Chapitre X

Entiers relatifs, arithmétique

1.⁻ Divisibilité

On rappelle que $(\mathbb{Z}, +, \times)$ est un anneau commutatif intègre sur lequel l'ordre naturel "$\leq$" est total.

a) Diviseurs, multiples

Définition X.1. Soient $a, b \in \mathbb{Z}$. On dit que a **divise** b si il existe $c \in \mathbb{Z}$ tel que $b = ac$. On dit alors que b est un **multiple** de a.

Notation. On notera $a|b$ si a divise b et on pose $a\mathbb{Z} = \{ak \,|\, k \in \mathbb{Z}\}$ l'ensemble des multiples de a.

✌ **Remarque X.1.**

- Si a divise b et que a et b ne sont pas tous les deux nuls, l'entier relatif c tel que $b = ac$ est unique par intégrité ; on l'appelle **quotient** de b par a et on le note, **si** $a \neq 0$, $\frac{b}{a}$. Cette notation est à utiliser avec parcimonie et à réserver au cas où $a|b$.
- On vérifie aisément que $a|b \iff b\mathbb{Z} \subset a\mathbb{Z}$.
- Pour tout $a \in \mathbb{Z}$, $0 = a \times 0$ et donc $a|0$: **tout le monde divise zéro**. À l'inverse, 0 ne divise que lui–même.

Proposition X.1. La relation "divise" est réflexive et transitive. De plus, si $a, b \in \mathbb{Z}$ alors :

$$(a|b) \wedge (b|a) \Leftrightarrow a = \pm b \,.$$

✌ **Remarque X.2.** Ceci implique que $a\mathbb{Z} = b\mathbb{Z} \Leftrightarrow a = \pm b$.

Démonstration. La réflexivité et la transitivité sont immédiates (*cf.* chapitre V). Il ensuite clair que si $a = \pm b$, alors $a = (\pm 1) \times b$ et donc $a|b$ et $b|a$. Réciproquement, si a et b se divisent mutuellement, il existe c et d dans $\mathbb{Z}$ tels que $b = ac$ et $a = bd$. On a alors $b = bdc$, ce qui entraîne par intégrité que $dc = 1$ et donc $d = c = \pm 1$. □

b) Division euclidienne

Théorème X.2.
Soient $a, b \in \mathbb{Z}$ tels que $b \neq 0$. Alors :

$$\exists!\,(q,r) \in \mathbb{Z}^2,\ \begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}.$$

Vocabulaire. a est appelé **dividende**, b **diviseur**, q **quotient** et r **reste** de la division euclidienne.

Démonstration. Il suffit pour l'existence de remarquer que si on pose $u = \left\lfloor \frac{a}{|b|} \right\rfloor$ on a :

$$|b|u \leq a < |b|(u+1)$$

puis de poser $q = |u|$ et $r = a - |b|u$.

Pour l'unicité, si on suppose qu'il existe deux tels couples (q,r) et (q',r') alors $b(q-q') = r' - r$ et donc $b|r'-r$. Or $r, r' \in [\![0, |b|[\![$, *ergo* $r' - r \in]\!] - |b|, |b|[\![$, ce qui entraîne que $r' - r = 0$. Par conséquent, $q - q' = 0$, d'où le résultat. □

➠ **Exemple X.1.** $15 = 7\times2+1$ est une division euclidienne, mais pas $15 = 7\times3-6$.

Proposition X.3. [Sous–groupes de $\mathbb{Z}$] Soit G un sous–groupe de $(\mathbb{Z}, +)$. Alors il existe un unique $n \in \mathbb{N}$ tel que $G = n\mathbb{Z}$.

Démonstration.

Existence : Considérons l'ensemble $\mathscr{E} = G \cap \mathbb{N}^*$. S'il est vide, alors $G = \{0\} = 0\mathbb{Z}$; dans le cas contraire, il admet par axiome D un plus petit élement n_0. Un sous–groupe étant stable par puissances (ici multiples), on a alors $n_0\mathbb{Z} \subset G$.

Pour montrer l'inclusion réciproque, prenons $a \in G$ et effectuons sa division euclidienne par n_0 (qui est non nul) : par le théorème X.2, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que :

$$\begin{cases} a = n_0 q + r \\ 0 \leq r < |n_0| = n_0 \end{cases}.$$

Le reste vérifie $r = a - n_0 q$ et donc appartient à G comme différence de deux éléments du sous–groupe. Il ne peut donc pas être dans $\mathscr{E}$ et strictement inférieur à n_0, *ergo* $r = 0$ d'où $a \in n_0\mathbb{Z}$.

Unicité : S'il existe deux tels entiers naturels n, n' alors $G = n\mathbb{Z} = n'\mathbb{Z}$ et donc $n = n'$ car $n, n' \geq 0$.

□

2.– PGCD, algorithme d'Euclide

a) Plus Grand Commun Diviseur

Proposition/définition X.2. Soient $a, b \in \mathbb{Z}$ tels que $b \neq 0$. On appelle **plus grand commun diviseur** (PGCD) de a et b la quantité :

$$\max\{\delta \in \mathbb{N}^* \mid (\delta|a) \wedge (\delta|b)\} .$$

Notation. $\text{pgcd}(a, b)$, $a \wedge b$.

Démonstration. L'ensemble $\mathscr{E} = \{\delta \in \mathbb{N}^* \mid (\delta|a) \wedge (\delta|b)\}$ est une partie de $\mathbb{N}$ non vide (elle contient 1) et majorée (brutalement) par $\max(|a|, |b|)$ donc le PGCD est bien défini. □

✌ **Remarque X.3.** On a alors naturellement, pour $a, b \in \mathbb{Z}$, l'égalité $a \wedge b = |a| \wedge |b|$.

➠ **Exemple X.2.**
- $2 \wedge 3 = 1$;
- $2 \wedge (-3) = 1$;
- $(-2) \wedge (-4) = 2$.

✖ **Attention :** le PGCD sera toujours, selon notre définition, un **entier naturel non nul**. D'autres conventions existent dans la littérature ; nous invitons le lecteur à faire preuve de vigilance.

✌ **Remarque X.4.** Si $a, b \in \mathbb{Z}$ et $k \in \mathbb{N}^*$, on vérifie aisément que $(ka) \wedge (kb) = k(a \wedge b)$.

b) Détermination pratique du PGCD

Pour des raisons d'efficacité heuristique, nous utiliserons dans ce paragraphe la notation, pour $a \in \mathbb{Z}$:

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

pour l'ensemble des diviseurs de a. Cet ensemble vérifie clairement que $\mathscr{D}(a) = \mathscr{D}(|a|)$ et, par définition :

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

Remarquons que si $a, b \in \mathbb{Z}$ sont tels que $b \neq 0$ ont pour division euclidienne

$$a = bq + r$$

avec q, r vérifiant les conditions du théorème X.2, alors on peut vérifier rapidement (il s'agit d'un bon exercice pour le lecteur avisé) que :

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

i.e pour tout $k \in \mathbb{Z}$:

$$(k|a) \wedge (k|b) \Leftrightarrow (k|b) \wedge (k|r) .$$

En particulier, cela implique que $a \wedge b = b \wedge r$.

Proposition X.4. Soient $a, b \in \mathbb{Z}$ tels que $b \neq 0$ et soit $\delta \in \mathbb{N}^*$. Alors :

$$\delta = a \wedge b$$

$$\Longleftrightarrow$$

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

✌ **Remarque X.5.** Remarquons que cet énoncé est équivalent au suivant, qui est une caractérisation, très utile en pratique, du PGCD :

$$\delta = a \wedge b$$

$$\Longleftrightarrow$$

$$\begin{cases} (\delta|a) \wedge (\delta|b) \\ \forall d \in \mathbb{Z},\ (d|a) \wedge (d|b) \Rightarrow (d|\delta) \end{cases} .$$

Cela signifie que le PGCD est en fait le "maximum", au sens de la relation "|" (qui n'est pas un ordre) des diviseurs communs à a et b.

Démonstration.

(⇐) Si d est un diviseur strictement positif de a et b alors $d|\delta$ et donc $d|\delta$. Comme δ divise a et b, on a bien $\delta = \max(\mathscr{D}(a) \cap \mathscr{D}(b)) \cap \mathbb{N}^* = a \wedge b$.

(⇒) Démontrons par récurrence forte sur $|b| \in \mathbb{N}^*$ que $\mathscr{D}(a \wedge b) = \mathscr{D}(a) \cap \mathscr{D}(b)$.

— Si $|b| = 1$, alors

$$\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(a) \cap \mathscr{D}(1) = \mathscr{D}(a) = \mathscr{D}(a \wedge 1) \ .$$

— Si la propriété est vraie pour tout $k \leq |b| - 1$, alors, en posant $a = bq + r$ la division euclidienne de a par b, on a :

$$\begin{aligned} \mathscr{D}(a) \cap \mathscr{D}(b) &= \mathscr{D}(b) \cap \mathscr{D}(r) \\ &= \mathscr{D}(b \wedge r) \text{ par hypohtèse de récurrence} \\ &= \mathscr{D}(a \wedge b) \end{aligned}$$

d'où le résultat.

□

◇ Algorithme d'Euclide

Soient $a, b \in \mathbb{Z}$ tels que $b \neq 0$; pour déterminer le PGCD de a et b on définit une suite récurrente $(r_n)_n$ selon le procédé suivant :

— $r_0 = |a|$;
— $r_1 = |b|$;
— pour $n \geq 0$, r_{n+2} sera le reste de la division euclidienne de r_n par r_{n+1} si ce dernier est non nul ; dans le cas contraire on pose $r_{n+2} = 0$.

Proposition X.5. La suite $(r_n)_n$ est décroissante et stationnaire à 0.

Démonstration. La décroissance est claire. Pour le côté stationnaire, commençons par remarquer que si il existe $N \geq 0$ tel que $r_N = 0$ alors $\forall n \geq N$, $r_n = 0$ par construction ; il nous suffit donc de démontrer l'existence d'un tel rang N.

Procédons par l'absurde en supposant que la suite $(r_n)_n$ ne s'annule jamais ; alors on a pour tout $n \geq 0$, $r_n < r_{n+1}$ par division euclidienne ; nous sommes donc en présence d'une suite décroissante d'entiers naturels ; d'après la proposition **??** cette dernière est stationnaire égale à $c \in \mathbb{N}$. Or, si $r_n = r_{n+1} = c \neq 0$ pour $n \geq 0$, $r_{n+2} = 0$, ce qui contredit notre hypothèse. □

Proposition X.6 (Euclide)**.** Posons :

$$N_0 = \min\{N \in \mathbb{N}^* \,|\, r_N = 0\} \,.$$

Alors :

$$a \wedge b = r_{N_0-1} \,.$$

Démonstration. Le minimum de l'énoncé existe par axiome D. D'après nos travaux préliminaires :

$$\begin{aligned} \mathscr{D}(a) \cap \mathscr{D}(b) &= \mathscr{D}(r_0) \cap \mathscr{D}(r_1) \\ &= \mathscr{D}(r_1) \cap \mathscr{D}(r_2) \\ &\vdots \\ &= \mathscr{D}(r_{N_0-1}) \cap \underbrace{\mathscr{D}(0)}_{=\mathbb{Z}} \\ &= \mathscr{D}(r_{N_0-1}) \end{aligned}$$

et donc $r_{N_0-1} = a \wedge b$. □

Cet algorithme peut se retranscrire sans trop de difficulté en langage `python`.

```
def euclide(a,b):
    s=a
    t=b
    while t!=0:
        s,t=t,s%t
    return s
```

➠ **Exemple X.3.** Pour 137 et 12, on passe par les étapes suivantes :
- $137 = 12 \times 11 + 5$;
- $12 = 5 \times 2 + 2$;
- $5 = 2 \times 2 + 1$;
- $2 = 1 \times 2 + 0$.

Ainsi $137 \wedge 12 = 1$.

c) Relation de Bézout

Proposition X.7. Soient $a, b \in \mathbb{Z}$ tels que $b \neq 0$. Alors :

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

✖ **Attention :** : cette proposition n'est pas une équivalence : 4 n'est pas le PGCD de 2 et 3 et pourtant $2 \times 2 + 3 \times 0 = 4$.

Démonstration. Comme $a \wedge b = |a| \wedge |b|$, on peut supposer $a, b \in \mathbb{N}$ sans perte de généralité. La démonstration de ce résultat repose sur l'**algorithme d'Euclide étendu**. Conservons la suite $(r_n)_n$ définie au paragraphe précédent et posons :

— $u_0 = 1$, $u_1 = 0$;
— $v_0 = 0$, $v_1 = 1$.

Démontrons par récurrence double sur $n \in \mathbb{N}$ que :

$$\forall n \in \mathbb{N},\ \exists\, u_n, v_n \in \mathbb{Z},\ au_n + bv_n = r_n\,.$$

— Pour $n = 0, 1$ c'est immédiat.
— Supposons la propriété vérifiée aux rangs n et $n+1$ pour un certain $n \geq 0$. Alors, par définition de la suite $(r_n)_n$ il existe $q \in \mathbb{Z}$ tel que (notons que r_{n+1} peut être nul) :

$$r_n = r_{n+1}q + r_{n+2}$$

et donc :

$$\begin{aligned} r_{n+2} &= r_n - r_{n+1}q \\ &= au_n + b_n - q(au_{n+1} + bv_{n+1}) \text{ par hypothèse de récurrence} \\ &= a(u_n - qu_{n+1}) + b(v_n - qv_{n+1})\,. \end{aligned}$$

Ne reste qu'à poser $u_{n+2} = u_n - qu_{n+1}$ et $v_{n+2} = v_n - qv_{n+1}$.

On conclut la démonstration en appliquant ce résultat à

$$n = \min\{N \in \mathbb{N} \,|\, r_N = 0\} - 1\,.$$

□

➠ **Exemple X.4.** Pour 33 et 21, l'algorithme d'Euclide livre les étapes suivantes :

— $33 = 21 \times 1 + 12$;
— $21 = 12 \times 1 + 9$;
— $12 = 9 \times 1 + 3$;
— $9 = 3 \times 3 + 0$.

En "remontant" ces opérations, on obtient :

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

d) Plus Petit Commun Multiple

Proposition/définition X.3. Soient $a, b \in \mathbb{Z} \setminus \{0\}$; on appelle **plus petit commun multiple** (PPCM) de a et b la quantité :

$$\min((a\mathbb{Z} \cap b\mathbb{Z}) \cap \mathbb{N}^*) \, .$$

Démonstration. Le minimum existe par axiome D. □

Notation. $\text{ppcm}(a, b), a \vee b$.

✌ **Remarque X.6.** Tout comme pour le PGCD, on dispose d'une caractérisation du PPCM ; si $\mu \in \mathbb{N}$ alors :

$$\begin{gathered} \mu = a \vee b \\ \Longleftrightarrow \\ \begin{cases} \mu \in a\mathbb{Z} \cap b\mathbb{Z} \\ \forall m \in \mathbb{Z},\ (m \in a\mathbb{Z} \cap b\mathbb{Z}) \Rightarrow (m \in \mu\mathbb{Z}) \end{cases} \\ \Longleftrightarrow \\ \begin{cases} \mu \geq 0 \\ \mu\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z} \end{cases} . \end{gathered}$$

Proposition X.8. Soient $a, b \in \mathbb{Z}$. Alors :

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

Nous démontrerons ce résultat ultérieurement ; nous le mentionnons cependant à ce stade du cours pour la raison qu'il s'agit de la meilleure façon de déterminer un PPCM en pratique.

✍ **Exercice X.1.** Soient $a, b \in \mathbb{Z}$ tel que $b \neq 0$. Démontrer que :

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

3.⁻ Entiers premiers entre eux

a) C'est quoi ?

Définition X.4. On dit que deux entiers entiers a et b sont **premiers entre eux** si $a \wedge b = 1$.

➠ **Exemple X.5.** 3 et 7 sont premiers entre eux.

Proposition X.9. Soient $a, b \in \mathbb{Z}$ tels que $b \neq 0$; alors $\dfrac{a}{a \wedge b}$ et $\dfrac{b}{a \wedge b}$ sont premiers entre eux.

Démonstration. Immédiat via la caractérisation du PGCD. □

b) Théorème de Bézout

Le théorème qui suit est du à Claude–Gaspard Bachet de Méziriac (français, 1581—1638). Étienne Bézout (français, 1730—1783) a généralisé cet énoncé à des structures plus générales, notamment les anneaux de polynômes (*cf.* chapitre XIV).

Théorème X.10 (Bézout)**.**
Soient $a, b \in \mathbb{Z}$ tels que $b \neq 0$. Alors :

$$a \text{ et } b \text{ sont premiers entre eux}$$

$$\iff$$

$$\exists\, u, v \in \mathbb{Z},\ au + bv = 1\ .$$

Démonstration. ($\Downarrow$) Il s'agit d'un cas particulier de la proposition X.7.

($\Uparrow$) Soit $d \in \mathscr{D}(a) \cap \mathscr{D}(b)$. Alors, comme il existe $u, v \in \mathbb{Z}$ tel que $au + bv = 1$ on a $d|1$. On en déduit que $a \wedge b = 1$.

□

Corollaire X.10.a. Soient $a, b, c \in \mathbb{Z}$ tels que $a \wedge c = b \wedge c = 1$. Alors $ab \wedge c = 1$.

Démonstration. Par théorème de Bézout (X.10), il existe $u, v, s, t \in \mathbb{Z}$ tels que

$$1 = au + cv = bs + ct\,.$$

Ainsi :

$$\begin{aligned} 1 &= au \times 1 + cv \\ &= au(bs + ct) + cv \\ &= abus + c(aut + v) \end{aligned}$$

d'où le résultat, toujours par théorème de Bézout. □

c) Lemme de Gauss

Le résultat qui suit est une généralisation, nommée en l'honneur de Johann Carl Friedrich Gauss (allemand, 1777—1855) d'un lemme apparaissant dans le livre VII des *Éléments* d'Euclide. Par ailleurs, cet énoncé apparaît sous sa forme moderne dans un traité de Jean Prestet (mathématicien et prêtre français, 1648—1690).

Théorème X.11 (Lemme de Gauss)**.**
Soient $a, b, c \in \mathbb{Z}$ tels que :
— a et b sont premiers entre eux ;
— $a|bc$.
Alors $a|c$.

Démonstration. D'après le théorème de Bézout (X.10), il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. De plus, comme $a|bc$, il existe $w \in \mathbb{Z}$ tel que $bc = aw$. Alors :

$$\begin{aligned} c &= c \times 1 \\ &= uac + bvc \\ &= uav + awv \end{aligned}$$

d'où le résultat. □

Corollaire X.11.a. Si a et b sont deux entiers premiers entre eux, alors $a \vee b = |ab|$.

Démonstration. Soit $m \in a\mathbb{Z} \cap b\mathbb{Z}$; alors il existe $g, h \in \mathbb{Z}$ tel que $m = ah = bg$ et donc $b|ah$ ce qui entraîne par lemme de Gauss que $b|h$ et donc $ab|m$. □

Ce corollaire nous permet de démontrer la proposition X.8 ; en effet, on a alors (avec les hypothèse de l'énoncé de cette proposition) :

$$\frac{a}{a \wedge b} \vee \frac{b}{a \wedge b} = \frac{a \vee b}{a \wedge b} = |ab|$$

car $\dfrac{a}{a \wedge b}$ et $\dfrac{b}{a \wedge b}$ sont premiers entre eux.*In fine*, on a bien :

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

Corollaire X.11.b. Soient $a, b, n \in \mathbb{Z}$ tels que $a \wedge b = 1$. Alors :

$$(a|n) \wedge (b|n) \Rightarrow (ab|n) \,.$$

Démonstration. Comme $a \wedge b = 1$, $a \vee b = |ab|$, d'où le résultat. □

◇ Application : équations diophantiennes

Considérons dans ce paragraphe une équation de la forme suivante, pour $a, b, c \in \mathbb{Z}$ fixés tels que $ab \neq 0$ et d'inconnues $x, y \in \mathbb{Z}$:

$$ax + by = c \,. \qquad (\mathbf{E} : \text{X.1})$$

Commençons par poser $\delta = a \wedge b$ et par remarquer que si $\delta \not| c$, alors l'équation ne possède aucune solution. Dans le cas contraire, celle–ci est équivalente à la forme réduite suivante :

$$a'x + b'x = c' \qquad (\mathbf{E} : \text{X.2})$$

avec $a' = \dfrac{a}{\delta}$, $b' = \dfrac{b}{\delta}$ et $c' = \dfrac{c}{\delta}$.

Les entiers a' et b' étant premiers entre eux, l'algorithme d'Euclide étendu nous permet de trouver $u, v \in \mathbb{Z}$ tels que $a'u + b'v = 1$; une solution particulière de (**E** :X.2) est alors le couple

$$(x_0, y_0) = (uc, vc)$$

et

Supposons que nous disposions d'une autre solution $(x, y) \in \mathbb{Z}^2$ de (**E** :X.2) ; on obtient alors par soustraction des égalités $a'x + b'y = c'$ et $a'x_0 + b'y_0 = c'$ que :

$$a'(x - x_0) = b'(y_0 - y)$$

ce qui implique que $a' | b'(y_0 - y)$. Or, $a' \wedge b' = 1$ donc, par lemme de Gauss :

$$a' | y_0 - y$$

et donc il existe $k \in \mathbb{Z}$ tel que :

$$y = y_0 - ka' \ .$$

Revenant à l'égalité précédente on a désormais :

$$a'(x - x_0) = ka'b'$$

et donc, par intégrité :

$$x = x_0 + kb' \ .$$

En conclusion les solutions de (**E** :X.2) sont les éléments de l'ensemble :

$$\mathscr{S}_{\text{red}} = \{(x_0 + kb', y_0 - ka') \,|\, k \in \mathbb{Z}\}$$

et donc les solutions de (**E** :X.1) parcourent cet ensemble, les deux équations étant équivalentes.

Exemple X.6. L'équation $12x + 4y = 8$ est équivalente à $3x + y = 2$. On trouve comme solution particulière le couple $(1, -1)$ et donc les solutions sont les $(1 + k, -1 - 3k)$, pour $k \in \mathbb{Z}$.

◇ Application : forme irréductible d'une fraction rationnelle

Soit $x \in \mathbb{Q}$; alors il existe, par définition, $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tels que $x = \dfrac{p}{q}$. Posons $\delta = p \wedge q$, $p' = \dfrac{p}{\delta}$ et $q' = \dfrac{q}{\delta}$; il est alors trivial que :

$$\frac{p'}{q'} = \frac{p}{q} = x.$$

Nous venons de trouver une écriture de x comme quotient de deux entiers premiers entre eux, le dénominateur étant strictement positif. Une telle écriture s'appelle **forme irréductible de** x et est unique. En effet si $x = \dfrac{a}{b}$ avec $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ tels que $a \wedge b = 1$ alors :

$$p'b = aq'$$

et donc $q' | p'b$, ce qui entraîne par lemme de Gauss que $q' | b$. On montre symétriquement que $b | q'$ et donc, par positivité, $q' = b$ *ergo* $p' = a$.

d) Généralisations diverses

Il est possible de définir le PGCD et le PPCM d'une famille d'entiers $a_1, \dots a_n$ via les formules récursives :

$$\text{pgcd}(a_1, \dots, a_n) = \text{pgcd}(\text{pgcd}(a_1, \dots, a_{n-1}), a_n)$$

et

$$\text{ppcm}(a_1, \dots, a_n) = \text{ppcm}(\text{ppcm}(a_1, \dots, a_{n-1}), a_n) \ .$$

On a alors un analogue de la relation de Bézout, à savoir l'existence d'une famille $(u_1, \dots, u_n) \in \mathbb{Z}^n$ telle que :

$$\sum_{i=1}^{n} u_i a_i = \text{pgcd}(a_1, \dots, a_n) \ .$$

✖ **Attention :** Il convient de différencier les familles d'entiers premiers entre eux deux à deux de celles dont le PGCD "global" est égal à 1 (on parle dans ce cas d'entiers **premiers entre eux dans leur ensemble**).

➠ **Exemple X.7.** Les entiers $2, 3, 4$ sont premiers entre eux dans leur ensemble mais $2 \wedge 4 \neq 1$.

4.⁻ Nombres premiers

a) C'est quoi ?

Définition X.5. Un entier $p \in \mathbb{N}$ est dit **premier** si $p \neq 1$ et

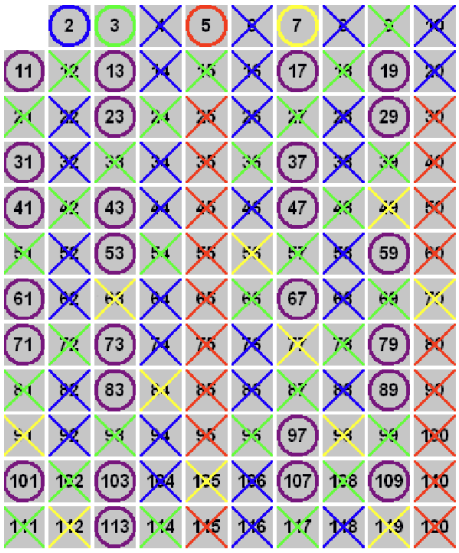
$$\mathscr{D}(p) = \{-1, -p, p, 1\} \ .$$

✖ **Attention :** : avec cette convention, les nombres premiers seront des entiers **naturels**.

➠ **Exemple X.8.** 1 n'est pas premier, 24 non plus ; 3 et 11 sont premiers.

Vocabulaire. Un entier naturel non premier différent de 1 sera dit **composé**.

✌ **Remarque X.7.** Pour dresser une table des premiers nombres premiers (ah ah), on peut utiliser un procédé appellé **crible d'Ératosthène** (grec, 276 av. J.-C. — 194 av. J.-C.) : il s'agit de supprimer d'une table des entiers tous les multiples d'un entier. En supprimant tous les multiples, à la fin il ne restera que les entiers qui ne sont multiples d'aucun entier, et qui sont donc les nombres premiers.



Proposition X.12.

(i) Deux nombres premiers distincts sont premiers entre eux ;

(ii) toute entier naturel supérieur ou égal à 2 admet un diviseur premier.

Démonstration. (i) Immédiat par intersection des ensembles de diviseurs.

(ii) Démontrons par récurrence forte sur $n \in \mathbb{N}$ que :

$$\forall n \in \mathbb{N} \setminus \{0,1\},\ \mathscr{P}(n)\ :\ n \text{ admet un diviseur premier.}$$

— $n = 2$ est divisible par 2, qui est premier.

— Soit $n \in \mathbb{N}$; supposons que $\mathscr{P}(k)$ soit vérifiée pour tout $k \in [\![2, n]\!]$. Si $n+1$ est premier, c'est terminé ; dans le cas contraire, il existe $a, b \in [\![2, n]\!]$ tels que $n + 1 = ab$. Or, par hypothèse de récurrence, a (par exemple) admet un diviseur premier, d'où le résultat.

□

Proposition X.13. Il existe une infinité de nombres premiers.

Démonstration. Supposons qu'il existe un nombre fini et notons les $p_1, \dots p_n$; posons :

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

L'entier p est supérieur ou égal à 2 donc admet un diviseur premier. Or, tous les p_i sont premiers avec p par Bézout, d'où absurdité. □

b) Décomposition en produits de facteurs premiers

Proposition X.14. Soit $a \geq 2$ un entier naturel. Alors, il existe une unique (à l'ordre près) famille de nombres premiers $p_1, \dots, p_n$ et d'exposants associés $\alpha_1, \dots, \alpha_n \in \mathbb{N}^*$ telle que :

$$a = \prod_{k=1}^{n} p_k^{\alpha_k} \ .$$

Démonstration. L'existence se démontre par récurrence forte sur le modèle de l'existence d'un diviseur premier. Pour l'unicité, supposons qu'il existe deux telles familles, *i.e* que a admette pour écritures

$$a = \prod_{k=1}^{n} p_k^{\alpha_k} \quad \text{et} \quad a = \prod_{k=1}^{m} q_k^{\beta_k} \ .$$

Commençons par remarquer que les p_k et q_k sont en fait nécessairement les diviseurs premiers de a et donc $m = n$ et, quitte à les réorganiser, $\forall k \in [\![1, n]\!]$ $p_k = q_k$. De plus, à k fixé on a :

$$p_k^{\alpha_k} | \prod_{j=1}^{n} p_k^{\beta_j}$$

ce qui entraîne par théorème de Gauss (p_k est premiers avec les p_j pour $j \neq k$) que $p_k^{\alpha_k} | p_k^{\beta_k}$ et donc α_k. Il ne nous reste qu'à démontrer symétriquement l'inégalité inverse pour conclure. □

➠ **Exemple X.9.** $12 = 2^2 \times 3$, $15 = 3 \times 5$, $32 = 2^5$.

c) Valuation p–adique

Proposition/définition X.6. Soit $n \in \mathbb{N}^*$ et soit p un nombre premier. On appelle **valuation p–adique de n** l'entier :

$$\nu_p(n) = \max\{k \in \mathbb{N} \,|\, p^k | n\} \ .$$

Démonstration. Le maximum existe par axiome D (la partie est majorée d'après la proposition X.14). □

➠ **Exemple X.10.** $\nu_5(250) = 3$.

✌ **Remarque X.8.**

— Pour $n \in \mathbb{N}$, p premier et $k \geq 0$ on a l'équivalence suivante :

$$\nu_p(n) = k \iff \begin{cases} p^k | n \ ; \\ p^{k+1} \nmid n \ . \end{cases}$$

— La proposition X.14 entraîne l'égalité :

$$n = \prod_{p \text{ premier}} p^{\nu_p(n)} .$$

Notons que ce produit est fini car seul un nombre fini de valuations sont non nulles.

Proposition X.15. Soient $a, b \in \mathbb{N}^*$ et soit p un nombre premier. Alors :

(i) $\nu_p(ab) = \nu_p(a) + \nu_p(b)$;

(ii) $\nu_p(a+b) \geq \min(\nu_p(a), \nu_p(b))$.

Démonstration. Il s'agit d'une conséquence de l'unicité dans la proposition X.14. □

Proposition X.16. Soient $a, b \in \mathbb{N}^*$ et soit p un nombre premier. Alors :

(i) $a|b \Leftrightarrow$ pour tout p premier, $\nu_p(a) \leq \nu_p(b)$;

(ii)
$$a \wedge b = \prod_{p \text{ premier}} p^{\min(\nu_p(a), \nu_p(b))}$$

(iii)
$$a \vee b = \prod_{p \text{ premier}} p^{\max(\nu_p(a), \nu_p(b))} .$$

Démonstration. (i) Immédiat.

(ii) Découle de la caractérisation : si d divise a et b alors pour tout p premier, $\nu_p(d) \leq \nu_p(a)$ et $\nu_p(d) \leq \nu_p(b)$ *ergo* $\nu_p(d) \leq \min(\nu_p(a), \nu_p(b))$ ce qui entraîne que :
$$d | \prod_{p \text{ premier}} p^{\min(\nu_p(a), \nu_p(b))} .$$

(iii) Adapter la démonstration du point précédent.

□

5. Congruences

On fixe dans tout ce paragraphe $n \in \mathbb{N}$.

◇ Rappels (chapitre V)

Soient $a, b \in \mathbb{Z}$. On dit que a **est congru à** b **modulo** n (noté $a \equiv b\,[n]$) si il existe $k \in \mathbb{Z}$ tel que $b = a + kn$. Ceci définit une relation d'équivalence admettant exactement n classes $\bar{0}, \bar{1}, \ldots, \overline{n-1}$.

a) Opérations sur les congruences

Proposition X.17. La relation de congruence modulo n est compatible avec l'addition et la multiplication.

Démonstration. Soient $a, b, a', b' \in \mathbb{Z}$ tels que $a \equiv a'\,[n]$ et $b \equiv b'\,[n]$. Alors il existe $k, h \in \mathbb{Z}$ tels que $a = a' + kn$ et $b = b' + hn$. Ainsi :

$$\begin{aligned} a + b &= a' + b' + n(k + h) \\ &\equiv a' + b'\,[n] \end{aligned}$$

et

$$\begin{aligned} ab =& (a' + kn)(b' + hn) \\ &= a'b' + n(kb' + ha' + kh)n \\ &\equiv a'b'\,[n] \end{aligned}$$

d'où le résultat. □

Remarque X.9.

— Notons que l'on ne peut pas *a priori* inverser dans une congruence. Par exemple, $2 \times 2 \equiv 0\,[4]$.

— Cependant, si $a \in \mathbb{Z}$ est premier avec $n \in \mathbb{N}^*$, le théorème de Bézout (X.10) nous livre l'existence de $u, v \in \mathbb{Z}$ tels que $1 = au + nv$. De fait, on a $au \equiv 1\,[n]$, ce qui signifie que multiplier par u revient à "diviser par a modulo n". Ceci est fort utile pour résoudre des équations mettant en jeu des congruences.

b) Petit théorème de Fermat

Lemme X.1. Soit p un nombre premier et soient $a, b \in \mathbb{Z}$. Alors :

(i) $\forall k \in [\![1, p-1]\!]$, $p | \binom{p}{k}$;

(ii) $(a + b)^p \equiv a^p + b^p\,[p]$.

Démonstration. (i) Soit $k \in [\![1, p-1]\!]$; alors :

$$p! = k!(p-k)!\binom{p}{k}$$

donc $p | k!(p-k)!\binom{p}{k}$. Or, p n'apparaît pas dans le produit $k!(p-k)!$ d'entiers compris entre 1 et $p-1$ donc, comme p est premier, $p \wedge (k!(p-k)!) = 1$ d'où, par lemme de Gauss (théorème X.11) :

$$p | \binom{p}{k}.$$

(ii) Il suffit d'appliquer le binôme de Newton :

$$\begin{aligned}(a+b)^p &= \sum_{k=0}^{p} \binom{p}{k} a^k b^{n-k} \\ &= a^p + b^p + \underbrace{\sum_{k=1}^{p-1} \binom{p}{k} a^k b^{n-k}}_{\text{divisible par } p} \\ &\equiv a^p + b^p \,[p]\ .\end{aligned}$$

□

Le théorème suivant est souvent appelé "petit théorème de Fermat", du nom de Pierre de Fermat (français, ∼1610—1665), qui l'énonce dans une lettre à Bernard Frénicle de Bessy, autre mathématicien français et son contemporain.

Théorème X.18 (Fermat)**.**
Soit p un nombre premier. Alors :

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

Démonstration. Supposons dans un premier temps a positif ; nous pouvons alors démontrer ce résultat par récurrence sur a.

— $a = 0$: immédiat.

— Supposons la propriété vraie au range $a \geq 0$. Alors :

$$\begin{aligned}(a+1)^p &\equiv a^p + 1^p \,[p] \\ &\equiv a + 1\,[p]\end{aligned}$$

d'où le résultat.

Dans le cas négatif, nous devons distinguer deux cas :

— si $p > 2$, alors p est impair et donc

$$\begin{aligned}a^p &= -(-a)^p \\ &\equiv -(-a)\,[p] \\ &\equiv a\,[p]\ ;\end{aligned}$$

— si $p = 2$ alors $-1 \equiv 1\,[2]$ donc $a \equiv -a\,[2]$.

Nous pouvons donc dans les deux cas conclure via le cas $a \geq 0$. □

Corollaire X.18.a. Soit p un nombre premier ; alors :

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

Démonstration. Nous savons par le théorème de Fermat que $p | a^p - a$. Or $a^p - a = a(a^{p-1} - 1)$ et $p \wedge a = 1$ car $a \notin p\mathbb{Z}$ donc, par lemme de Gauss (théorème X.11) :

$$p | a^{p-1} - 1$$

d'où le résultat. □

Ce dernier résultat a été quelques temps utilisé comme test de primalité : si p vérifie la congruence indiquée, on le considérait comme premier. Malheureusement, la réciproque du corollaire est fausse, donc le test est faussé : les faux positifs, appelés nombres de Carmichael (Robert Daniel Carmichael, américain, 1879—1967) comprennent $561, 1105, 1729, 2465, 2821, 6601$ et 8911. Il a été démontré en 1994 par William Alford, Andrew Granville et Carl Pomerance qu'il en existe une infinité.