UE : Arithmétique
LICENCE 2 - MI semestre 3
Crédits : 3
CM : 18 h
TD : 18 h
Responsable de l'activité : Dr ASSANE Abdoulaye, Maître de Conférences

PRE REQUIS : UE Algèbre 1 du semestre 1

Objectif :
- Consolider les notions d'arithmétique et de groupe sur Z.
- Compétences visées : Raisonner, démontrer, calculer, rédiger.

Contenu du cours :
I- Ensemble des entiers naturels, groupe
II- Arithmétique dans Z
III-Congruences dans Z

Chapitre 1 : Ensemble des entiers naturels, groupe
1.1 Propriétés de N
1.2 Principe de Récurrence
1.3 Groupes et congruences
Chapitre 2 : Arithmétique dans Z

Chapitre 3 : Congruences dans Z

Chap 1 : Ensemble des entiers naturels, groupe
1.1 Propriétés de $\mathbb{N}$

Introduction
L'arithmétique est l'étude des propriétés des nombres entiers, appelés aussi entiers
naturels.

L'ensemble $\mathbb{N}$ des entiers naturels est l'ensemble fondamental à partir duquel
se sont construites les mathématiques, nous admettrons l'existence de cet ensemble

ainsi que les trois propriétés qui le caractérisent :

N1 : L'ensemble $\mathbb{N}$ est un ensemble totalement ordonné qui admet l'entier 0 comme
plus petit élément.

N2 : Tout élément de n $\in \mathbb{N}$ admet un successeur, c'est-à-dire un élément $n_0 >$ n tel
qu'il n'existe aucun élément de N strictement compris entre n et n_0. (Montrer à titre
d'exercice que ce successeur est alors unique.)
Cela permet de définir l'entier $1 \in \mathbb{N}$ comme le successeur de 0, l'entier 2 comme le
successeur de 1, etc. Pour chaque entier n $\in \mathbb{N}$, on désigne par n + 1 le successeur
de n.

N3 : L'ensemble $\mathbb{N}$ obéit au principe de récurrence.

1. 2 Principe de récurrence

1.2.1 énoncé du principe
Soit A une partie de N vérifiant les deux conditions suivantes
1. $\exists n_0 \in$ N, $n_0 \in$ A,
2. $\forall n \geq n_0$, $[(n \in A) \Longrightarrow (n+1 \in A)]$.
alors $\forall n \geq n_0$, n $\in$ A.

Le principe de récurrence justifie ce qu'on appelle les démonstrations par récurrence,
qui ne concernent que les énoncés où interviennent des entiers.

1.2.2 Démonstration par récurrence simple

Soit à démontrer qu'un énoncé P(n) est vrai pour tout entier $n \geq n_0$.
Si on pose A = $\{n \in \mathbb{N}, \text{P(n) est vrai}\}$,
il suffit, en vertu du principe de récurrence, de démontrer que :

1. P(n_0) est vrai,
2. $\forall n \geq n_0$, $[P(n) \Longrightarrow P(n+1)]$.

exemple

démontrer par récurrence que

$\forall n \in \mathbb{N}$, $\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$

Soit P_n la propostion : $\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$

Montrons par récurrence que $\forall n \in \mathbb{N}, P_n$ est vraie

-initialisation

pour n=0, on a : $\sum_{k=0}^{0} k^2 = 0^2 = 0 = \frac{0(0+1)(2\times 0+1)}{6}$

donc P_0 est vraie

-hérédité

soit n>0, supposons P_n est vraie et montrons que P_{n+1} est aussi vraie

on a : $\sum_{k=0}^{n+1} k^2 = \sum_{k=0}^{n} k^2 + (n+1)^2$

comme P_n est vraie, alors $\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$

donc $\sum_{k=0}^{n+1} k^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2$

$= (n+1)\left[\frac{n(2n+1)}{6} + n + 1\right]$

$= (n+1)(\frac{2n^2+n+6n+6}{6})$

$= (n+1)\left(\frac{2n^2+7n+6}{6}\right)$

$\Delta = b^2 - 4ac = 49 - 48 = 1$

$x_1 = \frac{-7-1}{4} = -2, x_2 = \frac{-7+1}{4} = \frac{-3}{2}$

donc $2n^2 + 7n + 6 = 2(n+2)\left(n + \frac{3}{2}\right)$

$= (n+2)(2n+3)$

ainsi $\sum_{k=0}^{n+1} k^2 = \frac{(n+1)(n+2)(2n+3)}{6}$

$= \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}$ d'où P_{n+1} vraie

conclusion d'après le principe de la démonstration par récurrence

$\forall n \in \mathbb{N}$, $\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$

Il existe des variantes de démonstrations par récurrence :

1.2.3 : Récurrence double

Pour démontrer que P(n) est vrai pour tout $n \geq n_0$, il suffit de démontrer que

1. P(n_0) et P(n_0+1) sont vrais,
2. $\forall$n$\geq$ n_0, $[(P(n-1)$ et $P(n)) \Longrightarrow P(n+1)]$.

exemple
On considère la suite $(a_n)_{n\in\mathbb{N}}$
définie par : $\begin{cases} a_0=1=a_1 \\ a_{n+1}=a_n+\frac{2}{n+1}a_{n-1} \end{cases}$ montrer que $\forall n \in \mathbb{N}^\star, 1 \leq a_n \leq n^2$

preuve
soit P_n la proposition : $1 \leq a_n \leq n^2$
Montrons par récurrence que $\forall n \in \mathbb{N}^\star, P_n$ est vraie
-initialisation
pour n=1, on a $a_1 = 1$, et $1 \leq a_1 \leq 1^2 = 1$
donc P_1 est vraie
pour n=2 on a $a_2 = a_1 + \frac{2}{1+1}a_0$
$= 1+1$
$=2$
on a : $1 \leq a_2 = 2 \leq 2^2 = 4$ donc P_2 est aussi vraie
-hérédité
soit n>1, on suppose que P_n et P_{n+1} sont vraies et montrons que P_{n+2} est vraie
on a $a_{n+2} = a_{n+1} + \frac{2}{n+2}a_n$
comme P_n et P_{n+1} sont vraies alors
$1 \leq a_n \leq n^2$ et $1 \leq a_{n+1} \leq (n+1)^2$ $(\star)$
on a $\frac{2}{n+2} \leq \frac{2}{n+2}a_n \leq n^2\frac{2}{n+2}$ $(\star\star)$
$(\star) + (\star\star)$ on obtient

$$1 \leq 1+\frac{2}{n+2} \leq a_{n+1} + \frac{2}{n+2}a_n \leq (n+1)^2 + \frac{2n^2}{n+2}$$
$$1 \leq a_{n+2} \leq \frac{2n^2+(n+2)(n+1)^2}{n+2}$$
$$1 \leq a_{n+2} \leq \frac{2n^2+n^3+4n^2+5n+2}{n+2}$$
$$1 \leq a_{n+2} \leq \frac{n^3+6n^2+5n+2}{n+2}$$

on cherche à prouver $a_{n+2} \leq (n+2)^2$ et comme $a_{n+2} \leq \frac{n^3+6n^2+5n+2}{n+2}$,
alors il suffit de montrer que $\frac{n^3+6n^2+5n+2}{n+2} \leq (n+2)^2$ par transitivité
on va examiner le signe de

$$(n+2)^2 - \frac{n^3+6n^2+5n+2}{n+2} = \frac{(n+2)^3-\left(n^3+6n^2+5n+2\right)}{n+2}$$
$$=\frac{n^3+6n^2+12n+8-\left(n^3+6n^2+5n+2\right)}{n+2}$$

$= \frac{7n+6}{n+2} > 0$ donc $\frac{n^3+6n^2+5n+2}{n+2} \leq (n+2)^2$

par conséquent $1 \leq a_{n+2} \leq (n+2)^2$

d'où P_{n+2} est vraie

conclusion d'après le principe de récurrence double

$$\forall n \in \mathbb{N}^\star, 1 \leq a_n \leq n^2$$

exercice

On considère la suite (a_n)

définie par : $\begin{cases} a_0=1=a_1 \\ a_{n+1}=a_n+a_{n-1} \end{cases}$ montrer que $\forall n \in \mathbb{N}^\star, a_n \leq 2^{n-1}$

1.2.4 : Récurrence forte

Pour démontrer que P(n) est vrai pour tout n$\geq$ n_0, il suffit de démontrer que :

1. P(n_0) est vrai,
2. $\forall$n$\geq$ n_0, $[(\forall k \in [n_0, n]\,,\ P(k)) \Longrightarrow P(n+1)]$.

exemple

on definit une suite (v_n) par $v_0 = 1$

et $\forall n \geq 1, v_{n+1} = \sum_{k=0}^{n} v_k$

démontrer que $\forall n \geq 1, v_n = 2^{n-1}$

soit P_n la proposition : $v_n = 2^{n-1}$

Montrons par récurrence que $\forall n \in \mathbb{N}^\star, P_n$ est vraie

-initialisation

pour n=1, on a $v_1 = v_{0+1} = \sum_{k=0}^{0} v_k = v_0 = 1 = 2^{1-1}$

donc P_1 est vraie

-hérédité

soit n>1, on suppose que pour tout $1 \leq k \leq n$, P_k est vraie

$v_k = 2^{k-1}$

montrons que P_{n+1} est vraie

on a : $v_{n+1} = \sum_{k=0}^{n} v_k$, comme P_k pour tout $1 \leq k \leq n$, alors

on a : $v_k = 2^{k-1}$, $a$lors $v_{n+1} = \sum_{k=0}^{n} v_k = v_0 + \sum_{k=1}^{n} v_k$

$= 1 + \sum_{k=1}^{n} 2^{k-1}$ (rappel série géométrique

$U_{k_0} \times \frac{1-q^N}{1-q}$. $=1+\frac{1-2^n}{1-2}$

$=1+2^n-1$

$=2^n=2^{(n+1)-1}$

donc P_{n+1} est vraie

conclusion d'après le principe de la démonstration par récurrence

$$\forall n \geq 1, v_n = 2^{n-1}$$

exercice

soit f : $\mathbb{N} \longrightarrow \mathbb{N}$ une application injective telle que

$\forall n \in \mathbb{N}$,f(n)$\leq$n

Montrer par récurrence que $\forall n \in \mathbb{N}$,f(n)=n

1.3 Théorème : Propriété fondamentale de N

Toute partie non vide de $\mathbb{N}$ possède un plus petit élément.

Preuve : Soit A une partie non vide de $\mathbb{N}$.

Si $0 \in$ A, 0 est le plus petit élément de A.

Si $0 \notin$ A, alors $0 \in \mathbb{N} \setminus$ A, et il existe un entier $n_1 \in \mathbb{N}$ tel que

1.$[0, n_1] \subset \mathbb{N} \setminus$ A,

2. (n_1+1) $\in$ A qui signifie que

$\exists n_1 \in \mathbb{N}, [0, n_1] \subset \mathbb{N} \setminus$ A et $n_1+1 \notin \mathbb{N} \setminus$ A

En effet, si tel n'était pas le cas, on aurait

donc non ($\exists n_1 \in \mathbb{N}, [0, n_1] \subset \mathbb{N} \setminus$ A et $n_1+1 \notin \mathbb{N} \setminus$ A) est vraie

qui signifie $\forall n \in \mathbb{N}$, non ($[0, n] \subset \mathbb{N} \setminus$ A et n+1$\notin \mathbb{N} \setminus$ A)

$\iff$ $\forall n \in \mathbb{N}$,non($[0, n] \subset \mathbb{N} \setminus$ A) ou non($n_1+1 \notin \mathbb{N} \setminus$ A)

$\iff$ $\forall n \in \mathbb{N}$,non($[0, n] \subset \mathbb{N} \setminus$ A) ou non(non(n+1$\in \mathbb{N} \setminus$ A))

$\iff$ $\forall n \in \mathbb{N}$, non($[0, n] \subset \mathbb{N} \setminus$ A ou n+1$\in \mathbb{N} \setminus$ A

rappel (nonP ou Q) $\iff$ P$\Longrightarrow$Q

et non(P$\Longrightarrow$Q) $\iff$ P et nonQ

$\iff$ $\forall n \in \mathbb{N}, [0, n] \subset \mathbb{N} \setminus$ A$\Longrightarrow$n+1$\in \mathbb{N} \setminus$ A

comme $0 \in \mathbb{N} \setminus$ A, alors d'après le principe de la récurrence forte

$\forall n \in \mathbb{N}, n \in \mathbb{N} \setminus$ A$\Longrightarrow \mathbb{N} \setminus$ A=$\mathbb{N} \Longrightarrow A = \emptyset$ ce qui est absurde

donc l'assertion $\exists n_1 \in \mathbb{N}, [0, n_1] \subset \mathbb{N} \setminus$ A et $n_1+1 \notin \mathbb{N} \setminus$ A est vraie

par conséquent l'entier $n_1+1 \in A$ et il est le petit élément de A.

fin de la preuve

1.4 Coefficients binomiaux

1.4.1 Définition

Soient $0 \leq p \leq n$ deux entiers naturels.

On pose $\binom{n}{p} = \frac{n!}{p!(n-p)!}$, pour $p > n$ On pose $\binom{n}{p} = 0$.

Les nombres $\binom{n}{p}$ s'appellent coefficients binomiaux.

cas particuliers

$\binom{n}{0} = \frac{n!}{0!(n)!} = 1$

$\binom{n}{n} = \frac{n!}{n!(0!)} = 1$

$\binom{n}{1} = \frac{n!}{1!(n-1)!} = \frac{n(n-1)!}{1!(n-1)!} = n$

$\binom{n}{2} = \frac{n(n-1)}{2}$

1.4.2 Formules élémentaires

1) $\binom{n}{p} = \binom{n}{n-p}$ si $n \leq p$

en effef : $\binom{n}{n-p} = \frac{n!}{(n-p)!(n-(n-p))!} = \frac{n!}{p!(n-p)!} = \binom{n}{p}$

2) formule du triangle de pascal

$\binom{n+1}{p} = \binom{n}{p} + \binom{n}{p-1}$ $\forall n \geq 1, p \geq 1$.

en effet

$$\begin{aligned}\binom{n}{p} + \binom{n}{p-1} &= \frac{n!}{p!(n-p)!} + \frac{n!}{(p-1)!(n-(p-1))!} \\ &= \frac{n!}{p!(n-p)!} + \frac{n!}{(p-1)!(n+1-p)!} \\ &= \frac{(n+1-p)n!}{p!(n+1-p)(n-p)!} + \frac{pn!}{p(p-1)!(n+1-p)!} \\ &= \frac{(n+1-p)n!}{p!(n+1-p)!} + \frac{pn!}{p!(n+1-p)!} \\ &= \frac{pn!+(n+1-p)n!}{p!(n+1-p)!} = \frac{(n+1)n!}{p!(n+1-p)!} = \frac{(n+1)!}{p!(n+1-p)!} = \binom{n+1}{p}\end{aligned}$$

fin de la preuve.

3) $\binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1}$

preuve

$$\begin{aligned}\frac{n}{p}\binom{n-1}{p-1} &= \frac{n}{p}\frac{(n-1)!}{(p-1!(n-1-(p-1))!} \\ &= \frac{n(n-1)!}{p(p-1)!(n-1-(p-1))!} \\ &= \frac{n!}{p!(n-p)!} = \binom{n}{p}\end{aligned}$$ fin de la preuve.

4) $\binom{n}{p} = \frac{p+1}{n-p}\binom{n}{p+1}$ (exercice)

	p=0	1	2	3	4	5	6	7	8	9	10	11	12
n=0	1												
1	1	1											
2	1	2	1										
3	1	3	3	1									
4	1	4	6	4	1								
5	1	5	10	10	5	1							
6	1	6	15	20	15	6	1						
7	1	7	21	35	35	21	7	1					
8	1	8	28	56	70	56	28	8	1				
9	1	9	36	84	126	126	84	36	9	1			
10	1	10	45	120	210	252	210	120	45	10	1		
11	1	11	55	165	330	462	462	330	165	55	11	1	
12	1	12	66	220	495	792	924	792	495	220	66	12	1

5) $\binom{n}{p} = \frac{n-p+1}{p}\binom{n}{p-1}$ (exercice)

6) $\binom{n+m}{r} = \sum_{k+p=r} \binom{n}{k}\binom{m}{p}$

preuve

$(1+x)^{n+m} = (1+x)^n\ (1+x)^m$

$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \quad$ et $\quad (1+x)^m = \sum_{l=0}^{m} \binom{n}{l} x^l$

$$(1+x)^{n+m} = (1+x)^n\ (1+x)^m$$
$$= \left(\sum_{k=0}^{n} \binom{n}{k} x^k\right) \times \left(\sum_{l=0}^{m} \binom{m}{l} x^l\right)$$
$$= \sum_{p=0}^{n+m} \left(\sum_{l+k=p} \binom{m}{l}\binom{n}{k}\right) x^p$$
$$= \sum_{p=0}^{n+m} \binom{n+m}{p} x^p$$

donc $\sum_{l+k=p} \binom{m}{l}\binom{n}{k} = \sum_{p=0}^{n+m} \binom{n+m}{p}$

on déduit la formule

$\binom{n+m}{r} = \sum_{k+p=r} \binom{n}{k}\binom{m}{p}$

1.4.3 Formule du binôme de Newton

$\forall$ a; b $\in \mathbb{Z}$, $(a+b)^n = \sum_{p=0}^{n} \binom{n}{p} a^p b^{n-p}$, $\forall n \in \mathbb{N}$

preuve

par récurrence soit P_n la propriété : $(a+b)^n = \sum_{p=0}^{n} \binom{n}{p} a^p b^{n-p}$

-initialisation

pour n=0, $(a+b)^0 = 1$ et $\sum_{p=0}^{0} \binom{n}{p} a^p b^{n-p} = \binom{0}{0} a^0 b^0 = 1$

donc P_0 est vraie.

-hérédité

soit n>0, supposons P_n vraie, montrons que P_{n+1} est aussi vraie

on a : $(a+b)^{n+1} = (a+b)^n(a+b) = a\,(a+b)^n + b\,(a+b)^n$

$$= a\sum_{p=0}^{n} \binom{n}{p} a^p b^{n-p} + b\sum_{p=0}^{n} \binom{n}{p} a^p b^{n-p}$$

$$= \sum_{p=0}^{n} \binom{n}{p} a^{p+1} b^{n-p} + \sum_{p=0}^{n} \binom{n}{p} a^p b^{n+1-p}$$

dans la première expression on pose l=p+1

$$= \sum_{l=1}^{n+1} \binom{n}{l-1} a^l b^{n+1-l} + \sum_{p=0}^{n} \binom{n}{p} a^p b^{n+1-p}$$

dans la seconde expression on pose l=p

$$= \sum_{l=1}^{n+1} \binom{n}{l-1} a^l b^{n+1-l} + \sum_{l=0}^{n} \binom{n}{l} a^l b^{n+1-l}$$

$$= \sum_{l=1}^{n} \binom{n}{l-1} a^l b^{n+1-l} + \binom{n}{n} a^{n+1} b^0 + \binom{n}{0} a^0 b^{n+1} + \sum_{l=1}^{n} \binom{n}{l} a^l b^{n+1-l}$$

$$= \sum_{l=1}^{n} \binom{n}{l-1} a^l b^{n+1-l} + a^{n+1} + b^{n+1} + \sum_{l=1}^{n} \binom{n}{l} a^l b^{n+1-l}$$

$$= \sum_{l=1}^{n} \left(\binom{n}{l-1} + \binom{n}{l} \right) a^l b^{n+1-l} \quad + a^{n+1} + b^{n+1}$$

$$= \sum_{l=1}^{n} \binom{n+1}{l} a^l b^{n+1-l} \quad + a^{n+1} + b^{n+1}$$

$$= \sum_{l=0}^{n+1} \binom{n+1}{l} a^l b^{n+1-l} \quad \text{donc } P_{n+1} \text{ est vraie}$$

par conséquent $(a+b)^n = \sum_{p=0}^{n} \binom{n}{p} a^p b^{n-p}$, $\forall n \in \mathbb{N}$

1.5 Groupes

1.5.1 Une loi de composition interne,

ou opération sur un ensemble E est simplement
une application de E $\times$ E dans E,
que l'on note $(x, y) \longmapsto$ x$\star$ y.

1.5.2 Définition

Un groupe est la donnée d'un ensemble G muni d'une opération possédant les
propriétés suivantes.

1. Elle est associative.
2. Elle possède un élément neutre.
3. Tout élément de G admet un symétrique.

Si de plus l'opération est commutative, on dit que le groupe est commutatif ou abélien.

1.5.3 Définition

Soit G_1 et G_2 deux groupes.
Une application u de G_1 dans G_2 est un morphisme de groupes si
$\forall$(x, y) $\in$ $G_1\times$ G_2, $u(xy) = u(x)u(y)$.
Si de plus l'application u est une bijection, on dit que u est un isomorphisme de groupes, les groupes G_1 et G_2 sont alors dits isomorphes.

1.5.4 Definition (ordre d'un groupe)

Un groupe G est dit fini si l'ensemble G est fini. Le nombre d'éléments de G est alors appelé ordre du groupe G noté $|G|$.

exemples de groupes finis
(G=$\{f_1, f_2, f_3, f_4\}$; $\circ$) $\circ$ désigne la composition des applications
où $f_1 : \mathbb{R} \longrightarrow \mathbb{R}, x \longmapsto x$
$f_2 : \mathbb{R}^\star \longrightarrow \mathbb{R}^\star, x \longmapsto \frac{1}{x}$
$f_3 : \mathbb{R}^\star \longrightarrow \mathbb{R}^\star, x \longmapsto -\frac{1}{x}$
$f_4 : \mathbb{R} \longrightarrow \mathbb{R}, x \longmapsto -x$
déterminer la table de la loi $\circ$

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

$f_2 \circ f_2\,(x) = f_2\left(\frac{1}{x}\right) = \frac{1}{\frac{1}{x}} = x \Longrightarrow f_2 \circ f_2 = f_1$

$f_2 \circ f_3\,(x) = f_2\left(-\frac{1}{x}\right) = \frac{1}{-\frac{1}{x}} = -x \Longrightarrow f_2 \circ f_3 = f_4$

$f_2 \circ f_4\,(x) = f_2\,(-x) = -\frac{1}{x} \Longrightarrow f_2 \circ f_4 = f_3$

d'après la table la loi $\circ$ est une loi de composition interne sur G
car $\forall$f,g$\in$G, f$\circ$g$\in$G
On voit (G,$\circ$) est un groupe d'ordre 4 : $|G| = 4$

1.6 Sous-groupes
1.6.1 Définition
Soit G un groupe. Une partie H de G est un sous-groupe de G si les conditions suivantes sont réalisées
1. $\forall$(x, y) $\in$ H $\times$ H, xy $\in$ H. (stabilité pour la loi)
2. 1 $\in$ H. 1ou 1_G désigne l'élément neutre de G.(élément neutre)
3. $\forall$x $\in$ H, $x^{-1} \in$ H. (élément symétrique)

1.6 congruence modulo un sous groupe
1.6.1 congruence à gauche
Soit G un groupe et soit H un sous groupe de G.
On définint les deux relations suivantes
$\forall$ x; y $\in$ G,
1. $x \underset{g}{\equiv} y(\text{modH}) \Longleftrightarrow x^{-1}y \in H$
C'est une relation d'équivalence. On l'appelle la congruence à gauche modulo H.
-réflèxivité
$x^{-1}x = 1_G \in H \Longrightarrow x \underset{g}{\equiv} x(\text{modH})$
-symétrie
$x \underset{g}{\equiv} y(\text{modH}) \Longrightarrow x^{-1}y \in H$

$\Longrightarrow (x^{-1}y)^{-1} = y^{-1}x \in H \Longrightarrow y \underset{g}{\equiv} x(\text{modH})$

-transitivité
si $x \underset{g}{\equiv} y(\text{modH})$ et $y \underset{g}{\equiv} z(\text{modH})$

on a $x^{-1}y \in H$ et $y^{-1}z \in H \Longrightarrow (x^{-1}y)(y^{-1}z) = x^{-1}z \in H$
la loi du groupe est notée multiplicativement $x \star y$ est noté xy
donc $x \underset{g}{\equiv} z(\mathrm{mod}H)$

La classe d'un élément x de G est
$\overline{x}_g = \mathrm{cl}_g(x) = \left\{ y \in G \text{ tels que } x \underset{g}{\equiv} y(\mathrm{mod}H) \right\} = xH$
en effet : $x^{-1}y \in H \iff \exists h \in H \iff x^{-1}y = h \iff y = xh, h \in H$
or $\{xh, h \in H\} = xH$ donc $\overline{x}_g = xH$
L'ensemble quotient de G par cette relation d'équivalence, c'est à dire l'ensemble
des différentes classes d'équivalence se note (G/H)g.

1.6.2 congruence à droite
On définit de manière duale la congruence à droite modulo H par
$x \underset{d}{\equiv} y(\mathrm{mod}H) \iff yx^{-1} \in H$
C'est une relation d'équivalence. On l'appelle la congruence à droite modulo H.
$\overline{x}_d = \mathrm{cl}_d x = \left\{ y \in G \text{ tels que } x \underset{d}{\equiv} y(\mathrm{mod}H) \right\} = Hx$
L'ensemble quotient de G par cette relation d'équivalence, c'est à dire l'ensemble
des différentes classes à droite se note (G/H)d.

On remarquera les deux ensembles quotients (G/H)g et (G/H)d sont différents en général mais ils ont le même nombre d'éléments. En effet l'application
$\theta : xH \longmapsto Hx^{-1}$ de (G/H)g dans (G/H)d est une bijection .

1. elle est bien définie car si xH=yH, alors $x^{-1}y \in H$,
$x^{-1} \in Hy^{-1}$
donc $Hx^{-1} = Hy^{-1}$

2. elle est surjective,
$\forall Hy \in (G/H)$d, $H(y^{-1})^{-1} = Hy$

3. elle est injective,
si $Hx^{-1} = Hy^{-1}$, alors il existe h,k$\in$H,
$hx^{-1} = ky^{-1}$ donc $xh^{-1} = yk^{-1}$ et xH=Hy

Donc les deux ensembles ont le même cardinal, $|(G/H)g|$
$= |(G/H)d|$. Ce nombre commun s'appelle l'indice de H dans G et se note $[G : H]$.

De même toutes les classes d'équivalence modulo H ont le même nombre d'élément qui est égal à l'ordre de H.

En effet l'application φ :H$\longrightarrow$xH,h $\longmapsto$xh est une bijection.

1

$\forall$h,k$\in$H, xh=xk$\Longrightarrow$h=k en composant par x^{-1} à gauche, donc φ est injective.

$\forall$ z$\in$xH, $\exists$ h$\in$H, z=xh et donc φ(h)=z, d'où φ est surjective

1.6.3 Définition

Un sous-groupe H du groupe G est dit distingué ou invariant ou normal et

l'on écrit alors H$\lhd$ G si

$\forall$ x $\in$ G; $\forall$ h $\in$ H, on a $xhx^{-1} \in$ H

Exercice

Montrer que si f : G $\longrightarrow$ G'

un morphisme de groupes, alors Ker f $\lhd$ G:

preuve

$\forall$ x $\in$ G; $\forall$ h $\in$ kerf, $xhx^{-1} \in$?kerf

$f(xhx^{-1})$ =f(x)f(h)f(x^{-1}) car f est un morphisme de groupes

=f(x)$1_{G'}$f(x^{-1}) car h$\in$kerf

=f(x)f(x^{-1}) car $1_{G'}$est l'élément neutre de G'

=f(x)(f(x))$^{-1}$ car f est un morphisme de groupes

=$1_{G'}$ donc $xhx^{-1} \in$ kerf

conclusion Ker f $\lhd$ G:

Exercice

Soit H un sous-groupe du groupe G: Montrer que les quatre propriétés suiv-

antes sont équivalents :

(i) H $\lhd$ G

(ii) $\forall$ x $\in$ G; xH$\subset$ Hx
(iii) $\forall$ x $\in$ G; xH = Hx
(iv) (G$\diagup$H)g = (G$\diagup$H)d
preuve
(i) $\Longleftrightarrow$ (ii)
.($\Longrightarrow$)
on suppose H $\lhd$ G, montrons que $\forall$ x $\in$ G; xH$\subset$ Hx
$\forall$ x $\in$ G,$\forall$h$\in$H, on a xhx$^{-1} \in$ H car H $\lhd$ G
alors $\exists k \in H$, xhx$^{-1} = k \Longrightarrow xh = kx \in Hx$ donc
$xh \in Hx \Longrightarrow$xH$\subset$ Hx
.($\Longleftarrow$), on suppose $\forall$ x $\in$ G; xH$\subset$ Hx, montrons que H $\lhd$ G
$\forall$ x $\in$ G,$\forall$h$\in$H, a-t-on xhx$^{-1} \in$ H?
comme xH$\subset$ Hx, alors xh$\in$Hx, donc il existe k$\in$H tel que
xh=kx$\Longrightarrow$xhx$^{-1} = k \in$H, donc H $\lhd$ G
conclusion (i) $\Longleftrightarrow$ (ii)

Exercice : Le groupe symétrique S_n

Soit E un ensemble quelconque. On note S_E l'ensemble des bijections de E dans E.

1. Montrer que (S_E; o) est un groupe généralement non abélien, appelé le groupe symétrique de E .

Si E = E_n est un ensemble fini de n éléments, alors on note $S_{E_n} = S_n$:
on note En =$\{1; 2; ...; n\}$ Le cardinal de S_n est n! Les éléments
$\in S_n$ seront représentés par des tableaux :
exemple pour n=3 on am 6 éléments :

i=$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $t_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $t_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$t_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

1) Donner la table de S_3:

$\circ \curvearrowright$	i	t_1	t_2	t_3	σ_1	σ_2
i	i	t_1	t_2	t_3	σ_1	σ_2
t_1	t_1	i	σ_1	σ_2		
t_2	t_2					
t_3	t_3					
σ_1	σ_1					
σ_2	σ_2					

$t_1 \circ t_1(1) = t_1(1) = 1,\ t_1 \circ t_1(2) = t_1(3) = 2,\ t_1 \circ t_1(3) = t_1(2) = 3$
$\Longrightarrow t_1 \circ t_1 =$i
$t_1 \circ t_2(1) = t_1(3) = 2,\ \ t_1 \circ t_2(2) = t_1(2) = 3,\ \ t_1 \circ t_2(3) = t_1(1) = 1$
$\Longrightarrow t_1 \circ t_2 = \sigma_1$
$t_1 \circ t_3(1) = t_1(2) = 3,\ t_1 \circ t_3(2) = t_1(1) = 1,\ \ t_1 \circ t_3(3) = t_1(3) = 2$
$\Longrightarrow t_1 \circ t_3 = \sigma_2$
$t_1 \circ \sigma_1(1) = t_1(2) = 3,\ t_1 \circ \sigma_1(2) = t_1(3) = 2,\ \ t_1 \circ \sigma_1(3) = t_1(1) = 1$
$\Longrightarrow t_1 \circ \sigma_1 = t_2$
$t_1 \circ \sigma_2(1) = t_1(3) = 2,\ t_1 \circ \sigma_2(2) = t_1(1) = 1,\ \ t_1 \circ \sigma_2(3) = t_1(2) = 3$
$\Longrightarrow t_1 \circ \sigma_2 = t_3$
$t_2 \circ t_1 = \sigma_2,\ \ t_2 \circ t_2 =$i, $\ t_2 \circ t_3 = \sigma_1,\ t_2 \circ \sigma_1 = t_3,\ t_2 \circ \sigma_2 = t_1$
$t_3 \circ t_1 = \sigma_1,\ \ t_3 \circ t_2 = \sigma_2,\ \ t_3 \circ t_3 =$i, $t_3 \circ \sigma_1 = t_1,\ t_3 \circ \sigma_2 = t_2$
$\sigma_1 \circ t_1 = t_3,\ \ \sigma_1 \circ t_2 = t_1,\ \ \sigma_1 \circ t_3 = t_2,\ \sigma_1 \circ \sigma_1 = \sigma_2,\ \sigma_1 \circ \sigma_2 =$i
$\sigma_2 \circ t_1 = t_2,\ \ \sigma_2 \circ t_2 = t_3,\ \ \sigma_2 \circ t_3 = t_1,\ \sigma_2 \circ \sigma_1 =$i, $\sigma_2 \circ \sigma_2 = \sigma_1$
on pose H=$\{i, t_1\}$, A = $\{i, \sigma_1, \sigma_2\}$
a) Montrer que H et A sont des sous groupes de S3
preuve pour H
-stabilité
on a : i$\circ$i=i, i$\circ t_1 = t_1, t_1 \circ i = t_1, t_1 \circ t_1 = i$ donc H est stable
pour la loi $\circ$
-élément neutre
1_{S_3} =i$\in$H
-symétrisation
on a : $\mathrm{i}^{-1} = i \in H$, $t_1 \circ t_1 = i \Longrightarrow t_1^{-1} = t_1 \in H$ donc
H est stable par symétrisation
conclusion H est un sous groupe de S_3

b) Déterminer l'ensemble quotient (S_3/H)g et (S_3/H)d
(S_3/H)g=$\{$xH,x $\in S_3\}$ H=$\{i, t_1\}$
iH=H, t_1H=H, t_2H=$\{t_2, \sigma_2\}$, t_3H=$\{t_3, \sigma_1\}$, σ_1H=$\{\sigma_1, t_3\}$, σ_2H=$\{\sigma_2, t_2\}$
donc (S_3/H)g=$\{$H, $\{t_2, \sigma_2\}$, $\{\sigma_1, t_3\}\}$
on deduit $[S_3 : H] = 3$
determiner (S_3/H)d et le comparer à (S_3/H)g
c) H est- t- il un sous groupe distingué de S3?
d) Montrer que A $\lhd$ S3
1.7 **Groupe quotient**
1.7.1 Définition
Soit H un sous groupe distingué du groupe G: Alors

d'après l'exercice précé-
dent (G/H)g = (G/H)d : On note G/H cet ensemble.
On définit dans G/H une multiplication par :
$\forall$ x; y $\in$ G; xH yH = xyH.
Pour cette loi, G/H est un groupe appelé groupe quotient
de G par H.

1.7.2 Théorèime (Lagrange)
Dans un groupe fini, l'ordre d'un sous-groupe divise l'ordre
du groupe.
On a : $|G| = |H|\ [G : H]$
Preuve :
Soit G un groupe fini et H un sous-groupe de G. On sait
que les classes d'équivalence modulo H forment une partition de G,
donc $G = \bigcup_{x_i \in G} x_i H$ comme $x_i H \cap x_j H = \emptyset$ si x_i et
x_j ne sont pas dans la même classe.
soit m le nombre de classe et $x_1, x_2, ..., x_m$ les
représentants des m classes distinctes.
On a : $|G| = \sum_{i=1}^{m} |x_i H| = \sum_{i=1}^{m} |H| = m\,|H|$
par conséquent $|G| = |H|\ [G : H]$ car $m = [G : H]$
L'ensemble G étant fini, il n'y a qu'un nombre fini m de
classes, on en déduit que l'ordre de G est égal à m fois
l'ordre de H : $|G| = m \times |H|$ or m= $[G : H]$ d'où le résultat.

exemple dans le groupe S_3
on a $|S_3| = 6$, les diviseurs de 6 sont 1,2, 3, 6
les sous groupes possible pur S_3
ordre 1 $\{id\}$
ordre 2 $\{id, t_1\}$

ordre 3 $\{id, \sigma_1, \sigma_2\}$

1.7.3 Théorème d'isomorphisme
Soit f : G $\longrightarrow$ G'un morphisme de groupes.
Alors il existe un isomorphisme unique
f : G/kerf $\longrightarrow$ Imf tel que f (xN) = f(x) ,$\forall$ x $\in$ G, où N = kerf

Remarques
1. On retiendra le théorème d'isomorphisme sous sa forme pratique

- G/kerf $\simeq$Imf

1.7.4 Définition
Soit G un groupe fini et soit x $\in$ G.
On appelle ordre de x l'ordre du sous groupe noté <x> $=\{x^k, k \in \mathbb{Z}\}$ de G engendré par x.

1.7.5 Théorème
Soit G un groupe fini, soit x $\in$ G et soit m l'ordre de x. Alors
1. m divise l'ordre de G.
2. m est le plus petit entier positif tel que $x^m = 1$.
3. Les éléments 1, x, x^2, . . . , x^{m-1} sont tous distincts dans G.
4. <x> $=\{1, x, x^2, ..., x^{m-1}\}$.

Preuve :
1. Résulte du théorème de Lagrange.
2. Si m = 1, c'est évident.
On suppose m$\geq$ 2,

(a) On montre qu'il existe au moins un entier l , $1 \leq l \leq$ m tel que $x^l = 1$.
Soit A $= \{x, x^2, ..., x^m, x^{m+1}\} \subset$<x>,
comme l'ordre de <x> est égal à m, il existe au moins deux éléments égaux dans A,
$\exists$k, $\exists l$, 1 $\leq$k$\leq$ m, 1$\leq$ k +l$\leq$ m + 1 vérifiant $x^k = x^{k+l}$,
on en déduit $1 \leq l \leq$ m et $x^l = 1$.
(b) Soit n le plus petit entier positif tel que $x^n = 1$, il résulte de (a) que (n$\leq l \leq$ m).
Montrons que <x>$= \{1, x, x^2, ..., x^{n-1}\}$.
Soit en effet k $\in \mathbb{Z}$,
la division euclidienne de k par n
s'écrit k = nq + r, 0$\leq$r$\leq$ n -1,
ce qui donne $x^k = x^{nq}x^r = (x^n)^q x^r = x^r \in \{1, x, x^2, ..., x^{n-1}\}$,

donc <x>$\subset \{1, x, x^2, ..., x^{n-1}\}$
il en résulte m =$|< x >|$ $\leq$card $\{1, x, x^2, ..., x^{n-1}\} \leq$ n,
c'est-à-dire , en vertu de (a): n$\leq l \leq$ m et m$\leq$ n
m =$|< x >|$ =card $\{1, x, x^2, ..., x^{n-1}\}$=n
Cela démontre 2. et 4 et $.< x >= \{1, x, x^2, ..., x^{n-1}\}$
3. Résulte de l'égalité m =card $\{1, x, x^2, ..., x^{n-1}\}$
exemple de calcul de l'ordre d'un élément d'un groupe fini
dans S_3
on considère $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$
calculer l'ordre de σ_1 : $\min\{n \in \mathbb{N}^\star, \sigma_1^n = id = 1_{S_3}\}$
$\sigma_1^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \neq 1_{S_3}, \sigma_1^3 = \sigma_1\sigma_1^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = id = 1_{S_3}$
donc $|\sigma_1| = 3$ qui divise bien $|S_3|$

Chapitre 2 ARITHMETIQUE DANS $\mathbb{Z}$

2.1 La division euclidienne

2.1.1Théorème
Soit a et b deux éléments de $\mathbb{Z}$, avec b > 0.
Il existe un couple unique $(q, r) \in \mathbb{Z}^2$ vérifiant : a=bq+r et
0$\leq r < b$
On dit que q est le quotient et r le reste de la division
euclidienne de a par b

Preuve : a=bq+r et $0 \leq r < b-$

Existence. L'ensemble A = $\{a - bk, k \in \mathbb{Z}\} \cap \mathbb{N}$ n'est pas
vide, en effet
si a$>$ 0, on prend k = 0, et
si a$\leq$ -1, il suffit de prendre k = a,
de sorte que a - bk = a(1 - b) $\geq$0.
Il résulte alors de la propriété fondamentale de $\mathbb{N}$ que A
possède un plus petit élément r.
Par définition de A, il existe q $\in \mathbb{Z}$ tel que r = a - bq.
Supposons r $\geq$b, on écrit alors
0 $\leq$r - b = a - bq - b = a - b(q+1)) $\in$ A,
mais on a 0 $\leq$r - b $<$ r,ce qui contredit le fait que r est le
plus petit élément de A.

Unicité.
Supposons a = bq_1+ r_1 =bq_2+ r_2 ,
avec 0≤ r_1 < b et 0≤ r_2 < b.
Si $q_1 \neq q_2$, supposons q_1 - $q_2 \geq 1$
a = bq_1+ r_1 =bq_2+ r_2 $\Longrightarrow$b(q_1 - q_2) = r_2 - r_1
commme q_1 - $q_2 \geq 1$ $\Longrightarrow$ b≤b(q_1 - q_2) = r_2 - r_1< r_2
$\Longrightarrow$b<r_2
ce qui contredit l'hypothèse r_2 < b.
On en déduit q_1 =q_2 et
alors r_2 - r_1 =b(q_1 - q_2)=0
il s'en suit que r_1 = r_2.
On peut étendre la division euclidienne au cas où b $\neq$ 0 est de signe quelconque.

2.1.2 Théorème
Soit a et b deux éléments de $\mathbb{Z}$, avec b $\neq$ 0, il existe un couple unique $(q, r) \in \mathbb{Z}^2$
vérifiant a=bq+r et $0 \leq r < |b|$

Preuve : Si b < 0, on effectue la division euclidienne de a par -b selon le théorème 1
a = $(-b)$q + r, 0 r < -b, puis on remplace b par -b et q par -q, le reste r est inchangé.

2.2 Les sous-groupes de $\mathbb{Z}$

La première conséquence de la division euclidienne dans $\mathbb{Z}$ concerne la forme spécifique des sous-groupes de$\mathbb{Z}$.

Soit n $\in \mathbb{Z}$, on sait que l'ensemble n$\mathbb{Z}$ des multiples de n est un sous-groupe de $\mathbb{Z}$.
Nous allons démontrer la réciproque de ce résultat, réciproque qui aura des conséquences importantes par la suite.

2.2.1 Théorème
Soit H un sous-groupe de $\mathbb{Z}$, il existe un entier unique n≥ 0 tel que H = n$\mathbb{Z}$ = $\{nk, k \in \mathbb{Z}\}$.
Preuve :

Si H= $\{0\}$, on écrit H = $0\mathbb{Z}$.
Si H $\neq \{0\}$, on pose
A =$\{x \in H, x \geq 1\}$ = H $\cap \mathbb{N}^{\star}$.
Soit x un élément non nul de H, alors -x$\in$H
on a :
ou bien x $\geq$1$\Longrightarrow$x$\in A$
ou bien -x$\geq$ 1$\Longrightarrow -$x$\in A$
donc A $\neq \emptyset$.
Soit n$\geq$ 1 le plus petit élément de A, (propriété fondamentale de $\mathbb{N}$),
montrons que H = n$\mathbb{Z}$.
Comme n $\in$ H, il résulte que n$\mathbb{Z} \subset$ H.
Réciproquement, soit m $\in$ H, effectuons la division euclidienne
de m par n : m = nq + r, 0$\leq$ r $<$ n.
comme m $\in$ H et n $\in$ H, H étant un sous-groupe de $\mathbb{Z}$,
alors r = m - nq $\in$ H.
D'où r = 0, sinon r serait un élément de A strictement plus petit que n.
On a donc m = nq $\in$ n$\mathbb{Z}$. D'où H$\subset$ n$\mathbb{Z}$.
On en déduit H = n$\mathbb{Z}$.
Unicité
Si n$\mathbb{Z}$ = m$\mathbb{Z}$, m est multiple de n, et n est multiple de m,
d'où m = $\pm$n.

3 Diviseurs, nombres premiers

3.1 Définition

Soit a et b deux entiers, avec b $\neq$ 0.
1. Lorsque le reste de la division euclidienne de a par b
est nul, on dit que a est multiple
de b, que b est un diviseur de a ou que b divise a.
2. Lorsque a $\neq$0, un diviseur b de a est un diviseur propre
de a si b $\neq \pm 1$ et b $\neq \pm$a.

3. Un entier p est premier,
ou est un nombre premier, si p$\geq$ 2 et si p n'admet pas de
diviseur propre.

Remarques
1. Le nombre 1 n'est pas premier.

2. Remarquons que (b divise a) équivaut à$((-b)$ divise a),
on se ramènera donc le plus
souvent au cas où b > 0.
3. Tout entier b $\neq 0$ divise 0 puisque $0 =$ b $\times$ 0.

2.2.3 Proposition
Soit a, b et c dans $\mathbb{Z}$, si c divise a et b , alors c divise
am+bn pour tout m, n dans $\mathbb{Z}$

3.2 Théorème
Soit un entier a$\geq$ 2, le plus petit diviseur de a strictement
supérieur à 1 est
premier. Cela implique que tout entier a$\geq$ 2 admet au
moins un diviseur premier.
Preuve :
Désignons par D' (a) l'ensemble des éléments de
D(a)(ensemble des diviseurs de a) strictement supérieurs
à 1,
comme a > 1, a $\in$D'(a) donc D'(a) $\neq \emptyset$.
Soit p le plus petit élément de D' (a).
Si p n'est pas premier il possède un diviseur propre q,
on a donc $1 <$ q $<$ p et q $\in$D'(p) $\subset$D'(a),
ce qui contredit le fait que p est le plus petit élément de
D'(a).

3.3 Corollaire
L'ensemble des nombres premiers est infini.
Preuve :
Par l'absurde, supposons cet ensemble fini égal à
$\{p_1, p_2, ..., p_q\}$.
L'entier a = $p_1p_2 \ . \ . \ . \ p_q + 1$ n'est divisible par aucun des pi
mais admet un diviseur premier
d'après le théorème 3.2, d'où contradiction car a est premier et a$\notin \{p_1, p_2, ..., p_q\}$

3.4 Plus grand commun diviseur ou pgcd

3.4.1 Definition
Soit a et b deux entiers non tous deux nuls (cf. remarque 1. ci-dessous),
il est facile de vérifier que l'ensemble

H(a, b) = $\{au + bv, (u, v) \in \mathbb{Z}^2\} = a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ non réduit à $\{0\}$.

Il existe donc un entier unique d $\geq$1 tel que

(1) H(a, b)=$\{au + bv, (u, v) \in \mathbb{Z}^2\} = d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$.

Cet entier d est appelé le plus grand commun diviseur ou pgcd de a et b.

Étant donné un entier k $\in \mathbb{Z}$, on a donc l'équivalence suivante :

$\exists\,(u, v) \in \mathbb{Z}^2,\ k = au + bv \iff k$ est multiple de pgcd(a,b).

3.4.2 Théorème (Propriété caractéristique du pgcd)

Soit a et b deux entiers non tous deux nuls.

Un entier positif d est le pgcd de a et b si et seulement si

les deux conditions suivantes sont satisfaites :

1. d est un diviseur commun de a et b,

2. tout diviseur commun de a et b divise d.

Preuve :

Soit d le pgcd de a et b,

alors H(a, b) = $\{au + bv, (u, v) \in \mathbb{Z}^2\}$ =d$\mathbb{Z}$.

1. Comme a $\in a\mathbb{Z} + b\mathbb{Z}$ et b $\in a\mathbb{Z} + b\mathbb{Z}$, d divise a et b.

2. Comme d $\in a\mathbb{Z} + b\mathbb{Z}$, il existe deux entiers u et v de $\mathbb{Z}$ tels que d = au + bv, donc tout

entier c divisant a et b divise d.a=kc, b=qc$\Longrightarrow d$ =kc+qc=c(k+q)

Réciproquement, soit d' un entier positif vérifiant les conditions 1. et 2.,

la condition 1. implique d'après ce qui précède

que d'divise d,

et la condition 2. implique que d divise d',

d'où d' = d.

On voit donc que

(pgcd (a, b) = d équivaut à (D(a)$\cap$ D(b) = D(d)),

c'est-à-dire que d est le plus grand élément de D(a) $\cap$ D(b).

Cela justifie l'appellation de plus grand commun diviseur de a et b.

3.4.3. Définition

On dit que deux entiers a et b sont premiers entre eux si leur seul diviseur commun positif est 1, autrement dit si leur pgcd est égal à 1.

Remarquons qu'il résulte de cette définition que l'entier 1 est premier avec tout autre entier.

Le théorème suivant, dû au mathématicien français Étienne Bézout (1730-1783), synthétise ce qui précède

3.4.4 Théorème (Bézout)

Soit a, et b deux entiers.

1. Soit d$\geq$ 1 un diviseur commun de a et b, alors d est le pgcd de a et b si et seulement

s'il existe deux entiers u et v tels que : au + bv = d. (1)

2. Les entiers a et b sont premiers entre eux si et seulement s'il existe deux entiers u et v

tels que au + bv = 1. (2)

Cette relation est appelée identité de Bézout.

Preuve :

1. Si d = pgcd (a, b), l'existence de u et v vient de la définition de d.

Réciproquement, si d divise a et b et vérifie (1), tout diviseur commun de a et b divise d par combinaison

donc d = pgcd (a, b) d'après le théorème 3.4.2.

2. Il en résulte que la condition (2) est nécessaire. Elle est suffisante car elle implique que tout diviseur commun c > 0 de a et b divise 1 donc c = 1, ce qui veut dire que pgcd (a, b) = 1.

3.4.5 Proposition

Soit a et b deux entiers, et soit d 1 un diviseur commun de a et b.

Si on écrit (1) a =da_1 et b = db_1,

alors d = pgcd (a, b) si et seulement si pgcd (a_1, b_1) = 1.

Preuve : Soit u et v deux entiers, on a l'équivalence

(d = au + bv) $\Longleftrightarrow$ (1 = a_1u + b_1v).

3.4.6 Proposition

Soit p un nombre premier et soit a $\in \mathbb{Z}$. Alors ou bien p et a sont premiers entre eux, ou bien p divise a.

Preuve :

Soit d = pgcd (a, p). Puisque d divise p et p est premier, d est égal à 1 ou à p.

Si d = 1, p et a sont premiers entre eux.

Si d = p, p divise a.

3.4.7 Proposition

Soit a et b deux entiers, avec b $\neq$ 0. Si r est le reste de la division euclidienne

de a par b, on a pgcd (a, b) = pgcd (b, r).

Preuve : Si a = bq + r, (la double inégalité 0 $\leq$r$<$ b ne nous servira pas ici), les diviseurs

communs de a et b sont les diviseurs communs de b et r.

3.4.8 Lemme de Gauss

Parmi les corollaires les plus importants du théorème de Bézout figure le résultat suivant, connu sous le nom de lemme de Gauss.

3.4.9 Théorème

(Lemme Gauss) (Carl Friedrich Gauss, 1777-1855) Soit a, b et c trois entiers.

Si a divise le produit bc et si a est premier avec b, alors a divise c

preuve

a divise le produit bc,alors bc=ka

a est premier avec b,alors $\exists u, v, au + bv = 1 \Longrightarrow auc + bcv = c$

on a a$|bc$ et a$|auc$ donc a $|auc + bcv = c$

Attention

Si a et b ne sont pas premiers entre eux, la conclusion du lemme de Gauss est

fausse ; par exemple, 6 divise 3 $\times$ 4 mais ne divise ni 3 ni 4.

application : résolutions des équations de congruences

ax$\equiv b \bmod(n) \iff \exists k \in \mathbb{Z}, ax - nk = b$ (1)

si a et n sont premiers entre eux

il existe u et v tels que au+nv =1$\Longrightarrow aub + nvb = b$ (2)

(1)(1)-(2)$\Longrightarrow a(x - ub) = n(k - vb) \Longrightarrow n$ divise $a(x - ub)$ et comme

n est premier avec a, alors n divise $x - ub \Longrightarrow \exists q \in \mathbb{Z}, nq = x - ub$

x=nq+ub donc $S_{\mathbb{Z}} = \{nq + ub, q \in \mathbb{Z}\}$

exemple

résoudre dans $\mathbb{Z}$ l'équation de congruence

5x$\equiv 3 \bmod(17) \Longrightarrow \exists k \in \mathbb{Z}, 5x - 17k = 3$ (1)

comme 5 et 17 sont pre17miers entre eux $\exists u, v \in \mathbb{Z}, 5u + 17v = 1$

par l'algorithme d'euclide

17=5$\times$3 + 2

5=2$\times$2 + 1

ainsi 1=5-2$\times$2

1=5-(17-5×3) × 2

1=5×7− 17×2

par multipliant par 3 on obtient

5×21− 17×6 = 3 (2)

(1)-(2)$\Longrightarrow 5(x-21) = 17(k-6) \Longrightarrow$ 17 divise $5(x-21)$

et comme 17 est premier avec 5 alors 17 divise $(x-21)$

ainsi l existe q$\in \mathbb{Z}, x-21 = 17q \Longrightarrow x = 17q+21$

conclusion $S_{\mathbb{Z}} = \{17q+21, q \in \mathbb{Z}\}$

3.5 Plus petit commun multiple ou ppcm

3.5.1 Definition

Soit a et b deux entiers, on sait que l'intersection des sous-groupes a$\mathbb{Z}$ et b$\mathbb{Z}$ de $\mathbb{Z}$ est un

sous-groupe de $\mathbb{Z}$. Il existe donc un unique entier m$\geq$ 0 tel

que

(1) a$\mathbb{Z}\cap$b$\mathbb{Z}$ = m$\mathbb{Z}$.

Cet entier m est appelé le plus petit commun multiple ou ppcm de a et b, on le note

m = ppcm (a, b). La caractérisation qui suit résulte directement de la définition.

3.5.2 Proposition (Propriété caractéristique du ppcm)

Soit a et b deux entiers. Un entier m$\geq$ 0 est le ppcm de a et b si et seulement si les deux conditions suivantes sont satisfaites :

1. m est un multiple commun de a et b,
2. tout multiple commun de a et b est un multiple de m.

La proposition suivante ramène le calcul du ppcm à celui du pgcd.

2

3.5.3 Proposition

Soit a et b deux entiers non tous deux nuls et soit d leur pgcd . Si on pose

a = da$_1$, b = db$_1$, alors ppcm (a, b) = d$|a_1b_1|$. En particulier, on a l'égalité

pgcd (a, b) × ppcm (a, b) = $|ab|$.

Preuve :

Supposons pour simplifier que a et b sont non négatifs, et soit $m_1 = da_1b_1$.

Les entiers a_1 et b_1 sont premiers entre eux.

Soit M un multiple commun de a =da_1 et b = db_1. Si on pose M = dM_1, alors M_1 est un

multiple commun de a_1 et b_1, donc,

d'après le lemme de Gauss, un multiple du produit a_1b_1.

Il en résulte que M = dM_1 est un multiple de m1 = da1b1. Il est clair

d'autre part que m1 est lui-même un multiple commun de a et b.

On a donc prouvé, que m_1 = ppcm (a, b). Il est clair en fin que dm_1 = da_1db_1 = ab.

2.5 Décomposition d'un entier en facteurs premiers

2.5.1 Proposition

Soit p un nombre premier. Si p divise un produit q_1q_2 . . . q_n de n entiers, il

existe au moins un indice i $\in \{1, 2, ..., n\}$ tel que p divise q_i.

Preuve : Par récurrence. Supposons n = 2 et p divise q_1q_2.

Ou bien p divise q_2 ou bien p est premier avec q_2 donc divise q_1 d'après le lemme de Gauss. Supposons le résultat établi pour n - 1, si p divise q_1q_2 . . . q_n, alors ou bien p divise q_n ou bien p est premier avec q_n donc divise q_1q_2 . . . q_{n-1}, d'après le lemme de Gauss, le résultat découle alors de l'hypothèse de récurrence.

2.5.2 Corollaire

Soit p un nombre premier. Si p divise un produit p_1p_2 . . . p_n de n nombres

premiers, il existe un indice i $\in \{1, 2, ..., n\}$ tel que p = p_i.

2.5.3 Théorème (Théorème fondamental de l'arithmétique)

Tout entier a > 1 s'écrit de

façon unique : a= $p_1^{t_1}p_2^{t_2}$ . . . $p_n^{t_n}$

les entiers pi sont premiers et vérifient $p_1 < p_2 < \cdots < p_n$,

les entiers t_i sont positifs.

Preuve :

1. Existence. Soit p_1 le plus petit diviseur premier de a.

L'ensemble des entiers α positifs tels que (p^{α}

divise a) est fini, soit α_1 son plus grand élément, alors α_1 est l'unique entier positif tel que

(p^{α_1} divise a) et (p^{α_1+1} ne divise pas a),

on écrit $a = p_1^{\alpha_1} a_1$.

Si $a_1 = 1$, c'est terminé. Si $a_1 > 1$, on recommence.

Soit p_2 le plus petit diviseur premier de a_1,

et $\alpha_2 \geq 1$ le plus grand entier tel que $p_2^{\alpha_2}$ divise a_1.

On pose $a = p_1^{\alpha_1} p_2^{\alpha_2} a_2$, et on remarque que $p_2 > p_1$ et que $a > a_1 > a_2$.

On recommence l'opération jusqu'à obtenir un quotient $a_n = 1$, ce qui arrive au bout

d'un nombre fini d'opérations puisque

$a > a_1 > a_2 > \cdots > a_k > \cdots 1$.

Unicité. Supposons $a = p_1^{t_1} p_2^{t_2} \ldots p_n^{t'_n} = q_1^{t'_1} q_2^{t'_2} \ldots q_m^{t'_m}$ (1)

p_i, q_i sont premiers et vérifient $p_1 < p_2 < \cdots < p_n$ et $q_1 < q_2 < \cdots < q_n$

et où les t_i et les t_i' sont des entiers ≥ 1. Il faut montrer que

(a) $m = n$,

(b) $\forall i = 1, 2, \ldots, n$, $p_i = q_i$

i,

(c) $\forall i = 1, 2, \ldots, n$, $t_i = t_i$'.

(a) D'après le corollaire 15, chaque pi est égal à l'un des q_i

et chaque q_i égal à l'un des p_i. La famille des p_i coïncide donc avec celle des q_i d'où $m = n$.

(b) Comme de plus les pi et les q_i sont rangés par ordre croissant, on a $p_i = q_i$

pour chaque $i = 1, 2, \ldots, n$.

(c) Supposons qu'il existe un indice i tel que $t_i \neq t'_i$ i, par exemple $t_i < t'_i$.

En divisant les deux membres de (1) par $p_i^{t_i}$, on en déduit que p_i divise un produit de nombres premiers tous différents de lui-même, ce qui est impossible d'après le corollaire 15.

Chapitre 3

Arithmétique des congruences

3.1 Les anneaux quotients $\mathbb{Z}/n\mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z} = \{\overline{x}, x \in \mathbb{Z}\}$ ici G=$\mathbb{Z}$ et H=n$\mathbb{Z}$ (G/H)g=$\{xH, x \in G\}$ $\overline{x}$ =xH=x+n$\mathbb{Z}$

$\forall x \in \mathbb{Z}, \overline{x} = x + n\mathbb{Z} = \{nk + x, k \in \mathbb{Z}\}$

soit x=nq+r, $0 \leq r < n$ la division euclidienne de x par n

$\overline{x} = x + n\mathbb{Z} = nq + r + n\mathbb{Z} = r + n\mathbb{Z} = \overline{r}$ $nq + n\mathbb{Z} = n\mathbb{Z}$ car $nq \in n\mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z} = \{\overline{x}, x \in \mathbb{Z}\} = \{\overline{r}, 0 \leq r < n\} = \left\{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\right\}$

on a $\overline{x} = \overline{y} \iff x - y \equiv 0 \bmod(n) \iff$ x-y est divisible par n

3.1.1 Proposition

Soit a et b deux entiers, et soit n un entier positif, alors on a dans $\mathbb{Z}/n\mathbb{Z}$

($\overline{a}$=$\overline{a\prime}$ et $\overline{b}$=$\overline{b\prime}$) $\Longrightarrow \overline{aa'} = \overline{bb'}$

Preuve : Il existe q_1 et q_2 dans $\mathbb{Z}$ tels que a = a' + q_1n et b = b' + q_2n, ce qui donne

ab = a'b' + n(a'q_2 + b'q_1 + nq_1q_2).

Ceci justifie la définition suivante

3.1.2 Définition

Étant données deux classes $\alpha, \beta \in \mathbb{Z}/n\mathbb{Z}$,

on définit la classe produit $\alpha\beta \in \mathbb{Z}/n\mathbb{Z}$ comme suit.

1. On choisit un représentant a $\in \alpha$ et un représentant b $\in \beta$,

c'est à dire deux entiers a et b véri ant $\overline{a} = \alpha$ et $\overline{b} = \beta$.

2. On pose $\alpha\beta = \overline{ab}$.

3.1.3 Proposition

La multiplication définie ci-dessus fait du groupe quotient $\mathbb{Z}/$n$\mathbb{Z}$ un anneau commutatif d'élément neutre $\overline{0}$ et d'élément unité $\overline{1}$.

L'anneau $\mathbb{Z}/$n$\mathbb{Z}$ est appelé anneau quotient de l'anneau $\mathbb{Z}$ par le sous groupe n$\mathbb{Z}$.

exemple

table de (+) et (×) dans $\mathbb{Z}/4\mathbb{Z} = \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\right\}$

$+ \curvearrowright$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$			

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$				
$\overline{1}$				
$\overline{2}$				
$\overline{3}$	0		$\overline{2}$	$\overline{1}$

$\overline{1}$+$\overline{3}$ =$\overline{4} = \overline{0}$ car 0 est le reste de la division de 4 par 4 $3\times2 = 6 = 4+2 = 2$

$3\times3 = 9 = 8 + 1 = 1$

$\overline{2} + \overline{3} = \overline{5} = \overline{4+1}$ =$\overline{1}$

3.1.4 Théorème

Soit n un entier positif, soit q $\in \mathbb{Z}$ et soit $\overline{q}$ la classe de q modulo n.

1. On a l'équivalence

$(\overline{q} \in (Z/nZ))^{\times} \iff$ (pgcd $(q,n) = 1$) $.(Z/nZ))^{\times}$ ensemble des élments inversibles

$(Z/nZ))^{\times} = \left\{x \in Z/nZ, \exists y \in Z/nZ, xy = \overline{1}\right\}$ $\overline{xy} = \overline{1} \iff xy \equiv 1 \bmod(n)$

On dit alors que l'entier q est inversible modulo n.

2. L'anneau Z/nZ est un corps si et seulement si n est premier. On le désigne alors par F_n.

Preuve :

Soit q un élément inversible de Z/nZ, il existe l$\in \mathbb{Z}$ tel que $\overline{q}\overline{l} = 1$, c'est-à-dire qu'il

existe k $\in \mathbb{Z}$ tel que ql$= 1 + nk$, ce qui implique pgcd $(q,n) = 1$.

Réciproquement,

si pgcd $(q,n) = 1$, il existe d'après le théorème de Bézout deux entiers u et v

vérifiant $qu + nv = 1$, d'où, modulo n, $\overline{q}\ \overline{u} + \overline{n}\ \overline{v} = \overline{1}$, mais $\overline{n} = 0$, d'où $\overline{q}$ $\overline{u} = 1$, c'est-à-dire que q est inversible dans l'anneau Z/nZ.

Enfin, Z/nZ est un corps si et seulement si pour tout q$\in \{1, ..., n-1\}$, q $\in (Z/nZ)^{\times}$, c'est-à-

dire pgcd $(q,n) = 1$, ce qui signifie que n est premier.

Remarque :

La démonstration précédente montre que si q est inversible modulo n, son inverse peut

être calculé à l'aide de l'algorithme d'Euclide

Exercice

Déterminer l'inverse de 5 modulo 12, de 8 modulo 27 et de 14 modulo 25.

5 est premier avec 12 donc $\overline{5}$ est inversible dans $\frac{\mathbb{Z}}{12\mathbb{Z}}$

calcul de son inversible par l'algorithme d'euclide

12=5×2 + 2

5=2×2 + 1

on a 1=5-2×2

1=5-(12-5×2) × 2

$\underline{1=5\times5 - 12 \times 2}$

en modulo 12 ona $\overline{1} = \overline{5} \times \overline{5} - \overline{12} \times \overline{2}$ or $\overline{12} = \overline{0}$

donc $\overline{1} = \overline{5} \times \overline{5}$ ainsi $(\overline{5})^{-1} = \overline{5}$, alors l'inverse de 5 est 5 en modulo 12.

application
équations de congruences
ax=bmod(p) avec a premier avec p
soit a^{-1}

3.1.5 Théorème Petit théorème de Fermat (Pierre de Fermat(1601-1665)

Étant donné un nombre premier p et un entier a $\in \mathbb{Z}$,
on a $a^p \equiv a \pmod p$. si pgcd(p,a)=1 alors $a^{p-1} \equiv 1 \pmod p$

Preuve :
Soit a$\in \mathbb{Z}$. On sait qu'ou bien a est multiple de p ou bien a est premier avec p.
Soit $\overline{a}$ la classe de a modulo p.
Si a est multiple de p, a^p est aussi multiple de p, on a donc $a^p \equiv a \equiv 0 \pmod p$.
Si pgcd (a,p)=1, alors a $\in (Z/pZ)^\times$ d'après le théorème 3.3 .
Or $(Z/pZ)^\times$ est d'ordre p -1 donc $\overline{a}^{p-1} = \overline{1}$ d'après le corollaire 2.7.
Ceci s'écrit $a^{P-1} \equiv 1 \pmod p$, il en résulte $a^P \equiv a \pmod p$.

Exemple
1.Donner le reste de la division de 10^{15} par 13
2. 100^{1000} par 13 et
3.) $10^{121} + 11^{99}$ par 7.

résolution
on a : 13 est un nombre premier qui ne divise pas 100
donc d'après le petit théorème de Fermat
$100^{13-1} = 100^{12} \equiv 1 \bmod(13)$ on a $1000 \div 12 = 83.333$
et $1000 - 12 \times 83 = 4$
donc $1000 = 12 \times 83 + 4$
ainsi $100^{1000} = 100^{12\times 83+4} = (100^{12})^{83} \times 100^4 \equiv 100^4 \bmod(13)$ car $100^{12} \equiv 1 \bmod(13)$
on a : $100 \div 13 = 7.6923$
$100 - 13 \times 7 = 9$
$100 = 13 \times 7 + 9 \Longrightarrow 100 \equiv 9 \bmod(13)$
$100^4 \equiv 9^4 \bmod(13)$
on a $9^2 = 81$ et $81 \div 13 = 6.2308$

et $81 - 13 \times 6 = 3.0$
$81 = 13 \times 6 + 3$
$9^2 \equiv 3 \bmod(13) \Longrightarrow 9^4 = (9^2)^2 \equiv 3^2 = 9 \bmod(13)$
donc $100^{1000} \equiv 9 \bmod(13)$ comme $0 \leq 9 < 13$
alors le reste de la division euclidienne de 100^{1000} par 13 est 9.

3.1.6 Système chinois des restes)
Un système de congruences est un système de la forme :

$$(Sc) \begin{cases} x \equiv a_1 \bmod(m_1) \\ x \equiv a_2 \bmod(m_2) \\ \quad ... \\ x \equiv a_k \bmod(m_k) \end{cases}$$ où les a_i, et les m_i sont des entiers donnés

si les m_i sont premiers entre eux deux à deux
le système admet une solution unique modulo : $M=m_1 \times m_2 \times .... \times m_k$
donnée par :

$x=a_1M_1y_1+a_2M_2y_2 + ...+a_kM_ky_k$ S

avec $M_i = M/m_i$, $y_i = M_i^{-1} \bmod(m_i)$
$S_{\frac{\mathbb{Z}}{M\mathbb{Z}}} = \{\overline{x}\}$ avec $x=a_1M_1y_1+a_2M_2y_2 + ...+a_kM_ky_k$
$S_{\mathbb{Z}} = \{x + nM, n \in \mathbb{Z}\}$
Exemple
Resoudre dans Z le système suivant :

$$\begin{cases} x \equiv 4 \bmod(5) \\ x \equiv 3 \bmod(6) \\ x \equiv 2 \bmod(7) \end{cases}$$

5, 6 et 7 sont deux à premies entre eux
Posons $M=5 \times 6 \times 7 = 210$
$M_1 = \frac{M}{5} = 42$, $M_2 = \frac{M}{6} = 35$, $M_3 = \frac{M}{7} = 30$
la solution $x=a_1M_1y_1+a_2M_2y_2+a_3M_3y_3$
$y_1 = 42^{-1} \bmod(5)$
$y_2 = 35^{-1} \bmod(6)$
$y_3 = 30^{-1} \bmod(7)$
calcul de y_1 par l'algorithme d'euclide
$42=5 \times 8 + 2$
$5=2 \times 2 + 1 \Longrightarrow 1 = 5 - 2 \times 2$
$1=5-(42-5 \times 8) \times 2$

$1=5\times 17-42\times 2$
ainsi en modulo(5) $\overline{1}=\overline{42}\times\overline{(-2)}$
donc $42^{-1}\bmod(5)=-2=3\bmod(5)\Longrightarrow y_1=3$
calcul de $y_2=35^{-1}\bmod(6)$ par l'algorithme d'euclide avec 35 et 6
$35=6\times 5+5$
$6=5+1\Longrightarrow 1=6-5$
$1=6-(35-6\times 5)$
$1=6\times 6-35$
ainsi en modulo(6) $\overline{1}=\overline{35}\times\overline{(-1)}$
donc $y_2=35^{-1}\bmod(6)=-1\bmod(6)=5\bmod(6)\Longrightarrow y_2=5$
calcul de $y_3=30^{-1}\bmod(7)$ par l'algorithme d'euclide avec 30 et 7
$30=7\times 4+2$
$7=2\times 3+1\Longrightarrow 1=7-2\times 3$
$1=7-(30-7\times 4)\times 3$
$1=7\times 13-30\times 3$
ainsi en modulo(7) $\overline{1}=\overline{30}\times\overline{(-3)}$
donc $y_3=30^{-1}\bmod(7)=-3\bmod(7)=4\bmod(7)\Longrightarrow y_3=4$
ansi la solution du système en modulo $5\times 6\times 7=210$ est

$$\begin{cases} x\equiv 4\bmod(5)\\ x\equiv 3\bmod(6)\\ x\equiv 2\bmod(7)\end{cases}$$

$x=a_1M_1y_1+a_2M_2y_2+a_3M_3y_3$
$=4\times 42\times 3+3\times 5\times 35+2\times 4\times 30=1269$
$x=1269\bmod(210)\qquad 1269\div 210=6.042\,9\Longrightarrow q=6$
$r=1269-210\times 6=9$
$1269=210\times 6+9$
donc x=9mod(210)
$S_{\mathbb{Z}}=\{210k+9,k\in\mathbb{Z}\}$
vérification our x=9
x=9=5+4=4mod(5)
x=9=6+3=3mod(6)
x=9=7+2=2mod(7)
donc 9 est bien solution du système.

exemple système chinois

$$\begin{cases} 3x\equiv 4\bmod(11)\\ x\equiv 3\bmod(5)\\ x\equiv 2\bmod(9)\end{cases}$$

simplifier l'équation (1)

en mod(11), 3 est inversible

en utilisant 3^{-1} donc $3x \equiv 4 \bmod(11) \iff 3^{-1}3x \equiv 3^{-1}4 \bmod(11)$

$\iff \quad x \equiv 3^{-1}4 \bmod(11)$

calcul de 3^{-1} $en \bmod(11)$

11=3×3 + 2

3=2×1 + 1 $\Longrightarrow 1 = 3 - 2$

1=3-(11-3×3)

1=3×4 − 11

en modulo(11) $\overline{1} = \overline{3} \times \overline{4}$ donc $3^{-1} = 4$

ainsi (1) $\iff$ $x \equiv 3^{-1}4 \bmod(11)$

$x \equiv 4 \times 4 \bmod(11)$

$x \equiv 5 \bmod(11)$

le système devient

$$\begin{cases} 3x \equiv 4 \bmod(11) \\ x \equiv 3 \bmod(5) \\ x \equiv 2 \bmod(9) \end{cases} \iff \begin{cases} x \equiv 5 \bmod(11) \\ x \equiv 3 \bmod(5) \\ x \equiv 2 \bmod(9) \end{cases}$$

11, 5, 9 sont preiers deux à deux donc le système admet une solution unique

modulo : M=$11 \times 5 \times 9 = 495$

la solution est x= $5\times(5 \times 9) \times y_1 + 3 \times (11 \times 9) \times y_2 + 2 \times (11 \times 5) \times y_3$

$y_1 = (5 \times 9)^{-1} \bmod(11)$ $y_2 = (11 \times 9)^{-1} \bmod(5)$ $y_3 = (11 \times 5)^{-1} \bmod(9)$

45=11×4 + 1

1=45-11×4 $\overline{1} = \overline{45} \times \overline{1}$ donc $45^{-1} \bmod(11) = 1 = y_1$

99=5×19 + 4

5=4×1 + 1 $\Longrightarrow 1 = 5 - 4$

1=5-(99-5×19)

1=5×20 × −99

donc $99^{-1} \bmod(5) = -1 = 4 = y_2$

55=9×6 + 1 $\Longrightarrow 1 = 55 - 9 \times 6$ donc $\overline{1} = \overline{55} - \underbrace{\overline{9}}\times\overline{6} = \overline{55} = \overline{55} \times \overline{1}$

donc $55^{-1} \bmod(9) = 1 = y_3$

la solution particulière

x= $5\times(5 \times 9) \times y_1 + 3 \times (11 \times 9) \times y_2 + 2 \times (11 \times 5) \times y_3$

x=$5 \times 45 \times 1 + 3 \times 99 \times 4 + 2 \times 55 \times 1 = 1523 \bmod(495)$

$1523 \div 495 = 3.076\,8$

$1523 - 495 \times 3 = 38$

x=38mod(495) donc $S_{\mathbb{Z}} = \{38 + 495k, k \in \mathbb{Z}\}$

vérification avec x=38

$$\begin{cases} x \equiv 5 \bmod(11) \\ x \equiv 3 \bmod(5) \\ x \equiv 2 \bmod(9) \end{cases}$$

38=11×3 + 5 (1) est vérifiée
38=5×7 + 3 (2) est vérifiée
38=9×4 + 2 (3) est vérifiée
résoudre dans Z^2 :
17x + 6y = 1
retrouver l'identité de Bezout avec 17 et 6
17=6×2 + 5
6=5+1 1=6-5
1=6-(17-6×2)
1=6×3 − 17
on a
17x + 6y = 1 (1)
-17+6×3 = 1 (2)

(1)-(2) $\Longrightarrow 17(x+1) + 6(y-3) = 0$
17(x+1)=6(3-y) donc 6| $17(x+1)$
comme 6 est premier avec17 alors 6| $(x+1)$ lemme de Gauss
$\exists k \in \mathbb{Z}$, x+1=6k et 3-y=17k
x=6k-1, y=3-17k
$S_{\mathbb{Z}^2} = \{(6k-1, 3-17k), k \in \mathbb{Z}\}$
exemple
$x^2 = 3 \bmod(5)$
tableau de congruence modulo 5.
théorème chinois des restes (deux équations)
Soient m et n deux entier premiers entre eux.
1.Montrer que $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est naturellemet muni d'une structure d'anneau unitaire.
2. Montrer que le morphisme d'anneaux
φ : Z $\longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ défini par
$\forall$ k $\in \mathbb{Z}$, φ(k) = (k + m$\mathbb{Z}$, k + n$\mathbb{Z}$) induit un isomorphisme
$\overline{\varphi} : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$
3 . Montrer que $\forall (a,b) \in \mathbb{Z}^2$ le système de congruence :
$$(S)\begin{cases} x \equiv a \bmod(m) \\ x \equiv b \bmod(n) \end{cases}$$
admet au moins une solution $x_1 \in \mathbb{Z}$.

exemple

$\begin{cases} x \equiv 4 \bmod(5) \\ x \equiv 3 \bmod(6) \end{cases}$

4. soient k_1,k_2 deux solutions de (S).
montrer que $k_1 \equiv k_2 \bmod(mn)$
5.montrer que $U(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) = U(\mathbb{Z}/m\mathbb{Z}) \times U(\mathbb{Z}/n\mathbb{Z})$
6. montrer que $U(\mathbb{Z}/mn\mathbb{Z}) \simeq U(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$

Exercice
Trouver le reste de la division de 10^{100} par $247 = 13 \times 19$

on pose x=10^{100}
ona $10^{12} = 1 \bmod(13)$
$100 \div 12 = 8.333\,3 \Longrightarrow q = 8$
r=$100 - 12 \times 8 = 4.$
$100 = 12 \times 8 + 4$
$.10^{100} = (10^{12})^8 \times 10^4 = 10^4 \bmod 10^4(13)$
10=-3mod(13) donc $10^2 = 9 \bmod(13) = -4 \bmod(13)$
$10^4 = 16 \bmod 10^4(13) = 3 \bmod(13)$
x=$10^{100} = 3 \bmod(13)$
par 19
$10^{18} = 1 \bmod(19)$
$100 \div 18 = 5.555\,6 \Longrightarrow q = 5$
r=$100 - 18 \times 5. = 10.0$
$100 = 18 \times 5 + 10$
$10^{100} = (10^{18})^5 \times 10^{10} = 10^{10} \bmod 10^4(19)$
$100 \div 19 = 5.263$
$100 - 19 \times 5 = 5.0$
$10^2 = 5 \bmod(19) \Longrightarrow 10^4 = 25 = 6 \bmod(19)$
$10^8 = 36 \bmod(16)$
$10^{10} = 36 \times 5 = 180$
$180 \div 19 = 9.473\,7$
$180 - 19 \times 9 = 9$
180=$19 \times 9 + 9$
180=9mod(19)

x=$10^{100} = 3 \bmod(13)$
x=$10^{100} = 9 \bmod(19)$

d'où $\begin{cases} x = 3 \bmod(13) \\ x = 9 \bmod(19) \end{cases}$
soit M=$13 \times 19 = 247$
le système admet une solution unique modulo M
x=$3\times19 \times y_1 + 9 \times 13 \times y_2$
avec $y_1 = 13^{-1} \bmod(19)$ $\quad$ $y_2 = 19^{-1} \bmod(13)$
on a 19=13+6
$13=6\times2 + 1 \Longrightarrow 1 = 13 - 6 \times 2$
$1=13-(19-13)\times2$
$1=13\times3 - 19 \times 2$
donc $13^{-1} \bmod(19) = 3 \bmod(19) \Longrightarrow y_1 = 3$
$19^{-1} \bmod(13) = -2 \bmod(13) \Longrightarrow y_2 = 11$
x=$3 \times 19 \times 3 + 9 \times 13 \times 11 = 1458$
$1458 \div 247 = 5.902$
$1458 - 247 \times 5 = 223.$
x=223mod(19×13)

TD ARITHMETIQUE L2 MI : 19-20

EXERCICE 1

Soit n un entier naturel non nul et $q \in \mathbb{R}$ ou $\mathbb{C}$.
On pose $(n)_q = 1 + q + \cdots + q^{n-1}$, $(n!)_q = (1)_q (2)_q \cdots (n)_q$
$\left(\begin{array}{c} n \\ k \end{array} \right)_q = \dfrac{(n!)_q}{(k!)_q ((n-k)!)_q}$ et $(0!)_q = 1.$

a) Montrer que $(n!)_q = \frac{(q-1)(q^2-1)\cdots(q^n-1)}{(q-1)^n}$ avec $q \neq 1$

b) Montrer que $\left(\begin{array}{c} n \\ k \end{array} \right)_q = \left(\begin{array}{c} n \\ n-k \end{array} \right)_q$

c) Montrer que $\left(\begin{array}{c} n \\ k \end{array} \right)_q = \left(\begin{array}{c} n-1 \\ k-1 \end{array} \right)_q + q^k \left(\begin{array}{c} n-1 \\ k \end{array} \right)_q = \left(\begin{array}{c} n-1 \\ k \end{array} \right)_q +$
$q^{n-k} \left(\begin{array}{c} n-1 \\ k-1 \end{array} \right)_q$

EX 2

Soit G un groupe tel que l'application x$\longmapsto$x^{-1} soit un morphisme. Montrer que G est commutatif.

EX 3

Montrer qu'un sous-groupe d'indice 2 dans un groupe G est distingué dans G.

EX 4

Soit f : G $\longrightarrow$H un morphisme de groupes finis. Soit G' un sous-groupe de G. Montrer que

l'ordre de f(G') divise les ordres de G' et de H.

EX 5

Soit f : G$\longrightarrow$H un morphisme de groupes finis. Soit G' un sous-groupe de G d'ordre premier à l'ordre de H. Montrer que G'= ker(f).

Ex 6

Démontrer que pour tout $n \in \mathbb{N}$,

1. n^3 - n est divisible par 6 ,

2.n^5 - n est divisible par 30 ,

3. n^7 - n est divisible par 42 .

Ex 7

Pour tout $n \in \mathbb{N}$, on définit deux propriétés :

P_n : 3 divise 4^n-1 et Q_n : 3 divise 4^n+1 .

2. Montrer que P_n est vraie pour tout $n \in \mathbb{N}$.

3. Que penser de l'assertion :$\exists n_0 \in \mathbb{N}$ tel que $\forall n \geq n_0$ Q_n est vraie.

Ex 8

Démontrer par récurrence que :

a) $2^{2\times 3^n} - 1$ est divisible par 3^{n+1} pour tout entier n$\geq$ 0.

b) $5^{3^n} + 1$ est divisible par 3^{n+1} pour tout entier n$\geq$ 0.:

Ex 9

1.Montrer que pour tout n$\in \mathbb{N}$ et tout p$\in \mathbb{Z}$: $\mathrm{p}\begin{pmatrix} n \\ p \end{pmatrix} = n \begin{pmatrix} n-1 \\ p-1 \end{pmatrix}$

2.Calculer pour tout n

$\mathrm{S}_0 = \sum_{p=0}^{n} \begin{pmatrix} n \\ p \end{pmatrix}$; $\mathrm{S}_1 = \sum_{p=0}^{n} \mathrm{p}\begin{pmatrix} n \\ p \end{pmatrix}$; $\mathrm{S}_2 = \sum_{p=0}^{n} \mathrm{p}^2 \begin{pmatrix} n \\ p \end{pmatrix}$

EX 10

Soit $\sigma : \mathbb{Z} \longrightarrow \mathbb{N}$ qui à $n \in \mathbb{Z}$ associe le nombre de diviseurs positifs de n .

a) Soit p un nombre premier et $\alpha \in \mathbb{N}^*$ .Calculer $\sigma(p^\alpha)$.

b) Soient $a, b \in \mathbb{Z}$ premiers entre eux ,et $\varphi : \text{div}(a) \times \text{div}(b) \longrightarrow \text{div}(ab)$ définie par $\varphi(k,l) = kl$ montrer que φ est une bijection .div(n) désigne l'ensemble des diviseurs positifs d'un entier n

c) En déduire une relation entre $\sigma(ab)$, $\sigma(a)$ et $\sigma(b)$ si a et b sont premiers entre eux .

d) Soit n un entier naturel, $p_1^{\alpha_1}.\ p_2^{\alpha_2} \cdots\ p_r^{\alpha_r}$ la décomposition en nombre premiers de n .Exprimer $\sigma(n)$ en fonction des α_i .

Ex 11

On suppose que

n est un entier ≥ 2 tels que $2^n - 1$ est premier.

Montrer que n est un nombre premier.

Ex 12

Soient a et p deux entiers supérieurs à 2.

Montrer que si $a^p - 1$ est premier alors a=2 et p est premier.

Ex 13

Soit p un nombre premier, p$\geq$ 5. Montrer que p^2 - 1 est divisible par 24.

EX 14

Résoudre dans Z^2 les équations suivantes :

a) 17x + 6y = 1 b) 27x + 25y = 1 c) 118x + 35y = 1 d) 39x + 26y = 1

EX 15

1.Résoudre dans Z les équations : $x^2 = 2 \bmod 6$; $x^3 = 3 \bmod 9$.

2. Résoudre dans Z^2 les équations suivantes :

$5x^2 + 2xy - 3 = 0$; $y^2 + 4xy - 2 = 0$.

Ex 16

Résoudre dans $\mathbb{Z}$

$$1)\begin{cases} x = 2 \bmod 10 \\ x = 5 \bmod 13 \end{cases} \qquad 2)\begin{cases} x = 4 mod 6 \\ x = 7 mod 9 \end{cases} \quad 3)\begin{cases} 5x = 4 (mod 27) \\ 12x = 9 (mod 51) \end{cases}$$

Ex 17

Une bande de 17 pirates dipose d'un butin de N pièces d'or d'égale valeur. Ils décident de se le partager équitablement et de donner le reste au cuisinier (non pirate). Celui i reçoit 3 pièces. Mais une dispute éclate et 6 pirates sont tués. Tout le butin est reconstitué et partagé entre les survivants comme précédemment; le cusinier reçoit alors 4 pièces. Dans un naufrage ultérieur, seul le butin, 6 pirates et le cuisinier sont sauvés. Le butin est à nouveau partagé de la même manière et le cuisinier reçoit 5 pices.

Quelle est alors la fortune minimale que peut espérer le cuisinier lorsqu'il décide d'empoisonner le reste des pirates?

EX18

Combien l'armée de Han Xing comporte-t-elle de soldats (au minimum) si, rangés par 3 colonnes, il reste deux soldats, rangés par 5 colonnes, il reste trois soldats et, rangés par 7 colonnes, il reste deux soldats ?

Exercice 19

résoudre dans $\mathbb{Z}$ le système de congruence :

$$\begin{cases} x \equiv 3 \bmod 4 \\ x \equiv -2 \bmod 3 \\ x \equiv 7 \bmod 5 \end{cases}$$

Ex 20

Trouver le reste de la division euclidienne de
10^{2020} par 42.