

---

**Feuille d'exercices n° 2**  
ARITHMÉTIQUE

---

## 1 Lemme de Zorn

### 1.1

Soient  $X$  et  $Y$  deux ensembles. On dit que  $|X| \leq |Y|$  s'il existe une injection  $\varphi : X \rightarrow Y$ . La relation  $\leq$  est une relation d'ordre. En utilisant le Lemme de Zorn, montrez que cette relation est un ordre total, autrement dit, si  $X$  et  $Y$  sont deux ensembles, il y en a au moins un qui peut s'injecter dans l'autre.

### 1.2

Montrez que tout espace vectoriel  $V$  sur un corps  $\mathbb{K}$  admet une base.

Indication : considérez l'ensemble  $\mathcal{V}$  des familles libres dans  $V$  ordonné par l'inclusion et appliquez le Lemme de Zorn.

## 2 Division euclidienne

### 2.1 473 raisons de calculer

1. Effectuer la division euclidienne de 473 par 27.
2. 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. ?
3. 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. ?

### 2.2

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 ?

### 2.3 L'opération

1. 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 ?
2. 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 ?

## 2.4 Écriture en base $b$

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

1. 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  $b$ .*

2. On prend  $b$  égal à dix. Démontrer que  $n$  est divisible par 2 ou 5 si et seulement si  $a_0$  l'est.
3. 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  $k \geq 1$ .*

4. On écrit les chiffres en base dix<sup>1</sup>. 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.
5. Comment adapter ce critère pour la divisibilité par 11 ?
6. Expliquer la blague suivante.

Il y a 10 sortes de gens : ceux qui connaissent le binaire et les autres.

## 3 Divisibilité

### 3.1 Lemme de Gauss

1. Démontrer que si un entier  $n$  est multiple de 33 et de 77, il est multiple de 231.
2. Montrer que pour tout entier  $n$ ,  $n(n+1)(n+2)(n+3)(n+4)$  est divisible par 120.

### 3.2

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

### 3.3

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  $d$ .*

### 3.4 Test des racines rationnelles

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

1. 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.
2. 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 ?
3. 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  $a_n$ .

---

1. Pourquoi ne faut-il pas écrire : ■ On écrit les chiffres en base 10. ■ ?

### 3.5

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.

## 4 Congruences

### 4.1

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

### 4.2

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  $n \in \mathbb{N}$ .

### 4.3

Vérifier que 400 000 000 000 000 000 081 est divisible par 13.

### 4.4

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

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

### 4.5

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  $\sqrt{ab + bc + ca} \notin \mathbb{Q}$ .

### 4.6

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

## 5 Relation de Bézout

### 5.1

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

### 5.2

Déterminer un entier  $n$  tel que  $8n \equiv 1 \pmod{35}$ .

### 5.3

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

### 5.4

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

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

## 5.5

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

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

## 6 Théorèmes de Fermat et Wilson

### 6.1 Petit théorème de Fermat

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

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

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

est une bijection.

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

### 6.2 Théorème de Wilson

1. 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  $P = Q$ .

2. En déduire que  $(p-1)! \equiv -1 \pmod{p}$ .
3. Réciproquement, soit  $n \geq 2$  un entier tel que

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

Montrez que  $n$  est premier.

### 6.3

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

### 6.4

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

### 6.5

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