Examen M2 SeCReTS (seconde session) : Rappels de mathématiques

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.

Partie I : Théorie.

Question 1 (question de cours)

1. Montrer le théoreme de Lagrange.
2. Montrer que $a \in (\mathbb{Z}_n, *)$ est inversible si et seulement il existe un plus grand commun diviseur de a et de n valant 1.

Question 2 (application de la théorie)

Considérons les nombres $m_1, m_2, m_3 \in \mathbb{N} \setminus \{0, 1\}$. Il est possible de montrer que tout nombre (naturel) X dans l'intervalle $[0, m_1 \cdot m_2 \cdot m_3[$ peut s'écrire de façon unique comme

$$X = \mu_1 + \mu_2 \cdot m_1 + \mu_3 \cdot m_1 \cdot m_2 \tag{1}$$

avec $\mu_i \in [0, m_i[$ (naturel) pour $i = 1, 2, 3$.

Notre objectif est de trouver l'ensemble des solutions du système de congruences :

$$\begin{aligned} X &\equiv a_1 \bmod m_1 \\ X &\equiv a_2 \bmod m_2 \\ X &\equiv a_3 \bmod m_3 \end{aligned} \tag{2}$$

où les nombres $m_1, m_2, m_3 \in \mathbb{N} \setminus \{0, 1\}$ sont relativement premiers deux à deux et $a_1, a_2, a_3 \in \mathbb{Z}$.

1. Exprimer les coefficients μ_1, μ_2, μ_3 (voir équation (1)) en fonction de $a_1, a_2, a_3, m_1, m_2, m_3$ de telle sorte que X soit solution du système de congruences (2)
2. Déduisez-en l'ensemble des solutions du système de congruences (2).

3. Expliquez comment évaluer les différents formules (pour μ_1, μ_2 et μ_3) le plus efficacement possible.
4. Résoudre le système (2) avec les formules obtenues précédemment lorsque $a_1 = 1, a_2 = 2, a_3 = 3$ et $m_1 = 3, m_2 = 5, m_3 = 7$.

Partie II : Applications.

Question 3

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

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

b. Considérons le polynôme irréductible

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

et le corps fini

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

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

Question 4

1. Calculez un représentant minimal de la classe $[44 + 9\mathbb{Z}]$,
2. Calculez le représentant minimal de la classe $[13 + 14\mathbb{Z}]^{14}$,
3. Calculez la cardinalité du sous-groupe multiplicatif de $(\mathbb{Z}_{14}, +, \cdot)$,
4. Calculez $3^{43} \bmod 14$,
5. Soit $P(X) = X^2 + 1 \in \mathbb{Z}_2[X]$. Est-ce que $\mathbb{Z}_2[X]/(P(X))$. Est-ce un champ ? Justifiez.