Université de Franche-Comté / 2023-2024 Mathématiques
CMI Info 2ème année

Arithmétique 3

Exercice 1. Soit le corps fini $\mathbb{F}_{19}$.

(*i*) Donner les ordres possibles d'un élément de $\mathbb{F}_{19}^{\times}$.

(*ii*) Quel est l'ordre de $\overline{3}$?

(*iii*) Pour chaque ordre possible, donner un élément de $\mathbb{F}_{19}^{\times}$ qui a l'ordre en question.

Exercice 2. Vérifier que 107 est un nombre premier. Soit alors le corps $\mathbb{F}_{107}$. Quels sont les ordres de $\overline{2}$ et de $\overline{3}$?

Exercice 3. Montrer que $\overline{2}$ est une racine primitive de l'unité de $\mathbb{F}_{13}$. Donner alors la table des logarithmes en base $\overline{2}$ des éléments de $\mathbb{F}_{13}^{\times}$.

Exercice 4. Montrer que $\overline{7}$ est une racine primitive de l'unité de $\mathbb{F}_{11}$. Donner alors la table des logarithmes en base $\overline{7}$ des éléments de $\mathbb{F}_{11}^{\times}$.

Exercice 5. Soit le corps $\mathbb{F}_{29}$.

(*i*) Montrer que $\overline{2}$ est une racine primitive de l'unité.

(*ii*) Calculer $\log_{\overline{2}}(\overline{3})$.

(*iii*) En déduire $\log_{\overline{2}}(\overline{6})$ puis $\log_{\overline{2}}(\overline{5})$.

Exercice 6. Soit le corps $\mathbb{F}_{101}$. On admet que $\overline{2}$ est racine primitive de l'unité.

(*i*) Déterminer un représentant principal de $\overline{2}^{50}$.

(*ii*) En déduire $\log_{\overline{2}}(\overline{10})$, $\log_{\overline{2}}(\overline{20})$ puis $\log_{\overline{2}}(\overline{40})$.

Exercice 7.

(i) Donner quelques solutions de l'équation diophantienne $5X^2 - Y^2 = 1$, c'est à dire avec $X, Y \in \mathbb{Z}$.

(ii) Montrer que l'équation diophantienne $5X^2 - Y^2 = 3$ n'a pas de solution dans $\mathbb{Z}$.

Exercice 8. Résoudre dans $\mathbb{F}_7$ le système $\begin{cases} x + y = \overline{2} \\ x + 2y = \overline{1} \end{cases}$.

Exercice 9. Résoudre dans $\mathbb{F}_{11}$ le système $\begin{cases} -x + 2y = \overline{2} \\ 3x + 4y = \overline{1} \end{cases}$.

Exercice 10. A quelle condition sur le paramètre $\lambda \in \mathbb{F}_{13}$ la matrice $A = \begin{pmatrix} \overline{1} & \overline{3} \\ \overline{\lambda} & \overline{4} \end{pmatrix}$ est-elle inversible ?

Exercice 11. Dans $\mathbb{F}_7$, inverser la matrice $B = \begin{pmatrix} \overline{1} & \overline{2} \\ \overline{2} & \overline{1} \end{pmatrix}$.

Exercice 12. Dans $\mathbb{F}_2$, inverser la matrice $C = \begin{pmatrix} \overline{1} & \overline{0} & \overline{1} \\ \overline{1} & \overline{1} & \overline{0} \\ \overline{1} & \overline{1} & \overline{1} \end{pmatrix}$.

Exercice 13. Déterminer les polynômes irréductibles (unitaires) de $\mathbb{F}_2[X]$ de degré 1, de degré 2, de degré 3, degré 4 et de degré 5.

Exercice 14. Déterminer les polynômes irréductibles de degré 2 de $\mathbb{F}_3$ puis de $\mathbb{F}_5$.

Exercice 15. Dans $\mathbb{F}_2[X]$, factoriser les polynômes $P = X^4 + X^2 + X + \overline{1}$ et $Q = X^4 + X^3 + X + \overline{1}$.

Exercice 16. Dans $\mathbb{F}_5[X]$, factoriser les polynômes $P = X^3 + X^2 + X + \overline{1}$ puis $Q = X^3 + X^2 + X + \overline{2}$.

Exercice 17. Sur $\mathbb{F}_p$, soit la matrice $A = \begin{pmatrix} \overline{1} & \overline{2} & \overline{1} \\ \overline{1} & \overline{0} & -\overline{1} \\ \overline{0} & \overline{1} & -\overline{1} \end{pmatrix}$.

(*i*) Calculer le polynôme caractéristique de A.

(*ii*) Etudier la diagonalisation de la matrice A pour $p = 2$, pour $p = 3$, pour $p = 5$ et pour $p = 13$.

Exercice 18. Montrer qu'une matrice carrée A à coefficient dans $\mathbb{F}_p$ est diagonalisable si et seulement si, $A^p = A$.

Exercice 19. Donner les tables d'addition et de multiplication du corps $\mathbb{F}_4$. Déterminer l'ordre de chaque élément de $\mathbb{F}_4^\times$.

Exercice 20. Expliquer comment construire le corps à 1024 éléments.

Exercice 21. Soit le corps fini $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$, avec α vérifiant l'équation $\alpha^2 + 1 = 0$. Vérifier que le corps $\mathbb{F}_9$ contient les racines de tous les polynômes irréductibles de degré 2 de $\mathbb{F}_3[X]$.

Exercice 22. Donner les tables d'addition et de multiplication du corps $\mathbb{F}_9$. Déterminer l'ordre de chaque élément non nul de $\mathbb{F}_9$. Parmi les polynomes irréductibles de degré 2 sur $\mathbb{F}_3$, trouver les polynomes primitifs (c'est à dire ceux dont une racine engendre $\mathbb{F}_9^\times$).

Exercice 23. Reprendre l'exercice précédent avec $\mathbb{F}_8$.

Exercice 24. Soit le corps fini $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$, avec α vérifiant l'équation $\alpha^4 + \alpha + 1 = 0$. Exprimer les éléments α^{-1} et $(\alpha^5 + \alpha)^{-1}$ dans la $\mathbb{F}_2$-base $\{1, \alpha, \alpha^2, \alpha^3\}$.

Exercice 25. Soit $P = X^2 + X - \overline{1} \in \mathbb{F}_3[X]$ et soit $\alpha = \overline{X} \in \mathbb{F}_3[X]/(P)$. Vérifier que $\mathbb{F}_3(\alpha) = \mathbb{F}_9$.
On considère l'application Z_α définie par

$$\begin{array}{rcl} Z_\alpha : \{1, \cdots, 7\} & \to & \{1, \cdots, 7\} \\ i & \mapsto & \log_\alpha(1 - \alpha^i) \end{array}$$

Déterminer explicitement Z_α. En déduire :

(*i*) La simplification de $(1 + \alpha + \alpha^6) + \alpha(1 - \alpha^6)^4$.

(*ii*) La factorisation sur $\mathbb{F}_9$ du polynôme $X^3 + 1 + \alpha^7 \in \mathbb{F}_9[X]$.

Exercice 26. Soit $\mathbb{F}_q$ le corps à q éléments. On suppose q impair.

(*i*) Montrer que tout élément de $\mathbb{F}_q$ est somme de deux carrés.

(*ii*) Montrer que -1 est un carré dans $\mathbb{F}_q$ si et seulement si $q \equiv 1$ (modulo 4).