Arithmétique, congruences, $\mathbf{Z}/n\mathbf{Z}$

Exercice 1. ⋆ En utilisant l'algorithme d'Euclide étendu, donner une relation de Bezout pour 79326 et 26273.

Exercice 2. ⋆ Calculer $\mathsf{pgcd}(1000000000000000000000000000, 11111111111111111111111111111)$.

Exercice 3. ⋆ Dresser la table de multiplication de $\mathbf{Z}/6\mathbf{Z}$.

Exercice 4. ⋆ L'entier 193 est-il inversible modulo 2024 ? Si oui, calculer son inverse.

Exercice 5. ⋆ Déterminer l'ensemble des couples $(x, y) \in \mathbf{Z}^2$ tels que $19x + 3y = 2024$.

Exercice 6. ⋆ Montrer que pour tout $n \in \mathbf{Z}$, les fractions $\frac{21n+4}{14n+3}$ et $\frac{n^3+n}{2n^2+1}$ sont irréductibles.

Exercice 7. ⋆ Démontrer que si a et b sont des entiers premiers entre eux, il en est de même des entiers $a + b$ et ab.

Exercice 8. ⋆ Calculer $\varphi(2024)$, puis l'inverse de 507 modulo $\varphi(2024)$.

Exercice 9. ⋆ Solutions entières de l'équation $x^3 + 2y^3 = 4z^3$.

Exercice 10. ⋆ Montrer que pour tout $n \in \mathbf{Z}$, on a $n^7 \equiv n \mod 42$.

Exercice 11. ⋆ Montrer que pour tout entier n premier à 63, on a $n^6 \equiv 1 \mod 63\mathbf{Z}$.

Exercice 12. ⋆ Montrer que $x^2 = 2^n - 1$ n'a pas de solution entière si $n > 1$.

Exercice 13. ⋆ On veut déterminer les solutions de l'équation diophantienne

$$x^2 - 13y^2 = 7 \tag{$*$}$$

Soit donc $(x, y) \in \mathbf{Z}^2$ une solution de $(*)$.

(1) Montrer que ni x, ni y n'est divisible par 7.
(2) Montrer que $x^2 \equiv -y^2 \mod 7\mathbf{Z}$.
(3) En déduire que -1 est un carré modulo 7.
(4) Déterminer les carrés modulo 7, et en déduire que $(*)$ n'a pas de solutions entières.

Exercice 14. ⋆⋆ Résoudre le système de congruences :

$$\begin{cases} x & \equiv 1 \mod 3 \\ x & \equiv 2 \mod 11 \\ x & \equiv 51 \mod 61 \end{cases}$$

Exercice 15. ⋆⋆ Tout entier premier à 10 admet un multiple dont l'écriture en base 10 n'est composée que de 1.

Exercice 16. ⋆⋆ Déterminer $\mathsf{Hom}_{\mathsf{gr}}(\mathbf{Z}/n\mathbf{Z}, \mathbf{Z}/m\mathbf{Z})$.

Exercice 17. ⋆⋆ Calculer $5^{115633} \mod 2024$.

Exercice 18. ⋆⋆ Quel est le dernier chiffre de $7^{7^{7^{7^{7^{7^{7}}}}}}$?

Exercice 19. ⋆⋆ Déterminer les entiers naturels y et n tels que $y^2 = 2^n + 1$.

Exercice 20. ⋆ ⋆ ⋆ Montrer que $\frac{(2n)!(2m)!}{n!m!(n+m)!}$ et $\frac{(5n)!}{40^n n!}$ sont entiers.

Exercice 21. ⋆⋆ Quand on écrit 4444^{4444} en base 10, la somme des chiffres vaut A. Soit B la somme des chiffres de A. Trouver la somme des chiffres de B (A et B sont écrits en base 10).

Exercice 22. ⋆ Soit $n \in \mathbf{N}_{>0}$. Montrer que $\mathsf{Aut}(\mathbf{Z}/n\mathbf{Z}) \simeq (\mathbf{Z}/n\mathbf{Z})^{\times}$.

Exercice 23. ⋆ ⋆ ⋆ (1) Soit G un groupe abélien fini.

(a) Soient $x, y \in G$ d'ordre n et m respectivement. Montrer que si $\mathsf{pgcd}(n, m) = 1$, l'élément xy est d'ordre nm.

(b) On note μ le ppcm des ordres des éléments de G. Montrer que G contient un élément d'ordre μ.

(2) Montrer que si p est premier $(\mathbf{Z}/p\mathbf{Z})^{\times}$ est cyclique.

(3) Soient p un nombre premier impair et $r \in \mathbf{N}_{>0}$.

(a) Montrer que $(\mathbf{Z}/p^r\mathbf{Z})^{\times}$ contient un élément d'ordre $p-1$.

(b) Montrer que si $k \in \mathbf{N}$, il existe $a_k \in \mathbf{N}$ non divisible par p tel que $(p+1)^{p^k} = 1 + p^{k+1}a_k$.

(c) En déduire le groupe $(\mathbf{Z}/p^r\mathbf{Z})^{\times}$ est cyclique.

(4) Que se passe-t-il lorsque $p = 2$?