Examen Mat309 2023, session 2, durée: 2h

Feuille A4 manuscrite recto-verso autorisée. Autres documents et calculatrices interdits. Les réponses doivent être justifiées.

Questions de cours. ($\sim$ 8 points)

1. Donner la définition des coefficients de Bézout de deux entiers positifs a et b premiers entre eux.

2. Donner le nom de la fonction qui associe à un entier $N \geq 1$ le nombre de classes inversibles dans $\mathbb{Z}/N\mathbb{Z}$.

3. Pour quelles valeurs de N l'anneau $\mathbb{Z}/N\mathbb{Z}$ est-il un corps?

4. Donner un vecteur de norme de Hamming 4 dans $\mathbb{F}_2^5$.

5. Donner la définition d'un code linéaire sur le corps $\mathbb{F}_2$ à deux éléments.

6. Donner les paramètres du code de parité obtenu à partir d'un code de paramètres $(31, 2, 5)$.

Exercice 1. ($\sim$ 4 points)

1. Calculer $9! \pmod{13}$ et $(7+9)! \pmod{11}$.

2. Décrire toutes les solutions de $17x + 8y = 82$ avec x, y dans $\mathbb{Z}$, respectivement avec x, y dans $\mathbb{N}$.

3. Donner l'inverse de $7 \pmod{17}$.

4. Combien l'équation $16x = 5$ a-t-elle de solutions dans $\mathbb{Z}/23\mathbb{Z}$?

Exercice 2. ($\sim$ 6 points)

1. Donner la liste de tous les éléments du groupe multiplicatif $(\mathbb{Z}/7\mathbb{Z})^*$.

2. Écrire la table du groupe multiplicatif $(\mathbb{Z}/7\mathbb{Z})^*$.

3. Donner l'ordre de tous les éléments du groupe multiplicatif $(\mathbb{Z}/7\mathbb{Z})^*$.

4. Donner la liste de tous les éléments de $(\mathbb{Z}/7\mathbb{Z})^*$ qui sont des carrés dans $(\mathbb{Z}/7\mathbb{Z})^*$.

5. Montrer que les carrés de $(\mathbb{Z}/7\mathbb{Z})^*$ forment un sous-groupe de $(\mathbb{Z}/7\mathbb{Z})^*$.

Exercice 3. ($\sim$ 6 points) On considère l'application $f(x) = x^2 + 3$ de l'anneau $A = \mathbb{Z}/11\mathbb{Z}$ dans lui-même.

1. Donner la représentation graphique de f sous forme d'un graphe orienté avec sommets les éléments de A et avec une arête de x à y si $y = f(x)$.

2. Donner le sous-ensemble image $B = \text{Image}(f) = \{y \in A,\ \exists x \in A, y = f(x)\}$ de f.

3. Donner $C = f(B)$ et montrer que $f(C) = C$.

4. Combien d'itérations fait la méthode ρ de Pollard avec $f(x) = x^2 + 14$ et $x_0 = y_0 = 7,\ x_{n+1} = f(x_n),\ y_{n+1} = f(f(y_n))$ sur un entier divisible par 11 avant de détecter le diviseur 11?