SESSION 1: ELEMENTARY COMPUTATIONS OF GAUSS SUMS

Notations : We note $e(x) := \exp(2i\pi x)$ and the expression $e(x/p)$ is well defined for $x \in \mathbb{F}_p$. If q is a power of p, we consider the additive character :

$$\psi(x) = e(\tfrac{\mathrm{Tr}(x)}{p}),$$

where $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the trace morphism and $x \in \mathbb{F}_q$. Let $\chi : \mathbb{F}_q^* \to \mathbb{C}^*$ a non-trivial character (extended by zero on zero). If χ_0 is the trivial character we extend it by 1 on 0. We define Gauss sums for $a \in \mathbb{F}_q^*$ by :

$$G(\chi, \psi, a) = \sum_{x \in \mathbb{F}_q} \chi(x)\psi(ax) \text{ and } G(\chi, \psi) := G(\chi, \psi, 1).$$

Exercice I (A particular case of Hasse-Davenport) :

(i) Show that $G(\chi, \psi, a) = 0$, $G(\chi, \psi, a) = \bar{\chi}(a)G(\chi, \psi)$ and $|\,\mathrm{G}(\chi, \psi)\,| = \sqrt{q}$ $(\chi \neq \chi_0)$.

(ii) For $P(X) = X^n - a_1X^{n-1} + \cdots + (-1)^n a_n \in \mathbb{F}_q[X]$, we consider $\lambda(P) := \psi(a_1)\chi(a_n)$. Show that λ is multiplicative.

(iii) Show the identity :

$$1 + \mathrm{G}(\chi, \psi)\,T = \sum_f \lambda(f)T^{\deg(f)} = \prod_g (1 - \lambda(g)T^{\deg(g)})^{-1},$$

where the sum (resp. product) is over all unitary polynomials $f \in \mathbb{F}_q[X]$ and over irreducible unitary polynomials $g \in \mathbb{F}_q[X]$.

(iv) Deduce the Hasse-Davenport relation :

$$-G(\chi \circ N, \psi \circ \mathrm{Tr}) = (-G(\chi, \psi))^m,$$

where N and Tr are the trace and norm maps from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$.

Exercice 2 (Number of solutions of quadratic equations) :

Let $p \geq 3$, $Q_1(x) = \sum_{i=1}^n a_i x_i^2$ and $Q_2(x) = \sum_{i=1}^n b_i x_i^2$, two quadratic forms with coefficients in $\mathbb{F}_p$. We suppose that n is *odd* and that the following condition holds :

$$\forall\ 1 \leq i < j \leq n,\ a_i b_j - a_j b_i \neq 0.$$

We want to compute the number $N := \mathrm{card}\ \{x \in \mathbb{F}_p^n \mid Q_1(x) = Q_2(x) = 0\}$.

(i) Prove the following formula :

$$N = p^{n-2} + p^{-2} \sum_{(a,b) \neq (0,0)} \sum_{x \in \mathbb{F}_p^n} e(\tfrac{aQ_1(x) + bQ_2(x)}{p})$$

(ii) Let

$$D_i = \prod_{1 \leq j \leq n, j \neq i} (b_i a_j - a_i b_j) \text{ and } \epsilon_i = (\tfrac{D_i}{p}),$$

where $(\frac{\cdot}{p})$ is the Legendre symbol. Show the following formula :

$$N = p^{n-2} + (p-1)(\tfrac{-1}{p})^{\frac{n-1}{2}} (\sum_{i=1}^{n} \epsilon_i) p^{\frac{n-3}{2}}$$

(iii) State and prove a formula for the number of solutions N_m on $\mathbb{F}_{p^m}$.

(iv) Let $\bar{N}_m := \frac{N_m - 1}{p^m - 1}$. Show that the formal series

$$Z(T) := \exp(\sum_{m \geq 1} \bar{N}_m \tfrac{T^m}{m})$$

is a rational function.

(v) Show a functional equation between $Z(1/q^{n-3}T)$ and $Z(T)$.