Sorbonne Université
Cryptologie, cryptographie algébrique
4M035 - 2021/22 - Enseignement à distance
Alain Kraus

Correction du premier devoir

Exercice 1

1) Le polynôme $X^2+X+1 \in \mathbb{F}_5[X]$ n'a pas de racines dans $\mathbb{F}_5$ et il est de degré 2, donc il est irréductible sur $\mathbb{F}_5$. Le cardinal de K est donc égal à 25.

2) On a $\alpha^2 = -\alpha - 1$, d'où les égalités $\alpha^3 = -\alpha^2 - \alpha = 1$. Par suite, α est d'ordre 3. Par ailleurs, on a $(1+2\alpha)^2 = 1 + 4\alpha^2 + 4\alpha$, d'où l'égalité $(1+2\alpha)^2 = 2$. On a ainsi $(1+2\alpha)^4 = -1$, ce qui entraîne que $1+2\alpha$ est d'ordre 8 dans K^*.

3) On a l'égalité
$$\alpha(1+2\alpha) = 3+4\alpha.$$
D'après la question précédente, $3+4\alpha$ est donc d'ordre 24, d'où le résultat.

4) On vérifie que l'on a $(3+4\alpha)^3 = 2+4\alpha$, d'où $a=3$.

5) Soit m le message décrypté. Avec les notations du cours, on a
$$g = 3+4\alpha, \quad g^x = 1+\alpha \quad \text{et} \quad mg^{ax} = t.$$
On a $a=3$, d'où
$$m = t(1+\alpha)^{-3}.$$
Par ailleurs, on a $\alpha^2+\alpha+1=0$ i.e. $\alpha(1+\alpha) = -1$, d'où $(1+\alpha)^{-1} = -\alpha$. D'après la question 2, on a $\alpha^3 = 1$. On obtient $m = -t$.

Exercice 2

1) On a les égalités $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$, $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$ et $\left(\frac{-2}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{2}{n}\right)$. Par ailleurs, on a $\alpha_n = 2^{\frac{n}{2}} e^{\frac{n\pi i}{4}} - 1$. En examinant les congruences de n modulo 8, on vérifie que
$$\cos\left(\frac{n\pi i}{4}\right) = \left(\frac{2}{n}\right)\frac{1}{\sqrt{2}} \quad \text{et} \quad \sin\left(\frac{n\pi i}{4}\right) = \left(\frac{-2}{n}\right)\frac{1}{\sqrt{2}},$$
d'où l'égalité annoncée.

2) C'est une conséquence directe de la question 1.

3.1) Par hypothèse, il existe $k \in \mathbb{Z}$ tel que $b = ka$. On a les égalités
$$\alpha_b = \big((1+i)^a\big)^k - 1 = \alpha_a u \quad \text{où} \quad u = \sum_{s=0}^{k-1} (1+i)^{as} \in \mathbb{Z}[i],$$

donc α_a divise α_b dans $\mathbb{Z}[i]$. On a ainsi $M_b = M_a|u|^2$, d'où l'assertion.

3.2) Supposons $b = 1$. On a $M_b = 1$. Vu que $a > 1$ est impair, on a $a \geq 3$. Il résulte de la question 2 que l'on a $M_a > 1$, d'où le résultat dans ce cas.
Supposons $b \geq 3$. On a les inégalités

$$M_a \geq 2^{\frac{a+1}{2}}\big(2^{\frac{a-1}{2}} - 1\big) + 1 \quad \text{et} \quad 2^{\frac{b+1}{2}}\big(2^{\frac{b-1}{2}} + 1\big) + 1 \geq M_b.$$

Tout revient ainsi à vérifier que l'on a

$$2^{\frac{a-1}{2}} - 1 \geq 2^{\frac{b-1}{2}} + 1. \tag{1}$$

Parce que a et b sont impairs, on a $a \geq b+2$. On a donc $2^{\frac{a-1}{2}} \geq 2.2^{\frac{b-1}{2}}$. On a $b \geq 3$, d'où $\frac{b-1}{2} \geq 1$ puis $2.2^{\frac{b-1}{2}} \geq 2^{\frac{b-1}{2}} + 2$ et l'inégalité (1).

4) Supposons n non premier. Il existe un entier impair $a \geq 3$ divisant n et distinct de n. D'après la question 3, M_a divise M_n et $M_n > M_a$. Par ailleurs, on a $M_a > 1$ donc M_n n'est pas premier, d'où l'assertion.

5) D'après la question 2, on a

$$M_p = \begin{cases} 2^p + 2^{\frac{p+1}{2}} + 1 & \text{si } \ p \equiv 3 \text{ mod. } 8 \\ 2^p - 2^{\frac{p+1}{2}} + 1 & \text{si } \ p \equiv 7 \text{ mod. } 8. \end{cases}$$

Supposons $p \equiv 3$ mod. 8. On a $2^p \equiv 3$ mod. 5 et $2^{\frac{p+1}{2}} \equiv 4$ mod. 5. Par suite, on a $M_p \equiv 3$ mod. 5. D'après la loi de réciprocité quadratique on a donc

$$\left(\frac{5}{M_p}\right) = \left(\frac{M_p}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

De même, si $p \equiv 7$ mod. 8, on a $2^p \equiv 3$ mod. 5 et $2^{\frac{p+1}{2}} \equiv 1$ mod. 5. On obtient de nouveau $M_p \equiv 3$ mod. 5 puis $\left(\frac{5}{M_p}\right) = -1$.

6) D'après la question 2, on a

$$M_p = 2^{\frac{p+1}{2}}\left(2^{\frac{p-1}{2}} - \left(\frac{2}{p}\right)\right) + 1.$$

Posons $h = 2^{\frac{p-1}{2}} - \left(\frac{2}{p}\right)$. On a $h < 2^{\frac{p+1}{2}}$. Compte tenu de la question précedente, le critère de primalité de Proth (corollaire 2.4 du cours), utilisé avec $a = 5$ et $N = \frac{p+1}{2}$, entraîne alors l'équivalence annoncée.

7) On vérifie avec un logiciel de calcul que l'ensemble des nombres premiers $p \equiv 3$ mod. 4 plus petits que 100 pour lesquels M_p est premier est

$$\big\{3, 7, 11, 19, 47, 79\big\}.$$