

NOMBRES ENTIERS ET RATIONNELS, CONGRUENCES, PERMUTATIONS(A02)

Examen du Mardi 9 mai 2006

10 h 30 - 12 h 30

*Documents, notes de cours ou de TD, téléphones portables, calculatrices sont interdits.
Justifiez toutes vos réponses*

L'énoncé comporte cinq exercices indépendants.

EXERCICE 1

1. Montrer, par récurrence sur n , que pour tout entier $n \geq 1$, $4^n + 5$ est multiple de 3.
2. Proposer une démonstration de ce résultat qui n'utilise pas le principe du raisonnement par récurrence.

EXERCICE 2

1. Calculer le reste de la division euclidienne de 2^{11} par 23.
2. En déduire l'ordre multiplicatif modulo 23 de 2.
Bonus : 2 est-il un générateur multiplicatif modulo 23 ?

EXERCICE 3

1. Résoudre dans $\mathbb{Z}$ l'équation $5x \equiv 1 \pmod{13}$.
2. Calculer 3^6 modulo 13. En déduire si 10 est un carré ou non modulo 13.
3. Résoudre dans $\mathbb{Z}$ l'équation $5x^2 - 2x + 10 \equiv 0 \pmod{13}$.

EXERCICE 4

1. 5 est-il inversible modulo 22 ? Si oui, quel est son inverse ?
2. 110 est-il inversible modulo 63 ? Si oui, quel est son inverse ?
3. Trouver le plus petit entier x positif vérifiant

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 12 \pmod{22} \\ x \equiv 18 \pmod{63} \end{cases}$$

Suite au verso, TSVP

EXERCICE 5

Dans tout l'exercice n désignera l'entier 133.

1. Factoriser n et calculer $\varphi(n)$.
2. Montrer que l'ordre multiplicatif modulo n de 12 est égal à 6.
3. Quel est l'inverse de 5 modulo 108 ?
4. Dans le cryptosystème RSA, vous choisissez la clé publique $(133, 5)$. Le secrétariat veut vous transmettre un message $m \in \{0, \dots, 132\}$. Il chiffre m en $M = 12$ en utilisant le chiffrement RSA et vous transmet M .
Vous recevez M . Que vaut m ?