

Arithmétique dans  $\mathbb{Z}$ 

## I Divisibilité et division euclidienne

### 1 Multiples et diviseurs

#### Définition 1

Si  $a, b \in \mathbb{Z}$ , on dit que  $b$  **divise**  $a$  ou que  $a$  **est un multiple de**  $b$ , et on note  $b|a$  lorsque l'on a  $k \in \mathbb{Z}$  tel que  $a = kb$ .

L'ensemble des multiples de  $b$  est noté  $b\mathbb{Z}$ .

Si  $a|b$  et  $b|a$ ,  $a$  et  $b$  sont dit **associés**.

#### Remarques 1

R1 –  $b|a \iff$

R2 –  $b|a \iff$

R3 – Si  $a \neq 0$ ,  $b|a \implies \leq$

R4 – On s'intéresse souvent aux seuls diviseurs positifs.

#### Exemple 1

Diviseurs de 6 :

#### Propriétés 1

Soient  $a, b, c, d, k, \ell \in \mathbb{Z}$ .

(i) La relation  $|$  est

(ii)  $a$  et  $b$  sont associés si et seulement si si et seulement si

(iii)  $b|a \implies$

(iv)  $b|a$  et  $b|c \implies$

(v)  $b|a$  et  $d|c \implies$

(vi)  $b|a \implies \forall n \in \mathbb{N}$ ,

#### Remarque 1

Relation d'ordre sur

## 2 Division euclidienne

### Théorème 1 : Division euclidienne dans $\mathbb{Z}$

Soient  $a \in \mathbb{Z}$ ,  $b \in \mathbb{N}^*$ . Il existe un unique couple  $(q, r) \in \mathbb{Z}^2$  tel que

$$\left\{ \begin{array}{l} \\ \\ \end{array} \right.$$

$q$  est le quotient et  $r$  est le reste de la division euclidienne de  $a$  par  $b$ .

#### Remarque 2

$$q = \left\lfloor \frac{a}{b} \right\rfloor = \max \{k \in \mathbb{Z} \mid kb \leq a\}$$

(autre preuve possible).

### Propriété 1 : caractérisation de la divisibilité par le reste

Soient  $a \in \mathbb{Z}$ ,  $b \in \mathbb{N}^*$ .  $b|a$  si et seulement si le reste de la division euclidienne de  $a$  par  $b$  est nul.

## II Diviseurs communs

### 1 Définition

#### Définition – Propriété 1 : PGCD

Soient  $a, b \in \mathbb{N}$  dont l'un au moins est non nul. Alors l'ensemble des diviseurs (positifs) communs à  $a$  et  $b$  admet un plus grand élément, appelé **pgcd** de  $a$  et de  $b$ , noté  $a \wedge b$ . Par convention, on pose  $0 \wedge 0 = 0$ .

#### Exemple 2

$a = 12$  et  $b = 18$



**Remarques 2**

R1 –  $a \wedge 0 =$

R2 –  $a \wedge b = b \wedge a$

pour obtenir à chaque fois  $a \wedge b$  comme combinaison linéaire de  $r_k$  et  $r_{k-1}$ .

Si on a déjà  $a \wedge b = r_k U + r_{k+1} V$ , comme  $r_{k-1} = r_k q + r_{k+1}$ , on a alors

$$a \wedge b =$$

## 2 Algorithme d'Euclide

**Propriété 2 : Propriété d'Euclide**

Si  $(a, b) \in \mathbb{N}^2$ ,  $k \in \mathbb{N}$ , alors les diviseurs communs à  $a$  et  $b$  sont les diviseurs communs à  $a - bk$  et  $b$ , et en particulier  $a \wedge b = (a - bq) \wedge b$ .

**Propriété 3 : Algorithme d'Euclide**

Soient  $(a, b) \in \mathbb{N}^2 \setminus \{(0, 0)\}$ .  
On effectue les divisions euclidiennes successives

$$a = bq_1 + r_1$$

$$b = r_1q_2 + r_2$$

$$r_1 = r_2q_3 + r_3$$

⋮

$$\forall k, r_{k-1} = r_kq_{k+1} + r_{k+1}$$

$$\text{avec } 0 \leq r_{k+1} < r_k$$

(en notant  $a = r_{-1}$  et  $b = r_0$ ).

Le procédé s'arrête et le dernier reste non nul vaut  $a \wedge b$ .

**Algorithme d'Euclide étendu en Python et**

Ocaml : C'est facile en récursif.

Pour une version itérative, c'est plus compliqué.

- On peut garder en mémoire les quotients successifs puis les parcourir de nouveau pour les calculs successifs de  $u$  et  $v$ .

```

Python
1 def euclide(a,b):
2     """renvoie (d, u, v) où
3     d = pgcd(a, b) et au + bv = d"""
4     r, r1, quotients = a, b, []
5     while r1 != 0:
6         # Algorithme d'Euclide
7         # avec mémor. des quot.
8         quotients.append(r // r1)
9         r, r1 = r1, r % r1
10        # k_e tour : r = r[k-1],
11        # r1 = r[k], quotients
12        #           = [q[0], ..., q[k]]
13    u, v = 1, 0
14    while quotients != []:
15        # Parcours de la liste des
16        #   quotients
17        q = quotients.pop()
18        u, v = v, u - q * v
19    return r, u, v
    
```

**Exercice 1 : Implémentations itérative et récursive en Python et Ocaml**

**Exemple 3**

$$360 \wedge 84 = 12.$$

## 3 Relation de Bézout

**Propriété 4 : Relation de Bézout**

Si  $(a, b) \in \mathbb{N}^2$ , on peut trouver  $(u, v) \in \mathbb{Z}^2$  tels que  $au + bv = a \wedge b$ .

On peut donc tirer des coefficients de Bezout de l'algorithme d'euclide en remontant les étapes

- On peut chercher à chaque étape  $u_k, v_k$  tels que  $au_k + bv_k = r_k$  :
  - ★  $r_{-1} = a$  donc  $(u_{-1}, v_{-1}) = (1, 0)$ ,
  - ★  $r_0 = b$  donc  $(u_0, v_0) = (0, 1)$ ,
  - ★ puis comme  $r_{k-1} = r_k \cdot q_{k+1} + r_{k+1}$ ,

$$r_{k+1} = r_{k-1} - q_{k+1} \cdot r_k = a \cdot (u_{k-1} - q_{k+1} \cdot u_k) + b \cdot (v_{k-1} - q_{k+1} \cdot v_k),$$

donc

$$\begin{cases} u_{k+1} = u_{k-1} - q_{k+1} \cdot u_k \\ v_{k+1} = v_{k-1} - q_{k+1} \cdot v_k \end{cases}$$

```

Python
1 def euclide2(a,b):
2     """renvoie (d, u, v) où
3     d = pgcd(a, b) et au + bv = d"""
4     r, r1 = a, b
5     u, v = 1, 0
6     u1, v1 = 0, 1
7     while r1 != 0:
8         q = r // r1
9         r, r1 = r1, r % r1
10        u, u1 = u1, u - q * u1
11        v, v1 = v1, v - q * v1
12    return r, u, v
    
```

À la fin de la  $k^e$  étape,  $r$  contient  $r_{k-1}$  et  $r1$  contient  $r_k$ , et  $u$  et  $v$  sont tels que  $a \cdot u + b \cdot v = r$  et  $a \cdot u1 + b \cdot v1 = r1$ .

**Exemples 1**

E1 – Avec 360 et 84

E2 – Même question avec 302 et 112

**Remarques 3**

R1 – Il n'y a pas unicité, toutes les solutions seront trouvées plus tard (équation diophantienne).

R2 – La relation de Bézout nous permet d'écrire  $a \wedge b \mathbb{Z} \subset a \mathbb{Z} + b \mathbb{Z}$ .

Comme  $a \wedge b$  divise  $a$  et  $b$ , on a aussi  $a \mathbb{Z} + b \mathbb{Z} \subset a \wedge b \mathbb{Z}$ .

Ainsi,  $a \mathbb{Z} + b \mathbb{Z} = a \wedge b \mathbb{Z}$ .

En fait, comme  $a \mathbb{Z} + b \mathbb{Z}$  est un sous-groupe de  $(\mathbb{Z}, +)$ , on sait qu'il s'écrit  $d \mathbb{Z}$  avec  $d \in \mathbb{N}$  unique. C'est une définition alternative du pgcd (qui redonne directement la relation de Bézout, donc.)

**4 Caractérisation du pgcd**

**Propriété 5 : Caractérisation du pgcd**

Soient  $(a, b) \in \mathbb{N}^2, d \in \mathbb{Z}$ .

$$d = a \wedge b \iff \left\{ \begin{array}{l} d \mid a \text{ et } d \mid b \\ \forall d' \mid a \text{ et } d' \mid b, d' \mid d \end{array} \right.$$

Ainsi,  $a \wedge b$  est le plus grand diviseur commun au sens de l'ordre  $\mid$  également.

**Remarque 3**

Il est alors cohérent de poser  $0 \wedge 0 = 0$ , avec  $0 = \max \mathbb{N}$  pour  $\mid$ .

**Corollaire 1**

Les diviseurs communs à  $a$  et  $b$  sont les diviseurs de  $a \wedge b$ .

**Propriété 6 : Factorisation dans un pgcd**

Soient  $(a, b) \in \mathbb{N}^2, c \in \mathbb{N}$ , alors

$$(ca) \wedge (cb) =$$

**5 Extension aux entiers relatifs**

**Définition 2 : pgcd dans  $\mathbb{Z}$**

Si  $(a, b) \in \mathbb{Z}^2$ , alors on pose  $a \wedge b = |a| \wedge |b|$ .

Il s'agit du **plus grand diviseur commun** à  $a$  et à  $b$ .

**Propriété 7**

(i) Les diviseurs communs à  $a$  et  $b$  sont les diviseurs de  $a \wedge b$ .

(ii) Si  $a = bq + r$  (pas nécessairement une division euclidienne),  $a \wedge b = b \wedge r$ .

(iii) On a  $u, v \in \mathbb{Z}$  tels que  $au + bv = a \wedge b$ .

(iv) Si  $c \in \mathbb{Z}$ ,  $\triangle!$   $(ca) \wedge (cb) = |c|(a \wedge b)$ .

**6 Extension à plus de deux entiers**

**Définition 3 : pgcd de plus de deux entiers**

Soient  $(a_1, \dots, a_n) \in \mathbb{Z}^n$ . On note  $a_1 \wedge a_2 \wedge \dots \wedge a_n = \bigwedge_{k=1}^n a_k$  le **plus grand diviseur commun** à  $a_1, a_2, \dots, a_n$  s'il sont non tous nuls, 0 sinon.



### Propriété 8 : Associativité du pgcd

Si  $a, b, c \in \mathbb{Z}$ ,

$$a \wedge b \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c).$$

Plus généralement, les diviseurs communs à  $a_1, \dots, a_n$  sont les diviseurs de  $\bigwedge_{k=1}^n a_k$  et

$$a_1 \wedge a_2 \wedge \dots \wedge a_n = (a_1 \wedge a_2 \wedge \dots \wedge a_{n-1}) \wedge a_n.$$

### Propriété 9 : Relation de Bézout

On a  $u_1, \dots, u_n \in \mathbb{Z}$  tels que

$$a_1 u_1 + \dots + a_n u_n = \bigwedge_{k=1}^n a_k.$$

### Remarque 5

Les sens  $\Leftarrow$  n'est pas valable pour un  $\text{pgcd} \neq 1$ .

### Propriété 10

Si  $(a, b) \in \mathbb{Z}^2$ ,  $d = a \wedge b$ . On a  $(a', b') \in \mathbb{Z}^2$  tel que

$$\begin{cases} d \in \mathbb{N} \\ a = da' \\ b = db' \\ a' \wedge b' = 1 \end{cases}$$

### Propriété 11

$$a \wedge bc = 1 \iff a \wedge b = 1 \text{ et } a \wedge c = 1$$

### Remarque 6

Se généralise à un produit d'un nombre quelconque d'entiers.

## III Nombres premiers entre eux

### 1 Définition

#### Définition 4 : Nombres premiers entre eux

$(a, b) \in \mathbb{Z}^2$  sont dits **premiers entre eux** lorsque

c'est-à-dire lorsque le seul diviseur positif commun à  $a$  et  $b$  est 1.

#### Exemple 4

12 et 35 sont premiers entre eux.

#### Remarque 4

Tout diviseur de  $a$  est alors premier avec tout diviseur de  $b$ .

### 2 Propriétés

#### Théorème 2 : Théorème de Bézout

$$a \wedge b = 1 \iff$$

### 3 Lemme de Gauß et applications

#### Théorème 3 : Lemme de Gauß

Si  $a \wedge b = 1$  et  $a \mid c$  alors  $b \mid c$

#### Corollaire 2


Si  $a \wedge b = 1$  tels que  $a \mid c$  et  $b \mid c$ , alors  $ab \mid c$ .

#### Remarque 7

C'est faux si  $a \wedge b \neq 1$  :  $6 \mid 24$  et  $8 \mid 24$  mais  $6 \times 8 \nmid 24$ .

#### Corollaire 3 : Fractions irréductibles

Tout nombre rationnel  $r \in \mathbb{Q}$  s'écrit de manière unique sous la forme  $\frac{p}{q}$  avec  $p \in \mathbb{Z}$ ,  $q \in \mathbb{N}^*$  et  $p \wedge q = 1$ .

 **Méthode : résolution des équations diophantiennes**  $ax+by=c$

où  $a, b, c \in \mathbb{Z}^*$  sont fixés, on cherche les solutions entières.

On a facilement qu'il y a des solutions si et seulement si  $d = a \wedge b | c$ .

Lorsque c'est le cas, on peut trouver une solution particulière  $(x_0, y_0)$  avec l'algorithme d'Euclide par exemple.

Alors, si  $(x, y)$  solution,  $ax+by = ax_0+by_0$  puis  $a(x-x_0) = b(y_0-y)$  donc  $a'(x-x_0) = b'(y_0-y)$  avec  $a' \wedge b' = 1$  en divisant par  $d$ .

Par lemme de Gauß, on a  $k \in \mathbb{Z}$  tel que  $x = x_0 + b'k$  puis en réinjectant  $y = y_0 - a'k$ .

On vérifie enfin que la réciproque étant vraie. Ensemble des solutions :

$$\{(x_0 + b'k, y_0 - a'k) \mid k \in \mathbb{Z}\}.$$

**Exemple 5**

$$199x + 54y = 4.$$

**4 Généralisation à plus de deux entiers**

**Définition 5**

$a_1, \dots, a_n$  sont dits premiers entre eux dans leur ensemble lorsque  $\prod_{k=1}^n a_k = 1$ , c'est-à-dire que le seul diviseur positif commun à tous les  $a_k$  est 1.

$a_1, \dots, a_n$  sont dits premiers entre eux deux à deux lorsque  $\forall i \neq j, a_i \wedge a_j = 1$ .

**Exemple 6**

12, 15 et 20 sont premiers entre eux dans leur ensemble, mais pas deux à deux.

**Propriété 12**

Premiers entre eux deux à deux  $\implies$  premiers entre eux dans leur ensemble, mais la réciproque est fausse pour plus de deux entiers.

**Propriété 13 : Théorème de Bézout**

$a_1, \dots, a_n$  sont premiers entre eux dans leur ensemble si et seulement si on a  $u_1, \dots, u_n \in \mathbb{Z}$  tels que  $a_1u_1 + \dots + a_nu_n = 1$ .

**Propriété 14**

Si  $a_1, \dots, a_n$  sont premiers entre eux deux à deux et divisent  $c$ , alors  $a_1 \dots a_n | c$ .

**Remarque 8**

Faux si seulement premiers entre eux dans leur ensemble

**IV Multiples communs**

**1 Définition et caractérisation du ppcm**

**Définition – Propriété 2 : PPCM**

Soient  $a, b \in \mathbb{N}^*$ . Alors l'ensemble des multiples **strictement positifs** communs à  $a$  et  $b$  admet un plus petit élément, appelé **ppcm** de  $a$  et de  $b$ , noté  $a \vee b$ .

On pose, de plus,  $a \vee 0 = 0 \vee b = 0 \vee 0 = 0$ .

**Remarques 4**

**R1** –  $a \vee b = b \vee a$

**R2** – Utile pour mettre au même dénominateur!

**R3** – Cette fois, c'est l'ensemble des multiples communs de  $a$  et  $b$ ,  $a\mathbb{Z} \cap b\mathbb{Z}$  qui est un sous-groupe de  $(\mathbb{Z}, +)$  donc  $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$  avec  $m \in \mathbb{N}$  unique étant le ppcm de  $a$  et  $b$ .

**Exemple 7**

Multiples  $> 0$  de 6 : 6, 12, 18, ...  
 Multiples  $> 0$  de 9 : 9, 18, ...  
 Donc  $6 \vee 9 = 18$ .



### Propriété 15 : Caractérisation du ppcm

Soient  $(a, b) \in (\mathbb{N})^2$ ,  $m \in \mathbb{Z}$ .

$$m = a \vee b \iff \left\{ \begin{array}{l} m \text{ est multiple de } a \\ m \text{ est multiple de } b \end{array} \right.$$

Ainsi,  $a \vee b$  est le plus petit multiple commun  $> 0$  au sens de l'ordre | également.

### Corollaire 4

Les multiples communs à  $a$  et  $b$  sont les multiples de  $a \vee b$ .

### Propriété 16

Si  $a, b, c \in \mathbb{N}$ ,  $(ca) \vee (cb) = c(a \vee b)$ .

## 2 Lien avec le pgcd

### Propriété 17

Si  $a, b \in \mathbb{N}$ ,

$$(a \wedge b)(a \vee b) = ab.$$

En particulier, si  $a \wedge b = 1$ ,

$$a \vee b = ab.$$

### Exemple 8

$$6 \wedge 9 = 3 \text{ donc } 6 \vee 9 = \frac{6 \times 9}{3} = 18.$$

$$\text{Ou : } 6 \vee 9 = 3(2 \vee 3) = 3 \times 6 = 18.$$

## 3 Extension aux entiers relatifs

### Définition 6

Si  $(a, b) \in \mathbb{Z}^2$ , alors on pose  $a \vee b = |a| \vee |b|$ .

Il s'agit du plus petit multiple commun  $> 0$  de  $a$  et  $b$  s'ils sont non nuls.

### Propriété 18

(i) Si  $c \in \mathbb{Z}$ ,  $\triangleleft (ca) \vee (cb) = |c|(a \vee b)$ .

(ii)  $\triangleleft (a \wedge b)(a \vee b) = |ab|$ .

## V Nombres premiers

### 1 Définition

#### Définition 7 : Nombre premier

Un **nombre premier** est

On notera  $\mathcal{P}$  l'ensemble des nombres premiers.

#### Remarques 5

**R1** – 1 n'est pas premier.

**R2** – 2 est le seul nombre premier pair.

**R3** – Un nombre premier possède exactement 4 diviseurs :  $\pm 1$  et  $\pm p$ .

**R4** – Pour qu'un nombre entier  $n$  soit premier, il faut et il suffit qu'il n'ait pas de diviseur entre 2 et  $\sqrt{n}$ . D'où un test basique de primalité en Python .

**R5** – **Crible d'Eratosthène** : Pour déterminer les nombres premiers  $\leq n$ , il suffit de dessiner dans un tableau contenant tous les entiers de 2 à  $n$ , puis barrer successivement les multiples (stricts) de 2, puis de 3, etc. jusqu'à  $\sqrt{n}$ .

À implémenter en Python .

### 2 Propriétés

#### Propriété 19

Tout entier  $\notin \{0, \pm 1\}$  possède un diviseur premier.

**Remarques 6**

**R1** – Tout entier  $n \in \mathbb{N}^* \setminus \{1\}$  composé possède un diviseur premier  $\leq \sqrt{n}$  (car si  $n = k\ell$  alors  $k \leq \sqrt{n}$  ou  $\ell \leq \sqrt{n}$ .)

**R2** – Conséquence :  $a$  et  $b$  sont premiers entre eux si et seulement s'ils n'ont pas de diviseur premier en commun.

**Propriété 20**

L'ensemble des nombres premiers est infini.

**Propriété 21**

Si  $p \in \mathcal{P}$  et  $n \in \mathbb{Z}$ , soit  $p|n$ , soit  $p \wedge n = 1$ .

**Propriété 22**

Soient  $p \in \mathcal{P}$  et  $a_1, \dots, a_n \in \mathbb{Z}$ .  
 $p|(a_1 \times \dots \times a_n)$  si et seulement si  $p$  divise l'un des  $a_k$ .

**Remarque 9**

C'est faux si  $p$  n'est pas premier!

**3 Décomposition primaire et valuations  $p$ -adiques**

**Théorème 4 : Décomposition primaire**

Soit  $n \in \mathbb{Z}^*$ . On peut trouver  $k \in \mathbb{N}$ ,  $p_1, \dots, p_k$  premiers deux à deux distincts,  $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$  tels que

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

appelée décomposition primaire de  $n$ .

De plus, cette écriture est unique à l'ordre des facteurs près.

$p_1, \dots, p_k$  sont les diviseurs premiers de  $n$ .

**Remarque 10**

Cette décomposition peut aussi s'écrire  $n = \pm \prod_{p \in \mathcal{P}} p^{\alpha_p}$  avec les  $\alpha_p$  éventuellement nuls lorsque  $p$  n'est pas un diviseur de  $n$ . Les coefficients  $\alpha_p$  sont toujours uniques.

**Exemple 9**

7007

**Définition 8 : valuation  $p$ -adique**

Soit  $p \in \mathcal{P}$  et  $n \in \mathbb{Z}^*$ .

On appelle **valuation  $p$ -adique** de  $n$  l'entier

$$v_p(n) = \max \{i \in \mathbb{N} \mid p^i | n\}.$$

**Exemple 10**

Avec 7007

**Remarque 11**

La décomposition primaire se réécrit

$$n = \pm \prod_{p \in \mathcal{P}, p|n} p^{v_p(n)} = \pm \prod_{p \in \mathcal{P}} p^{v_p(n)}.$$

**Propriété 23**

Soient  $n, m \in \mathbb{Z}^*$ ,  $p \in \mathcal{P}$ .

(i)  $v_p(n) \neq 0 \iff$

(ii)  $v_p(n \times m) =$

(iii)  $n|m \iff$

(iv)  $v_p(n \wedge m) =$

et  $v_p(n \vee m) =$

**Propriété 24**

Si  $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  et  $b = \pm p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$  avec des exposants éventuellement nuls et chaque  $p_i$  premier, alors

$$a \wedge b = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \dots p_k^{\min(\alpha_k, \beta_k)}$$

et

$$a \vee b = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \dots p_k^{\max(\alpha_k, \beta_k)}.$$

**Exemple 11**

$352 \wedge 1452$

**Exercices 1**

**Ex1** – Si  $p$  est premier, montrer que  $\sqrt{p} \notin \mathbb{Q}$ .

**Ex2** – Déterminer le nombre de diviseurs positifs de  $n$ .



# VI Congruences

## 1 Définition (rappel)

### Définition 9 : Congruence

Soit  $n \in \mathbb{N}^*$ . On dit que  $a, b \in \mathbb{Z}$  sont **congrus modulo  $n$**  et on note  $a \equiv b [n]$  lorsque

$$n | (a - b)$$

ie lorsqu'il existe  $k \in \mathbb{Z}$  tel que  $a = b + kn$ .

### Remarque 12

On a déjà vu qu'il s'agit d'une relation d'équivalence, dont l'ensemble des classes noté  $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$  contient les entiers modulo  $n$ .

## 2 Propriétés

### Propriété 25

$$\forall a \in \mathbb{Z}, \exists ! r \in [0, n-1], a \equiv r [n].$$

$r$  est le reste de la division euclidienne de  $k$  par  $n$ .

Il y a donc exactement  $n$  classes d'équivalences :  $\bar{0}, \bar{1}, \dots, \overline{n-1}$ .

### Propriété 26

$$n | k \iff k \equiv 0 [n]$$

### Propriété 27 : Compatibilité de + et ×

Soient  $n \in \mathbb{N}^*$  et  $a, b, c, d \in \mathbb{Z}$  tels que  $a \equiv b [n]$  et  $c \equiv d [n]$ .

alors

$$a + c \equiv b + d [n]$$

et

$$a \times c \equiv b \times d [n].$$

Plus généralement, si  $m \in \mathbb{N}$ ,

$$a^m \equiv b^m [n].$$

### Exemples 2

E1 – Reste de la division euclidienne de  $2^{10}$  par 3 ?

E2 –  $\forall n \in \mathbb{N}, 7 | 3^{2n+1} + 2^{n+2}$

### Remarques 7

R1 – Pour effectuer des calculs modulaires, il est souvent intéressant de se ramener à un nombre le plus petit possible en valeurs absolue : entre  $-\lfloor \frac{n}{2} \rfloor$  et  $\lfloor \frac{n}{2} \rfloor$ .

R2 – Ces propriétés permettent de créer des lois + et × sur  $\mathbb{Z}/n\mathbb{Z}$  (la somme et le produit de deux entiers modulo  $n$  ne dépendent pas des représentants choisis.)

### Propriété 28

Soit  $c \neq 0$ .

(i)  $ac \equiv bc [nc] \Rightarrow a \equiv b [n].$

(ii) Si  $c \wedge n = 1$  alors  $ac \equiv bc [n] \Rightarrow a \equiv b [n].$

### Remarque 13

Pour que  $\bar{k}$  soit inversible dans  $\mathbb{Z}/n\mathbb{Z}$ , il faut trouver  $\bar{\ell}$  tel que  $\bar{k} \times \bar{\ell} = \bar{1}$ , c'est-à-dire  $k\ell \equiv 1 [n]$  soit encore  $k\ell + np = 1$  ce qui équivaut à  $k \wedge n = 1$ .

En particulier,  $\mathbb{Z}/n\mathbb{Z}$  est un corps si et seulement si  $n$  est un nombre premier.

### Exemple 12

$$2 \equiv 12 [10] \text{ mais } 1 \not\equiv 6 [10].$$

$$\text{Cependant, } 1 \equiv 6 [5].$$

## 3 Petit théorème de Fermat

### Lemme 1

Soit  $p$  un nombre premier et  $k \in [1, p-1]$ . Alors  $p | \binom{p}{k}$ .

**Théorème 5 : Petit théorème de Fermat**

Soit  $p$  un nombre premier et  $a \in \mathbb{Z}$ .

En particulier, si  $p \nmid a$ , alors  $a^{p-1} \equiv 1 \pmod{p}$ .

**Divisibilité par 4 :**

**Remarque 14**

Si  $p|a$ ,  $a^{p-1} \equiv 0 \pmod{p}$ .

**Divisibilité par 5 :**

**Exemple 13**

Reste de la division euclidienne de  $2713^{217}$  par 5

**Divisibilité par 8 :**

**4 Critères de divisibilité**

Si  $a_0, \dots, a_k$  sont les chiffres de  $n$  en base 10,

$$n = a_0 + a_1 \times 10 + \dots + a_k \times 10^k,$$

$$\forall i \in \llbracket 0, k \rrbracket, a_i \in \llbracket 0, 9 \rrbracket.$$

**Divisibilité par 9 :**

**Divisibilité par 2 :**

**Divisibilité par 11 :**

**Divisibilité par 3 :**

**Exercices 2**

**Ex 1** – Justifier que le calcul

$$1\,994\,996 \times 26\,399\,273 = 52\,666\,454\,037\,908$$

est faux .

**Ex 2** – Soit  $n = 4444^{4444}$ .

$f : k \mapsto$  somme des chiffres de  $k$ .

Calculer  $f \circ f \circ f(n)$ .