

CHAPITRE 10

Nombre

IN

Hugo SALOU MP2I

Dernière mise à jour le 14 juin 2022

TABLE DES MATIÈRES

I	Axiomatique de $\mathbb{N}$	2
II	Récurrence	5
III	Divisibilité	8
IV	Arithmétique modulaire	13
V	Axiomatique de $\mathbb{N}$	16
VI	Réurrences	19
VII	Divisibilité	21
VIII	Division Euclidienne	23
IX	Arithmétique Modulaire	27
X	PCGD et PPCM	31
XI	Décomposition en Facteurs Premiers	38

Première partie

Axiomatique de $\mathbb{N}$

Axiome: $(\mathbb{N}, \leq)$ est un ensemble non vide totalement ordonné vérifiant

- Toute partie non vide de $\mathbb{N}$ a un plus petit élément ;
- Toute partie non vide majorée de $\mathbb{N}$ a un plus grand élément ;
- $\mathbb{N}$ n'est pas majoré.

Définition: — 0 est le plus petit élément de $\mathbb{N}$: $0 = \min(\mathbb{N})$.

- $1 = \min(\mathbb{N}^*) = \min(\mathbb{N} \setminus \{0\})$.
- Soit $n \in \mathbb{N}$. On pose $n + 1 = \min(\{k \in \mathbb{N} \mid k > n\})$. On dit que $n + 1$ est le successeur de n .
- Soit $n \in \mathbb{N}^*$. On pose $n - 1 = \max(\{k \in \mathbb{N} \mid k < n\})$. On dit que $n - 1$ est le prédécesseur de n .

Proposition:

$$\begin{cases} \forall n \in \mathbb{N}, (n + 1) - 1 = n; \\ \forall n \in \mathbb{N}^*, (n - 1) + 1 = n. \end{cases}$$

Preuve:

Soit $n \in \mathbb{N}$. On pose $p = n + 1$ et $q = p - 1$. On a donc $n < p$ et $q < p$ et donc $n \leq q$ car $q = \max(\{k \in \mathbb{N} \mid k < p\})$.

Si $q > n$, alors $q \geq p$ car $p = \min(\{k \in \mathbb{N} \mid k > n\})$: une contradiction.

On a donc $q = n$. □

Proposition: Pour tout $n \in \mathbb{N}$, $\mathbb{N} \cap]n, n + 1[= \emptyset$.

Preuve:

Soit $n \in \mathbb{N}$. On sait que $n + 1 > n$. Soit $p \in \mathbb{N}$ tel que $n < p < n + 1$. Comme $p > n$, $p \geq n + 1$: une contradiction. □

Théorème (récurrence): Soit P un prédicat sur $\mathbb{N}$ et $n_0 \in \mathbb{N}$. Si

$$\begin{cases} P(n_0) \text{ est vrai,} \\ \forall n \geq n_0, P(n) \implies P(n + 1), \end{cases}$$

alors

$$\forall n \geq n_0, P(n) \text{ est vrai.}$$

Preuve:

Soit $A = \{n \in \mathbb{N} \mid n \geq n_0 \text{ et } P(n) \text{ faux}\}$. Supposons $A \neq \emptyset$; A a donc un plus petit élément. On pose $N = \min(A)$.

CAS 1 $N = 0$, alors, comme $N \in A$, on a $n_0 \leq 0$ et $P(0)$ fausse. On en déduit que $n_0 = 0$: une contradiction car $P(n_0) = P(0)$ est vraie.

CAS 2 $N \neq 0$. Alors $N - 1 \in \mathbb{N}$ et $N - 1 \notin A$ (car $N - 1 < N$). On en déduit que $N - 1 < n_0$ ou $P(N - 1)$ vraie.

- Supposons $N - 1 < n_0$. $N \in A$ donc $N \geq n_0$ et donc $N - 1 < n_0 \leq N$ donc $N = n_0$. Or, $N \in A$ donc $P(N)$ fausse alors que $P(n_0)$ est vraie.
 - Supposons $N - 1 > n_0$ et $P(N - 1)$ vraie. Comme $N - 1 \geq n_0$, $P(N - 1) \implies P(N)$ et donc $P(N)$ est vraie. Or, $N \in A$ et donc $P(N)$ est fausse.
- On en déduit que $A = \emptyset$.

□

Deuxième partie

Récurrence

Proposition (récurrence double): Soit P un prédicat sur $\mathbb{N}$ et $n_0 \in \mathbb{N}$. Si

$$\begin{cases} P(n_0) \text{ vraie} \\ P(n_0 + 1) \text{ vraie} \\ \forall n \in \mathbb{N} \text{ avec } n \geq n_0, P(n) \text{ et } P(n+1) \implies P(n+2) \end{cases}$$

Alors

$$\forall n \in \mathbb{N} \text{ avec } n \geq n_0, P(n) \text{ vraie.}$$

Preuve:

On pose, pour tout $n \geq n_0$,

$$Q(n) : "P(n) \text{ et } P(n+1)".$$

- $Q(0)$ est vraie.
- Soit $n \geq n_0$. On suppose $Q(n)$ vraie. On sait alors que $P(n+2)$ est vraie. De plus, par hypothèse de récurrence, $P(n+1)$ est vraie. Donc $Q(n+1)$ est vraie.

□

EXEMPLE:

On pose $u_0 = 0$, $u_1 = 1$ et

$$\forall n \in \mathbb{N}, u_{n+2} = u_{n+1} + u_n$$

Montrons que $\forall n \in \mathbb{N}, u_n \geq 0$.

- $u_0 = 0 \geq 0$;
- $u_1 = 1 \geq 0$;
- Soit $n \in \mathbb{N}$. On suppose que $u_n \geq 0$ et $u_{n+1} \geq 0$. Alors $u_{n+2} = u_n + u_{n+1} \geq 0$.

Par récurrence double,

$$\forall n \in \mathbb{N}, u_n \geq 0.$$

Proposition: Soit P un prédicat, $p \in \mathbb{N}^*$ et $n_0 \in \mathbb{N}$. Si

$$\begin{cases} \forall k \in \llbracket 0, p-1 \rrbracket, P(n_0 + k) \text{ vraie;} \\ \forall n \geq n_0, (P(n) \text{ et } P(n+1) \text{ et } \dots \text{ et } P(n+p-1)) \implies P(n+p). \end{cases}$$

Alors,

$$\forall n \geq n_0, P(n) \text{ vraie.}$$

□

EXEMPLE:

On pose $u_0 = 0$, $u_1 = 1$, $u_2 = 2$, $u_3 = 3$ et

$$\forall n \in \mathbb{N}, u_{n+4} = u_n + 2u_{n+1} + 3u_{n+2} + u_{n+3}.$$

Montrons que $\forall n \in \mathbb{N}, u_n \geq 0$.

- $u_0 \geq 0$, $u_1 \geq 0$, $u_2 \geq 0$ et $u_3 \geq 0$.
- Soit $n \in \mathbb{N}$. On suppose $u_n \geq 0$, $u_{n+1} \geq 0$, $u_{n+2} \geq 0$ et $u_{n+3} \geq 0$. Comme u_{n+4} est la somme de réels positifs, $u_{n+4} \geq 0$.

Proposition (récurrence forte): Soit P un prédicat sur $\mathbb{N}$ et $n_0 \in \mathbb{N}$. Si $P(n_0)$ est vrai et

$$\forall n \geq n_0, (P(n_0) \text{ et } \dots \text{ et } P(n-1) \text{ et } P(n)) \implies P(n+1).$$

Alors,

$$\forall n \geq n_0, P(n) \text{ est vraie.}$$

Preuve:

On pose, pour tout $n \in \mathbb{N}$,

$$Q(n) : \text{“}\forall k \in \llbracket n_0, n \rrbracket, P(k) \text{ vraie”}.$$

- $Q(n_0)$ est vraie car $P(n_0)$ est vraie.
- Soit $n \geq n_0$. On suppose $Q(n)$ vraie. On sait donc que $\forall k \in \llbracket n_0, n \rrbracket, P(k)$ vraie. Alors, $P(n+1)$ est vraie et donc

$$\forall k \in \llbracket n_0, n+1 \rrbracket, P(k) \text{ est vraie.}$$

Ainsi, $Q(n+1)$ est vraie. □

EXEMPLE:

Montrer que tout entier supérieur ou égal à 2 peut s'écrire comme un produit de nombres premiers. On prouve ce résultat par récurrence forte.

- Le nombre 2 est un nombre premier : $2 = 2$.
- Soit $n \geq 2$. On suppose que, tout entier $k \in \llbracket 2, n \rrbracket$ est un produit de nombres premiers. On pose $N = n+1$.
 CAS 1 N est premier et donc, on peut l'exprimer comme un produit de nombres premiers : $N = N$.
 CAS 2 N n'est pas un nombre premier. Alors, il existe p, q tels que $N = p \times q$ avec $1 < p < N$ et $1 < q < N$. Comme $p \in \llbracket 2, n \rrbracket$, p est un produit de nombres premiers. De même pour q . Donc, le produit $N = p \times q$ est un produit de nombres premiers.

EXEMPLE:

Avec $u_0 = 0, u_1 = 1, u_2 = 2, u_3 = 3$ et, pour tout $n \in \mathbb{N}$, $u_{n+4} = u_n + 2u_{n+1} + 3u_{n+2} + u_{n+3}$, montrer que, pour tout $n \in \mathbb{N}$, $u_n \geq 0$. On prouve ce résultat par récurrence forte.

- $u_0 = 0 \geq 0$.
- Soit $n \in \mathbb{N}$. On suppose que $\forall k \in \llbracket 1, n \rrbracket, u_k \geq 0$.
 — Si $n = 0, u_{n+1} = u_1 = 1 \geq 0$.
 — Si $n = 1, u_{n+1} = u_2 = 2 \geq 0$.
 — Si $n = 2, u_{n+1} = u_3 = 3 \geq 0$.
 — Si $n \geq 3, u_{n+1} = \underbrace{u_{n-3}}_{\geq 0} + 2 \underbrace{u_{n-2}}_{\geq 0} + 2 \underbrace{u_{n-1}}_{\geq 0} + 3 \underbrace{u_n}_{\geq 0} \geq 0$.

Troisième partie

Divisibilité

Définition: Soient $a, b \in \mathbb{Z}$. On dit que a divise b s'il existe $k \in \mathbb{Z}$ tel que $b = k \times a$. Dans ce cas, on écrit $a \mid b$. On dit aussi que a est un diviseur de b ; et que b est un multiple de a .

EXEMPLE: — $\forall x \in \mathbb{Z}, 1 \mid x$.
 — $0 \mid 0$ mais $\forall x \in \mathbb{Z}^*, 0 \nmid x$.
 — $\forall x \in \mathbb{Z}, x \mid 0$.

Proposition: “ $\mid$ ” est une relation d'ordre sur $\mathbb{Z}$. □

Proposition: Soient $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$.

$$a \mid b \implies |a| \leq |b|.$$

□

Proposition: Soient $a, b, c \in \mathbb{Z}$.

$$\left. \begin{array}{l} a \mid b \\ a \mid c \end{array} \right\} \implies (\forall (k, \ell) \in \mathbb{Z}^2, a \mid (kb + \ell c)).$$

Preuve:

On pose $u, v \in \mathbb{Z}$ tels que

$$\begin{cases} b = au, \\ c = av. \end{cases}$$

Soient $k, \ell \in \mathbb{Z}$.

$$bk + \ell c = aku + a\ell v = a \underbrace{ku + \ell v}_{\in \mathbb{Z}}.$$

et donc $a \mid (ku + \ell v)$. □

EXEMPLE:
 Soient $n \in \mathbb{N}$.

$$\left. \begin{array}{l} a \mid n \\ a \mid n+1 \end{array} \right\} \implies a \mid ((n+1) - n) \implies a \mid 1 \implies a = \pm 1.$$

Définition: Soient $a, b \in \mathbb{Z}$. On dit que a et b sont associés si

$$a = b \text{ ou } a = -b.$$

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

$$a \mid b \iff -a \mid b \iff a \mid -b.$$

Proposition (division euclidienne dans $\mathbb{N}$): Soient $(a, b) \in \mathbb{N} \times \mathbb{N}^*$.

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

$$\begin{array}{r|l} a & b \\ \hline r & q \end{array}$$

Preuve: **EXISTENCE** On considère $A = \{q \in \mathbb{N} \mid qb \leq a\}$. $A \neq \emptyset$ car $0 \in A$: $0 \times b = 0 \leq a$. A est majoré :

$$\forall q \in A, a \geq qb \geq q \text{ car } b \geq 1.$$

Soit $q = \max(A)$. On pose $r = a - bq$. Comme a, b et q sont des entiers positifs, $r \in \mathbb{Z}$. On sait que $q \in A$, donc $qb \leq a$ et donc $r \geq 0$. $q + 1 > \max A$ donc $q + 1 \notin A$ i.e. $(q + 1)b > a$ et donc $r < b$.

UNICITÉ Soient $(q', r') \in \mathbb{N}^2$ tels que $\begin{cases} a = q'b + r', \\ 0 \leq r' < b. \end{cases}$ Or, $a = bq + r$ et donc, en soustrayant les deux égalités, on a

$$0 = b(q' - q) + r' - r.$$

De plus, $0 \leq r < b$ et $-b < -r' \leq 0$, et donc

$$r - r' = \underbrace{b(q' - q)}_{\in \mathbb{Z}}.$$

On en déduit que $-b < r - r' < b$. Le seul multiple de b dans $]-b, b[$ est 0. Ainsi, $r' = r$ et donc $b(q' - q) = 0$. Or, $b > 0$, donc $q' = q$. □

Proposition (division euclidienne dans $\mathbb{Z}$): Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$.

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

Preuve: **EXISTENCE** CAS 1 $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. D'après la proposition précédente,

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

Comme $b > 0$, on a bien $0 \leq r < |b| = b$ et $q \in \mathbb{N} \subset \mathbb{Z}$.
CAS 2 $a \in \mathbb{Z}^-$ et $b \in \mathbb{N}^*$. Comme $-a \in \mathbb{N}$,

$$\exists (q', r') \in \mathbb{N}^2, \begin{cases} -a = bq' + r', \\ 0 \leq r' < b \end{cases}$$

donc

$$\begin{aligned} a &= b(-q') - r' \\ &= b(q' - 1) + b - r'. \end{aligned}$$

En posant,

$$q = \begin{cases} -q' - 1 & \text{si } r' \neq 0, \\ -q' & \text{si } r' = 0; \end{cases}$$

$$r = \begin{cases} b - r' & \text{si } r' \neq 0, \\ -r' & \text{si } r' = 0; \end{cases}$$

on a bien

$$\begin{cases} a = bq + r, \\ q \in \mathbb{Z}, \\ 0 \leq r < b. \end{cases}$$

CAS 3 $a \in \mathbb{N}$ et $b \in \mathbb{Z}_+^*$. On sait que

$$\exists (q', r') \in \mathbb{N}^2, \begin{cases} a = (-b)q' + r', \\ 0 \leq r' < -b. \end{cases}$$

En posant $q = -q'$ et $r = r'$, on a bien $a = bq + r$ et $0 \leq r < |b|$.

CAS 4 $a \in \mathbb{Z}^-$ et $b \in \mathbb{Z}_+^*$. On sait que

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

Donc,

$$\begin{aligned} a &= bq' - r' \\ &= b(q' + 1) - r' - b. \end{aligned}$$

En posant

$$q = \begin{cases} q' & \text{si } r' = 0, \\ q' + 1 & \text{si } r' \neq 0; \end{cases}$$

$$r = \begin{cases} r' & \text{si } r' = 0, \\ -r' - b & \text{si } r' \neq 0; \end{cases}$$

on a bien

$$\begin{cases} a = bq + r \\ q \in \mathbb{Z} \\ 0 \leq r < |b|. \end{cases}$$

UNICITÉ Soient $(q', r') \in \mathbb{Z}^2$ tels que

$$\begin{cases} a = bq' + r' \\ \leq r' < |b|. \end{cases}$$

Or, on sait que $a = bq + r$ et $0 \leq r < |b|$. D'où

$$\begin{cases} b(q' - q) = r' - r \\ -|b| < r - r' < |b| \end{cases}$$

donc $r - r' = 0$ et donc $q = q'$.

□

Définition: Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. D'après le théorème précédent, il existe un unique

couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que

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

On dit que r est le quotient, et r le reste dans la division (euclidienne) de a par b .

EXEMPLE:

Soit $n \in \mathbb{N}$ impair. On divise n par 2 : soient $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tels que $\begin{cases} n = 2q + r \\ 0 \leq r < 2. \end{cases}$

Si $r = 0$, n est pair : une contradiction. Ainsi, $r \neq 0$ et donc $r = 1$. On a donc $n = 2q + 1$.

Proposition: Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. On note r le reste de la division euclidienne de a par b .

$$r = 0 \iff a \mid b.$$

Preuve:

On pose $a = bq + r$ avec $q \in \mathbb{Z}$.

“ $\implies$ ” Si $r = 0$, alors $a = bq$ avec $q \in \mathbb{Z}$ et donc $b \mid a$.

“ $\impliedby$ ” Si $b \mid a$, il existe $k \in \mathbb{Z}$ tel que $a = bk$. Donc, $a = bk + 0$ et $0 \leq 0 < |b|$. Par unicité de la division euclidienne, $r = 0$.

□

Quatrième partie

Arithmétique modulaire

Définition: Soient $a, b \in \mathbb{Z}$ et $c \in \mathbb{N}^*$. On dit que a est congrus à b modulo c si a et b ont le même reste dans la division euclidienne par c . Dans ce cas, on écrit $a \equiv b \pmod{c}$.

Proposition: La congruence modulo c est une relation d'équivalence. □

REMARQUE (Notation):

On note $\mathbb{Z}/c\mathbb{Z}$ l'ensemble des classes d'équivalences modulo c .

Par exemple, $\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

Proposition: Soient $a, b \in \mathbb{Z}$ et $c \in \mathbb{N}^*$.

$$a \equiv b \pmod{c} \iff c \mid (b - a).$$

Preuve: “ $\implies$ ” Soient $q, q' \in \mathbb{Z}$ et $r \in \mathbb{N}$ tels que

$$\begin{cases} a = cq + r \\ b = cq' + r \end{cases}$$

avec $0 < r < c$. En soustrayant les égalités, on obtient

$$b - a = c \underbrace{(q' - q)}_{\in \mathbb{Z}}.$$

Ainsi, $c \mid (b - a)$.

“ $\impliedby$ ” On pose $\begin{cases} a = cq + r \\ b = cq' + r' \end{cases}$ avec $(q, q') \in \mathbb{Z}$ et $\begin{cases} 0 \leq r < c \\ 0 \leq r' < c. \end{cases}$ En soustrayant les égalités et inégalités, on obtient

$$\begin{cases} b - a = c(q' - q) + r' - r \\ -c < r' - r < c. \end{cases}$$

□

La suite du cours provient d'Aubin. Je ne suis pas responsable pour les éventuelles bêtises qu'il a pu taper.

Cinquième partie

Axiomatique de $\mathbb{N}$

Axiome (Axiomatique de Von Neumann): $(\mathbb{N}, \leq)$ est un ensemble totalement ordonné vérifiant
 Toute partie non vide de $\mathbb{N}$ a un plus petit élément
 Toute partie non vide majorée de $\mathbb{N}$ a un plus grand élément
 $\mathbb{N}$ n'est pas majoré

Définition (0): $0 = \min(\mathbb{N})$

Définition (1): $1 = \min(\mathbb{N} \setminus \{0\})$

Définition ($n + 1$): Soit $n \in \mathbb{N}$
 On pose $n + 1 = \min(\{k \in \mathbb{N} \mid k > n\})$
 On dit que $n + 1$ est le successeur de n

Proposition ($+1 - 1$): $\forall n \in \mathbb{N}, (n + 1) - 1 = n$
 $\forall n \in \mathbb{N}, (n - 1) + 1 = n$

Preuve:

Soient $n \in \mathbb{N}$, $p = n + 1$, $q = p - 1$

$n < p$ et $q < p$

Donc $n \leq q$ car $q = \max(\{k \in \mathbb{N} \mid k < p\})$

Si $q > n$, alors $q \geq p$ car $p = \min(\{k \in \mathbb{N} \mid k > n\})$

Donc $q = n$

□

Proposition (Ensemble Ouvert Vide): $\forall n \in \mathbb{N},]n, n + 1[= \emptyset$

Preuve:

Soit $n \in \mathbb{N}$, on sait que $n + 1 > n$

Soit $p > n$, on suppose $n < p < n + 1$

Comme $p > n, p \geq n + 1$ Contradiction

□

Proposition (Théorème de Récurrence): Soit P un prédicat sur $\mathbb{N}$ et $n \in \mathbb{N}$

Si $\begin{cases} P(n_0) \text{ est vrai} \\ \forall n \geq n_0, P(n) \implies P(n+1) \end{cases}$
 Alors $\forall n \geq n_0, P(n)$ est vrai

Preuve:

Soit $A = \{n \in \mathbb{N} | n \geq n_0\}$ et $P(n)$ faux

Supposons $A \neq \emptyset$

A a donc un plus petit élément, soit $N = \min(A)$

Cas 1 : $N = 0$

Alors, comme $N \in A$, on a $n_0 \leq 0$ et $P(0)$ est faux

Alors $n_0 = 0$ Contradiction avec " $P(n)$ est vrai"

Cas 2 : $N \neq 0$

Alors $N - 1 \in \mathbb{N}$

$N - 1 \notin A$ car $N - 1 < N$

Donc $N - 1 < n_0$ ou $P(n)$ vrai

Supposons $N - 1 < n_0$

$N \in A$ donc $N \geq n_0$

$N - 1 < n_0 < N$

Donc $N = n_0$

Or, $N \in A$ donc $P(n)$ est faux alors que $P(n)$ est vrai

Supposons $\begin{cases} P(n-1) \text{ vrai} \\ N-1 \geq n_0 \end{cases}$ Comme $N-1 \geq n_0, P(N-1) \implies P(N)$

Donc $P(N)$ est vrai

Or, $N \in A$ donc $P(N)$ est faux

Donc $A = \emptyset$

□

Sixième partie

Réurrences

Proposition (Récurrence Double): Soient P un prédicat sur $\mathbb{N}$ et $n_0 \in \mathbb{N}$

Si $\begin{cases} P(n_0) \text{ est vrai} \\ P(n_0 + 1) \text{ est vrai} \\ \forall n \geq n_0, P(n) \text{ et } P(n + 1) \implies P(n + 2) \end{cases}$
 Alors $\forall n \geq n_0, P(n)$ est vrai

Preuve:

On pose $\forall n \in \mathbb{N}, Q(n) : "P(n) \text{ et } P(n + 1) \text{ vrais}"$

$Q(n_0)$ est vrai

Soit $n \geq n_0$, on suppose $Q(n)$ vrai

On sait alors que $P(n + 2)$ est vrai

On sait par hypothèse de récurrence que $P(n + 1)$ est vrai

Donc $Q(n + 1)$ est vrai

□

Proposition (Récurrence Multiple): Soient P un prédicat sur $\mathbb{N}$ et $(p, n_0) \in \mathbb{N}^2$

Si $\begin{cases} \forall k \in \llbracket 0, p \rrbracket, P(n_0 - k) \text{ est vrai} \\ \forall n \geq n_0, (P(n) \text{ et } \dots P(n + p - 1)) \implies P(n + p) \end{cases}$
 Alors $\forall n \geq n_0, P(n)$ est vrai

Proposition (Récurrence Forte): Soient P un prédicat sur $\mathbb{N}$ et $n_0 \in \mathbb{N}$

Si $\begin{cases} P(n_0) \text{ est vrai} \\ \forall n \geq n_0, (P(n_0) \text{ et } \dots P(n - 1)) \implies P(n) \end{cases}$
 Alors $\forall n \geq n_0, P(n)$ est vrai

Preuve:

On pose $\forall n \in \mathbb{N}, Q(n) : "\forall k \in \llbracket n_0, n \rrbracket, P(k) \text{ vrai}"$

$Q(n_0)$ est vrai car $P(n_0)$ est vrai

Soit $n \geq n_0$, on suppose $Q(n)$ vrai

On sait que $\forall k \in \llbracket n_0, n \rrbracket, P(k)$ est vrai

Alors $P(n + 1)$ est vrai

Donc $\forall k \in \llbracket n_0, n + 1 \rrbracket, P(k)$ est vrai

Donc $Q(n + 1)$ est vrai

□

Septième partie

Divisibilité

Définition (Divisibilité): Soient $(a, b) \in \mathbb{Z}^2$
On dit que a divise b si il existe $k \in \mathbb{Z}$ tel que $b = ka$
On écrit $a|b$ et on dit que $\begin{cases} a \text{ est un diviseur de } b \\ b \text{ est un multiple de } a \end{cases}$

Proposition (Caractéristiques de la Divisibilité): $|$ est une relation d'ordre sur $\mathbb{Z}$
Ce n'est pas une relation totale

Proposition (Ordonnancement et Divisibilité): Soient $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$
Si $a|b$, $|a| \leq |b|$

Proposition (Divisibilité et Combinaison Linéaire): Soient $(a, b, c) \in (\mathbb{Z}^*)^3$
 $\begin{cases} a|b \\ a|c \end{cases} \implies \forall (k, l) \in \mathbb{Z}^2, a|(bk + cl)$

Preuve:
 $\begin{cases} b = au \text{ avec } u \in \mathbb{Z} \\ c = av \text{ avec } v \in \mathbb{Z} \end{cases}$
Soient $(k, l) \in \mathbb{Z}^2$
 $bk + cl = auk + avl = a(uk + vl)$
Donc $a|(bk + cl)$

□

Définition (Nombres Associés): Soient $(a, b) \in \mathbb{Z}^2$

a et b sont associés si $a = b$ ou $a = -b$

Proposition (Nombres Associés et Divisibilité): Soient $(a, b) \in \mathbb{Z}^2$
 $a|b \iff -a|b \iff a|-b \iff -a|-b$

Huitième partie

Division Euclidienne

Proposition (Division Euclidienne dans $\mathbb{N}$): Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$

$$\exists!(q, r) \in \mathbb{N}^2, \begin{cases} a = bq + r \\ r \in [0, b[\end{cases}$$

Preuve:

Existence : On considère $A = \{q \in \mathbb{N} | qb \leq a\}$ A est non vide car $0 \in A$
 A est majoré : $\forall q \in A, q \leq a$ car $a \geq qb \geq q$

Soit $q = \max(A)$, on pose $r = a - bq$
 Comme a, b et $q \in \mathbb{N}, r \in \mathbb{Z}$
 $q \in A$ donc $qb \leq a$ donc $r \geq 0$
 $q + 1 > \max(A)$ donc $q + 1 \notin A$ donc $(q + 1)b > a$
 Donc $r < b$

Unicité : Soit $(q', r') \in \mathbb{N}^2$ tel que $\begin{cases} a = bq' + r' \\ 0 \leq r' < b \end{cases}$

On sait aussi que $a = bq + r$
 Donc $0 = b(q' - q) + r' - r$
 $-r' + r = b(q' - q)$

De plus, $\begin{cases} 0 \leq r < b \\ -b < -r \leq 0 \end{cases}$
 Donc $-b < r' - r < b$

Le seul multiple de b dans $] -b, b[$ est 0
 Donc $r' - r = 0$, donc $r = r'$
 et $b(q' - q) = 0$
 Or, $b \neq 0$ donc $q' - q = 0$ donc $q = q'$

□

Proposition (Division Euclidienne dans $\mathbb{Z}$): Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$

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

Preuve:

Existence :

Cas 1 : $a \in \mathbb{N}, b \in \mathbb{N}^*$

D'après ce qui précède, $\exists!(q, r) \in \mathbb{N}^2, \begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$

Comme $b \in \mathbb{N}^*$, on a bien $0 \leq r < |b|$
 $q \in \mathbb{N} \subset \mathbb{Z}$

Cas 2 : $a \in \mathbb{Z}, b \in \mathbb{N}^*$

Comme $-a \in \mathbb{N}, \exists!(q', r') \in \mathbb{N}^2, \begin{cases} -a = bq' + r' \\ 0 \leq r' < b \end{cases}$

Donc $a = b(-q') - r'$
 $= b(-q' - 1) - r' + b$

On pose $q = \begin{cases} -q' - 1 & \text{si } r \neq 0 \\ -q' & \text{si } r = 0 \end{cases}$ et $r = \begin{cases} -r' + b & \text{si } r' \neq 0 \\ r' & \text{si } r' = 0 \end{cases}$

On a bien $\begin{cases} a = bq + r \\ q \in \mathbb{Z} \\ 0 \leq r < |b| \end{cases}$

Cas 3 : $a \in \mathbb{N}, b \in \mathbb{Z}_-^*$

$\exists!(q', r') \in \mathbb{N}^2, \begin{cases} a = (-b)q' + r' \\ 0 \leq r' < -b \end{cases}$

On pose $\begin{cases} q = -q' \\ r = r' \end{cases}$

Et on a bien $\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$

Cas 4 : $a \in \mathbb{Z}^-, b \in \mathbb{Z}_-^*$

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

Donc $a = bq' - r'$
 $= b(q' + 1) - r' - b$

On pose $q = \begin{cases} q' + 1 & \text{si } r \neq 0 \\ q' & \text{si } r = 0 \end{cases}$ et $r = \begin{cases} -r - b' & \text{si } r' \neq 0 \\ r' & \text{si } r' = 0 \end{cases}$

On a bien $\begin{cases} a = bq + r \\ q \in \mathbb{Z} \\ 0 \leq r < |b| \end{cases}$

Unicité :

Soit $(q', r') \in \mathbb{Z}^2$ tel que $\begin{cases} a = bq' + r' \\ 0 \leq r' < |b| \end{cases}$ et $\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$

D'où $\begin{cases} b(q' - q) = r' - r \\ -|b| < r - r' < |b| \end{cases}$

Donc $r - r' = 0$

Donc $r' = r$ et $q' = q$

□

Définition (Quotient et Reste): Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$

D'après le théorème précédent, $\exists!(q, r) \in \mathbb{Z} \times \mathbb{N}, \begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$

On dit que q est le quotient et r le reste dans la division (euclidienne) de a par b

Proposition (Reste et Divisibilité): Soient $a \in \mathbb{Z}, b \in \mathbb{Z}^*$

On note r le reste de la division de a par b

$r = 0 \iff b|a$

Preuve:

On pose $a = bq + r, q \in \mathbb{Z}$

“ $\implies$ ” : Si $r = 0$, alors $\begin{cases} a = bq \\ q \in \mathbb{Z} \end{cases}$ donc $b|a$

“ $\impliedby$ ” : Si $b|a$, $\exists k \in \mathbb{Z}, a = bk$

Donc $\begin{cases} a = bk + 0 \\ 0 \leq 0 < |b| \end{cases}$

Par unicité du reste, $r = 0$

□

Neuvième partie

Arithmétique Modulaire

Définition (Congruences): Soient $(a, b) \in \mathbb{Z}^2, c \in \mathbb{N}^*$
On dit que a et b sont congrus modulo c si a et b ont le même reste dans la division par c
On note $a \equiv b[c]$

Proposition (Congruence et Relation D'Equivalence): La relation de congruence modulo c est une relation d'équivalence

REMARQUE (Classes d'Equivalence Modulo c):
On note $\mathbb{Z}/c\mathbb{Z}$ l'ensemble des classes d'équivalence modulo c
 $\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

Proposition (Modulo et Divisibilité): Soient $(a, b) \in \mathbb{Z}^2$ et $c \in \mathbb{N}^*$
 $a \equiv b[c] \iff c|b - a$

Preuve:
“ $\implies$ ” : On pose $\begin{cases} a = cq + r, q \in \mathbb{Z}, 0 \leq r < c \\ b = cq' + r', q' \in \mathbb{Z} \end{cases}$
Donc $b - a = c(q' - q)$
Donc $c|b - a$

“ $\impliedby$ ” : On pose $\begin{cases} a = cq + r, q \in \mathbb{Z}, 0 \leq r < c \\ b = cq' + r', q' \in \mathbb{Z}, 0 \leq r' < c \end{cases}$
 $b - a = c(q' - q) + r' - r$
 $-c \leq r' - r \leq c$

Si $r' - r \geq 0, r' - r$ est le reste de la division de $a - b$ par c
Donc $r' = r$ donc $a \equiv b[c]$

Si $r' - r < 0, r - r'$ est le reste de la division de $a - b$ par c
Donc $r' = r$ donc $a \equiv b[c]$

□

Proposition (Addition et Multiplication de Congruences): Soient $(a, b, x, y) \in \mathbb{Z}^4$ et $c \in \mathbb{N}^*$
On suppose $\begin{cases} a \equiv b[c] \\ x \equiv y[c] \end{cases}$

Alors $\begin{cases} a + x \equiv b + y[c] \\ ax \equiv by[c] \end{cases}$

Preuve:
 $c|b - a$ et $c|y - x$

Donc $c|(b - a + y - x)$
 Donc $c|(b + y - (a + x))$
 Donc $a + x \equiv b + y[c]$

On pose $\begin{cases} a = ck + b, k \in \mathbb{Z} \\ x = cl + y, l \in \mathbb{Z} \end{cases}$
 $ax = (ck + b)(cl + y)$
 $= by + cky + clk + c^2kl$
 $= by + c(ky + bl + clk)$
 Donc $ax \equiv by[c]$

□

Proposition (Critères de Divisibilité en Base 10): Soit $N \in \mathbb{N}$, on notera ses chiffres

$a_0 \dots a_n$

$$N = \sum_{k=0}^n 10^k a_k$$

Divisibilité par 2 :

$$N \text{ pair} \iff N \equiv 0[2]$$

$$\iff \sum_{k=0}^n 10^k a_k \equiv 0[2]$$

$$\iff a_0 \equiv 0[2] \text{ car } \forall k \geq 1, 10^k \equiv 0[2]$$

$$10^0 = 1 \equiv 1[2]$$

Divisibilité par 3 :

$$\forall k \in \mathbb{N}, 10^k \equiv 1^k \equiv 1[3] \text{ car } 10 \equiv 1[3]$$

$$3|N \iff N \equiv 0[3]$$

$$\iff \sum_{k=0}^n 10^k a_k \equiv 0[3]$$

Divisibilité par 9 :

$$\forall k \in \mathbb{N}, 10^k \equiv 1[9]$$

$$9|N \iff N \equiv 0[9]$$

$$\iff \sum_{k=0}^n 10^k a_k \equiv 0[9]$$

Divisibilité par 5 :

$$\begin{cases} 10^0 \equiv 1[5] \\ \forall k \in \mathbb{N}^*, 10^k \equiv 0[5] \end{cases}$$

$$5|N \iff a_0 \equiv 0[5]$$

$$\iff a_0 \in \{0, 5\}$$

Divisibilité par 11 :

$$10^0 \equiv -1[11]$$

$$\text{Donc } \forall k \in \mathbb{N}, 10^k \equiv (-1)^k[11]$$

$$N \equiv 0[11] \iff \sum_{k=0}^n (-1)^k a_k \equiv 0[11]$$

$$\iff a_0 - a_1 + a_2 \dots + (-1)^n a_n \equiv 0[11]$$

REMARQUE (Réécriture en Classes d'Equivalence):
 On peut réécrire le calcul précédent dans $\mathbb{Z}/11\mathbb{Z}$

$$\overline{N} = \overline{\sum_{k=0}^n 10^k a_k} = \sum_{k=0}^n \overline{10^k} \overline{a_k} = \sum_{k=0}^n \overline{(-1)^k} \overline{a_k}$$

REMARQUE (Opération dans $\mathbb{Z}/n\mathbb{Z}$):

Dans $\mathbb{Z}/n\mathbb{Z}$, on dispose $\left\{ \begin{array}{ll} \text{d'une addition :} & \overline{a} + \overline{b} = \overline{a+b} \\ \text{d'une multiplication :} & \overline{a} * \overline{b} = \overline{a*b} \end{array} \right.$

L'addition est commutative, associative, n'élément neutre $\overline{0}$ et l'opposé de $\overline{a}$ est $\overline{-a}$

La multiplication est commutative, associative, d'élément neutre $\overline{1}$ et distributive par rapport à +

Dixième partie

PCGD et PPCM

Définition (PGCD): Soient $(a, b) \in \mathbb{Z}^2$
 Le PGCD de a et b est le plus grand diviseur commun à a et b
 Il existe car $\mathcal{D} = \{d \in \mathbb{N} \mid d|a \text{ et } d|b\}$ est non vide car $a \in \mathcal{D}$
 $\mathcal{D}$ est majoré par $|a|$
 On le note $\text{PGCD}(a, b)$ ou $a \wedge b$

Proposition (Théorème d'Euclide): Soient $a \in \mathbb{Z}, b \in \mathbb{N}^*$
 Soit r le reste de la division de a par b
 $a \wedge b = b \wedge r$

Preuve:
 On pose $\begin{cases} d = a \wedge b \\ \varsigma = b \wedge r \\ a = bq + r \end{cases}$

$$\begin{cases} d|a \\ d|b \end{cases} \implies \begin{cases} d|a - bq \\ d|b \end{cases} \implies \begin{cases} d|r \\ d|b \end{cases} \implies d \leq \varsigma$$

$$\begin{cases} \varsigma|b \\ \varsigma|r \end{cases} \implies \begin{cases} \varsigma|bq + r \\ \varsigma|b \end{cases} \implies \begin{cases} \varsigma|a \\ \varsigma|b \end{cases} \implies \varsigma \leq d$$

Donc $d = \varsigma$

□

Proposition (PGCD et Diviseurs): Soient $(a, b) \in \mathbb{Z}^2$ et $d = a \wedge b$
 $\mathcal{D} = \{k \in \mathbb{Z} \mid k|a, k|b\}$
 $\forall k \in \mathbb{Z}, k \in \mathcal{D} \iff k|d$

Preuve:
 “ $\Leftarrow$ ” : Soit $k \in \mathbb{Z}$, on suppose $k|d$
 $d|a$ donc $k|a$
 $d|b$ donc $k|b$

Donc $k \in \mathcal{D}$

“ $\Rightarrow$ ” : Soit $k \in \mathcal{D}$
 On pose r_0 le reste de la division de a par b ,
 r_1 le reste de la division de b par r_0
 et $\forall n \in \mathbb{N}, r_{n+1}$ le reste de la division de r_{n-1} par r_n si $r_n \neq 0$

La suite (r_n) est décroissante, minorée par 0 et à valeurs entières
 Soit $N \in \mathbb{N}$ tel que $r_N = 0$ (si $N = 0$, on pose $r_{-1} = b$)

D'après la proposition précédente,
 $d = a \wedge b = b \wedge r_0 = r_0 \wedge r_1 \dots r_{N-1} \wedge r_N$
 $= r_{N-1} \wedge 0 = r_N$

On pose aussi $\forall n \in \llbracket 1, N-1 \rrbracket, r_{n-1} = r_n q_n + r_{n+1}$
 On en déduit que $\exists (\alpha_n, \beta_n) \in \mathbb{Z}^2, r_{N-1} = a\alpha_N + b\beta_N$

$$\begin{cases} k|a \\ k|b \end{cases} \implies k|a\alpha_N + b\beta_N \implies k|r_{N-1} \implies k|d$$

□

Définition (PPCM): Soit $(a, b) \in \mathbb{Z}^2$, on pose $M = \{k \in \mathbb{N} \mid a|k, b|k\}$
 $M \neq \emptyset$ car $ab \in M$
 $M \neq \emptyset$ donc admet un plus petit élément noté $\text{PPCM}(a, b)$ ou $a \vee b$

Proposition (Produit PGCD PPCM): $\forall (a, b) \in \mathbb{Z}^2, (a \wedge b)(a \vee b) = ab$

Preuve:

Voir paragraphe Facteurs Premiers

□

Proposition (Propriétés de $\wedge$ et $\vee$): $\wedge$ est commutative, associative sur $\mathbb{Z}^*$
 $\vee$ est commutative, associative sur $\mathbb{Z}^*$

Preuve:

Soient $(a, b, c) \in (\mathbb{Z}^*)^3, d = (a \wedge b) \wedge c, \varsigma = a \wedge (b \wedge c)$

$$\begin{cases} d|c \\ d|a \wedge b \end{cases} \implies \begin{cases} d|c \\ d|a \\ d|b \end{cases}$$

$$\begin{cases} \varsigma|a \\ \varsigma|b \wedge c \end{cases} \implies \begin{cases} \varsigma|a \\ \varsigma|b \\ \varsigma|c \end{cases}$$

On pose $\varepsilon = \text{PGCD}(a, b, c)$

On a $\begin{cases} d \leq \varepsilon \\ \varsigma \leq \varepsilon \end{cases}$

$$\begin{cases} \varepsilon|a \\ \varepsilon|b \\ \varepsilon|c \end{cases} \implies \begin{cases} \varepsilon|a \\ \varepsilon|b \wedge c \end{cases} \implies \varepsilon|a \wedge (b \wedge c) \implies \varepsilon \leq d$$

De même, on $\varepsilon \leq \varsigma$

Donc $d = \varepsilon = \varsigma$

□

Proposition (Théorème de Bézout): Soient $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, $d = a \wedge b$
 $\exists (u, v) \in \mathbb{Z}^2$, $d = au + bv$

Preuve:

On pose $A = \{au + bv \mid (u, v) \in \mathbb{Z}^2\}$

On veut montrer que $d \in A$

$a = a * 1 + b * 0$ donc $a \in A$

$b = a * 0 + b * 1$ donc $b \in A$

$0 = a * 0 + b * 0$ donc $0 \in A$

Soit $(x, y) \in A^2$

$x = au_1 + bv_1, (u_1, v_1) \in \mathbb{Z}^2$

$y = au_2 + bv_2, (u_2, v_2) \in \mathbb{Z}^2$

$x + y = a(u_1 + u_2) + b(v_1 + v_2) \in A$

Soit $x \in A, k \in \mathbb{Z}$

$x = au + bv, (u, v) \in \mathbb{Z}^2$

$kx = aku + bkv \in A$

Soit $n = \min(A \cap \mathbb{N}^*)$ ($|b| \in A \cap \mathbb{N}^*$)

Soit $x \in A$

Par division euclidienne de x par n :

$$\begin{cases} x = nq + r \\ q \in A, 0 \leq r < n \end{cases}$$

$$\begin{cases} x \in A \\ n \in A \end{cases} \implies \begin{cases} x \in A \\ -qn \in A \end{cases} \implies x - qn \in A \implies r \in A$$

$$\begin{cases} r < n \\ r \in A \end{cases} \implies r \leq 0$$

Donc $r = 0$

Donc $n \mid x$

D'où $A = n\mathbb{Z}$

$$\text{Or, } \begin{cases} a \in A \\ b \in A \end{cases} \implies \begin{cases} n \mid a \\ n \mid b \end{cases}$$

Cas particulier : $a \wedge b = d = 1$, alors 1 est le seul diviseur positif de a et b

Donc $n = 1$ donc $A = \mathbb{Z}$ donc $1 \in \mathbb{Z}$

Cas général : On pose $a' = \frac{a}{d} \in \mathbb{Z}$, $b' = \frac{b}{d} \in \mathbb{Z}$, $a' \wedge b' = 1$

D'après le cas particulier, $\exists (u, v) \in \mathbb{Z}^2$, $a'u + b'v = 1$

D'où $au + bv = d$

□

Proposition (Réciproque du Théorème de Bézout): Soient $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$
 On suppose qu'il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$

Alors $a \wedge b = 1$

Preuve:

On pose $d = a \wedge b$

$$\begin{cases} d|a \\ d|b \end{cases} \implies d|au + bv \implies d|1 \implies d = 1$$

□

Proposition (Théorème de Gauß): Soient $(a, b, c) \in \mathbb{Z}^3$ tels que $\begin{cases} a \wedge b = 1 \\ a|bc \end{cases}$
Alors $a|c$

Preuve:

D'après le théorème de Bézout,

$au + bv = 1$ avec $(u, v) \in \mathbb{Z}^2$

D'où $acu + bcv = c$

$$\begin{cases} a|acu \\ a|bcv \end{cases}$$

Donc $a|acu + bcv$

Donc $a|c$

□

REMARQUE (Inversion Modulo n):

Soit $x \in \mathbb{Z}$

$\exists? y \in \mathbb{Z}, xy \equiv 1[n]$

($\iff$ dans $\mathbb{Z}/n\mathbb{Z}, \bar{x} + \bar{y} = \bar{1}$?)

Avec $n = 4$:

x 0123

0 0000

1 0123

2 0202

3 0321

$$3x \equiv 2[4]$$

$$\iff 3 * 3x \equiv 3 * 2[4]$$

$$\iff x \equiv 2[4]$$

$$2x \equiv 1[4]$$

$$\implies 2 * 2x \equiv 2[4]$$

$$\implies 0 \equiv 2[4]$$

Proposition (Congruences et Nombres Premiers): Soit p un nombre premier
Alors $\forall x \in \mathbb{Z}, x \not\equiv 0[p] \implies \exists y \in \mathbb{Z}, xy \equiv 1[p]$

Preuve:

Soit $x \in \mathbb{Z}$ tel que $x \not\equiv 0[p]$

Soit $y \in \mathbb{Z}$

$$xy \equiv 1[p] \iff \exists u \in \mathbb{Z}, xy = 1 + pu$$

$$\iff \exists u \in \mathbb{Z}, xy - pu = 1$$

$$y \text{ existe} \iff x \wedge p = 1$$

$$\iff p \nmid x$$

□

Proposition (Inversibilité Modulo n): Soit $n \in \mathbb{N}^*, x \in \mathbb{Z}$
 x inversible modulo $n \iff x \wedge n = 1$

Preuve:

Voir précédent

□

Proposition (Petit Théorème de Fermat): Soit p premier, $a \in \mathbb{Z}$
 $a^p \equiv a[p]$

Preuve:

Cas 1 : $a \equiv 0[p]$

$$a^p \equiv 0^p[p]$$

$$a^p \equiv 0[p] \equiv a[p]$$

Cas 2 : $a \not\equiv 0[p]$

$$\text{Alors } a \wedge p = 1$$

On pose $\forall i \in \mathbb{N}^*, r_i$ le reste de la division de ia par p

Soit $i \in \llbracket 1, p-1 \rrbracket$

$$r_i = 0 \implies p \mid ia \implies p \mid i \text{ Contradiction}$$

$$\forall i \in \mathbb{N}^*, r_i \neq 0$$

Soit $(i, j) \in \llbracket 1, p-1 \rrbracket^2, i \neq j$

On suppose $r_i = r_j$, alors $ia \equiv ja[p]$

Or, $a \wedge p = 1$ donc a est inversible modulo p

Donc $a \equiv j[p]$ donc $i = j$ Contradiction

Ainsi, $r_1 \dots r_{p-1} \in \llbracket 1, p-1 \rrbracket$ distincts donc ils prennent toutes les valeurs de $\llbracket 1, p-1 \rrbracket$

$i \mapsto r_i$ est injective

$$\{r_1 \dots r_{p-1}\} = \llbracket 1, p-1 \rrbracket$$

$$\text{Donc } \prod_{k=1}^{p-1} r_k = (p-1)!$$

$$\text{Donc } \prod_{k=1}^{p-1} ia \equiv (p-1)! [p]$$

$$\text{Donc } (p-1)! a^{p-1} \equiv (p-1)! [p]$$

$$\text{D'où } (p-1)! \equiv 0[p] \iff p \mid 1 * 2 * 3 \cdots * (p-1)$$

$$\iff \exists i \in \llbracket 1, p-1 \rrbracket, p \mid i$$

$$\text{Donc } (p-1)! \not\equiv 0[p]$$

$$\text{Donc } (p-1)! \text{ est inversible modulo } p$$

$$\text{Donc } a^p \equiv 1[p]$$

$$\text{Donc } a^p \equiv a[p]$$

□

Onzième partie

Décomposition en Facteurs
Premiers

Définition (Nombre Premier): Soit $n \in \mathbb{N}$
 On dit que n est premier si
 $n \geq 2$
 les seuls diviseurs entiers de n sont 1 et n

Proposition (Infinité de Nombres Premiers): Il y a une infinité de nombres premiers

Preuve:

On suppose qu'il n'y a qu'un nombre fini de nombres premiers
 $p_1 < \dots < p_n$

On pose $N = p_n * \dots * p_1 + 1$
 $N > p_n$ donc N n'est pas premier
 N a d'autres diviseurs positifs que 1 et N
 N est divisible par un nombre entre 2 et $N - 1$

Soit $p = \min(\{k \in \llbracket 2, N - 1 \rrbracket \mid k \mid N\})$
 p est premier (Tout diviseur de p divise aussi N)
 $\exists i \in \llbracket 1, n \rrbracket, p_i = p$
 $p_i \mid N$
 $p_i \mid N - p_1 \dots p_n$
 $p_i \mid 1$ Contradiction

Donc il y a une infinité de nombres premiers

□

Proposition (Théorème Fondamental de l'Arithmétique): "Tout entier se décompose en un unique produit de nombres premiers"

Soient $n \in \mathbb{N}$ tel que $n \geq 2$ et $\mathcal{P}$ l'ensemble des nombres premiers

$\exists ! \nu : \mathcal{P} \longrightarrow \mathbb{N}$ telle que $\begin{cases} \{p \in \mathcal{P} \mid \nu(p) \neq 0\} \text{ est fini} \\ n = \prod_{p \in \mathcal{P}} p^{\nu(p)} \end{cases}$

Preuve:

Existence : Déjà vue : Récurrence Forte (Chapitre 9)

Unicité : Soit $n \geq 2$ et $\nu : \mathcal{P} \longrightarrow \mathbb{N}$ telle que

(*) $\prod_{p \in \mathcal{P}} p^{\mu(p)} = \prod_{p \in \mathcal{P}} p^{\nu(p)}$ avec $\begin{cases} \mu \neq \nu \\ M = \{p \in \mathcal{P} \mid \mu(p) \neq 0\} \text{ fini} \\ M = \{p \in \mathcal{P} \mid \nu(p) \neq 0\} \text{ fini} \\ n \text{ minimale pour cette propriété} \end{cases}$

Soit $p \in M, \mu(p) \neq 0$ donc $p \mid n$

Si $\nu(p) = 0, \forall q \in \mathbb{N}, p \wedge q = 1$ donc $p \mid 1$ Contradiction avec le théorème de Gauß

Donc on peut simplifier (*) par p
 On a alors 2 décompositions de $\frac{n}{p} < n$ Contradiction
 Donc n n'existe pas

□

Proposition (Divisibilité et Nombres Premiers): Soient $(, b, c) \in \mathbb{N}^3$ supérieurs à 2

On pose $a = \prod_{p \in \mathcal{P}} p^{\alpha(p)}$ et $b = \prod_{p \in \mathcal{P}} p^{\beta(p)}$

$a|b \iff \forall p \in \mathcal{P}, \alpha(p) \leq \beta(p)$

Preuve:

“ $\implies$ ” : On suppose $a|b, \exists k, b = ak$

On pose $k = \prod_{p \in \mathcal{P}} p^{\kappa(p)}$

et donc $b = \prod_{p \in \mathcal{P}} p^{\alpha(p)} \prod_{p \in \mathcal{P}} p^{\kappa(p)} = \prod_{p \in \mathcal{P}} p^{\alpha(p) + \kappa(p)}$

Par unicité de la décomposition en facteurs premiers,
 $\forall p \in \mathcal{P}, \beta(p) = \alpha(p) + \kappa(p) \geq \alpha(p)$

“ $\impliedby$ ” : On suppose $\forall p \in \mathcal{P}, \beta(p) \geq \alpha(p)$

On pose $\forall p \in \mathcal{P}, \kappa(p) = \beta(p) - \alpha(p) \in \mathbb{N}$

Tous les $\alpha(p)$ et $\beta(p)$ sont nuls à partir d'un certain rang

C'est donc le cas aussi pour les $\kappa(p)$

Donc on a le droit de former le produit

$\prod_{p \in \mathcal{P}} p^{\kappa(p)} \in \mathbb{N}$

On pose $k = \prod_{p \in \mathcal{P}} p^{\kappa(p)}$ et $ak = \prod_{p \in \mathcal{P}} p^{\alpha(p)} \prod_{p \in \mathcal{P}} p^{\kappa(p)} = \prod_{p \in \mathcal{P}} p^{\alpha(p) + \kappa(p)} = \prod_{p \in \mathcal{P}} p^{\beta(p)} = b$

□

Proposition (Produit de Facteurs Premiers, PGCD et PPCM): Avec les notations précédentes,

$a \wedge b = \prod_{p \in \mathcal{P}} p^{\min(\alpha(p), \beta(p))}$ et $a \vee b = \prod_{p \in \mathcal{P}} p^{\max(\alpha(p), \beta(p))}$

Corollaire: $(a \wedge b)(a \vee b) = ab$

Preuve:

$$\begin{aligned}
(a \wedge b)(a \vee b) &= \prod_{p \in \mathcal{P}} p^{\min(\alpha(p), \beta(p))} \prod_{p \in \mathcal{P}} p^{\max(\alpha(p), \beta(p))} \\
&= \prod_{p \in \mathcal{P}} p^{\min(\alpha(p), \beta(p)) + \max(\alpha(p), \beta(p))} \\
&= \prod_{p \in \mathcal{P}} p^{\alpha(p) + \beta(p)} = ab
\end{aligned}$$

□