

FICHE N°8 :

**Exercice 1.** Montrer que le théorème de Wilson implique d'une racine de  $-1 \pmod p$  si  $p$  est congru à 1 mod 4. *Indication: Poser  $X := 1 \cdot 2 \cdots \frac{p-1}{2}$  et montrer  $X^2 \equiv -1[p]$ .*

**Exercice 2.** Combien y a-t-il de cubes dans  $(\mathbb{Z}/p\mathbb{Z})^\times$  ?

**Exercice 3.** Montrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.

**Exercice 4.** Ici, on travaille sur  $\mathbb{F}_3$ .

1. Décomposer  $\Phi_7$ .
2. Déterminer le corps  $\mathbb{F}_3(\alpha)$  où  $\alpha$  est une 7ième racine d'unité.

**Exercice 5.** Montrer que le polynôme  $X^2 + X + 1$  est irréductible dans  $\mathbb{F}_8$ .

**Exercice 6.**

1. Montrer que le polynôme  $X^3 + X + 1$  est irréductible sur  $\mathbb{F}_{16}$ . Soit  $x$  une racine du polynôme.
2. En considérant  $\mathbb{F}_2 \subset \mathbb{F}_2(x) \subset \mathbb{F}_{16}(x)$ , montrer que 3 divise  $[\mathbb{F}_{16}(x) : \mathbb{F}_2]$ .
3. En considérant  $\mathbb{F}_2 \subset \mathbb{F}_{16} \subset \mathbb{F}_{16}(x)$ , montrer que 4 divise  $[\mathbb{F}_{16}(x) : \mathbb{F}_2]$  et que  $[\mathbb{F}_{16}(x) : \mathbb{F}_2] \leq 12$ .
4. En déduire que  $[\mathbb{F}_{16}(x) : \mathbb{F}_2] = 12$ .

**Exercice 7.** Soient  $K$  un corps commutatif,  $P$  un polynôme irréductible de degré  $n > 1$  et  $L$  le corps de décomposition de  $P$ . Montrer que  $[L : K] \leq n!$ .

**Exercice 8.** Montrer que  $GL_n(\mathbb{F}_{p^2})$  est isomorphe à un sous-groupe de  $GL_{2n}(\mathbb{F}_p)$ .

**Exercice 9.** Soit  $f : \mathbb{F}_q^n \rightarrow \mathbb{F}_q$  une forme quadratique non triviale. Montrer que si  $n$  est au moins 3, alors le cône isotrope  $N(f) := \{x \in \mathbb{F}_q^n \mid f(x) = 0\}$  a au moins un point non trivial, i.e.,  $N(f) \setminus \{0\} \neq \emptyset$ .

**Exercice 10.** Soit  $p$  un nombre premier. Montrer que, parmi  $2p - 1$  entiers, on peut toujours en trouver  $p$  dont la somme est divisible par  $p$ . *Indication: On appelle  $a_1, \dots, a_{2p-1}$  les entiers modulo  $p$ . Considérer le polynôme  $(X_1^{p-1} + \dots + X_{2p-1}^{p-1})^2 - \omega(a_1 X_1^{p-1} + \dots + a_{2p-1} X_{2p-1}^{p-1})^2$ , où  $\omega \in \mathbb{F}_p$  n'est pas un carré.*

**Exercice 11.** Soit  $p, q$  deux nombres premiers distincts  $> 2$ . Le but de cet exercice est de montrer la loi de réciprocité quadratique de Gauss:

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

Soit  $\zeta$  une racine primitive  $q$ -ième d'unité dans une clôture algébrique de  $\mathbb{F}_p$ . On pose

$$\tau := \sum_{x \in \mathbb{F}_q^*} \left(\frac{x}{q}\right) \zeta^x.$$

Cette somme est appelée la *somme de Gauss*.

1. Montrer que

$$\tau^2 = \sum_{u \in \mathbb{F}_q} \zeta^u \left( \sum_{t \in \mathbb{F}_q} \left( \frac{t(u-t)}{q} \right) \right).$$

2. Montrer que, si  $t \neq 0$ , on a

$$\left( \frac{t(u-t)}{q} \right) = (-1)^{\frac{q-1}{2}} \left( \frac{1-ut^{-1}}{q} \right).$$

3. Poser  $C_u := \sum_{t \in \mathbb{F}_q^*} \left( \frac{1-ut^{-1}}{q} \right)$ .

(a) Montrer que  $C_0 = q-1$  et que  $C_u = -1$  pour  $u \neq 0$ .

(b) En déduire que  $\tau^2 = (-1)^{\frac{q-1}{2}} q$ .

(c) Montrer que

$$\tau^{p-1} = (\tau^2)^{\frac{p-1}{2}} = \left( \frac{q}{p} \right) (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

4. Par la définition de  $\tau$ , calculer  $\tau^p$ . En déduire que  $\tau^{p-1} = \left( \frac{p}{q} \right)$ .

5. Conclure.

On remarque que la somme de Gauss est un analogue de la fonction gamma :

$$\Gamma(s) := \int_0^\infty e^{-x} x^s \frac{dx}{x} \quad \text{Re } s > 0.$$

Il y a aussi un analogue de la fonction bêta appelé la *somme de Jacobi*.

**Exercice 12.** Soit  $p$  un nombre premier  $> 2$  et  $\zeta$  une racine primitive  $p$ -ème d'unité dans  $\mathbb{C}^\times$ . Pour  $a \in \mathbb{F}_p$ , posons

$$\tau_a := \sum_{x \in \mathbb{F}_p^\times} \left( \frac{x}{p} \right) \zeta^{ax}.$$

Cette somme est aussi appelée la *somme de Gauss*. En particulier, on pose  $\tau = \tau_1$ .

1. Montrer que  $\tau_a = \left( \frac{a}{p} \right) \tau$  pour  $a \in \mathbb{F}_p$ .

2. On pose  $S := \sum_{a \in \mathbb{F}_p} \tau_a \tau_{-a}$ .

(a) Montrer que  $\tau_a \tau_{-a} = (-1)^{\frac{p-1}{2}} \tau^2$  pour  $a \in \mathbb{F}_p^\times$ . En déduire que  $S = (-1)^{\frac{p-1}{2}} (p-1) \tau^2$ .

(b) Avec l'aide du caractère de  $\mathbb{F}_p^\times$ , vérifier que  $\sum_{a \in \mathbb{F}_p} \zeta^{a(x-y)} = p \delta_{x,y}$ .

En déduire que  $S = p \sum_{x \in \mathbb{F}_p} \left( \frac{x}{p} \right)^2 = p(p-1)$ .

(c) En déduire que  $\tau_a^2 = \tau^2 = (-1)^{\frac{p-1}{2}} p$  si  $a \in \mathbb{F}_p^\times$ .

3. En déduire que toute extension quadratique de  $\mathbb{Q}$  (i.e., de la forme  $\mathbb{Q}(\sqrt{d})$  avec  $d \in \mathbb{Q}$ ) est contenue dans une extension cyclotomique (i.e., de la forme  $\mathbb{Q}(\zeta)$  avec  $\zeta$  racine d'unité). (C'est un cas très particulier du *théorème de Kronecker et Weber* selon lequel toute extension abélienne de  $\mathbb{Q}$  se plonge dans une extension cyclotomique de  $\mathbb{Q}$ . La généralisation de ce théorème est le *Kronecker Jugendtraum* qui traite des extensions abéliennes de toute extension quadratique imaginaire de  $\mathbb{Q}$ .)

**Exercice 13.** On considère l'équation  $x^2 \equiv 59 \pmod{103}$  dans  $\mathbb{Z}$ .

1. A l'aide de la loi de réciprocité quadratique, montrer que l'équation admet une solution.
2. Trouver tous les solutions de l'équation.
3. Montrer que  $59^{51} - 1$  est divisible par 103.

**Exercice 14.** Soit  $F_n := 2^{2^n} + 1$  le  $n$ ième nombre de Fermat.

1. Montrer que si  $p$  est un nombre premier qui divise  $F_n$ , alors  $p$  est congru à 1 modulo  $2^{n+1}$ .
2. En utilisant le fait que si 16 divise  $p^2 - 1$  alors 2 est un carré de  $\mathbb{F}_p^\times$ , montrer que  $p$  est congru à 1 modulo  $2^{n+2}$  dès que  $n \geq 2$ .