TD 6 - Arithmétique dans $\mathbb{Z}$

Exercice 1 (Propriétés de la relation de divisibilité)**.** Soit $a, b \in \mathbb{Z}$.

a. Montrer que les seuls diviseurs de 1 sont 1 et -1.
(On pourra passer aux valeurs absolues et utiliser la relation d'ordre $\leq$ sur $\mathbb{N}$)

b. Montrer que : $a \mid b$ et $b \mid a$ si et seulement si $a = \pm b$.

c. Pour tout entier relatif k, on note D_k l'ensemble des diviseurs de k. Montrer que : $D_a = D_b$ si et seulement si $a = \pm b$.

d. Pour tout entier relatif k, on note $k\mathbb{Z}$ l'ensemble défini par $k\mathbb{Z} = \{kq, q \in \mathbb{Z}\}$. Montrer que $a \mid b$ si et seulement si $b\mathbb{Z} \subset a\mathbb{Z}$.

Exercice 2 (Division par soustractions)**.** On considére l'algorithme suivant.

Entrée: $a \geq 0, b > 0$.
Sortie: q, r le quotient et reste de la division euclidienne de a par b

```
r ← a
q ← 0
while r ≥ b do
    r ← r − b
    q = q + 1
end while
return q, r
```

a. Prouver que $a = bq + r$ est un invariant de boucle.

b. Prouver la terminaison et la correction de cet algorithme.

Exercice 3 (Division euclidienne et divisibilité)**.** Soit $a, b \in \mathbb{Z}$. Montrer que $b \mid a$ si et seulement si le reste de la division euclidienne de a par b est nul.

Exercice 4 (Écriture en base b)**.** **a.** Écrire $n = 10011_{10}$ en base 3.

b. Écrire $n = 110011_2$ en base 6.

c. Écrire $3n$ en base 3 où $n = 21001_3$ sans aucun calcul.

Exercice 5 (Exemples)**.** **a.** Décrire la classe d'équivalence de -3 modulo 7.

b. Les égalités suivantes sont-elles vraies ou fausses ?

$$6 \equiv 4 \bmod 2 \qquad 5 \equiv -5 \bmod 12 \qquad 11 \equiv -2 \bmod 13 \qquad 24 \equiv 0 \bmod 12$$

c. Le cas particulier de $n = 2$. Montrer que pour tout $a, b \in \mathbb{Z}$, $a \equiv b \bmod 2 \iff 2 \mid (a + b)$.

Exercice 6 (Quelques propriétés des congruences)**.** Soit $a \in \mathbb{Z}, b \in \mathbb{N}^*$ Montrer les propositions suivantes :

a. Soit $a = bq + r$ la division euclidienne de a par b. Alors $a \equiv r \bmod b$ et $a \equiv r \bmod q$.

b. Soit t un entier vérifiant $a \equiv t \bmod b$ et tel que $0 \leq t < b$. Alors t est le reste de la division euclidienne de a par b.

Exercice 7. Simplifier les expressions modulaires suivantes.

a. $1234 \bmod 7$

b. $2025 \bmod 13$

c. $10! \bmod 17$

d. $5^{10} \bmod 11$

e. $2005^{2006} \bmod 7$

Exercice 8. **a.** Montrer que $10^6 \equiv 1 \bmod 7$

b. Quel est le chiffre des unités de 3^{12} ?

c. Montrer que pour tout $n \in \mathbb{N}$, $\quad 7 \mid 2^{4^n} + 5$

Exercice 9 (Critères de divisibilités)**.** Soit $n = (a_m \dots a_0)_{10}$.

a. Montrer que $2 \mid n$ si et seulement si $a_0 \in \{0, 2, 4, 6, 8\}$.

b. Montrer que $3 \mid n$ si et seulement si $3 \mid a_0 + \cdots + a_m$.

c. Montrer que $9 \mid n$ si et seulement si $9 \mid a_0 + \cdots + a_m$.

d. Montrer que $5 \mid n$ si et seulement si $a_0 \in \{0, 5\}$.