

Exercice 1

7 est-il un carré modulo 13 ?

Exercice 2

Trouver les racines modulo 7 de

- 1 $2x^2 - 3x - 2$
- 2 $x^3 + x^2 + 4x + 1$
- 3 $x^3 + 4x^2 + 3x + 6$

Exercice 3

Trouver les racines modulo 8 de $x^2 + x + 4$.

Exercice 4

Pour chaque valeur de l'entier n , $2 \leq n \leq 20$, calculer $\varphi(n)$ en dénombrant les entiers de $\{1, \dots, n\}$ qui sont premiers avec n .

Exercice 5

Montrer en utilisant la définition de φ que si n est un entier impair alors $\varphi(2n) = \varphi(n)$ et si n est un entier pair alors $\varphi(2n) = 2\varphi(n)$.

Exercice 6

Trouver l'ordre multiplicatif de 2 modulo n et vérifier qu'il divise $\varphi(n)$ pour

- 1 $n = 63$
- 2 $n = 105$

Exercice 7

- 1 Calculer $\varphi(n)$ si n est une puissance d'un nombre premier p .
- 2 En utilisant le théorème chinois, démontrer que $\varphi(mn) = \varphi(m)\varphi(n)$ si m et n sont des entiers premiers entre eux.
- 3 En déduire $\varphi(n)$ en fonction de la décomposition en facteurs premiers de n .

Exercice 8

Soit n un entier qui est le produit de deux nombres premiers distincts. Montrer que

pour tout $x \in \mathbf{Z}$, on a $x^{\varphi(n)+1} \equiv x \pmod{n}$.

Exercice 9

Juliette et Roméo ont lu dans la revue *Pour la Science* un article sur le principe de cryptographie RSA. Ils décident de tester sur un exemple simple pour vérifier qu'ils ont compris. Pour cela Juliette choisit la clef publique ($n = 143$, $e = 7$) Roméo choisit alors un entier compris entre 0 et 142 puis le chiffre avant de transmettre à Juliette le résultat : 27. Pouvez-vous aider Juliette à retrouver l'entier choisi par Roméo? Justifiez soigneusement votre réponse; en particulier, rappelez le principe du chiffrement et du déchiffrement et calculez la clef secrète qui permet le déchiffrement.

Exercice 10

On précise que $5 \times 317 = 1 + 4 \times 396$ et que $154 = 115 \times 437 + 370$. Alice veut transmettre un message codé à Bertrand. Bertrand choisit deux nombres premiers 19 et 23 et obtient une clé publique ($e = 317$, $n = 437$) qu'il envoie à Alice.

- 1 Alice veut transmettre le message M . Comment fait-elle pour chiffrer le message?
- 2 Bertrand reçoit le message chiffré 15. Retrouver l'information transmise par Alice.

Exercice 11

- 1 Écrire le développement décimal de $22/7$.
- 2 Calculer l'ordre multiplicatif de 10 modulo 7.
- 3 Écrire sous forme de fraction irréductible le nombre rationnel dont le développement décimal est 3,14159.

Exercice 12

Dans tout l'exercice n désignera l'entier 187.

- 1 Factoriser n et calculer $\varphi(n)$.
- 2 Quel est l'inverse de 7 modulo 160?
- 3 Montrer que l'ordre multiplicatif modulo n de 21 est égal à 4.
- 4 Lucas souhaite transmettre un message m à Antoine en utilisant le cryptosystème RSA. Il chiffre le message m en un message $M = 21$ puis envoie M à Antoine. Sachant que la clé publique d'Antoine est $(n, e) = (187, 7)$, retrouver le message initial m .

Exercice 13

- 1 Calculer $\varphi(100)$.
- 2 En déduire 53^{799} modulo 100.
- 3 En déduire les deux derniers chiffres de 999953^{799} .

Exercice 14

Déterminer le chiffre des unités et celui des dizaines de 123456^{789} .

Exercice 15

Trouver les trois derniers chiffres de 7^{9999} .

Exercice 16

Soit n un entier supérieur à 2 ; si $0 \leq k \leq n - 1$, on note $c_k = \exp(2ik\pi/n)$.

- 1 Montrer que $\{c_0, \dots, c_n\}$ est l'ensemble des racines complexes du polynôme $X^n - 1$.
- 2 Soit $c \in \mathbf{C}^*$; on suppose que $c^n = 1$. Soit d le plus petit entier strictement positif tel que $c^d = 1$ (on dit que d est l'ordre de c). Montrer que n est multiple de d .
- 3 On suppose que n est le plus petit entier strictement positif tel que $c^n = 1$. Montrer qu'il existe un unique entier $k \in \{0, \dots, n\}$ tel que $\text{pgcd}(k, n) = 1$ et tel que $c = c^k$. Combien y a-t-il de tels nombres complexes c ? Plus généralement, si d divise n , combien y a-t-il d'éléments $c \in \mathbf{C}^*$ dont l'ordre est d ?
- 4 Montrer la relation $\sum_{d|n} \varphi(d) = n$, où la somme est prise sur l'ensemble des diviseurs positifs de n .