# Chap. C1 : structure et arithmétique dans $\mathbb{Z}$ (fin)

*The aftermath of Gauss... or the math after Gauss* (P. Ribenboim, My Number My friends).

**Reprise du tout le programme précédent :** *(début du C1) et surtout la partie arithmétique PPCM, PGCD, Euclide.*

## V Nombres premiers

### 1) Propriétés élémentaires

#### a) Définition :

(i) **Terminologie :** soit $a \in \mathbb{Z}^*$. Le nombre $a$ est toujours divisible par $1, -1, a, -a$. Ces diviseurs sont appelés les *diviseurs triviaux* de $a$.

(ii) **Déf. :** un nombre $a \in \mathbb{Z}^*$ est dit *premier* si les deux conditions suivantes sont réalisées :
(C1) le nombre $a$ n'est pas inversible i.e. $a \notin \{-1, 1\}$,
(C2) le nombre $a$ n'admet pas de diviseur non trivial.
Autrement dit $a$ est premier si, et seulement si, il admet exactement quatre diviseurs distincts $1, -1, a, -a$.

(iii) **Scholie :** La déf. du (ii) semble un peu lourde mais il est essentiel, pour la suite de la théorie, de bien mentionner que les inversibles 1 et $-1$ ne sont pas premiers.

La condition (C2) contient beaucoup de négations : il sera plus commode par la suite de la remplacer par la caractérisation ci-dessous des nombres *non premiers*.

Pour formuler cette caractérisation, encore un peu de :

**Terminologie :** On dit qu'un nombre $n$ s'écrit comme un *produit non trivial* $n = ab$ si ni $a$ ni $b$ ne sont inversibles i.e. ni $a$ ni $b$ ne valent $\pm 1$.

A contrario, on dira par exemple que l'écriture $2 = 1 \times 2$ ou $2 = (-1) \times (-2)$ sont des produits triviaux ou des *décompositions triviales* de 2.

**Remarque :** Pour qu'un produit $n = a.b$ soit non trivial il est équivalent de dire que (trois formulations équivalentes) :

$$\begin{cases} |a| \neq 1 \text{ et } |b| \neq 1, \\ |a| \neq |n| \text{ et } |b| \neq |n| \\ 1 < |a| < |n|. \end{cases}$$

(iv) **Caractérisation (working-def. de la primalité, par la négation)**
Soit $n \in \mathbb{Z}^* \setminus \{-1, 1\}$ (on exclut les inversibles). Alors :
$n$ n'est pas premier si, et seulement si, $n$ s'écrit comme un produit non trivial $n = a.b$ avec $1 < |a| < |n|$ (et donc $1 < |b| < |n|$).

*Preuve :* Sens $\Leftarrow$ : si $n$ s'écrit comme un produit non trivial $n = a.b$ alors $a$ et $b$ sont des diviseurs non triviaux de $n$ et donc $n$ n'est pas premier (cf. (C2) du (ii)).

Sens $\Rightarrow$ : si $n$ n'est pas premier, comme la condition (C1) du (ii) est vérifié, c'est que la condition (C2) ne l'est pas, donc il a un diviseur $a$ non trivial, tel que $1 < |a| < |n|$.

Par déf. de la divisibilité, on a donc un $b$ tel que $n = a.b$, avec $1 < |a| < |n|$, donc une écriture de $n$ comme un produit non trivial. □

(v) **Exemples de petits nombres premiers :** $2, 3, 5, 7, 11$ mais aussi $-2, -3, -5, -7, -11$.

**N.B.** Rapidement, on se réduira à considérer les nombres premiers dans $\mathbb{N}$, et on notera (ce n'est pas standard) $\mathbb{P}$ l'ensemble des nombres premiers dans $\mathbb{N}$.

#### b) Divisibilité *par* les nombres premiers , lemme d'Euclide

(i) **Rem. facile mais efficace :** Soit $p \in \mathbb{P}$ un nombre premier. Soit $a \in \mathbb{Z}$ quelconque. On a toujours l'alternative suivante : $\begin{cases} \text{ou bien } & p | a, \\ \text{ou bien } & p \wedge a = 1. \end{cases}$

*Preuve :* Notons $d = p \wedge a$. Comme $p$ est premier et que $d$ est un diviseur positif de $p$, on a deux cas possibles seulement $d = p$ ou $d = 1$, qui donnent les deux cas de l'énoncé. □

L'alternative précédente, alliée à une propriété démontrée à l'aide de Bézout, a la très importante propriété suivante :

(ii) **Prop. (lemme d'Euclide) :** Soit $p \in \mathbb{Z}$ un nombre premier. Soient $(a, b) \in \mathbb{Z}^2$ quelconque tels que $p|(ab)$.
Alors $p|a$ ou $p|b$.
**Généralisation :** Si $p \in \mathbb{P}$ et $p|(a_1 \dots a_n)$ alors $\exists\, i \in [\![1, n]\!]$, $p|a_i$.

Retenir, en français : si un nombre premier divise un produit, il divise un des facteurs.

*Preuve* – On prouve directement la version générale, par contraposée. Par l'alternative du (i), comme $p$ est premier, dire que $p$ ne divise aucun des $a_i$ signifie qu'il est premier avec chacun des $a_i$. Alors par le lemme conséquence de Bézout du IV 7 b), on en déduit que $p$ est premier avec le produit $a_1 \dots a_n$ et donc que $p$ ne divise par $a_1 \dots a_n$. □

### c) Obtention des nombres premiers inférieurs à un $N$ donné : crible d'Eratosthène.

| | 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 |

**d) Prop.** Tout nombre $a \in \mathbb{Z} \smallsetminus \{-1, 1\}$ admet un diviseur premier.

*Démonstration 1 :* par réc. forte, cf. chap. A2.
*Démonstration 2.* en remplaçant la récurrence par l'existence d'un min. pour toute partie non vide de $\mathbb{N}$. Soit $a \in \mathbb{Z} \smallsetminus \{-1, 0, 1\}$. (Le cas de 0 est trivial, tout le monde divise 0).

L'ensemble $\Delta$ des diviseurs de $a$ dans $\mathbb{N} \smallsetminus \{1\}$ est une partie non vide de $\mathbb{N}$ (car elle contient $|a|$), donc admet un plus petit élément qu'on note $p$. Alors $p$ est premier, car si $p$ n'était pas premier, un diviseur positif non trivial de $p$ donnerait un élément de $\Delta$ strictement inférieur à $p$, *contradiction.* □

**e) Théorème d'Euclide :** L'ensemble $\mathbb{P}$ des nombres premiers dans $\mathbb{N}$ est *infini*

*Preuve* (à bien connaître, au patrimoine mondial de l'humanité).
*Par l'absurde*, supposons que $\mathbb{P}$ est fini, de cardinal $n$, et notons $\mathbb{P} = \{p_1, \dots, p_n\}$.
Considérons $A = (p_1 \dots p_n) + 1 \in \mathbb{N}$.
Alors pour tout $i \in [\![1, n]\!]$, on a une relation de Bézout évidente $A - c_i p_i = 1$ où $c_i = p_1 \dots p_{i-1} p_{i+1} \dots p_n$ de sorte que $A \wedge p_i = 1$.
Or, par le d), $A$ doit avoir un diviseur premier $p_{i_0} \in \mathbb{P}$, *contradiction.* □

## 2) Décomposition en facteur premiers : théorème fondamental de l'arithmétique (Gauss)

### a) Théorème d'existence et d'unicité de la D.F.P.

(i) **Théorème** Soit $a \in \mathbb{Z} \smallsetminus \{0, -1, 1\}$. Soit $\mathbb{P}$ l'ensemble des nombres premiers dans $\mathbb{N}$. Alors $a$ s'écrit de manière unique $a = \varepsilon p_1^{\alpha_1} \dots p_r^{\alpha_r}$, où : $\varepsilon \in \{-1, 1\}$ est donné par le signe de $a$, $p_1 < p_2 < \dots < p_r$ sont dans $\mathbb{P}$ et les exposants $\alpha_1, \dots \alpha_r$ sont des entiers *non nuls.*

(ii) **Scholie :** La partie la plus importante de ce théorème est *l'unicité* de la décomposition.

(iii) Preuve (non exigible, mais pas difficile. L'unicité repose de manière essentielle sur le lemme d'Euclide du 1) b) (ii)).)
• Existence : preuve par récurrence forte avec le 1) d).
• Unicité : Supposons que $n \in \mathbb{N}$ ait deux écritures

$$n = \prod_{i=1}^{r} p_i^{\alpha_i} = \prod_{j=1}^{s} q_j^{\beta_j} \quad (*)$$

vérifiant les conditions du théorème.

Alors, pour chaque $j \in [\![1,s]\!]$, $q_j | \left(\prod_{i=1}^{r} p_i^{\alpha_i}\right)$.

Par la prop. fondamentale pour la divisibilité par les nombres premiers (lemme d'Euclide 1) b) (ii)), on en déduit qu'il existe un $i \in [\![1,r]\!]$ tel que $q_j$ divise l'un des $p_i$, et comme ils sont premiers, $q_j = p_i$.

En notant $\mathcal{P} = \{p_1,\dots,p_r\}$ et $\mathcal{Q} = \{q_1,\dots,q_s\}$ ceci montre que $\mathcal{Q} \subset \mathcal{P}$ et par symétrie du raisonnement, on a l'égalité $\mathcal{P} = \mathcal{Q}$ et en particulier $r = s$ et comme les nombres sont ordonnés dans l'ordre croissant $p_i = q_i$ pour tout $i \in [\![1,r]\!]$.

Ainsi $(*)$ devient :

$$n = \prod_{i=1}^{r} p_i^{\alpha_i} = \prod_{i=1}^{r} p_i^{\beta_i} \quad (**)$$

et reste à montrer que pour tout $i = 1,\dots,r$, on a $\alpha_i = \beta_i$.

Or si, *par l'absurde*, pour un $i \in [\![1,r]\!]$ p.ex. $\alpha_i > \beta_i$ alors en simplifiant $(**)$ par $p_i^{\beta_i}$, on obtient que le premier membre contient encore une puissance non triviale de $p_i$ alors que le second non et donc $p_i$ divise le produit $\prod_{j\in[\![1,r]\!]\setminus\{i\}} p_j^{\beta_j}$ et avec le même raisonnement que dans la première partie de la preuve, on en déduit que $p_i$ est égal à l'un des $p_j$ pour $j \neq i$, ce qui est une *contradiction.*

Ceci achève la preuve de l'unicité. □

**b) Définition des valuations $p$-adiques :**

(i) Déf. (ne nécessite pas le thme de D.F.P.) : Soit $n \in \mathbb{Z}^*$ et $p \in \mathbb{P}$. La valuation $p$-adique de $n$, notée $v_p(n)$ est par déf. le plus grand entier $\alpha$ tel que $p^\alpha | n$.

*Existence claire, car $\{a \in \mathbb{N}, p^a | n\}$ contient $0$, donc est non vide, et majoré par $n$ par exemple.*

(ii) Remarque : $v_p(n) = 0$ si, et seulement si, $p$ ne divise pas $n$.

(iii) Caract. (working-def.) $\alpha = v_p(n) \Leftrightarrow n = p^\alpha m$ avec $m \wedge p = 1$.

*Preuve :* Pour $p$ premier, on se souvient que $p$ ne divise pas $m$ équivaut à $p \wedge m = 1$.

(iv) Exemple : pour $n = 2^4 \times 3^6 \times 5$, $v_2(n) = 4$, $v_3(n) = 6$, $v_5(n) = 1$ et les autres $v_p(n)$ sont nulles.

**c) Traduction efficace du théorème de D.F.P. avec les valuations $p$-adiques :**

(i) Réécriture de la décomposition en facteur premier :

Pour $n \in \mathbb{Z}^*$, $n = \varepsilon p_1^{v_{p_1}(n)} \dots p_r^{v_{p_r}(n)}$ où $\varepsilon \in \{-1,1\}$ et $p_1 < p_2 < \dots < p_r$ sont les nombres premiers divisant $n$.
Version plus snob : $n = \varepsilon \prod_{p\in\mathbb{P}} p^{v_p(n)}$.
**N.B.** produit faussement infini, car il n'y a qu'un nombre fini de facteurs différents de 1.

(ii) Conséq. du thme de D.F.P. :

$\forall (m,n) \in \mathbb{Z}^2,\ m|n \Leftrightarrow \forall p \in \mathbb{P},\ v_p(m) \leq v_p(n).$

*Preuve :* Le sens $\Rightarrow$ est évident : si $v_p(m) = \alpha$ on a $m = p^\alpha m_1$ et il existe $k \in \mathbb{Z}$ tel que $n = km$ donc $n = kp^\alpha m_1$.

Le sens $\Leftarrow$ utilise le thme de D.F.P. : on note $k = \varepsilon \prod_{p\in\mathbb{P}} p^{v_p(n)-v_p(m)}$, où $\varepsilon = \mathrm{sgn}(n/m)$.

Comme les $v_p(n) - v_p(m)$ sont tous positifs, on sait que $k \in \mathbb{N}$. En outre $n = km$ par le thme de D.F.P.

La caract. précédente de la divisibilité avec les $v_p$ est très utile pour les exercices .

(iii) Exercice d'application à faire : montrer que $\forall (m,n) \in \mathbb{Z}^2,\ m|n \Leftrightarrow m^2|n^2$.

(iv) Conséq. du (ii), mais aussi, formulation équivalente de l'unicité de la D.F.P. :

$\forall (m,n) \in (\mathbb{Z}^*)^2,\ |m| = |n| \Leftrightarrow \forall p \in \mathbb{P},\ v_p(m) = v_p(n).$

**d) Propriété utile des valuations $p$-adiques :**

$\forall (a,b) \in (\mathbb{Z}^*)^2,\ \forall p \in \mathbb{P},\ v_p(ab) = v_p(a) + v_p(b)$ et $v_p(a+b) \geq \min(v_p(a), v_p(b)).$

**e) Application au P.G.C.D., P.P.C.M. :**

(i) Exemple concret.

(ii) Prop. Soit $(a,b) \in (\mathbb{Z}^*)^2$. Alors
- $d = a \wedge b$ ssi $d > 0$ et $\forall p \in \mathbb{P}$, $v_p(d) = \min(v_p(a), v_p(b))$.
- $m = a \vee b$ ssi $m > 0$ et $\forall p \in \mathbb{P}$, $v_p(m) = \max(v_p(a), v_p(b))$.

*Preuve :* Soit $\delta \in \mathbb{Z}$.

$$\begin{cases} \delta | a, \\ \delta | b \end{cases} \Leftrightarrow \forall p \in \mathbb{P}, \begin{cases} v_p(\delta) \le v_p(a), \\ v_p(\delta) \le v_p(b) \end{cases} \Leftrightarrow \forall p \in \mathbb{P},\ v_p(\delta) \le min(v_p(a), v_p(b))$$

En notant $\delta_m = \prod_{p \in \mathbb{P}} p^{\min(v_p(a), v_p(b))} \in \mathbb{N}^*$, on vient de montrer que, pour tout $\delta \in \mathbb{Z}$, $\begin{cases} \delta | a, \\ \delta | b \end{cases} \Leftrightarrow \delta | \delta_m$ ce qui est exactement la caractérisation du pgcd, i.e. $\delta_m = a \wedge b$. □

(iii) Prop. : Egalité $|ab| = \text{pgcd}(a,b)\,\text{ppcm}(a,b)$.

## VI Application de l'arithmétique aux nombres rationnels et irrationnels

### 1) Ecriture irréductible d'un nombre rationnel

**Prop-déf.** (i) $\forall r \in \mathbb{Q}^*$, $\exists ! (a,b) \in \mathbb{Z}^* \times \mathbb{N}^*$, $r = \dfrac{a}{b}$, et $a \wedge b = 1$. L'écriture $\dfrac{a}{b}$ s'appelle *l'écriture irréductible* de la fraction $r$.
(ii) Mieux si $r = a/b$ est l'écriture irréductible de $r$ alors pour toute autre écriture $r = x/y$ il existe un $k \in \mathbb{Z}$ tel que $x = ka$ et $y = kb$.

**Exemple** L'écriture irréductible de 6/8 est 3/4.

*Preuve de l'existence au (i).* Par déf. des rationnels, si $r \in \mathbb{Q}^*$, on peut l'écrire $r = x/y$ avec $x \in \mathbb{Z}^*$ et $y \in \mathbb{N}^*$. Soit $d = x \wedge y$, et $x = ad$, $y = bd$. Alors on a vu que $a \wedge b = 1$, et en simplifiant $x = a/b$.

*Preuve de la propriété du (ii).* Si on a une écriture $r = x/y = a/b$ avec $a \wedge b = 1$, alors $bx = ay \quad (*)$ donc $a | bx$ et comme $a \wedge b = 1$, par lemme de Gauss, on conclut que $a | x$, donc qu'il existe $k \in \mathbb{Z}$ tel que $x = ka$. Ceci, dans $(*)$, donne à son tour que $y = kb$.

*Preuve de l'unicité au (i).* Avec la prop. du (ii), si on a deux écriture $x = a/b = a'/b'$ avec $a \wedge b = 1$ et $a' \wedge b' = 1$, par (ii), $b | b'$ et $b' | b$ et comme ils sont positifs, $b = b'$, puis on en déduit $a = a'$. □

### 2) Exemples de nombres irrationnels

a) **Exercice fait en Terminale :** Montrer que $\sqrt{2}$ n'est pas un nombre rationnel.

*La preuve vue sans doute en Terminale , qui est celle d'Euclide, éléments Livre X.*
*Par l'absurde* supposons que $\sqrt{2} = \dfrac{m}{n}$ avec $(m,n) \in (\mathbb{N}^*)^2$ *premiers entre eux.*
On en déduit que $m^2 = 2n^2 \quad (*)$ (*Réflexe : toujours se ramener à une égalité dans* $\mathbb{Z}$).
On a alors 2 divise $m^2$.
Montrons que cela entraîne que 2 divise $m$ : *plusieurs justifications possibles*
(i) *Si un nombre premier divise un produit, il divise un des facteurs* (lemme d'Euclide) ici : 2 divise $m^2 = m \times m$ donc divise $m$.
(ii) *Avec la D.F.P.* $v_2(m^2) = 2v_2(m)$, donc si $v_2(m^2) > 0$ alors $v_2(m) > 0$.
Ainsi $m = 2m_1$ ce qui avec $(*)$ entraîne que $2n^2 = 4m_1^2$, donc $2m_1^2 = n^2$ donc $2 | n^2$ et donc de même $2 | n$ et cela entraîne que 2 est un diviseur commun à $m$ et $n$ *contradiction.*

**b) Preuve simplifiée quand on a mieux compris la D.F.P.**

Si on a $\sqrt{2} = \dfrac{m}{n}$ avec $(m,n) \in \mathbb{Z}^2$ alors on a une égalité $m^2 = 2n^2 \quad (*)$ avec $(m,n) \in \mathbb{Z}^2$.
Mais cette égalité est impossible par unicité de la D.F.P. : dans l'équation à gauche la valuation 2-adique est paire, à droite elle est impaire, *contradiction*

**c) Généralisation :** Soit $a \in \mathbb{N}$ qui n'est pas le carré d'un entier. Montrer que $\sqrt{a} \notin \mathbb{Q}$.

Soit $a \in \mathbb{N}$ qui n'est pas le carré d'un autre entier. En terme de D.F.P., cela équivaut à dire qu'il existe un $p \in \mathbb{P}$ tel que $v_p(a)$ est *impaire* (H).
Montrons qu'alors $\sqrt{a} \notin \mathbb{Q}$.
*Par l'absurde*, si on a un couple $(m,n) \in \mathbb{Z}^2$ tel que $\sqrt{a} = m/n$ alors $m^2 = an^2 \quad (*)$.
Considérons alors la valuation $p$-adique des deux membres de $(*)$.

Par $(H)$ celle du membre de droite est impaire alors que celle du membre de gauche est paire. *Contradiction.* □

**VII Retours aux anneaux de congruence :**

**1) Intégrité, inversibilité pour la multiplication, les corps $\mathbb{Z}/p\mathbb{Z}$**

a) (i) Définition : un anneau *commutatif* $(A,+,\times)$ est dit *intègre* si, et seulement si, $\forall\,(a,b)\in A^2,\ a.b=0\Rightarrow a=0$ ou $b=0$.

(ii) Exemple : $(\mathbb{Z},+,\times)$ est *intègre*. Tout corps, tout sous-anneau d'un corps est *intègre*. (*En effet, si $A\subset K$ où $K$ est un corps, et si $ab=0$ avec $a\neq 0$, en multipliant par l'inverse de a qui existe dans $K$, on obtient $b=0$*).

En revanche, $(\mathbb{Z}/6\mathbb{Z},+,\times)$ n'est pas intègre.

b) Thme : $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi il est intègre ssi $n$ est premier (*dém.*).
L'inverse d'un $\bar{k}\in\mathbb{Z}/p\mathbb{Z}$ est obtenu avec le coeff. $u$ d'une identité de Bézout entre $k$ et $p$.

c) Généralisation : pour $n\in\mathbb{N}_{\geq 2}$ quelconque, $\bar{k}\in\mathbb{Z}/n\mathbb{Z}$ est inversible ssi $k\wedge n=1$.

**2) Applications de la structure de corps, d'anneau de $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$**

a) Résolution d'équations du premier degré : $ax+b\equiv c[p]$ : inverser $\bar{a}\in\mathbb{Z}/p\mathbb{Z}$. Exple.
Même pour $n$ non premier, la méthode précédente s'applique dès que $\bar{a}$ inversible dans $\mathbb{Z}/n\mathbb{Z}$.
Exple de $5x+3\equiv 4\ \ [24]$. Cas contraire $6x\ \equiv 0\,[24]$.

b) Recherches de "racines carrées".
(i) Equation du second degré la plus simple : $\bar{x}^2=\bar{a}$ dans $\mathbb{Z}/p\mathbb{Z}$. Exple : équation $x^2=2$ dans $\mathbb{Z}/7\mathbb{Z}$. On regarde la liste de tous les carrés dans $\mathbb{Z}/p\mathbb{Z}$.
(ii) Prop. (*dém.*) Dans tout corps (ou même tout anneau intègre) un nombre a au plus deux "racines carrées", opposées.

c) Equation générale du second degré $ax^2+bx+c=0$.
(i) *Dans tous les corps où $2\neq 0$ (i.e. $2.1_K\neq 0_K$)* : la "forme canonique" ramène au pb de savoir si $\Delta$ est un carré.
Ensuite les formules sont les mêmes une fois trouvé $\delta$ tel que $\delta^2=\Delta$.
(ii) Exple : Equation $x^2-x-1=0$ dans $\mathbb{Z}/11\mathbb{Z}$.
Soit on refait la forme canonique, soit (dans un pb. où on aurait déjà fait le (i)) on applique directement les formules en cherchant une "racine carrée" de $\delta$.

**3) Congruences simultanées : théorème des restes Chinois**

Problème : résolution d'un système $\begin{cases}x\equiv a\,[m]\\ x\equiv b\,[n].\end{cases}$ ou avec davantage de congruences.

a) Premiers exemples "à la main" :
Résoudre le système $\begin{cases}x\equiv 4\ \ [5],\\ x\ \equiv 3\ \ [6]\end{cases}$ .

b) Cas général pour deux congruences :
(i) C.N. $m\wedge n=1$ pour l'existence de solution pour tout $(a,b)\in\mathbb{Z}^2$.
(ii) Récip. Théorème Chinois :
Pour tout couple $(m,n)\in\mathbb{Z}^2$ avec $m\wedge n=1$, et pour tout $(a,b)\in\mathbb{Z}^2$, en notant $S$ $\begin{cases}x\equiv a\,[m]\\ x\equiv b\,[n].\end{cases}$ ,
le système $S$ admet toujours une solution $x_0\in\mathbb{Z}$ et $x$ vérifie $(S)$ ssi $x\equiv x_0\,[mn]$.
(iii) Cas particulier important : pour $m\wedge n=1$, $x\equiv a\,[mn]\Leftrightarrow\begin{cases}x\equiv a\,[m]\\ x\ \equiv a\,[n]\end{cases}$

c) Exemple concret : chercher les $x$ tels que $x\equiv 3\,[7]$ et $x\ \equiv 12\,[20]$.
(i) On peut faire comme au a).
(ii) Avec le théorème Chinois du (b) (ii), on sait que l'ensemble des solutions est de la forme $x_0+140\mathbb{Z}$ car $7\wedge 20=1$.
On trouve l'unique $x_0\in[\![1,140]\!]$ en testant les différents représentants de 12 modulo 20...

**4) Suites de puissances dans $\mathbb{Z}/p\mathbb{Z}$, petit théorème de Fermat**

a) Thm (au programme !) (Fermat) Si $p$ premier, $\forall a \in \mathbb{Z}$, $a^p \equiv a\ [p]$
Corollaire : si $\bar{a} \neq 0$ dans $\mathbb{Z}/p\mathbb{Z}$, $\bar{a}^{p-1} = \bar{1}$.
La suites de $(\bar{a}^k)_{k\in\mathbb{N}}$ est $p-1$-périodique (Très utile en exercice, comparer ex. § III)

b) Un détour par la formule du binôme :
(i) La formule du binôme est valable pour $(a,b) \in A^2$, avec $A$ anneau *commutatif.*
(ii) Une égalité sur les binomiaux : $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$.
Conséquence : si $n \wedge k = 1$ alors $n | \binom{n}{k}$.
Cas particulier $p$ premier : $p | \binom{p}{k}$ pour $k \in [\![1, p-1]\!]$.
(iii) Appl. $(x+y)^p = x^p + y^p$ pour $(x,y) \in (\mathbb{Z}/p\mathbb{Z})^2$.

c) Application : preuve par récurrence du petit thm. de Fermat.

## Appendice : mémento sur les structures groupes-anneaux-corps

**Groupe :** Soit $G$ un ensemble. On dit que $(G, *)$ est un *groupe* ssi

a) $*$ est une l.c.i. de $G$,
b) $*$ est associative,
c) $*$ admet un élément neutre,
d) tout élément de $G$ admet un symétrique pour $*$

**N.B.**Si la loi n'est pas commutative, la vérification pour le neutre et les symétriques consiste en chaque fois en *deux égalités.* Moralité :

**Pour montrer que $(G, *)$ est un groupe abélien** on montre (*dans cet ordre !*)) que :

a) $*$ est une l.c.i. de $G$,
b) $*$ est associative,
c) $*$ est commutative,
d) $*$ admet un élément neutre,
e) tout élément de $G$ admet un symétrique pour $*$.

Une fois montrée la commutativité, la vérification qu'un élément $e$ est neutre est plus commode : on montre que $\forall\, a \in G,\ e * a = a$ (au lieu de ceci *et* $a * e = a$).

De même pour les symétriques.

On rappelle aussi que si la loi est notée + le neutre est noté 0 ou $0_G$ et dans ce cas les symétriques sont notés avec un $-$.

**Sous-groupe, point de vue pratique (Working-def.)**
Soit $(G, *)$ un groupe et $H$ un sous-ensemble de $G$.
Pour montrer que : $H$ est un sous-groupe de $(G, *)$, on montre que :

a) pour tout $(h, h') \in H^2$, $h * h' \in H$,
b) le neutre $e$ de $G$ est dans $H$,
c) pour chaque élément de $H$, son symétrique pour $*$ (qui existe dans $G$) est dans $H$

**Prop. :** Un sous-groupe d'un groupe $(G, *)$ est alors automatiquement un groupe et un sous-groupe d'un groupe abélien est automatiquement abélien.

**Sous-groupe, point de vue conceptuel**
Soit $(G, *)$ un groupe et $H \subset G$. Alors : $H$ est un sous-groupe de $(G, *)$ si, et seulement si, la restriction de $*$ à $H \times H$ fait de $H$ un groupe de même neutre que $G$.

*Détail pour la preuve :* On prend comme déf. de sous-groupe les 3 axiomes donnés à la W-def. précédente.

Le sens $\Rightarrow$ a été vu en cours. Il suffit de savoir que l'associativité, vraie dans $G$, se transmet automatiquement à $H$.

Le sens $\Leftarrow$ : on veut montrer les trois axiomes de la working-def. ci-dessus.

Or on sait que

• $*_{|H\times H}\ :\ H \times H \to H$ autrement dit, on a la propriété (1) de stabilité de $H$ par $*$,
• On a le même neutre par hyp.
• Sachant que le neutre $e$ de $G$ est dans $H$, $b$ est symétrique de $a$ dans $H$ ssi $a * b = b * a = e$, ce qui est la même déf que dans $G$. Le fait que $(H, *)$ soit un groupe donne donc que pour tout $a \in H$, son symétrique $\tilde{a} \in G$ est dans $H$. D'où la prop. (3). □

**Anneau :** Soit $A$ un ensemble muni de deux l.c.i. qu'on note + et ×. On dit que $(A,+,\times)$ est un *anneau* ssi

a) $(A,+)$ est un *groupe abélien*, dont le neutre est noté $0_A$.

b) × est une l.c.i. de $A$ associative avec neutre, ce neutre est noté $1_A$.

c) × est distributive par rapport à + ce qui, dans le cas où × n'est pas commutative, signifie deux égalités :$\forall\ (a,b,c)\in A^3,\ \begin{cases} a\times(b+c) = a\times b + a\times c,\\ (b+c)\times a = b\times a + c\times a.\end{cases}$

**Remarque :** Ainsi + est toujours supposée commutative, alors que × pas forcément, On verra des exemples d'anneaux non commutatifs quand on parlera de matrices.

**Anneau commutatif :** les axiomes précédents et × commutatif.
Cette définition est taillée sur mesure pour :

$(\mathbb{Z},+,\times)$ le seigneur des anneaux commutatifs.

Pour chaque structure, on peut définir une sous-structure :

**Sous-anneaux, point de vue pratique (W-Def) :** Soit $(A,+,\times)$ un anneau et $B\subset A$. On dit que $B$ est un sous-anneau de $(A,+,\times)$ ssi :

a) $B$ est un sous-groupe de $(A,+)$,

b) $B$ est stable par × (ou encore × est une l.c.i. de $B$),

c) $B$ contient l'élément unité $1_A$.

**Prop. :** Si $B$ est un sous-anneau de $(A,+,\times)$ alors $(B,+,\times)$ est un anneau.

*Preuve de la propriété :* Toutes les propriétés qui s'écrivent par des égalités sur les éléments, si elles sont vraies pour tous les éléments de $A$, seront vraies en particulier pour tous les éléments de $B$. Ici, avec la déf. de $B$ sous-anneau, on a automatiquement les prop. suivantes : commutativité et associativité de + dans $B$, associativité de × dans $B$, et distributivité. Ce sont exactement les prop. qui manquaient pour vérifier les axiomes d'anneau pour $B$. □

• Les prop. que l'on doit garder pour vérifier sous-truc (ici sous-anneau) sont les prop. assurant la *stabilité par les lois* et la *présence d'éléments (neutres, symétriques.*
• Celles qui sont automatiques : les prop. vérifiées par tous les éléments...

Comme pour les groupes, on a aussi un autre point de vue pour donner la déf. de sous-anneau

**Sous-anneaux, point de vue conceptuel** Soit $(A,+,\times)$ un anneau et $B\subset A$. On dit que $B$ est un sous-anneau de $(A,+,\times)$ ssi les restrictions de + et × à $B$ font de $B$ un anneau avec les mêmes neutres.

*Preuve :* analogue à celle donnée pour les groupes. □

**Corps :** On dit que $(K,+,\times)$ est un corps ssi

a) $(K,+)$ est un groupe abélien, dont le neutre est noté $0_K$,

b) en notant $K^* := K\smallsetminus\{0_K\}$, $(K^*,\times)$ est un groupe abélien

c) × est distributive par rapport à +.

**Remarque :** Les corps sont des anneaux meilleurs que les autres, car tous les éléments non nuls sont inversibles. Exemples $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$. Notez bien que dans la déf. ci-dessus, on suppose que la multiplication est commutative, ce qui est spécifié dans le programme. On parlera (du coup bizarrement) de *corps non commutatif* si la multiplication n'est pas commutative.

**Sous-corps :** Si $(K,+\times)$ est un corps, et $L\subset K$, on dit que $L$ est un sous-corps de $(K,+,\times)$ ssi

a) $L$ est un sous-groupe de $(K,+)$,

b) $L^* := L\smallsetminus\{0\}$ est un sous-groupe de $(K^*,\times)$.