# Feuille d'exercices 4

## 1. Nombres premiers. PGCD. Algorithme d'Euclide. Relation de Bézout

**1.1.** Décomposer 999999 en produit de facteurs premiers et en déduire la liste de ses diviseurs.

**1.2.** Les nombres suivants sont-ils des carrés (respectivement des cubes) : $2^3 5^2 7^4$ ; $2^4 7^6 11^2$ ; $2^6 3^3 5^3$ ?

**1.3.** $a$ et $b$ sont-ils premiers entre eux pour $(a, b) = (241{,}120)$, $(2221{,}15)$, $(721{,}13)$ et $(346{,}12)$ ?

**1.4.** Décomposer $a$ et $b$ en produits de facteurs premiers ; en déduire le *pgcd* de $a$ et $b$ ainsi que la décomposition en produits de facteurs premiers du ppcm de $a$ et $b$ pour $(a, b) = (9348{,}1640)$, $(315{,}98)$, $(1050{,}735)$, $(306{,}198)$, $(169{,}36)$ et $(16900{,}3600)$.

**1.5.** Trouver les couples d'entiers naturels $(x, y)$ tels que $x + y = 224$ et $\text{pgcd}(x, y) = 16$.

**1.6.** Trouver les couples d'entiers naturels $(x, y)$ tels que $xy = 9072$ et $\text{pgcd}(x, y) = 18$.

**1.7.** Calculer les pgcd suivants en utilisant l'algorithme d'Euclide : $\text{pgcd}(94, 267)$, $\text{pgcd}(106, 317)$, $\text{pgcd}(82, 519)$, $\text{pgcd}(9348, 1640)$, $\text{pgcd}(1050, 735)$, $\text{pgcd}(306, 198)$.
En déduire une relation de Bézout de la forme $au + bv = \text{pgcd}(a, b)$.

**1.8.** Pour chaque couple $(a, b)$ ci-dessous, démontrer que $a$ et $b$ sont premiers entre eux et construire une relation de Bézout de la forme $au + bv = 1$ : $(a, b) = (25, 38)$, $(19, 54)$, $(18, 29)$, $(51, 148)$, $(94, 205)$, $(293, 107)$.

**1.9.**

1. Utiliser l'algorithme d'Euclide pour déterminer $\text{pgcd}(368, 161)$.
   En déduire une relation de Bézout de la forme
   $$368u + 161v = \text{pgcd}(368, 161)$$
2. Déterminer tous les entiers $x$ et $y$ tels que $368x + 161y = 115$.
3. Montrer que l'équation
   $$368x + 161y = 47$$
   n'admet pas des solutions entières.

**1.10.** Résoudre dans $\mathbb{Z}^2$ les équations :

1. $95x + 71y = 46$.
2. $20x - 53y = 3$.
3. $23x - 13y = 5$.
4. $10x - 3y = 2$.
5. $91x - 112y = 14$.
6. $91x - 112y = 10$.

## 2. Congruences

**2.1.** Montrer que si $n \equiv m\ (3)$, alors $n^3 \equiv m^3\ (9)$. En déduire que si $a^3 + b^3 + c^3$ est un multiple de 9, alors l'un au moins des entiers $a$, $b$, $c$ est multiple de 3.

**2.2.**

1. Quel est le reste de la division euclidienne de $692^{732}$ par 5 ?
2. Quel est le reste de la division euclidienne de $812^{4710}$ par 9 ?
3. Quel est le reste de la division euclidienne de $2^{18}$ par 37 ?

**2.3.** Soit $n$ un entier, dont l'écriture décimale est $a_N a_{N-1} \dots a_1 a_0$ (où $a_0, \dots, a_N$ sont des chiffres compris entre 0 et 9). Cela signifie qu'on a $n = a_N \times 10^N + a_{N-1} \times 10^{N-1} + \cdots + a_1 \times 10 + a_0$.
Montrer que $n$ est divisible par 11 si et seulement si la somme *alternée* de ses chiffres (c'est-à-dire $a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^N a_N$) est divisible par 11.

**2.4.**

1. Déterminer, pour chaque entier $n$ compris entre 0 et 6, le reste dans la division euclidienne de $3^n$ par 10.
2. Soit $n \in \mathbb{N}$ un entier quelconque. Exprimer, en fonction de $n$, le reste dans la division euclidienne de $3^n$ par 10.
3. Quel est le chiffre des unités dans l'écriture en base 10 de $2013^{2011}$ ?

## 3. $\mathbb{Z}/n\mathbb{Z}$

**3.1.**

1. Déterminer les éléments inversibles de $\mathbb{Z}/9\mathbb{Z}$ et préciser leurs inverses.
2. Résoudre dans $\mathbb{Z}/9\mathbb{Z}$ l'équation $\overline{5}X = \overline{7}$.
   Quels sont les entiers $x$ vérifiant $5x \equiv 7\ (9)$ ?
3. Résoudre dans $\mathbb{Z}/27\mathbb{Z}$ l'équation $\overline{15}X = \overline{21}$.

**3.2.**

1. Donner la liste des éléments inversibles de $\mathbb{Z}/12\mathbb{Z}$ et préciser leurs inverses.
2. Résoudre dans $\mathbb{Z}/12\mathbb{Z}$ l'équation $\overline{5}X = \overline{7}$.
3. Donner en fonction du paramètre $a \in \mathbb{Z}/12\mathbb{Z}$ les solutions de l'équation dans $\mathbb{Z}/12\mathbb{Z}$

$$a\,X = \overline{3}$$

**3.3.** Montrer que $\overline{34}$ est inversible dans $\mathbb{Z}/91\mathbb{Z}$ et calculer son inverse.

**3.4.**

1. Soit $b \in \mathbb{Z}$. Montrer qu'il existe $x \in \mathbb{Z}$ tel que

$$24x \equiv b\ (182) \qquad (E)$$

   si et seulement si $b$ est pair.
2. Supposons $b$ pair et posons $b = 2c$.
   Montrer que les entiers $x$ solutions de $(E)$ sont les entiers $x$ tels que $x \equiv 38c\ (91)$.

**3.5.** Résoudre dans $\mathbb{Z}/6\mathbb{Z}$ le système :

$$\begin{cases} \overline{2}X + \overline{3}Y = \overline{1} \\ \overline{1}X + \overline{4}Y = \overline{4} \end{cases}$$

**3.6.** Résoudre dans $\mathbb{Z}/5\mathbb{Z}$ le système :

$$\begin{cases} \overline{3}X + \overline{2}Y = \overline{1} \\ \overline{2}X + \overline{4}Y = \overline{3} \end{cases}$$

## 4. Petit théorème de Fermat

**4.1.** Soient $a$ et $b$ des entiers. Montrer que 3 divise $a^3 - b^3$ si et seulement si 3 divise $a - b$.

**4.2.** Soit $p$ un nombre premier. Montrer que pour tout $n \in \mathbb{N}$, $3^{n+p} - 3^{n+1}$ est divisible par $p$.

**4.3.** Montrer que, quel que soit l'entier $a$, $a^{13} - a$ est divisible par 26.

**4.4.** Déterminer le reste dans la division euclidienne de $44^{45}$ par 7.

**4.5.**

1. Montrer que 223 est un nombre premier.
2. Calculer $1998^{1998}$ modulo 223.

**4.6.** Déterminer le reste de la division euclidienne de $7^{1998}$ par 13.

**4.7.**

1. Factoriser 1729 en produit de nombres premiers.
2. Soient $a$ et $n$ des entiers positifs. Montrer que l'on a $a^n \equiv 1\ (1729)$ si et seulement si $a^n \equiv 1\ (7)$, $a^n \equiv 1\ (13)$ et $a^n \equiv 1\ (19)$.
3. Soit $a$ un entier positif tel que $\text{pgcd}(a, 1729) = 1$. Démontrer que l'on a $a^{1728} \equiv 1\ (1729)$.

**4.8.** Soient $p$ un nombre premier et $a$ un entier positif non multiple de $p$.

1. Montrer qu'il existe un plus petit entier positif $k$ tel que $a^k \equiv 1\ (p)$.
2. Soit $n \in \mathbb{N}$. Notons $r$ le reste de la division euclidienne de $n$ par $k$. Montrer que l'on a $a^n \equiv a^r\ (p)$.
3. Soit $n \in \mathbb{N}$. Montrer que l'on a $a^n \equiv 1\ (p)$ si et seulement si $n$ est multiple de $k$.

**4.9.** Cet exercice utilise le résultat de l'exercice précédent.

1. Soit $a$ un entier positif. Montrer que tous les chiffres de $a$ sont égaux à 1 si et seulement s'il existe un entier positif $n$ tel que $9a = 10^n - 1$.
2. Soit $n \in \mathbb{N}$. Montrer que l'on a $10^n \equiv 1\ (63)$ si et seulement si $10^n \equiv 1\ (7)$.
3. Trouver le plus petit entier positif $k$ tel que $10^k \equiv 1\ (7)$.
4. En déduire que 111111 est le plus petit multiple de 7 dont tous les chiffres sont égaux à 1.

## 5. Exercices supplémentaires

### 5.1. Cryptographie : Protocole d'échange de messages.

Alice et Bob veulent échanger des messages sans que le contenu puisse être lu par quelqu'un qui les intercepterait. Ils se mettent d'accord sur un nombre premier $p$ (qui peut éventuellement être connu de tout le monde). Si Alice veut envoyer le message $M$ à Bob, où $M$ est un entier avec $0 \leq M < p$, voici ce qu'ils font :

1) Alice choisit un entier $a$ premier avec $p-1$, puis calcule un entier $a'$ tel que $aa' \equiv 1\ (p-1)$. Elle garde $a$ et $a'$ secrets.

2) Bob fait de même pour avoir deux entiers $b, b'$ tels que $bb' \equiv 1\ (p-1)$. Il garde $b$ et $b'$ secrets.

3) Alice calcule $C_1 \equiv M^a\ (p)$ avec $0 \leq C_1 < p$ et envoie $C_1$ à Bob.

4) Bob calcule $C_2 \equiv (C_1)^b\ (p)$ avec $0 \leq C_2 < p$ et envoie $C_2$ à Alice.

5) Alice calcule $C_3 \equiv (C_2)^{a'}\ (p)$ avec $0 \leq C_3 < p$ et envoie $C_3$ à Bob.

6) Bob calcule $C_4 \equiv (C_3)^{b'}\ (p)$ avec $0 \leq C_4 < p$.

Montrer que $C_4 = M$.

*Ce protocole d'échange s'appelle "protocole des valises" par analogie avec la situation suivante : Alice met le message dans une valise et met un cadenas dont elle seule a la clé (c'est a). Bob reçoit la valise, met un autre cadenas (b) et renvoie la valise à Alice. Alice ouvre son propre cadenas ($a'$) et renvoie la valise. Bob peut alors ouvrir la valise en ouvrant son propre cadenas ($b'$). La valise est toujours fermée quand elle voyage. La sécurité supplémentaire est qu'il n'y a pas de transmission de clefs entre Alice et Bob.*

### 5.2. Un exemple de code correcteur d'erreurs : Le code ISBN.

Dans cet exercice, on s'intéresse aux codes ISBN à 10 symboles (depuis 2007, les numéros ISBN ont 13 symboles).

Tous les livres qui paraissent sont porteurs d'un numéro ISBN. Il s'agit d'une suite $x_1x_2\ldots x_{10}$ de 10 symboles. Les neuf premiers ($x_1$, ..., $x_9$) sont des chiffres, compris (au sens large) entre 0 et 9. Le dernier, $x_{10}$, peut être soit un chiffre (entre 0 et 9), soit la lettre $X$.

Les chiffres $x_1$, ..., $x_9$ codent des informations relatives au livre (langue, éditeur, numéro, ...). Le dernier symbole, $x_{10}$, est un chiffre de contrôle. Quand il s'agit de la lettre $X$, on convient de dire que c'est en fait le nombre 10. Ce symbole $x_{10}$ est alors un nombre compris entre 0 et 10 ; il est choisi de telle sorte que

$$1x_1 + 2x_2 + 3x_3 + 4x_4 + \ldots + 10x_{10}$$

soit un multiple de 11. On dit qu'une suite $x_1x_2\ldots x_{10}$ est un code ISBN valide si cette propriété est vérifiée.

L'intérêt de ce code (et notamment du chiffre de contrôle $x_{10}$) est qu'il permet de détecter des erreurs éventuelles (voir questions c) et d) ).

a) Le code 3540902449 est-il un code ISBN valide ?

b) Etant donnés $x_1$, ..., $x_9$, démontrer qu'il existe un nombre $x_{10}$ compris entre 0 et 10, et un seul, tel que $x_1x_2\ldots x_{10}$ soit un code ISBN valide.

c) On part d'un code ISBN valide, et on change la valeur d'un chiffre. Démontrer que le code ISBN obtenu n'est pas valide.

d) On part d'un code ISBN valide, et on permute deux chiffres. Démontrer que le code ISBN obtenu n'est pas valide.

e) Le code ISBN permet-il de corriger une erreur faite sur un chiffre ? Autrement dit, si on part d'un code ISBN valide, et que l'on change un chiffre (par exemple suite à une erreur en recopiant ce code), peut-on retrouver le code valide initial à partir du code erronné ?