

# Chapitre 11

## $\mathbb{N}$ et Arithmétique dans $\mathbb{Z}$

---

### 11.1 Arithmétique dans $\mathbb{Z}$

---

#### 11.1.1 Division Euclidienne

Th. ▷ Division euclidienne

Soient  $a$  un entier relatif et  $b$  un entier naturel non nul.

$$\exists! (q, r) \in \mathbb{Z}^2 \mid a = bq + r \text{ et } 0 \leq r < b$$

On dit qu'on a effectué la division euclidienne de  $a$  par  $b$ .  
 $q$  est le quotient et  $r$  le reste de la division euclidienne.

#### 11.1.2 Division et multiples

Soit  $a$  et  $b$  dans  $\mathbb{Z}$ .

Dire que  $a$  divise  $b$  (ou  $b$  est multiple de  $a$ ) ssi  $\exists n \in \mathbb{Z}$  tel que  $b = na$ .

On note  $a|b$ .

**Important:**

$$a|b \Leftrightarrow b \in a\mathbb{Z} \Leftrightarrow b\mathbb{Z} \subset a\mathbb{Z}$$



- La relation "divise" est une relation d'ordre partiel sur  $\mathbb{N}$  mais n'est pas un ordre sur  $\mathbb{Z}$

#### 11.1.3 Congruence

Dire que  $\mathcal{R}$  est une relation d'équivalence sur un ensemble  $E$  signifie que  $\mathcal{R}$  est

- réflexive :  $\forall x \in E, x\mathcal{R}x$ .
- symétrique :  $\forall (x, y) \in E^2, x\mathcal{R}y \Rightarrow y\mathcal{R}x$ .
- transitive :  $\forall (x, y, z) \in E^3, (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z$ .

Th. ▷ Relation d'équivalence

Soit  $n \in \mathbb{N}$ .

La relation définie sur  $\mathbb{Z}$  par  $x \equiv y[n] \Leftrightarrow \exists k \in \mathbb{Z} \ x - y = kn$  est une relation d'équivalence.

**Test 286**

Soit  $n \in \mathbb{N}$ . Montrer que  $x \equiv y[n] \Leftrightarrow x$  et  $y$  ont le même reste dans la division euclidienne par  $n$ .

Soit  $\mathcal{R}$  une relation d'équivalence sur une ensemble  $E$  et soit  $x \in E$ ,

On appelle classe d'équivalence de  $x$  pour  $\mathcal{R}$  l'ensemble  $\{y \in E \mid x\mathcal{R}y\}$ ; cet ensemble est noté  $\bar{x}$  ou  $cl(x)$ .

Un sous-ensemble  $X$  de  $E$  est une classe d'équivalence s'il existe  $x \in E$  tel que  $X = \bar{x}$ , un tel  $x$  est alors appelé un représentant de  $X$ .

**Propriétés :**

Soit  $\mathcal{R}$  une relation d'équivalence sur un ensemble  $E$  et  $x, y$  deux éléments de  $E$ .

- $x\mathcal{R}y \implies y \in \bar{x} \implies \bar{x} = \bar{y}$
- Les classes d'équivalence forment une partition de  $E$ , autrement dit sont un ensemble de parties non vides, disjointes 2 à 2 et de réunion  $E$ .

Sur  $\mathbb{Z}$ , la congruence modulo  $n$  donne  $n$  classes d'équivalences :  $\bar{0}, \bar{1}, \dots, \overline{n-1}$ .

La congruence est compatible avec les opérations usuelles dans  $\mathbb{Z}$  :

- $x \equiv y [n] \iff x + a \equiv y + a [n]$  (équivalence)
- $x \equiv y [n] \implies xa \equiv ya [n]$  (implication seule)

**Test 287** Quelles sont les classes d'équivalence de la congruence modulo 2.

### 11.1.4 Les sous-groupes de $\mathbb{Z}$

$\mathbb{Z}$  est un groupe pour l'addition.

**Th.** ▷ Sous-groupes de  $\mathbb{Z}$

|| Tout sous-groupe de  $\mathbb{Z}$  est de la forme  $n\mathbb{Z}$  (il est engendré par un singleton)

$$n\mathbb{Z} = m\mathbb{Z} \iff |n| = |m|.$$

ainsi tout sous-groupe de  $\mathbb{Z}$  admet un unique générateur positif ou nul.

**Test 288**

- Soit  $G$  un sous-groupe de  $\mathbb{Z}$  qui contient les éléments 10 et 14.
1. Montrer que  $2 \in G$ .
  2. En déduire que soit  $G = \mathbb{Z}$ , soit  $G = 2\mathbb{Z}$ .

### 11.1.5 PPCM de deux entiers

$\forall a, b \in \mathbb{Z}$ ,  $a\mathbb{Z} \cap b\mathbb{Z}$  est un sous groupe de  $\mathbb{Z}$  donc admet un unique générateur positif  $m$  appelé le **Plus Petit Commun Multiple** de  $a$  et  $b$ .

**Justification de la dénomination**

- $m$  est multiple de  $a$  et  $b$
- Tout multiple commun à  $a$  et  $b$  est multiple de  $m$

**Test 289** Montrer que  $\text{PPCM}(10,15)=30$ .

**Test 290** Donner une condition nécessaire et suffisante sur  $a$  et  $b$  dans  $\mathbb{Z}$  pour que  $\text{PPCM}(a, b) = a$ .

**Propriétés :**

- L'opération PPCM définit une loi de composition interne sur  $\mathbb{Z}$  parfois notée " $\vee$ ".
- $\vee$  est associative  $\forall a, b, c \in \mathbb{Z}$ ,  $a \vee (b \vee c) = (a \vee b) \vee c$
- $\vee$  est commutative  $\forall a, b \in \mathbb{Z}$ ,  $a \vee b = b \vee a$
- $\forall a \in \mathbb{Z}$ ,  $a \vee 1 = |a|$
- $\forall a \in \mathbb{Z}$ ,  $a \vee 0 = 0$
- $\forall a, b, c \in \mathbb{Z}$ ,  $ac \vee bc = (a \vee b)|c|$

### 11.1.6 PGCD de deux entiers

$\forall a, b \in \mathbb{Z}$ ,  $a\mathbb{Z} + b\mathbb{Z}$  est un sous groupe de  $\mathbb{Z}$  donc admet un unique générateur positif  $d$  appelé le **Plus grand Commun Diviseur** de  $a$  et  $b$ .

**Justification de la dénomination**

- $d$  divise  $a$  et  $b$
- Tout diviseur commun à  $a$  et  $b$  divise  $d$

**Test 291** Montrer que  $\text{PGCD}(10,15)=5$ .

**Test 292** Donner une condition nécessaire et suffisante sur  $a$  et  $b$  dans  $\mathbb{Z}$  pour que  $\text{PGCD}(a, b) = a$ .

**Propriétés :**

- L'opération PGCD définit une loi de composition interne sur  $\mathbb{Z}$  parfois notée " $\wedge$ ".
- $\wedge$  est associative  $\forall a, b, c \in \mathbb{Z}, a \wedge (b \wedge c) = (a \wedge b) \wedge c$
- $\wedge$  est commutative  $\forall a, b \in \mathbb{Z}, a \wedge b = b \wedge a$
- $\forall a \in \mathbb{Z}, a \wedge 1 = 1$
- $\forall a \in \mathbb{Z}, a \wedge 0 = |a|$
- $\forall a, b, c \in \mathbb{Z}, ac \wedge bc = (a \wedge b)|c|$

**Test 293**

Montrer que si l'entier naturel  $d$  divise  $(a+b)^2$  et  $(a-b)^2$ , alors  $d$  divise  $4ab$  et divise  $2(a^2 + b^2)$ .  
En déduire que si  $\delta = \text{PGCD}((a+1)^2, (a-1)^2)$  alors  $\delta = 1$  ou  $\delta = 2$  ou  $\delta = 4$ .

**11.1.7 Algorithme d'euclide****Lemme :**

Si  $a = bq + r$  est la division euclidienne de  $a$  par  $b \in \mathbb{N}^*$ , alors

$$\text{PGCD}(a, b) = \text{PGCD}(b, r)$$

**L'algorithme d'euclide** (pour le calcul du PGCD)

Si  $a$  et  $b$  sont deux entiers relatifs avec  $b > 0$ , le PGCD de  $a$  et  $b$  est le dernier reste non nul dans la suite des divisions euclidiennes :

$$\begin{array}{rcl}
 a & = & bq_1 + r_1 \\
 b & = & r_1q_2 + r_2 \\
 r_1 & = & r_2q_3 + r_3 \\
 \dots & & \dots \\
 r_{n-2} & = & r_{n-1}q_n + \boxed{r_n} \quad \leftarrow \text{dernier reste non nul} \\
 r_{n-1} & = & r_nq_{n+1} + \mathbf{0}
 \end{array}$$

**Utilisation de l'algorithme pour déterminer  $p$  et  $q$** 

Si  $d = \text{PGCD}(a, b)$ , nous savons que :  $\exists p, q \in \mathbb{Z}, d = ap + bq$

On peut déterminer un des couples  $(p, q)$  en "remontant l'algorithme d'euclide".

**Test 294**

Utiliser l'algorithme d'euclide pour déterminer le PGCD de 4148 et 1122 que l'on notera  $d$   
En déduire deux entiers  $\alpha$  et  $\beta$  tels que  $d = \alpha 4148 + \beta 1122$

**Remarque**

Une présentation des calculs en 3 colonnes est possible :

| Division euclidienne         | Reste                        | Reste en fonction de $a$ et $b$ |
|------------------------------|------------------------------|---------------------------------|
| $4148 = 1122 \times 3 + 782$ | $782 = 4148 - 3 \times 1122$ | $782 = a - 3b$                  |
| $\vdots$                     | $\vdots$                     | $\vdots$                        |

**11.1.8 Théorèmes d'arithmétique**

Les entiers  $a$  et  $b$  sont **premiers entre eux** si et seulement si  $a \wedge b = 1$ .

**Attention :** ne pas confondre "nombre premier" et "premiers entre eux" qui ont des sens très différents. Deux entiers sont premiers entre eux si et seulement si 1 est le seul diviseur commun positif.

**Th. > Théorème de Bézout**<sup>1</sup>

Les entiers  $a$  et  $b$  sont premiers entre eux

$$\text{ssi} \quad \exists p, q \in \mathbb{Z} \quad a \cdot p + b \cdot q = 1$$

1. Etienne Bézout (1730-1783) mathématicien français

**Test 295**

En cherchant les diviseurs communs, montrer que  $2n+1$  et  $2(n+1)$  sont premiers entre eux. Confirmer ceci par le théorème de Bézout.

**Th.**  $\triangleright$  **Théorème de Gauss**<sup>2</sup>

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

$$\left. \begin{array}{l} a \text{ divise } bc \\ a \text{ premier avec } b \end{array} \right\} \begin{array}{l} a|bc \\ a \wedge b = 1 \end{array} \Rightarrow a|c \quad (a \text{ divise } c)$$

**Test 296**

Utiliser l'algorithme d'Euclide pour montrer que 125 et 12 sont premiers entre eux et pour trouver le couple  $(p_0, q_0)$  qui vérifie  $125p_0 + 12q_0 = 1$ .  
En déduire tous les couples  $(p, q)$  qui vérifient  $125p + 12q = 1$

**Test 297**

Trouver les couples  $(p, q)$  qui vérifient  $34p + 38q = 1$ .

**Trois théorèmes indispensables :**

- Si  $a$  est premier avec  $n$  nombres, alors  $a$  est premier avec leur produit.

$$\left. \begin{array}{l} a \wedge b_1 = 1 \\ a \wedge b_2 = 1 \end{array} \right\} \Rightarrow a \wedge (b_1 b_2) = 1$$

- Si  $n$  nombres premiers entre eux deux à deux divisent  $b$ , alors leur produit divise  $b$

$$\left. \begin{array}{l} a_1|b \\ a_2|b \\ a_1 \wedge a_2 = 1 \end{array} \right\} \Rightarrow a_1 a_2 | b$$

- Le PPCM de deux nombres premiers entre eux est leur produit (en valeur absolue)

$$a \wedge b = 1 \Rightarrow a \vee b = |ab|$$

**Très utile pour les exercices**

Les théorèmes manipulent principalement des nombres premiers entre eux. Pour pouvoir les utiliser avec des entiers quelconques  $a$  et  $b$ , on pose  $\delta = a \wedge b$ . L'exercice est équivalent à  $a = \delta a'$ ,  $b = \delta b'$  et  $a' \wedge b' = 1$ .

**Conséquences :**  $PPCM(a, b) \times PGCD(a, b) = |ab|$

**Test 298**

Trouver un couple d'entiers naturels  $a$  et  $b$  tels que  $a + b = 123PGCD(a, b)$

**Forme irréductible d'un rationnel**

Tout rationnel  $r$  s'écrit de manière unique sous la forme  $r = \frac{a}{b}$  où  $a \in \mathbb{Z}$ ,  $b \in \mathbb{N}^*$  et  $a \wedge b = 1$

**11.1.9 PGCD de  $n$  entiers**

Soient  $a_1, a_2, \dots, a_n$   $n$  entiers. Alors il existe un unique entier positif  $d$  tel que

- $d$  divise les  $a_k$  pour  $1 \leq k \leq n$ .
- pour tout  $d'$  entier divisant les  $a_k$ ,  $d'$  divise  $d$ .

$d$  est appelé **PGCD** des  $a_k$ , et est noté

$$d = \bigwedge_{k=1}^n a_k$$

Soit  $(a_k)_{1 \leq k \leq n}$  une famille finie de nombres entiers.

- Les  $a_k$  sont *premiers dans leur ensemble* si leur PGCD est 1.
- Les  $a_k$  sont *premiers deux à deux* si pour tout  $k \neq k'$ ,  $a_k$  et  $a_{k'}$  sont premiers entre eux.

2. Carl Friedrich GAUSS (1777-1855) mathématicien allemand

**Th.** ▷ **Relation de Bézout**

Si  $(a_k)_{1 \leq k \leq n}$  est une famille finie de nombres entiers de PGCD noté  $d$ , il existe une famille d'entiers  $(u_k)_{1 \leq k \leq n}$  telle que

$$\sum_{k=1}^n u_k a_k = d$$

## 11.2 Nombres premiers

### 11.2.1 Généralités

$p \in \mathbb{N}$  est un **nombre premier** ssi  $p$  admet exactement deux diviseurs dans  $\mathbb{N}$ , 1 et lui-même.

**Remarque :** Donc exactement 4 dans  $\mathbb{Z}$ . Et 1 n'est pas premier !

**Propriétés :**

- Si  $p$  est un nombre premier alors  $p$  est premier avec tous les entiers sauf avec ses multiples :

$$p \wedge a = 1 \Leftrightarrow a \notin p\mathbb{Z}$$

- Deux entiers naturels premiers et distincts sont premiers entre eux.
- Si  $a$  est premier et divise le produit  $bc$  alors  $a$  divise  $b$  ou  $c$

**Test 299**

Un nombre pair peut-il être premier ? En déduire tous les entiers naturels  $p$  premiers tels que  $p+1$  soit premier.

**Test 300**

$p$  est un naturel premier. Trouver tous les diviseurs dans  $\mathbb{N}$  de  $p^n$  ( $n \geq 2$ ) et leur somme.

### 11.2.2 Diviseurs premiers

**Propriétés :**

- Tout entier naturel  $n \geq 2$  admet au moins un diviseur premier
- L'ensemble des nombres premiers est infini

### 11.2.3 Décomposition en facteurs premiers

**Th.** ▷ **Décomposition en facteurs premiers**

Tout entier  $n \geq 2$  admet une et une seule décomposition en facteurs premiers (à l'ordre près) :

$$\forall n \geq 2 \exists k \in \mathbb{N}^* \exists p_1, p_2, \dots, p_k \text{ nombres premiers distincts } 2 \text{ à } 2,$$

$$\exists \alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{N}^* \quad n = \prod_{i=1}^k p_i^{\alpha_i}$$

**Corollaire :** Tout entier naturel  $n \geq 2$  non premier admet au moins un diviseur premier  $p$  vérifiant :  $p \leq \sqrt{n}$ .

Nous obtenons alors le critère de primalité suivant :

Soit  $n$  un entier naturel supérieur ou égal à 2.  
Si  $n$  n'est divisible par aucun nombre premier plus petit que sa racine carrée,  
alors  $n$  est premier.

**Test 301**

Quelle est la forme de la décomposition en facteurs premiers de tout diviseur naturel de 4200 ?  
En déduire le nombre de diviseurs.

Le résultat s'étend aux entiers relatifs quitte à mettre comme facteur un terme  $\epsilon \in \{-1; 1\}$ .

Si  $p$  est un nombre premier, la **Valuation p-adique**, ou  $p$ -valuation, d'un entier  $N$ , est l'entier  $\nu_p(N)$  exposant de  $p$  dans la décomposition de  $N$  en produit de facteurs premiers.

En particulier,  $\nu_p(N) = 0$  si  $p$  ne divise pas  $N$ .

Si l'on note  $\mathbb{P}$  l'ensemble des nombres premiers, on peut écrire

$$N = \prod_{p \in \mathbb{P}} p^{\nu_p(N)}$$

ce produit infini pouvant être vu comme fini dans la mesure où seul un nombre fini de termes  $p^{\nu_p(N)}$  est distinct de 1.

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Remarque</b> | <p>Si <math>a</math> et <math>b</math> sont deux entiers, alors</p> <ol style="list-style-type: none"> <li>1. <math>a</math> divise <math>b</math> si, et seulement si pour tout <math>p</math> premier, <math>\nu_p(a) \leq \nu_p(b)</math>.</li> <li>2. pour tout <math>p</math> premier, <math>\nu_p(ab) = \nu_p(a) + \nu_p(b)</math></li> <li>3. pour tout <math>p</math> premier, <math>\nu_p(a \wedge b) = \min(\nu_p(a), \nu_p(b))</math>.</li> <li>4. pour tout <math>p</math> premier, <math>\nu_p(a \vee b) = \max(\nu_p(a), \nu_p(b))</math>.</li> </ol> |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                    |                           |
|--------------------|---------------------------|
| <b>Utilisation</b> | recherche de PGCD et PPCM |
|--------------------|---------------------------|

**Test 302** Décomposer 208 et 270 en facteurs premiers. En déduire leur PGCD et PPCM.

### 11.3 Calculs avec les congruences

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Rappel</b> | <p>La congruence est une relation d'équivalence donc symétrique et transitive. Elle est compatible avec l'addition et partiellement avec la multiplication.</p> <p>► <math>x \equiv y [n] \Leftrightarrow x + a \equiv y + a[n]</math> (équivalence)</p> <p>► <math>x \equiv y [n] \Rightarrow xa \equiv ya[n]</math> (implication seule)</p> <p>Elle permet des calculs simplifiés, tous les résultats intermédiaires pouvant être ramenés à l'intervalle <math>\llbracket 0; n-1 \rrbracket</math>.</p> |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Multiplier au fur et à mesure en simplifiant à chaque fois.**

On pourra décomposer les nombres à multiplier et faire les multiplications successivement en simplifiant modulo  $[n]$  à chaque fois.

**Test 303** Soit  $a \in \mathbb{Z}$  tel que  $a \equiv 34[6]$ . Calculer modulo 6 le nombre  $22a$ .

**Trouver une puissance congrue à 1 ou à -1.**

Si  $z^b \equiv 1[n]$  alors pour toute puissance  $a$ , en déterminant la division euclidienne de  $a$  par  $b$  donnée par  $a = bq + r$ , on a

$$z^a \equiv z^{bq} z^r \equiv 1^q z^r \equiv z^r[n]$$

**Test 304** Déterminer le reste de la division euclidienne de  $2^{1495}$  par 15.

**Disjonction de cas sur les classes d'équivalence.**

On teste chacun des restes possibles dans la division euclidienne par  $n$ .

**Test 305** Soit  $x \in \mathbb{Z}$ . Résoudre  $x^2 \equiv 4[5]$ .

**Inverse modulaire.**

Soit  $a \in \mathbb{Z}$  premier avec  $n$ . On cherche  $u$  tel que  $au \equiv 1[n]$ .

$a$  et  $n$  étant premiers entre eux, par Bézout il existe  $(u, v) \in \mathbb{Z}^2$  tels que  $au + nv = 1$  autrement dit  $au \equiv 1[n]$ .

La descente et la remontée d'Euclide nous donne  $u$  de manière explicite.

Cette technique permet de résoudre des équations modulo  $[n]$ .

**Test 306**    Soit  $x \in \mathbb{Z}$ . Résoudre  $3x \equiv 7[16]$ .

**Th.** > **Combinaison et congruence**

Soit  $p$  un nombre premier.

1. Pour tout  $k \in \llbracket 1, p-1 \rrbracket$ , le coefficient binomial  $\binom{p}{k}$  est divisible par  $p$ .
2. Pour tout  $(a, b) \in \mathbb{Z}^2$ , on a  $(a+b)^p \equiv a^p + b^p [p]$



**Th.** > **Petit théorème de Fermat**<sup>3</sup>

|| Pour tout nombre premier  $p$  et tout entier relatif  $n$ , on a  $n^p \equiv n [p]$



3. Pierre de Fermat (1605-1665) mathématicien français

## 11.4 Exercices

---

**Exercice 1**

Soient  $a, b, c$  trois entiers relatifs. On considère l'équation :  $ax + by = c$ , dont on recherche les solutions dans  $\mathbb{Z}^2$ .

1. Donner une condition nécessaire et suffisante pour que cette équation admette une solution.
2. Soit  $(x_0, y_0)$  une solution du problème de Bézout :  $ax_0 + by_0 = c$ . Déterminer toutes les solutions de  $ax + by = c$  en fonction de  $a, b, c, d, x_0$  et  $y_0$ .
3. Résoudre dans  $\mathbb{Z}^2$  :  $2520x - 3960y = 6480$ .

**Exercice 2**

Résoudre dans  $\mathbb{Z}$  :

1.  $95x + 71y = 46$ .
2.  $20x - 53y = 3$ .
3.  $12x + 15y + 20z = 7$ .

**Exercice 3**

**Congruences simultanées**

Résoudre :

1. 
$$\begin{cases} x \equiv 2 \pmod{140} \\ x \equiv -3 \pmod{99} \end{cases}$$
2. 
$$\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv -2 \pmod{3} \\ x \equiv 7 \pmod{5} \end{cases}$$

**Exercice 4**

**Décomposition à coefficients positifs**

Soient  $a, b \in \mathbb{N}^*$  premiers entre eux. Montrer que :  $\forall x \geq ab, \exists u, v \in \mathbb{N}$  tels que  $au + bv = x$ .

**Exercice 5**

**Sommes de nombres impairs**

Soit  $n \in \mathbb{N}, n \geq 2$ . Montrer que si  $N$  est la somme de  $n$  nombres impairs consécutifs, alors  $N$  n'est pas premier.

**Exercice 6**

Montrer que :  $\forall n \in \mathbb{Z}, n^7 \equiv n \pmod{42}$ .

**Exercice 7**

1. Vérifier que  $10^6 \equiv 1 \pmod{7}$ .
2. Montrer que  $\sum_{k=1}^{10} (10^{10})^k \equiv 4 \pmod{7}$ .

**Exercice 8**

**Suites récurrentes linéaires**

Montrer que pour tout  $n \in \mathbb{N}$ ,  $3^{2n+1} + 2^{n+2}$  est divisible par 7.

**Exercice 9****Nombres de Mersenne**

On note  $M_n = 2^n - 1$  ( $n$ -ième nombre de Mersenne).

1. Montrer que :  $M_n$  est premier  $\Rightarrow n$  est premier.
2. Vérifier que  $M_{11}$  n'est pas premier.

**Exercice 10**

Soit  $n \in \mathbb{N}^*$ , déterminer le reste de la division euclidienne de  $2^{10n-7} + 3^{5n-2}$  par 11.

**Exercice 11****Cubes consécutifs**

Montrer que la somme de trois cubes consécutifs est toujours divisible par 9.

**Exercice 12**

Montrer que pour tout entier  $n \in \mathbb{Z}$ ,  $n(n+1)(7n+2)$  est divisible par 6.

**Exercice 13**

Soient  $a, b, c \in \mathbb{Z}$  tels que  $a \wedge b = 1$ . Montrer que  $a \wedge (bc) = a \wedge c$ .

**Exercice 14**

Soient  $a, b$  entiers,  $d = a \wedge b$ ,  $m = a \vee b$ . Chercher  $(a + b) \wedge m$ .

**Exercice 15****pgcd et ppcm imposés**

Soient  $d, m \in \mathbb{N}^*$ . Donner une condition nécessaire et suffisante sur  $d$  et  $m$  pour qu'il existe  $a, b \in \mathbb{Z}$  tels que  $a \wedge b = d$  et  $a \vee b = m$ .

Résoudre ce problème pour  $d = 50$  et  $m = 600$ .

## 11.5 Exercices Complémentaires

---

**Exercice 1**

Soient  $a, b, a', b' \in \mathbb{Z}$  avec  $b \wedge b' = 1$ . Montrer que le système :  $\begin{cases} x \equiv a [b] \\ x \equiv a' [b'] \end{cases}$  possède des solutions et qu'elles sont congrues entre elles modulo  $bb'$ . Généraliser.

**Exercice 2**

Une bande de 17 pirates dispose d'un butin composé de  $N$  pièces d'or d'égale valeur. Ils décident de se le partager également et de donner le reste au cuisinier (non pirate). Celui ci reçoit 3 pièces. Mais une rixe éclate et 6 pirates sont tués. Tout le butin est reconstitué et partagé entre les survivants comme précédemment ; le cuisinier reçoit alors 4 pièces.

Dans un naufrage ultérieur, seuls le butin, 6 pirates et le cuisinier sont sauvés. Le butin est à nouveau partagé de la même manière et le cuisinier reçoit 5 pièces.

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

**Exercice 3**

Soit  $p \in \mathbb{N}^*$  premier et  $n \in \mathbb{N}^*$ ,  $n < p$ . Montrer que  $\frac{(p-1)(p-2)\dots(p-n)}{n!} - (-1)^n$  est un entier divisible par  $p$ .

**Exercice 4**

Soient  $x, y \in \mathbb{N}$ ,  $y \geq 3$ . Montrer par récurrence sur  $y$  que :  $3^x \equiv 1 [2^y] \Leftrightarrow 2^{y-2} \mid x$ . Trouver tous les couples d'entiers  $x, y \in \mathbb{N}$  tels que  $3^x = 2^y + 1$ .

**Exercice 5**

Soient  $a, b, c \in \mathbb{N}^*$ . Quand a-t-on  $\text{pgcd}(a, b, c) \times \text{ppcm}(a, b, c) = abc$  ?

**Exercice 6**

Soient  $a, b \in \mathbb{N}^*$  premiers entre eux tels que  $ab$  est un carré parfait. Montrer que  $a$  et  $b$  sont des carrés parfaits.

**Exercice 7**

Soient  $a, b \in \mathbb{N}^*$  et  $m, n$  premiers entre eux tels que  $a^n = b^m$ . Montrer qu'il existe  $c \in \mathbb{N}^*$  tel que  $a = c^m$  et  $b = c^n$ .

**Exercice 8**

Soit  $n \in \mathbb{N}$ . Chercher  $(n^3 + n) \wedge (2n + 1)$ .

**Exercice 9**

Soient  $a, m, n \in \mathbb{N}^*$ ,  $a \geq 2$ , et  $d = (a^n - 1) \wedge (a^m - 1)$ .

1. Soit  $n = qm + r$  la division euclidienne de  $n$  par  $m$ . Démontrer que  $a^n \equiv a^r [a^m - 1]$ .
2. En déduire que  $d = (a^r - 1) \wedge (a^m - 1)$ , puis  $d = a^{(n \wedge m)} - 1$ .
3. A quelle condition  $a^m - 1$  divise-t-il  $a^n - 1$  ?