123 – Corps finis. Applications.

2013 – 2014

Question.

Utiliser l'algorithme de Berlekamp pour factoriser X^4+1 sur $\mathbb{F}_7$.

Réponse.

On pose $P := X^4+1$, alors $P'(X) = 4X^3$ donc $P \wedge P' = 1$, donc P est sans facteur carré.

En notant

$$\begin{aligned} S_p : \mathbb{F}_7[X]/(P) &\longrightarrow \mathbb{F}_7[X]/(P) \\ Q(X) &\longmapsto Q(X^7), \end{aligned}$$

on doit calculer la matrice de $S_p - \mathrm{id}$ dans la base $(1, X, X^2, X^3)$. On obtient

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & -1 \\ 0 & 0 & -2 & 0 \\ 0 & -1 & 0 & -1 \end{pmatrix}.$$

Le noyau de cette matrice est engendré par 1 et $X^3 - X$.

On calcule maintenant le pgcd de $X^3 - X - 3$ avec P. On trouve X^2+3X+1, ce qui constitue un des facteurs de P, on trouve l'autre en divisant P par X^2+3X+1. On obtient

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

Question.

Est-ce que $2+\sqrt{3}$ est un carré de $\mathbb{F}_{49}$?

Réponse.

On regarde d'abord si $\sqrt{3} \in \mathbb{F}_7$.

$$\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

Donc $\sqrt{3} \notin \mathbb{F}_7$. On calcule alors la norme de $2+\sqrt{3}$:

$$N(2+\sqrt{3}) = 2^2 - 3 = 1,$$

qui est bien un carré de $\mathbb{F}^7$. Donc $2+\sqrt{3}$ est un carré de $\mathbb{F}_{49}$.

Question.

Trouver un générateur de $\mathbb{F}_8$.

Réponse.

$\mathbb{F}_8^\times$ est d'ordre 7 donc tout élément différent de 0 et 1 est générateur.

Question

Soit N un nombre de Fermat : $N = 2^{2^n}+1$, avec $n \geq 2$. Montrer que 5 n'est pas un carré modulo N lorsque N est premier.

Réponse.

$$\left(\frac{5}{N}\right) = \left(\frac{N}{5}\right) = \left(\frac{(-1)^{2^{n-1}}+1}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

Question

Que vaut 5^{N-1} mod N lorsque N est premier ? Et $5^{\frac{N-1}{2}}$ mod N ?

Réponse.

D'après le théorème de Fermat, $5^{N-1} \equiv 1[N]$ lorsque N est premier. De plus, puisque 5 n'est pas un carré modulo N, $5^{\frac{N-1}{2}} \equiv -1[N]$.

Question.

On suppose seulement que $5^{\frac{N-1}{2}} \equiv -1[N]$. En considérant un diviseur premier p de N, montrer que N est premier.

Réponse.

On regarde l'ordre de 5 dans $\mathbb{F}_p$. On a $5^{N-1} \equiv 1[p]$, donc l'ordre de 5 divise $N-1 = 2^{2^n}$, donc est une puissance de 2. Or $5^{\frac{N-1}{2}} \equiv -1[p]$ donc 5 est d'ordre $N-1$. Or $5^{p-1} \equiv 1[p]$ par le théorème de Fermat, donc $N-1 \mid p-1$, donc $N = p$ et N est premier.

Question.

On considère θ un générateur de $\mathbb{F}_{p^2}^\times$, quel est l'ordre de θ dans $\mathbb{F}_{p^2}^\times/\mathbb{F}_p^\times$?

Réponse.

L'ordre de $\mathbb{F}_{p^2}^\times/\mathbb{F}_p^\times$ est $\frac{p^2-1}{p-1} = p+1$, donc l'ordre de θ est $p+1$ car θ engendre le quotient.

Question.

Soit $x \in \mathbb{F}_{p^2}$, étudier les zéros de la suite $u_n := x^n - \mathcal{F}(x^n)$, où $\mathcal{F}$ est le Frobenius.

Réponse.

$u_n = 0$ lorsque $x^n \in \mathbb{F}_p$. Pour $x \in \mathbb{F}_p$, alors $u_n = 0$ pour tout n.

Réciproquement, si $u_n = 0$ pour tout n, alors en particulier $x = \mathcal{F}(x)$ donc $x \in \mathbb{F}_p$.

On pose $x := \theta$, alors $u_n = 0$ si et seulement si $\theta^n \in \mathbb{F}_p$, c'est-à-dire si et seulement si $p+1$ divise n par la question précédente.