Chapitre 3

Arithmétique dans $\mathbb{Z}$

3.1 Divisibilité

Définition 19

(Divisibilité) : Si m, n sont des entiers et $n \neq 0$, on dit que n divise m s'il existe un entier $k \in \mathbb{Z}$ tel que $m = kn$. On note $n \mid m$.
On dit que n divise m˘, que m est un multiple de n.

Lemme 6

Soient $m, n \in \mathbb{Z}^*$ tels que $n \mid m$. L'entier k tel que $m = kn$ est unique.

Proposition 28

Si $m, n, p \in \mathbb{Z}$, on a
(i) $n \mid m$ et $m|p \Longrightarrow n|p$
(ii) $n \mid m$ et $m \mid n \Longleftrightarrow n = \pm m$.
(iii) $n \mid m$ et $n|p \Longrightarrow n|m + p$. Plus généralement, pour tous $a, b \in \mathbb{Z}, n \mid (am + bp)$.

Proposition 29

Si $n \in \mathbb{Z}, m \in \mathbb{N}^*$ et si $n \mid m$, alors $-m \leq n \leq m$.

Corollaire 7

L'ensemble des diviseurs d'un entier $m \in \mathbb{Z}^*$ est fini.

Théorème 13

(Division euclidienne) : Soient $n \in \mathbb{Z}$ et $m \in \mathbb{N}^*$. Il existe deux uniques entiers q, $r \in \mathbb{Z}$ tels que $n = mq + r$ et $0 \leq r < m$. L'entier q s'appelle le quotient dans la division euclidienne de n par m et r le reste. Donc

Exemple : $n = 37$ et $m = 5 \in \mathbb{N}^*$. On a $37 = 5 \times \underline{7} + \underline{2}$. On a bien $0 \leq 2 < 5$, donc 7 et 2 sont bien le quotient et le reste de la division euclidienne de 37 par 5.

(2) $n = -18$ et $m = 7 \in \mathbb{N}^*$: $-18 = 7 \times \underline{-3} + \underline{3}$. On a bien $0 \leq 3 < 7$.

3.2 PGCD et PPCM

Définition 20

(**Plus Grand Commun Diviseur**) : Soient $n, m \in \mathbb{Z}$ deux entiers non tous deux nuls. Le plus grand entier qui divise à la fois m et n est appelé le Plus Grand Commun Diviseur (ou pgcd) de m et n. On le note $\text{pgcd}(m, n)$ ou encore $m \wedge n$. C'est un entier strictement positif.

Exemple : $\text{pgcd}(7, 11) = 1$

Lemme 7

Soient $m, n \in \mathbb{N}^*$ et r le reste de la division euclidienne de n par m. Alors pgcd $(n, m) = \text{pgcd}(m, r)$

Proposition 30

Soient $m, n \in \mathbb{N}^*$. Le pgcd de m et n est le dernier reste non nul dans l'algorithme d'Euclide.

Preuve. $\text{pgcd}(n, m) = \text{pgcd}\,(m, r_1) = \text{pgcd}\,(r_1, r_2) = \ldots = \text{pgcd}\,(r_{N-1}, r_N) = \text{pgcd}\,(r_{N-1}, 0) = r_{N-1}$ où r_N est le premier reste nul.

Exemple : Calculons pgcd $(129, 12)$.

(1) $129 = 12 \times 10 + 9$

(2) $12 = 9 \times 1 + 3$

(3) $9 = 3 \times 3 + 0$.

Donc $\text{pgcd}(129, 12) = 3$.

Exemple : Soit $n \in \mathbb{N}^*$. Quel est le pgcd de $9n+4$ et $2n+1$?
(1) $9n+4 = (2n+1) \times 4 + n \, (0 \leq n < 2n+1 \forall n \in \mathbb{N}^*)$
(2) $2n+1 = n \times 2 + 1 (0 \leq 1 < n$ sauf si $n = 1)$
(3) $n = 1 \times n + 0 (0 \leq 0 < 1)$
Donc $pgcd(9n+4, 2n+1) = 1$ pour tout $n \geq 2$. Pour $n = 1$, pgcd $(13, 3) = 1$ aussi.

Définition 21

(**Entiers premiers entre eux**) : Soient m, n deux entiers non tous deux nuls. On dit que m et n sont premiers entre eux si $\text{pgcd}(m, n) = 1$.

Lemme 8

Soient $m, n \in \mathbb{Z}^*$ deux entiers et d leur pgcd. Les entiers $n' = n/d$ et $m' = m/d$ sont premiers entre eux.

3.3 Théorème de Bezout

Le théorème suivant est très important et a de nombreuses conséquences. Nous en verrons plusieurs.

Théorème 14

(**Bezout**) : Soient $m, n \in \mathbb{Z}^*$. Alors il existe $(u, v) \in \mathbb{Z}^2$ tel que un $+vm = \text{pgcd}(n, m)$. Une telle relation s'appelle une relation de Bezout.

Exemple :

$$\begin{aligned} 129 = 12 \times 10 + 9 &\implies & 9 &= 129 - 12 \times 10 \\ 12 = 9 \times 1 + 3 &\implies 3 & &= 12 - 9 \times 1 \\ &\iff 3 & &= 12 - (129 - 12 \times 10) \times 1 \\ &\iff 3 & &= 129 \times (-1) + 12 \times (11) = \text{pgcd}(129, 12). \end{aligned}$$

Exemple : Soit $n \geq 2$.

$$\begin{aligned} &9n+4 = (2n+1) \times 4 + n \implies n = 9n+4-(2n+1) \times 4 \\ &2n+1 = n \times 2 + 1 \implies 1 = (2n+1) - n \times 2 \\ &\iff 1 = (2n+1) - ((9n+4) - (2n+1) \times 4) \times 2 \\ &\iff 1 = (9n+4) \times (-2) + (2n+1) \times (9) = \text{pgcd}(9n+4, 2n+1). \end{aligned}$$

Corollaire 8

Si $m, n \in \mathbb{Z}^*$, alors $\text{pgcd}(m,n) = 1 \iff \exists (u,v) \in \mathbb{Z}^2 : \text{un } + vm = 1.$

Preuve. ($\Rightarrow$) C'est un cas particulier du théorème de Bezout.

($\Leftarrow$) Si $1 = nu + mv$ et si $d = \text{pgcd}(n,m)$, alors $d \mid n$ et $d \mid m$ implique $d \mid nu + mv = 1$, donc $d = \pm 1$ et comme $d > 0$(c'est un pgcd), $d = 1$.

Proposition 31

Soient $m, n \in \mathbb{Z}^*$ et $d \in \mathbb{Z}^*$. Alors,
(i) $d|n, d|m \iff d \mid \text{pgcd}(n,m)$,
(ii) $\forall k \in \mathbb{N}^*, \quad \text{pgcd}(km, kn) = k \cdot \text{pgcd}(m,n)$.

Théorème 15

(de Gauss) : Soient $m, n, p \in \mathbb{Z}^*$. Si $n \mid mp$ et que pgcd $(m,n) = 1$, alors $n \mid p$.

Définition 22

(**Plus Petit Commun Multiple**) : Le plus petit entier positif à la fois multiple des entiers m et n est appelé le Plus Petit Commun multiple (ou ppcm) de m et n. On le note $ppcm(m,n)$ ou encore $m \vee n$.

Exemple : Pour tout $n \in \mathbb{Z}$,
$\text{ppcm}(n,0) = 0$
$\text{ppcm}(n,1) = n$,
$\text{ppcm}(n,m) = \text{ppcm}(n,-m) = \text{ppcm}(-n,m) = \text{ppcm}(-n,-m)$,
$\text{ppcm}(7,21) = 21 = 21 \times 1 = 7 \times 3$,
$\text{ppcm}(11,9) = 99 = 9 \times 11$,
$\text{ppcm}(15,6) = 30 = 15 \times 2 = 6 \times 5$.

Proposition 32

Soient $n, m \in \mathbb{N}$ deux entiers naturels non tous deux nuls, alors nm $= pgcd(m,n)$. $\text{ppcm}(m,n)$. En particulier, si $\text{pgcd}(m,n) = 1, \text{ppcm}(m,n) = mn$.

Corollaire 9

Si $n, m \in \mathbb{Z}^*$. Alors un entier k est un multiple commun à n et m, si et seulement si $\text{ppcm}(m,n)$ divise k.

3.4 Equations diophantiennes

Définition 23

(**Equation diophantienne**) : On appelle équation diophantienne toute équation dont on recherche les solutions entières.
Soient $a, b \in \mathbb{Z}^*$ et $c \in \mathbb{Z}$. On considère l'équation suivante :

$$ax + by = c$$

dont on recherche les solutions $(x, y) \in \mathbb{Z}^2$.

Lemme 9

(**Existence des solutions**) : Soient $a, b \in \mathbb{Z}^*$ et $c \in \mathbb{Z}$. L'équation diophantienne $ax + by = c$ admet au moins une solution si et seulement si $pgcd(a, b) \mid c$.

Proposition 33

Soient $a, b \in \mathbb{Z}^*$ et $c \in \mathbb{Z}$ tels que $\text{pgcd}(a, b) \mid c$. Soient $a' = \frac{a}{pgcd(a,b)}$ et $b' = \frac{b}{pgcd(a,b)}$. Si $(x_0, y_0) \in \mathbb{Z}^2$ est une solution de l'équation diophantienne ax $+by = c$, alors l'ensemble des solutions est $S = \{(x_0 + kb', y_0 - ka') \in \mathbb{Z}^2, k \in \mathbb{Z}\}$.

Exemple : On considère l'équation $252x + 69y = 7$. Vérifions que celle-ci n'a pas de solutions dans $\mathbb{Z}^2$. Pour cela, on commence par calculer $\text{pgcd}(252, 69)$:

$$\begin{aligned} 252 &= 69 \times 3 + 45 \\ 69 &= 45 \times 1 + 24 \\ 45 &= 24 \times 1 + 21 \\ 24 &= 21 \times 1 + 3 \\ 21 &= 7 \times 3 + 0. \end{aligned}$$

D'où $\text{pgcd}(252, 69) = 3$ et 3 ne divise pas 7 .

Exemple : Considérons l'équation $252x + 69y = 6$. Comme $\text{pgcd}(252, 69) = 3$, ce qui divise 6 , l'équation admet des solutions. Cherchons une solution particulière avec l'algorithme d'Euclide étendu :

$$\begin{aligned} 3 &= 24 - 21 \times 1 \\ &= 24 - (45 - 24) = 24 \times 2 - 45 \\ &= (69 - 45) \times 2 - 45 = 69 \times 2 - 3 \times 45 \\ &= 69 \times 2 - 3 \times (252 - 69 \times 3) = 252 \times (-3) + 69 \times 11 \end{aligned}$$

donc $252 \times (-6) + 69 \times 22 = 6$. Ainsi, $(x_0, y_0) = (-6, 22)$ est une solution particulière de l'équation. On en déduit que la forme générale des solutions est $(x, y) = (-6 + k \times 23, 22 - k \times 84)$ où $k \in \mathbb{Z}$.

3.5 Nombres premiers

Définition 24

(Nombre premier) : Soit $n \in \mathbb{N}^*$. On dit que n est premier s'il n'admet que deux diviseurs positifs distincts : 1 et lui-même. Un facteur premier de n est un nombre premier qui divise n.

Remarque : Par convention 1 n'est pas un nombre premier.

Exemple : $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$ sont premiers.

$6 = 2 \times 3$ n'est pas premier.

7 est un facteur premier de 21 .

Lemme 10

(**Facteur premier**) : Tout entier $n \geq 2$ admet au moins un facteur premier.

Exemple : Les facteurs premiers de $24 = 2^3 \times 3$ sont 2,3 et ceux de $8160 = 2^5 \times 3 \times 5 \times 17$ sont $2, 3, 5$ et 17 .

Proposition 34

(**Infinité de nombres premiers**) : Il existe une infinité de nombres premiers.

Preuve. Supposons par l'absurde qu'il y en a un nombre fini $N \geq 1$ et notons les $p_1, \ldots, p_N$.

Considérons

$$n = p_1 \times \cdots \times p_N + 1 \geq 2.$$

Comme $n \geq 2$, il admet un facteur premier $p \geq 2$ d'après le lemme 5. Si p est l'un des p_i, alors

$$\begin{cases} p \mid p_1 p_2 \cdots p_N \\ p \mid n \end{cases} \Longrightarrow p \mid n - p_1 p_2 \cdots p_N = 1$$

ce qui est impossible. Donc p est un nombre premier différent des $p_1, \ldots, p_N$: contradiction.

Lemme 11

(**d'Euclide**) : Soient p un nombre premier et $n, m \in \mathbb{Z}$. Si p divise le produit nm, alors p divise n ou p divise m.

Corollaire 10

Si un nombre premier p divise un produit d'entiers $n_1 n_2 \cdots n_k$, alors p divise l'un des n_i.

Théorème 16

Tout entier $n \geq 2$ s'écrit comme un produit de nombres premiers.

Théorème 17

(**Décomposition en produit de facteurs premiers**) : Tout entier $n \geq 2$ s'écrit de manière unique sous la forme $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ avec $r \in \mathbb{N}^*, a_i \in \mathbb{N}$ et les p_i sont des nombres premiers tels que $p_1 < p_2 < \cdots < p_r$. Cette égalité est appelée la décomposition en produit de facteurs premiers de n.

Exemple : $24 = 2^3 \times 3$ et $8160 = 2^5 \times 3 \times 5 \times 17$.

Proposition 35

Soit $n \geq 2$. Si n n'est pas premier, alors il admet un facteur premier $p \leq \sqrt{n}$.

Exemple : 641 est premier. En effet, les nombres premiers $\leq \sqrt{641} \simeq 25.32$ sont

$$2, 3, 5, 7, 11, 13, 17, 19, 23$$

et on vérifie en posant les divisions qu'aucun de ces nombres premiers ne divise 641 .

Lemme 12

Soit $n \geq 2$ et $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ sa décomposition en produit de facteurs premiers. Alors tout diviseur positif d de n s'écrit sous la forme $d = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$ où les b_i vérifient $0 \leq b_i \leq a_i$.

Exemple : Les diviseurs positifs de $24 = 2^3 \times 3$ sont

$$2^3 \times 3 = 24 \quad 2^2 \times 3 = 12 \quad 2 \times 3 = 6 \quad 3 \quad 2^3 = 8 \quad 2^2 = 4 \quad 2 \quad 1.$$

Proposition 36

Soient $m, n \in \mathbb{N}^*, m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ et $n = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$ pour certains entiers a_i, b_i éventuellement nuls et des p_i premiers. Alors,
$d := \text{pgcd}(m, n) = \prod_{i=1}^{r} p_i^{\min(a_i, b_i)}$
$p := \text{ppcm}(m, n) = \prod_{i=1}^{r} p_i^{\max(a_i, b_i)}$.

Exemple : $12 = 2^2 \times 3$ et $129 = 3 \times 43$, ce que l'on peut aussi réécrire

$$12 = 2^2 \times 3 \times 43^0 \quad \text{et} \quad 129 = 2^0 \times 3 \times 43.$$

Alors

$$\text{pgcd}(12, 129) = 2^0 \times 3^1 \times 43^0 = 3 \quad \text{et} \quad \text{ppcm}(12, 129) = 2^2 \times 3 \times 43 = 516.$$

3.6 Congruences

Définition 25

(**Congruence**) : Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. On dit que a et b sont congrus modulo n si l'entier n divise $a - b$. On note $a \equiv b \bmod n$ ou encore $a \equiv b[n]$. Cette relation s'appelle relation de congruence modulo n.

Exemple : (1) $7 \equiv 1 \bmod 6$ car $7 - 1 = 1 \times 6$ est divisible par 6.
(2) $31 \equiv 11 \bmod 4$ car $31 - 11 = 20 = 5 \times 4$.
Fait 1 (important) : (1) $a \equiv b \bmod n \iff \exists k \in \mathbb{Z} : a = b + kn$.
(2) $a \equiv 0 \bmod n \iff n \mid a$.

Lemme 13

(Propriétés des congruences) : Soient a, b, c, $d \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Alors,
(i) Réflexivité : $a \equiv a \bmod n$,
(ii) Symétrie : $a \equiv b \bmod n \implies b \equiv a \bmod n$,
(iii) Transitivité : $a \equiv b \bmod n$ et $b \equiv c \bmod n \implies a \equiv c \bmod n$,
(iv) $a \equiv c \bmod n$ et $b \equiv d \bmod n \implies a + b \equiv c + d \bmod n$,
(v) $a \equiv c \bmod n$ et $b \equiv d \bmod n \implies ab \equiv cd \bmod n$. En particulier, pour tout $k \in \mathbb{N}$, on a $a^k \equiv c^k \bmod n$.

Exemple : $7^n - 1$ est divisible par 6 pour tout $n \in \mathbb{N}$ (ou encore $7^n \equiv 1 \bmod 6$).

Définition 26

(**Classe de congruence**) : Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. La classe de a mod n est l'ensemble

$$\begin{aligned}\bar{a} &= \{b \in \mathbb{Z} \mid a \equiv b \mod n\} \\ &= \{b \in \mathbb{Z} \mid b \equiv a \mod n\} \\ &= \{b \in \mathbb{Z} | n | b - a\} \\ &= \{b \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : b - a = kn\} \\ &= \{a + kn \in \mathbb{Z} \mid k \in \mathbb{Z}\} \subset \mathbb{Z}\end{aligned}$$

On note $\mathbb{Z}/n\mathbb{Z} = \{\bar{a}, a \in \mathbb{Z}\}$ (on prononce $\mathbb{Z}$ sur $n\mathbb{Z}$)

Lemme 14

Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. On a $\bar{a} = \bar{b} \iff a \in \bar{b} \iff b \in \bar{a} \iff a \equiv b \bmod n$.

Proposition 37

Soit $a \in \mathbb{Z}$. Alors $a \equiv r \bmod n$ où r est le reste de la division euclidienne de a par n. De plus, si $r \equiv r' \bmod n$ avec $0 \leq r < n$ et $0 \leq r' < n$, alors $r = r'$.

Exemple (Important : Puissance modulo un entier) : Quel est le reste de la division euclidienne par 13 de 100^{1000} ?

Comme $100 = 7 \times 13 + 9, 100 \equiv 9 \bmod 13$. Par propriété (v) des congruences, $100^{1000} \equiv 9^{1000} \bmod 13$. Or $9^2 \equiv 81 \equiv 3 \bmod 13$(car $81 = 13 \times 6 + 3$) et donc $9^3 \equiv 9 \times 9^2 \equiv 9 \times 3 \equiv 1 \bmod 13$. Finalement,

$$100^{1000} \equiv 9^{1000} \equiv 9^{3\times 333+1} \equiv \left(9^3\right)^{333} \times 9 \equiv 1^{333} \times 9 \equiv 9 \bmod 13.$$

Ainsi le reste de la division euclidienne de 100^{1000} par 13 est 9.
On obtient aussi le corollaire suivant :

Corollaire 11

Si $a \in \mathbb{Z}$, il existe un unique $0 \leq r < n$ tel que a $\equiv r \bmod n$. On en déduit que $\mathbb{Z}/n\mathbb{Z}$ possède n éléments et $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Exemple : Pour $n = 4, \mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.

De manière générale, on a toujours $\bar{n} = \overline{0}$ dans $\mathbb{Z}/n\mathbb{Z}$. En effet, 0 est le reste dans la division euclidienne de n par n. De même, $\overline{n+1} = \overline{1}, \overline{n+2} = \overline{2}$,etc.

Définition 27

(Somme et produit de classes) : On considère deux éléments $\bar{a}$ et $\bar{b}$ de $\mathbb{Z}/n\mathbb{Z}$. on définit la somme et le produit de $\bar{a}$ et $\bar{b}$ par

$$\bar{a} + \bar{b} := \overline{a+b}$$
$$\bar{a} \cdot \bar{b} := \overline{a \cdot b} \quad \text{ou noté plus simplement } \bar{a}\bar{b}.$$

Proposition 38

(Eléments neutres) : Pour tout $a \in \mathbb{Z}$, on a $\bar{a} + \overline{0} = \bar{a}$ et $\bar{a} \cdot \overline{1} = \bar{a}$.

Exemple (Table d'addition de $\mathbb{Z}/6\mathbb{Z}$) :

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

Définition 28

(Classe inversible) : Un élément $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ est dit inversible s'il existe $\bar{b} \in \mathbb{Z}/n\mathbb{Z}$, appelé inverse de $\bar{a}$ tel que $\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a} = \overline{1}$.

Notation : On note $(\mathbb{Z}/n\mathbb{Z})^\times$ l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Exemple : Dans $\mathbb{Z}/4\mathbb{Z}$, on a $\overline{3} \times \overline{3} = \overline{3 \times 3} = \overline{9} = \overline{1}$ car le reste de la division euclidienne de 9 par 4 est 1. Ainsi $\overline{3}$ est inversible et son inverse est lui-même :

$$\overline{3} \in (\mathbb{Z}/4\mathbb{Z})^\times .$$

Proposition 39

(**Caractérisation des éléments inversibles**) : Un élément $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si $\text{pgcd}(a, n) = 1$ (c'est-à -dire si et seulement si $\exists u \in \mathbb{Z}$, au $\equiv 1 \mod n$).

Preuve. $(\Rightarrow)$ On suppose $\bar{a}$ inversible. Donc il existe $\bar{u} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\bar{a} \cdot \bar{u} = \overline{1}$. Or

$$\begin{aligned} \bar{a} \cdot \bar{u} = \overline{1} &\iff \overline{au} = \overline{1} \\ &\iff \overline{1} - \overline{au} = \overline{0} \\ &\iff \overline{1 - au} = \overline{0}. \end{aligned}$$

Donc $1 - au$ est divisible par n :

$$\exists k \in \mathbb{Z} : \quad 1 - au = nk$$

c'est-à -dire $au + nk = 1$. Dans ce cas, $d = \text{pgcd}(a, n) = 1$ d'après un corollaire du théorème de Bezout (dem : $d := \text{pgcd}(a, n)$, alors $d \mid a$ et $d \mid n$ donc $d \mid ab + nk = 1$ et finalement $d = 1$(car $d > 0$).

$(\Leftarrow)$ Si $\text{pgcd}(a, n) = 1$, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + nv = 1$; Donc

$$\begin{aligned} &\overline{au + nv} = \overline{1} \iff \overline{au} + \overline{nv} = \overline{1} \\ &\iff \bar{a} \cdot \bar{u} + \bar{n} \cdot \bar{v} = \overline{1} \\ &\iff \bar{a} \cdot \bar{u} + \overline{0} \cdot \bar{v} = \overline{1} \\ &\iff \bar{a} \cdot \bar{u} + \overline{0} = \overline{1} \\ &\iff \bar{a} \cdot \bar{u} = \overline{1} \end{aligned}$$

et $\bar{a}$ est bien inversible dans $\mathbb{Z}/n\mathbb{Z}$, d'inverse $\bar{u}$.

Conséquence : Si p est un nombre premier, tous les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles.

3.6.1 Equation diophantienne $ax \equiv b \bmod n$.

Lemme 15

Soient $a, b \in \mathbb{Z}$ et un entier $n \geq 2$. L'équation $ax \equiv b \bmod n$ admet une solution dans $\mathbb{Z}$ si et seulement si $\text{pgcd}(a, n) \mid b$.

Proposition 40

Notons $\mathcal{S}$ l'ensemble des solutions de l'équation $\text{ax} \equiv b \bmod n$.
(1) Si $\text{pgcd}(a, n)$ ne divise pas b, alors $\mathcal{S} = \varnothing$.
(2) Sinon $\text{pgcd}(a, n) \mid b$. Posons $n' = \frac{n}{pgcd(a,n)}$. Soit $x_0 \in \mathbb{Z}$ est une solution particulière de l'équation $ax \equiv b \bmod n$. Alors

$$\mathcal{S} = \left\{ x_0 + kn' \in \mathbb{Z} \mid k \in \mathbb{Z} \right\}.$$

Exemple : Résoudre l'équation $24x \equiv 4 \bmod [10]$.
Comme $24 = 2^3 \cdot 3$ et $10 = 2 \cdot 5, \text{pgcd}(24, 10) = 2$ qui divise 4 . Donc cette équation admet au moins une solution.

On a par l'algorithme d'Euclide :

$$\begin{aligned} 24 &= 2 \times 10 + 4 \\ 10 &= 2 \times 4 + 2 \\ 4 &= 2 \times 2 + 0 \end{aligned}$$

Ainsi,

$$\begin{aligned} 2 &= 10 - 2 \times 4 \\ &= 10 - 2 \times (24 - 2 \times 10) \\ &= 24 \times (-2) + 10 \times 5. \end{aligned}$$

Il s'ensuit que $24 \times (-4) + 10 \times (10) = 4$ et donc que $24 \times (-4) \equiv 4 \bmod 10$. Donc $x_0 = -4$ est une solution particulière.

Cherchons la solution générale. Soit $x \in \mathbb{Z}$ solution

$$\begin{aligned} 24x \equiv 4 \bmod 10 &\iff 24x \equiv 24x_0 \quad \bmod 10 \\ &\iff 10 \mid 24(x+4) \\ &\iff 5 \mid 12(x+4) \\ &\iff 5 \mid x+4 \text{ par le théorème de Gauss} \\ &\iff \exists k \in \mathbb{Z} : x = -4 + 5k. \end{aligned}$$

L'ensemble des solutions de l'équation est donc

$$\mathcal{S} = \{-4 + 5k \in \mathbb{Z} \mid k \in \mathbb{Z}\}.$$

3.7 Système d'équations diophantiennes

On considère le système

$$(2) \begin{cases} x \equiv a \mod n \\ x \equiv b \mod m \end{cases}$$

Proposition 41

Soient $m, n \geq 2$. Le système (2) admet une solution si et seulement si pgcd $(m, n) \mid (a - b)$.

Théorème 18

On suppose que $d = \text{pgcd}(n, m)$ divise $a - b$. Soient $n' = \frac{n}{d}, m' = \frac{m}{d}$ et $(u, v) \in \mathbb{Z}^2$ vérifiant $n'u + m'v = 1$. Alors l'entier

$$x_0 = bn'u + am'v$$

est une solution particulière du système précédent. De plus, ce système est équivalent à l'équation

$$x \equiv x_0 \mod \text{ppcm}(m, n).$$

Ainsi, l'ensemble des solution du système (2) est donné par

$$\mathcal{S}' = \{x_0 + k \cdot \text{ppcm}(n, m) \mid k \in \mathbb{Z}\}.$$

3.8 Le petit théorème de Fermat

Définition 29

(Coefficients binomiaux) : Soient $0 \leq k \leq n$ deux entiers. On définit le coefficient binomial comme étant l'entier

$$C_n^k = \begin{pmatrix} n \\ k \end{pmatrix} = \frac{n!}{k!(n-k)!} \in \mathbb{N}.$$

où par définition pour un entier $p \in \mathbb{N}^*$, $p! = p(p-1)(p-2)\cdots 1$ et $0! = 1$.

Proposition 42

$$\begin{pmatrix} n \\ k \end{pmatrix} = \begin{pmatrix} n \\ n-k \end{pmatrix}, \quad \begin{pmatrix} n \\ 0 \end{pmatrix} = 1, \quad \begin{pmatrix} n \\ 1 \end{pmatrix} = n.$$

Proposition 43

(Formule de Pascal) :

$$\begin{pmatrix} n \\ k \end{pmatrix} + \begin{pmatrix} n \\ k+1 \end{pmatrix} = \begin{pmatrix} n+1 \\ k+1 \end{pmatrix}$$

Proposition 44

(**Formule du binome de Newton**) : Soient $x, y \in \mathbb{C}$. Alors pour tout $n \in \mathbb{N}^*$,

$$(x+y)^n = \sum_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix} x^k y^{n-k} = \sum_{i=0}^{n} \begin{pmatrix} n \\ i \end{pmatrix} x^{n-i} y^i$$

Lemme 16

Soit p un nombre premier. Si k est un entier tel que $0 < k < p$, alors p divise $\begin{pmatrix} p \\ k \end{pmatrix}$.

Théorème 19

(Petit théorème de Fermat) : Soit p un nombre premier. Si $x \in \mathbb{Z}$, alors on a

$$x^p \equiv x \bmod p$$

Corollaire 12

Soit p un nombre premier. Si p ne divise pas x, alors $x^{p-1} \equiv 1 \bmod p$.

Exemple : Calculons $7^{241} \bmod 13$. Puisque 13 est un nombre premier et que 13 ne divise pas 7 , on obtient $7^{12} \equiv 1 \bmod 13$. Comme $241 = 12 \times 20 + 1$, on en déduit que

$$7^{241} \equiv 7^{12\times 20+1} \equiv \left(7^{12}\right)^{20} \times 7 \equiv 1^{20} \times 7 \equiv 7 \bmod 13.$$