1. Arithmétique élémentaire

Exercice 1.1
1. Déterminer tous les diviseurs de 18 dans $\mathbb{Z}$.
2. Déterminer tous les diviseurs de 24 dans $\mathbb{Z}$.
3. Quel est le PGCD de 18 et 24 ?

PPCM. Soient $a, b \in \mathbb{Z}$ tous deux non nuls. On appelle $\mathrm{PPCM}(a, b)$ le plus petit nombre m positif qui est un multiple commun de a et b.

Exercice 1.2
1. Décomposer 198 et 195 en facteurs premiers.
2. Quel est le PGCD de 198 et 195 ?
3. Quel est le PPCM de 198 et 195 ?

Exercice 1.3
1. Décomposer 8160 en facteurs premiers.
2. Trouver tous les entiers positifs a, b tels que $a \geq b$, $\mathrm{PGCD}(a, b) = 5$ et $\mathrm{PPCM}(a, b) = 8160$.

Identité de Bézout. Pour deux entiers a et b non tous deux nuls, il existe deux entiers u et v tels que $au + bv = \mathrm{PGCD}(a, b)$.

Exercice 1.4 En utilisant l'algorithme d'Euclide, calculer le PGCD de 437 et 263, puis trouver deux entiers u et v tel que

$$437u + 263v = \mathrm{PGCD}(437, 263).$$

(Même exercice avec les nombres 26999 et 1337.)

Exercice 1.5 Montrer par récurrence que pour tout entier $n \in \mathbb{N}$, $7 | (3^{2n} - 2^n)$.

Exercice 1.6
1. Montrer qu'un entier impair a tous ses diviseurs impairs.
2. Soit n un entier, $n \geq 2$. On suppose que si un entier d divise n et $d \geq 2$ alors d est pair. Montrer que n est une puissance de 2.

Exercice 1.7 Soit $a \in \mathbb{Z}$ tel que $(a + 1) | (a^2 + 1)$.
1. Simplifier $a(a + 1) - (a - 1)$.
2. En déduire que $(a + 1) | (a - 1)$ puis que $(a + 1) | 2$.
3. Montrer que $a = 1$ ou $a = 0$ ou $a = -2$ ou $a = -3$.

Définition. Soit n un entier supérieur ou égal à 2. Pour tous entiers a et b, on dit que a est *congru* à b *modulo* n si n divise $a - b$. On note cette propriété $a \equiv b \pmod{n}$.

Exercice 1.8 On fixe un entier $n \geq 2$. Vérifier les règles de calcul suivantes. Soient a, b, c et d des entiers.
1. Si $a \equiv b \pmod{n}$ alors $b \equiv a \pmod{n}$.
2. Si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$ alors $a \equiv c \pmod{n}$.
3. Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$ alors $a + c \equiv b + d \pmod{n}$ et $ac \equiv bd \pmod{n}$

Exercice 1.9 Vous connaissez sans doute le critère de divisibilité par 9 : on fait la somme des chiffres, puis la somme des chiffres du résultat, et ainsi de suite... Si le résultat final est 9, le nombre de départ était divisible par 9.

1. Montrer que ce critère repose sur le fait que $10 \equiv 1 \pmod 9$.
2. De façon analogue, donner un critère de divisibilité par 3, puis par 11.

Propriété. Soit un entier $n \geq 2$. Pour tout entier a, le reste de la division euclidienne de a par n est l'unique entier r tel que $a \equiv r \pmod n$ et $0 \leq r < n$.

Exercice 1.10 Soit $a \in \mathbb{Z}$. Montrer que a^2 est congru à 0, 1, 2 ou 4 modulo 7.

Exercice 1.11 Quel est le dernier chiffre de 2013^{2012} dans l'écriture décimale ? Dans l'écriture diadique ? Dans l'écriture triadique ?

Exercice 1.12 Soient x et y deux entiers. Montrer que $3x \equiv 7y \pmod{11}$ si et seulement si $x \equiv 6y \pmod{11}$. (Indication : pour l'implication on pourra multiplier par 4.)