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

Premier devoir

À rendre pour le lundi 21 mars

Exercice 1

Soit f le polynôme X^2+X+1 dans $\mathbb{F}_5[X]$. Considérons l'anneau quotient

$$K=\mathbb{F}_5[X]/(f).$$

1) Montrer que K est un corps. Quel est son cardinal ?

Soit α la classe de X modulo l'idéal (f).

2) Quels sont les ordres de α et de $1+2\alpha$ dans K^* ?
3) En déduire que $3+4\alpha$ est un générateur de K^*.

Une personne Alice utilise l'algorithme de El Gamal afin de permettre à quiconque de lui envoyer des messages confidentiels. Pour cela, elle publie le triplet

$$(K, 3+4\alpha, 2+4\alpha).$$

4) Quel est le plus petit entier $a\geq 1$ tel que $(3+4\alpha)^a=2+4\alpha$?
5) Alice reçoit le couple $(1+\alpha, t)$ où $t\in K^*$. Quel est le message décrypté ?

Exercice 2

Cet exercice concerne l'analogue des nombres de Mersenne dans l'anneau $\mathbb{Z}[i]$ formé des nombres complexes $a+ib$ où $a,b\in\mathbb{Z}$.

Soit $n\geq 1$ un entier impair. Posons dans $\mathbb{Z}[i]$

$$\alpha_n=(1+i)^n-1.$$

1) Montrer que l'on a

$$\alpha_n=\Big(\frac{2}{n}\Big)2^{\frac{n-1}{2}}-1+i\Big(\frac{-2}{n}\Big)2^{\frac{n-1}{2}},$$

où $\big(\frac{2}{n}\big)$ et $\big(\frac{-2}{n}\big)$ désignent les symboles de Jacobi.

Indication : Utiliser l'égalité $1+i=\sqrt{2}e^{\frac{\pi i}{4}}$.

Soit $|\alpha_n|$ le module de α_n. Posons

$$M_n = |\alpha_n|^2.$$

2) En déduire que l'on a

$$M_n = 2^n - \Big(\frac{2}{n}\Big) 2^{\frac{n+1}{2}} + 1.$$

3) Soient a et b des entiers naturels impairs.

3.1) Supposons que a divise b. Montrer que α_a divise α_b dans $\mathbb{Z}[i]$. En déduire que M_a divise M_b.

3.2) Supposons $a > b$. Montrer que l'on a $M_a > M_b$.

4) En déduire que si M_n est premier, alors n est premier.

Soit p un nombre premier congru à 3 modulo 4.

5) Supposons M_p premier. Calculer le symbole de Legendre $\big(\frac{5}{M_p}\big)$.

6) En utilisant un résultat du cours que l'on précisera, en déduire l'équivalence

$$M_p \text{ est premier } \iff 5^{\frac{M_p-1}{2}} \equiv -1 \text{ mod. } M_p.$$

7) Si vous disposez d'un logiciel de calcul, établir la liste des nombres premiers $p < 100$ congrus à 3 modulo 4, pour lesquels M_p est premier.

Remarque. Si p est nombre premier congru à 1 modulo 4, on peut démontrer, mais c'est plus difficile, que l'on a l'équivalence

$$M_p \text{ est premier } \iff 5^{\frac{M_p-1}{4}} \equiv -1 \text{ mod. } M_p.$$
