Partiel de Cryptologie

15 mars 2023
Durée 1h30

Auteurs
Valérie Ménissier-Morain & Jérémy Berthomieu

Version du 24 avril 2023

Le seul document autorisé est une feuille manuscrite A4 recto-verso.
L'utilisation d'un appareil électronique est proscrite pendant toute la durée de l'épreuve.
Le barème sur 28 points est indicatif. La note finale sera le minimum entre les points obtenus et 20.

Exercice 1 – Questions diverses – 17,5 points

1. (**1 point**) Qu'est-ce qui provoque la révolution de la cryptologie moderne ?

> **Solution :**
> L'avènement de l'ordinateur commercial nécessite de partager des clefs de chiffrement avec un nombre de plus en plus grand d'interlocuteurs sans les connaître préalablement (n interlocuteurs partagent $O(n^2)$ clefs), il faut donc un mécanisme d'échange de clefs sans intervention humaine directe.
> Autre réponse tolérée : description des causes de la transition entre la crypto moderne et la crypto post-quantique.

2. (**Types d'éléments dans un anneau – 3,5 points**) Soit $(A, +, \times)$ un anneau, d'éléments neutres 0 pour $+$ et 1 pour $\times$. Donnez la définition d'un élément inversible, d'un diviseur de 0. Montrez qu'un élément inversible ne peut être un diviseur de 0. En vous appuyant sur les anneaux que vous avez rencontrés dans ce cours, dites s'il existe des anneaux qui ne contiennent pas de diviseur de 0 ? des anneaux qui ne contiennent que 0, des diviseurs de 0 et des éléments inversibles ? des anneaux qui contiennent des éléments autres que 0, des diviseurs de 0 et des éléments inversibles ?

> **Solution :**
> Un élément x est inversible s'il existe un élément y tel que $x \times y = y \times x = 1$.
> Un élément x est un diviseur de 0 s'il existe un élément $y \neq 0$ tel que $x \times y = y \times x = 0$.
> Soit x un élément inversible et y un élément tel que $x \times y = 0$, alors $y = (x^{-1} \times x) \times y = x^{-1} \times (x \times y) = x^{-1} \times 0 = 0$ donc x n'est pas un diviseur de 0.
> Il existe des anneaux qui ne contiennent pas de diviseurs de 0, ce sont par définition les anneaux intègres , dont $\mathbb{Z}$ ou $\mathbb{Z}/p\mathbb{Z}$ avec p premier sont des exemples.
> Les anneaux $\mathbb{Z}/n\mathbb{Z}$ avec n non premier ne contiennent que 0, des diviseurs de 0 (les nombres non premiers avec n) et des éléments inversibles (les éléments premiers avec n).
> $\mathbb{Z}$ contient 0, des éléments inversibles (1 et -1), aucun diviseur de 0 et d'autres éléments (tous ceux de valeur absolue supérieure à 1) qui sont irréductibles ou produit d'irréductibles.

3. (**Ordre des éléments – 1 point**) Soit p un nombre premier et G un groupe à p^2 éléments, quel peut être l'ordre d'un élément du groupe ? Justifiez votre réponse.

Solution :
D'après le théorème de Lagrange, l'ordre des éléments divise l'ordre du groupe.
Or, le groupe est de cardinal, donc d'ordre p^2.
Les ordres possibles pour les éléments de G sont les diviseurs de p^2 , c'est-à-dire 1, p et p^2 puisque p est premier .

4. (**Calcul modulaire – 2 points**) Calculez 12^{27} mod 17.

Solution :
$12 = (-5)$ mod 17, $12^2 = (-5)^2 = 25 = 8$ mod 17, $12^4 = 8^2 = 64 = -4$ mod 17, $12^8 - (-4)^2 = -1$ mod 17. Donc $12^{27} = 12^{3*8+3} = (12^8)^3 \times 12^3 = (-1)^3 \times 12^3 = 5^3 = 6$ mod 17.
Autre solution : utiliser l'algorithme d'exponentiation *square and multiply* : $27 = 110011_2$ donc

$$12^{27} = (((12^2 * 12)^2)^2)^2) * 12^2 * 12.$$

Or $12 = (-5)$ mod 17 donc $12^2 = (-5)^2 = 25 = 8$ mod 17 et $12^2 * 12 = (-5) * 8 = -6$ mod 17. Par conséquent $12^{27} = ((((-6)^2)^2)^2) * (-6) = (-6)^8 * (-6)$. Or $(-6)^2 = 36 = 2$ mod 17 donc $12^{27} = 2^4 * (-6) = 16 * (-6) = (-1) * (-6) = 6$ mod 17.
s'ils utilisent et citent le théorème d'Euler.

5. (**Équation – 4 points**) Résoudre l'équation $x^2 + 3x + 4 = 0$ dans $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/11\mathbb{Z}$ et $\mathbb{Z}/13\mathbb{Z}$.

Solution :
En cas de calcul exhaustif de toutes les valeurs du polynôme pour chaque anneau .

On vérifie rapidement que pour tout $x \in \mathbb{Z}/6\mathbb{Z}$, $x^2 + 3x + 4 \neq 0$ donc l'équation n'a pas de solution dans $\mathbb{Z}/6\mathbb{Z}$
Pour les trois autres anneaux, on a à résoudre une équation du second degré $ax^2 + bx + c = 0$ avec $a = 1$, $b = 3$ et $c = 4$ dans un corps. On adapte la méthode vue dans $\mathbb{R}$ au lycée à un corps avec un nombre fini d'éléments.
Puisqu'il s'agit d'un corps on sait que $2a$ avec $a \neq 0$ sera inversible
Il nous reste à calculer le discriminant de l'équation $\Delta = b^2 - 4ac = 3 * 3 - 4 * 1 * 4 = 9 - 16 = -7$ et à déterminer s'il s'agit d'un carré dans le corps .

- Dans $\mathbb{Z}/7\mathbb{Z}$, $\Delta = 0$ donc l'équation a une solution double $x_0 = (2a)^{-1} \times (-b) = 2^{-1} \times (-3)$. Or, $2^{-1} = 4$ mod 7 donc $x_0 = 4 \times (-3) = -12 = 2$.
- Dans $\mathbb{Z}/11\mathbb{Z}$, $\Delta = 4 = 2^2$ donc l'équation a deux solutions simples $(2a)^{-1}(-b \pm \sqrt{\Delta}) = 2^{-1}(-3 \pm 2)$. Or, $2^{-1} = 6$ dans $\mathbb{Z}/11\mathbb{Z}$ donc les deux solutions sont $x_1 = 6 \times (-3 - 2) = -30 = 3$ et $x_2 = 6 \times (-3 + 2) = -6 = 5$.
- Dans $\mathbb{Z}/13\mathbb{Z}$, $\Delta = 6$. Or, les carrés de $\mathbb{Z}/13\mathbb{Z}$ sont $0^2 = 0$, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 = 9$, $(\pm 4)^2 = 3$, $(\pm 5)^2 = 12$, $(\pm 6)^2 = 10$, donc Δ n'est pas un carré et l'équation n'a pas de solutions dans $\mathbb{Z}/13\mathbb{Z}$.

6. (**Pgcd – 2 points**) Que vaut pgcd$(7^{100k} - 1, 303)$ pour $k > 0$? Justifiez votre réponse.

Solution :
Puisqu'il s'agit du pgcd d'un nombre avec $303 = 3 \times 101$, ce pgcd est un diviseur de 303 donc 1, 3, 101 ou 303. Il suffit donc de déterminer si $7^{100k} - 1$ est divisible par 3 et/ou par 101.

- $7 = 6 + 1$ donc 6 divise $7^n - 1$ pour tout $n \in \mathbb{N}$, donc 3 divise $7^{100k} - 1$.

— 101 est premier donc $\mathbb{Z}/101\mathbb{Z}^\times$ est d'ordre 100 et d'après le théorème de Lagrange tout élément n de $\mathbb{Z}/100\mathbb{Z}^\times$ a un ordre diviseur de 100, donc $n^{100} = 1 \mod 101$. Donc ici $7^{100k} - 1 = 0 \mod 101$ et 101 divise $7^{100k} - 1$.

Par conséquent pgcd$(7^{100k} - 1, 303) = 303$.

Autre solution : 7 et $303 = 3 * 101$ sont premiers entre eux donc il existe u et v tels que $7\,u + 303\,v = 1$ donc $7 = 1 \mod 303$ et si $k > 0$, alors $7^{100k} = 1 \mod 303$, d'où $7^{100k} - 1 = 0 \mod 303$, donc 303 divise $7^{100k} - 1$ et pgcd$(7^{100k} - 1, 303) = 303$.

7. **(1+3 points)** Expliquez sans calcul complexe pourquoi il n'existe pas d'entiers u et v tels que $1023\,u + 978\,v = 8$. Calculez deux entiers u et v tels que $1023\,u + 978\,v = 9$. Justifiez votre démarche.

Solution :

Par définition le pgcd de 1023 et 978 divise toute combinaison de la forme $1023\,u + 987\,v$ avec u et v entiers.

Le critère de divisibilité par 3 nous indique que ces deux nombres sont des multiples de 3 donc leur pgcd est un multiple de 3 et puisque 3 ne divise pas 8, il n'existe pas d'entiers u et v tels que $1023\,u + 978\,v = 8$.

9 est multiple de 3 donc il y a des chances de trouver la combinaison attendue. Nous allons y regarder de plus près avec l'algorithme d'Euclide étendu pour $a = 1023$ et $b = 978$.

On applique l'algorithme d'Euclide étendu à $a = 1023$ et $n = 978$.

Dans le tableau suivant chaque ligne à partir de la ligne $i = 1$ se lit :

- la partie gauche (colorée en rose), si $r_i \neq 0$, la division euclidienne de r_{i-1} par r_i est $r_{i-1} = q_i * r_i + r_{i+1}$ qui définit le quotient $q_i = \lfloor \frac{r_{i-1}}{r_i} \rfloor$ et le reste suivant $r_{i+1} = r_{i-1} - q_i * r_i$; sinon on s'arrête.
- pour la partie droite (colorée en jaune), $u_{i+1} = u_{i-1} - q_i * u_i$ et $v_{i+1} = v_{i-1} - q_i * v_i$
- avec l'initialisation (partie en haut, colorée en bleu) : $r_0 = a$, $r_1 = b$, $u_0 = v_1 = 1$, $v_0 = u_1 = 0$
- à chaque étape on a $r_i = u_i\,a + v_i\,b \ \ \forall i$.

À l'avant-dernière ligne (de numéro k), on trouve r_{k+1} (dans la cinquième colonne) le dernier reste positif, c'est-à-dire le pgcd de a et b et $r_{k+1} = u_{k+1}\,a + v_{k+1}\,b$ est une relation de Bézout.

i	r_{i-1}	q_i	r_i	r_{i+1}	u_{i+1}	v_{i+1}
-1					1	0
0			1023	978	0	1
1	1023	1	978	45	1	-1
2	978	21	45	33	-21	22
3	45	1	33	12	22	-23
4	33	2	12	9	-65	68
5	12	1	3	3	87	-91
6	9	3	3	0	-326	341

La relation de Bézout entre 1023 et 978 se lit donc sur l'avant-dernière ligne : $87 * 1023 - 91 * 978 = 3$.

À la ligne précédente on lit $-65 * 1023 + 68 * 987 = 9$ ce qui fournit un couple de valeurs de $x = -65$ et $y = 68$.

Si on ne s'en était pas aperçu, dans la mesure où $9 = 3 * 3$, on aurait multiplié la relation de Bézout par 3 et on aurait obtenu $3 * 87 * 1023 - 3 * 91 * 978 = 3 * 3$ et proposé le couple $x = 3 * 87 = 261$ et $y = 3 * (-91) = -273$.

Exercice 2 – Message chiffré – 5 points

L'abbé Tritheme a vécu l'apparition de l'imprimerie et est connu pour ses nombreuses méthodes de dissimulation de ses écrits, notamment un système de chiffrement auquel il a laissé son nom. Ce chiffrement, antérieur à celui de Vigenère, en est un cas particulier où chaque colonne au-delà de la première est décalé d'un cran de plus que la colonne précédente.

Il vous adresse ce message

```
ZTLAN EQKMM DSQRL BNCZL MQAKF RHUJS SKAMW ZJXZW WXJZB TNMWO YIBKA
KJAXS SRLAN VJSLV CCJYZ MWDNK SACEH NVQBS WGZBA SYNLU N
```

Saurez-vous le déchiffrer ? Expliquez vos hypothèses de travail et votre façon de procéder.

Solution :
Nous allons supposer que le message clair est signé Tritheme et que la clef a une longueur inférieure ou égale à 8. Nous isolons les 8 derniers caractères `BASYNLUN` et nous examinons le décalage avec `TRITHEME` :

Caractères	Positions dans l'alphabet							
BASYNLUN	1	0	18	24	13	11	20	13
- TRITHEME	- 19	17	8	19	7	4	12	4
Décalage modulo 26	8	9	10	5	6	7	8	9

On en déduit donc que le texte est écrit sur $10 - 5 + 1 = 6$ colonnes avec un décalage de départ de 5 , autrement dit une clef de Vigenère de la forme `FGHIJK` et le texte clair est

```
Une seule feuille te suffira
À la main et en personne tu l'écriras
Avec soin les éléments essentiels tu choisiras
(Tritheme)
```

Remarque : ce message a été évidemment fabriqué pour les besoins de ce cours, mais l'idée en a été inspirée par les écrits de Tritheme de défense des manuscrits par rapport aux ouvrages imprimés.

Exercice 3 – Structures algébriques – 5,5 points

On considère les sous-ensembles suivants de $\mathbb{R}^{2\times 2}$:

$$\mathcal{A} = \left\{ \begin{pmatrix} a & b \\ b & -a \end{pmatrix},\ (a,b) \in \mathbb{R}^2 \right\}, \quad \mathcal{B} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix},\ (a,b) \in \mathbb{R}^2 \right\}, \quad \mathcal{C} = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix},\ (a,b) \in \mathbb{R}^2 \right\}.$$

De plus, on note $\mathcal{A}^*$ (resp. $\mathcal{B}^*$, resp. $\mathcal{C}^*$) l'ensemble $\mathcal{A}$ (resp. $\mathcal{B}$, resp. $\mathcal{C}$) privé de la matrice nulle.

1. a. $\mathcal{A}$ est-il un groupe pour l'addition ? Si oui, le prouver. Sinon, le justifier.
   b. $\mathcal{A}^*$ est-il un groupe pour la multiplication ? Si oui, le prouver. Sinon, le justifier.
   c. $\mathcal{A}$ est-il un anneau ? Si oui, le prouver. Sinon, le justifier.
   d. $\mathcal{A}$ est-il un corps ? Si oui, le prouver. Sinon, le justifier.
2. Mêmes questions pour $\mathcal{B}$.
3. Mêmes questions pour $\mathcal{C}$.

Solution :

1. On note $M_{a,b} = \left(\begin{smallmatrix} a & b \\ b & -a \end{smallmatrix}\right)$.
   a. Clairement la matrice nulle est dedans, la somme de $M_{a,b}$ et de $M_{c,d}$ est $M_{a+c,b+d}$ et l'opposée de $M_{a,b}$ est $M_{-a,-b}$. L'associativité de la somme découle directement de celle des matrices dans $\mathbb{R}^{2\times 2}$. *En cas de démonstration de l'associativité* . Donc $\mathcal{A}$ est un groupe (et même un espace vectoriel).
   b. On remarque que $M_{1,0}^2$ est la matrice identité qui n'est pas dans $\mathcal{A}$! Donc $\mathcal{A}^*$ n'est pas un groupe.
   c. Comme à la question précédente, $\mathcal{A}$ n'est pas stable par multiplication donc ce n'est pas un anneau.
   d. Comme $\mathcal{A}$ n'est pas un anneau, il ne peut pas être un corps non plus.
2. On note $N_{a,b} = \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$.

a. Clairement la matrice nulle est dedans, la somme de $N_{a,b}$ et de $N_{c,d}$ est $N_{a+c,b+d}$ et l'opposée de $N_{a,b}$ est $N_{-a,-b}$. L'associativité de la somme découle directement de celle des matrices dans $\mathbb{R}^{2\times 2}$. Donc $\mathcal{B}$ est un groupe (et même un espace vectoriel).

b. Clairement la matrice identité est dedans, le produit de $N_{a,b}$ et de $N_{c,d}$ est $N_{ac-bd,ad+bc}$ et l'inverse de $N_{a,b}$ est $N_{\frac{a}{a^2+b^2},-\frac{b}{a^2+b^2}}$ avec $a^2+b^2 \neq 0$ pour $(a,b) \neq (0,0)$. L'associativité du produit découle directement de celle des matrices dans $\mathbb{R}^{2\times 2}$. Donc $\mathcal{B}^*$ est un groupe.

c. $\mathcal{B}$ est un groupe pour l'addition et $\mathcal{B}$ est stable par multiplication. La distributivité du produit par rapport à la somme découle directement de celle des matrices dans $\mathbb{R}^{2\times 2}$.*En cas de démonstration de la distributivité* . Donc $\mathcal{B}$ est un anneau (et même une algèbre).

d. $\mathcal{B}$ est un anneau et $\mathcal{B}^*$ est un groupe. Donc $\mathcal{B}$ est un corps.

3. On note $P_{a,b} = \left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right)$.

a. Clairement la matrice nulle est dedans, la somme de $P_{a,b}$ et de $P_{c,d}$ est $P_{a+c,b+d}$ et l'opposée de $P_{a,b}$ est $P_{-a,-b}$. L'associativité de la somme découle directement de celle des matrices dans $\mathbb{R}^{2\times 2}$. Donc $\mathcal{C}$ est un groupe (et même un espace vectoriel).

b. Clairement la matrice $P_{1,1}$ n'y a pas d'inverse. Donc $\mathcal{C}^*$ n'est pas un groupe.

c. $\mathcal{C}$ est un groupe pour l'addition et le produit de $P_{a,b}$ et de $P_{c,d}$ est $P_{ac+bd,ad+bc}$. L'associativité du produit et la distributivité du produit par rapport à la somme découle directement de celles des matrices dans $\mathbb{R}^{2\times 2}$. Donc $\mathcal{C}$ est un anneau (et même une algèbre).

d. $\mathcal{C}^*$ n'est pas un groupe. Donc $\mathcal{C}$ n'est pas un corps.