Contrôle de maths L2 : arithmétique et anneau Z/nZ

Fiche du contrôle

- **Niveau :** licence L2
- **Chapitre :** Arithmétique et anneau Z/nZ
- **Durée conseillée :** 2 heures
- **Barème :** sur 20 points (exercice 1 : 3 points ; exercice 2 : 4 points ; exercice 3 : 4 points ; exercice 4 : 4 points ; exercice 5 : 5 points)
- **Compétences évaluées :**
  - Calculer : dérouler l'algorithme d'Euclide étendu et inverser une classe modulo n
  - Raisonner : démontrer que Z/pZ est un corps lorsque p est premier
  - Chercher : réduire une grande puissance à l'aide des théorèmes d'Euler et de Fermat
  - Modéliser : résoudre un système de congruences et justifier le chiffrement RSA

Exercice 1 : Question de cours : inversibles de Z/nZ (3 points)

Calculatrice interdite. Documents interdits.

Soit $n \geq 2$ un entier. Pour $k \in \mathbb{Z}$, on note $\overline{k}$ sa classe dans $\mathbb{Z}/n\mathbb{Z}$.

a. Démontrez que $\overline{k}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \wedge n = 1$. *(1,5 point)*

b. Démontrez que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier. *(1,5 point)*

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

Exercice 2 : Algorithme d'Euclide étendu (4 points)

a. À l'aide de l'algorithme d'Euclide, calculez $97 \wedge 35$. *(1 point)*

b. Déterminez deux entiers u et v tels que $97u + 35v = 1$. *(1 point)*

c. Déduisez-en l'inverse de $\overline{35}$ dans $\mathbb{Z}/97\mathbb{Z}$, puis résolvez l'équation $35x \equiv 4 \pmod{97}$ d'inconnue $x \in \mathbb{Z}$. *(1 point)*

d. Déterminez tous les couples $(u, v) \in \mathbb{Z}^2$ tels que $97u + 35v = 1$. *(1 point)*

Exercice 3 : Grandes puissances modulo n (4 points)

a. Rappelez la définition de l'indicatrice d'Euler φ et calculez $\varphi(100)$. *(1 point)*

b. Énoncez le théorème d'Euler et appliquez-le à 7 modulo 100. Calculez ensuite 7^4 modulo 100 et déduisez-en l'ordre de $\overline{7}$ dans le groupe $(\mathbb{Z}/100\mathbb{Z})^\times$. *(1 point)*

c. Déterminez les deux derniers chiffres de l'écriture décimale de 7^{2026}. *(1 point)*

d. À l'aide du petit théorème de Fermat, déterminez le reste de la division euclidienne de 2^{2026} par 13. *(1 point)*

Exercice 4 : Lemme chinois (4 points)

a. Énoncez le théorème chinois pour des entiers m_1, m_2, m_3 deux à deux premiers entre eux, sous la forme d'un isomorphisme d'anneaux. *(1 point)*

b. Déterminez tous les entiers x tels que $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$ et $x \equiv 2 \pmod{7}$. *(2 points)*

c. Déduisez de a le nombre d'éléments inversibles de $\mathbb{Z}/105\mathbb{Z}$. *(1 point)*

Exercice 5 : Problème : le chiffrement RSA (5 points)

Alice choisit les nombres premiers $p = 11$ et $q = 17$, puis pose $n = pq = 187$. Elle publie la clé (n, e) avec $e = 7$. Un message est un entier m tel que $0 \leq m < n$; il est chiffré en c, reste de m^e modulo n.

a. Calculez $\varphi(n)$. Justifiez que $\bar{e}$ est inversible dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$ et déterminez l'entier d, avec $0 < d < \varphi(n)$, tel que $ed \equiv 1 \pmod{\varphi(n)}$. *(1 point)*

b. Soit $m \in \mathbb{Z}$. Montrez que $m^{ed} \equiv m \pmod{p}$, en distinguant le cas où p divise m. *(1,5 point)*

c. Déduisez-en que $m^{ed} \equiv m \pmod{n}$ pour tout entier m. Expliquez pourquoi Alice retrouve le message à partir de c. *(1 point)*

d. Bob envoie le message $m = 2$. Calculez le chiffré c. Vérifiez ensuite, en travaillant modulo 11 puis modulo 17, que $c^d \equiv 2 \pmod{187}$. *(1,5 point)*

Réviser avant le contrôle : arithmétique et anneau Z/nZ

Avant de faire ce contrôle, relisez le cours « Arithmétique et Z/nZ » en L2 puis entraînez-vous avec les **exercices corrigés** arithmétique et z/nz.

Retrouvez tous les **contrôles de maths de L2** classés par chapitre, ou choisissez un autre niveau sur la page contrôles de maths du CP au post-bac.

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.