Arithmétique

Exercice 1. Résoudre les équations

$$3x = 5 \mod 17 \qquad 6x = 4 \mod 22 \qquad 4x = 3 \mod 46$$

Exercice 2. Résoudre le système $\begin{cases} 2x = 67 \mod 17 \\ 30x = 11 \mod 23 \end{cases}$.

Exercice 3. Résoudre le système $\begin{cases} 2x + 3y = 5 \mod 11 \\ 3x + 7y = -7 \mod 11 \end{cases}$.

Exercice 4. Soit $n \in \mathbb{Z}$. Calculer $(n^2 + n + 1) \wedge (2n^2 - 3n + 1)$ (indication : on pourra être amené à utiliser le résultat suivant, après l'avoir démontré : $a \wedge (5b + 1) = (5a) \wedge (5b + 1)$).

Exercice 5. Montrer que si $a = b \mod n$ alors $a^n = b^n \mod n^2$.

Exercice 6. Résoudre $n^2 + n + 7 = 0 \mod 13$ (mettre le polynôme sous forme canonique mais modulo 13).

Exercice 7. On considère l'équation $(E) : 18x^2 + 7x + 10 = 0\,[35]$ où l'inconnue est $x \in \mathbb{Z}$.

1. Déterminer l'inverse de 18 modulo 35.
2. Montrer que x est solution de (E) ssi
$$(x = 0\,[5] \text{ ou } x = 1\,[5]) \text{ et } (x = 1\,[7] \text{ ou } x = -1\,[7])$$
3. Résoudre (E) en utilisant le théorème des restes chinois.

Exercice 8. Soit $n \geq 1$. Montrer que si $2^n + 1$ est premier alors n est une puissance de 2.

Exercice 9. Soit $a \in \mathbb{N}$ tel que pour tout $n \geq 2$, il existe $x \in \mathbb{Z}$ tel que $x^2 = a\,[n]$. Montrer qu'il existe $b \in \mathbb{Z}$ tel que $a = b^2$.

Exercice 10. Déterminer les $n \in \mathbb{N}$ tels que $n3^n \equiv 1 \mod 7$.

Exercice 11.

1. Soient $a, b, c \in \mathbb{N}^*$ et $m \geq 2$ tels que $ab = c^m$ et $a \wedge b = 1$. Que dire de a et b ?
2. Soit $y \in \mathbb{N}^*$ et $m \geq 2$. Montrer que l'équation $x(x + 1) = y^m$ n'a pas de solutions.

Exercice 12.

1. Soient $n \in \mathbb{N}$ et $p \geq 3$ un diviseur premier de $n^2 + 1$. Montrer que $p \equiv 1 \mod 4$.

2. En déduire qu'il y a une infinité de nombres premiers de la forme $4k+1$.

Exercice 13. Trouver 861 entiers consécutifs non premiers.

Exercice 14.

Montrer que la somme de trois cubes consécutifs est toujours divisible par 9.

Exercice 15.

Montrer que quelques soient les entiers m et n, le nombre $mn(m^{60}-n^{60})$ est divisible par 56786730.

Exercice 16.

Soit $p \in \mathbb{N}^*$, montrer que

$$(p-1)! \equiv -1 \quad [p] \Longleftrightarrow p \text{ est premier.}$$

Pour la réciproque, on pourra considérer les inversibles de $\mathbb{Z}/p\mathbb{Z}$.

Exercice 17. Soient $m, n \in \mathbb{N}^*$.

1. Soient $a, b \in \mathbb{Z}$, justifier
$$a \equiv b[nm] \Longrightarrow a \equiv b[n],$$
On peut donc définir sans ambiguïté l'application f de $\mathbb{Z}/nm\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ qui a modulo nm associe a modulo n.
2. Si $n \wedge m = 1$,t montrer que l'application ψ de $\mathbb{Z}/nm\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ définie par $\psi(x[nm]) = (x[n], x[m])$ est un isomorphisme d'anneaux.
3. On définit l'indicatrice d'euler φ de $\mathbb{N} \setminus \{0;1\}$ dans $\mathbb{N}$ tel que $\varphi(n)$ est le nombre d'inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.
   (a) Soit $p \in \mathcal{P}$ et $k \in \mathbb{N}^*$, calculer $\varphi(p^k)$.
   (b) En utilisant la question 2, montrer que si $n \wedge m = 1$ alors $\varphi(nm) = \varphi(n)\varphi(m)$.
   (c) Soit $n \in \mathbb{N}^*$ et $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ sa décomposition en nombres premiers, calculer $\varphi(n)$.

Exercice 18.

1. Montrer que pour tout entier a impair et tout $n \geq 3$: $a^{2^{n-2}} \equiv 1[2^n]$.
2. Le groupe $(\mathbb{Z}/2^n\mathbb{Z})^\times$ est-il cyclique ?
   (*Un groupe G est cyclique, si il est fini et qu'il existe un élément x de G tel que $G = \{x^k; k \in \mathbb{N}\}$*)

Exercice 19.

Déterminer la valuation 2-adique de $5^{2^n} - 1$.

Exercice 20.

Soit $p \in \mathcal{P}$ et $k \in \mathbb{N}$, déterminer la valuation p-adique de $(1+p)^{p^k} - 1$.