Plaquette 5 – Structures en action : cryptographie, codes, calendriers

Structures algébriques — Prépa MP / MPI (2e année)

Exercices

Méthode

Les structures algébriques sont au cœur de technologies quotidiennes. La **cryptographie** utilise l'arithmétique de $\mathbb{Z}/n\mathbb{Z}$ et des groupes cycliques $\mathrm{F}_p^\times$ (exponentiation rapide facile, logarithme discret et factorisation difficiles). Les **codes détecteurs et correcteurs** sont des sous-espaces ou des idéaux de $\mathrm{F}_2[X]/(X^n-1)$, ou des sommes de contrôle modulo un entier bien choisi. Les **calendriers**, les **mélanges de cartes**, les **générateurs pseudo-aléatoires** se lisent dans $\mathbb{Z}/n\mathbb{Z}$ ou dans les groupes de permutations. Dans chaque cas, on identifie la structure, puis on applique les théorèmes : Lagrange, Euler, chinois, Bézout.

Exercice 1 – Échange de clés de Diffie-Hellman

Alice et Bob conviennent publiquement de $p = 23$ et $g = 5$. Alice choisit secrètement $a = 6$, Bob $b = 15$.

a) Calculer les valeurs publiques $A = g^a \bmod p$ et $B = g^b \bmod p$.

b) Calculer la clé commune $K = B^a \bmod p$ et vérifier qu'elle vaut $A^b \bmod p$.

c) Pourquoi un espion qui connaît p, g, A, B ne peut-il pas facilement retrouver K (pour de grands p) ?

Exercice 2 – Pourquoi 5 est un bon générateur modulo 23

a) Montrer que les ordres possibles d'un élément de $\mathrm{F}_{23}^\times$ sont $1, 2, 11, 22$.

b) En déduire que g est générateur si et seulement si $g^2 \neq 1$ et $g^{11} \neq 1$.

c) Calculer l'ordre de 2 et celui de 5 modulo 23.

d) Combien $\mathrm{F}_{23}^\times$ a-t-il de générateurs ?

Exercice 3 – Chiffrement d'ElGamal

Avec $p = 23$, $g = 5$, Alice a pour clé privée $x = 6$ et publie $h = g^x = 8$. Bob chiffre le message $m = 10$ avec l'aléa $k = 3$: il envoie $(c_1, c_2) = (g^k, mh^k) \bmod p$.

a) Calculer c_1 et c_2.

b) Montrer qu'Alice retrouve $m = c_2\,(c_1^x)^{-1}$, et effectuer le déchiffrement.

c) Pourquoi faut-il changer d'aléa k à chaque message ?

Exercice 4 – Un code polynomial

On code des messages de 4 bits par des mots de 7 bits : au message $m(X)$ (degré ≤ 3) on associe $c(X) = X^3 m(X) + r(X)$, où r est le reste de $X^3 m(X)$ dans la division par $g = X^3 + X + 1$ dans $\mathrm{F}_2[X]$.

a) Montrer que c est un multiple de g.

b) Coder $m = 1 + X$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

c) À la réception, on calcule le reste de la division par g. Montrer qu'une erreur portant sur un seul bit ($e = X^i$, $0 \le i \le 6$) est toujours détectée.

d) L'erreur $e = X^3 + X + 1$ est-elle détectée ?

Exercice 5 – Le jour de la semaine

On numérote les jours de la semaine modulo 7 (0 = lundi, 1 = mardi, jusqu'à 6 = dimanche). Le 1er janvier 2026 est un jeudi (3).

a) Quel jour de la semaine est le 1er janvier 2027 ? le 1er janvier 2029 (2028 est bissextile) ?

b) Le 30 septembre 2026 est le 273e jour de l'année. Quel jour de la semaine est-ce ?

c) Montrer que le calendrier grégorien a une période de 400 ans (146 097 jours) et que cette période est un nombre entier de semaines.

Exercice 6 – Clé de contrôle des ISBN-13

a) **ISBN-13** : les 13 chiffres $d_1 \cdots d_{13}$ vérifient $\sum_i w_i d_i \equiv 0 \pmod{10}$ avec des poids w_i alternant 1 et 3. Calculer le chiffre de contrôle d'un ISBN commençant par 978270111234.

b) Montrer que l'ISBN-13 détecte toute erreur sur un seul chiffre (pourquoi les poids 1 et 3 conviennent-ils et pas 2 ?).

c) Montrer qu'il ne détecte pas toutes les transpositions de chiffres adjacents (donner une condition sur les chiffres échangés).

Exercice 7 – La clé modulo 97 des IBAN

Un numéro N (écrit en base 10) est accepté si $N \equiv 1 \pmod{97}$.

a) Montrer qu'une erreur sur un seul chiffre est toujours détectée.

b) Montrer qu'une transposition de deux chiffres adjacents distincts est toujours détectée.

c) Pourquoi le choix d'un nombre premier 97, plutôt que 100 par exemple, est-il judicieux ?

Exercice 8 – Chiffrement de Hill

On chiffre des paires de lettres ($A = 0$, $B = 1$, jusqu'à $Z = 25$) par $Y = KX \bmod 26$, avec $K = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$.

a) Chiffrer « HI » ($H = 7$, $I = 8$).

b) Montrer que K est inversible modulo 26 et calculer $K^{-1} \bmod 26$.

c) Déchiffrer le résultat de a).

d) Pourquoi la matrice $\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$ ne convient-elle pas ? (Chiffrer $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ et $\begin{pmatrix} 13 \\ 0 \end{pmatrix}$.)

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

Exercice 9 – Partage de secret de Shamir

On veut partager un secret $s \in \mathrm{F}_{11}$ entre trois personnes, de sorte que deux quelconques puissent le reconstituer mais qu'une seule n'apprenne rien. On choisit $f(x) = s + ax$ avec a aléatoire, et la personne i reçoit $f(i)$.

a) Avec $s = 7$, $a = 3$, calculer les trois parts.

b) Les personnes 2 et 3 mettent en commun leurs parts. Reconstituer $s = f(0)$ par interpolation de Lagrange dans F_{11}.

c) Montrer qu'une seule part, $f(1)$, est compatible avec chacun des 11 secrets possibles.

Exercice 10 – Mélanges parfaits d'un jeu de cartes

Un **mélange parfait extérieur** d'un jeu de 52 cartes (positions 0 à 51) coupe le jeu en deux moitiés et les intercale en gardant la carte du dessus en place. La carte en position k ($0 \le k \le 50$) va en position $2k \bmod 51$, et la carte 51 reste en place.

a) Vérifier la règle sur les premières positions.

b) En déduire que le nombre de mélanges nécessaires pour revenir à l'ordre initial est l'ordre de 2 dans $(\mathbb{Z}/51\mathbb{Z})^{\times}$.

c) Calculer cet ordre.

Exercice 11 – Un générateur pseudo-aléatoire congruentiel

On considère la suite $x_{k+1} = 5x_k + 3 \bmod 16$, $x_0 = 0$.

a) Calculer les termes jusqu'au retour de 0. Quelle est la période ?

b) Vérifier les conditions de Hull-Dobell pour $m = 16$, $a = 5$, $c = 3$.

c) Avec $a = 3$ au lieu de 5, la période est-elle encore maximale ? (Calculer.)

d) Pourquoi les bits de poids faible de tels générateurs sont-ils peu aléatoires ? (Regarder $x_k \bmod 2$.)

Exercice 12 – Le taquin et la signature

Le taquin 4×4 comporte 15 pièces et une case vide. On montre qu'on ne peut pas passer de la position rangée à la position où seules les pièces 14 et 15 sont échangées.

a) On note chaque position par une permutation de $\{1, \dots, 16\}$ (la case vide est « 16 »). Un coup échange la case vide avec une voisine : c'est une transposition. Quelle est la signature d'une suite de k coups ?

b) Colorions les cases en damier : à chaque coup, la case vide change de couleur. Si la case vide revient à sa place, que dire de la parité de k ?

c) Conclure : la permutation « échange de 14 et 15 » est-elle atteignable ?

Exercice 13 – Calculer une grande puissance rapidement

a) Écrire 13 en base 2 et calculer $3^{13} \bmod 17$ par élévations au carré successives ; combien de multiplications faut-il ?

b) Écrire une fonction Python *puissance(a, k, n)* qui calcule $a^k \bmod n$ par cette méthode.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

c) Montrer que le nombre de multiplications est au plus $2\log_2 k + 1$. Comparer avec la méthode naïve pour $k = 10^{100}$.

Exercice 14 – Ordre d'une manœuvre

Un mécanisme permute 7 jetons selon $\sigma = (1\,2\,3)(4\,5)$ à chaque actionnement, et un second mécanisme selon $\tau = (3\,4\,5\,6\,7)$.

a) Combien d'actionnements de σ ramènent les jetons à leur place ?

b) Calculer $\sigma\tau$ (on applique d'abord τ) et son ordre.

c) Montrer que $\sigma\tau$ et $\tau\sigma$ ont le même ordre (ils sont conjugués).

Exercice 15 – Synthèse : signature RSA

Avec $n = 55$, $e = 3$, $d = 27$ (clés RSA : $ed \equiv 1 \pmod{40}$), Alice **signe** un message m en calculant $\sigma = m^d \bmod n$ avec sa clé privée.

a) Signer $m = 7$.

b) Montrer que n'importe qui peut vérifier la signature en calculant $\sigma^e \bmod n$. Effectuer la vérification.

c) Pourquoi un faussaire ne peut-il pas signer un message à la place d'Alice ?

d) Montrer que si σ_1, σ_2 sont les signatures de m_1, m_2, alors $\sigma_1\sigma_2$ est celle de $m_1 m_2$: quelle faiblesse cela révèle-t-il, et comment la contourne-t-on ?

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).