Exercise 1.

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

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

Then $S^2 = \{s_{i,j}\}_{i,j}$, where

$$ s_{i,j} = \sum_{k=0}^{p-1} \zeta^{ki} \zeta^{kj} = \sum_{k=0}^{p-1} \zeta^{k(i+j)} = \sum_{k=0}^{p-1} e\left(\frac{k(i+j)}{n}\right). $$

Then, by the orthogonality of the additive character we get

$$ s_{i,j} = \begin{cases} n & \text{if } i+j \equiv 0 \pmod{n}, \\ 0 & \text{otherwise}. \end{cases} $$

Hence, we have

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

as we wanted. It is clear that $\det(S^2) = (-1)^{n(n-1)}n^n$ (observe that $(\pm1)^n = \pm1$ since $n$ is odd), thus we get $\det(S) = \pm n^{(n-1)/2}n^{n/2}$.

ii) Since $S$ is a Vandermonde, matrix we have that

$$ \det(S) = \prod_{0 \leq j < k \leq n-1} (\zeta^k - \zeta^j). $$

Moreover one has

$$ \zeta^k - \zeta^j = \zeta^j(\zeta^{k-j} - 1) = \eta^{2j}(\eta^{2(k-j)} - 1) = \eta^{k+j}(\eta^{k-j} - \eta^{-k+j}), $$

and that

$$ \eta^{k-j} - \eta^{-k+j} = e\left(\frac{k-j}{n}\right) - e\left(-\frac{j-k}{n}\right) = 2i \sin((k-j)\pi/n). $$
Hence we conclude
\[ \det(S) = \eta^{U} \cdot i^{n(n-1)/2} \prod_{0 \leq j < k \leq n-1} 2 \sin((k - j)\pi/2), \]
where
\[ U = \sum_{0 \leq j < k \leq n-1} j + k. \]

\textit{iii)} We start proving that
\[ \sum_{t=1}^{m} t = \frac{m(m + 1)}{2}, \quad \sum_{t=1}^{m} t^2 = \frac{m(m + 1)(2m + 1)}{6}. \]
Let us start with the first one. Using that
\[ (m + 1)^2 = m^2 + 2m + 1, \]
one obtains
\[ (m + 1)^2 = \sum_{t=0}^{m} 1 + 2t, \]
thus
\[ \sum_{t=1}^{m} t = \frac{(m + 1)m}{2}. \]
For the other formula similarly one start from
\[ (m + 1)^3 = \sum_{t=0}^{m} 1 + 3t + 3t^2. \]

Now we have
\[ U = \sum_{k=1}^{n-1} \sum_{j=1}^{k-1} j + k \]
\[ = \frac{1}{2} \sum_{k=1}^{n-1} 3k^2 - k \]
\[ = 2n((n - 1)/2)^2. \]
In particular \( \eta^U = 1 \) since \( 2n \mid U \). Thus
\[ \det(S) = i^{n(n-1)/2} \prod_{0 \leq j < k \leq n-1} 2 \sin((k - j)\pi/2). \]
On the other hand \( \sin((k - j)\pi/2) > 0 \), for any \( 0 \leq j < k \leq n - 1 \). Combining this with part \( (i) \) we conclude
\[ \det(S) = i^{n(n-1)/2} \eta^{n/2}. \]

\textit{iv)} By definition we have
\[ \text{Trace}(S) = \sum_{k=0}^{n-1} \zeta^k = \sum_{k=0}^{p-1} e \left( \frac{k^2}{n} \right) = G(2, 1; n). \]
Since the Trace is invariant with respect to a change of basis, one gets
\[ G(2, 1; n) = \text{Trace}(S) = \lambda_1 + \cdots + \lambda_n, \]
where \( \lambda_1, \ldots, \lambda_n \) are the eigenvalues of \( S \).
Let us consider the matrix $S^2 - x I$

$$S^2 - x I = \begin{pmatrix} n - x & 0 & \cdots & 0 & 0 \\ 0 & -x & \cdots & 0 & n \\ 0 & 0 & \cdots & n & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & n & \cdots & 0 & -x \end{pmatrix}.$$ 

Then $\det(S^2 - x I) = (n - x) \det(T^2_{0,0})$ where $T^2_{0,0} = \{t_{i,j}\}$ is the minor obtained from $S^2 - x I$ removing from $S^2 - x I$ the 0-th column and the 0-th row. By the definition of the determinant we get

$$\det(T) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^{n-1} t_{i,\sigma(i)}.$$ 

On the other hand we have that

$$t_{i,\sigma(i)} = \begin{cases} -x & \text{if } \sigma(i) = i, \\ n & \text{if } \sigma(i) = n - i, \\ 0 & \text{otherwise.} \end{cases}$$

This implies that

$$\prod_{i=1}^{n-1} t_{i,\sigma(i)} \neq 0$$

if and only if $\sigma = \prod_{j \in J}(j, n - j)$ for some $J \subset \{1, \ldots, \frac{n-1}{2}\}$, and moreover

$$\prod_{i=1}^{n-1} t_{i,\sigma(i)} = n^{2|J|}(-x)^{n-1-2|J|} = (n^2)^{|J|}(x^2)^{(n-1)/2-|J|}$$

in this case. Thus we have

$$\det(T) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^{n-1} t_{i,\sigma(i)}$$

$$= \sum_{J \subset \{1, \ldots, \frac{n-1}{2}\}} (-1)^{|J|} \prod_{i=1}^{n-1} t_{i,\sigma_{J(i)}},$$

where for any $J \subset \{1, \ldots, \frac{n-1}{2}\}$

$$\sigma_J = \prod_{j \in J}(j, n - j).$$

3
Thus we have

\[
\det(T) = \sum_{J \subset \{1, \ldots, \frac{n-1}{2}\}} (-1)^{|J|} \prod_{i=1}^{n-1} t_{i,\sigma(j)}(t)
\]

\[
= \sum_{J \subset \{1, \ldots, \frac{n-1}{2}\}} (-1)^{|J|} \prod_{i=1}^{n-1} (n^2)^{|J|}(x^2)^{(n-1)/2-|J|}
\]

\[
= \sum_{J \subset \{1, \ldots, \frac{n-1}{2}\}} \prod_{i=1}^{(n-1)/2} (-n^2)^{|J|}(x^2)^{(n-1)/2-\ell}
\]

\[
= \sum_{\ell=0}^{(n-1)/2} \left(\frac{(n-1)}{2}\right)\ell \left(-n^2\right)^{\ell}(x^2)^{(n-1)/2-\ell}
\]

\[
= (x^2 - n^2)^{(n-1)/2}
\]

\[
= (x + n)^{(n-1)/2}(x - n)^{(n-1)/2}.
\]

Hence

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

For any \(\lambda_j\) eigenvalue of \(S\), one has

\[
S^2 - \lambda_j^2 I = (S - \lambda_j I)(S + \lambda_j I) = 0,
\]

then \(\lambda_j^2\) is an eigenvalue of \(S^2\). Hence \(\lambda_j^2\) is a solution of the polynomial \(\det(S^2 - xI) = -(x + n)^{(n-1)/2}(x - n)^{(n+1)/2}\), i.e. \(\lambda_j = \pm \sqrt{n}\) or \(\lambda_j = \pm i\sqrt{n}\).

\(vi)\) if \(\lambda_1, \ldots, \lambda_n\) are the eigenvalues of \(S\), then \(\lambda_1^2, \ldots, \lambda_n^2\) are eigenvalues of \(S^2\), this implies that

\[
p(t) := \prod_{j=1}^n (\lambda_j^2 - x) \det(S^2 - xI) = -(x + n)^{(n-1)/2}(x - n)^{(n+1)/2},
\]

on the other hand \(n = \deg(p(x)) = \deg(\det(S^2 - xI))\), thus

\[
p(t) = -(x + n)^{(n-1)/2}(x - n)^{(n+1)/2}.
\]

This implies that

\[
|\{j : \lambda_j^2 = n\}| = \frac{n + 1}{2}, \quad |\{j : \lambda_j^2 = -n\}| = \frac{n - 1}{2},
\]

thus

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

By part \((iv)\) we know that

\[
G(2, 1; n) = \sum_{j=1}^n \lambda_j = (r - s)\sqrt{n} + (t - u)i\sqrt{n}.
\]

Let us assume that \(n \equiv 1 \mod 4\), then since \(G(2, 1; n) = \pm \sqrt{n}\), it follows that

\[
r - s = \pm 1, \quad t - u = 0.
\]

If \(n \equiv 3 \mod 4\), then it follows that

\[
r - s = 0, \quad t - u = \pm 1,
\]

since in this case \(G(2, 1; n) = \pm i\sqrt{n}\).
vii) We know that
\[
\det(S) = \prod_{j=1}^{n} \lambda_j = (\sqrt{n})(-\sqrt{n})^s(i\sqrt{n})^t(-i\sqrt{n})^u = i^{2s+t-u}n^{n/2}.
\]
On the other hand by part (iii) we have
\[
\det(S) = i^{n(n-1)/2}n^{n/2}.
\]
Hence \(i^{n(n-1)/2} = i^{2s+t-u}\) and this is true if and only if
\[
2s + t - u \equiv n(n-1)/2 \mod 4.
\]
viii) Let us discuss first the case when \(n \equiv 1 \mod 4\). Thanks to part (vii) we deduce
\[
2s = n(n-1)/2 = (n-1)/2 \mod 4, \quad \text{i.e.} \quad 2s \equiv 0 \mod 4.
\]
Thus
\[
t - u = n(n+1)/2 - 2s \mod 4
\]
\[
= 3(n-1)/2 - (n+1)/2 \mod 4
\]
\[
= 1 \mod 4,
\]
and this implies \(r - s = 1\). Instead, if \(n \equiv 3 \mod 4\) we have
\[
2s = (n+1)/2,
\]
thus
\[
t - u = n(n+1)/2 - 2s \mod 4
\]
\[
= 3(n-1)/2 - (n+1)/2 \mod 4
\]
\[
= 1 \mod 4,
\]
and this implies \(t - u = 1\).

Exercise 2.

i) Since \((n_1, n_2) = 1\), the Chinese Remainder Theorem implies that for any \(a \in \left(\mathbb{Z}/(n_1n_2)\mathbb{Z}\right)^\times\)
there exists an unique pair \((a_1, a_2) \in \left(\mathbb{Z}/n_1\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/n_2\mathbb{Z}\right)^\times\) such that
\[
a = a_1n_2 + a_1n_2 \mod n_1n_2.
\]

Thus we have that
\[
\tau_{\chi_1\chi_2} = \sum_{a=0}^{n_1n_2} \chi_1\chi_2(a)e\left(\frac{a}{n}\right)
\]
\[
= \sum_{a=0}^{n_1n_2} \chi_1(a)\chi_2(a)e\left(\frac{a}{n}\right)
\]
\[
= \sum_{a_1=0}^{n_1} \sum_{a_2=0}^{n_2} \chi_1(a_1n_2)\chi_2(a_2n_1)e\left(\frac{a_1}{n_1}\right)e\left(\frac{a_2}{n_2}\right)
\]
\[
= \chi_1(n_2)\chi_2(n_1)\tau_{\chi_1}\tau_{\chi_2}.
\]
Let $p, q > 2$ be two distinct prime numbers. Using the previous point we have

$$\tau(pq) = \left( \frac{q}{p} \right) \left( \frac{p}{q} \right) \tau(p) \tau(q).$$

Moreover it is easy to see that

$$\tau(pq) = G(2, 1; pq).$$

To simplify the notation for any $n$ odd we write $G(2, 1; n) = \epsilon_n \sqrt{n}$, where

$$\epsilon_n = \begin{cases} 1 & \text{if } n \equiv 1 \mod 4 \\ i & \text{if } n \equiv 3 \mod 4, \end{cases}$$

thanks to Exercise 1. Thus we have

$$\epsilon_{pq} = \left( \frac{q}{p} \right) \left( \frac{p}{q} \right) \epsilon_p \epsilon_q.$$

If $p \equiv 1 \mod 4$, then $q \equiv pq \mod 4$. This implies $\epsilon_p = 1$ and $\epsilon_q = \epsilon_{pq}$. Hence

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

The case when $p \equiv 3 \mod 4$ is analogue.

**Exercise 3, Exercise 4.** You can find the solutions of these two exercises in the lecture notes "Exponential sums over finite fields, I: elementary methods" pages 19 – 23.