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

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

Corrections détaillées

**Boîte à outils**

**Boîte à outils appliquée.**

- **Exponentiation modulaire** : on calcule $a^k$ mod $n$ par élévations au carré successives ; **Euler** réduit l'exposant modulo $\varphi(n)$.
- **Diffie-Hellman** : $g$ générateur de $\mathrm{F}_p^\times$, clés publiques $g^a$, $g^b$, secret commun $g^{ab}$.
- **Codes polynomiaux** : un mot est un polynôme de $\mathrm{F}_2[X]$ ; il appartient au code s'il est multiple du générateur $g$ ; une erreur $e$ passe inaperçue si et seulement si $g \mid e$.
- **Clés de contrôle** : on choisit un module premier avec les poids pour détecter les erreurs d'un chiffre et les transpositions.
- **Inverse modulaire** d'une matrice : $K$ est inversible modulo $n$ si et seulement si $\det K \wedge n = 1$, et
$$K^{-1} = (\det K)^{-1}\, {}^t\mathrm{com} K \pmod n$$
- **Générateur congruentiel** $x_{k+1} = ax_k + c \bmod m$ : période maximale $m$ si $c \wedge m = 1$, $a-1$ divisible par tout facteur premier de $m$, et par 4 si $4 \mid m$ (Hull-Dobell).

## Correction de l'exercice 1 – Échange de clés de Diffie-Hellman

a) Par carrés successifs : $5^2 = 25 \equiv 2$, $5^4 \equiv 4$, $5^6 = 5^4 \times 5^2 \equiv 8$ : $A = 8$. $5^8 \equiv 16$, $5^{15} = 5^8 \times 5^4 \times 5^2 \times 5 \equiv 16 \times 4 \times 2 \times 5 = 640 \equiv 640 - 621 = 19$ : $B = 19$.

b) $K = 19^6$ : $19 \equiv -4$, $(-4)^2 = 16$, $(-4)^4 = 256 \equiv 3$, $(-4)^6 = 3 \times 16 = 48 \equiv 2$. Et $A^b = 8^{15}$ : $8 = 5^6$, donc $8^{15} = 5^{90} = (5^{22})^4 \times 5^2 \equiv 2$ (Fermat). Les deux valent 2 :
$$K = g^{ab} = (g^a)^b = (g^b)^a = 2$$

c) Il faudrait retrouver $a$ à partir de $g^a$ (**logarithme discret**), problème qu'on ne sait pas résoudre rapidement pour $p$ de plusieurs centaines de chiffres, alors que le calcul de $g^a$ est rapide.

**Réponse.** $A = 8$, $B = 19$ ; $K = 2$.

## Correction de l'exercice 2 – Pourquoi 5 est un bon générateur modulo 23

a) $\mathrm{card}\,\mathrm{F}_{23}^\times = 22 = 2 \times 11$ ; par Lagrange, l'ordre divise 22.

b) Un élément d'ordre $d < 22$ a un ordre 1, 2 ou 11, donc vérifie $g^2 = 1$ ou $g^{11} = 1$. Réciproquement, si $g^2 \neq 1$ et $g^{11} \neq 1$, l'ordre n'est ni 1, ni 2, ni 11 : il vaut 22.

c) $2^{11} = 2\,048 = 89 \times 23 + 1$ : 2 est d'ordre 11 (pas générateur). Pour 5 : $5^2 = 25 \equiv 2 \neq 1$ et $5^{11} = 5 \times (5^2)^5 \equiv 5 \times 2^5 = 160 \equiv 160 - 138 = 22 \equiv -1 \neq 1$ : 5 est générateur.
$$\mathrm{ord}(2) = 11, \qquad \mathrm{ord}(5) = 22$$

d) $\mathrm{F}_{23}^\times$ est cyclique d'ordre 22 : $\varphi(22) = 10$ générateurs.

**Réponse.** Ordres $1, 2, 11, 22$ ; $\mathrm{ord}(2) = 11$, $\mathrm{ord}(5) = 22$ ; 10 générateurs.

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).

## Correction de l'exercice 3 – Chiffrement d'ElGamal

a) $c_1 = 5^3 = 125 \equiv 125 - 115 = 10$. $h^3 = 512 \equiv 512 - 506 = 6$, donc $c_2 = 10 \times 6 = 60 \equiv 14$.

b) $c_1^x = g^{kx} = h^k$, donc

$$c_2 (c_1^x)^{-1} = m h^k (h^k)^{-1} = m$$

— Calcul : $c_1^6 = 10^6$ ; $10^2 = 100 \equiv 8$, $10^4 \equiv 64 \equiv 18$, $10^6 \equiv 18 \times 8 = 144 \equiv 6$. L'inverse de 6 modulo 23 est 4 ($24 \equiv 1$). $m = 14 \times 4 = 56 \equiv 10$.

c) Si deux messages $m$, $m'$ utilisent le même $k$, le quotient $\frac{c_2}{c_2'} = \frac{m}{m'}$ est connu : la connaissance d'un message révèle l'autre.

**Réponse.** $(c_1, c_2) = (10, 14)$ ; déchiffrement : $m = 14 \times 6^{-1} = 14 \times 4 \equiv 10$.

## Correction de l'exercice 4 – Un code polynomial

a) $X^3 m = gq + r$, donc $c = X^3 m + r = gq + 2r = gq$ dans $\mathrm{F}_2[X]$ ($-r = r$).

b) $X^3 m = X^3 + X^4$. Division par $g$ : $X^4 = Xg + X^2 + X$, donc $X^4 + X^3 \equiv X^2 + X + X^3 \equiv X^2 + X + X + 1 = X^2 + 1$. Ainsi $r = X^2 + 1$ et

$$c = X^4 + X^3 + X^2 + 1 = (X + 1)(X^3 + X + 1)$$

— (en bits, du degré 0 au degré 6 : 1011100).

c) Le mot reçu est $c + e$, de reste $e$ mod $g$ ; l'erreur passe inaperçue si et seulement si $g \mid e$. Or $g$, de degré 3 et de terme constant 1, ne divise aucun monôme $X^i$ (il n'est pas une puissance de $X$, et $X$ ne divise pas $g$). Toute erreur simple est détectée.

d) Non : $e = g$ est multiple de $g$, le mot erroné est un mot du code. Aucun code ne détecte toutes les erreurs.

**Réponse.** $c = gq$ ; $m = 1 + X \mapsto c = X^4 + X^3 + X^2 + 1$ ; erreurs simples détectées ; $e = g$ non détectée.

## Correction de l'exercice 5 – Le jour de la semaine

a) $365 = 52 \times 7 + 1 \equiv 1 \pmod 7$ : une année ordinaire décale d'un jour. Le 1er janvier 2027 est un vendredi ($3 + 1 = 4$). Entre 2027 et 2029 : $365 + 366 = 731 \equiv 3$, donc le 1er janvier 2029 est le jour $4 + 3 = 7 \equiv 0$ : un lundi.

b) Le 273e jour est 272 jours après le 1er janvier ; $272 = 38 \times 7 + 6$, donc jour $3 + 6 = 9 \equiv 2$ : un mercredi.

c) En 400 ans : 97 années bissextiles ($100 - 4 + 1$), soit $400 \times 365 + 97 = 146\,097$ jours. Et $146\,097 = 7 \times 20\,871$ : multiple de 7. Le calendrier (jours de la semaine compris) se répète tous les 400 ans.

**Réponse.** 1er janvier 2027 : vendredi ; 2029 : lundi ; 30 septembre 2026 : mercredi ; $146\,097 = 7 \times 20\,871$.

## Correction de l'exercice 6 – Clé de contrôle des ISBN-13

a) $9 + 3 \times 7 + 8 + 3 \times 2 + 7 + 3 \times 0 + 1 + 3 \times 1 + 1 + 3 \times 2 + 3 + 3 \times 4 = 77$ ; il faut ajouter $d_{13}$ de poids 1 tel que $77 + d_{13} \equiv 0 \pmod{10}$ : $d_{13} = 3$.

b) Remplacer $d_i$ par $d_i'$ change la somme de $w_i(d_i' - d_i)$ avec $0 < |d_i' - d_i| \leq 9$. Comme $w_i \in \{1, 3\}$ est **inversible** modulo 10, ce produit n'est pas divisible par 10 :

$$w_i(d_i' - d_i) \equiv 0 \pmod{10} \Leftrightarrow d_i' = d_i$$

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).

— Un poids 2 ne conviendrait pas : $2 \times 5 \equiv 0$.

c) Échanger $d_i$ et $d_{i+1}$ (poids 1 et 3) change la somme de $2(d_{i+1} - d_i)$, multiple de 10 si et seulement si $|d_{i+1} - d_i| = 5$ : la transposition de 1 et 6, par exemple, n'est pas détectée.

**Réponse.** Chiffre de contrôle 3 ; erreurs simples détectées (1, 3 inversibles mod 10) ; transpositions non détectées si les chiffres diffèrent de 5.

## Correction de l'exercice 7 – La clé modulo 97 des IBAN

a) Changer le chiffre de rang $k$ de $a$ en $b$ modifie $N$ de $(b-a)10^k$, avec $0 < |b-a| \leq 9$. Comme 97 est premier et ne divise ni $b-a$ ni $10^k$ (lemme d'Euclide), 97 ne divise pas la différence : $N$ n'est plus $\equiv 1$.

b) Échanger les chiffres $a$ (rang $k+1$) et $b$ (rang $k$) modifie $N$ de

$$(b-a)10^{k+1} + (a-b)10^k = 9(b-a)10^k$$

— non divisible par 97 (premier ne divisant ni 9, ni $b-a \neq 0$, ni $10^k$).

c) Modulo 100, une modification $(b-a)10^k$ avec $k \geq 2$ serait invisible (multiple de 100). Un module premier avec 10 et assez grand ($> 9 \times 9$) détecte ces deux types d'erreurs, les plus fréquentes à la saisie.

**Réponse.** Erreurs simples et transpositions adjacentes toujours détectées (97 premier, ne divise ni 9, ni $b-a$, ni $10^k$).

## Correction de l'exercice 8 – Chiffrement de Hill

a) $K\begin{pmatrix}7\\8\end{pmatrix} = \begin{pmatrix}21+24\\14+40\end{pmatrix} = \begin{pmatrix}45\\54\end{pmatrix} \equiv \begin{pmatrix}19\\2\end{pmatrix}$ : « TC ».

b) $\det K = 15 - 6 = 9$, premier avec 26 : inversible, d'inverse 3 ($27 \equiv 1$). Avec la comatrice transposée :

$$K^{-1} \equiv 3\begin{pmatrix}5 & -3\\-2 & 3\end{pmatrix} = \begin{pmatrix}15 & -9\\-6 & 9\end{pmatrix} \equiv \begin{pmatrix}15 & 17\\20 & 9\end{pmatrix} \pmod{26}$$

c) $K^{-1}\begin{pmatrix}19\\2\end{pmatrix} = \begin{pmatrix}285+34\\380+18\end{pmatrix} = \begin{pmatrix}319\\398\end{pmatrix} \equiv \begin{pmatrix}7\\8\end{pmatrix}$ ($319 = 12 \times 26 + 7$, $398 = 15 \times 26 + 8$) : « HI ».

d) Son déterminant vaut 2, non premier avec 26 : elle n'est pas inversible modulo 26. Concrètement, $\begin{pmatrix}0\\0\end{pmatrix}$ et $\begin{pmatrix}13\\0\end{pmatrix}$ (« AA » et « NA ») ont le même chiffré $\begin{pmatrix}0\\0\end{pmatrix}$, car $2 \times 13 = 26 \equiv 0$ : le déchiffrement est impossible.

**Réponse.** « HI » → « TC » ; $K^{-1} = \begin{pmatrix}15 & 17\\20 & 9\end{pmatrix}$ ; condition $\det K \wedge 26 = 1$.

## Correction de l'exercice 9 – Partage de secret de Shamir

a) $f(1) = 10$, $f(2) = 13 \equiv 2$, $f(3) = 16 \equiv 5$.

b) Lagrange aux points 2 et 3, évalué en 0 :

$$f(0) = f(2)\frac{0-3}{2-3} + f(3)\frac{0-2}{3-2} = 3f(2) - 2f(3) = 6 - 10 = -4 \equiv 7$$

— On retrouve $s = 7$ (dans $\mathrm{F}_{11}$, tous les dénominateurs sont inversibles).

c) Pour tout $s' \in \mathrm{F}_{11}$, il existe un unique $a' = f(1) - s'$ tel que $s' + a' \times 1 = f(1)$ : la part $f(1)$ ne privilégie aucun secret. Avec $a$ uniforme, $f(1)$ est uniforme et indépendante de $s$.

**Réponse.** Parts $10, 2, 5$ ; $f(0) = 3f(2) - 2f(3) \equiv 7$ ; une part seule ne révèle rien.

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).

## Correction de l'exercice 10 – Mélanges parfaits d'un jeu de cartes

a) Après le mélange, l'ordre est $0, 26, 1, 27, 2, \ldots$ : la carte $k$ de la première moitié va en position $2k$, et la carte $26 + j$ en position $2j + 1 = 2(26 + j) - 51$, soit $2k \bmod 51$.

b) Après $n$ mélanges, la carte $k$ est en position $2^n k \bmod 51$. Le jeu revient à l'ordre initial si et seulement si $2^n k \equiv k$ pour tout $k$, en particulier pour $k = 1$ :

$$2^n \equiv 1 \pmod{51}$$

c) Puissances de 2 modulo 51 : $2, 4, 8, 16, 32, 64 \equiv 13, 26, 52 \equiv 1$. L'ordre de 2 est 8 : **huit** mélanges parfaits rétablissent l'ordre d'un jeu de 52 cartes (alors que $\varphi(51) = 32$).

**Réponse.** Position $k \mapsto 2k \bmod 51$ ; ordre de 2 modulo 51 : 8 mélanges.

## Correction de l'exercice 11 – Un générateur pseudo-aléatoire congruentiel

a) $0, 3, 2, 13, 4, 7, 6, 1, 8, 11, 10, 5, 12, 15, 14, 9$, puis 0 : période 16, maximale (tous les restes apparaissent).

b) $c = 3$ est premier avec 16 ; le seul facteur premier de 16 est 2, qui divise $a - 1 = 4$ ; et $4 \mid 16$ impose $4 \mid a - 1$ : vrai. Les conditions sont remplies.

c) $a = 3$ : $a - 1 = 2$ n'est pas divisible par 4. Calcul : $0, 3, 12, 7, 8, 11, 4, 15, 0$ : période 8 seulement.

d) Modulo 2 : $x_{k+1} \equiv x_k + 1$ (car $a$ et $c$ sont impairs), donc la parité alterne : $0, 1, 0, 1, \ldots$ Le bit de poids faible est parfaitement prévisible.

**Réponse.** Période 16 ; conditions vérifiées ; $a = 3$ : période 8 ; bit de poids faible alterné.

## Correction de l'exercice 12 – Le taquin et la signature

a) Une transposition a pour signature $-1$ ; par multiplicativité de la signature, $k$ coups donnent une permutation de signature $(-1)^k$.

b) La case vide alterne entre les deux couleurs du damier : pour revenir à sa case de départ, il faut un nombre **pair** de coups.

c) Dans la position visée, la case vide est à sa place et la permutation est une transposition, de signature $-1$. Or toute position atteinte avec la case vide à sa place correspond à $k$ pair, donc à une signature $(-1)^k = 1$. Impossible :

$$\varepsilon(\sigma) = (-1)^k = 1 \neq -1 = \varepsilon((14\ 15))$$

— (C'est la célèbre énigme de Sam Loyd : la moitié des positions sont inaccessibles.)

**Réponse.** Signature $(-1)^k$ ; $k$ pair si le vide revient ; l'échange $14 \leftrightarrow 15$ (signature $-1$) est impossible.

## Correction de l'exercice 13 – Calculer une grande puissance rapidement

a) $13 = 8 + 4 + 1$ (en binaire 1101). Carrés : $3^2 = 9$, $3^4 = 81 \equiv 13$, $3^8 \equiv 169 \equiv 16$. Puis $3^{13} = 3^8 \times 3^4 \times 3 \equiv 16 \times 13 \times 3 = 624 \equiv 624 - 612 = 12$. Soit 3 élévations au carré et 2 multiplications, au lieu de 12.

b) Script :

```
def puissance(a, k, n):
    r = 1
    a = a % n
    while k > 0:
        if k % 2 == 1:
```

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).

```
            r = (r * a) % n
        a = (a * a) % n
        k = k // 2
    return r
```

c) La boucle s'exécute autant de fois que $k$ a de chiffres binaires, $\lfloor \log_2 k \rfloor + 1$, avec au plus 2 multiplications par tour. Pour $k = 10^{100}$ : environ $2 \times 333 = 666$ multiplications, contre $10^{100}$ pour la méthode naïve. C'est ce qui rend RSA et Diffie-Hellman praticables.

$$\text{coût} = O(\log k)$$

**Réponse.** $3^{13} \equiv 12 \pmod{17}$ ; exponentiation rapide ; $\approx 2\log_2 k$ multiplications.

## Correction de l'exercice 14 – Ordre d'une manœuvre

a) $\text{ord}(\sigma) = \text{ppcm}(3, 2) = 6$.

b) On suit chaque élément : $1 \xrightarrow{\tau} 1 \xrightarrow{\sigma} 2$ ; $2 \to 2 \to 3$ ; $3 \to 4 \to 5$ ; $5 \to 6 \to 6$ ; $6 \to 7 \to 7$ ; $7 \to 3 \to 1$ ; $4 \to 5 \to 4$. Donc

$$\sigma\tau = (1\,2\,3\,5\,6\,7), \qquad \text{ord}(\sigma\tau) = 6$$

— (4 est fixe).

c) $\tau\sigma = \tau(\sigma\tau)\tau^{-1}$ : conjugués, ils ont la même structure de cycles, donc le même ordre ( $\text{ord}(gxg^{-1}) = \text{ord}(x)$ car $(gxg^{-1})^k = gx^kg^{-1}$).

**Réponse.** ord$\sigma = 6$ ; $\sigma\tau = (1\,2\,3\,5\,6\,7)$, d'ordre 6 ; $\tau\sigma$ conjugué, même ordre.

## Correction de l'exercice 15 – Synthèse : signature RSA

a) $7^{27}$ mod 55 par le théorème chinois. Modulo 5 : $7 \equiv 2$, $2^{27} = (2^4)^6 \times 2^3 \equiv 8 \equiv 3$. Modulo 11 : $7^{27} = (7^{10})^2 \times 7^7 \equiv 7^7$ ; $7^2 = 49 \equiv 5$, $7^4 \equiv 25 \equiv 3$,
$7^7 = 7^4 \times 7^2 \times 7 \equiv 3 \times 5 \times 7 = 105 \equiv 6$. On cherche $\sigma \equiv 3 \pmod 5$, $\sigma \equiv 6 \pmod{11}$ : $\sigma = 28$.

b) $\sigma^e = m^{de} \equiv m$ (RSA). Vérification : $28^3 = 21\,952 = 399 \times 55 + 7$ :

$$28^3 \equiv 7 \pmod{55}$$

c) Produire $\sigma$ tel que $\sigma^3 \equiv m$ revient à extraire une racine cubique modulo $n$, ce qu'on ne sait faire qu'en connaissant $d$, donc $\varphi(n)$, donc la factorisation de $n$.

d) $(\sigma_1\sigma_2)^e = \sigma_1^e\sigma_2^e \equiv m_1m_2$ : on fabrique une signature valide du produit sans connaître $d$. En pratique, on signe une **empreinte** (hachage) du message, et non le message lui-même, ce qui détruit cette multiplicativité exploitable.

**Réponse.** $\sigma = 28$ ; $28^3 \equiv 7 \pmod{55}$ ; signer exige $d$ ; multiplicativité contournée par hachage.

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).