13. Gauss sums

Let \( \chi \) be a Dirichlet character mod \( q \).

**Definition 13.1.** The Gauss sum \( \tau(\chi) \) of \( \chi \) is defined to be

\[
\tau(\chi) = \sum_{a=1}^{q} \chi(a)e(a/q).
\]

The Gauss sum is a special case of the more general sum

\[
\tau(n, \chi) = \sum_{a=1}^{q} \chi(a)e(an/q).
\]

Note that \( \tau(\chi) = \tau(1, \chi) \). More generally:

**Lemma 13.2.** Suppose \( \chi \) is a Dirichlet character mod \( q \) and \( (n, q) = 1 \). Then \( \tau(n, \chi) = \bar{\chi}(n)\tau(\chi) \).

**Proof.** If \( (n, q) = 1 \) then the map \( a \mapsto an \) permutes the residues modulo \( q \). Hence

\[
\chi(n)\tau(n, \chi) = \sum_{a=1}^{q} \chi(an)e(an/q) = \tau(\chi).
\]

**Lemma 13.3.** Suppose \( (q_1, q_2) = 1 \) and \( \chi_i \) is a Dirichlet character mod \( q_i \) for \( i = 1, 2 \). Let \( \chi = \chi_1\chi_2 \). Then \( \tau(\chi) = \tau(\chi_1)\tau(\chi_2)\chi_1(q_2)\chi_2(q_1) \).

**Proof.** The Chinese remainder theorem implies that each \( a \) mod \( q_1q_2 \) can be written uniquely as \( a_1q_2 + a_2q_1 \) for \( 1 \leq a_i \leq q_i \). Thus the general term in \( \tau(\chi) \) is

\[
\chi_1(a_1q_2 + a_2q_1)\chi_2(a_1q_2 + a_2q_1)e\left(\frac{a_1q_2}{q_1q_2}\right)e\left(\frac{a_2q_1}{q_1q_2}\right) = \chi_1(a_1q_2)\chi_2(a_2q_1)e\left(\frac{a_1}{q_1}\right)e\left(\frac{a_2}{q_2}\right).
\]

For primitive characters the hypothesis \( (n, q) = 1 \) can be removed from Lemma 13.2.

**Theorem 13.4.** Suppose \( \chi \) is a primitive Dirichlet character mod \( q \). Then \( \tau(n, \chi) = \bar{\chi}(n)\tau(\chi) \) for all \( n \in \mathbb{Z} \). Moreover \( |\tau(\chi)| = \sqrt{q} \).

**Proof.** Without loss of generality we may assume that \( (n, q) = h > 1 \). Let us write \( n = hn' \) and \( q = hq' \). Then

\[
\tau(n, \chi) = \sum_{a=1}^{q} \chi(a)e(an/q) = \sum_{a=1}^{q} \chi(a)e(an'/q') = \sum_{b \text{ mod } q'} e(bn'/q') \sum_{a \equiv b \text{ mod } q'} \chi(a).
\]

But then inner sum is 0 by Lemma 11.14 and the fact that \( \chi \) is primitive. On the other hand \( \bar{\chi}(n)\tau(\chi) = 0 \), which therefore establishes the first part of the theorem.

The second part follows from the first part on observing that

\[
\sum_{n=1}^{q} \tau(n, \chi)\overline{\tau(n, \chi)} = \sum_{n=1}^{q} |\chi(n)|^2|\tau(\chi)|^2 = \varphi(q)|\tau(\chi)|^2.
\]
But the left hand side is
\[ \sum_{n=1}^{q} \tau(n, \chi) \overline{\tau(n, \chi)} = \sum_{n=1}^{q} \sum_{a \mod q} \chi(a)e(an/q) \sum_{b \mod q} \tilde{\chi}(b)e(-bn/q) \]
\[ = \sum_{a \mod q} \chi(a) \sum_{b \mod q} \tilde{\chi}(b) \sum_{n=1}^{q} e((a - b)n/q). \]

For any \( c \in \mathbb{Z} \) the function
\[ e(c \cdot /q) : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}^*, \quad n \mapsto e(cn/q), \]
defines an additive character on the finite abelian group \( \mathbb{Z}/q\mathbb{Z} \). Hence Corollary 11.6 implies that
\[ \sum_{n \mod q} e(cn/q) = \begin{cases} q & \text{if } c \equiv 0 \mod q, \\ 0 & \text{otherwise.} \end{cases} \]

Thus
\[ \sum_{n=1}^{q} \tau(n, \chi) \overline{\tau(n, \chi)} = q \sum_{a \mod q} \chi(a) \sum_{b \mod q} \tilde{\chi}(b) \sum_{b=\equiv a \mod q} \sum_{n=1}^{q} e((a - b)n/q). \]
\[ = q \sum_{a \mod q} \lvert \chi(a) \rvert \]
\[ = q \varphi(q). \]

It finally follows that \( |\tau(\chi)| = \sqrt{q} \), as claimed. \( \square \)

A very useful connection between Dirichlet characters and additive characters is given by the following result.

**Corollary 13.5.** Suppose that \( \chi \) is a primitive Dirichlet character mod \( q \). Then for all \( n \in \mathbb{Z} \) we have
\[ \chi(n) = \frac{1}{\tau(\tilde{\chi})} \sum_{a=1}^{q} \tilde{\chi}(a)e(an/q). \]

**Proof.** Note that \( \tau(\tilde{\chi}) \neq 0 \) if \( \chi \) is primitive, by Theorem 13.4. \( \square \)

We know that \( |\tau(\chi)| = \sqrt{q} \) for a primitive character \( \chi \) mod \( q \), but in general it hard to say anything about the argument of \( \tau(\chi) \) — except when \( \chi \) is real!

If \( \chi \) is a primitive character modulo \( q \) and \( \chi = \tilde{\chi} \), then Lemma 13.2 implies that \( \overline{\tau(\chi)} = \tau(-1, n) = \tilde{\chi}(-1) \tau(\chi) \). Hence
\[ \overline{\tau(\chi)} = \tilde{\chi}(-1) \tau(\chi) \Rightarrow \tau(\chi) = \chi(-1) \overline{\tau(\chi)} \]
\[ \Rightarrow \tau(\chi)^2 = \chi(-1) \tau(\chi) \overline{\tau(\chi)} \]
\[ \Rightarrow q = |\tau(\chi)|^2 = \tilde{\chi}(-1) \tau(\chi)^2 \]
\[ \Rightarrow \tau(\chi) = \pm \sqrt[4]{q}. \]

Gauss was the first to work out the correct sign. We will give a sketch of the proof for a real primitive character.
Theorem 13.6 (Gauss). Let $p > 2$ be a prime and let $\chi(n) = \left(\frac{n}{p}\right)$. Then

$$
\tau(\chi) = \begin{cases} 
\sqrt{p} & \text{if } p \equiv 1 \mod 4, \\
i\sqrt{p} & \text{if } p \equiv 3 \mod 4.
\end{cases}
$$

Proof. Let us put

$$
G(a, p) = \sum_{x=1}^{p} e\left(\frac{a x^2}{p}\right).
$$

Since $\#\{x \mod p : x^2 \equiv n \mod p\} = 1 + \left(\frac{n}{p}\right)$, we find that

$$
G(a, p) = \sum_{n=1}^{p} \left(1 + \left(\frac{n}{p}\right)\right) e\left(\frac{an}{p}\right) = \sum_{n=1}^{p} e\left(\frac{an}{p}\right) + \sum_{n=1}^{p} \left(\frac{n}{p}\right) e\left(\frac{an}{p}\right).
$$

The first term is 0 if $p \nmid a$, as we now assume, by orthogonality of additive characters. Hence for $p \nmid a$ we have

$$
G(a, p) = \tau(a, \chi) = \chi(a)\tau(\chi),
$$

by Lemma 13.2 and the fact that $\bar{\chi} = \chi$. In particular, it follows that

$$
\tau(\chi) = G(1, p) = \sum_{x=1}^{p} e\left(\frac{x^2}{p}\right) = G,
$$

say.

We will study $G$ using Poisson summation. We will apply Theorem 6.8 with

$$
f(x) = \begin{cases} 
e(x^2/p) & \text{if } x \in \left(\frac{1}{2}, p + \frac{1}{2}\right), \\
0 & \text{otherwise.}
\end{cases}
$$

Note that

$$
\hat{f}(n) = \int_{1/2}^{p+1/2} e\left(\frac{x^2}{p} - nx\right) dx.
$$

Complete the square by writing

$$
\frac{x^2}{p} - nx = \frac{1}{p} \left(x - \frac{np}{2}\right)^2 - \frac{n^2p}{4}.
$$

Making the change of variables $u = (x - np/2)/p$, we therefore obtain

$$
\hat{f}(n) = pe\left(-\frac{n^2p}{4}\right) \int_{\frac{1}{2}p+1-\frac{n}{2}}^{\frac{1}{2}p+1-\frac{n}{2}} e\left(\frac{pu^2}{4}\right) du.
$$

Now integration by parts yields

$$
\int_{U}^{V} e(cu^2) du = \frac{1}{4\pi i} \int_{U}^{V} \frac{1}{u} \cdot 4\pi i e(cu^2) du
$$

$$
= \frac{1}{4\pi i} \left\{ \left[\frac{e(cu^2)}{u}\right]_{U}^{V} + \int_{U}^{V} \frac{e(cu^2)}{u^2} du \right\}
$$

$$
\ll \frac{1}{U}.
$$
Hence
\[ \hat{f}(n) \ll \frac{1}{1 + |n|}. \]

We conclude from Theorem 6.8 that
\[ G = \sum_{n \in \mathbb{Z}} f(n) = \sum_{n \in \mathbb{Z}} \hat{f}(n). \]

Sorting according to the parity of \( n \), we obtain
\[ \sum_{n=-M}^{M} \hat{f}(n) = \sum_{\varepsilon \in \{0,1\}} \sum_{k=-(M-\varepsilon)/2}^{(M-\varepsilon)/2} \hat{f}(2k + \varepsilon) \]
\[ = p \sum_{\varepsilon \in \{0,1\}} e \left( -\frac{\varepsilon^2 p}{4} \right) \sum_{k=-(M-\varepsilon)/2}^{(M-\varepsilon)/2} \int_{\frac{1}{2p} - k + \frac{\varepsilon}{2}}^{1\frac{1}{2p} + k + \frac{\varepsilon}{2}} e(pu^2)du. \]

The integrals may be combined to form one integral, which as \( M \to \infty \) tends to
\[ \int_{-\infty}^{\infty} e(pu^2)du = \frac{1}{\sqrt{p}} \int_{-\infty}^{\infty} e(u^2)du = \frac{1}{\sqrt{p}} \cdot \frac{1}{1 - i}, \]

since (see §3.322 of Gradshteyn–Ryzhik)
\[ \int_{0}^{\infty} e^{2\pi ix^2}dx = \frac{1}{2\sqrt{2}} e^{\frac{\pi i}{4}} = \frac{1 + i}{4} = \frac{1}{2(1 - i)}. \]

Hence
\[ G = \frac{\sqrt{p}}{1 - i} \sum_{\varepsilon \in \{0,1\}} e \left( -\frac{\varepsilon^2 p}{4} \right) \]
\[ = \frac{\sqrt{p}}{1 - i} \left( 1 + e \left( -\frac{p}{4} \right) \right) \]
\[ = \frac{1 + i^{-p}}{1 - i} \sqrt{p}, \]

since \( e(\frac{1}{2}) = i \). One easily checks that
\[ \frac{1 + i^{-p}}{1 - i} = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4, \\ i & \text{if } p \equiv 3 \mod 4, \end{cases} \]

which thereby completes the proof of the theorem. \( \square \)