**Feuille d'exercices n° 2**

ARITHMÉTIQUE

# 1 Division euclidienne

## 1.1 473 raisons de calculer

a) Effectuer la division euclidienne de 473 par 27.

b) Quel est le plus petit entier $x$ que l'on doit ajouter à 473 pour que, dans la division de $473 + x$ par 27, le quotient augmente de 1 par rapport au résultat de la question 1. ?

c) Quel est le plus grand entier $y$ que l'on peut ajouter à 473 pour que, dans la division de $473 + y$ par 27, le quotient augmente de 1 par rapport au résultat de la question 1. ?

## 1.2

Le capitaine Crochet a cinq matelots entre lesquels il doit partager équitablement un trésor. Une fois qu'il a pris sa part, il reste 1 723 pièces d'or pour son équipage, qu'il distribue ainsi : chaque matelot est associé à un doigt de sa main droite ; du crochet de sa main gauche, il désigne ses doigts dans l'ordre : pouce, index, majeur, annulaire, auriculaire, annulaire, majeur, index, pouce, index, etc. ; à chaque doigt désigné, le matelot correspondant prend une pièce.
Sur quel doigt le capitaine va-t-il terminer son décompte ?

## 1.3 L'opération

a) Donner une division euclidienne dont le diviseur est 23 et le reste est 10.
Dans cette opération, de combien peut-on augmenter le dividende sans changer le quotient ?
Quels nombres peut-on retrancher au dividende pour que le quotient diminue d'une unité ?

b) Quels sont les nombres $a$ tels que dans la division de $a$ par 5, le reste est égal au quotient ?
Quels sont les nombres $a$ tels que dans la division de $a$ par 4, le quotient est le triple du reste ?

## 1.4 Écriture en base $b$

Soit $b$ un entier, $b \geq 2$. Pour $n$ entier naturel non nul.

a) Démontrer qu'il existe $r \in \mathbb{N}$ et $(a_k)_{0 \leq k \leq r} \in \{0, \dots, b-1\}^r$ uniques tels que

$$n = \sum_{k=0}^{r} a_k b^k \quad \text{et} \quad a_r \neq 0.$$

*Démontrer la propriété pour $n \in \{1, \dots, b-1\}$ puis procéder par récurrence. Il est utile de remarquer que $a_0$ est le reste de la division de $n$ par $b$.*

b) On prend $b$ égal à dix. Démontrer que $n$ est divisible par 2 ou 5 si et seulement si $a_0$ l'est.

c) La somme des chiffres de $n$ est $S(n) = \sum_{k=0}^{r} a_k$. Démontrer que $b-1$ divise $n - S(n)$.

*Commencer par factoriser $b^k - 1$ pour $k \geq 1$.*

d) On écrit les chiffres en base dix*. Démontrer que $n$ est divisible par 9 si et seulement si $S(n)$ est divisible par 9. En déduire que le même résultat est vrai en remplaçant 9 par 3.

e) Comment adapter ce critère pour la divisibilité par 11 ?

f) Expliquer la blague suivante : « *Il y a 10 sortes de gens : ceux qui connaissent le binaire et les autres.* »

# 2 Divisibilité

## 2.1 Lemme de Gauss

a) Démontrer que si un entier $n$ est multiple de 33 et de 77, il est multiple de 231.

b) Montrer que pour tout entier $n$, $n(n+1)(n+2)(n+3)(n+4)$ est divisible par 120.

## 2.2

Résoudre dans $\mathbb{Z}^2$ l'équation : $\text{pgcd}(x,y)\text{ppcm}(x,y) = xy$.

## 2.3

Résoudre dans $\mathbb{N} \times \mathbb{N}$ le système $\begin{cases} a^2 + b^2 = 5409 \\ \text{ppcm}(a,b) = 360 \end{cases}$.

*Montrer d'abord que $a$ et $b$ sont multiples de 3 et ramener à $c^2 + d^2 = 601$, $\text{ppcm}(c,d) = 120$. Supposer $c \leq d$ et en déduire des contraintes sur les valeurs minimale et maximale possible pour $d$.*

## 2.4 Test des racines rationnelles

Soit $P(X) = \sum_{k=0}^{n} a_k X^k$ un polynôme à coefficients entiers.

a) On suppose $P$ unitaire, c'est-à-dire que $a_n = 1$. Montrer que si $r$ est une racine rationnelle de $P$, alors $r$ est entier.

b) Exemple : Soient $n \in \mathbb{N}^*$ et $k \in \mathbb{N}^*$ tels que $n^{1/k}$ est rationnel. Montrer que $n^{1/k}$ est un entier. Que peut-on dire des de la décomposition de $n$ en facteurs premiers ?

c) Supposons que $r = p/q$ soit une racine rationnelle de $P$ ($p$, $q$ entiers premiers entre eux). Montrer que $p$ divise $a_0$ et $q$ divise $a_n$.

## 2.5

Soit $x$ un réel. On suppose qu'il existe un entier naturel $n$ tel que $x^n$ et $x^{n+1}$ sont entiers. Montrer que $x$ est un entier.

# 3 Congruences

## 3.1

Montrer que $3^{512} - 2^{256}$ est divisible par 7 et que $2^{70} + 3^{70}$ est divisible par 13.

∗. Pourquoi ne faut-il pas écrire : « On écrit les chiffres en base 10. » ?

### 3.2

Déterminer le dernier chiffre de $2012^{2001}$ en base 3, en base 7 et en base 10. Mêmes questions pour $u_{7777}$ où $u_0 = 7$ et $u_{n+1} = 7^{u_n}$ pour $n \in \mathbb{N}$.

### 3.3

Vérifier que $400\,000\,000\,000\,000\,000\,081$ est divisible par 13.

### 3.4

En utilisant des congruences modulo un entier bien choisi, montrer que les équations suivantes n'ont pas de solutions entières :

$$\text{(i) } 7x - 4y^3 = 1 \text{ ; } \quad \text{(ii) } x^3 + y^3 + z^3 + 9t = 4 \text{ ; } \quad \text{(iii) } x^2 + xy + 2y^2 = 7003.$$

### 3.5

Pour $a$, $b$, $c$ entiers impairs, calculer $(a+b+c)^2$ et $a^2+b^2+c^2$ modulo 8, puis $ab+bc+ca$ modulo 4. En supposant de plus que $ab+bc+ca \geq 0$, démontrer que $\sqrt{ab+bc+ca} \notin \mathbb{Q}$.

### 3.6

Résoudre dans $\mathbb{N}^2$ l'équation $2^x - 3^y = 1$.

## 4 Relation de Bézout

### 4.1

Calculer $d = \text{pgcd}(210, 48)$ et donner des entiers $(u, v)$ tels que $210u + 48v = d$.

### 4.2

Déterminer un entier $n$ tel que $8n \equiv 1\ [35]$.

### 4.3

Résoudre dans $\mathbb{Z}^2$ les équations $237x + 81y = 1$ et $237x + 81y = 9$.

### 4.4

Résoudre dans $\mathbb{Z}$ les équations suivantes :

$$\text{(i) } x^2 \equiv x\ [6] \text{ ; } \quad \text{(ii) } 12x + 14 \equiv 0\ [8] \text{ ; } \quad \text{(iii) } 12x + 14 \equiv 0\ [37].$$

### 4.5

Résoudre dans $\mathbb{Z}$ les équations suivantes :

$$\text{(i) } \begin{cases} x \equiv 13\ [19] \\ x \equiv 6\ [12]; \end{cases} \qquad \text{(ii) } \begin{cases} x \equiv 3\ [17] \\ x \equiv 4\ [11] \\ x \equiv 5\ [6]; \end{cases} \qquad \text{(iii) } \begin{cases} 3x \equiv 1\ [5] \\ 4x \equiv 6\ [14] \\ 5x \equiv 11\ [3]. \end{cases}$$

### 4.6 Matrices unimodulaires

Soient $a, b, c$ trois entiers premiers entre eux dans leur ensemble [†]. Montrer que l'on peut *compléter* la colonne $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ en une matrice à coefficients entiers $\begin{pmatrix} a & a' & a'' \\ b & b' & b'' \\ c & c' & c'' \end{pmatrix}$ de déterminant 1.

*Indication. Il existe $x, y, z \in \mathbb{Z}$ tels que $ax + by + cz = 1$. Justifier l'existence d'entiers $x', y', z'$ premiers entre eux dans leur ensemble tels que $ax' + by' + cz' = 0$. Justifier ensuite l'existence d'entiers $a', b', c'$ tels que $a'x' + b'y' + c'z' = 1$ puis l'existence d'entiers $x'', y'', z''$ premiers entre eux dans leur ensemble tels que*

$$ax'' + by'' + cz'' = a'x'' + b'y'' + c'z'' = 0 \dots$$

## 5 Théorèmes de Fermat et Wilson

### 5.1 Petit théorème de Fermat

Soit $p$ un nombre premier, et $a \in \mathbb{Z}$ non multiple de $p$.

a) Montrez que la fonction $\Psi : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$ définie par :

$$\Psi(\overline{n}) = \overline{a} \cdot \overline{n}$$

est une bijection.

b) En considérant le produit $\Psi(\overline{1}) \cdots \Psi(\overline{p-1})$ en déduire que $a^{p-1} \equiv 1 \pmod{p}$.

### 5.2 Théorème de Wilson

a) Soit $p$ un nombre premier. On considère les polynômes suivants à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ :

$$P = (X - (p-1))(X - (p-2)) \cdots (X-2)(X-1) \quad \text{et} \quad Q = X^{p-1} - 1.$$

Montrez que $1, 2, \dots, p-1$ sont racines de $Q$ et en déduire que $P = Q$.

b) En déduire que $(p-1)! \equiv -1 \pmod{p}$.

c) Réciproquement, soit $n \geq 2$ un entier tel que

$$(n-1)! \equiv -1 \pmod{n}.$$

Montrez que $n$ est premier.

### 5.3

Pour quels entiers $n$ est-ce que 11 divise $n^{10} - 1$ (resp. 13 divise $n^6 - 1$ ou $n^6 + 1$) ?

### 5.4

Déterminer les restes de la division euclidienne de $2^{1137}$ par 13, 17 et 221.

### 5.5

Déterminer le reste de la division euclidienne de 26! par 29.

†. *i.e.* $\operatorname{pgcd}(a, b, c) = 1$

### 5.6 Sur les nombres de Fermat

On pose $^{\forall}n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$.

a) Montrer que $F_0, F_1, F_2, F_3$ sont premiers.

b) Soit $p$ premier tel que $p \,|65537$, montrer que $p = 1 \bmod 32$.

c) En déduire que $F_4 = 65537$ est premier.

d) Montrer que $641 \,|\, F_5$ et en déduire que $F_5$ n'est pas premier.