Exercice 1

Soit G un groupe multiplicatif de cardinal fini $N \in \mathbb{N}^*$.

1. Montrer que a^{N-1} est un inverse de a dans G.
2. On considère la décomposition en base 2 de $N-1$:

$$N-1 = \sum_{i=0}^{k} x_i 2^i \quad \text{avec } k \in \mathbb{N},\ x_i \in \{0,1\},\ i \in \{0,1,\dots,k\} \text{ et } x_k \neq 0.$$

On considère les suites finies $(a_i)_{0\leq i\leq k+1}$ et $(b_i)_{0\leq i\leq k+1}$ définies par :

$$a_0 = 1, \quad b_0 = a, \quad \forall i \in \{0,1,\dots,k\}, \quad a_{i+1} = a_i b_i^{x_i}, \quad b_{i+1} = b_i^2.$$

(a) Montrer que a_{k+1} est l'inverse de a dans G.

(b) En déduire un algorithme de calcul de a^{-1} et préciser en fonction de k son coût (ie le nombre maximum de multiplications dans G que nécessite le calcul de a^{-1}). L'algorithme doit prendre comme argument a et N.

Exercice 2

Soit G le groupe des éléments inversibles de $\mathbb{Z}/148\mathbb{Z}$.

1. Déterminer le cardinal de G.
2. Démontrer que 5 est un élément de G et déterminer son inverse par la méthode de la question 2(b) de l'exercice 1.
3. Donner une autre méthode pour déterminer cet inverse.

Exercice 3

1. Soit G un groupe multiplicatif. Soit $\pi \in G$. Soit e un entier relatif. Soit $\alpha = \pi^e$. On considère l'application :

$$\begin{aligned} f_\alpha : \mathbb{Z} \times G &\longrightarrow G^2, \\ (k,\tau) &\longmapsto (\pi^k, \tau\alpha^k). \end{aligned}$$

(a) Exhiber une fonction $\phi_e : G^2 \longrightarrow G$ ne dépendant que de e et vérifiant :

$$\tau = \phi_e \circ f_\alpha(k,\tau) \quad \forall (k,\tau) \in \mathbb{Z} \times G.$$

(b) On suppose le groupe G et l'élément π connus de tous les membres d'une association. L'un deux, **A**, garde secret l'entier e et rend public l'élément $\alpha = \pi^e$, ainsi donc que la fonction f_α. On recherche une procédure permettant à chacun d'envoyer à **A** un message crypté sous la forme d'un (ou de plusieurs) élément(s) τ de G, telle que la seule connaissance de e suffise à retrouver le message initial.
Justifier le fait que, si l'auteur décompose son message en parties telles que chacune puisse être représentée par un élément τ_i du groupe, choisit pour chacune d'elles un entier k_i et envoie les couples $f_\alpha(k_i,\tau_i) = (\lambda_i, \mu_i)$ à **A**, alors ce dernier peut les décrypter grâce à ϕ_e.

2. Dans cette question G est le groupe $\mathbb{F}_{29}^*$ des inversibles du corps à 29 éléments et les nombres $\pi = 2$ et $\alpha = 18$ sont supposés publics. Chaque associé sait que les entiers $(1,2,\dots,26,27,28)$ modulo 29, dans cet ordre, représentent les éléments du 28-uplet $(A,B,\dots,Z,\text{`'},.)$ où `' figure l'espace séparant deux mots et . est le point de fin de phrase.

(a) Sachant que l'algorithme de décryptage employé par **A** repose sur la seule table ci-dessous des résidus modulo 29 des puissances dix-septièmes des entiers entre 2 et 28 :

λ	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
λ^{17}	21	2	6	9	13	24	10	4	15	3	12	22	11	18	7	17	26	14

20	21	22	23	24	25	26	27	28
25	19	5	16	20	23	27	8	28

Conjecturer la valeur de e et la contrôler grâce à α.

(b) Décrypter le message suivant (on donne les couples (λ_i, μ_i)) :

$$(16,17) \quad (18,24) \quad (28,22) \quad (17,21) \quad (23,23) \quad (24,8).$$

Exercice 4

Soit $\mathbb{F}_{16}$ le corps fini à 16 éléments.

1. (a) Comment peut-on construire $\mathbb{F}_{16}$?
   (b) Démontrer que le groupe multiplicatif $\mathbb{F}_{16}^*$ est formé des puissances successives d'un élément ω vérifiant l'égalité $\omega^4 + \omega^3 + 1 = 0$.
   (c) Démontrer que ω, ω^2, ω^4 et ω^8 sont les racines du polynôme $X^4 + X^3 + 1$ dans $\mathbb{F}_{16}$.
   (d) Démontrer que la famille $(\omega, \omega^2, \omega^4, \omega^8)$ est une base de $\mathbb{F}_{16}$ sur $\mathbb{F}^2$.
2. Soit $a \in \mathbb{F}_{16}$. Résoudre dans $\mathbb{F}_{16}$ l'équation $x^5 = a$, en discutant éventuellement selon la valeur de a.