Examen M2 SeCReTS : Rattrapage : Rappels de mathématiques et d'informatique.

Remarques :

- Pour chacune des questions, on demande de justifier les étapes en mentionnant notamment les algorithmes utilisés.
- Aucun document ni aucune calculatrice ne sont admis.
- La durée de l'examen est de deux heures.

Question 1 (Preuve)

Montrez le théorème des restes chinois dans le cas des entiers (en incluant l'étude des systèmes de congruences).

Question 2 (Application de la théorie)

Considérons l'ensemble des classes de congruence $\mathbb{Z}_{15}$ muni de la multiplication modulo 15 que l'on note $\cdot$. Considérons la relation binaire, pour tous $x, y \in \mathbb{Z}_{15}$,

$x \sim y$ si et seulement si il existe $i \in \mathbb{Z}$ tel que $x = 2^i \cdot y \bmod 15$.

1. Montrez que $\sim$ est une relation d'équivalence sur $\mathbb{Z}_{15} \times \mathbb{Z}_{15}$.
2. Donnez l'ensemble des classes d'équivalence de l'ensemble $\mathbb{Z}_{15}$ pour cette relation d'équivalence.

Question 3 (Calcul)

Considérons le polynôme irréductible

$$P(X) = 2X^3 + X + 2 \in \mathbb{Z}_3[X]$$

et le corps fini

$$\mathbb{Z}_3[X]/(P(X)).$$

Considérons les classes A et B dont les représentants sont $X^2 + 1$ et $X + 2$.

1. Déterminer le nombre d'éléments de ce corps.
2. Calculez le représentant minimal de la somme de A et B.
3. Calculez le représentant minimal du produit de A et B.
4. Calculez le représentant minimal de l'inverse de A en utilisant un algorithme systématique.

Question 4 (Calcul)

En précisant les résultats que vous utilisez, calculez toutes les solutions $X \in \mathbb{Z}$ du système de congruences suivant :

$$\begin{cases} X = 1 \bmod 18 \\ X = 2 \bmod 13 \end{cases}$$

Question 1 (Théorie)

- Enoncez un résultat précisant de l'isomorphisme qu'il peut y avoir entre un anneau $(\mathbb{Z}/n\mathbb{Z}, +, *)$ et le produit cartésien d'anneaux de même type (mais avec d'autres paramètres). Montrez ce résultat.
- Enoncez un résultat caractérisant l'inversibilité (multiplicative) d'une classe de $(\mathbb{Z}/n\mathbb{Z}, +, *)$. Montrez ce résultat.

PGCD(a,n)=1.
Preuve de l'inversibilité

Question 2 (Application de la théorie)

Considérons l'ensemble des nombres naturels $\mathbb{N}$ (c-à-d $\{0, 1, 2, 3, \cdots\}$) muni de l'opération binaire addition $+$ classique. On supposera les propriétés de cette opération comme acquises. Considérez l'ensemble produit $\mathbb{N} \times \mathbb{N}$. Considérez la relation binaire, pour tous $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$,

$$(a, b) \sim (c, d) \text{ si et seulement si } a + d = b + c$$

1. Montrez que $\sim$ est une relation d'équivalence sur $\mathbb{N} \times \mathbb{N}$.
2. Définissez les classes d'équivalence que l'on notera $\overline{(a, b)}$ si (a, b) est une représentant. Représentez graphiquement chacune d'entre-elles sur le plan dont les points sont les points de $\mathbb{N} \times \mathbb{N}$.

Notre but est de définir une opération binaire $\oplus$ sur ces classes d'équivalence.

3. Montrez que si $(a, b) \sim (a', b')$ et $(c, d) \sim (c', d')$ alors $(a + c, b + d) \sim (a' + c', b' + d')$.
4. Déduisez-en que l'opération binaire $\overline{(a, b)} \oplus \overline{(c, d)} = \overline{(a + c, b + d)}$ pour tous $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$ est bien définie (ne dépend pas du représentant choisi). Nous avons donc construit une structure quotient muni d'une opération $\oplus$.
5. Donnez la classe d'équivalence qui est l'élément neutre de la structure quotient.
6. Donnez l'opposé de la classe de représentant (a, b).

Question 3 (Calcul)

a. Considérons le groupe multiplicatif de $(\mathbb{Z}_{539}, +, *)$.

1. Calculez le nombre d'éléments de ce groupe en justifiant le raisonnement.

deg de représentant ne dépasse pas 3,

b. Considérons le polynôme irréductible

$$P(X) = X^3 + 2X + 1 \in \mathbb{Z}_3[X]$$

les coeff ne dépassent jamais 3.

et le corps fini

$$\mathbb{Z}_3[X]/(P(X)).$$

1. Déterminez le nombre d'éléments de ce corps.
2. Soit les classes de représentants $A = 2X^2 + 1$ et $B = X^2$. Donnez le représentant minimal de la somme et du produit de ces classes.
3. En utilisant un algorithme systématique, donnez le représentant minimal de l'inverse de la classe dont le présentant est $X^2 + 1$

Question 4

Dénotons par $\bar{\cdot}$ les classes de $(\mathbb{Z}_{11}, +, \cdot)$. On cherche à déterminer le polynôme de degré minimal $P(x)$ de l'ensemble $\mathbb{Z}_{11}[X]$ tel que $P(\overline{1}) = \overline{2}$, $P(\overline{2}) = \overline{5}$ et $P(\overline{4}) = \overline{6}$.

1. Exprimez ce problème sous forme de la résolution d'un système de congruences. Expliquez le raisonnement.
2. Résolvez le système de congruences ci-dessus à l'aide d'une formule explicite et exhibez le polynôme de degré minimal que l'on recherche.