# CHAPITRE 14
# ARITHMÉTIQUE

⊙ L'**arithmétique** est originellement (avec l'école pythagoricienne) la branche des mathématiques qui étudie les entiers et les rationnels et les propriétés des opérations les reliant. Mais elle s'est étendue à l'étude d'autres objets mathématiques faisant partie d'anneaux comme les entiers de Gauss, les entiers algébriques de certains extensions, les polynômes, etc.... ; elle comprend la **théorie des nombres** qui utilise des méthodes de la **géométrie algébrique**, de l'analyse et de la théorie des groupes.

## PARTIE 14.1 : DIVISIBILITÉ

### 14.1.1 : Division euclidienne

⊙ On a déjà vu l'existence de la **division euclidienne** par récurrence pour des **diviseurs** et **dividendes** positifs mais on peut généraliser en utilisant la partie entière et rajouter l'unicité :

**Théorème 14.1**

**Soit** $(a,b) \in \mathbb{Z}^2$ **avec la condition** $|a| \geqslant 2$**, alors il existe un unique couple** $(q,r) \in \mathbb{Z} \times [\![0; |a|-1]\!]$ **avec** $b = aq + r$ **(**$b$ **est le dividende,** $a$ **le diviseur,** $q$ **le quotient et** $r$ **le reste).**

***EXEMPLE 14.1*** **:** Voyons ce que cela donne en changeant les signes des dividendes et diviseurs :

$$23 = 5 \times 4 + 3 \ ; \ 23 = (-5) \times (-4) + 3 \ ; \ (-23) = 5 \times (-5) + 2 \ ; \ (-23) = (-5) \times 5 + 2.$$

*REMARQUE 14.1 : Il est clair que :* $a|b \iff r = 0$ *(si* $r$ *est le reste de la division de* $b$ *par* $a$*).*

### 14.1.2 : Congruences

**Définition 14.1**

*On rappelle la relation binaire dite de* **congruence***, pour* $(a,b,n) \in \mathbb{Z}^3$*, on pose* $a \equiv b \ [n] \iff n|(b-a)$ *: on dit alors que* $a$ *et* $b$ *sont* **congrus** *modulo* $n$*.*

*REMARQUE 14.2 :* • *On rappelle que si* $(a,b,c,d) \in \mathbb{Z}^2$ *et* $p \in \mathbb{N}$ *on a :*

$(a \equiv b \ [n] \ \text{ et } \ c \equiv d \ [n]) \Longrightarrow (a + c \equiv b + d \ [n] \ \text{ et } \ ac \equiv bd \ [n])$ ; et $(a \equiv b \ [n] \Longrightarrow a^p \equiv b^p \ [n])$.

• *On peut traduire ceci synthétiquement par :* $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ *est un anneau.*

• *Si* $(b,r) \in \mathbb{Z}^2$ *et* $n \geqslant 2$*, on a une caractérisation du reste utilisant les congruences :*

$\big(r$ *est le reste de la division euclidienne de* $b$ *par* $n\big) \iff \big(b \equiv r \ [n]$ *et* $r \in [\![0; n-1]\!]\big)$.

### 14.1.3 : Sous-groupes de $\mathbb{Z}$

**Proposition 14.1**

**Pour** $(a,b) \in \mathbb{Z}^2$**,** $a|b \iff b\mathbb{Z} \subset a\mathbb{Z}$ **(on rappelle que** $a\mathbb{Z} = \{ ak \mid k \in Z \}$**).**

**Théorème 14.2**

**Les seuls sous-groupes de** $\mathbb{Z}$ **sont les** $a\mathbb{Z}$ **avec** $a \in \mathbb{Z}$ **(c'est le sous-groupe engendré par** $a$**).**

Démonstration : Soit $H$ est un sous-groupe de $\mathbb{Z}$ différent de $\{0\} = 0\mathbb{Z}$, on pose $a = \mathrm{Min}(H \cap \mathbb{N}^*)$.

*REMARQUE 14.3 :*

• *Soit deux sous-groupes* $H$ *et* $H'$ *de* $\mathbb{Z}$*, comme il s'agit de traduire l'inclusion sur les sous-groupes de* $\mathbb{Z}$*, on a des outils adaptés que sont l'intersection (*$H \cap H'$ *est un sous-groupe de* $\mathbb{Z}$*) et la somme* $H + H' = \{ h + h' \mid h \in H \text{ et } h' \in H' \} = < H \cup H' >$ *(c'est le sous-groupe engendré par* $H \cup H'$*) et c'est donc le plus petit sous-groupe de* $\mathbb{Z}$ *parmi tous les sous-groupes de* $\mathbb{Z}$ *qui contiennent* $H$ *et* $H'$*.*

• *On peut généraliser le procédé à plusieurs sous-groupes* $H_1, \cdots, H_n$ *de* $\mathbb{Z}$ *:* $\bigcap_{k=1}^{n} H_k$ *est le plus grand sous-groupe de* $\mathbb{Z}$ *à être contenu dans chacun des* $H_k$ *et le plus petit sous-groupe de* $\mathbb{Z}$ *à contenir tous les* $H_k$ *est la somme* $\sum_{k=1}^{n} H_k = \{ h_1 + \cdots + h_n \mid (h_1, \cdots, h_n) \in H_1 \times \cdots \times H_n \}$.

### 14.1.4 : Numération

**Définition 14.2**

*Soit un entier* $a \geqslant 2$ *(la* **base***) et un autre entier* $b \in \mathbb{N}^*$*, alors on appelle* **écriture de** $b$ **en base** $a$ *une expression de* $b$ *sous la forme* $b = \sum_{k=0}^{n} c_k a^k$ *avec* $n \in \mathbb{N}$*,* $(c_0, \cdots, c_n) \in [\![0; a-1]\!]^{n+1}$ *et* $c_n \neq 0$*. Les entiers* $c_0, \cdots, c_n$ *sont appelés les* **chiffres** *de l'écriture de* $b$ *en base* $a$ *:* $b = (c_n \cdots c_0)_a$.

*REMARQUE 14.4 : Traditionnellement bien sûr, on utilise les symboles* $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ *pour les premiers chiffres (les premiers entiers) mais on est bloqués si la base* $a$ *est strictement supérieure à 10 car on n'a pas de chiffre au delà de 9, si par exemple on compte en hexadécimal (base* $a = 16$*) on utilise les chiffres* $A, B, C, D, E, F$ *pour signifier* $10, 11, 12, 13, 14, 15$.

***EXEMPLE 14.2 :***

• $(ABACAB)_{16} = 10 \times 16^5 + 11 \times 16^4 + 10 \times 16^3 + 12 \times 16^2 + 10 \times 16^1 + 11 \times 16^0$.

• Bien sûr, d'après le binôme de NEWTON, si $a > 6$, on a $(a+1)^4 = (14641)_a$.

• De même, si $a \geqslant 2$, l'entier $a^n - 1$ s'écrit $a^n - 1 = (c c \cdots c)_a$ avec $c = a - 1$.

**Théorème 14.3**

**Soit un entier** $a \geqslant 2$**, alors tout entier** $b \in \mathbb{N}^*$ **possède une unique écriture en base** $a$ **:**

$$\forall b \in \mathbb{N}^*,\ \exists! n \in \mathbb{N},\ \exists! (c_0, \cdots, c_n) \in [\![0; a-1]\!]^{n+1},\ b = \sum_{k=0}^{n} c_k a^k \quad \text{avec} \quad c_n \neq 0$$

*REMARQUE 14.5 : Avec ces notations, le nombre de chiffres de l'écriture en base* $a$ *de l'entier* $b$ *est* $n+1$ *avec* $n$ *qui est caractérisé par* $a^n \leqslant b < a^{n+1}$ *donc, en passant au logarithme, le nombre de chiffres de l'écriture en base* $a$ *de* $b$ *est* $\lfloor \log_a(b) \rfloor + 1$*. Le premier entier ayant* $n$ *chiffres est* $a^{n-1} = (10 \cdots 0)_a$.

*REMARQUE 14.6 : Il existe deux algorithmes efficaces pour l'écriture en base* $a$ *d'un entier.*

*On commence par celui qui parle des quotients.*

• *Soit donc* $b \in \mathbb{N}^*$ *un entier et* $a \geqslant 2$ *la base, on commence par chercher l'unique entier* $n$ *tel que* $a^n \leqslant b < a^{n+1}$ *puis on effectue la division de* $b$ *par* $a^n$*,* $x_n = b = c_n a^n + x_{n-1}$*, on continue en effectuant celle de* $x_{n-1}$ *par* $a^{n-1}$*, soit* $x_{n-1} = c_{n-1} a^{n-1} + x_{n-2}$*, etc... ; alors* $b = (c_n \cdots c_0)_a$.

*Il en existe un autre qui ne nécessite pas ce calcul initial et qui parle de restes.*

• *Avec les mêmes notations, on effectue la division euclidienne de* $b$ *par* $a$*,* $x_0 = b = x_1 a + c_0$*, on continue en effectuant celle de* $x_1$ *par* $a$*, soit* $x_1 = x_2 a + c_1$*, etc... ; une fois de plus* $b = (c_n \cdots c_0)_a$.

***EXEMPLE 14.3 :*** On veut écrire $b = 514$ en base 7, on constate que $7^3 = 343 \leqslant 514 < 2401 = 7^4$.

*REMARQUE 14.7 : Pour les besoins de la cryptographie, on a besoin de calculer les puissances d'un entier (le tout modulo un autre) : on se donne en général un élément $x$ d'un ensemble $E$ muni d'une loi de composition associative $*$ et un entier $n$, et on souhaite calculer $x^n$.*

- *Il y a l'algorithme naïf qui consiste à commencer à $x$ et à multiplier $n-1$ fois par $x$ mais c'est un algorithme de complexité linéaire (le calcul de $x^n$ prend $O(n)$ opérations : produit, stockage, ...).*
- *Un algorithme plus efficace est l'algorithme d'exponentiation rapide, on commence par écrire l'entier $n$ en base 2, ce qui se fait d'après ce qui précède en $r$ étapes ($r$ étant le nombre de chiffres de l'écriture de $n$ en base 2). Alors on a $n = (c_{r-1}\cdots c_0)_2$ et $x^n = \left(\left(...\left((x^2 * x^{c_{r-2}})^2 * x^{c_{r-3}}...\right)^2 * x^{c_1}\right)^2 * x^{c_0}\right.$.*

  *On suppose connue la liste $[c_0, \cdots, c_{r-1}]$ des $r$ chiffres et on initialise $y = x$ :*

  *Pour $k$ allant de $r-2$ à 0 par pas de -1*
  *$y := y^2$;*
  *si $c_k = 1$ alors $y := y * x$;*
  *retour.*

  *On constate que la complexité de cet algorithme est en $O(r)$, soit en $O\big(\ln(n)\big)$, ce qui est un gain considérable (et même infini) par rapport à l'algorithme naïf.*

***EXEMPLE 14.4 :*** Comme $26 = (11010)_2$, on a $x^{26} = \Big(\big((x^2 * x)^2\big)^2 * x\Big)^2$ ce qui nécessite beaucoup moins d'opérations que les 26 attendues.

# PARTIE 14.2 : DIVISEURS ET MULTIPLES COMMUNS

## 14.2.1 : Définition des ppcm et pgcd

**Définition 14.3**

*Soit $n \in \mathbb{N}^*$ et $(a_1, \cdots, a_n) \in \mathbb{Z}^n$, on définit le* **plus grand commun diviseur** *(en abrégé* **pgcd***) $d$ de cette famille d'entiers, c'est le générateur positif du sous-groupe $\sum_{k=1}^{n} a_k\mathbb{Z}$. De même et avec ces notations, on définit le* **plus petit commun multiple** *(en abrégé* **ppcm***) $m$ de cette famille, c'est le générateur positif du sous-groupe $\bigcap_{k=1}^{n} a_k\mathbb{Z}$. On note $d = a_1 \wedge \cdots \wedge a_n$ et $m = a_1 \vee \cdots \vee a_n$.*

***EXEMPLE 14.5 :*** Montrer à la main que $5\mathbb{Z} \cap 3\mathbb{Z} = 15\mathbb{Z}$. Ainsi $5 \vee 3 = 15$.

## 14.2.2 : Propriétés des ppcm et pgcd

**Théorème 14.4**

**Avec les notations précédentes et si $p \in \mathbb{Z}$, on a les équivalences pratiques :**
$\big(\forall k \in [\![1;n]\!],\ p|a_k\big) \iff (p|d = a_1 \wedge \cdots \wedge a_n)$ **et** $\big(\forall k \in [\![1;n]\!],\ a_k|p\big) \iff (a_1 \vee \cdots \vee a_n = m|p)$**.**

*REMARQUE 14.8 :*

- *Par conséquent, les noms de ces deux entiers $d$ et $m$ sont justifiés car $d$ est bien le plus grand (au sens de $\leqslant$) parmi tous les diviseurs communs de $a_1, \cdots, a_n$ (et même au sens de $|$) ; de même $m$ est bien le plus petit (au sens de $\leqslant$) parmi les multiples communs des entiers $a_1, \cdots, a_n$.*
- *Il y a un seul cas pour lequel la définition algébrique ne correspond pas exactement avec le sens de "plus grand commun diviseur", et c'est quand $a_1 = \cdots = a_n = 0$ car alors $d = 0$ alors qu'il n'existe pas de plus grand commun diviseur au sens usuel.*

**Proposition 14.2**

**Nous disposons des équivalences suivantes, pour** $(a,b)\in\mathbb{Z}^2$ **:**

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

**De plus, si** $(a,b,c)\in\mathbb{Z}^3$**, on a :** $(ac)\wedge(bc)=|c|\,(a\wedge b)$ **et** $(ac)\vee(bc)=|c|\,(a\vee b)$**.**

DÉMONSTRATION : Ceci découle de la proposition 14.1 et des égalités de sous-groupes qui se vérifient par double inclusion : $ac\,\mathbb{Z}+bc\,\mathbb{Z}=c(a\,\mathbb{Z}+b\,\mathbb{Z})$ et $(ac\,\mathbb{Z})\cap(bc\,\mathbb{Z})=c(a\,\mathbb{Z}\cap b\,\mathbb{Z})$.

*REMARQUE 14.9 : Si* $(a,b,c)\in\mathbb{Z}^3$*, on a clairement* $a\,\mathbb{Z}+b\,\mathbb{Z}=b\,\mathbb{Z}+a\,\mathbb{Z}$ *et* $a\,\mathbb{Z}\cap b\,\mathbb{Z}=b\,\mathbb{Z}\cap a\,\mathbb{Z}$*, et même* $(a\,\mathbb{Z}+b\,\mathbb{Z})+c\,\mathbb{Z}=a\,\mathbb{Z}+(b\,\mathbb{Z}+c\,\mathbb{Z})$ *et* $(a\,\mathbb{Z}\cap b\,\mathbb{Z})\cap c\,\mathbb{Z}=a\,\mathbb{Z}\cap(b\,\mathbb{Z}\cap c\,\mathbb{Z})$ *ce qui justifie l'associativité et la commutativité des lois internes (à* $\mathbb{Z}$*)* $\wedge$ *et* $\vee$*.*

### 14.2.3 : Algorithme d'EUCLIDE

**Proposition 14.3**

**Si** $(a,b)\in\mathbb{Z}^2$ **et si on a** $b=aq+r$ **alors** $b\wedge a=a\wedge r$**.**

*REMARQUE 14.10 : L'algorithme consiste donc, à partir d'un couple* $(a,b)\in\mathbb{N}^2$ *tel que* $b>a$*, à poser* $a_0=b$ *et* $a_1=a$ *et à effectuer successivement les divisions euclidiennes :* $a_0=a_1q_0+a_2$*,* $a_1=a_2q_1+a_3$*, etc... Il est clair que l'on a* $a_0>a_1>a_2>\cdots$ *de sorte que, puisque l'on a affaire à des entiers naturels, il existe un indice* $r$ *tel que* $a_r=0$*. Ensuite, il suffit d'écrire* $a\wedge b=a_0\wedge a_1=\cdots=a_{r-1}\wedge a_r=a_{r-1}$ *donc le pgcd de* $a$ *et* $b$ *est le dernier reste non nul dans l'algorithme d'*EUCLIDE*.*

***EXEMPLE 14.6 :*** $105=1\times66+39$ ; $66=1\times39+27$ ; $39=1\times27+12$ ; $27=2\times12+3$ ; $12=4\times3+0$ donc $105\wedge66=3$.

*REMARQUE 14.11 : Supposons toujours que* $b>a$*, comme les quotients* $q_0,\cdots,q_{r-2}$ *et* $a_{r-1}$ *sont supérieurs ou égaux à 1, on a* $a_{r-2}\geqslant1$ *et par une récurrence simple,* $a_0\geqslant F_{r-1}\underset{\infty}{\sim}\dfrac{\omega^r}{\sqrt{5}}$ *(terme de la suite de* FIBONACCI *avec* $\omega$ *le nombre d'or). Alors le nombre d'opérations est* $O\left(\dfrac{\ln(b)}{\ln(\omega)}\right)$*, il est donc dominé par le nombre de chiffres de* $b$ *en base* $10$ *(par exemple).*

## PARTIE 14.3 : ENTIERS PREMIERS ENTRE EUX

### 14.3.1 : Définition et propriétés

**Définition 14.4**

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

***EXEMPLE 14.7 :*** Si $a\in\mathbb{Z}$, on a $a$ et $a+1$ qui sont premiers entre eux.

**Proposition 14.4**

**Soit** $(a,b)\in\mathbb{Z}^2$**, et** $d\in\mathbb{N}^*$**, alors on a l'équivalence :**

$$d=a\wedge b \iff \big(\exists(a',b')\in\mathbb{Z}^2,\ a=da',\ b=db' \text{ et } a'\wedge b'=1\big).$$

*REMARQUE 14.12 : On a donc l'existence de l'écriture d'un rationnel sous forme irréductible en simplifiant par le pgcd du numérateur et du dénominateur.*

**Proposition 14.5**

**Soit** $a$**,** $b$ **et** $c$ **trois entiers :** $\big(a\wedge b=1 \text{ et } c|b\big) \implies a\wedge c=1$**.**

### 14.3.2 : Théorèmes de Bézout et Gauss

*REMARQUE 14.13 : Voici enfin ce fameux théorème du à* Bachet de Méziriac *(Claude-Gaspard* Bachet *dit* de Méziriac *: mathématicien, poète et traducteur français* 1581-1638*) mais qui porte bizarrement le nom de* Bézout *(Étienne* Bézout *: mathématicien français* 1730-1783*) :*

**Théorème 14.5**

**Soit** $(a,b) \in \mathbb{Z}^2$**, alors on a l'équivalence :** $a \wedge b = 1 \iff \exists (u,v) \in \mathbb{Z}^2,\ au + bv = 1$**.**

*REMARQUE 14.14 : Soit* $(a,b) \in \mathbb{Z}^2$ *et* $d \in \mathbb{N}$*, alors on a en général juste une implication qui ressemble au théorème de* Bézout *:* $a \wedge b = d \implies \exists (u,v) \in \mathbb{Z}^2,\ au + bv = d$.

*REMARQUE 14.15 : En pratique on utilise l'algorithme d'*Euclide *en remontant les calculs pour trouver des coefficients de* Bézout *(*$u$ *et* $v$*) mais il y a un algorithme général (*Euclide *étendu).*

***EXEMPLE 14.8 :*** Si on se donne $a = 27$ et $b = 16$ alors $27 = 1 \times 16 + 11$, $16 = 1 \times 11 + 5$, $11 = 2 \times 5 + 1$ et $5 = 5 \times 1 + 0$ ce qui fait que $a$ et $b$ sont premiers entre eux et on part de la relation $1 = 11 - 2 \times 5 = 11 - 2 \times (16 - 11) = 3 \times 11 - 2 \times 16 = 3 \times (27 - 16) - 2 \times 16 = 3 \times 27 - 5 \times 16$ pour avoir les coefficients de Bézout $u = 3$ et $v = -5$.

*REMARQUE 14.16 : On peut généraliser à plusieurs entiers le théorème de* Bézout*, si* $(a_1, \cdots, a_n) \in \mathbb{Z}^n$ *est une famille d'entiers* **premiers entre eux dans leur ensemble***, c'est-à-dire* $a_1 \wedge \cdots \wedge a_n = 1$*, alors il existe une famille* $(u_1, \cdots, u_n) \in \mathbb{Z}^n$ *telle que* $u_1 a_1 + \cdots + u_n a_n = 1$ *(car* $1 \in a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$*).*

**Théorème 14.6**

**Soit** $(a,b,c) \in \mathbb{Z}^3$**, on a :** $\big(a|bc$ **et** $a \wedge b = 1\big) \implies a|c$ **(théorème de** Gauss**).**

*REMARQUE 14.17 : Ceci nous permet d'établir l'unicité de l'écriture d'un rationnel sous la forme* $\frac{p}{q}$ *avec les contraintes* $p \in \mathbb{Z}$*,* $q \in \mathbb{N}^*$ *et* $p \wedge q = 1$.

**Proposition 14.6**

**Soit** $a$ **et** $b$ **deux entiers tels que** $a \geqslant 2$**,** $b \geqslant 2$ **et** $a$ **et** $b$ **premiers entre eux, alors il existe un unique couple** $(u,v) \in [\![1; b-1]\!] \times [\![1; a-1]\!],\ au - bv = 1$**.**

*REMARQUE 14.18 : Comme dans l'exemple 14.4, c'est ce couple* $(u,v)$ *qu'on obtient (ou celui qui vérifie* $(u',v') \in [\![1; b-1]\!] \times [\![1; a-1]\!],\ bv' - au' = 1$*) par l'algorithme d'*Euclide.

*REMARQUE 14.19 : Soit* $(a,b,c) \in \mathbb{Z}^3$*, on se donne l'équation diophantienne (c'est-à-dire qu'on en cherche les solutions entières)* $(E)$ *:* $ax + by = c$*. On a alors deux cas, en posant* $d = a \wedge b$ *:*

- *Si* $d \not| c$ *alors* $(E)$ *n'admet aucune solution.*
- *Si* $d|c$ *alors en posant* $a = da'$*,* $b = db'$ *et* $c = dc'$*, on a* $a' \wedge b' = 1$ *et* $(E)$ *:* $a'x + b'y = c'$*, donc on peut ramener la resolution de* $(E)$ *au cas où les entiers* $a$ *et* $b$ *sont premiers entre eux.*

*On suppose donc maintenant que* $a \wedge b = 1$ *de sorte qu'il existe* $(u,v) \in \mathbb{Z}^2$ *tel que* $au + bv = 1$*. On montre alors que les solutions de* $(E)$ *sont les couples* $(kb + uc, -ka + vc)$ *où* $k$ *parcourt* $\mathbb{Z}$*.*

*REMARQUE 14.20 : Soit* $(E)$ *:* $a_n x^n + \cdots + a_0 = 0$ *une équation polynomiale de degré* $n$ *à coefficients entiers. On montre facilement avec le théorème de* Gauss *que si un rationnel* $\frac{p}{q}$ *est une solution de* $(E)$ *(avec* $p$ *et* $q$ *premiers entre eux), alors* $q|a_n$ *et* $p|a_0$*. Ceci nous fournit un nombre fini de rationnels parmi lesquels chercher des solutions rationnelles de* $(E)$*.*

***EXEMPLE 14.9 :*** Soit $(E)$ : $x^5 + x + 1 = 0$, si $(E)$ admet une solution rationnelle, elle ne peut être que $\pm 1$ d'après la remarque 14.20 ce qui n'est pas le cas. Ainsi $(E)$ n'admet pas de solution rationnelle.

### 14.3.3 : Propriétés arithmétiques

**Proposition 14.7**

**Soit $p \in \mathbb{Z}$, $n \in \mathbb{N}^*$ et $(a_1, \cdots, a_n)$ une famille d'entiers, alors on a l'équivalence :**
$$\big(\forall k \in [\![1;n]\!],\ p \wedge a_k = 1\big) \iff p \wedge \Big(\prod_{k=1}^{n} a_k\Big) = 1\,.$$

**Proposition 14.8**

**Soit $(a,b) \in \mathbb{Z}^2$ et $(n,m) \in (\mathbb{N}^*)^2$, alors : $a \wedge b = 1 \iff a^n \wedge b^m = 1$.**

**Proposition 14.9**

**Soit $p \in \mathbb{Z}$, $n \in \mathbb{N}^*$ et $(a_1, \cdots, a_n)$ une famille d'entiers premiers entre eux deux à deux, alors on a l'équivalence : $\big(\forall k \in [\![1;n]\!],\ a_k | p\big) \iff \prod_{k=1}^{n} a_k \Big| p$.**

*REMARQUE 14.21 : Cette proposition est intéressante pour l'utilisation des critères de divisibilité car, par exemple, un entier est un multiple de 6 si et seulement si c'est un multiple de 2 et de 3.*

**Proposition 14.10**

**Soit $n \in \mathbb{N}^*$ et $a_1, \cdots, a_n$ des entiers premiers entre eux deux à deux : $a_1 \vee \cdots \vee a_n = \Big|\prod_{k=1}^{n} a_k\Big|$.**

**Proposition 14.11**

**Soit $(a,b) \in \mathbb{Z}^2$ alors : $(a \wedge b) \times (a \vee b) = |ab|$.**

DÉMONSTRATION : C'est évident si $a = b = 0$. Sinon, on pose $d = a \wedge b > 0$ et $a = da'$, $b = db'$, on sait qu'alors $a' \wedge b' = 1$ donc, d'après la proposition précédente : $a' \vee b' = |a'b'|$. C'est bon.

## PARTIE 14.4 : NOMBRES PREMIERS

### 14.4.1 : Définition et propriétés

**Définition 14.5**

*Soit $p \in \mathbb{N}^*$, on dit que $p$ est un* **nombre premier** *s'il a exactement 2 diviseurs positifs ou, ce qui est équivalent, 4 diviseurs entiers relatifs. On note $\mathcal{P}$ l'ensemble de tous les nombres premiers ($1 \notin \mathcal{P}$).*

**Proposition 14.12**

**Soit $p \in \mathbb{N}^*$ un nombre premier et $a \in \mathbb{Z}$, alors $\big(p|a$ ou $p \wedge a = 1\big)$.**

**Proposition 14.13**

**Soit $p \in \mathbb{N}^*$ premier, $n \in \mathbb{N}^*$ et $(a_1, \cdots, a_n)$ une famille d'entiers, alors on a la nouvelle équivalence : $p \Big| \prod_{k=1}^{n} a_k \iff (\exists k \in [\![1;n]\!],\ p|a_k\big)$**

DÉMONSTRATION : Dans le sens direct, si $\forall k \in [\![1;n]\!]$, non$(p|a_k)$ alors d'après la proposition 14.13, on a $p \wedge a_k = 1$ et on utilise la proposition 14.8. L'autre sens est évident.

### 14.4.2 : Décomposition primaire

**Théorème 14.7**

**Soit $n \geqslant 2$, alors il existe une unique décomposition de $n$ en produit de nombres premiers :** $\exists! r \in \mathbb{N}^*,\ \exists!(p_1, \cdots, p_r) \in \mathcal{P}^r$ **(distincts deux à deux),** $\exists!(\alpha_1, \cdots, \alpha_r) \in (\mathbb{N}^*)^r,\ n = \prod_{k=1}^{r} p_k^{\alpha_k}$.

*REMARQUE 14.22 :* • *L'ensemble $\mathcal{P}$ est infini : on en a déjà vu une démonstration d'*Euclide.

• *On peut déterminer tous les nombres premiers $p \leqslant n$ ($n$ fixé) grâce au* **crible** *d'*Eratosthène *(*Eratosthène *: astronome, géographe, philosophe et mathématicien grec 276 av. J.-C. - 194 av. J.-C.) car si $m \in [\![2; n]\!]$ n'est pas premier, alors il existe un nombre premier $p \leqslant \sqrt{n}$ tel que $p|m$.*

### 14.4.3 : Valuation et rapport avec la divisibilité

**Définition 14.6**

*Soit $p$ un nombre premier et $n \in \mathbb{Z}^*$, on note $\nu_p(n)$ l'unique entier naturel intervenant dans l'écriture de $|n|$ en produit de facteurs premiers comme exposant de $p$. On appelle $\nu_p(n)$ la* **valuation $p$-adique** *de $n$.*

***EXEMPLE 14.10 :*** $\nu_2(120) = 3$, $\nu_3(120) = \nu_5(120) = 1$ et $\forall p \in \mathcal{P},\ p > 5 \Longrightarrow \nu_p(120) = 0$.

*REMARQUE 14.23 :* • *On pourrait la définir par : $\nu_p(n) = \mathrm{Max}(k \in \mathbb{N} \mid p^k | n)$ ce qui impose $n \neq 0$.*

• *Il est clair que $p|n$ si et seulement si $\nu_p(n) > 0$. Comme les diviseurs premiers d'un entier sont inférieurs ou égaux à sa valeur absolue, il ne peut en exister qu'un nombre fini donc la famille $\big(\nu_p(n)\big)_{p \in \mathcal{P}}$ est une famille à support fini (elle ne contient qu'un nombre fini de termes non nuls).*

• *Grâce à cette remarque, on peut justifier l'écriture $n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$ pour tous les entiers $n \in \mathbb{N}^*$ et même l'écriture $n = \mathrm{sgn}(n) \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$ pour tous les entiers $n \in \mathbb{Z}^*$.*

**Proposition 14.14**

**Soit $p$ un nombre premier et $(n, m) \in (\mathbb{Z}^*)^2$ : $\nu_p(nm) = \nu_p(n) + \nu_p(m)$.**

**Proposition 14.15**

**Soit $(n, m) \in (\mathbb{Z}^*)^2$, on a :** $n|m \iff \big(\forall p \in \mathcal{P},\ \nu_p(n) \leqslant \nu_p(m)\big)$.

*REMARQUE 14.24 : Cela marche moins bien avec la somme mais on a tout de même un renseignement exploitable, avec les mêmes notations :* $\nu_p(n+m) \geqslant \mathrm{Min}\big(\nu_p(n), \nu_p(m)\big)$.

**Proposition 14.16**

**Soit $(n, m) \in (\mathbb{Z}^*)^2$, on a les formules classiques :**

$$n \wedge m = \prod_{p \in \mathcal{P}} p^{\mathrm{Min}(\nu_p(n), \nu_p(m))} \quad \text{et} \quad n \vee m = \prod_{p \in \mathcal{P}} p^{\mathrm{Max}(\nu_p(n), \nu_p(m))}.$$

*REMARQUE 14.25 :*

• *Bien sûr, ces formules de calcul du pgcd ou du ppcm à l'aide de la décomposition primaire des entiers se généralisent à plusieurs entiers.*

• *Grâce à deux formules et comme les fonctions $\mathrm{Min}$ et $\mathrm{Max}$ sont distributives l'une par rapport à l'autre, on en déduit que le $\wedge$ est distributif par rapport à $\vee$ et vice-versa.*

• *On retrouve aussi la formule de la proposition 14.12 grâce à ces deux dernières relations.*

***EXEMPLE 14.11 :*** Comme on a les décompositions $360 = 2^3 \times 3^2 \times 5^1$ et $1350 = 2^1 \times 3^3 \times 5^2$, on a $360 \wedge 1350 = 2^1 \times 3^2 \times 5^1 = 90$ et $360 \vee 1350 = 2^3 \times 3^3 \times 5^2 = 5400$.

*REMARQUE 14.26 : Pour un nombre premier $p$, on peut prolonger la fonction $\nu_p$ à $\mathbb{Q}^*$ en posant $\nu_p : \mathbb{Q}^* \to \mathbb{Z}$ définie par : $\forall (a,b) \in \mathbb{Z}^* \times \mathbb{N}^*,\ \nu_p\left(\frac{a}{b}\right) = \nu_p(a) - \nu_p(b)$. On vérifie tout d'abord grâce à la proposition 14.15 que cette fonction est bien définie, qu'elle prolonge bien celle déjà vue sur $\mathbb{Z}^*$ (car $\nu_p(1) = 0$). On vérifie encore à l'aide de 14.15 cette nouvelle fonction est maintenant un morphisme de groupes de $(\mathbb{Q}^*, \times)$ dans $(\mathbb{Z}, +)$ et qu'on a : $\forall r \in \mathbb{Q}_+^*,\ r = \prod_{p \in \mathcal{P}} p^{\nu_p(r)}$.*

# PARTIE 14.5 : ANNEXE (HP)

⊙ Pour la cryptographie, les tests de primalité et les algorithmes de factorisation, quelques connaissances en plus sur les anneaux de congruences $\mathbb{Z}/n\mathbb{Z}$ (pour des entiers $n \geqslant 2$) ne sont pas de refus.

*REMARQUE 14.27 : Bien sûr si $n$ n'est pas premier alors $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre donc pas un corps. De plus, on montre assez facilement avec le théorème de* Bézout *que, pour un entier $k \in \mathbb{Z}$, on a l'équivalence bien pratique : $\overline{k}$ inversible dans $\mathbb{Z}/n\mathbb{Z} \iff k \wedge n = 1$. Ceci amène naturellement :*

**Théorème 14.8**

**$\mathbb{Z}/n\mathbb{Z}$ est un corps $\iff$ $n$ est premier.**

*REMARQUE 14.28 : Dans le cas où $n \geqslant 2$ n'est pas premier mais $k \in [\![2; n-1]\!]$ est premier avec $n$, l'algorithme d'*Euclide *étendu permet de trouver $(u,v) \in [\![1; n-1]\!] \times [\![1; k-1]\!]$, $ku - nv = 1$ ce qui se traduit en termes de congruences par $ku \equiv 1\ [n]$ et donc à $\overline{k} \times \overline{u} = \overline{1}$ dans $\mathbb{Z}/n\mathbb{Z}$ donc cela nous permet de calculer l'inverse de $\overline{k}$.*

***EXEMPLE 14.12 :*** D'après l'exemple 14.8, comme $3 \times 27 - 5 \times 16 = 1$, on a $\overline{16}^{-1} = \overline{-5} = \overline{22}$ dans $\mathbb{Z}/27\mathbb{Z}$ qui n'est pas un corps.

**Définition 14.7**

*Soit $n \in \mathbb{N}^*$, on note $\varphi(n)$ le cardinal du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ des inversibles dans l'anneau $\mathbb{Z}/n\mathbb{Z}$. La fonction $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ est appelée l'***indicatrice d'Euler***.*

*REMARQUE 14.29 : Pour un entier $n \in \mathbb{N}^*$, $\varphi(n)$ est donc aussi le nombre d'entiers $k \in [\![1; n-1]\!]$ qui sont premiers avec $n$ grâce à la remarque précédente.*

**Théorème 14.9**

**Soit $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$ tels que $a \wedge n = 1$, alors on a : $a^{\varphi(n)} \equiv 1\ [n]$ (Euler).**

Démonstration : $\overline{a}$ est un élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ de cardinal $\varphi(n)$ et Lagrange permet de conclure.

*REMARQUE 14.30 : Si on se donne un nombre premier $p$ et $a \in \mathbb{Z}$ tel que $a \wedge p = 1$, alors on déduit du théorème précédent que $a^{p-1} \equiv 1\ [p]$ car $\varphi(p) = p - 1$ : on voit donc que le petit théorème de* Fermat *n'est qu'un ridicule corollaire de ce résultat d'*Euler *(mais un siècle plus tard).*

*REMARQUE 14.31 : On montre que la fonction $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ fait partie de la classe très étudiée des fonctions dites* **multiplicatives***, ce qui signifie dans ce contexte que :*

$$\forall (n,m) \in (\mathbb{N}^*)^2,\ n \wedge m = 1 \implies \varphi(nm) = \varphi(n)\varphi(m).$$

*Comme on connaît les images par $\varphi$ des puissances de nombres premiers ($\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$), on peut donc calculer grâce à ce résultat l'image de tout entier dont on connaît la décomposition en produit de puissances de nombres premiers. Ainsi, on peut montrer que $\varphi\left(\prod_{k=1}^{r} p_k^{\alpha_k}\right) = n \prod_{k=1}^{r} \left(1 - \frac{1}{p_k}\right)$.*