# Arithmétique

## 1 Divisibilité, division euclidienne

### *Relation de divisibilité*

### *Congruence, division euclidienne*

**Exercice 1 : Exercice**

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

$$a^n \equiv b^n \ \left[n^2\right].$$

## 2 pgcd, ppcm

### *Plus grand commun diviseur*

### *Algorithme d'Euclide*

**Exercice 2 : Divers calculs de** pgcd

Soit $a, b \in \mathbb{Z}$. Calculer

**a.** $(a^3 + 3a^2 - 5) \wedge (a + 2)$, **b.** $(15a^2 + 8a + 6) \wedge (30a^2 + 21a + 13)$,

**c.** $(a^4 + 3a^2 - a + 2) \wedge (a^2 + a + 1)$, **d.** $(a^3 + a) \wedge (2a + 1)$,

**e.** $(a - b)^3 \wedge (a^3 - b^3)$.

### *Relation de Bézout*

**Exercice 3 : Calculs des coefficients de** Bézout

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

**a.** $95x + 71y = 1$, **b.** $24x - 15y = 3$, **c.** $12x + 15y + 20z = 1$.

### *Lemme de Gauss*

**Exercice 4 : Autour de la suite de Fibonacci**

On définit la suite de Fibonacci par :

$$F_0 \coloneqq 0, \quad F_1 \coloneqq 1 \quad \text{et} \quad \forall n \in \mathbb{N}, \quad F_{n+2} \coloneqq F_{n+1} + F_n.$$

1. Démontrer que
$$\forall n \in \mathbb{N}^*, \quad F_{n+1}F_{n-1} - F_n^2 = (-1)^n.$$
En déduire que $F_n$ et $F_{n+1}$ sont premiers entre eux.
2. Démontrer que
$$\forall n \in \mathbb{N}, \quad \forall p \in \mathbb{N}^*, \quad F_{n+p} = F_pF_{n+1} + F_{p-1}F_n.$$
En déduire que $F_n \wedge F_p = F_{n+p} \wedge F_p$.
3. Montrer que
$$\forall n, p \in \mathbb{N}, \quad F_n \wedge F_p = F_{n \wedge p}.$$

**Exercice 5 : Reste de la division euclidienne d'une puissance**

Soit $n$ un entier supérieur à 2 et $a \in \mathbb{Z}$, premier avec $n$. Pour tout entier $k$ on note $r_k$ le reste de la division euclidienne de $a^k$ par $n$.

1. Montrer que la suite $r$ est périodique. Pour cela on montrera dans l'ordre :
   (a) Il existe $k_1, k_2 \in \mathbb{N}$ tels que $k_1 < k_2$ et $a^{k_1} \equiv a^{k_2}\ [n]$.
   (b) Il existe $T \in \mathbb{N}^*$ tel que $a^T \equiv 1\ [n]$.
   (c) Conclure.
2. Quel est le reste de la division euclidienne de $3^{1998}$ par 5 ?
3. Montrer que 13 divise $3^{126} + 5^{126}$.

**Exercice 6 : Le théorème chinois**

On se donne $p_1, p_2 \in \mathbb{N}^*$ deux entiers premiers entre eux, et $a_1$ et $a_2 \in \mathbb{Z}$.

1. On souhaite montrer qu'il existe $n \in \mathbb{Z}$ tel que
$$n \equiv a_1 \quad [p_1] \qquad \text{et} \qquad n \equiv a_2 \quad [p_2].$$
   (a) Prouver l'existence d'un tel $n$ lorsque $a_1 = 1$ et $a_2 = 0$, puis lorsque $a_1 = 0$ et $a_2 = 1$.
   (b) En déduire le cas général.
2. En déduire l'ensemble des solutions du système
$$n \equiv a_1 \quad [p_1] \qquad \text{et} \qquad n \equiv a_2 \quad [p_2].$$
3. Résoudre le système
$$n \equiv 3 \quad [21] \qquad \text{et} \qquad n \equiv 1 \quad [5].$$

**Exercice 7 : Les pirates**

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 8 : Ordre d'un produit**

Soit $(G, \star)$ un groupe fini et $x, y$ deux éléments de $G$ d'ordres respectifs $\omega_x$ et $\omega_y \in \mathbb{N}^*$. On suppose que $x \star y = y \star x$ et que $\omega_x \wedge \omega_y = 1$.

1. Montrer que $\mathrm{Gr}(x) \cap \mathrm{Gr}(y) = \{e\}$.
2. En déduire que $xy$ est d'ordre $\omega_x \omega_y$.

### *Plus petit commun multiple*

**Exercice 9 : Calcul de** ppcm

Soit $a, b \in \mathbb{Z}$. Calculer
$$(a + b) \vee (a \wedge b).$$

## 3 Nombres premiers

### *Nombres premiers*

**Exercice 10 : Système de chiffrement RSA**

On se donne deux nombres premiers $p$ et $q$ distincts, on pose $n \coloneqq pq$ et on définit
$$\varphi(n) \coloneqq \mathrm{Card}\{k \in [\![0, n-1]\!] \mid k \wedge n = 1\}.$$

1. Soit $c \in \mathbb{N}$ tel que $c \wedge \varphi(n) = 1$. Montrer qu'il existe $d \in \mathbb{N}$ tel que $cd \equiv 1\ [\varphi(n)]$.
2. Montrer que $\varphi(n) = (p-1)(q-1)$.
3. Montrer que si $t \in \mathbb{Z}$, alors $t^{cd} \equiv t \quad [n]$.

**Exercice 11 : Encadrement du n-ième nombre premier**

Pour tout $n \in \mathbb{N}^*$, on note $p_n$ le $n$-ième nombre premier.

1. Montrer que
$$\forall n \in \mathbb{N}^*, \quad p_{n+1} \leqslant p_1 \cdots p_n + 1.$$
2. En déduire que
$$\forall n \in \mathbb{N}^*, \quad p_n \leqslant 2^{2^n}.$$
3. Soit $x \in \mathbb{R}_+$. On note $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à $x$. Montrer que pour $x$ assez grand
$$\ln(\ln x) \leqslant \pi(x) \leqslant x.$$
*On démontrera le fait que pour $n \geqslant 3$, $\mathrm{e}^{\mathrm{e}^{n-1}} \geqslant 2^{2^n}$.*

**Exercice 12 : Cas particuliers du théorème de Dirichlet**

1. (a) Montrer que tout entier naturel congru à 3 modulo 4 possède au moins un diviseur premier congru à 3 modulo 4.
   (b) Montrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.
2. Montrer qu'il existe une infinité de nombres premiers congrus à 5 modulo 6.

*Le théorème de Dirichlet affirme que si $a$ et $b$ sont premiers entre eux, il existe une infinité de nombres premiers de la forme $ak + b$.*

**Exercice 13 : Pour les Toulousaings**

Soit $a_1, \ldots, a_{1789} \in \mathbb{Z}$ tels que
$$\sum_{k=1}^{1789} a_k = 0$$
Montrer que
$$\sum_{k=1}^{1789} a_k^{37} \equiv 0 \ [399].$$

## *Valuation $p$-adique, décomposition en facteurs premiers*

**Exercice 14 : Divisibilité**

Soit $a, b \in \mathbb{Z}$. Montrer que
$$a|b \quad \Longleftrightarrow \quad a^2|b^2.$$