CHAPITRE 1

DIVISEURS ET CONGRUENCES

L'arithmétique des entiers est présente chez les mathématiciens grecs, par exemple dans "les éléments d'Euclide", chez **Nicomaque de Gérase**, **Théon de Smurne** ou encore **Diophante**. Les aspects algorithmiques sont présents depuis l'origine. Les congruences apparaissent à la fin du XVIII^{e} siècle dans les écrits de **Carl Friedrick Gauss**.

Les contenus du chapitre

▷ Divisibilité dans $\mathbb{Z}$.
▷ Division euclidienne d'un élément de $\mathbb{Z}$ par un élément de $\mathbb{N}^*$.
▷ Congruences dans $\mathbb{Z}$. Compatibilité des congruences avec les opérations.

Les capacités attendues du chapitre

▷ Déterminer les diviseurs d'un entier.
▷ Résoudre une congruence $ax \equiv b\ [n]$. Déterminer un inverse de a modulo n lorsque a et n sont premiers entre eux.
▷ Établir et utiliser des tests de divisibilité.
▷ Résoudre des équations diophantiennes simples.

Cours

1. Rappels sur les nombres entiers

1.1. Les entiers naturels

Définition 1 – Les entiers naturels

$\mathbb{N}$ est l'ensemble des entiers positifs ou nuls.

$$\mathbb{N} = \{0; 1; 2; 3; 4; 5; 6; ...\}$$

Propriété 1 – Stabilité de $\mathbb{N}$

$\mathbb{N}$ est stable pour l'addition et la multiplication seulement.
Pour tout $n \in \mathbb{N}$ et $m \in \mathbb{N}$, $m + n \in \mathbb{N}$ et $m \times n \in \mathbb{N}$

Par contre $\mathbb{N}$ n'est pas stable pour la soustraction et la division.
Exemples :
▷ $(+1) - (+3)$ n'existe pas dans $\mathbb{N}$.
▷ $\dfrac{+1}{+3}$ n'existe pas dans $\mathbb{N}$.

1.2. Les entiers relatifs

Définition 2 – Les entiers relatifs

$\mathbb{Z}$ est l'ensemble des entiers négatifs, positifs ou nuls.

$$\mathbb{Z} = \{...; -5; -4; -3; -2; -1; 0; 1; 2; 3; 4; 5; ...\}$$

Propriété 2 – Stabilité de $\mathbb{Z}$

$\mathbb{Z}$ est stable pour l'addition, soustraction et la multiplication seulement.
Pour tout $n \in \mathbb{Z}$ et $m \in \mathbb{Z}$, $m + n \in \mathbb{Z}$, $m - n \in \mathbb{Z}$ et $m \times n \in \mathbb{Z}$

Par contre $\mathbb{Z}$ n'est pas stable pour la division.
Exemple :
▷ $\dfrac{-1}{+3}$ n'existe pas dans $\mathbb{Z}$.

Propriété 3 – Opposé d'un relatif

Tout nombre entier relatif admet un opposé entier relatif.
Pour tout $n \in \mathbb{Z}$ alors $-n \in \mathbb{Z}$

Propriété 4 – $\mathbb{N}$ est inclus dans $\mathbb{Z}$

Tout nombre entier naturel est un entier relatif.
Pour tout $n \in \mathbb{N}$ alors $n \in \mathbb{Z}$

1.3. Axiomes importants

Le mot **axiome** vient du grec $\alpha\xi\iota\omega\mu\alpha$ (axioma), qui signifie "qui est considéré comme digne ou convenable" ou "qui est considéré comme **évident en soi**."
Pour certains philiosophes grecs de l'antiquité cela représentait une affirmation qu'ils considéraient comme évidente et qui n'avait nul besoin de preuve.

Axiome 1 – Partie non vide de $\mathbb{N}$

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

Exemple :
▷ $E = \{2;4;6;8;10;12;14;...\}$ admet 2 comme plus petit élément mais pas de plus grand élément.

Axiome 2 – Partie non vide majorée de $\mathbb{N}$

Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.

Exemple :
▷ $E = \{2;4;6;8;10;12;14\}$ admet 14 comme plus grand élément.

Axiome 3 – Suite d'entiers naturels

Toute suite d'entiers naturels strictement décroissante est stagnante en 0 à partir d'un certain rang.

Exemple :
▷ Dans l'algorithme d'Euclide, la suite des restes des divisions euclidiennes est une suite strictement décroissante d'entiers donc elle atteint 0 au bout d'un certain temps.
Cet axiome permet de prouver que certains algorithmes ne tournent pas à l'infini donc que les boucles s'arrêtent au bout d'un certain temps.

⚠ Dans $\mathbb{Z}$ l'axiome 1 et l'axiome 3 sont faux mais par contre l'axiome 2 reste vrai.

Axiome 4 – Suite d'entiers relatifs

Toute partie non vide et majorée de $\mathbb{Z}$ admet un plus grand élément.

Exemple :
▷ $E = \{...; -5; -4; -3\}$ admet -3 comme plus grand élément.

2. Diviseurs et multiples

2.1. Multiple d'un entier

On note m et n deux entiers relatifs.

Définition 3 – Multiple

On dit que m est un multiple de n si et seulement si il existe un entier relatif k tel que :

$$m = k \times n$$

Exemples :
▷ 15 est un multiple de 3.
▷ 0 est un multiple de tous les nombres entiers car pour tout $n \in \mathbb{Z}$, $0 = 0 \times n$.
▷ Les multiples de 7 sont $\{...; -21; -14; -7; 0; 7; 14; 21; ...\}$.
▷ Les multiples de -2 sont $\{...; -6; -4; -2; 0; 2; 4; 6; ...\}$.

2.2. Diviseur d'un entier

On note m et n deux entiers relatifs avec $n \neq 0$.

Définition 4 – Diviseur

On dit que n est un diviseur de m (ou que n divise m) si et seulement si il existe un entier relatif k tel que :

$$m = k \times n$$

m est donc un multiple de n.

Exemple :
▷ Les diviseurs de 12 sont $\{-12; -6; -4; -3; -2; -1; 1; 2; 3; 4; 6; 12\}$

Notation : on notera $n|m$ pour dire que n divise m.

Remarques :
▷ Pour tout $n \in \mathbb{Z}$, $1|n$ et $-1|n$.
▷ Pour tout $n \in \mathbb{Z}$, $n|0$.
▷ Pour tout $n \in \mathbb{Z}$, n admet au moins quatre diviseurs $\{-n; -1; 1; n\}$.

2.3. Propriétés sur la divisibilité

Propriété 5

Pour tout $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$,

$$\text{Si } b|a \text{ alors } -b|a$$

Démonstration

Si $b|a$ alors il existe $k \in \mathbb{Z}$ tel que $a = bk$.
On a donc $a = (-b) \times (-k)$ avec $-k \in \mathbb{Z}$,
donc $-b|a$

Exemple :
▷ $3|15$ et $-3|15$.

Propriété 6

Pour tout $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$,

$$\text{Si } b|a \text{ et } a \neq 0 \text{ alors } |b| \leq |a|$$

Démonstration

Si $b|a$ alors il existe $k \in \mathbb{Z}$ tel que $a = bk$.
On a donc $|a| = |bk| = |b||k|$ avec $|a| \neq 0$ et comme $|k| \in \mathbb{N}^*$,
alors $|b| \leq |a|$

Exemple :
▷ $-3|-15$ et $3|15$.

Propriété 7

Pour tout $a \in \mathbb{Z}^*$, $b \in \mathbb{Z}^*$ et $c \in \mathbb{Z}$,

$$\text{Si } b|a \text{ et } a|c \text{ alors } b|c$$

Démonstration

Si $b|a$ alors il existe $k_1 \in \mathbb{Z}$ tel que $a = bk_1$.
Si $a|c$ alors il existe $k_2 \in \mathbb{Z}$ tel que $c = ak_2$.
On a donc $c = ak_2 = (bk_1)k_2 = bk_1k_2 = b(k_1k_2)$ or $k_1k_2 \in \mathbb{Z}$
donc $b|c$.

Exemples :
▷ 3|15 et 15|210 alors 3|210.

Propriété 8

Pour tout $a \in \mathbb{Z}^*$ et $b \in \mathbb{Z}^*$,

$$\text{Si } b|a \text{ et } a|b \text{ alors } a = b \text{ ou } a = -b$$

Démonstration

D'après la propriété 6 :

Si $b|a$ alors $|b| \leq |a|$.
Si $a|b$ alors $|a| \leq |b|$.
On a donc $|b| \leq |a|$ et $|a| \leq |b|$ donc $|a| = |b|$
, ainsi $a = b$ ou $a = -b$.

Propriété 9

Pour tout $a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$,

$$\text{Si } b|a \text{ alors pour tout } c \in \mathbb{Z} \text{ on a } b|ac$$

Démonstration

Si $b|a$ alors il existe $k \in \mathbb{Z}$ tel que $a = bk$
Pour tout $c \in \mathbb{Z}$, on a donc,
$ac = bkc = b(kc)$ avec $kc \in \mathbb{Z}$,
donc $b|ac$.

Exemple :
▷ 3|15 alors 3|7 × 15 donc 3|105.

Propriété 10

Pour tout $a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$ et $c \in \mathbb{Z}$,

$$\text{Si } b|a \text{ et } b|c \text{ alors pour tout } u \in \mathbb{Z} \text{ et } v \in \mathbb{Z} \text{ alors } b|(au + cv)$$

On dit que si $b|a$ et $b|c$ alors b divise toute combinaison linéaire de a et de c.

Démonstration

Si $b|a$ alors il existe $k_1 \in \mathbb{Z}$ tel que $a = bk_1$
Si $b|c$ alors il existe $k_2 \in \mathbb{Z}$ tel que $c = bk_2$
On a donc pour tout $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$,
$au + cv = bk_1u + bk_2v = b(k_1u + k_2v)$ or $k_1u + k_2v \in \mathbb{Z}$
donc $b|(au + cv)$.

Exemple :
▷ $3|9$ et $3|12$ alors $3|(9 \times 11 + 12 \times 10)$ donc $3|219$.

Cette propriété est très importante dans les exercices et permet de répondre à de nombreuses questions.

Méthode 1 – Trouver des diviseurs communs

Exemple : on note $k \in \mathbb{N}$, $a = 6k + 5$ et $b = 8k + 3$
Montrer que a et b admettent seulement deux diviseurs communs positifs à a et b.

On cherche des diviseurs d de a et de b.
On va chercher une combinaison linéaire de a et b annulant les k.
$d|a$ et $d|b$ alors $d|4a - 3b$ donc $d|11$.
Or les seuls diviseurs positifs de 11 sont 1 et 11,
donc les seuls diviseurs communs positifs possible de a et b sont 1 et 11.

Propriété 11

Pour tout $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$,

Si $b|a$ alors pour tout $c \in \mathbb{Z}^*$ alors $bc|ac$

Démonstration

Si $b|a$ alors il existe $k \in \mathbb{Z}$ tel que $a = bk$.
Pour tout $c \in \mathbb{Z}^*$, on a $ac = bkc = (bc)k$,
donc $bc|ac$.

Exemple :
▷ $3|9$ donc $(3 \times 4)|(9 \times 4)$ ainsi $12|36$

3. Division euclidienne

On note $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$

Propriété 12 – Division euclidienne dans $\mathbb{N}$

Il existe un couple unique (q,r) d'entiers naturels tels que :

$$a = bq + r \text{ avec } 0 \leq r < b$$

On dit alors que q est le **quotient** et r le **reste** de la division euclidienne de b par a.

Démonstration

► Existence :
On note $E = \{n \in \mathbb{N} \text{ tels que } nb \leq a\}$

• $0 \times b = 0 \leq a$ donc E est non vide puisqu'il contient 0.
• E est donc une partie non vide et majorée de $\mathbb{N}$ donc d'après l'axiome 2 l'ensemble E admet un plus grand élément que l'on nomme q. De plus on nomme $r = a - bq$ et de ce fait on a bien $a = bq + r$.

Comme $q \in E$ alors $bq \leq a \Leftrightarrow a - bq \geq 0$ donc $r \geq 0$.
Comme $q + 1 \notin E$ alors $(q+1)b > a \Leftrightarrow a - bq < b$ donc $r < b$.
Conclusion :
Il existe un couple (q,r) d'entiers naturels tels que :

$$a = bq + r \text{ avec } 0 \leq r < b$$

► Unicité :
Raisonnons par l'absurde et supposons qu'il existe deux couples (q_1, r_1) et (q_2, r_2) d'entiers naturels tels que :
▷ $a = bq_1 + r_1$ avec $0 \leq r_1 < b$
▷ $a = bq_2 + r_2$ avec $0 \leq r_2 < b$
Par soustraction des deux égalités on obtient $0 = b(q_1 - q_2) + (r_1 - r_2)$ donc $r_1 - r_2 = b(q_2 - q_1)$ et b divise $r_1 - r_2$
▷ $0 \leq r_2 < b$ donc $-b < -r_2 \leq 0$ et comme $0 \leq r_1 < b$ alors par addition :

$$-b < r_1 - r_2 < b$$

or le seul multiple de b dans $]-b; b[$ est 0 donc $r_1 - r_2 = 0 \Leftrightarrow r_1 = r_2$.
Comme $r_1 = r_2$ alors $b(q_1 - q_2) = 0 \Leftrightarrow q_1 = q_2$ car $b \neq 0$.
Conclusion : le couple (q,r) est unique.

Exemple :
$17 = 5 \times 3 + 2$
3 est le quotient et 2 est le reste de la division euclidienne de 17 par 5.
5 est le quotient et 2 est le reste de la division euclidienne de 17 par 3.

Propriété 13 – Division euclidienne dans $\mathbb{Z}$

On note $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$.

Il existe un couple unique (q, r) où q est un entier relatif et r un entier naturel tels que :

$$a = bq + r \text{ avec } 0 \leq r < b$$

On dit alors que q est le **quotient** et r le **reste** de la division euclidienne de b par a.

Démonstration

► Existence :
On note $E = \{n \in \mathbb{Z} \text{ tels que } nb \leq a\}$.

• Si $a \geq 0$ alors $0 \times b = 0 \leq a$ donc E est non vide puisqu'il contient 0.
• Si $a < 0$ alors $ab \leq a$ donc E est non vide puisqu'il contient a.

• E est donc une partie non vide et majorée (par a ou par 0 suivant le signe de a) de $\mathbb{Z}$ donc d'après l'axiome 4, l'ensemble E admet un plus grand élément que l'on nomme q. De plus on nomme $r = a - bq$ et de ce fait on a bien $a = bq + r$.

Comme $q \in E$ alors $bq \leq a \Leftrightarrow a - bq \geq 0$ donc $r \geq 0$.
Comme $q + 1 \notin E$ alors $(q+1)b > a \Leftrightarrow a - bq < b$ donc $r < b$.
Conclusion :
Il existe un couple (q, r) où q est un entier relatif et r un entier naturel tels que :

$$a = bq + r \text{ avec } 0 \leq r < b.$$

► Unicité :
Raisonnons par l'absurde et supposons qu'il existe deux couples (q_1, r_1) et (q_2, r_2) d'entiers naturels tels que :
▷ $a = bq_1 + r_1$ avec $0 \leq r_1 < b$
▷ $a = bq_2 + r_2$ avec $0 \leq r_2 < b$
Par soustraction des deux égalités on obtient $0 = b(q_1 - q_2) + (r_1 - r_2)$ donc $r_1 - r_2 = b(q_2 - q_1)$ et b divise $r_1 - r_2$.
▷ $0 \leq r_2 < b$ donc $-b < -r_2 \leq 0$ et comme $0 \leq r_1 < b$ alors par addition :

$$-b < r_1 - r_2 < b$$

or le seul multiple de b dans $]-b; b[$ est 0 donc $r_1 - r_2 = 0 \Leftrightarrow r_1 = r_2$.
Comme $r_1 = r_2$ alors $b(q_1 - q_2) = 0 \Leftrightarrow q_1 = q_2$ car $b \neq 0$.
Conclusion : le couple (q, r) est unique.

Exemples :
▷ $-17 = 5 \times -4 + 3$

▷ $-126 = 7 \times -18 + 0$

⚠ Si on prend a et $b \in \mathbb{Z}^*$ alors il existe un couple unique (q, r) d'entiers relatifs tels que :

$$a = bq + r \text{ avec } 0 \leq r < |b|$$

Pour la démonstration on prendra $E = \{n \in \mathbb{Z} \text{ tels que } n|b| \leq a\}$.

4. Congruences

4.1. Définition

Définition 5 – Congruence

On note $n \geq 1$ un entier naturel, a et b deux entiers relatifs. On dit que a et b sont congrus modulo n et on note $a \equiv b\ [n]$ si la différence $a - b$ est un multiple de n ou si $n|(a-b)$

Exemples :

▷ $33 \equiv 13\ [5]$
▷ $29 \equiv -121\ [5]$
▷ $11 \equiv -1\ [12]$
▷ $15 \equiv 0\ [5]$

4.2. Propriétés

On note n et n' deux entiers naturels supérieurs ou égaux à 1, a et b deux entiers relatifs.

Propriété 14

$$a \equiv 0\ [n] \Leftrightarrow n|a$$

Démonstration

$\Rightarrow$
Si $a \equiv 0\ [n]$ alors $n|(a-0)$ donc $n|a$

$\Leftarrow$
Si $n|a$ alors il existe $k \in \mathbb{Z}$ tel que $a = kn$ donc $a - 0 = kn$ donc $a \equiv 0\ [n]$

Exemple :
▷ $3|39$ donc $39 \equiv 0\ [3]$

Méthode 2 – Démontrer qu'un nombre divise un autre

Exemple :
Démontrons le critère de divisibilité par 2 : un nombre est divisible par deux si et seulement si son chiffre des unités est pair.

On note $x = a_n a_{n-1} \ldots a_3 a_2 a_1 a_0$
On veut montrer que $2|x \Leftrightarrow 2|a_0$

$$x = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \ldots + a_3 \times 10^3 + a_2 \times 10^2 + a_1 \times 10 + a_0$$

Pour tout $k \in \mathbb{N}$, $2|10^k$ donc $10^k \equiv 0\ [2]$
On a donc

$$x \equiv 0\ [2] + 0\ [2] + \ldots + 0\ [2] + 0\ [2] + 0\ [2] + a_0 \equiv a_0\ [2]$$

Conclusion : $2|x \Leftrightarrow x \equiv 0\ [2] \Leftrightarrow a_0 \equiv 0\ [2] \Leftrightarrow 2|a_0$.

Propriété 15

Si $n'|n$ alors

$$\text{si } a \equiv b\ [n] \text{ alors } a \equiv b\ [n']$$

Démonstration

$n'|n$ donc il existe $k \in \mathbb{Z}$ tel que $n = kn'$,

$a \equiv b\ [n] \Leftrightarrow n|a-b$ donc il existe $k' \in \mathbb{Z}$ tel que $a - b = k'n = k'kn'$ avec $k'k \in \mathbb{Z}$
ainsi $n'|(a-b)$ et $a \equiv b\ [n']$.

Exemple :
$2|6$ et $57 \equiv 3\ [6]$ donc $57 \equiv 3\ [2]$.

Propriété 16

$$a \equiv b\ [n]$$

$$\Leftrightarrow$$

Les divisions euclidiennes de a et b par n ont le même reste.

Démonstration

Division de a par n : $a = qn + r$ avec $0 \leq r < n$
Division de b par n : $b = q'n + r'$ avec $0 \leq r' < n$ donc $-n < -r' \leq 0$
Par addition des deux inégalités on obtient : $-n < r - r' < n$.
$\Rightarrow$
Si $a \equiv b\ [n]$ alors $n|a-b$ donc $n|(n(q-q') + (r-r'))$ avec $-n < r - r' < n$.
$n|a-b$ et $n|n(q-q')$ donc n divise toutes les combinaisons linéaires de $a-b$ et $n(q-q')$ donc $n|((a-b) - n(q-q'))$ ainsi $n|r-r'$.
or le seul multiple de n dans $]-n;n[$ est 0 donc $r - r' = 0$ et $r = r'$.

$\Leftarrow$
Si les divisions euclidiennes de a et b par n ont le même reste alors $r = r'$.
On a donc $a - b = n(q-q')$ avec $q - q' \in \mathbb{Z}$ donc $n|a-b$ et $a \equiv b\ [n]$.

⚠ Si $a \equiv b\ [n]$ et si $0 \leq b < n$ alors b est le reste de la division euclidienne de a par n.

4.3. Congruences et opérations

On note a, a', b et b' quatre entiers relatifs quelconques.

Propriété 17 – Addition

Si $a \equiv a'\ [n]$ et $b \equiv b'\ [n]$ alors $a + b \equiv a' + b'\ [n]$

Démonstration

Si $a \equiv a'\ [n]$ alors il existe $k_1 \in \mathbb{Z}$ tel que $a - a' = k_1 n$.
Si $b \equiv b'\ [n]$ alors il existe $k_2 \in \mathbb{Z}$ tel que $b - b' = k_2 n$.
On a donc $(a-a') + (b-b') = k_1 n + k_2 n = (k_1 + k_2)n \Leftrightarrow (a+b) - (a'+b') = (k_1+k_2)n$
or $k_1 + k_2 \in \mathbb{Z}$ donc $(a+b) - (a'+b')$ est un multiple de n et $a + b \equiv a' + b'\ [n]$

Propriété 18 – Soustraction

Si $a \equiv a'\ [n]$ et $b \equiv b'\ [n]$ alors $a - b \equiv a' - b'\ [n]$

Démonstration

Si $a \equiv a'\ [n]$ alors il existe $k_1 \in \mathbb{Z}$ tel que $a - a' = k_1 n$.
Si $b \equiv b'\ [n]$ alors il existe $k_2 \in \mathbb{Z}$ tel que $b - b' = k_2 n$.
On a donc $(a-a') - (b-b') = k_1 n - k_2 n = (k_1 - k_2)n \Leftrightarrow (a-b) - (a'-b') = (k_1-k_2)n$
or $k_1 - k_2 \in \mathbb{Z}$ donc $(a-b) - (a'-b')$ est un multiple de n et $a - b \equiv a' - b'\ [n]$.

Propriété 19 – Produit par un entier relatif

Si $a \equiv a' \ [n]$ et $k \in \mathbb{Z}$ alors $ka \equiv ka' \ [n]$.

Démonstration

Si $a \equiv a' \ [n]$ alors il existe $\ell \in \mathbb{Z}$ tel que $a - a' = \ell n$.
On a donc $k(a-a') = k\ell n \Leftrightarrow ka - ka' = \underbrace{(k\ell)}_{\in\mathbb{Z}} n$ donc si $ka \equiv ka' \ [n]$.

Propriété 20 – Produit

Si $a \equiv a' \ [n]$ et $b \equiv b' \ [n]$ alors $a \times b \equiv a' \times b' \ [n]$.

Démonstration

Si $a \equiv a' \ [n]$ alors il existe $k_1 \in \mathbb{Z}$ tel que $a - a' = k_1 n$.
Si $b \equiv b' \ [n]$ alors il existe $k_2 \in \mathbb{Z}$ tel que $b - b' = k_2 n$.
On a donc :

$$\begin{aligned}(ab) - (a'b') &= ab - ab' + ab' - a'b' = a(b-b') + b'(a-a') = ak_2 n + b'k_1 n \\ &= (ak_2 + b'k_1)n\end{aligned}$$

or $ak_2 + b'k_1 \in \mathbb{Z}$ donc $(ab) - (a'b')$ est un multiple de n et $a \times b \equiv a' \times b' \ [n]$.

Propriété 21 – Puissances

Si $a \equiv b \ [n]$ et $r \in \mathbb{N}$ alors $a^r \equiv b^r \ [n]$.

Démonstration

On va faire une démonstration par récurrence :
On note $\mathbf{P}_r$ la propriété : $a^r \equiv b^r \ [n]$
Initialisation : (Pour $r = 0$)
$a^0 - b^0 = 1 - 1 = 0 = 0 \times n$ donc $a^0 \equiv b^0 \ [n]$ et $\mathbf{P}_0$ est vraie.
Hérédité : on suppose que $\mathbf{P}_k$ est vraie pour un rang k, montrons que dans ce cas $\mathbf{P}_{k+1}$ l'est aussi.
$a \equiv b \ [n]$ et $a^k \equiv b^k \ [n]$
donc d'après la propriété précédente $a \times a^k \equiv b \times b^k \ [n]$
et ainsi $a^{k+1} \equiv b^{k+1} \ [n]$ et $\mathbf{P}_{k+1}$ est vraie.
Conclusion :

$$\left.\begin{array}{l}\mathbf{P}_0 \text{ est vraie} \\ \mathbf{P}_k \text{ implique } \mathbf{P}_{k+1}\end{array}\right\} \text{ donc pour tout } r \in \mathbb{N} \ a^r \equiv b^r \ [n]$$

Méthode 3 – Reste de la division euclidienne

On utilise souvent les propriétés précédentes pour déterminer le reste d'une division euclidienne.
Si $a \equiv b\ [n]$ et si $0 \leq b < n$ alors b est le reste de la division euclidienne de a par n.

Exemple :
Déterminer le reste de la division euclidienne de 12^{1527} par 5.
$12^0 = 1 \equiv 1\ [5]$
$12^1 = 2 + 10 \equiv 2\ [5]$
$12^2 \equiv 12 \times 2\ [5] \equiv 4 + 20\ [5] \equiv 4\ [5]$
$12^3 \equiv 12 \times 4\ [5] \equiv -2 + 50\ [5] \equiv -2\ [5]$
$12^4 \equiv 12 \times (-2)\ [5] \equiv 1 - 25\ [5] \equiv 1\ [5]$

Comme $12^4 \equiv 1\ [5]$ alors pour tout $k \in \mathbb{N}$, $12^{4k} \equiv 1^k\ [5] \equiv 1\ [5]$

or $1527 = 4 \times 381 + 3$ donc $12^{1527} = 12^{4\times 381} \times 12^3$
or $12^{4\times 381} \equiv 1\ [5]$ et $12^3 \equiv -2\ [5]$
ainsi $12^{1527} \equiv 1 \times (-2)\ [5] \equiv -2\ [5] \equiv 3\ [5]$
Conclusion : le reste de la division euclidienne de 12^{1527} par 5 est 3.

4.4. Inverse de a modulo n avec a et n premiers entre eux

Définition 6 – Nombres premiers entre eux

Deux nombres a et n sont premiers entre eux s'ils n'ont pas de diviseurs communs à l'exception de 1.

Exemples :
▷ 4 et 35 sont premiers entre eux.
▷ 3 et 11 sont premiers entre eux.
▷ 4 et 14 ne sont pas premiers entre eux car 2 et 1 sont des diviseurs communs de 4 et 14.

Définition 7 – Inverse de a modulo n

On dit que b est un inverse de a modulo n si et seulement si $b \times a \equiv 1\ [n]$.

Exemples :

▷ -5 et 17 sont inverses modulo 43 car $-5 \times 17 \equiv 1\ [43]$
▷ 2 et 3 sont inverses modulo 5 car $2 \times 3 = 6 \equiv 1\ [5]$

4.5. Résolution de $ax \equiv b\ [n]$

On suppose que a et n sont premiers entre eux.

Propriété 22 – Résolution de $ax \equiv b\ [n]$

On note c l'inverse de a modulo n.

$$ax \equiv b\ [n] \Leftrightarrow x \equiv cb\ [n]$$

Démonstration

$ax \equiv b\ [n]$ et $ca \equiv 1\ [n]$
donc :

$$cax \equiv cb\ [n] \Leftrightarrow 1x \equiv cb\ [n] \Leftrightarrow x \equiv cb\ [n].$$

Exemple :
▷ On cherche à résoudre $2x \equiv 3\ [5]$

On commence par chercher l'inverse de 2 modulo 5.
$2 \times 3 = 6 \equiv 1\ [5]$ donc 3 est un inverse de 2 modulo 5.
On a donc :

$$2x \times 3 \equiv 3 \times 3\ [5] \Leftrightarrow x \equiv 9\ [5] \equiv 4\ [5].$$

5. Changement de base

En base 10 les nombres peuvent s'écrire à l'aide des puissances de 10 :

$$x = a_n.10^n + a_{n-1}.10^{n-1} + \ldots + a_1.10 + a_0$$

On peut écrire le même nombre en base 2 ou 3 ou 16 etc.

Par exemple, en base 2 les nombres s'écrivent à l'aide des puissances de 2 :

$$x = b_n.2^n + b_{n-1}.2^{n-1} + \ldots + b_1.2 + b_0$$

Le système binaire (base 2) est fondamental pour l'électronique ou en informatique car il se compose seulement de deux chiffres 0 et 1 le courant passe ou ne passe pas).

Méthode 4 – Système décimal vers système binaire

Pour passer du système décimal (base 10) au système binaire (base 2) on utilise la division euclidienne par 2.

Exemple : On souhaite convertir 234 en base 2.
$234 = 117 \times 2 + 0$

$117 = 58 \times 2 + 1$
$58 = 29 \times 2 + 0$
$29 = 14 \times 2 + 1$
$14 = 7 \times 2 + 0$
$7 = 3 \times 2 + 1$
$3 = 1 \times 2 + 1$
$1 = 0 \times 2 + 1$
donc en écriture binaire 234 est 11101010,
et $234 = 1 \times 2^7 + 1 \times 2^6 + 1 \times 2^5 + 0 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 0 \times 2^0$.

Méthode 5 – Convertir en base 5

Exemple : On souhaite convertir 234 en base 5.
$234 = 46 \times 5 + 4$
$46 = 9 \times 5 + 1$
$9 = 1 \times 5 + 4$
$1 = 0 \times 5 + 1$
donc en base cinq 234 est 1414
et $234 = 1 \times 5^3 + 4 \times 5^2 + 1 \times 5^1 + 4 \times 5^0$.

Méthode 6 – Convertir en base hexadécimale (16)

Exemple : On souhaite convertir 234 en base 16 (hexadécimale).
On dispose dans cette base de 16 symboles :0; 1; 2; 3; 4; 5; 6; 7; 8; 9; A; B; C; D; E; F
$234 = 14 \times 16 + 10$
$14 = 0 \times 16 + 14$
donc en base hexadécimale 234 est EA et ainsi prend beaucoup moins de mémoire que 234 ou 1414 ou 11101010.
La base hexadécimale est utilisée en informatique comme par exemple pour coder les différentes couleurs.