Arithmétique modulaire

Énoncés

Exercice 1 – La comète A passe tous les 5 ans et a été observée l'année dernière. La comète B passe tous les 8 ans et a été observée il y a deux ans. Quelle est la prochaine fois où l'on pourra observer les deux comètes la même année?

Exercice 2 – Determiner tous les multiples de 7 congrus à 1 modulo $2, 3, 4, 5$ et 6. Parmi eux, quel est le plus petit en valeur absolue?

Exercice 3 – Montrer que l'entier $2^{70} + 3^{70}$ est divisible par 13.

Exercice 4 – Trouver le reste de la division euclidienne de 100^{1000} par 13.

Exercice 5 – Notons G le groupe $(\mathbb{Z}/12\mathbb{Z})^\times$ des éléments inversibles de l'anneau $\mathbb{Z}/12\mathbb{Z}$.

1. Quel est l'ordre de G.
2. Énumérer les éléments de G et determiner leurs ordres respectifs.
3. Le groupe G est-il cyclique?

Exercice 6 – Soient $a > 1$ et $n > 0$ deux entiers. Montrer que $\varphi(a^n - 1)$ est divisible par n.

Exercice 7 – Soient n et m deux entiers strictement positifs et posons $N = \text{ppcm}(n, m)$.

1. Montrer que pour tout $x \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, on a $Nx = 0$.
2. En déduire que si $\text{pgcd}(n, m) > 1$ alors les anneaux $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ ne sont pas isomorphes.

Exercice 8 – Montrer que pour tout entier $n > 0$, l'entier $2^{2^{6n+2}} + 3$ est divisible par 19.

Exercice 9– On rappelle qu'un élément a d'un anneau A est *nilpotent* s'il existe un entier $n > 0$ tel que $a^n = 0$. L'anneau A est *réduit* s'il ne possède pas déléments nilpotents non nuls.

1. Montrer que l'anneau $\mathbb{Z}/n\mathbb{Z}$ est réduit si et seulement s'il est sans facteur carré.
2. Déterminer tous les éléments nilpotents de l'anneau $\mathbb{Z}/40\mathbb{Z}$.

Exercice 10 – Afin de communiquer en utilisant le protocole RSA, Alice choisit la clé publique $(e, n) = (37, 65)$.

1. Déterminer la clé secrète d'Alice.

2. Bob transmet le cryptogramme 3. Quel est le message initial?

Exercice 11 – Lors d'un protocole RSA, un même message M (considéré comme un entier) est chiffré en utilisant les trois clés publiques distinctes $(3, a), (3, b)$ et $(3, c)$, avec a, b et c premiers entre eux deux à deux (en particullier, on a l'inégalité $M < \min\{a, b, c\}$. Notons A, B et C les cryptogrammes correspondants (avec $0 < A < a, 0 < B < b$ et $0 < C < c$).

1. Montrer qu'il est possible de déterminer M en ne connaissant que A, B et C (indication : utiliser le théorème des restes chinois).

2. Déterminer M, sachant que $(a, b, c) = (35, 38, 39)$ et $(A, B, C) = (1, 1, 5)$.