Feuille de TD 1

Arithmétique dans $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$

Exercice 1. Trouver toutes les relations de Bézout entre 650 et 66.

Exercice 2. Montrer que 429 est inversible dans $\mathbb{Z}/700\mathbb{Z}$ et calculer son inverse.

Exercice 3. Calculer en fonction de $n \in \mathbb{N}$ le pgcd $(n^3 + n^2 + 1) \wedge (n^2 + 2n - 1)$. De même, calculer le pgcd $(n^3 + n^2 - 6n + 2) \wedge (2n^2 + 5n - 3)$.

Exercice 4. Résoudre les congruences suivantes, pour $x \in \mathbb{Z}$:

(1) $3x \equiv 4 \pmod 7$,

(2) $9x \equiv 12 \pmod{21}$,

(3) $103x \equiv 612 \pmod{676}$.

Exercice 5. Calculer les congruences suivantes :

(1) 135463^{2315} modulo 19,

(2) 763^{234} modulo 20,

(3) 2222^{321} modulo 20.

Exercice 6 (**Fractions égyptiennes**)**.** Les fractions égyptiennes sont celles de la forme $\frac{1}{n}$ pour $n \in \mathbb{N}^*$. On s'intéresse au problème de l'écriture d'une fraction rationnelle positive $\frac{a}{b}$ sous la forme d'une somme de fractions égyptiennes distinctes.

(1) En utilisant l'identité $\frac{1}{b} = \frac{1}{b+1} + \frac{1}{b(b+1)}$, montrer que toute fraction $\frac{a}{b}$ avec $a, b \in \mathbb{N}^*$ peut s'écrire comme somme d'une nombre fini de fractions égyptiennes distinctes, en donnant un algorithme produisant une telle décomposition. Donner le nombre de termes dans la somme, en fonction de a, ainsi qu'une borne sur le plus grand dénominateur apparaissant dans la décomposition, en fonction de a et b.

(2) On suppose $\frac{a}{b} < 1$ et $a \wedge b = 1$. À l'aide du théorème de Bézout, donner un autre algorithme de décomposition en somme de fractions égyptiennes, utilisant au plus a termes et dont tous les dénominateurs sont inférieurs ou égaux à $b(b-1)$.

Exercice 7. (1) Montrer que 7 divise $3^{105} + 4^{105}$.

(2) Pour a, b, c entiers, montrer que $6 | a + b + c$ si et seulement si $6 | a^3 + b^3 + c^3$.

(3) Montrer que pour tout n entier, on a la congruence $n^7 \equiv n \pmod{42}$.

Exercice 8. Donner tous les morphismes de groupe $\mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$, puis ceux $\mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/15\mathbb{Z}$. Donner une condition nécessaire et suffisante sur m et n pour que tout morphisme $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ soit nul.

Exercice 9 (Jeu de la marchande). Supposons que l'on dispose uniquement de pièces de monnaie de valeurs entières a et b, avec a et b premiers entre eux.

(1) Quelles sommes peut-on payer si on nous rend la monnaie ?

(2) Supposons maintenant qu'on ne puisse pas nous rendre la monnaie. On pose $N = ab - a - b$. Montrer que si $N = n + m$, avec $n, m \in \mathbb{Z}$, alors exactement une somme parmi n et m est payable. En particulier, si $n > N$, alors la somme n est payable.

(3) Plus généralement, montrer que pour tout entier $n \geqslant 2$, si $a_1, \dots, a_n \in \mathbb{N}^*$ sont deux à deux premiers entre eux, alors

$$M_n = a_1 \cdot \dots \cdot a_n \left(n - 1 - \sum_{i=1}^{n} \frac{1}{a_i} \right)$$

est le plus grand entier qui ne peut pas s'écrire sous la forme $\sum_{i=1}^{n} x_i \prod_{j \neq i} a_j$ avec $x_i \in \mathbb{N}$.

Exercice 10. Soit $n \in \mathbb{N}^*$. Pour $k \in \mathbb{Z}/n\mathbb{Z}$, montrer que $\langle k \rangle$ est le sous-groupe engendré par $k \wedge n$. En déduire que $n = \sum_{d|n} \varphi(d)$.