TD2. Propriétés arithmétiques de $\mathbb{Z}$

Exercice 1. Calculs de relations de Bézout
Calculer le pgcd et une relation de Bézout pour chacun des couples d'entiers suivants.

a. $(159, 15)$

b. $(5278, 634)$

c. $(723, 76)$

Exercice 2. Nombres premiers entre eux dans leur ensemble
Soient $a_1, a_2, \ldots, a_n$ des entiers relatifs non nuls. Le $\text{pgcd}(a_1, a_2, \ldots, a_n)$ est le plus grand entier qui divise tous les a_i. Si ce pgcd vaut 1, on dit que les a_i sont premiers entre eux dans leur ensemble.

1. Montrer que si deux des entiers $a_1, a_2, \ldots, a_n$ sont premiers entre eux, alors $\text{pgcd}(a_1, a_2, \ldots, a_n) = 1$.

2. Trouver trois entiers positifs a_1, a_2, a_3 tels que $\text{pgcd}(a_1, a_2, a_3) = 1$ mais $\text{pgcd}(a_1, a_2) \neq 1$, $\text{pgcd}(a_2, a_3) \neq 1$ et $\text{pgcd}(a_1, a_3) \neq 1$.

3. Montrer que pour tous entiers relatifs non nuls a_1, a_2, a_3, on a $\text{pgcd}(a_1, a_2, a_3) = \text{pgcd}(a_1, \text{pgcd}(a_2, a_3))$.

4. Montrer qu'il existe des entiers relatifs $u_1, u_2, \ldots, u_n$ tels que

$$a_1u_1 + a_2u_2 + \cdots + a_nu_n = \text{pgcd}(a_1, a_2, \ldots, a_n)$$

5. En déduire que $a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z} = \text{pgcd}(a_1, a_2, \ldots, a_n)\mathbb{Z}$

Exercice 3.

1. Montrer que pour tout entier relatif n, 24 divise $n(n+1)(n+2)(n+3)$.

2. Montrer que pour tout entier relatif n, 120 divise $n(n+1)(n+2)(n+3)(n+4)$.

Exercice 4. Nombres premiers congrus à 3 modulo 4

1. Soit n un entier tel que $n \geqslant 2$ et $n \equiv 3 \mod 4$. Montrer que pour tout facteur premier p de n, on a $p \equiv 1 \mod 4$ ou $p \equiv 3 \mod 4$. En déduire que n a au moins un facteur premier p congru à 3 modulo 4.

2. Soit k un entier positif. Soient $p_1, p_2, \ldots, p_k$ des nombres premiers tous congrus à $3 \mod 4$. Montrer que l'entier $n = 4p_1p_2 \ldots p_k - 1$ a un facteur premier différent de tous les p_i et congru à 3 modulo 4.

3. Démontrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.

Exercice 5. On considère les entiers $m = 2^3 3^5 5^2 7^1$ et $n = 2^2 3^6 5^1 7^2$.

1. Déterminer le nombre de diviseurs positifs de m et le nombre de diviseurs positifs de n.

2. Calculer $\text{pgcd}(m, n)$ et $\text{ppcm}(m, n)$.

3. Quel est le plus grand cube parfait qui divise m ?

Exercice 6. Soient a, b des entiers relatifs.

1. Montrer que si p est un nombre premier qui divise $\text{pgcd}(a+b, ab)$, alors p divise $\text{pgcd}(a, b)$.

2. Montrer que si a et b sont premiers entre eux, alors $a+b$ et ab sont aussi premiers entre eux.

Exercice 7. Résolution d'équations à deux inconnues

1. A quelle condition sur $c \in \mathbb{Z}$ l'équation $351x + 325y = c$ admet-elle au moins une solution dans $\mathbb{Z} \times \mathbb{Z}$?

2. Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ l'équation $351x + 325y = 39$.

3. Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ l'équation $5278x + 634y = 12$.
On pourra utiliser une relation de Bézout établie lors de l'exercice 1.

Exercice 8. Résolution de systèmes de congruences

1. Calculer $\text{pgcd}(25, 6)$. Déterminer une relation de Bézout entre $25, 6$ et leur pgcd.

2. On cherche à résoudre le système de congruences suivant :

$$(S) : \begin{cases} x & \equiv & 2 & \mod 6 \\ x & \equiv & 15 & \mod 25 \end{cases}$$

c'est-à-dire qu'on cherche tous les entiers relatifs x vérifiant les deux congruences ci-dessus.

a. Grâce à la relation de Bézout de la question **1.**, déterminer un entier m et un entier n tels que

$$\begin{cases} m & \equiv & 2 & \mod 6 \\ m & \equiv & 0 & \mod 25 \end{cases} \quad \begin{cases} n & \equiv & 0 & \mod 6 \\ n & \equiv & 15 & \mod 25 \end{cases}$$

b. En déduire une solution particulière x_0 du système (S).

c. Démontrer qu'un entier relatif x est solution de (S) si et seulement si $150|(x - x_0)$.

d. Conclure.

3. Résoudre dans $\mathbb{Z}$ le système de congruences suivant :

$$\begin{cases} x & \equiv & 5 & \mod 12 \\ x & \equiv & 3 & \mod 35 \end{cases}$$

Exercice 9. Entiers "inversibles" modulo n
Soient a un entier relatif non nul et n un entier naturel non nul.

1. Montrer que si $\text{pgcd}(a, n) = 1$, alors il existe $u \in \mathbb{Z}$ tel que $au \equiv 1 \mod n$.

2. Réciproquement, montrer que s'il existe $u \in \mathbb{Z}$ tel que $au \equiv 1 \mod n$ alors $\text{pgcd}(a, n) = 1$.

3. Dans le cas où $\text{pgcd}(a, n) = 1$, on dira qu'un tel u est un "inverse" de a modulo n.

a. Calculer un "inverse" de 12 modulo 5.

b. Calculer un "inverse" de 76 modulo 723.

4. Résoudre le système de congruences suivant :

$$\begin{cases} 3x & \equiv & 1 & \mod 14 \\ 5x & \equiv & 2 & \mod 11 \end{cases}$$

Exercice 10. On rappelle que si p est un nombre premier, alors pour tout $a \in \mathbb{Z}$, on a $a^p \equiv a \mod p$.

1. Un critère de non primalité. Soit $n \geqslant 2$ un entier naturel. On dit que n est *composé* s'il existe un entier m tel que $1 < m < n$ et $m|n$.
Montrer que s'il existe un entier a tel que $1 < a < n$ et $a^{n-1} \not\equiv 1 \mod n$, alors n est composé.

2. Réciproque ?

a. Soit $n \geqslant 2$ un entier sans facteur carré. Supposons que pour tout facteur premier p de n, on a $(p-1)|(n-1)$.
Montrer que

- $a^{n-1} \equiv 1 \mod n$ pour tout entier a premier à n,
- $a^n \equiv a \mod n$ pour tout entier a.

b. Montrer que $n = 561$ vérifie les conditions du **2.a**.
Le résultat de la question **1** admet-il une réciproque ?

Un nombre ayant les propriétés du **2** *s'appelle un nombre de Carmichaël.*