Chapitre 1: Rappels et Généralités

Tadmori Abdelhamid

1 Rappels sur l'arithmétique dans $\mathbb{Z}$

• **Activité :** On pose $a = 218$, $b = 20$

1. Déterminer q_0 *et* r_0 tels que $a = b.q_0 + r_0$, avec $0 \leqslant r_0 < b$.
2. Comparer q_0, *et* $E(\frac{a}{b})$, avec $E(\frac{a}{b})$ est la partie entière de $\frac{a}{b}$.
3. Comparer r_0 *et* $a - b.E(\frac{a}{b})$.
4. Soient $x, y \in \mathbb{N}$ tel que $y \neq 0$. Posons $q = E(\frac{x}{y})$ *et* $r = x - y.E(\frac{x}{y})$.
   i) vérifier que $x = y.q + r$, où $0 \leqslant r < y$.
   ii) que peut on dire de l'unicité de q et r ?.

Remarque 1.1 *L'opération qui nous permet de déterminer q et r tels que* $a = bq + r$ *où* $0 \leqslant r < |b|$, *s'appelle la division euclidienne de a par b dans* $\mathbb{Z}$.

Exercice 1 : Déterminer q et r dans chaque cas.

$$118 = -37q + r;\ -118 = 37q + r;\ -118 = -37q + r.$$

1.1 Divisibilité

Définition 1.2 *On dit qu'un entier* $b \in \mathbb{Z}$ *divise un autre entier a ssi il existe* $k \in \mathbb{Z}$ *tel que* $a = b.k$ *et on note* $b \mid a$. *Si b ne divise pas a, on le note* $b \nmid a$, *et on note* $D(a)$ *l'ensemble des diviseurs de a.*

Exemples 1.3 $D(4) = \{-4, -2, -1, 1, 2, 4\}; D(-3) = \{-3, -1, 1, 3\}$.

Propriétés 1.4 *Soient* $a, b, c \in \mathbb{Z}$. *On a :*

1. $\forall\ a \in \mathbb{Z}^* : 1 \mid a,\ a \mid a,\ a \mid 0$ *et* $0 \nmid a$
2. $a \mid b \Longleftrightarrow a \mid -b$.
3. *Si* $a \mid b$ *et* $b \mid c$ *alors* $a \mid c$.
4. *Si* $a \mid b$ *et* $b \mid a$, *alors* $|a| = |b|$.
5. *Si* $a \mid b$ *et* $c \mid d$, *alors* $ac \mid bd$.
6. *Si* $a \mid b$ *et* $a \mid c$, *alors* $\forall\ \alpha, \beta \in \mathbb{Z} : a \mid (\alpha.b + \beta.c)$
7. *Si* $a > 0, b > 0$ *et* $a \mid b$, *alors* $a \leqslant b$.

Preuve 1 *Comme exercice.*

Définition 1.5 *Étant donné deux entiers a et b non nuls.*

i) le plus grand commun diviseur de a et b, c'est le plus grand des diviseurs commun de a et b positif, on le note par $pgcd(a, b)$ *ou* $a \wedge b$.

ii) le $ppcm(a, b)$ *est le plus petit commun multiple strictement positif et se note aussi par* $a \vee b$.

Exemples 1.6 *Déterminer* $(-30) \wedge 12$, *et* $21 \vee 15$.

Exercice 2 : Soient p *et* n deux éléments de $\mathbb{Z}$ tels que $p \mid (13n+1)$ *et* $p \mid (-2n+3)$. Montrer que $p \mid 41$.

Propriétés 1.7 *Soient* $a, b, c \in \mathbb{Z}$.

1. *Les propriétés de pgcd sont :*
   i) $a \wedge 1 = 1$; $a \wedge b = |a| \wedge |b|$; $a \wedge b = b \wedge a$; $a \wedge a = a \wedge 0 = |a|$.
   ii) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$.
   iii) $a \wedge b = |a| \Longleftrightarrow a \mid b$.
2. *Les propriétés de ppcm sont :*
   i) $a \vee b = b \vee a$; $a \vee b = |a| \vee |b|$; $a \vee a = |a|$; $a \vee 1 = |a|$.
   ii) $(a \vee b) \vee c = a \vee (b \vee c)$.
   iii) $a \mid a \vee b$; $b \mid a \vee b$; $a \vee 0 = 0$.
   iv) si $b \mid a$, *alors* $a \vee b = |a|$, *et inversement.*

1.2 Division Euclidienne

Théorème 1.8 *Soient* a, b *dans* $\mathbb{Z}$ *où* $b \neq 0$. *Il existe un unique couple* $(q, r) \in \mathbb{Z} \times \mathbb{N}$ *tel que* $a = b \times q + r$ *avec* $0 \leqslant r < |b|$, q *s'appelle le quotient et* r *le reste de la D.E.*

Preuve 2
1. *Cas* $b > 0$; *ie* : $b \in \mathbb{N}^*$.
   — *si* $a \geqslant 0, \exists!(q, r) \in \mathbb{N} \times \mathbb{N}$ *tel que* $a = b \times q + r$ *avec* $0 \leqslant r < b$. *(Voir l'activité précédente).*
   — *si* $a < 0$ *alors* $-a > 0$, *donc d'après ce qui précède, aussi* $\exists!(q', r') \in \mathbb{N} \times \mathbb{N}$ *tel que* $-a = b \times q' + r'$ *avec* $0 \leqslant r' < b$. *Ceci implique* $-b < -r' \leqslant 0$ *donc* $0 < b - r' \leqslant b$.
   Si $r' \neq 0$, *on aura* $0 < b - r' < b$, *et*

$$-a = b \times q' + r' \Longrightarrow a = -b \times q' - r' \Longrightarrow a = -b \times (q' + 1) + b - r';$$

   on pose alors $q = -(q' + 1)$ *et* $r = b - r'$, *on obtient* $a = b \times q + r$. *Puisque* q' *et* r' *sont uniques, alors* q *et* r *sont aussi uniques.*
   Si $r' = 0$, *alors ;* $-a = b \times q' + 0 \Longrightarrow a =, -b \times q' \Longrightarrow a = b \times q$ *avec* $q = -q'$.
2. *Cas* $b < 0$. *De la même manière. (comme exercice).*

1.3 Algorithme d'Euclide pour calculer le pgcd

Puisque $pgcd(a, b) = pgcd(|a|, |b|)$, *on peut considérer* a *et* b *des entières naturels.*

Théorème 1.9 *Soient* a *et* b *dans* $\mathbb{N}^*$ *tels que* $b \nmid a$ *et* r *le reste de la division euclidienne de* a *par* b; *on a :* $a \wedge b = b \wedge r$.

Preuve 3 *Notons* $D(a), D(b)$ *et* $D(r)$ *respectivement l'ensemble des diviseurs de* a, b *et de* r, *avec* r *est le reste de la D.E de* a *par* b; *c'est à dire* $a = b \times q + r$. *On a ;*

$$\begin{aligned} x \in D(a) \cap D(b) &\Longrightarrow x \mid a \text{ et } x \mid b \\ &\Longrightarrow x \mid a - bq \\ &\Longrightarrow x \mid r \text{ et } x \mid b \end{aligned}$$

Donc $x \in D(b) \cap D(r)$. *Inversement ;*

$$\begin{aligned} x \in D(b) \cap D(r) &\Longrightarrow x \mid b \text{ et } x \mid r \\ &\Longrightarrow x \mid a \text{ et } x \mid b \end{aligned}$$

D'où $D(a) \cap D(b) = D(b) \cap D(r)$, *ce qui montre* $a \wedge b = b \wedge r$.

Corollaire 1.10 *Soient* $a, b \in \mathbb{N}^*$ *tels que* $b \nmid a$. *le pgcd(a, b) est égal au dernier reste non nul dans les divisions successives de a par b.*

Preuve 4 *On applique successivement le théorème précédent.*

$$\begin{cases} a = bq_1 + r_1 \text{ avec } 0 \leqslant r_1 < b \Longrightarrow a \wedge b = b \wedge r_1 \\ b = r_1 q_2 + r_2 \text{ avec } 0 \leqslant r_2 < r_1 \Longrightarrow b \wedge r_1 = r_1 \wedge r_2 \\ \vdots \\ r_{n-2} = r_{n-1} q_n + r_n \text{ avec } 0 \leqslant r_n < r_{n-1} \Longrightarrow r_{n-2} \wedge r_{n-1} = r_{n-1} \wedge r_n \\ r_{n-1} = r_n q_{n+1} + r_{n+1} \text{ avec } 0 \leqslant r_{n+1} < r_n \Longrightarrow r_{n-1} \wedge r_n = r_n \wedge r_{n+1} \end{cases}$$

et si $r_{n+1} = 0$, *alors* $r_n \wedge 0 = r_n$. *Donc* $a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = \cdots = r_{n-1} \wedge r_n = r_n \wedge 0 = r_n$. *D'où* $a \wedge b = r_n$.

Exercice 3 : *Déterminer* $48 \wedge 27$, $126 \wedge 216$.

1.4 Identité de Bezout

Théorème 1.11 *Si $a, b \in \mathbb{Z}$, alors il existe $u, v \in \mathbb{Z}$ tels que $a \times u + b \times v = a \wedge b$. En général ; si $d = pgcd(a_1, a_2, \ldots, a_n)$, alors il existe $u_1, u_2, \ldots, u_n \in \mathbb{Z}$ tq $d = a_1u_1 + a_2u_2 + \cdots + a_nu_n$.*

Preuve 5 *On utilise les différentes équations obtenues dans l'algorithme d' Euclide, en partant de $a \wedge b = r_n$ et en remontant jusqu'à l'obtention de u et v. Pour le cas général on montre ça par récurrence en utilisant le fait que $a_1 \wedge a_2 \wedge a_3 \wedge \cdots \wedge a_n = a_1 \wedge (a_2 \wedge a_3 \wedge \cdots \wedge a_n)$, ie; $pgcd(a_1, a_2, a_3, \ldots, a_n) = pgcd(a_1, pgcd(a_2, a_3, \ldots, a_n))$.*

Exemples 1.12 *Pour a= 48, b=27 on applique l'algorithme d'Euclide, et les différentes équations obtenues dans cet algorithme, on trouve ; $a \wedge b = 3 = 48 \times 4 + 27 \times \times(-7)$. Donc $u = 4$ et $v = -7$.*

Corollaire 1.13 *1. $d \mid a$ et $d \mid b \Longleftrightarrow d \mid (a \wedge b)$. Autrement dit $D_a \cap D_b = D_{a \wedge b}$.*

2. $\forall\, k \in \mathbb{Z}^*$; $(ka) \wedge (kb) = |k| \times (a \wedge b)$.

Preuve 6 *1. $\Longrightarrow$); D'après le théorème précédent il existe $u, v \in \mathbb{Z}$; $au + bv = (a \wedge b)$. Or $d \mid a$ et $d \mid b$, alors $d \mid au$ et $d \mid bv$, ce qui montre que $d \mid (a \wedge b)$.*
$\Longleftarrow$); l'inverse c'est évident.

2. Posons $d = a \wedge b$, $\beta = (ka) \wedge (kb)$ et on montre que $\beta = |k|.d$. On a d'après l'identité de Bezout ; $d = au + bv$, et $\beta = ka.u' + kb.v'$. Or $d \mid a$ et $d \mid b$, alors $|k|.d \mid k.a$ et $|k|.d \mid k.b$, donc $|k|.d \mid \beta$. D'autre part $\beta \mid ka$ et $\beta \mid kb \Longrightarrow \beta \mid |k|.a$ et $\beta \mid |k|.b \Longrightarrow \beta \mid |k|.d$, d'où l'égalité $\beta = |k|.d$, ce qui donne le résultat.

Remarque 1.14 *Plus général, soient $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. On a*

1. *$D_{a_1} \cap D_{a_2} \cap \cdots \cap D_{a_n} = D_{pgcd(a_1, a_2, \ldots, a_n)}$.*
2. *$pgcd(ka_1, ka_2, \ldots, ka_n) = |k| pgcd(a_1, a_2, \ldots, a_n)$.*
3. *$\forall\, k \in D_{a_1} \cap D_{a_2} \cap \cdots \cap D_{a_n}$; $pgcd(\frac{a_1}{k}, \frac{a_2}{k}, \ldots, \frac{a_n}{k}) = \frac{pgcd(a_1, a_2, \ldots, a_n)}{|k|}$.*

Définition 1.15 *i) on dit que deux entiers $a, b \in \mathbb{Z}$, sont premiers entre eux si pgcd(a, b)=1. En général ; $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ sont dits premiers entre eux si $pgcd(a_1, a_2, \ldots, a_k) = 1$.*
ii) on dit que $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ sont premiers entre eux deux à deux si $\forall\, i \neq j : pgcd(a_i, a_j) = 1$.

Exemples 1.16 *— les entiers 9 et 10 sont premiers entre eux.*
— les entiers 4, 6, 9 sont premiers entre eux , mais ne sont pas premiers entre eux deux à deux, car on a par exemple $4 \wedge 6 = 2$.

Théorème 1.17 Théorème de Gauss : *Soient a, b et c trois entiers. Si a, et b sont premiers entre eux, et a divise b.c, alors a divise c, c'est à dire ;*

$$\begin{cases} a \wedge b = 1 \\ a \mid b.c \end{cases} \Longrightarrow a \mid c.$$

Preuve 7 *D'après le théorème de Bezout, il existe u et v deux entiers tels que $a.u + b.v = 1$, il vient alors en multipliant les deux membres par c, on obtient $ac.u + bc.v = c$. Or $a \mid ac$ et par hypothèse $a \mid bc$, donc $a \mid ac.u + bc.v$, ce qui montre que $a \mid c$.*

Proposition 1.18 *Soient $a, b \in \mathbb{Z}^*$. On a*

1. *$a \mid x$ et $b \mid x \Longleftrightarrow (a \vee b) \mid x$.*
2. *$(a \wedge b) \times (a \vee b) = |a \times b|$.*
3. *$\forall\, k \in \mathbb{Z}^*$; $ka \vee kb = |k| \times (a \vee b)$.*
4. *Si d est un diviseur commun de a et b, alors $\frac{a}{d} \vee \frac{b}{d} = \frac{a \vee b}{|d|}$.*
5. *$m = a \vee b \Longleftrightarrow \frac{m}{a} \vee \frac{m}{b} = 1$.*

Preuve 8 *1. Notons M_a, M_b et $M_{(a \vee b)}$ respectivement les ensembles des multiples de a, b et $a \vee b$, et montrons que $M_a \cap M_b = M_{(a \vee b)}$.*

$$\begin{aligned} x \in M_{(a \vee b)} &\Longrightarrow (a \vee b) \mid x \\ &\Longrightarrow a \mid x \text{ et } b \mid x \text{; car } a \mid (a \vee b) \text{ et } b \mid (a \vee b) \\ &\Longrightarrow x \in M_a \text{ et } x \in M_b \\ &\Longrightarrow x \in M_a \cap M_b. \end{aligned}$$

En autre ; $x \in M_a \cap M_b \Longrightarrow a \mid x$ et $b \mid x$, et d'après la D.E de x par $a \vee b$, il existe q et r tels que $x = q.(a \vee b) + r$, où $0 \leqslant r < a \vee b$, si $r \neq 0$, alors $r = x - q \times (a \vee b)$ et donc $a \mid r$ et $b \mid r$. Ceci dit que $a \vee b \leqslant r$, absurde au fait que $r < a \vee b$, donc $r = 0$. D'où $(a \vee b) \mid x$.

2. *Posons $a\wedge b=d$ et $a\vee b=m$, donc $a=d.a'$ et $b=d.b'$ avec $a'\wedge b'=1$, aussi on écrit $m=a.u=b.v$, ceci implique $m=da'u=db'v$, et donc $a'u=b'v$. D'après Gauss $a'\mid v$ c'est à dire il existe $k\in\mathbb{Z}$; $v=ka'$, donc $m=bv=bka'=db'a'k$, alors $db'a'\mid m$. D'autre part or $a\mid db'a'$ et $b\mid db'a'$, alors d'après la propriété 1 $m\mid db'a'$, par conséquent $m=d|a'.b'|$, ce qui donne $m.d=|a.b|$, d'où le résultat.*

3. *D'après la propriété 2 on a $(ka\vee kb)\times(ka\wedge kb)=k^2|a.b|=k^2(a\vee b)\times(a\wedge b)=|k|(a\vee b)\times|k|(a\wedge b)$ et puisque $|k|(a\wedge b)\neq 0$, alors $(ka\vee kb)=|k|(a\vee b)$.*

4. *On a ; $a\vee b=(d\times\frac{a}{d})\vee(d\times\frac{b}{d})=|d|(\frac{a}{d}\vee\frac{b}{d})$, d'où le résultat.*

5. *$\Longrightarrow$); on pose $d=a\wedge b$, donc $\frac{a}{d}\wedge\frac{b}{d}=1$, et puisque $d\times|m|=|a|\times|b|$, alors $\frac{|m|}{|a|}=\frac{|b|}{d}$ et $\frac{|m|}{|b|}=\frac{|a|}{d}$, donc $\frac{|m|}{|b|}\wedge\frac{|m|}{|a|}=\frac{|a|}{d}\wedge\frac{|b|}{d}=1$ ce qui montre $\frac{m}{b}\wedge\frac{m}{a}=1$.*

   $\Longleftarrow$); Or $m.a\vee m.b=|m|(a\vee b)=\frac{m}{b}\times ab\vee\frac{m}{a}\times ab=|ab|(\frac{m}{b}\vee\frac{m}{a})=|a.b|\times\frac{m^2}{|a.b|}=m^2$, donc $|m|\times(a\vee b)=|m|^2$, d'où $|m|=a\vee b$.

Corollaire 1.19 *1. Soient $a,b\in\mathbb{Z}$. On a : $a\wedge b=1\Longleftrightarrow a\vee b=|a.b|$.*

2. *Si $a_1,a_2,\ldots,a_n$ sont des entiers non nuls, premiers entre eux deux à deux, alors $ppcm(a_1,a_2,\ldots,a_n)=|a_1\times a_2\times\cdots\times a_n|$.*

Preuve 9 *Pour 1) ; se déduit directement de la propriété 2 précédente. Pour 2) ; on utilise la récurrence et la règle $a_1\vee a_2\vee\cdots\vee a_n=a_1\vee(a_2\vee a_3\vee\ldots,\vee a_n)$, et le fait que $\forall\, i$; $a_i\wedge\prod_{j\neq i}a_j=1$.*

Attention : *Le $ppcm(4,6,9)=36$ et leur produit égal 216. Pourtant 4, 6, 9 sont premiers entre eux, quelle explication donner ?. Vraiment la réponse c'est que les entiers 4, 6, 9 ne sont pas premiers entre eux deux à deux, car on a par exemple $4\wedge 6=2$.*

Proposition 1.20 Théorème de Bezout : *$a_1,a_2,\ldots,a_n$ sont premiers entre eux $\Longleftrightarrow\exists\, u_1,\, u_2,\ldots,u_n\in\mathbb{Z}$; $a_1u_1+a_2u_2+\cdots+a_nu_n=1$.*

Preuve 10 *$\Longrightarrow$). On utilise l'identité de Bezout précédente.*
$\Longleftarrow$). Réciproquement ; si il existe des u_i tels que $a_1u_1+a_2u_2+\cdots+a_nu_n=1$, alors tout diviseur commun aux a_i divise 1 et donc 1 est le $pgcd(a_1,a_2,\ldots,a_n)$.

Proposition 1.21 *Soient $a_1,a_2,\ldots,a_n\in\mathbb{Z}$, non tous nuls.*

1. *Si $d=pgcd(a_1,a_2,\ldots,a_n)$, alors $\frac{a_1}{d},\frac{a_2}{d},\ldots,\frac{a_n}{d}$, sont premiers entre eux.*

2. *Si $\sigma\in\mathbb{N}^*$ est un diviseur commun aux a_i tel que $\frac{a_1}{\sigma},\frac{a_2}{\sigma},\ldots,\frac{a_n}{\sigma}$, soient premiers entre eux, alors $\sigma=pgcd(a_1,a_2,\ldots,a_n)$.*

Preuve 11 *1. Posons $a_i=d.a'_i$. Comme $d=pgcd(a_1,a_2,\ldots,a_n)$, alors $d=pgcd(d.a'_1,d.a'_2,\ldots,d.a'_n)=d.pgcd(a'_1,a'_2,\ldots,a'_n)$, d'où $pgcd(a'_1,a'_2,\ldots,a'_n)=1$, ce qui donne le résultat, $pgcd(\frac{a_1}{d},\frac{a_2}{d},\ldots,\frac{a_n}{d})=1$.*

2. *Laissé aux lecteurs.*

1.5 Résolution de l'équation $a.x+b.y=c$ dans $\mathbb{Z}$ où a,b et c sont connus dans $\mathbb{Z}$

On suit les étapes suivantes :

1. *Calcul de $pgcd(a,b)$ via l'algorithme d'Euclide ;*
2. *Si $pgcd(a,b)$ ne divise pas c, alors l'équation n'a pas de solution dans $\mathbb{Z}$;*
3. *Si $pgcd(a,b)$ divise c, on cherche une identité de Bezout $a.u+b.v=a\wedge b$;*
4. *En multipliant l'identité de Bezout par $\frac{c}{a\wedge b}$ qu'est bien un entier, on obtient une solution (x_0,y_0); avec $x_0=\frac{u\times c}{a\wedge b}$; $y_0=\frac{v\times c}{a\wedge b}$;*
5. *A partir de (x_0,y_0) on obtient toutes les autres solutions (x,y); $x=x_0+\frac{b\times k}{a\wedge b}$ et $y=y_0-\frac{a\times k}{a\wedge b}$ avec $k\in\mathbb{Z}$. (ici c'est le même k).*

Exercice 4 : *Résoudre dans $\mathbb{Z}$ l'équation $48x+27y=6$.*

1.6 Nombres premiers

Définition 1.22 *On dit qu'un nombre entier p est premier dans $\mathbb{Z}$, si p est différent de 1 et -1, et admet exactement 4 diviseurs dans $\mathbb{Z}$, à savoir $1, -1, p$ et $-p$.*

Exemples 1.23 *Les entiers 2,3, 5, 7,..etc sont des nombres premiers positifs, et -2, -3,-7,..etc sont des nombres premiers négatifs.*

Remarque 1.24
1. *Si $p \in \mathbb{N}$, premier, alors il est différent de 1, et il a exactement deux diviseurs dans $\mathbb{N}$, 1 et p.*
2. *Si $p \in \mathbb{N}$, premier, alors $-p$ est premier dans $\mathbb{Z}$, pour cela on s'intéresse à des nombres premiers positifs, et on note par $\mathbb{P}$ l'ensemble des nombres premiers positifs.*

$$x \in \mathbb{P} \Longleftrightarrow \begin{cases} x \in \mathbb{N} \\ x \ est premier \end{cases}$$

Théorème 1.25 *Soit $n \in \mathbb{N}\backslash\{0;1\}$ n'est pas premier. Il existe un nombre premier $p > 0$ tel que $p \mid n$ et $p^2 \leqslant n$. Autrement dit ; $p \leqslant \sqrt{n}$.*

Preuve 12 *Soit $n \in \mathbb{N}\backslash\{0;1\}$ non premier, et p le plus petit entier positif différent de n et de 1, divisant n. On a ; p est premier car si non il ne sera pas le plus petit diviseur de n. Alors $\exists k \in \mathbb{N}^*$; $n = p.k$, or $k \mid n$ donc $p \leqslant k$. Ce qui donne ;*

$$p^2 \leqslant p.k \Longrightarrow p^2 \leqslant n \Longrightarrow p \leqslant \sqrt{n}.$$

Théorème 1.26 *L'ensemble $\mathbb{P}$ des nombres premiers contient une infinité d'éléments.*

Preuve 13 *Démontrons ce résultat par absurde. Supposons que $\mathbb{P} = \{p_1, p_2, \ldots, p_n\}$ soit fini. Posons $\alpha = p_1 \times p_2 \times \cdots \times p_n + 1$, il est alors clair que $\alpha \notin \mathbb{P}$, et donc α n'est pas premier. Ainsi α admet un diviseur premier p de plus $p \in \mathbb{P}$, ce qui est contradiction avec le fait qu'aucun des p_i ne divise α.*

Remarque 1.27
1. *L'un des méthodes (ou algorithmes) pour déterminer des nombres premiers positifs plus petits qu'un entier naturel donné "n" est connu sous le nom **crible d'Eratosthène**, en faisant barré les multiples des nombres premiers 2, 3, 5, 7, 11,..etc, dans la liste des nombres naturels inférieurs ou égales à n, sauf les nombres premiers 2, 3, 5, 7, 11,..etc.*
2. *Pour connaitre , si n est premier ou non on effectue la division euclidienne de n par les nombres premiers 2, 3, 5, 7,..etc, respectivement. Si on trouvera le reste de la D.E de n par l'un des premiers est nul, alors n n'est pas premier, si non ; on doit s'arrêter à la D.E par un nombre premier p tel que $p^2 > n$.*

1.7 Décomposition en facteurs premiers

Théorème 1.28 *Tout entier $n \in \mathbb{Z}^*$ différent de 1 et -1 admet une unique décomposition en facteurs premiers sous la forme $n = \varepsilon \times p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_k^{\alpha_k}$, avec $p_1, p_2, \ldots, p_k$ sont des nombres premiers positifs, $\alpha_1, \alpha_2, \ldots, \alpha_k$ des nombres naturels non nuls et $\varepsilon = 1$ si $n > 0$ et $\varepsilon = -1$ si $n < 0$.*

Preuve 14 *Soit $n \geqslant 2$. On a deux cas ;*

1. $n > 0$
   - *si n est premier, dans ce cas n=n.*
   - *si n est non premier, dans ce cas il existe p_1 le plus petit diviseur de n ; p_1 est premier, donc $n = p_1 \times q_1$. Si q_1 est premier, alors $n = p_1 \times q_1$ est un produit de nombres premiers. Si q_1 n'est pas premier, alors $\exists p_2$ le plus petit diviseur de q_1 qu'est premier, ie ; $q_1 = p_2 \times q_2$, ce qui donne $n = p_1 \times p_2 \times q_2$, et on fait de même pour q_2, ainsi de suite ; on obtient $n = p_1 \times p_2 \times \cdots \times p_r$, avec p_i sont premiers, mais ne sont pas obligatoire distincts. D'où $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_k^{\alpha_k}$.*
2. *$n < 0$, alors $-n$ est positif, donc $-n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_k^{\alpha_k}$, d'où le résultat $n = -p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_k^{\alpha_k}$.*

Théorème 1.29 *Soient a et b deux entiers positifs, on note leurs décomposition en facteurs premiers ; $a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r}$, $b = p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_r^{\beta_r}$. Alors ;*

$$a \wedge b = p_1^{min(\alpha_1,\beta_1)} \times p_2^{min(\alpha_2,\beta_2)} \times \cdots \times p_r^{min(\alpha_r,\beta_r)}$$

$$a \vee b = p_1^{max(\alpha_1,\beta_1)} \times p_2^{max(\alpha_2,\beta_2)} \times \cdots \times p_r^{max(\alpha_r,\beta_r)}.$$

Preuve 15 *On utilise le faite que tout diviseur commun d de a et b, a une décomposition sous la forme $d = p_1^{m_1} \times p_2^{m_2} \times \cdots \times p_r^{m_r}$ où $m_i \leqslant min(\alpha_i, \beta_i)$. Or le pgcd(a, b) est le plus grand commun diviseur de a et b, alors $pgcd(a,b) = p_1^{min(\alpha_1,\beta_i)} \times p_2^{min(\alpha_2,\beta_i)} \times \cdots \times p_r^{min(\alpha_r,\beta_r)}$. De même tout multiple commun M de a et b, a une décomposition sous la forme ; $M = p_1^{m_1} \times p_2^{m_2} \times \cdots \times p_r^{m_r}$ où $m_i \geqslant max(\alpha_i, \beta_i)$. Or le ppcm(a, b) c'est le plus petit commun multiple, alors $ppcm(a,b) = p_1^{max(\alpha_1,\beta_i)} \times p_2^{max(\alpha_2,\beta_i)} \times \cdots \times p_r^{max(\alpha_r,\beta_r)}$.*

1.8 Nombre de diviseurs d'un entier

Proposition 1.30 *Soit $n \in \mathbb{N}^*$, n'est pas premier et $n = p_1^{\alpha_1} \times_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r}$, sa décomposition en facteurs premiers. Le nombre de diviseurs de n dans $\mathbb{N}^*$ est ; $N = (1+\alpha_1) \times (1+\alpha_2) \times \cdots \times (1+\alpha_r)$, en particulier le nombre de diviseurs de n dans $\mathbb{Z}^*$ est $N = 2(1+\alpha_1) \times (1+\alpha_2) \times \cdots \times (1+\alpha_r)$.*

Preuve 16 *Si d divise n, alors $d = p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_r^{\beta_r}$, avec $0 \leqslant \beta_i \leqslant \alpha_i$, le nombre de diviseurs de n, c'est le nombre des d, lorsque chaque β_i varie dans $\{0, 1, \ldots, \alpha_i\}$. Il y a $(1+\alpha_i)$ possibilités de choisir β_i, pour $1 \leqslant i \leqslant r$, donc d'après le principe fondamentale de dénombrement le nombre de diviseurs de n dans $\mathbb{N}^*$ est $N = (1+\alpha_1) \times (1+\alpha_2) \times \cdots \times (1+\alpha_r)$, et dans $\mathbb{Z}^*$ sera égal $N = 2(1+\alpha_1) \times (1+\alpha_2) \times \cdots \times (1+\alpha_r)$.*

Définition 1.31 (La fonction indicatrice d'Euler) : *La fonction Φ telle que $\Phi(1) = 1$ et $\Phi(n)$; $n > 1$ est le nombre d'entiers premiers avec n et compris entre 1 et $n-1$.*

$$\Phi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$$

$$n \longmapsto \Phi(n)$$

s'appelle la fonction indicatrice d'Euler.

Exemples 1.32

1. $\Phi(7) = 6$, *car 7 est premier, donc premier avec 1,2,3, 4,5,6.*
2. $\Phi(10) = 4$, *car 10 est premier avec 1, 3 ,7, 9.*
3. $\Phi(12) = 4$, *car 12 est premier avec 1, 5, 7,11.*

Par contre si n devient grand il devient très lourd de vérifier pour tout $p < n$ si p est premier avec n. On a donc besoin d'une formule de calcul efficace pour Φ.

Proposition 1.33

1. *Si p est premier, alors $\Phi(p) = p - 1$.*
2. *Si p est premier et $\alpha \geqslant 1$, alors $\Phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p})$.*
3. *Si pgcd(a, b)=1, alors $\Phi(a.b) = \Phi(a).\Phi(b)$.*
4. *Si $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_k^{\alpha_k}$ non premier, alors*

$$\Phi(n) = n(1 - \frac{1}{p_1}) \times (1 - \frac{1}{p_2}) \times \cdots \times (1 - \frac{1}{p_k}).$$

Preuve 17

1. *Si p est premier, alors p est premier avec tous les entiers d tels que $1 \leqslant d \leqslant p-1$. Donc $\Phi(p) = p - 1$.*
2. *Si p est premier, et α un exposant entier, alors $\Phi(p^\alpha) = p^\alpha - p^{\alpha-1}$, en effet, les seuls entiers plus petits que P^α, qui ne soient pas premiers avec p^α sont les multiples de p, entiers de la forme N.p, avec $1 \leqslant N \leqslant p^{\alpha-1}$ qui sont précisément égales au nombre $p^{\alpha-1}$. D'où le résultat.*
3. *$\Phi(a.b)$ est le nombre d'entiers naturels $x < a.b$, premier avec ab.*
   a) *soit x un entier de cette sorte, en écrivant $x = z.a + y$. Certainement $y \neq 0$, si non a diviserait x et donc x ne serait pas premier avec a.b, on a donc $0 < y < a$ et $0 \leqslant z < b$, car $x \leqslant a.b$. Donc y est nécessairement premier avec a, si non un diviseur commun à y et a diviserait x et alors x ne serait pas premier avec a, donc avec a.b, ce qui 'est contraire à l'hypothèse. On a donc $\Phi(a)$ possibilités pour le choix de y.*
   b) *choisissons alors y premier avec a, $(0 < y < a)$ ce qui détermine un x premier avec a par $x = a.z + y$, où $0 \leqslant z < b$ qu'est pour le moment arbitraire. Il faut que x soit premier avec a.b, et pour cela nous devrons choisir z. De même on divise x par b, ce qui donne un quotient t et un reste r, $x = bt + r$, et comme précédemment, on a $r \neq 0$ et r premier avec b, par conséquent, on aura $\Phi(b)$ possibilités de choix de r, $(0 < r < b)$. Donc si x est un entier vérifiant $x < a.b$, premier avec a.b, les restes y et r des divisions de x par a et b respectivement sont des entiers vérifiant : $0 < y < a$, y premier avec a et $0 < r < b$, r premier avec b.*

   • *Réciproquement : Si on se donne arbitrairement deux entiers y et r vérifiant ces conditions, ils déterminent un entier x unique tel que $x < a.b$ et x premier avec a.b; en effet, supposons par exemple $r \geqslant y$ et considérons tous les entiers de la forme a.z, pour tous les entiers z vérifiant $0 \leqslant z \leqslant b$. Pour ces entiers z, la division de l'un quelconque des a.z par b, fournit un reste r_z tel que $0 \leqslant r_z < b$ et ce reste peut prendre b valeurs possible. Or, si $z \neq z'$ on a nécessairement $r_z \neq r_{z'}$, car si non ; il existe un couple d'entiers (z, z') avec $z > z'$ tel que $r_z = r_{z'}$, alors b diviserait $az - az' = a(z - z')$, et puisque $a \wedge b = 1$, donc devrait diviser $z - z'$, ce qui est impossible ; car z et z' sont tous les deux inférieurs à b, donc à fortiori leur différence. Par suite, les b restes sont exactement les b entiers, $0, 1, 2 \ldots, b-1$ pris chacun une fois et dans un ordre quelconque. Il y en a donc un et un seul qui ait la valeur $r - y$ et par suite*

il existe un quotient t tel que $az = bt + (r - y)$ ce qui donne $az + y = bt + r$ et $x = az + y = bt + r$. Comme $0 < y < a$ et $0 \leqslant z < b$, on a bien $x < a.b$ et x est premier séparément avec a et b (car y est premier avec a ,et r l'est avec b), donc avec leur produit a.b. Il existe donc autant d'entiers x qu'il existe de couples (y, r) d'entiers tels que,
i) $0 < y < a$, y premier avec a, et qui avait le $\Phi(a)$ choix possible.
ii) $0 < r < b$, r premier avec b, et qui avait le $\Phi(b)$ choix possible.
et par suite on a bien $\Phi(a.b) = \Phi(a).\Phi(b)$.

4. *On applique la propriété 3 et 2.*

Remarque 1.34 *On verra d'autre démonstration pour la propriété 3.*

Conjecture 1.35 *Voici deux conjectures qui n'ont pas de démonstration.*

1. ***Conjecture de Lehmer 1905-1991 :***
   n est premier ssi $n \equiv 1\, mod(\Phi(n))$.
2. ***Conjecture de Carmichael 1907 :*** $\forall\, n > 0;\ \exists\, m \neq n :\ \Phi(n) = \Phi(m)$.

1.9 Relation de congruence dans $\mathbb{Z}$

Définition 1.36 *Soient $a, b \in \mathbb{Z}$, et $n \in \mathbb{N}$. On dit que a et b sont congrus modulo n et l'on note $a \equiv b\, mod(n)$ ou par $a \equiv b[n]$ si n divise $(a - b)$.*

$$a \equiv b[n] \Longleftrightarrow \exists k \in \mathbb{Z};\ a = b + k.n.$$

Exemples 1.37 $29 \equiv 3[13];\ 29 \equiv 16[13];\ 29 \equiv -10[13]$.

Exercice 5 :

1. *Montrer que si a et b ont même reste dans la division euclidienne par n, alors ils sont congrus modulo n.*
2. *Compléter les expressions suivantes : $-7 \equiv ...[4];\ 5 \equiv 0[..];\ -1 \equiv ..[3]$.*

Propriétés 1.38 *Soient $a, b, c \in \mathbb{Z}$ et $n, e \in \mathbb{N}^*$. On a les règles suivantes :*

1. $a \equiv a[n]$.
2. $a \equiv b[n] \Longleftrightarrow b \equiv a[n]$.
3. $\left\{ \begin{array}{l} a \equiv b[n] \\ b \equiv b'[n] \end{array} \right. \Longrightarrow a \equiv b'[n]$.
4. $\left\{ \begin{array}{l} a \equiv a'[n] \\ b \equiv b'[n] \end{array} \right. \Longrightarrow a + b \equiv (a' + b')[n]$.
5. $\left\{ \begin{array}{l} a \equiv a'[n] \\ b \equiv b'[n] \end{array} \right. \Longrightarrow a \times b \equiv (a' \times b')[n]$.
6. $a \equiv b[n] \Longrightarrow a^e \equiv b^e[n]$.

Preuve 18 *Laissé aux lecteurs.*

Remarque 1.39
1. *La relation de congruence est une relation d'équivalence.*
2. *Les propriétés 4 et 5 nous permet de dire que la relation de congruence est compatible avec l'opération d'addition et de multiplication.*

1.10 Classes d'équivalences de la relation de congruence

Définition 1.40 *Soit $n \in \mathbb{N}^*$ et $r \in \mathbb{Z}$, l'ensemble $\{a \in \mathbb{Z} \,|\, a \equiv r[n]\}$ s'appelle la classe d'équivalence de r associe à la relation de congruence modulo n et se note par $\bar{r}$, et on écrit $\bar{r} = \{a \in \mathbb{Z} \,|\, a \equiv r[n]\}$. Autrement dit ;*

$$x \in \bar{r} \Longleftrightarrow x \equiv r[n] \Longleftrightarrow \exists k \in \mathbb{Z};\ x = r + k.n$$

Exemples 1.41 *Pour $n = 2$, on a $\bar{0} = \{x \in \mathbb{Z} \,|\, x \equiv 0[2]\} = \{2k \,|\, k \in \mathbb{Z}\}$, et $\bar{1} = \{x \in \mathbb{Z} \,|\, x \equiv 1[2]\} = \{1 + 2k \,|\, k \in \mathbb{Z}\}$.*

Question : *Pour $n = 3$, déterminer $\bar{0}$, $\bar{1}$ et $\bar{2}$.*

Définition 1.42 *Soit $n \in \mathbb{N}^*$. L'ensemble $\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$, s'appelle l'ensemble des classes d'équivalences associe à la relation de congruence modulo n, se note par $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$, ou par $\mathbb{Z}/n\mathbb{Z}$, et on écrit $\dfrac{\mathbb{Z}}{n\mathbb{Z}} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$.*

Exemples 1.43 $\dfrac{\mathbb{Z}}{2\mathbb{Z}} = \{\bar{0}, \bar{1}\},\ \dfrac{\mathbb{Z}}{3\mathbb{Z}} = \{\bar{0}, \bar{1}, \bar{3}\}$.

1.11 Opérations dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$

Si $\bar{x}, \bar{y} \in \frac{\mathbb{Z}}{n\mathbb{Z}}$, alors ils existent respectivement r et $r' \in \{0, 1, \ldots, n-1\}$ tels que $\bar{x} = \bar{r}$ et $\bar{y} = \bar{r'}$; c'est à dire $x \in \bar{r}$, $y \in \bar{r'}$. Donc

$$\begin{cases} x \in \bar{r} \Longleftrightarrow x \equiv r[n] \\ y \in \bar{r'} \Longleftrightarrow y \equiv r'[n] \end{cases} \Longrightarrow x + y \equiv (r + r')[n] \Longrightarrow (x + y) \in \overline{r + r'}$$

Or l'ensemble $\bar{r} + \bar{r'} = \{a + b \,|\, a \in \bar{r} \text{ et } b \in \bar{r'}\}$, alors $x + y \in \bar{r} + \bar{r'}$, d'où $\overline{r + r'} \subset \bar{r} + \bar{r'}$. D'autre part ; il est clair que $\bar{r} + \bar{r'} \subset \overline{r + r'}$, donc $\overline{r + r'} = \bar{r} + \bar{r'}$. On montre de la même manière que $\overline{r \times r'} = \bar{r}.\bar{r'}$. Ceci nous permet de donner la définition suivante :

Définition 1.44 *Pour tous $\bar{x}, \bar{y} \in \frac{\mathbb{Z}}{n\mathbb{Z}}$.*

i) on définit l'addition " + " dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$ comme suivante : $\bar{x} + \bar{y} = \overline{x + y}$.

ii) on définit la multiplication "." dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$ comme suivante : $\bar{x}.\bar{y} = \overline{x \times y}$.

Exemples 1.45 *Dans $\frac{\mathbb{Z}}{8\mathbb{Z}}$, $\bar{7} + \bar{2} = \bar{9} = \bar{1}$, car $9 \equiv 1[8]$; $\bar{4}.\bar{6} = \bar{24} = \bar{0}$, car $24 \equiv 0[8]$.*

Remarque 1.46

1. *On a $\bar{1}$ est l'élément neutre pour la loi ".".*
2. *Si il existe $u \in \mathbb{Z}$ tel que $x \times u \equiv 1[n], ie; \bar{x}.\bar{u} = \bar{1}$, on dit que $\bar{x}$ est inversible pour la loi "." dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$. On note par $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$, l'ensemble des éléments inversible (ou bien l'ensemble des unités) pour la loi multiplicative ".".*
3. *On verra plus loin que $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, .)$ est un anneau, et si n est premier il est un corps.*

Exercice 6 :

1. *Montrer que $\forall\, n \in \mathbb{N}$; $4^{2n+2} \equiv 1[15]$.*
2. *Montrer que $\forall\, n \in \mathbb{N}^*$; $(n+1)^{2006} - 1 \equiv 0[n]$.*
3. *Résoudre dans $\frac{\mathbb{Z}}{29\mathbb{Z}}$ l'équation ; $15x + 24 = 17$.*

Proposition 1.47 *Soient $n > 1$ et a deux entiers, $\bar{a}$ la classe de a modulo n. Les conditions suivantes sont équivalentes :*

i) $a \wedge n = 1$;

ii) $\bar{a} \in (\frac{\mathbb{Z}}{n\mathbb{Z}})^*$;

iii) $\bar{a}$ engendre le groupe additif $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +)$.

Preuve 19 *i) $\Longrightarrow$ ii); a et n sont premiers entre eux, donc d'après le théorème de Bezout il existe deux entiers u et v tels que $a \times u + n \times v = 1$, ce qui implique $a \times u = 1 - n \times v$. D'où $a \times u \equiv 1[n]$, donc $\bar{a} \in (\frac{\mathbb{Z}}{n\mathbb{Z}})^*$.*
ii) $\Longrightarrow$ iii); il existe par hypothèse un élément $\bar{u}$ tel que $\bar{a}.\bar{u} = \bar{1}$. Pour les $1 \leqslant k \leqslant n-1$ les classes $k\bar{a}$ sont alors toutes distincts, car si $k\bar{a} = k'\bar{a}$ pour $1 \leqslant k' < k < n$, alors $(k - k')\bar{a} = \bar{0}$, absurde, en effet ; en multipliant par $\bar{u}$, on trouve $(k - k')\bar{1} = \bar{0} \Longrightarrow \overline{k - k'} = \bar{0}$, ceci dit que $\exists\, r > 0; k - k' = r \times n$, et donc $k = k' + r \times n > n$, ce qui donne la contradiction avec le fait $k < n$. En autre si $k\bar{a} = \bar{0}$, alors $k\bar{1} = \bar{0}$ ce qui implique $\bar{k} = \bar{0}$, et donc $\exists\, r \in \mathbb{N}$; $k = r \times n$, or $1 \leqslant k \leqslant n-1$, alors impossible, sauf si $k = 0$ on aura bien sur $r = 0$. Cela implique que tout élément de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est de la forme $k\bar{a}$, où $0 \leqslant k \leqslant n-1$, en ajoutant le fait que $0.\bar{a} = \bar{0}$.
iii) $\Longrightarrow$ i); si $\bar{a}$ engendre $\frac{\mathbb{Z}}{n\mathbb{Z}}$, alors l'élément $\bar{1}$ est engendré par a, il existe donc $u \in \mathbb{Z}$ tel que $\bar{1} = \bar{u}.\bar{a}$, ce qui implique $\exists\, v \in \mathbb{Z} : 1 = u \times a + v \times n$. Donc $a \wedge n = 1$.

Corollaire 1.48 $\left((\frac{\mathbb{Z}}{n\mathbb{Z}})^*, .\right)$ *est un groupe et* $card\left((\frac{\mathbb{Z}}{n\mathbb{Z}})^*\right) = \Phi(n)$.

Preuve 20 *On montre facilement que $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$ est un groupe pour la loi multiple ".", et d'après la proposition précédente ; le nombre d'éléments de ce groupe égal $\Phi(n)$.*

Théorème 1.49 (Théorème d'Euler) : *Soient a et n deux entiers premiers entre eux. Alors $a^{\Phi(n)} \equiv 1\,[n]$, où Φ est la fonction indicatrice d'Euler.*

Preuve 21 *Soit $\bar{a}$ la classe de a modulo n. Or $a \wedge n = 1$, alors d'après la proposition précédente, $\bar{a} \in (\frac{\mathbb{Z}}{n\mathbb{Z}})^*$, et donc l'ordre de $\bar{a}$ divise $\Phi(n)$. D'où $\bar{a}^{\Phi(n)} = \bar{1}$, ce qui est équivalent à $a^{\Phi(n)} \equiv 1\,[n]$.*

Théorème 1.50 (Petit théorème de Fermat) : *Si n est premier alors $\forall\, a \in \mathbb{Z}^*$ non divisible par n on a ; $a^{n-1} \equiv 1\,[n]$.*

Preuve 22 *On applique le théorème d'Euler précédent, car pour n premier on a, $\Phi(n) = n - 1$.*

1.12 Théorème des restes Chinois

Théorème 1.51 *Soient $m_1, m_2, \ldots, m_k \in \mathbb{N}^*$ et $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ et le système d'équations :*

$$(E) : \begin{cases} x \equiv a_1\,[m_1] \\ x \equiv a_2\,[m_2] \\ \vdots \equiv \vdots \\ x \equiv a_k\,[m_k] \end{cases}$$

i) si (E) possède une solution x_0, alors il en possède une infinité données par la formule :

$$x \equiv x_0\, mod(ppcm(m_1, m_2, \ldots, m_k)).$$

ii) si $m_1, m_2, \ldots, m_k$ sont premiers entre eux deux à deux (ie : $pgcd(m_i, m_j) = 1, \forall\, i \neq j$), alors il existe une unique solution x_0 modulo $ppcm(m_1, m_2, \ldots, m_k) = m_1 \times m_2 \times \cdots \times m_k$.

Cette solution s'obtient à partir d'une identité de Bezout entre $M_i = \prod_{i \neq j} m_j$ et m_i. En effet ; M_i et m_i sont premières entre eux, donc d'après Bezout il existe u_i, $v_i \in \mathbb{Z}$ tels que $u_i.m_i + v_i.M_i = 1$. On pose $e_i = v_i.M_i$, nous avons alors $e_i \equiv 1\,[m_i]$ et $e_i \equiv 0\,[m_j]$ pour $j \neq i$. L'entier $x_0 = \sum_{i=1}^{k} a_i.e_i = \sum_{i=1}^{k} a_i v_i M_i = a_1v_1M_1 + a_2v_2M_2 + \cdots + a_kv_kM_k$ est bien une solution particulière car,

$$\begin{aligned} x_0 &\equiv a_1v_1M_1 \equiv a_1\,[m_1], \text{ car seul } M_1 \text{ n'est pas divisible par } m_1. \\ x_0 &\equiv a_2v_2M_2 \equiv a_2\,[m_2], \text{ car seul } M_2 \text{ n'est pas divisible par } m_2. \\ &\vdots \\ x_0 &\equiv a_kv_kM_k \equiv a_k\,[m_k], \text{ car seul } M_k \text{ n'est pas divisible par } m_k. \end{aligned}$$

Et les autres solutions sont les entiers congrus à x modulo $ppcm(m_1, m_2, \ldots, m_k) = m_1 \times m_2 \times \cdots \times m_k$.

Exemples 1.52 *Résoudre le système suivant :*

$$\begin{cases} x \equiv 5\,[17] \\ x \equiv 8\,[29] \end{cases}$$

2 Généralités sur les ensembles et structures

Définition 2.1 *Intuitivement, un ensemble E est une collection d'objets appelés éléments. Soit x un objet mathématique, la relation d'appartenance de x à E est soit vraie, soit fausse :*

i) si elle est vraie on dit que x est un élément de E ou x appartient à E et on écrit $x \in E$.

ii) si elle est fausse on dit que x n'est pas un élément de E ou x n'appartient pas à E et on écrit $x \notin E$.

Lorsque l'ensemble E est fini, l'ensemble qui se note par $\mathcal{P}(E)$ s'appelle l'ensemble des parties de E, il est de cardinal égale ; $card(\mathcal{P}(E)) = 2^{card(E)}$.

2.1 Lois de Morgan

Théorème 2.2 *Soit E un ensemble et A et B deux parties de E (ie, $A, B \in \mathcal{P}(E)$) on a :*

i) $C_E^{A \cap B} = C_E^A \cup C_E^B$.

ii) $C_E^{A \cup B} = C_E^A \cap C_E^B$.

Preuve 23 *Comme exercice.*

2.2 Relation binaire

Définition 2.3 *Étant donné deux ensembles non vides E et F, on appelle relation binaire de E vers F, la donné d'un triplet $\mathcal{R} = (E, F, G)$ de coordonnées E, F et un sous ensemble G de $E \times F$.*

i) si $\mathcal{R}$ est vraie pour le couple (x, y) on écrit $x\mathcal{R}y$.

ii) l'ensemble $G_{\mathcal{R}} = \{(x, y) \in E \times F \,|\, x\mathcal{R}y\}$ s'appelle le graphe de la relation $\mathcal{R}$, et se note par $G_{\mathcal{R}}$.

iii) lorsque $E = F$ on dit que $\mathcal{R}$ est une relation binaire sur E.

Exemples 2.4 *Soit $E = \{0; -1; 1; 2; 4\}$ et soit $\mathcal{R}$, la relation sur E définie par $x\mathcal{R}y \Longleftrightarrow x^2 = y^2$. Donner le graphe de $\mathcal{R}$.*

2.3 Relation d'équivalence

Définition 2.5 *Une relation binaire sur un ensemble E est appelé relation d'équivalence si elle est réflexive, symétrique et transitive.*

i) La réflexivité ; c'est à dire $\forall x \in E : x\mathcal{R}x$.

ii) La symétrie ; $\forall (x; y) \in E^2 : x\mathcal{R}y \Longrightarrow y\mathcal{R}x$.

iii) La transitivité ; pour tous x, y et z dans E : $x\mathcal{R}y$ et $y\mathcal{R}z \Longrightarrow x\mathcal{R}z$.

Exemples 2.6 *Soit $f : E \Longrightarrow F$ une application et $\mathcal{R}$ une relation binaire sur E définie par*

$$x\mathcal{R}y \Longleftrightarrow f(x) = f(y).$$

La relation $\mathcal{R}$ est une relation d'équivalence.

Remarque 2.7 *Nous verrons que toutes les relations d'équivalence peuvent être obtenue de cette façon.*

Exercice 7 : *Sur $\mathbb{R}^*$ on définit une relation $\mathcal{R}$ par ; $x\mathcal{R}y \Longleftrightarrow x + \dfrac{1}{x} = y + \dfrac{1}{y}$.*

Étudier la relation $\mathcal{R}$ et donner son graphe.

Définition 2.8 *Soit E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E.*

1. *Pour $x \in E$ l'ensemble qu'on note $\bar{x} = \{y \,|\, y \in E \text{ et } x\mathcal{R}y\}$ s'appelle classe d'équivalence de x modulo $\mathcal{R}$.*
2. *L'ensemble des classes d'équivalence $\{\bar{x} \,|\, x \in E\}$ s'appelle ensemble quotient de E par $\mathcal{R}$ et se note $\dfrac{E}{\mathcal{R}}$ ou $E/\mathcal{R}$.*
3. *L'ensemble $\mathcal{E}$ qui vérifie la propriété suivante :*

$$\forall x \in E; \exists! x' \in \mathcal{E} \text{ tel que } x\mathcal{R}x'$$

s'appelle l'ensemble de représentants pour $\mathcal{R}$.

4. *L'application*

$$S_{\mathcal{R}} : E \longrightarrow E/\mathcal{R}$$
$$x \longmapsto \bar{x}$$

est surjective appelée surjection canonique associée à $\mathcal{R}$.

Remarque 2.9 *Il existe toujours des ensembles représentants pour une telle relation $\mathcal{R}$, en effet : Par l'axiome du choix il existe une application ;*

$$g : E/\mathcal{R} \longrightarrow E$$
$$\bar{x} \longmapsto g(\bar{x}) \in \bar{x}$$

alors l'ensemble $\mathcal{E} = \{g(\bar{x}) \mid \bar{x} \in E/\mathcal{R}\}$ est un ensemble de représentants pour $\mathcal{R}$.

Propriétés 2.10 *Voici les propriétés fondamentales des classes d'équivalences :*

1. *$\forall x, y \in E : x\mathcal{R}y \Longleftrightarrow \bar{x} = \bar{y}$.*
2. *$\forall x, y \in E$; on a soit $\bar{x} = \bar{y}$, soit $\bar{x} \cap \bar{y} = \emptyset$.*
3. *$\bigcup_{x \in \mathcal{E}} \bar{x} = E$. (ie ; la famille $(\bar{x})_{x \in \mathcal{E}}$ forme une partition de E).*
4. *$\bigcap_{x \in \mathcal{E}} \bar{x} = \emptyset$.*

2.4 Décomposition canonique d'une application

Soit $f : E \longrightarrow F$ une application. Reprenons la relation $\mathcal{R}$ associée à f

$$x\mathcal{R}y \Longleftrightarrow f(x) = f(y)$$

Notons $f(E) = \{f(x) \ / \ x \in E\}$ l'image de E par f. On montre que l'application

$$\bar{f} : \frac{E}{\mathcal{R}} \longrightarrow f(E)$$

$$\bar{x} \longrightarrow \bar{f}(\bar{x}) = f(x)$$

est bijective appelée bijection canonique associée à f.
L'application

$$i : f(E) \longrightarrow F$$

$$y = f(x) \longmapsto f(x)$$

est injective appelée injection canonique. Voir que

$$\begin{array}{ccc} E & \xrightarrow{\ f\ } & F \\ {\scriptstyle s}\downarrow & & \uparrow{\scriptstyle i} \\ E/\mathcal{R} & \xrightarrow{\ \bar{f}\ } & f(E) \end{array}$$

On a bien $f = i \circ \bar{f} \circ S$. Cette décomposition est appelée décomposition canonique de f.

2.5 Liste des structures algébriques

Dans la théorie des ensembles, l'objet principal est un ensemble qui se dissimule parfois sous d'autre noms tels que classe, collection, ou famille. Cependant, dans d'autre discipline mathématiques, un ensemble est toujours muni d'une structure. En algèbre tout particulièrement, un ensemble est combiné avec une ou plusieurs lois de compositions, il s'appelle une structure algébrique et voici une liste des structures algébriques importantes.

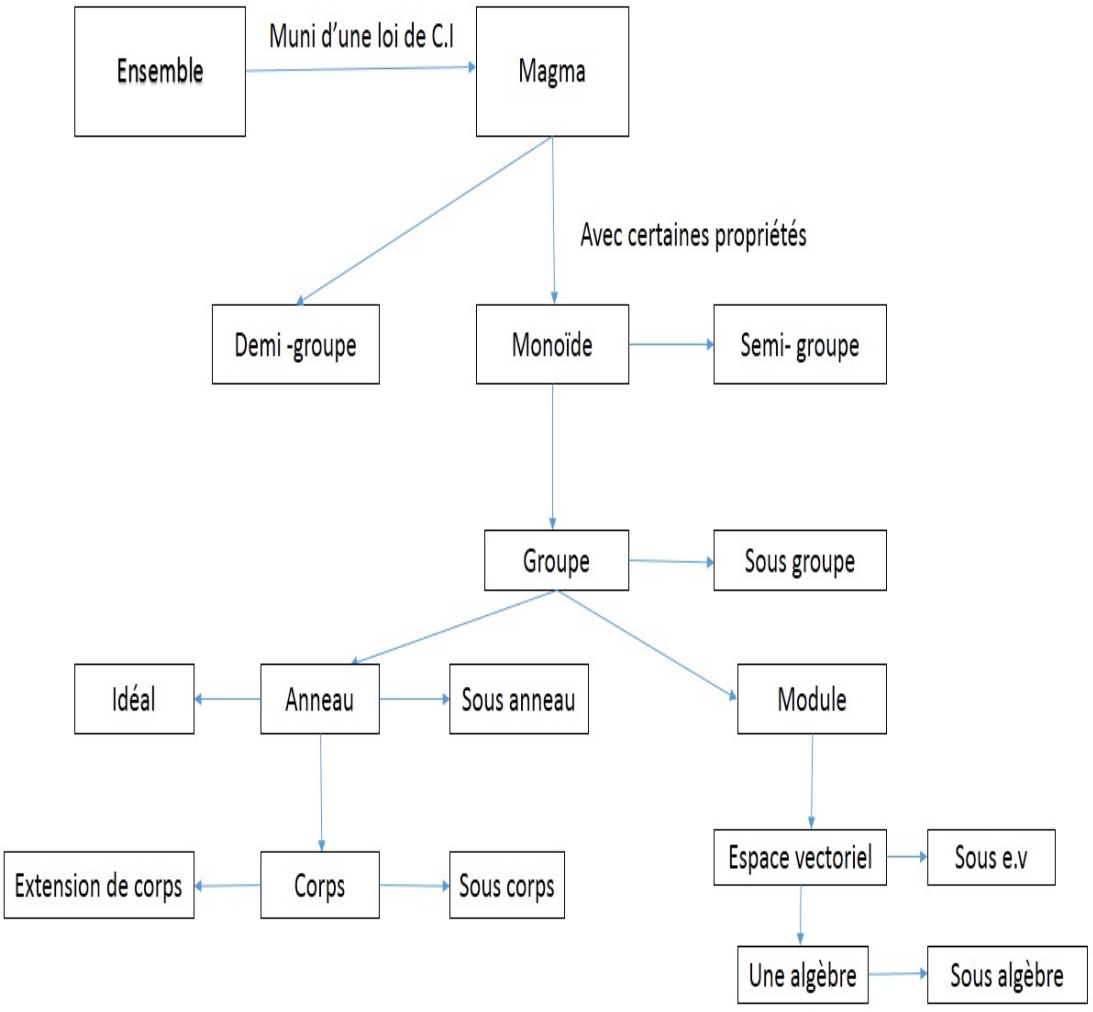

FIGURE 1 – 1) Liste des structures.