# Feuille d'exercices n° 2

## Théorème de Bézout, Algorithme d'Euclide, Groupes, Congruences.

### Théorème de Bézout, Algorithme d'Euclide

Exercice 1. Résoudre l'équation $37x + 21y = 1$ en nombres entiers.

Exercice 2. Soient $a$, $b$, $c$ des entiers non-nuls. Montrer que l'équation $ax + by = c$ admet des solutions entières si et seulement si $c$ est un multiple du pgcd de $a$ et $b$.

Exercice 3.

1. Calculer le pgcd de 187 et 323.
2. Trouver tous les entiers $x$ et $y$ tels que $187x + 323y = 51$.
3. Trouver tous les entiers $x$ et $y$ tels que $187x + 323y = 85$.

Exercice 4. Résoudre les équations suivantes en nombres entiers :

1. $283x + 1722y = 17$.
2. $730x + 144y = 18$.
3. $1111x + 2345y = 66$.

Exercice 5. Soient $a$ et $b$ des entiers non nuls.

1. Montrer que pour tout entier $x$, $\text{pgcd}(a, b + ax) = \text{pgcd}(a, b)$.
2. Montrer que si $x$ est un entier strictement positif, $\text{pgcd}(xa, xb) = x\text{pgcd}(a, b)$.
3. Montrer que si $x$ est un entier strictement positif tel que $\text{pgcd}(x, b) = 1$, alors $\text{pgcd}(ax, b) = \text{pgcd}(a, b)$.

Exercice 6. Soit $n$ un entier.

1. Déterminer le pgcd de $9n + 15$ et $4n + 7$ en fonction de $n$.
2. Montrer que $n^2$ et $2n + 1$ sont premiers entre eux.

Exercice 7. Considérons les polynômes en $x$ à coefficients dans $\mathbb{Q}$.
Trouver $f(x), g(x) \in \mathbb{Q}[x]$ tels que $(x^3 + 2x^2 + 2x + 1) \cdot f(x) + (x^2 + 1) \cdot g(x) = 1$.

### Groupes

Exercice 8. Soit $G$ un groupe, $a, b \in G$, et $n \in \mathbb{Z}_{>0}$. Montrer que :

1. $(aba^{-1})^n = ab^n a^{-1}$.
2. $(ab)^{-1} = b^{-1}a^{-1}$.
3. Si $(ab)^n = e$, alors $(ba)^n = e$.
4. Si $ab = ba$, alors $(ab)^n = a^n b^n$. Donner un contre-exemple si $ab \neq ba$.
5. Si $a^{-1}ba = b^{-1}$ et $b^{-1}ab = a^{-1}$, alors $a^2 = b^2$ et $a^4 = b^4 = e$.

Exercice 9. Soit $G$ un groupe tel que $x^2 = e$ pour tout $x \in G$. Montrer que $G$ est commutatif.

Exercice 10. Soit $G$ un groupe fini. On suppose que pour tout $g \in G$ il existe un nombre impair $n$ tel que $g^n = e$. Montrer que l'application $g \mapsto g^2$ est une bijection de $G$ dans lui-même.
Plus généralement, soit $m$ un entier strictement positif. Supposons que $m$ et le cardinal de $G$ sont premiers entre eux, montrer que l'application $g \mapsto g^m$ est une bijection de $G$ dans lui-même. (allusion : appliquer le théorème de Bézout et le théorème de Lagrange.)

Exercice 11. Soit $G$ un groupe, et soit $a, b \in G$.

1. Montrer que l'ordre de $a$ et l'ordre de $a^{-1}$ sont égaux.
2. Montrer que l'ordre de $a$ et $bab^{-1}$ sont égaux
3. Montrer que l'ordre de $ab$ et l'ordre de $ba$ sont égaux.

Exercice 12. Soit $G$ un groupe.

1. Quels sont les éléments de $G$ d'ordre 1 ?
2. Soit $x$ un élément de $G$ d'ordre $rs$ avec $r, s \in \mathbb{Z}_{\geqslant 1}$. Quel est l'ordre de $x^r$ ?
3. Soit $x$ un élément de $G$ d'ordre $n$. Soit $t$ un entier strictement positif premier à $n$, montrer que $x^r$ est d'ordre $n$.
4. Soit $x$ un élément de $G$ d'ordre $n$. Quel est l'ordre de $x^r$, pour $r \geqslant 1$ ?

Exercice 13. Soit $G$ un groupe. Considère $a, b \in G$

1. Si $a$ est d'ordre $n$ et $a^m = e$, montrer que $n$ divise $m$.
2. On suppose que $m$ l'ordre de $a$ et $n$ l'ordre de $b$ sont premiers entre eux. En utilisant l'exercice précédent, montrer que l'ordre de $ab$ est égal à $mn$ si $G$ est commutatif.
3. Vérifier que, dans le groupe symétrique $S_6$, l'élément $\tau = (123)$ est d'ordre 3, l'élément $\sigma = (12)$ est d'ordre 2, mais $\sigma\tau$ n'est pas d'ordre 6.

## Congruences, $\mathbb{Z}/n\mathbb{Z}$

Exercice 14 (générateur de $(\mathbb{Z}/17\mathbb{Z})^*$). Déterminer l'ordre de 2 dans $(\mathbb{Z}/17\mathbb{Z})^*$. Montrer que $(\mathbb{Z}/17\mathbb{Z})^*$ est cyclique, c'est-à-dire qu'il existe $a \in (\mathbb{Z}/17\mathbb{Z})^*$ tel que $\langle a \rangle = (\mathbb{Z}/17\mathbb{Z})^*$. [Indication : on pourra chercher $a$ tel que $a^2 = 2$.]
Il sera vu en cours que $(\mathbb{Z}/p\mathbb{Z})^*$ est toujours cyclique si $p$ est premier.

Exercice 15. Soit $n$ un entier naturel. Montrer que :

1. $2^{3n+5} + 3^{n+1}$ est multiple de 5 mais pas de 10.
2. $3n^5 + 5n^3 + 7n$ est multiple de 15.
3. $n^5 - n$ est multiple de 30.

Exercice 16 (calcul de puissances).

1. Quel est le dernier chiffre de $2013^{2013}$ ?
2. Quels sont les restes des divisions euclidiennes de $900^{2000}$ et de $101^{102^{103}}$ par 7 ?
3. Quel est le reste de la division euclidienne de $31^{32^{33}}$ par 11 ?

Exercice 17 (diviseurs premiers des nombres de Fermat). Soit $n \in \mathbb{N}$ et $F_n = 2^{2^n} + 1$ le $n$-ième nombre de Fermat. Soit $p$ un diviseur premier de $F_n$. Remarquer $2^{2^n} = -1 \mod p$, puis montrer que l'ordre de 2 dans $(\mathbb{Z}/p\mathbb{Z})^*$ est $2^{n+1}$. En déduire qu'il existe $k \in \mathbb{N}$ tel que $p = 2^{n+1}k + 1$. Trouver un diviseur de $F_5 = 4\,294\,967\,297$. Ce fut la démarche d'Euler pour réfuter la conjecture de Fermat, selon laquelle tous les nombres $F_n$ sont premiers.

Exercice 18. Soit $n > 1$ un entier tel que $2^n = 1 \mod n$. Soit $p$ le plus petit diviseur premier de $n$.

1. Montrer que $p > 2$.
2. Soit $r$ l'ordre de 2 dans le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$. Montrer que $r > 1$ et que $r$ divise $n$ et $p-1$.
3. Conclure qu'il n'existe pas de $n > 1$ tel que $2^n = 1 \mod n$.

Exercice 19 (équations modulaires linéaires). Soit $n \geqslant 1$ un entier naturel, et soit $a, b \in \mathbb{Z}/n\mathbb{Z}$. On considère l'équation suivante dans $\mathbb{Z}/n\mathbb{Z}$ :

$$ax = b, \quad x \in \mathbb{Z}/n\mathbb{Z}. \tag{1}$$

1. Soit $d = \text{pgcd}(a, n)$. Montrer que l'équation (1) admet des solutions si et seulement si $d|b$.
2. Soit $u, v \in \mathbb{Z}$ des coefficients de Bézout tels que $au + nv = d$ dans $\mathbb{Z}$. On pose

$$x_0 = u\frac{b}{d} \mod n.$$

   Montrer que $x_0$ est solution de l'équation (1).
3. Soit $x \in \mathbb{Z}/n\mathbb{Z}$ une solution de l'équation (1). Montrer que $x$ est de la forme :

$$x_i = x_0 + i\frac{n}{d}, \quad i \in \mathbb{Z}.$$

4. Montrer que toutes les solutions de l'équation (1) sont les $x_0, \ldots, x_{d-1}$, et qu'ils sont au nombre de $d$.
5. Exemples : résoudre les équations $6x = 10 \mod 16$ et $7x = 4 \mod 30$. Combien de solutions à l'équation $ax = 0 \mod n$ ? Déterminer le nombre de solutions à l'équation $ax = b \mod p$ si $p$ est un nombre premier.

Exercice 20 (inverses dans $\mathbb{Z}/n\mathbb{Z}$). Rappeler à quelle condition un élément $a$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$. Donner une procédure utilisant l'algorithme d'Euclide-Bézout pour calculer l'inverse d'un élément.

Exercice 21 (Théorème de Wilson). Soit $p > 2$ un nombre premier.

1. Montrer que $-1$ est le seul élément d'ordre 2 de $(\mathbb{Z}/p\mathbb{Z})^*$.
2. Montrer que $(p-1)! = -1 \mod p$. Indication : on pourra regrouper $x$ et $x^{-1}$ dans le produit des $x$ pour $x \in (\mathbb{Z}/p\mathbb{Z})^*$.
3. Que dire de la réciproque : si $(n-1)! = -1 \mod n$, peut-on en conclure que $n$ est premier ?

Exercice 22. Résoudre les sytèmes de congruences :

$$(a) \begin{cases} x = 3 \mod 37 \\ x = 4 \mod 52 \end{cases} \qquad (b) \begin{cases} x = 21 \mod 12 \\ x = 12 \mod 21 \end{cases}$$

Exercice 23. Résoudre les équations :

1. $x^2 + 4x - 1 = 0$ dans $\mathbb{Z}/11\mathbb{Z}$.
2. $x^2 + 7x + 3 = 0$ dans $\mathbb{Z}/11\mathbb{Z}$.
3. $x^2 + 4x - 13 = 0$ dans $\mathbb{Z}/21\mathbb{Z}$.
4. $x^2 + 2x + 6 = 0$ dans $\mathbb{Z}/9\mathbb{Z}$.
5. $2x^2 + 3x + 1 = 0$ dans $\mathbb{Z}/5\mathbb{Z}$