**4MA035**
Master de mathématiques
Année académique 2023-2024

SCIENCES SORBONNE UNIVERSITÉ

# Partiel du 21 mars

**Corrigé**

**Exercice 1 (facultatif)** – Soit $f \in \mathbb{Z}[X]$ un polynôme tel que tous ses coefficients soient des entiers naturels.

1. Montrer que pour tout entier $n > f(1)$, le polynôme $f$ est univoquement déterminé par l'entier $f(n)$.

   En posant $f = a_0 + a_1 X + \cdots + a_d X^d$, avec $a_0, \ldots, a_d \in \mathbb{N}$, on a les relations
   $$f(1) = a_0 + \cdots + a_d \geq \max\{a_0, \ldots, a_d\},$$
   ce qui implique que
   $$f(n) = a_0 + a_1 n + \cdots + a_d n^d,$$
   est l'écriture en base $n$ de $f(n)$, car $0 \leq a_0, \ldots, a_d < n$. L'unicité d'une telle écriture permet de conclure.

2. Déterminer $f$ en sachant que $f(1) = 8$ et $f(17) = 2024$.

   On a l'inégalité stricte $17 > f(1)$, ce qui implique que le polynôme $f$ est univoquement déterminé par l'écriture en base 17 de 2024. Un simple calcul donne $2024 = 7 \cdot 17^2 + 1$, d'où $f = 7X^2 + 1$.

**Exercice 2**– Lors d'un protocole RSA, Alice transmet la clé publique $(9, n)$. Elle reçoit le cryptogramme 29, le déchiffre, et obtient le message initial 2.

1. Déterminer l'entier $n$.

   Par définition, l'entier $n$ est le produit de deux nombres premiers distincts et divise
   $$2^9 - 29 = 483 = 3 \cdot 7 \cdot 23.$$
   On a donc $n \in \{21, 69, 161\}$. De plus, l'entier 9 est premier avec $\varphi(n)$, ce qui donne nécessairement $n = 69$.

2. En déduire la clé secrète d'Alice ainsi que toutes les clés de déchiffrement.

   La clé secrète $d$ d'Alice est l'inverse de 9 modulo $\varphi(69) = 44$, d'où $d = 5$.

3. Bob transmet le cryptogramme 67. Déterminer le message initial.

On a les congruences
$$67^5 \equiv (-2)^5 \equiv -32 \equiv 37 \pmod{69},$$
ce qui implique que le message initial est égal à 37.

**Exercice 3** – Afin de communiquer de manière confidentielle, Alice utilise le cryptosystème de Rabin. Voulant envoyer le message 22, Bob transmet le cryptogramme 1. Par ailleurs, Charlotte transmet le cryptogramme 2.

1. Déterminer la clé publique $n$ d'Alice ainsi que sa privée $(p, q)$.

Par définition, on a la congruence
$$22^2 \equiv 1 \pmod{n},$$
ce qui implique que l'entier $n = pq$ divise
$$22^2 - 1 = 483 = 3 \cdot 7 \cdot 23,$$
d'où $n \in \{21, 69, 161\}$. Par ailleurs, l'élément 2 est un carré dans $\mathbb{Z}/n\mathbb{Z}$, ce qui implique que c'est un carré dans $\mathbb{F}_p$ et dans $\mathbb{F}_q$. L'élément 2 n'étant pas un carré dans $\mathbb{F}_3$, on a nécessairement $n = 161$ et la clé privée d'Alice est alors égale à $(7, 23)$.

2. Déterminer les quatre possibilités pour le message envoyé par Charlotte.

On doit résoudre la congruence
$$x^2 \equiv 2 \pmod{161}.$$
Le théorème des restes chinois affirme que celle-ci est équivalente au système de congruences
$$\begin{cases} x^2 \equiv 2 \pmod{7}, \\ x^2 \equiv 2 \pmod{23}. \end{cases}$$
On est donc ramené à déterminer les racines carrées de 2 dans $\mathbb{F}_7$ et dans $\mathbb{F}_{23}$. Le nombre premier 7 étant congru à 3 modulo 4, une racine carrée de 2 dans $\mathbb{F}_7$ est égale à $2^{\frac{7+1}{4}} = 4$, la seconde est alors égale à $-4$. De même, les éléments $2^{\frac{23+1}{4}} = 2^6 = 64 = 18$ et $-18$ sont les racines carrées de 2 dans $\mathbb{F}_{23}$. En remarquant que l'entier 4 est congru à 18 modulo 7, le système de congruences ci-dessus se traduit alors par les quatre systèmes
$$\begin{cases} x \equiv \pm 18 \pmod{7}, \\ x \equiv \pm 18 \pmod{23} \end{cases}$$
En utilisant l'identité de Bézout $10 \cdot 7 - 3 \cdot 23 = 1$, on obtient les solutions $x \equiv \pm 18 \pmod{161}$ et
$$x \equiv \pm 18(10 \cdot 7 + 3 \cdot 23) \equiv \pm 87 \pmod{161}.$$

3. Afin de recevoir la valeur d'un bit, Alice utilise protocole de Goldwasser-Micali et transmet la clé publique $(x, n)$. Justifier le fait que 6 n'est pas un cryptogramme et déchiffrer le cryptogramme 5.

Si un élément $x \in \mathbb{Z}/161\mathbb{Z}$ est un cryptogramme alors on a l'identité $\left(\frac{x}{7}\right) = \left(\frac{x}{23}\right)$ et le bit envoyé est égal à 1 si et seulement si $\left(\frac{x}{7}\right) = -1$. En utilisant le théorème d'Euler, on obtient facilement les relations $\left(\frac{6}{7}\right) = -1$ et $\left(\frac{6}{23}\right) = 1$, ce qui implique que 6 n'est pas un cryptogramme.

Afin de déchiffrer le cryptogramme 5, il suffit de déterminer le symbole de Legendre $\left(\frac{5}{7}\right)$. En appliquant une fois de plus le théorème d'Euler, on en déduit les congruences

$$\left(\frac{5}{7}\right) \equiv 5^{\frac{7-1}{2}} \equiv 5^3 \equiv (-2)^3 \equiv -8 \equiv -1 \pmod 7,$$

d'où $\left(\frac{5}{7}\right) = -1$. Le bit envoyé est donc égal à 1.

**Exercice 4**

1. Soit $K$ un corps et notons $p$ sa caractéristique. On suppose que le polynôme $f = X^2 + X + 1$ possède une racine $x \in K$. Montrer que pour $p \neq 3$, l'élément $x$ est d'ordre 3 dans $K^\times$ et que pour $p = 3$, on a $x = 1$.

L'élément $x$ est également racine du polynôme $X^3 - 1 = (X-1)f$, ce qui implique que $x$ est d'ordre divisant 3. Si $x$ est d'ordre 1, ce qui se traduit par $x = 1$, on a $f(1) = 3 = 0$, d'où $p = 3$. En particulier, pour $p \neq 3$, l'élément $x$ est d'ordre 3. Réciproquement, pour $p = 3$, on a l'identité

$$X^2 + X + 1 = X^2 - 2X + 1 = (X-1)^2$$

dans $\mathbb{F}_3[X]$, ce qui implique que 1 est l'unique racine de $f$ dans $K$.

2. En déduire que $f$ est irréductible dans $\mathbb{F}_p[X]$ si et seulement si $p = 2$ ou $p$ est congru à 5 modulo 6.

On rappelle qu'un polynôme de degré 2 est irréductible dans $\mathbb{F}_p[X]$ si et seulement s'il ne possède pas de racine dans $\mathbb{F}_p$. Pour $p = 2$, on a $f(0) = f(1) = 1$, ce qui implique que $f$ est irréductible dans $\mathbb{F}_2[X]$. Si $p$ est congru à 5 modulo 6, alors $p - 1$ n'est pas divisible par 3. Le groupe $\mathbb{F}_p^\times$ étant d'ordre $p - 1$, le théorème de Lagrange implique alors qu'il ne possède pas d'élément d'ordre 3. D'après le point précédent, le polynôme $f$ ne possède aucune racine dans $\mathbb{F}_p$, ce qui implique qu'il est irréductible dans $\mathbb{F}_p[X]$. Réciproquement, si $p \neq 2$ n'est pas congru à 5 modulo 6, on a $p = 3$ ou $p \equiv 1 \pmod 6$. Dans le premier cas, 1 est une racine de $f$. Dans le second, le théorème de Cauchy affirme que $\mathbb{F}_p^\times$ possède un élément $x$ d'ordre 3 (car son ordre est divisible par 3), d'où les identités

$$0 = x^3 - 1 = (x-1)f(x)$$

et, par suite, $f(x) = 0$ (car $x \neq 1$ et $\mathbb{F}_p$ est intègre). Dans les deux cas, le polynôme $f$ possède une racine dans $\mathbb{F}_p$, ce qui implique qu'il est réductible dans $\mathbb{F}_p[X]$.

3. Justifier le fait que l'anneau $L = \mathbb{F}_5[X]/(f)$ est un corps fini. Quel est son cardinal ? Quels sont les ordres possibles des éléments de $L^\times$ ?

L'anneau $\mathbb{F}_5[X]$ étant principal, l'idéal engendré par un polynôme irréductible $g \in \mathbb{F}_5[X]$ est maximal, ce qui traduit le fait que l'anneau quotient $\mathbb{F}_5[X]/(g)$ est un corps. Dans le cas présent, le point précédent affirme que $f$ est irréductible dans $\mathbb{F}_5[X]$, ce qui implique que $L$ est un corps. L'extension $L/K$ étant de degré $\deg(f) = 2$, on en déduit que $L$ est de cardinal $5^2 = 25$. Finalement, le groupe $L^\times$ est cyclique d'ordre 24, ce qui implique que les ordres possibles de ses éléments sont $1, 2, 3, 4, 6, 8, 12$ et 24.

4. Notons $\alpha \in L$ la classe de $X$. Vérifier que l'élément $\beta = 1 + 2\alpha$ est une racine carrée de 2 dans $L$.

Par construction, $\alpha$ est une racine de $f$ dans $L$, qui est un corps de caractéristique 5 d'où les identités

$$\beta^2 = (1+2\alpha)^2 = 1 + 4\alpha + 4\alpha^2 = 1 - \alpha - \alpha^2 = 2 - 1 - \alpha - \alpha^2 = 2 - f(\alpha) = 2.$$

5. Déterminer les ordres respectifs de $\alpha$ et $\beta$. En déduire que l'élément $\gamma = \alpha\beta$ est un générateur de $L^\times$ et expliciter ses coordonnées dans la $\mathbb{F}_5$-base $(1, \alpha)$ de $L$.

L'élément $\alpha$ étant une racine de $f$ dans $L$, qui est de caractéristique 5, le premier point de l'exercice affirme que son ordre dans $L^\times$ est égal à 3. L'élément 2 est d'ordre 4 et engendre le sous-groupe $\mathbb{F}_5^\times$ de $L^\times$. L'identité $\beta^2 = 2$ implique que $\beta$ est d'ordre divisant 8. Si son ordre divisait 4, on aurait $\beta \in \mathbb{F}_5^\times$ (car le groupe $L^\times$, qui est cyclique d'ordre 24, possède un unique sous-groupe d'ordre 4, qui coïncide avec $\mathbb{F}_5^\times$), ce qui est exclu. On en déduit que $\beta$ est d'ordre 8 dans $L^\times$. Les entiers 3 et 8 étant premiers entre eux et le groupe $L^\times$ étant abélien, leur produit est d'ordre $3 \cdot 8 = 24$ et engendre donc $L^\times$. D'un point de vue explicite, on a les identités

$$\gamma = \alpha\beta = \alpha(1 + 2\alpha) = \alpha + 2\alpha^2 = \alpha - 2(1 + \alpha) = -2 - \alpha.$$

Les coordonnées de $\gamma$ dans la base $(1, \alpha)$ sont donc $(-2, -1)$.

6. Déterminer les logarithmes discrets $\log_\gamma(\alpha)$ et $\log_\gamma(\beta)$.

Les éléments $\alpha$ et $\beta$ étant d'ordres respectifs 3 et 8 dans $L^\times$, on a les relations $\gamma^9 = \alpha^9\beta^9 = \beta$, d'où l'identité $\log_\gamma(\beta) = 9$. De même, on a $\gamma^{16} = \alpha^{16}\gamma^{16} = \alpha$, d'où $\log_\gamma(\alpha) = 16$. Cette dernière identité aurait pu être également déduite par la relation $\gamma = \alpha\beta$, qui se traduit par l'identité $1 = \log_\gamma(\alpha) + \log_\gamma(\beta)$.

7. Alice utilise le cryptosystème El Gamal et transmet la clé publique $(L^\times, \gamma, 3\alpha)$. Déterminer sa clé privée.

Par définition, la clé privée d'Alice est le logarithme discret de $3\alpha$ en base $\gamma$. En tenant compte des identités $3 = 2^3 = \beta^6$ dans $L$ et des expressions de $\log_\gamma(\alpha)$ et $\log_\gamma(\beta)$ obtenues dans le point précédent, on en déduit les relations

$$\log_\gamma(3\alpha) = \log_\gamma(3) + \log_\gamma(\alpha) = \log_\gamma(\beta^6) + 16 = 6\log(\beta) + 16 = 6 \cdot 9 + 16 = 70 = 22$$

dans $\mathbb{Z}/24\mathbb{Z}$.