} \quad \overline{x} \times \overline{y} = \overline{x \times y}.$$

Exemple 13 Le reste de la division euclidienne de 2^{65362} par 7 est 2.

2 PGCD et PPCM

Définition 14 – Diviseur/multiple commun

Soit $a_1, \dots, a_r$ des entiers relatifs.

- On appelle *diviseur commun* de $a_1, \dots, a_r$ tout entier relatif qui divise à la fois $a_1, \dots, a_{r-1}$ et a_r.
- On appelle *multiple commun* de $a_1, \dots, a_r$ tout entier relatif divisible à la fois par $a_1, \dots, a_{r-1}$ et a_r.

Exemple 15 Les diviseurs communs de 12 et 18 sont $\pm1, \pm2, \pm3, \pm6$, *i.e.* les diviseurs de 6,

$$\mathcal{D}(12) \cap \mathcal{D}(18) = \{\pm1, \pm2, \pm3, \pm4, \pm6, \pm12\} \cap \{\pm1, \pm2, \pm3, \pm6, \pm9, \pm18\} = \{\pm1, \pm2, \pm3, \pm6\} = \mathcal{D}(6).$$

Les multiples communs de 12 et 18 sont tous les multiples de 36, *i.e.* $12\mathbb{Z} \cap 18\mathbb{Z} = 36\mathbb{Z}$ (cf. théorème 41 pour une justification).

2.1 PGCD et PPCM de deux entiers

Soit a et b deux entiers relatifs.

- Si $(a, b) \neq (0, 0)$, l'ensemble des diviseurs communs à a et b est une partie de $\mathbb{Z}$, non vide (elle contient 1) et majorée par $\max\{|a|, |b|\}$. Elle possède donc un plus grand élément supérieur ou égal à 1.
- Si $ab \neq 0$, l'ensemble des multiples strictement positifs communs à a et b est une partie de $\mathbb{N}$ non vide (elle contient $|ab|$). Elle possède donc un plus petit élément.

Ces remarques liminaires légitiment les deux définitions suivantes.

Définition 16 – PGCD/PPCM de deux entiers

Soit a et b deux entiers relatifs.

- **PGCD.** Lorsque $(a, b) \neq (0, 0)$, on appelle *plus grand commun diviseur (ou PGCD) de a et b*, noté $a \wedge b$, le plus grand élément (pour l'ordre usuel $\leqslant$) de l'ensemble des diviseurs communs de a et b, soit
$$a \wedge b = \max(\mathcal{D}(a) \cap \mathcal{D}(b)).$$
Par ailleurs, par convention, $0 \wedge 0 = 0$.
- **PPCM.** Lorsque $ab \neq 0$, on appelle *plus petit commun multiple (ou PPCM) de a et b*, noté $a \vee b$, le plus petit élément (pour l'ordre usuel $\leqslant$) de l'ensemble des multiples communs strictement positifs de a et b, soit
$$a \vee b = \min(|a|\mathbb{N}^* \cap |b|\mathbb{N}^*).$$
Par ailleurs, par convention, $0 \vee a = a \vee 0 = 0$, pour tout $a \in \mathbb{Z}$.

Exemple 17
- $12 \wedge 18 = 6$, d'après l'exemple 15.
- Pour tout $a \in \mathbb{Z}$, $a \wedge 1 = 1$ et $a \wedge 0 = |a|$.

Remarque 18 Pour tous $a, b \in \mathbb{Z}$,

$$a \wedge b = |a| \wedge |b|, \quad a \vee b = |a| \vee |b|, \quad a \wedge b = b \wedge a \quad \text{et} \quad a \vee b = b \vee a,$$

dans la mesure où $\mathcal{D}(a) = \mathcal{D}(|a|)$ et par commutativité de $\cap$. Par la suite, on pourra donc sans perte de généralité supposer que a et b sont des entiers naturels.

2.2 Algorithme d'Euclide et relations de Bézout

Théorème 19 – Principe à la base de l'algorithme d'Euclide

Pour tous $a, b, r \in \mathbb{Z}$, si $a \equiv r\,[b]$, alors
$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(r)$$
et par conséquent $a \wedge b = b \wedge r$.

Démonstration. Si $a \equiv r\,[b]$, alors il existe $k \in \mathbb{Z}$ tel que $a = r + kb$. Ainsi, d'une part, tout diviseur commun de b et r divise aussi $a = r + kb$ et b (point **(iii)** du théorème 3). D'autre part, tout diviseur commun de a et b divise aussi $r = a - kb$ et b (idem). Par conséquent,
$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(r).$$
Si $b \neq 0$, le résultat sur le pgcd en découle par définition. Et ce dernier est trivial pour $b = 0$. ∎

Exemple 20 Pour tout $n \in \mathbb{Z}$, $(3n + 1) \wedge (2n + 5) = \begin{cases} 13 & \text{si } n \equiv 4\,[13] \\ 1 & \text{sinon.} \end{cases}$

Algorithme d'Euclide L'*algorithme d'Euclide*[†] décrit ci-après est un algorithme de calcul effectif du PGCD de deux entiers relatifs. Précisément, étant donnés deux entiers naturels a et b, définissons une suite d'entiers r_k par

- $r_0 = a$ et $r_1 = b$;
- pour tout $k \in \mathbb{N}$, tant que $r_{k+1} \neq 0$, r_{k+2} est le reste de la division euclidienne de r_k par r_{k+1}.

Lors de la deuxième étape, si $r_{k+1} \neq 0$, on a par construction $0 \leqslant r_{k+2} < r_{k+1}$. La suite d'entiers r_k ainsi construite est strictement décroissante à partir du rang 1 et à valeurs dans $\mathbb{N}$, il existe donc un rang N tel que $r_N \neq 0$ et $r_{N+1} = 0$, ce qui assure la terminaison de l'algorithme. Par ailleurs, dans la mesure où $r_k \equiv r_{k+2}\,[r_{k+1}]$, pour tout $k \in [\![0\,, N-1]\!]$, le théorème 19 garantit que

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(r_0) \cap \mathcal{D}(r_1) = \mathcal{D}(r_1) \cap \mathcal{D}(r_2) = \ldots = \mathcal{D}(r_N) \cap \mathcal{D}(r_{N+1}) = \mathcal{D}(r_N)$$

et

$$a \wedge b = r_0 \wedge r_1 = r_1 \wedge r_2 = \ldots = r_N \wedge r_{N+1} = r_N,$$

puisque $r_{N+1} = 0$. Par conséquent,

> Le PGCD de a et b est le dernier reste non nul obtenu dans la suite des divisions successives des r_k.

Notons en outre que cet algorithme reste valable pour deux entiers relatifs quelconques, dans la mesure où $a \wedge b = |a| \wedge |b|$. Le théorème suivant en découle alors directement.

Théorème 21 – Diviseurs communs *vs* diviseurs du PGCD

Les diviseurs communs de deux entiers a et b sont exactement les diviseurs de leur PGCD $a \wedge b$, autrement dit

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a \wedge b).$$

Exemple 22 $2020 \wedge 150 = 10$.

En effet, des divisions euclidiennes successives donnent

$$\underset{r_0}{2020} = \underset{r_1}{150} \times 13 + \underset{r_2}{70}\ ; \qquad \underset{r_1}{150} = \underset{r_2}{70} \times 2 + \underset{r_3}{10}\ ; \qquad \underset{r_2}{70} = \underset{r_3}{10} \times 7 + \underset{r_4}{0}.$$

Algorithme d'Euclide étendu À la différence de l'algorithme d'Euclide qui ne s'intéresse qu'aux restes successifs r_k des divisions euclidiennes, sa version étendue, en prenant également en compte les quotients successifs, va permettre à chaque étape de construire un couple d'entiers (u_k, v_k) tel que $au_k + bv_k = r_k$.
Précisément, étant donnés deux entiers naturels a et b, définissons des suites d'entiers r_k, u_k et v_k par

- $r_0 = a$, $u_0 = 1$ et $v_0 = 0$;
- $r_1 = b$, $u_1 = 0$ et $v_1 = 1$;
- pour tout $k \in \mathbb{N}$, tant que $r_{k+1} \neq 0$, on considère r_{k+2} et q_{k+2} le reste et le quotient de la division euclidienne de r_k par r_{k+1}, ainsi $r_{k+2} = r_k - q_{k+2}r_{k+1}$, et on pose

$$u_{k+2} = u_k - q_{k+2}u_{k+1} \quad \text{et} \quad v_{k+2} = v_k - q_{k+2}v_{k+1}.$$

Considérons le rang N tel que $r_N \neq 0$ et $r_{N+1} = 0$ (cf. algorithme d'Euclide), une récurrence double sur $k \in [\![0\,, N]\!]$ permet alors d'établir la propriété

$$\mathscr{P}(k) : \text{« } r_k = au_k + bv_k \text{ »}.$$

- **Initialisation.** $\mathscr{P}(0)$ et $\mathscr{P}(1)$ sont clairement vraies.
- **Hérédité.** Soit $k \in [\![0\,, N-2]\!]$. Supposons $\mathscr{P}(k)$ et $\mathscr{P}(k+1)$ vraies, alors

$$r_{k+2} = r_k - q_{k+2}r_{k+1} \overset{\text{H.R.}}{=} au_k + bv_k - q_{k+2}(au_{k+1} + bv_{k+1}) = a(u_k - q_{k+2}u_{k+1}) + b(v_k - q_{k+2}v_{k+1}) = au_{k+2} + bv_{k+2},$$

  soit $\mathscr{P}(k+2)$, ce qui achève la récurrence.

En particulier, au rang N, $a \wedge b = r_N = au_N + bv_N$, ce qui démontre le théorème fondamental suivant (l'hypothèse initiale $a, b \in \mathbb{N}$ n'étant pas restrictive).

†. Euclide ($\approx$ 300 av. J.-C.) est un mathématicien de la Grèce antique, auteur d'un traité de mathématiques qui constitue l'un des textes fondateurs de cette discipline en Occident : *Les Éléments*. Il s'agit d'un des plus anciens traités connus présentant de manière systématique, à partir d'axiomes et de postulats, un large ensemble de théorèmes accompagnés de leurs démonstrations. *Les Éléments* porte sur la géométrie, tant plane que solide, et l'arithmétique théorique.

Théorème 23 – Relations de Bézout

Soit $a, b \in \mathbb{Z}$. Il existe deux entiers relatifs u, v tels que $au + bv = a \wedge b$. Une telle relation est appelée *une relation de Bézout*[†] *de a et b.*

✖ Attention ! ✖

- Il n'y a pas unicité des entiers u et v. Par exemple, $4 \wedge 6 = 2$ et $2 = 4 \times (-1) + 6 \times 1 = 4 \times 2 + 6 \times (-1)$.
- **Péché mortel.** Soit $a, b, d \in \mathbb{Z}$. S'il existe deux entiers $u, v \in \mathbb{Z}$ tels que $au + bv = d$, alors $a \wedge b$ divise d, mais on ne peut certainement pas garantir que $d = a \wedge b$.

Exemple 24 $3080 \wedge 525 = 35 = 7 \times 3080 - 41 \times 525$.

En effet, l'obtention d'une telle relation de Bézout découle de la mise en œuvre de l'algorithme d'Euclide étendu pour laquelle une présentation sous forme de tableau s'avère tout indiquée.

k	r_k	q_k	u_k	v_k
0	3080		1	0
1	525		0	1
2	455	5	1	-5
3	70	1	-1	6
4	35	6	7	-41

$$\begin{aligned} 3080 &= \underset{q_2}{5} \times 525 + \underset{r_2}{455} \\ 525 &= \underset{q_3}{1} \times 455 + \underset{r_3}{70} \\ 455 &= \underset{q_4}{6} \times 70 + \underset{r_4}{35} \\ 70 &= 2 \times 35 + \underset{r_5}{0}. \end{aligned}$$

Théorème 25 – Propriétés du PGCD de deux entiers

Soit a, b, c, k des entiers relatifs.

(i) Associativité. $(a \wedge b) \wedge c = a \wedge (b \wedge c)$. **(ii) Factorisation par un diviseur commun.** $(ka) \wedge (kb) = |k|(a \wedge b)$.

Démonstration.

(i) Le théorème 21 et l'associativité de $\cap$ donnent

$$\mathcal{D}((a \wedge b) \wedge c) = \mathcal{D}(a \wedge b) \cap \mathcal{D}(c) = \mathcal{D}(a) \cap \mathcal{D}(b) \cap \mathcal{D}(c) = \mathcal{D}(a) \cap \mathcal{D}(b \wedge c) = \mathcal{D}(a \wedge (b \wedge c)).$$

(ii) D'une part,

$$|k|(a \wedge b) \in \mathcal{D}(ka) \cap \mathcal{D}(kb) = \mathcal{D}((ka) \wedge (kb)),$$

autrement dit $|k|(a \wedge b)$ divise $(ka) \wedge (kb)$. D'autre part, il existe $u, v \in \mathbb{Z}$ tels que $a \wedge b = au + bv$, d'où

$$k(a \wedge b) = kau + kbv,$$

or $(ka) \wedge (kb)$ divise ka et kb, donc $kau + kbv = k(a \wedge b)$. Ainsi $|k|(a \wedge b)$ et $(ka) \wedge (kb)$ sont associés dans $\mathbb{N}$ et donc égaux. ∎

2.3 PGCD d'une famille finie d'entiers

La notion de PGCD et les propriétés afférentes se généralisent à une famille finie d'entiers relatifs. Dans l'ensemble de ce paragraphe, r désigne un entier supérieur ou égal à 2.

Définition 26 – PGCD d'une famille finie d'entiers

Soit $a_1, \ldots, a_r$ des entiers relatifs dont l'un au moins est non nul. On appelle *plus grand commun diviseur (ou PGCD) de $a_1, \ldots, a_r$*, noté $a_1 \wedge \ldots \wedge a_r$, le plus grand élément (pour l'ordre usuel $\leqslant$) de l'ensemble des diviseurs communs de $a_1, \ldots, a_r$, soit

$$a_1 \wedge \ldots \wedge a_r = \max(\mathcal{D}(a_1) \cap \cdots \cap \mathcal{D}(a_r)).$$

Par ailleurs, par convention, $0 \wedge \ldots \wedge 0 = 0$.

Exemple 27 $28 \wedge 42 \wedge 98 = 14$.

En effet, il suffit de vérifier que $\mathcal{D}(28) \cap \mathcal{D}(42) \cap \mathcal{D}(98) = \mathcal{D}(14)$.

†. Étienne Bézout (1730 à Nemours - 1783 aux Basses-Loges) est un mathématicien français, passé à la postérité pour le théorème de Bachet-Bézout en arithmétique et pour son théorème sur le nombre de points d'intersection de deux courbes algébriques, résultat crucial en géométrie algébrique.

Toutefois, l'associativité du PGCD (théorème 25) nous autorise aussi à ramener le calcul du PGCD d'une famille finie d'entiers à des calculs successifs de PGCD de deux entiers.

Exemple 28 $28\wedge 42\wedge 98 = (28\wedge 42)\wedge 98 = 14\wedge 98 = 14$.

Théorème 29

Soit $a_1,\dots,a_r$ des entiers relatifs.

(i) Les diviseurs communs de $a_1,\dots,a_r$ sont exactement les diviseurs de $a_1\wedge\dots\wedge a_r$, *i.e.*

$$\mathcal{D}(a_1)\cap\dots\cap\mathcal{D}(a_r) = \mathcal{D}(a_1\wedge\dots\wedge a_r).$$

(ii) Pour tout $k\in\mathbb{Z}$, $(ka_1)\wedge\dots\wedge(ka_r) = |k|(a_1\wedge\dots\wedge a_r)$.

(iii) Il existe des entiers relatifs $u_1,\dots,u_r$ tels que $a_1\wedge\dots\wedge a_r = a_1u_1+\dots+a_ru_r$. Une telle relation est appelé UNE *relation de Bézout de* $a_1,\dots,a_r$.

Démonstration. Laissée en exercice (procéder par récurrence sur r). ■

2.4 Entiers premiers entre eux

2.4.1 Définitions

Définition 30 – Entiers premiers entre eux

Deux entiers relatifs a et b sont dit *premiers entre eux* lorsque leurs seuls diviseurs communs sont ±1, *i.e.* $a\wedge b = 1$.

Exemple 31 10 et 21 sont premiers entre eux.

En effet, on a au choix :

- $\mathcal{D}(10) = \{\pm1,\pm2,\pm5,\pm10\}$ et $\mathcal{D}(21) = \{\pm1,\pm3,\pm7,\pm21\}$;
- par l'algorithme d'Euclide : $21\wedge 10 = 10\wedge 1 = 1$.

✖ ATTENTION ! ✖ On veillera à ne pas confondre $a\nmid b$ et $a\wedge b = 1$. Par exemple, $14\nmid 6$, $6\nmid 14$, mais $14\wedge 6 = 2$. Avoir $a\wedge b = 1$ signifie que a et b n'ont aucun diviseur commun hormis ±1, tandis que la relation $a\nmid b$ exclu seulement que a soit parmi les diviseurs de b.

On dispose d'un premier résultat souvent utile en pratique.

Théorème 32

Soit $a,b\in\mathbb{Z}$. Si $d = a\wedge b$, alors il existe deux entiers a' et b' premiers entre eux tels que $a = da'$ et $b = db'$.

Démonstration. Le cas $a = b = 0$ est trivial. Sinon, on a simplement $d = a\wedge b = (da')\wedge(db') = d(a'\wedge b')$ et donc $a'\wedge b' = 1$, puisque $d\neq 0$. ■

Exemple 33 L'équation $x^2 = y^2 + x\wedge y + 2$, d'inconnue $(x,y)\in\mathbb{N}^2$ admet $(2,1)$ et $(2,0)$ pour seules solutions.

Définition 34 – Entiers premiers entre eux dans leur ensemble/deux à deux

- **Dans leur ensemble.** Des entiers $a_1,\dots,a_r$ sont dits *premiers entre eux dans leur ensemble* lorsque leurs seuls diviseurs communs sont ±1, *i.e.* $a_1\wedge\dots\wedge a_r = 1$.
- **Deux à deux.** Des entiers $a_1,\dots,a_r$ sont dits *premiers entre eux deux à deux* lorsque $a_i\wedge a_j = 1$, pour tous $i,j\in[\![1,r]\!]$ distincts.

✖ ATTENTION ! ✖ Premiers entre eux DEUX À DEUX $\Longrightarrow$ Premiers entre eux DANS LEUR ENSEMBLE

mais la réciproque est bien sûr fausse ! Par exemple, 6, 10 et 15 sont premiers entre eux dans leur ensemble, alors que $6\wedge 10 = 2$, $10\wedge 15 = 5$ et $6\wedge 15 = 3$.

2.4.2 Les théorèmes de Bézout et Gauss

Théorème 35 – Théorème de Bézout

Deux entiers a et b sont premiers entre eux si et seulement s'il existe $(u,v)\in\mathbb{Z}^2$ tel que $au+bv=1$.

Démonstration. Le sens direct est une simple relation de Bézout découlant du théorème 23. Pour la réciproque, s'il existe $u,v\in\mathbb{Z}$ tels que $au+bv=1$, alors tout diviseur commun d à a et b divise $au+bv=1$ et vaut donc ±1, d'où $a\wedge b=1$. ■

Corollaire 36

Soit $a,b,a_1,\dots,a_r\in\mathbb{Z}$.

(i) Les entiers $a_1,\dots,a_r$ sont premiers entre eux dans leur ensemble si et seulement s'il existe des entiers relatifs $u_1,\dots,u_r$ tels que $a_1u_1+\dots+a_ru_r=1$.

(ii) Chacun des entiers $a_1,\dots,a_r$ est premier avec b si et seulement si leur produit est premier avec b.

(iii) Si $a\wedge b=1$, alors $a^m\wedge b^n=1$, pour tous $m,n\in\mathbb{N}$.

Démonstration. **(i)** Idem à la preuve précédente, via le point **(iii)** du théorème 29 pour le sens direct.

(ii) Il suffit d'établir, pour trois entiers a,a',b, l'équivalence « $\big(a\wedge b=1 \text{ et } a'\wedge b=1\big) \iff (aa')\wedge b=1$ », le cas général s'obtenant alors par récurrence sur r. Or on dispose des équivalences suivantes

$$\begin{array}{lll} & a\wedge b=1 \text{ et } a'\wedge b=1 & \\ \iff & \exists u,v,u',v'\in\mathbb{Z},\quad 1=au+bv=a'u'+bv' & \text{(th. de Bézout)}\\ \implies & \exists u,v,u',v'\in\mathbb{Z},\quad 1=(au+bv)(a'u'+bv') & \\ \iff & \exists u,v,u',v'\in\mathbb{Z},\quad 1=aa'\times uu'+b\times\big(auv'+a'u'v+bvv'\big) & \\ \iff & (aa')\wedge b=1 & \text{(th. de Bézout).}\end{array}$$

La réciproque est évidente puisque $a\wedge b$ et $a'\wedge b$ sont des diviseurs communs de aa' et b.

(iii) Conséquence du point précédent, par récurrence. ■

Théorème 37 – Théorème (ou Lemme) de Gauss[†]

Soit a,b,c trois entiers relatifs. Si $a\mid bc$ et $a\wedge b=1$, alors $a\mid c$.

Démonstration. D'après le théorème de Bézout, il existe $u,v\in\mathbb{Z}$ tels que $au+bv=1$, ce qui implique $acu+bcv=c$. Or $a\mid bc$, ainsi $a\mid acu+bcv=c$. ■

Corollaire 38

Soit $a,b,m,n,a_1,\dots,a_r\in\mathbb{Z}$.

(i) Division dans une congruence. Si $am\equiv bm\,[n]$ et $m\wedge n=1$, alors $a\equiv b\,[n]$

(ii) Produits d'entiers. Si les entiers $a_1,\dots,a_r$ divisent n et sont premiers entre eux DEUX À DEUX, alors leur produit divise n.

Démonstration. ... ■

✖ ATTENTION ! ✖

(i) L'hypothèse $m\wedge n=1$ est indispensable pour simplifier dans une relation de congruence.
Par exemple, $2\times3\equiv2\times0\,[6]$, mais $3\not\equiv0\,[6]$.

(ii) En général, $\boxed{(a\mid n \text{ et } b\mid n) \not\Longrightarrow ab\mid n.}$ Par exemple, $4\mid12$ et $6\mid12$, mais $24\nmid12$.
Par ailleurs, il est indispensable de supposer les entiers a_i premiers entre eux deux à deux. Par exemple, pour $a_1=6$, $a_2=10$, $a_3=15$ et $n=30$, les entiers a_1,a_2 et a_3 sont seulement premiers dans leur ensemble et leur produit $a_1a_2a_3=900$ ne divise pas n.

†. Johann Carl Friedrich Gauss (1777 à Brunswick – 1855 à Göttingen) est un mathématicien, astronome et physicien allemand, dont la contribution aux mathématiques est extraordinaire.

Exemple 39 Les solutions de l'équation $5x \equiv 2\,[7]$ sont les entiers de la forme $6 + 7\mathbb{Z}$.

Théorème 40 – Forme irréductible d'un rationnel

Tout nombre rationnel s'écrit d'une et une seule manière sous la forme $\frac{p}{q}$ avec $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ et $p \wedge q = 1$, appelée sa *forme irréductible*.

Démonstration. ... ∎

En choisissant p dans $\mathbb{Z}$ et q dans $\mathbb{N}^*$, on impose que le signe de la fraction soit porté par son numérateur. Sans cela, l'unicité de cette forme irréductible ne serait pas garantie.

2.5 Propriétés du PPCM

Nous sommes maintenant en mesure de présenter les propriétés essentielles du PPCM.

Théorème 41 – Propriétés du PPCM

Soit a, b, k des entiers relatifs.

(i) Lien avec le PGCD. $(a \wedge b)(a \vee b) = |ab|$.

(ii) Multiples communs. Les multiples communs de a et b sont les multiples de $a \vee b$, *i.e.* $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.

(iii) Factorisation par un diviseur commun. $(ak) \vee (bk) = |k|(a \vee b)$.

Démonstration. Nous pouvons supposer $a > 0$, $b > 0$, sans perte de généralité (les cas $a = 0$ ou $b = 0$ étant triviaux).

(i) En particulier $a \wedge b \neq 0$ et nous pouvons donc considérer deux entiers $a', b' \in \mathbb{N}$ premiers entre eux tels que $a = (a \wedge b)a'$ et $b = (a \wedge b)b'$. On a alors $\frac{ab}{a \wedge b} = a'b = ab'$ et $\frac{ab}{a \wedge b}$ est donc un multiple commun de a et b. Montrons qu'il s'agit du plus petit. Soit m un multiple commun de a et b, il existe alors $u, v \in \mathbb{Z}$ tel que $m = au = bv$, soit $ua' = vb'$, après division par $a \wedge b \neq 0$. En particulier, $a' \mid vb'$, or $a' \wedge b' = 1$, ainsi, d'après le théorème de Gauss, $a' \mid v$ et il existe donc $n \in \mathbb{Z}$ tel que $v = a'n$. En somme, $m = ba'n$, ainsi $\frac{ab}{a \wedge b} \mid m$, ce qui prouve que $\frac{ab}{a \wedge b}$ minore pour $\leqslant$ l'ensemble des multiples communs strictement positifs de a et b.

(ii) Puisque $a \vee b$ est un multiple commun de a et b, tout multiple de $a \vee b$ est a fortiori un multiple de a et b, autrement dit

$$(a \vee b)\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}.$$

Réciproquement, si $m \in a\mathbb{Z} \cap b\mathbb{Z}$, alors $m \in (a \vee b)\mathbb{Z}$, d'après le point précédent, soit l'inclusion réciproque.

(iii) Supposons aussi, sans perte de généralité $k \neq 0$, alors

$$(ak) \vee (bk) \underset{\text{(i)}}{=} \frac{|ak \times bk|}{(ak) \wedge (bk)} = \frac{|ab| \times |k|^2}{|k|(a \wedge b)} = |k| \frac{|ab|}{a \wedge b} \underset{\text{(i)}}{=} |k|(a \vee b).$$ ∎

Exemple 42 Les multiples communs de 12 et 18 sont les multiples de 36, dans la mesure où $12 \vee 18 = \frac{12 \times 18}{12 \wedge 18} = 36$.

Remarque 43 – Lien avec la relation d'ordre $\mid$ sur $\mathbb{N}$ Soit $a, b \in \mathbb{N}$.
D'après le théorème 3, la relation de divisibilité $\mid$ est une relation d'ordre sur $\mathbb{N}$ (mais pas sur $\mathbb{Z}$!), ainsi dire que « a divise b » signifie que a est plus petit que b au sens de la divisibilité. Par conséquent,

- les diviseurs communs POSITIFS de a et b sont exactement les minorants de la paire $\{a, b\}$ au sens de la divisibilité ;
- les multiples communs POSITIFS de a et b sont exactement les majorants de la paire $\{a, b\}$ au sens de la divisibilité.

Dans ce cadre, les égalités $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a \wedge b)$ et $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$ signifient respectivement que

- $a \wedge b$ est le plus grand élément de $\mathcal{D}(a) \cap \mathcal{D}(b) \cap \mathbb{N}$ au sens de la divisibilté ;
- $a \vee b$ est le plus petit élément de $a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}$ au sens de la divisibilté.

En somme, $a \wedge b$ est le plus grand minorant de $\{a, b\}$ et $a \vee b$ est le plus petit majorant de $\{a, b\}$ au sens de la divisibilité, autrement dit

$$a \wedge b = \inf\{a, b\} \qquad \text{et} \qquad a \vee b = \sup\{a, b\}.$$

Notons que cette interprétation reste valable dans les cas particuliers $(a, b) = (0, 0)$ pour le PGCD et $a = 0$ ou $b = 0$ pour le PPCM, 0 étant le plus grand élément de $\mathbb{N}$ pour la relation de divisibilité.

3 Nombres premiers

3.1 Définition et premières propriétés

Définition 44 – Nombre premier

On appelle *nombre premier* tout entier naturel distinct de 1 et admettant pour seuls diviseurs positifs 1 et lui-même. Un entier naturel est dit *composé* lorsqu'il est distinct de 1 et qu'il n'est pas premier.

Exemple 45 Il est utile de connaître la liste des premiers nombres premiers : $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$

Notation 46 L'ensemble des nombres premiers est souvent noté $\mathbb{P}$ ou $\mathcal{P}$.

Théorème 47 – Premières propriétés

(i) Soit $p \in \mathbb{P}$. Alors p est premier avec un entier si et seulement s'il ne le divise pas. En particulier,

$$\forall k \in [\![1\,, p-1]\!], \quad k \wedge p = 1.$$

(ii) Lemme d'Euclide. Un nombre premier divise un produit si et seulement s'il divise l'un de ses facteurs.

(iii) Tout entier naturel strictement supérieur à 1 admet un diviseur premier.

(iv) Il existe une infinité de nombres premiers.

Démonstration. ... ∎

✖ ATTENTION ! ✖ La primalité de p est indispensable au lemme d'Euclide. Par exemple, $4 \mid 2 \times 2$, mais $4 \nmid 2$.

Exemple 48

- Deux nombres premiers distincts sont premiers entre eux.
- Soit $p \in \mathbb{P}$. Pour tout $k \in [\![1\,, p-1]\!]$, $p \mid \binom{p}{k}$.
- Soit $a, b \in \mathbb{Z}$. Si $a \wedge b = 1$, alors $(a+b) \wedge (ab) = 1$.

Crible d'Ératosthène Le crible d'Ératosthène[†] permet une détermination simple de tous les nombres premiers inférieurs à un seuil donné et repose sur la propriété suivante.

Théorème 49 – Principe à la base du crible d'Ératosthène

Tout entier COMPOSÉ $n \in \mathbb{N}^*$ possède un diviseur premier inférieur ou égal à $\sqrt{n}$.

Démonstration. Soit $n \in \mathbb{N}^*$ un entier composé et notons p le plus petit de ses diviseurs premiers. On a alors $n = pk$ avec $k \in \mathbb{N}^*$. Par ailleurs, tout diviseur premier de k est aussi un diviseur premier de n et est donc supérieur ou égal à p. En particulier $k \geqslant p$ et on a donc $n = pk \geqslant p^2$. ∎

Exemple 50 Nous pouvons en déduire la liste de tous les nombres premiers inférieurs ou égaux à 100. On part d'une liste des entiers de 2 à 100, dont on va peu à peu rayer les entiers composés et dont ne resteront vierges à la fin que les nombres premiers.

†. Ératosthène de Cyrène (≈276 av. J.-C à Cyrène – ≈194 av. J.-C. à Alexandrie) est un astronome, géographe, philosophe et mathématicien grec, considéré comme le plus grand savant du III^{e} siècle av. J.-C. Il invente la discipline de la géographie, dont le terme est encore utilisé aujourd'hui, et sera nommé directeur de la bibliothèque d'Alexandrie par Ptolémée III.

- L'entier 2 est premier, c'est notre point de départ. On raye tous ses multiples hormis lui-même, car ceux-ci sont composés.
- Le premier entier non rayé est alors 3. Il estnécessairement premier car s'il était composé, il aurait un diviseur premier strictement inférieur (ici 2) et on l'aurait déjà rayé. On raye tous les multiples de 3 hormis lui-même, car ceux-ci sont composés.
- Même chose avec 5, puis avec 7. Le premier entier non rayé est alors 11. Or tout entier compris entre 2 et 100 possède un diviseur premier inférieur ou égal à $\sqrt{100} = 10$ Ainsi nous avons déjà rayé tous les entiers composés compris entre 2 et 100. Les entiers non rayés restants sont exactement les nombres premiers de la liste étudiée.

	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

3.2 Valuations p-adiques et décomposition primaire

Définition-théorème 51 – Valuation p-adique

Soit p un nombre premier et n un entier relatif NON NUL. L'ensemble $\left\{k \in \mathbb{N} \,\middle|\, p^k \mid n\right\}$ possède un plus grand élément, appelé la *valuation p-adique de n* et noté $v_p(n)$.

Démonstration. D'une part $p^0 \mid n$. D'autre part, pour tout $k \in \mathbb{N}$, si $p^k \mid n$, alors $k \leqslant p^k \leqslant |n|$. Ainsi $\left\{k \in \mathbb{N} \,\middle|\, p^k \mid n\right\}$ est une partie non vide et majorée de $\mathbb{N}$, elle possède donc un plus grand élément. ■

Pour un entier non nul n et un nombre premier p, la définition même de la valuation p-adique $v_p(n)$ mène aux équivalences fondamentales suivantes :

- $v_p(n) = k \iff \left(p^k \mid n \text{ et } p^{k+1} \nmid n\right) \iff \left(\exists m \in \mathbb{Z},\quad n = p^k m \text{ et } p \nmid m\right)$;
- $v_p(n) \geqslant k \iff p^k \mid n$.

Exemple 52

- Puisque $24 = 2^3 \times 3$, on a $v_2(24) = 3$, $v_3(24) = 1$ et, pour tout $p \in \mathbb{P}\backslash\{2,3\}$, $v_p(24) = 0$.
- Pour tout $n \in \mathbb{Z}^*$, $v_p(n) = v_p(|n|)$, dans la mesure où $\mathcal{D}(n) = \mathcal{D}(|n|)$.

Théorème 53 – Additivité des valuations p-adiques

Soit $p \in \mathbb{P}$. Pour tous $a, b \in \mathbb{Z}^*$, $\quad v_p(ab) = v_p(a) + v_p(b)$.

Démonstration. Par définition, il existe $a', b' \in \mathbb{Z}^*$ non divisibles par p tels que $a = p^{v_p(a)}a'$ et $b = p^{v_p(b)}b'$. Or, p étant premier, ceci équivaut à $p \nmid a'b'$ (lemme d'Euclide). Par ailleurs, $ab = p^{v_p(a)+v_p(b)}a'b'$, d'où l'égalité annoncée. ■

Exemple 54 Pour tous $p, q \in \mathbb{P}$ et $k \in \mathbb{N}$, $\quad v_p\left(q^k\right) = kv_p(q) = \begin{cases} k & \text{si } q = p \\ 0 & \text{sinon.} \end{cases}$

Exemple 55 $\sqrt[5]{\dfrac{4}{3}}$ est irrationnel.

Le théorème suivant énonce que tout entier naturel non nul se décompose de façon unique, à l'ordre près des facteurs, en un produit de nombres premiers. En cela, les nombres premiers peuvent être considérés comme les briques élémentaires dans la construction des entiers en lien avec la multiplication.

Théorème 56 – Décomposition primaire

Pour tout $n \in \mathbb{N}^*$, il existe une unique famille *presque nulle*† $(\alpha_p)_{p\in\mathbb{P}}$ d'entiers naturels telle que $n = \prod_{p\in\mathbb{P}} p^{\alpha_p}$.

En l'occurence, il s'agit de $(v_p(n))_{p\in\mathbb{P}}$ et cette décomposition est appelée la *décomposition primaire de n*.

Démonstration. ... ■

†. Une famille $(a_i)_{i\in I}$ de réels dont tous les éléments, sauf peut être un nombre fini, sont nuls, *i.e.* lorsque $\{i \in I \mid a_i \neq 0\}$ est un ensemble fini, est qualifiée de *presque nulle*.

Remarque 57 Bien qu'indexé par un ensemble infini, le produit $\prod_{p\in\mathbb{P}} p^{v_p(n)}$ apparaissant dans le théorème précédent ne contient qu'un nombre fini de facteurs non triviaux (*i.e.* distincts de 1).

Théorème 58 – Divisibilité, PGCD, PPCM *vs* valuations p-adiques

Soit a, b deux entiers relatifs NON NULS.

(i) a divise b si et seulement si, pour tout $p \in \mathbb{P}$, $v_p(a) \leqslant v_p(b)$.

(ii) $a \wedge b = \prod_{p\in\mathbb{P}} p^{\min\{v_p(a),v_p(b)\}}$ et $a \vee b = \prod_{p\in\mathbb{P}} p^{\max\{v_p(a),v_p(b)\}}$.

Démonstration. ... ■

Exemple 59 $280 \wedge 300 = 20$ et $280 \vee 300 = 4200$.

En effet, $280 = 2^3 \times 5 \times 7$ et $300 = 2^2 \times 3 \times 5^2$, ainsi $280 \wedge 300 = 2^2 \times 5$ et $280 \vee 300 = 2^3 \times 3 \times 5^2 \times 7$.

✎ **En pratique** ✎ L'expression du PPCM de deux entiers indiquée au théorème 58 est celle que l'on met en œuvre pour déterminer le dénominateur commun optimal utilisé pour sommer deux fractions. Par exemple

$$\frac{13}{12} + \frac{7}{30} = \frac{13}{2^2 \times 3} + \frac{7}{2 \times 3 \times 5} = \frac{13 \times 5 + 7 \times 2}{2^2 \times 3 \times 5} = \frac{79}{60}.$$

Remarque 60 Le point **(ii)** du théorème précédent permet de retrouver la formule

$$\forall a, b \in \mathbb{Z}, \quad (a \wedge b)(a \vee b) = |ab|,$$

du théorème 41, dans la mesure où, pour tous $x, y \in \mathbb{R}$, $\min\{x, y\} + \max\{x, y\} = x + y$.

3.3 Petit théorème de Fermat

Théorème 61 – Petit théorème de Fermat[†]

Pour tous $p \in \mathbb{P}$ et $a \in \mathbb{Z}$, $a^p \equiv a\,[p]$. En particulier, si $p \nmid a$, $a^{p-1} \equiv 1\,[p]$.

Démonstration. ... ■

Exemple 62 Pour tout $n \in \mathbb{Z}$, tout diviseur premier impair de $n^2 + 1$ est congru à 1 modulo 4.

Exemple 63 Il existe une infinité de nombres premiers congrus à 1 modulo 4.

Remarque 64

- Plus généralement, le difficile *théorème de la progression arithmétique*, démontré par Dirichlet[‡] en 1838, énonce que pour tout entier non nul n et tout entier m premier à n, il existe une infinité de nombres premiers congrus à m modulo n.
- Le *grand théorème de Fermat* (ou *théorème de Fermat-Wiles*) énonce qu'il n'existe pas de nombres entiers strictement positifs x, y et z tels que $x^n + y^n = z^n$ dès que n est un entier strictement supérieur à 2. Cet énoncé, initialement formulé par Pierre de Fermat en marge d'une traduction des *Arithmétiques* de Diophante, ne sera finalement démontré que trois siècles plus tard par le mathématicien britannique Andrew Wiles en 1994. Bien que d'un intérêt limité, l'acharnement des mathématiciens à en trouver une démonstration aura stimulé la création et le développement de pans entiers de l'édifice mathématique moderne.

†. Pierre de Fermat (160? à Beaumont-de-Lomagne – 1665 à Castres) est un magistrat, polymathe et surtout mathématicien français, surnommé « le prince des amateurs ». On lui doit notamment le principe de Fermat en optique et il contribue dans son échange épistolaire avec Blaise Pascal à élaborer les bases du calcul des probabilités. Sa contribution majeure concerne la théorie des nombres et les équations diophantiennes. Il est notamment connu pour avoir énoncé le dernier théorème de Fermat, dont la démonstration n'a été établie que plus de 300 ans plus tard par le mathématicien britannique Andrew Wiles en 1994.

Compétences à acquérir

- Établir des relations de divisibilité : exercices 1, 2, 4 à 6 et 9.
- Effectuer des calculs modulaires : exercices 2 à 4, 7 et 8.
- Calculer des PGCD (algorithme d'Euclide) : exercices 10 à 13.
- Établir et utiliser que des entiers sont premiers entre eux : exercices 11 et 13 à 17.
- Traiter des questions de primalité : exercices 20 à 28.
- Manipuler les valuations p-adiques : exercices 29 à 37.
- Utiliser la décomposition primaire des entiers : exercices 31, 32 et 38.
- Résoudre des équations diophantiennes : exercices 41 à 49.

Quelques résultats classiques :

- Divisibilité par un facteur premier de coefficients binomiaux (exemple 48).
- Critères de divisibilité (exercice 2).
- Sous-groupes de $\mathbb{Z}$ (exercice 18).
- Intersection de sous-groupes de racines de l'unité (exercice 19).
- La divisibilité des carrés entraîne la divisibilité (exercice 29).
- Puissance d'un PGCD (exercice 31).
- Formule de Legendre pour la valuation p-adique de la factorielle (exercice 33).
- Résolution de l'équation du premier degré modulaire (exercice 43).
- Résolution des équations diophantiennes du premier degré à deux variables (exercice 44).

‡. Johann Peter Gustav Lejeune Dirichlet (1805 à Düren – 1859 à Göttingen) est un mathématicien prussien qui apporta de profondes contributions à la théorie des nombres, en créant le domaine de la théorie analytique des nombres, et à la théorie des séries de Fourier. On lui attribue la définition formelle moderne d'une fonction.