D-MATH HS 2018 Prof. Emmanuel Kowalski
Exponential sums over Finite Fields. Exercise Sheet 2

October 19, 2018

Exercise 1. Let n be an odd integer. The goal of this exercise is to prove that

$$G(2,1;n) = \begin{cases} \sqrt{n} & \text{if } n \equiv 1 \mod 4, \\ i\sqrt{n} & \text{if } n \equiv 3 \mod 4. \end{cases}$$

proceed stepwise as follows:

i) Let S be the $n \times n$ matrix whose (j,k)-th element is ζ^{jk} where $\zeta = e\left(\frac{1}{n}\right)$ and $0 \le j,k \le n-1$, i.e.

$$S = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \zeta & \cdots & \zeta^{n-1} \\ 1 & \zeta^2 & \cdots & \zeta^{2(n-1)} \\ . & . & \cdots & . \\ 1 & \zeta^{n-1} & \cdots & \zeta^{(n-1)^2} \end{pmatrix}.$$

Show that

$$S^2 = \begin{pmatrix} n & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & n \\ 0 & 0 & \cdots & n & 0 \\ . & . & \cdots & . & . \\ 0 & n & \cdots & 0 & 0 \end{pmatrix},$$

and conclude that $\det(S) = \pm i^{n(n-1)/2} n^{n/2}$.

ii) Show that

$$\det(S) = \prod_{0 \le j < k \le n-1} (\zeta^k - \zeta^j) = \eta^U \prod_{0 \le j < k \le n-1} (\eta^{k-j} - \eta^{-k+j}) = \eta^U i^{n(n-1)/2} \prod_{0 \le j < k \le n-1} 2\sin((k-j)\pi/n),$$

where $\eta = e\left(\frac{1}{2n}\right)$ and

$$U := \sum_{0 \le j < k \le n-1} j + k.$$

Hint: Observe that S is a Vandermonde matrix and that

$$\zeta^k - \zeta^j = \eta^{j+k}(\eta^{k-j} - \eta^{-k+j}) = \eta^{j+k} 2i \sin((k-j)\pi/n).$$

iii) Prove that $U = 2n((n-1)/2)^2$ and conclude that $\det(S) = i^{n(n-1)/2} n^{n/2}$.

iv) Show that

$$G(2,1;n) = \mathrm{Trace}(S) = \lambda_1 + \cdots + \lambda_n,$$

where $\lambda_1, ..., \lambda_n$ are the eigenvalues of S.

v) Show that

$$\det(S^2 - xI) = -(x-n)^{(n+1)/2}(x-n)^{(n-1)/2}$$

and conclude that for any $j = 1, .., n$ one has

$$\lambda_j = \pm\sqrt{n} \text{ or } \pm i\sqrt{n}.$$

vi) Suppose that $\sqrt{n}$ occurs r times, $-\sqrt{n}$ occurs s times, $i\sqrt{n}$ occurs t times and $\sqrt{n}$ occurs u. Show that

$$r+s = \frac{n+1}{2}, \quad t+u = \frac{n-1}{2}$$

and that

$$\begin{cases} r-s = \pm 1, \quad t = u & \text{if } n \equiv 1 \mod 4, \\ r = s, \quad t-u = \pm 1 & \text{if } n \equiv 3 \mod 4. \end{cases}$$

vii) Show that

$$\det(S) = i^{2s+t-u} n^{\frac{n}{2}}$$

and use part *(iii)* to conclude that

$$2s + t - u \equiv n(n-1)/2 \mod 4.$$

viii) Conclude.

Exercise 2. In this exercise we are going to prove *the law of quadratic reciprocity*: let p, q two distinct odd prime number, then one has:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Proceed as follows:

i) Let n_1, n_2 be two coprime integer, χ_1 a multiplicative character of $(\mathbb{Z}/n_1\mathbb{Z})^\times$ and χ_2 a multiplicative character of $(\mathbb{Z}/n_2\mathbb{Z})^\times$. Show that

$$\tau_{\chi_1\chi_2} = \chi_1(n_2)\chi_2(n_1)\tau_{\chi_1}\tau_{\chi_2}.$$

ii) Conclude using Exercise 1.

Exercise 3. Let ψ, η be two additive character over $\mathbb{F}_q$, one define the *Kloosterman sum associated to ψ and η* as

$$S(\psi, \eta) := \sum_{x \in \mathbb{F}_q^\times} \psi(x)\eta(\overline{x}),$$

where $\overline{x}$ denotes the inverse of x in $\mathbb{F}_q$. Our goal is to show that

$$|S(\psi, \eta)| < 2q^{3/4},$$

the so called *Kloosterman's Bound.*

i) Show that for any $b \in \mathbb{F}_q^\times$, one has

$$S(\psi, \eta) = S(\psi_b, \eta_{\overline{b}}),$$

where $\psi_b(x) := \psi(bx)$ and $\eta_{\overline{b}}(x) := \eta(\overline{b}x)$. Conclude that

$$|S(\psi, \eta)| \leq \left(\frac{M_{k,q}}{q-1}\right)^{1/2k},$$

for any $k \geq 2$, where

$$M_{k,q} := \sum_{\substack{\psi,\eta \\ \psi \neq 1, \eta \neq 1}} |S(\psi, \eta)|^{2k}.$$

ii) Show that

$$M_{k,q} = q^2 N_{k,q} - 2(q-1) - (q-1)^{2k},$$

where $N_{k,q}$ is the number of solution over $\mathbb{F}_q$ of the system

$$\begin{cases} x_1 + ... + x_k = y_1 + ... + y_k, \\ \overline{x}_1 + ... + \overline{x}_k = \overline{y}_1 + ... + \overline{y}_k. \end{cases}$$

iii) Prove that $M_{0,q} = (q-1)^2$ and $M_{1,q} = (q^2 - q - 1)(q-1)$.

iv) For any $a, b \in \mathbb{F}_q^\times$ consider the system

$$\begin{cases} x_1 + x_2 = a, \\ \overline{x}_1 + \overline{x}_2 = b. \end{cases} \tag{1}$$

Show that (1) has an unique pair of solution if and only if $b = a^2/4$. Moreover show that

$$|\{(a, b) \in \mathbb{F}_q^\times \times \mathbb{F}_q^\times : (1) \text{ has two distinct pairs of solutions}\}| = (q-1)(q-3).$$

Conclude that the contribution of the solution of (x_1, x_2, y_1, y_2) of the system

$$\begin{cases} x_1 + x_2 = y_1 + y_2, \\ \overline{x}_1 + \overline{x}_2 = \overline{y}_1 + \overline{y}_2. \end{cases}$$

with $x_1 + x_2 \neq 0$ is given by $2(q-1)(q-3) + q - 1$.

v) Show that the contribution of the solution of (x_1, x_2, y_1, y_2) of the system

$$\begin{cases} x_1 + x_2 = y_1 + y_2, \\ \overline{x}_1 + \overline{x}_2 = \overline{y}_1 + \overline{y}_2. \end{cases}$$

with $x_1 + x_2 = 0$ is given by $(q-1)^2$ and conclude that

$$N_{2,q} = 3(q-1)(q-2).$$

vi) Compute $M_{2,q}$ and conclude the exercise.

Exercise 4. Same notation of Exercise 3.

i) Show that

$$M_{2,q} \leq (\max_{\psi,\eta} |S(\psi,\eta)|^2) M_{1,q}.$$

ii) Deduce that there exist ψ, η non trivial characters such that

$$|S(\psi,\eta)|^2 \geq 2q - 2.$$

Conclude that the Weil's Bound

$$|S(\psi,\eta)| \leq 2\sqrt{q}$$

is sharp.