Chapter 3

Characters and Gauss sums

3.1 Characters on finite abelian groups

In what follows, abelian groups are multiplicatively written, and the unit element of an abelian group \( A \) is denoted by 1. We denote the order (number of elements) of \( A \) by \(|A|\).

Let \( A \) be a finite abelian group. A character on \( A \) is a group homomorphism \( \chi : A \to \mathbb{C}^* \) (i.e., \( \mathbb{C} \setminus \{0\} \) with multiplication).

If \(|A| = n\) then \( a^n = 1\), hence \( \chi(a)^n = 1 \) for each \( a \in A \) and each character \( \chi \) on \( A \). Therefore, a character on \( A \) maps \( A \) to the roots of unity.

The product \( \chi_1 \chi_2 \) of two characters \( \chi_1, \chi_2 \) on \( A \) is defined by \( (\chi_1 \chi_2)(a) := \chi_1(a)\chi_2(a) \) for \( a \in A \). With this product, the characters on \( A \) form an abelian group, the so-called character group of \( A \), which we denote by \( \hat{A} \) (or \( \text{Hom}(A, \mathbb{C}^*) \)). The unit element of \( \hat{A} \) is the trivial character \( \chi_0^{(A)} \) that maps \( A \) to 1. Since any character on \( A \) maps \( A \) to the roots of unity, the inverse \( \chi^{-1} : a \mapsto \chi(a)^{-1} \) of a character \( \chi \) is equal to its complex conjugate \( \overline{\chi} : a \mapsto \overline{\chi(a)} \).

We first construct an isomorphism from \( A \) to \( \hat{A} \). This will not be canonical, since it will depend on a choice of generators for \( A \).

Lemma 3.1.1. Let \( A \) be a cyclic group of order \( n \). Then \( \hat{A} \) is also a cyclic group of order \( n \).
Proof. Let \( A = \langle g \rangle \). Let \( \rho_1 \) be a primitive \( n \)-th root of unity. Since \( g \) has order \( n \), there is a character \( \chi_1 \) on \( A \) with \( \chi_1(g) = \rho_1 \). Clearly, \( \chi_1 \) has order \( n \). Let \( \chi \in \hat{A} \). Then \( \chi(g)^n = 1 \), so \( \chi(g) = \rho_1^k \) for some integer \( k \), and hence \( \chi = \chi_1^k \) since a character on \( A \) is determined by its value in \( g \). So \( \hat{A} = \langle \chi_1 \rangle \) is a cyclic group of order \( n \). □

**Lemma 3.1.2.** Let \( A = A_1 \times \cdots \times A_r \) be the direct product of finite abelian groups \( A_1, \ldots, A_r \). Then \( \hat{A} \) is isomorphic to \( \hat{A}_1 \times \cdots \times \hat{A}_r \).

**Proof.** Define a map

\[
\varphi : \hat{A}_1 \times \cdots \times \hat{A}_r \to \hat{A} : (\chi_1, \ldots, \chi_r) \mapsto \chi_1 \cdots \chi_r,
\]

\[\chi_1 \cdots \chi_r((g_1, \ldots, g_r)) := \chi_1(g_1) \cdots \chi_r(g_r) \text{ for } g_i \in A_i, \ i = 1, \ldots, r.\]

It is easy to see that \( \varphi \) is a group homomorphism. Substituting \( g_j = 1_{A_j} \) for \( j \neq i \), we see that \( \chi_i \) is uniquely determined by \( \chi_1 \cdots \chi_r \), for \( i = 1, \ldots, r \). Hence \( \varphi \) is injective. Conversely, let \( \chi \in \hat{A} \), and for \( i = 1, \ldots, r \) define \( \chi_i \in \hat{A}_i \) by

\[\chi_i(g_i) := \chi(\ldots, g_i, \ldots) \text{ for } g_i \in A_i,\]

with on the \( j \)-th place the unit element of \( A_i \), for \( j \neq i \). Then one easily verifies that \( \chi = \chi_1 \cdots \chi_r \). Hence \( \varphi \) is also surjective. □

**Proposition 3.1.3.** Every finite abelian group is isomorphic to a direct product of cyclic groups.

**Proof.** See S. Lang, Algebra, Chap.1, §10. □

**Theorem 3.1.4.** Let \( A \) be a finite abelian group. Then there exists an isomorphism from \( A \) to \( \hat{A} \). So in particular, \( |\hat{A}| = |A| \).

**Proof.** By Proposition 3.1.3, \( A \) is isomorphic to a direct product \( C_1 \times \cdots \times C_r \) of finite cyclic groups. By Lemmas 3.1.1, 3.1.2, \( \hat{C}_i \) is a cyclic group of the same order as \( C_i \), for \( i = 1, \ldots, r \), and \( \hat{A} \) is isomorphic to \( \hat{C}_1 \times \cdots \times \hat{C}_r \). Now the isomorphism from \( A \) to \( \hat{A} \) can be established by mapping a generator of \( C_i \) to one of \( \hat{C}_i \), for \( i = 1, \ldots, r \). □

**Remark.** The isomorphism constructed above depends on choices for generators of \( C_i, \hat{C}_i \), for \( i = 1, \ldots, r \). So it is not canonical.
Corollary 3.1.5. Let $A$ be a finite abelian group, and $g \in A$ with $g \neq 1$. Then there is a character $\chi$ on $A$ with $\chi(g) \neq 1$.

Proof. First assume that $A = \langle g_1 \rangle$ is a cyclic group of order $n$. Then $g = g_1^k$ with $1 \leq k < n$. Let $\chi_1$ be a generator of $\hat{A}$ as constructed in the proof of Lemma 3.1.1. Then clearly, $\chi_1(g) \neq 1$.

Now let $A$ be an arbitrary finite abelian group. We may assume that $A = C_1 \times \cdots \times C_r$, where $C_1, \ldots, C_r$ are finite cyclic groups, and $g = (g_1, \ldots, g_r)$ with $g_i \in C_i$ for $i = 1, \ldots, r$ and, say, $g_1 \neq 1_{C_1}$. Choose $\chi_1 \in \hat{C_1}$ with $\chi_1(g_1) \neq 1$, let $\chi_2, \ldots, \chi_r$ be the principal characters on $C_2, \ldots, C_r$, and put $\chi := \chi_1 \cdots \chi_r$. Then clearly, $\chi(g) = \chi_1(g_1) \neq 1$.

For a finite abelian group $A$, let $\hat{\hat{A}}$ denote the character group of $\hat{A}$. We construct a canonical isomorphism from $A$ to $\hat{\hat{A}}$. Notice that each element $a \in A$ gives rise to a character $\hat{a}$ on $\hat{A}$, given by $\hat{a}(\chi) := \chi(a)$.

Theorem 3.1.6 (Duality). Let $A$ be a finite abelian group. Then the map $a \mapsto \hat{a}$ defines an isomorphism from $A$ to $\hat{\hat{A}}$.

Proof. The map $\varphi : a \mapsto \hat{a}$ obviously defines a group homomorphism from $A$ to $\hat{\hat{A}}$. By Corollary 3.1.5 we have $\text{Ker}(\varphi) = \{ a \in A : \hat{\hat{a}}(\chi) = 1 \forall \chi \in \hat{A} \} = \{1\}$; hence $\varphi$ is injective. By Theorem 3.1.4 we have $|\hat{\hat{A}}| = |\hat{\hat{A}}| = |A|$. Hence $\varphi$ is also surjective.

Theorem 3.1.7 (Orthogonality relations for characters). Let $A$ be a finite abelian group.

(i) For any two characters $\chi_1, \chi_2$ on $A$ we have

$$\sum_{a \in A} \overline{\chi_1(a)} \chi_2(a) = \begin{cases} |A| & \text{if } \chi_1 = \chi_2, \\ 0 & \text{if } \chi_1 \neq \chi_2. \end{cases}$$

(ii) For any two elements $a, b$ of $A$ we have

$$\sum_{\chi \in \hat{A}} \overline{\chi(a)} \chi(b) = \begin{cases} |A| & \text{if } a = b, \\ 0 & \text{if } a \neq b. \end{cases}$$
Proof. Part (ii) follows by applying part (i) with \( \hat{A} \) instead of \( A \), and using Theorem 3.1.6 and \( |\hat{A}| = |A| \). So we prove only (i). Let \( \chi_1, \chi_2 \in \hat{A} \) and put \( S := \sum_{a \in A} \chi_1(a)\chi_2(a) \). Let \( \chi := \chi_1\chi_2 = \chi_1\chi_2^{-1} \). Then \( S = \sum_{a \in A} \chi(a) \). Clearly, if \( \chi_1 = \chi_2 \) then \( \chi = \chi_0^{(A)} \), hence \( S = |A| \). Let \( \chi_1 \neq \chi_2 \). Then \( \chi \neq \chi_0^{(A)} \), hence there is \( g \in A \) with \( \chi(g) \neq 1 \). Further, 
\[
\chi(g)S = \sum_{a \in A} \chi(ga) = S,
\]

since \( ga \) runs through the elements of \( A \). Hence \( S = 0 \). \( \square \)

### 3.2 Dirichlet characters

Let \( q \in \mathbb{Z}_{\geq 2} \). Denote the residue class of \( a \) mod \( q \) by \( \bar{a} \). Recall that the prime residue classes mod \( q \), \( (\mathbb{Z}/q\mathbb{Z})^* = \{ \bar{a} : \gcd(a, q) = 1 \} \) form a group of order \( \varphi(q) \) under multiplication of residue classes. We can lift any character \( \bar{\chi} \) on \( (\mathbb{Z}/q\mathbb{Z})^* \) to a map \( \chi : \mathbb{Z} \to \mathbb{C} \) by setting
\[
\chi(a) := \begin{cases} 
\bar{\chi}(\bar{a}) & \text{if } \gcd(a, q) = 1; \\
0 & \text{if } \gcd(a, q) > 1.
\end{cases}
\]

Notice that \( \chi \) has the following properties:

(i) \( \chi(1) = 1 \);
(ii) \( \chi(ab) = \chi(a)\chi(b) \) for \( a, b \in \mathbb{Z} \);
(iii) \( \chi(a) = \chi(b) \) if \( a \equiv b \pmod{q} \);
(iv) \( \chi(a) = 0 \) if \( \gcd(a, q) > 1 \).

Any map \( \chi : \mathbb{Z} \to \mathbb{C} \) with properties (i)–(iv) is called a (Dirichlet) character modulo \( q \). Conversely, from a character \( \chi \) mod \( q \) one easily obtains a character \( \bar{\chi} \) on \( (\mathbb{Z}/q\mathbb{Z})^* \) by setting \( \bar{\chi}(\bar{a}) := \chi(a) \) for \( a \in \mathbb{Z} \) with \( \gcd(a, q) = 1 \).

Let \( G(q) \) be the set of characters modulo \( q \). We define the product \( \chi_1\chi_2 \) of \( \chi_1, \chi_2 \in G(q) \) by \( \chi_1\chi_2(a) = \chi_1(a)\chi_2(a) \) for \( a \in \mathbb{Z} \). With this operation, \( G(q) \) becomes a group, with unit element the principal character modulo \( q \) given by
\[
\chi_0^{(q)}(a) = \begin{cases} 
1 & \text{if } \gcd(a, q) = 1; \\
0 & \text{if } \gcd(a, q) > 1.
\end{cases}
\]
The inverse of $\chi \in G(q)$ is its complex conjugate

$$\bar{\chi} : a \mapsto \overline{\chi(a)}.$$ 

It is clear, that this makes $G(q)$ into a group, and that $\chi \mapsto \bar{\chi}$ defines an isomorphism from $G(q)$ to the character group of $(\mathbb{Z}/q\mathbb{Z})^\ast$.

One of the advantages of viewing characters as maps from $\mathbb{Z}$ to $\mathbb{C}$ is that this allows to multiply characters of different moduli: if $\chi_1$ is a character mod $q_1$ and $\chi_2$ a character mod $q_2$, then their product $\chi_1 \chi_2$ is a character mod lcm$(q_1, q_2)$.

We can easily translate the orthogonality relations for characters of $(\mathbb{Z}/q\mathbb{Z})^\ast$ into orthogonality relations for Dirichlet characters modulo $q$. Recall that a complete residue system modulo $q$ is a set, consisting of precisely one integer from every residue class modulo $q$, e.g., $\{3, 5, 11, 22, 104\}$ is a complete residue system modulo $5$.

**Theorem 3.2.1.** Let $q \in \mathbb{Z}_{\geq 2}$, and let $S_q$ be a complete residue system modulo $q$.

(i) Let $\chi_1, \chi_2 \in G(q)$. Then

$$\sum_{a \in S_q} \chi_1(a) \overline{\chi_2(a)} = \begin{cases} \varphi(q) & \text{if } \chi_1 = \chi_2; \\ 0 & \text{if } \chi_1 \neq \chi_2. \end{cases}$$

(ii) Let $a, b \in \mathbb{Z}$. Then

$$\sum_{\chi \in G(q)} \chi(a) \overline{\chi(b)} = \begin{cases} \varphi(q) & \text{if } \gcd(ab, q) = 1, \ a \equiv b \pmod{q}; \\ 0 & \text{if } \gcd(ab, q) = 1, \ a \not\equiv b \pmod{q}; \\ 0 & \text{if } \gcd(ab, q) > 1. \end{cases}$$

**Proof.** Easy exercise. \hfill $\square$

Let $\chi$ be a character mod $q$ and $d$ a positive divisor of $q$.

We say that $\chi$ is *induced* by a character $\chi'$ mod $d$ if $\chi(a) = \chi'(a)$ for every $a \in \mathbb{Z}$ with $\gcd(a, q) = 1$. Here we define the principal character mod 1 by $\chi_0^{(1)}(a) = 1$ for $a \in \mathbb{Z}$. For instance, $\chi_0^{(q)}$ is induced by $\chi_0^{(1)}$. Notice that if $\gcd(a, d) = 1$ and $\gcd(a, q) > 1$, then $\chi'(a) \neq 0$ but $\chi(a) = 0$.

An alternative formulation of $\chi$ being induced by $\chi'$ is that $\chi = \chi' \cdot \chi_0^{(q)}$. 

93
The conductor of $\chi$ is the smallest positive divisor $d$ of $q$ such that $\chi$ is induced by a character mod $d$.

We define the principal character mod 1 by $\chi_0^{(1)}(n) = 1$ for all $n \in \mathbb{Z}$. Clearly, if $q$ is an integer $\geq 2$ then $\chi_{0}^{(q)}$ is induced by $\chi_{0}^{(1)}$, so $\chi_{0}^{(q)}$ has conductor 1.

A character $\chi$ is called primitive if there is no divisor $d < q$ of $q$ such that $\chi$ is induced by a character mod $d$, in other words, if $\chi$ has conductor $q$.

**Theorem 3.2.2.** Let $q \in \mathbb{Z}_{\geq 2}$, $\chi$ a character mod $q$. Denote by $f$ the conductor of $\chi$.

(i) There is a unique character $\chi^*$ mod $f$ that induces $\chi$, and this is necessarily primitive.

(ii) Let $d$ be a divisor of $q$ and $\chi'$ a character mod $d$ that induces $\chi$. Then $f$ is a divisor of $d$ and $\chi^*$ induces $\chi'$.

We need some lemmas.

**Lemma 3.2.3.** Let $d$ be a divisor of $q$ and $a$ an integer with $\gcd(a, d) = 1$. Then there is $b \in \mathbb{Z}$ with $b \equiv a \pmod{d}$, $\gcd(b, q) = 1$.

*Proof.* Write $q = q_1 q_2$, where $q_1$ is composed of the primes occurring in the factorization of $d$, and where $q_2$ is composed of primes not dividing $d$. Thus, $d$ and $q_2$ are coprime. By the Chinese Remainder Theorem, there is $b \in \mathbb{Z}$ with

$$b \equiv a \pmod{d}, \quad b \equiv 1 \pmod{q_2}.$$ 

This integer $b$ is coprime with $d$, hence with $q_1$, and also coprime with $q_2$, so it is coprime with $q$. \qed

**Lemma 3.2.4.** Let $\chi$ be a character mod $q$, and $d$ a divisor of $q$. Then there is at most one character mod $d$ that induces $\chi$.

*Proof.* Suppose $\chi$ is induced by a character $\chi_1$ mod $d$. Let $a \in \mathbb{Z}$ with $\gcd(a, d) = 1$. Choose $b \in \mathbb{Z}$ with $b \equiv a \pmod{d}$ and $\gcd(b, q) = 1$. Then $\chi_1(a) = \chi_1(b) = \chi(b)$. Hence $\chi_1$ is uniquely determined by $\chi$. \qed

The next lemma gives a method to verify if a character $\chi$ is induced by a character mod $d$. 

94
Lemma 3.2.5. Let $\chi$ be a character mod $q$, and $d$ a divisor of $q$. Then the following assertions are equivalent:

(i) $\chi$ is induced by a character mod $d$;
(ii) $\chi(a) = \chi(b)$ for all $a, b \in \mathbb{Z}$ with $a \equiv b \pmod{d}$ and $\gcd(ab, q) = 1$;
(iii) $\chi(a) = 1$ for all $a \in \mathbb{Z}$ with $a \equiv 1 \pmod{d}$ and $\gcd(a, q) = 1$.

Proof. The implications (i)$\Rightarrow$(ii)$\Rightarrow$(iii) are trivial.

(iii) $\Rightarrow$ (ii). Let $a, b \in \mathbb{Z}$ with $a \equiv b \pmod{d}$ and $\gcd(ab, q) = 1$. There is $c \in \mathbb{Z}$ with $\gcd(c, q) = 1$ such that $a \equiv bc \pmod{q}$. For this $c$ we have $c \equiv 1 \pmod{d}$. Now by (iii) we have $\chi(a) = \chi(b)\chi(c) = \chi(b)$.

(ii)$\Rightarrow$(i). We define a character $\chi'$ mod $d$ as follows. For $a \in \mathbb{Z}$ with $\gcd(a, d) > 1$ put $\chi'(a) := 0$. For $a \in \mathbb{Z}$ with $\gcd(a, d) = 1$, choose $b \in \mathbb{Z}$ such that $b \equiv a \pmod{d}$ and $\gcd(b, q) = 1$ (which is possible by Lemma 3.2.3), and put $\chi'(a) := \chi(b)$. By (ii) this gives a well-defined character mod $d$ that clearly induces $\chi$.

Remark. Notice that this lemma provides a method to compute the conductor of a character $\chi$ mod $q$: check for every divisor $d$ of $q$ whether $\chi(a) = 1$ for all integers $a$ with $1 \leq a < q$, $a \equiv 1 \pmod{d}$ and $\gcd(a, q) = 1$. The smallest divisor $d$ of $q$ for which this holds is the conductor of $\chi$.

Lemma 3.2.6. Let $\chi$ be a character mod $q$. Let $d_1, d_2$ be divisors of $q$. Assume that $\chi$ is induced by characters $\chi_1 \pmod{d_1}$, $\chi_2 \pmod{d_2}$. Then there is a character $\chi_3 \pmod{\gcd(d_1, d_2)}$ that induces $\chi$, $\chi_1$ and $\chi_2$.

Proof. Let $d := \gcd(d_1, d_2)$, $d_0 := \text{lcm}(d_1, d_2)$. We first show that $\chi_1$ is induced by a character mod $d$. We apply criterion (iii) of the previous lemma. That is, we have to show that if $a$ is an integer with $\gcd(a, d_1) = 1$ and $a \equiv 1 \pmod{d}$, then $\chi_1(a) = 1$.

Take such $a$. Then $a = 1 + td$ with $t \in \mathbb{Z}$. There are $x, y \in \mathbb{Z}$ with $xd_1 + yd_2 = d$. Hence $a = 1 + txd_1 + tyd_2$. The number $c := 1 + tyd_2 = a - txd_1$ is clearly coprime with $d_2$, and it is also coprime with $d_1$ since $a$ is coprime with $d_1$. Hence $c$ is coprime with $d_0$. By Lemma 3.2.3, there is $b$ with $b \equiv c \pmod{d_0}$ and $\gcd(b, q) = 1$. We have $b \equiv a \pmod{d_1}$, $b \equiv 1 \pmod{d_2}$. So by Lemma 3.2.5 applied with $d_1$ and $d_2$, $\chi_1(a) = \chi(b) = \chi_2(1) = 1$.

It follows that $\chi_1$ is induced by a character, say $\chi_3 \pmod{d}$. Similarly, $\chi_2$ is induced by a character $\chi'_3 \pmod{d}$. Both $\chi_3, \chi'_3$ induce $\chi$. So by Lemma 3.2.4, $\chi_3 = \chi'_3$. □
Proof of Theorem 3.2.2. (i) By Lemma 3.2.4 there is a unique character $\chi^\ast \mod f$ inducing $\chi$. If $\chi^\ast$ were induced by a character $\chi'$ modulo a divisor $d < f$ of $f$, then $\chi$ were induced by $\chi'$, contradicting the definition of the conductor. So $\chi^\ast$ is primitive.

(ii) By Lemma 3.2.6 there is a character $\chi'' \mod \gcd(d, f)$ inducing $\chi$, $\chi^\ast$ and $\chi'$. Since $\chi^\ast$ is primitive we must have $f \mid d$ and $\chi'' = \chi^\ast$. So $\chi^\ast$ induces $\chi'$.

\section{Computation of $G(q)$}

We give a method to compute the character group modulo $q$. We first make a reduction to prime powers.

\textbf{Theorem 3.3.1.} Let $q = p_1^{k_1} \cdots q_t^{k_t}$, where $p_1, \ldots, p_t$ are distinct primes and $k_1, \ldots, k_t$ positive integers. Then the map

$$G(p_1^{k_1}) \times \cdots \times G(p_t^{k_t}) \to G(q) : (\chi_1, \ldots, \chi_t) \mapsto \chi_1 \cdots \chi_t$$

is a group isomorphism.

\textbf{Proof.} Let $\rho$ denote the map under consideration. Then $\rho$ is a homomorphism. Since $G(p_1^{k_1}) \times \cdots \times G(p_t^{k_t})$ and $G(q)$ have the same order $\varphi(q)$, it suffices to show that $\rho$ is injective. That is, we have to show that if $\chi_i \in G(p_i^{k_i})$ ($i = 1, \ldots, t$) are such that $\chi_1 \cdots \chi_t = \chi_0^{(q)}$, then $\chi_i = \chi_0^{(p_i^{k_i})}$ for $i = 1, \ldots, t$.

To prove this, let $i \in \{1, \ldots, t\}$ and $a \in \mathbb{Z}$ with $\gcd(a, p_i) = 1$. By the Chinese Remainder Theorem, there is $b \in \mathbb{Z}$ such that

$$b \equiv a \pmod{p_i^{k_i}}, \quad b \equiv 1 \pmod{p_j^{k_j}} \text{ for } j \neq i,$$

and using this $b$ we infer $\chi_i(a) = \chi_1(b) \cdots \chi_t(b) = \chi_0^{(q)}(b) = 1$. Hence $\chi_i = \chi_0^{(p_i^{k_i})}$. \qed

To compute $G(p^k)$ for a prime power $p^k$, we need some information about the structure of $(\mathbb{Z}/p^k\mathbb{Z})^\ast$. This is provided by the following theorem.

\textbf{Theorem 3.3.2.} (i) Let $p$ be a prime $\geq 3$. Then the group $(\mathbb{Z}/p^k\mathbb{Z})^\ast$ is cyclic of order $p^{k-1}(p-1)$.

(ii) $(\mathbb{Z}/4\mathbb{Z})^\ast$ is cyclic of order 2.

Further, if $k \geq 3$ then $(\mathbb{Z}/2^k\mathbb{Z})^\ast = \langle -1 \rangle \times \langle 5 \rangle$ is isomorphic to the direct product of a cyclic group of order 2 and a cyclic group of order $2^{k-2}$.
We skip the proof of \( k = 1 \) of (i), which belongs to a basic algebra course. For the proof of the remaining parts, we need a lemma.

For a prime number \( p \), and for \( a \in \mathbb{Z} \setminus \{0\} \), we denote by \( \text{ord}_p(a) \) the largest integer \( k \) such that \( p^k \) divides \( a \).

**Lemma 3.3.3.** Let \( p \) be a prime number and \( a \) an integer such that \( \text{ord}_p(a - 1) \geq 1 \) if \( p \geq 3 \) and \( \text{ord}_p(a - 1) \geq 2 \) if \( p = 2 \). Then

\[
\text{ord}_p(a^{p^k} - 1) = \text{ord}_p(a - 1) + k.
\]

**Proof.** We prove the assertion only for \( k = 1 \); then the general statement follows easily by induction on \( k \). Our assumption on \( a \) implies that \( a = 1 + ptb \), where \( t \geq 1 \) if \( p \geq 3 \) and \( t \geq 2 \) if \( p = 2 \), and where \( b \) is an integer not divisible by \( p \). By the binomial formula,

\[
a^p - 1 = p^{t+1}b + \binom{p}{2}p^2b^2 + \cdots + \binom{p}{p-1}p^{p-1}tb^{p-1}t + p^tbt^t \equiv p^{t+1}b \pmod{p^{t+2}}
\]

since \( \binom{p}{2}, \ldots, \binom{p}{p-1} \) are all divisible by \( p \) and \( pt \geq t + 2 \) in both the cases \( p \geq 3 \), \( p = 2 \). So \( \text{ord}_p(a^p - 1) = t + 1 \). \( \square \)

**Lemma 3.3.4.** Let \( p \geq 3 \) be a prime number. Then there is an integer \( g \) such that \( g \pmod{p} \) is a generator of \( (\mathbb{Z}/p\mathbb{Z})^* \) and \( \text{ord}_p(g^{p-1} - 1) = 1 \).

**Proof.** We take for granted that \( (\mathbb{Z}/p\mathbb{Z})^* \) is cyclic of order \( p - 1 \); then there is an integer \( h \) such that \( h \pmod{p} \) is a generator of \( (\mathbb{Z}/p\mathbb{Z})^* \). So \( \text{ord}_p(h^{p-1} - 1) \geq 1 \). Put \( g := h \) if \( \text{ord}_p(h^{p-1} - 1) = 1 \) and \( g := h + p \) if \( \text{ord}_p(h^{p-1} - 1) \geq 2 \). In the latter case, we have

\[
g^{p-1} - 1 = h^{p-1} - 1 + (p - 1)h^{p-2}p + \binom{p-1}{2}h^{p-3}p^2 + \cdots + p^{p-1} \equiv -h^{p-2}p \pmod{p^2},
\]

hence \( \text{ord}_p(g^{p-1} - 1) = 1 \). \( \square \)

**Proof of Theorem 3.3.2.** (i). Let \( p \geq 3 \) and \( k \geq 2 \). Take \( g \) as in Lemma 3.3.4. We show that \( \bar{g} := g \pmod{p^k} \) generates \( (\mathbb{Z}/p^k\mathbb{Z})^* \) or equivalently, that the order \( n \) of \( \bar{g} \) in \( (\mathbb{Z}/p^k\mathbb{Z})^* \) equals the order of \( (\mathbb{Z}/p\mathbb{Z})^* \), which is \( p^{k-1}(p - 1) \). In any case, \( n \) divides \( p^{k-1}(p - 1) \). Further, \( g^n \equiv 1 \pmod{p} \), hence \( p - 1 \) divides \( n \). So \( n = p^s(p - 1) \) with \( s \leq k - 1 \). By Lemma 3.3.3 we have

\[
\text{ord}_p(g^n - 1) = \text{ord}_p(g^{p-1} - 1) + s = s + 1.
\]
This has to be at least $k$, so $s = k - 1$. Hence indeed $n = p^{k-1}(p - 1)$.

(ii). Assume that $k \geq 3$. Define the subgroup

$$H := \{ \bar{a} \in (\mathbb{Z}/2^k \mathbb{Z})^* : a \equiv 1 \pmod{4} \}.$$ 

Note that $\bar{a} \in (\mathbb{Z}/2^k \mathbb{Z})^*$ if $a \equiv 3 \pmod{4}$. So

$$(\mathbb{Z}/2^k \mathbb{Z})^* = H \cup (\mathbb{Z}/2^k \mathbb{Z}) = \langle -1 \rangle \times H.$$ 

Similarly as above, one shows that $H$ is cyclic of order $2^{k-2}$, and that $H = \langle 5 \rangle$. \qed

We can now give an explicit description for the groups $G(p^k)$, following the proofs of Lemmas 3.1.1, 3.1.2.

If $p > 2$, choose $g \in \mathbb{Z}$ such that $g \pmod{p^k}$ generates $(\mathbb{Z}/p^k \mathbb{Z})^*$, and choose a primitive $p^{k-1}(p - 1)$-th root of unity $\rho$. Then $G(p^k) = \langle \chi_1 \rangle$ where $\chi_1$ is the Dirichlet character determined by $\chi_1(g) = \rho$, and $G(p^k)$ is cyclic of order $p^{k-1}(p - 1)$.

Clearly, $G(2) = \{ \chi_0^{(2)} \}$ and $G(4) = \{ \chi_0^{(4)}, \chi_4 \}$, where $\chi_4(a) = 1$ if $a \equiv 1 \pmod{4}$, $\chi_4(a) = -1$ if $a \equiv 3 \pmod{4}$, $\chi_4(a) = 0$ if $a$ is even.

As for $2^k$ with $k \geq 3$, choose a primitive $2^{k-2}$-th root of unity $\rho$. Then $G(2^k) = \langle \chi_1 \rangle \times \langle \chi_2 \rangle$, where $\chi_1, \chi_2$ are given by

$$\chi_1(-1) = -1, \; \chi_1(5) = 1; \; \chi_2(-1) = 1, \; \chi_2(5) = \rho,$$

$\chi_1$ has order 2, and $\chi_2$ has order $2^{k-2}$.

### 3.4 Gauss sums

Let $q \in \mathbb{Z}_{\geq 2}$. For a character $\chi \mod q$ and for $b \in \mathbb{Z}$, we define the Gauss sum

$$\tau(b, \chi) := \sum_{a \in S_q} \chi(a)e^{2\pi iba/q},$$

where $S_q$ is a full system of representatives modulo $q$. This does not depend on the choice of $S_q$. The Gauss sum $\tau(1, \chi)$ occurs for instance in the functional equation for the L-function $L(s, \chi) = \sum_{n=1}^\infty \chi(n)n^{-s}$ (later).

We prove some basic properties of Gauss sums.
Theorem 3.4.1. Let \( q \in \mathbb{Z}_{\geq 2} \) and let \( \chi \) be a character mod \( q \). Further, let \( b \in \mathbb{Z} \).

(i) If \( \gcd(b, q) = 1 \), then \( \tau(b, \chi) = \overline{\chi(b)} \cdot \tau(1, \chi) \).

(ii) If \( \gcd(b, q) > 1 \) and \( \chi \) is primitive, then \( \tau(b, \chi) = \overline{\chi(b)} \cdot \tau(1, \chi) = 0 \).

Proof. (i) Suppose \( \gcd(b, q) = 1 \). If \( a \) runs through a complete residue system \( S_q \) mod \( q \), then \( ba \) runs through another complete residue system \( S'_q \) mod \( q \). Write \( y = ba \). Then \( \chi(y) = \chi(b)\chi(a) \), hence \( \chi(a) = \overline{\chi(b)}\chi(y) \). Therefore,

\[
\tau(b, \chi) = \sum_{a \in S_q} \chi(a)e^{2\pi i ba/q} = \sum_{y \in S'_q} \overline{\chi(b)}\chi(y)e^{2\pi iy/q} = \overline{\chi(b)} \cdot \tau(1, \chi).
\]

(ii) Let \( \gcd(b, q) = d > 1 \) and put \( b_1 := b/d, \ q_1 := q/d \). Then \( \chi \) is not induced by a character mod \( q_1 \), so by Lemma 3.2.5 there is \( c \in \mathbb{Z} \) such that \( c \equiv 1 \pmod{q_1} \), \( \gcd(c, q) = 1 \), and \( \chi(c) \not\equiv 1 \). With this \( c \) we have

\[
\chi(c)\tau(b, \chi) = \sum_{a \in S_q} \chi(ca)e^{2\pi i ba/q}.
\]

If \( a \) runs through a complete residue system \( S_q \) mod \( q \), then \( y := ca \) runs through another complete residue system \( S'_q \) mod \( q \). Further, since \( c \equiv 1 \pmod{q_1} \) we have

\[
e^{2\pi i ab/q} = e^{2\pi i b_1/q_1} = e^{2\pi i c b_1/q_1} = e^{2\pi i yb/q}.
\]

Hence

\[
\chi(c)\tau(b, \chi) = \sum_{y \in S'_q} \chi(y)e^{2\pi iyb/q} = \tau(b, \chi).
\]

Since \( \chi(c) \not\equiv 1 \) this implies that \( \tau(b, \chi) = 0 \).

\[\square\]

Theorem 3.4.2. Let \( q \in \mathbb{Z}_{\geq 2} \) and let \( \chi \) be a primitive character mod \( q \). Then

\[|\tau(1, \chi)| = \sqrt{q}.
\]
Proof. We have by Theorem 3.4.1,

\[ |\tau(1, \chi)|^2 = \tau(1, \chi) \cdot \tau(1, \chi) = \sum_{a=0}^{q-1} \chi(a) e^{-2\pi ia/q} \tau(1, \chi) \]

\[ = \sum_{a=0}^{q-1} e^{-2\pi ia/q} \tau(a, \chi) = \sum_{a=0}^{q-1} e^{-2\pi ia/q} \left( \sum_{b=0}^{q-1} \chi(b) e^{2\pi iab/q} \right) \]

\[ = \sum_{a=0}^{q-1} \left( \sum_{b=0}^{q-1} \chi(b) e^{2\pi iab/q} \right) \]

If \( b = 1 \), then \( S(b) = \sum_{a=0}^{q-1} 1 = q \), while if \( b \neq 1 \), then by the sum formula for geometric sequences,

\[ S(b) = \frac{e^{2\pi i(b-1)} - 1}{e^{2\pi i(b-1)/q} - 1} = 0. \]

Hence \( |\tau(1, \chi)|^2 = \chi(1)q = q. \)

Remark. Theorem 3.4.2 implies that \( \varepsilon_\chi := \tau(1, \chi)/\sqrt{q} \) lies on the unit circle. Gauss gave an easy explicit expression for \( \varepsilon_\chi \) in the case that \( \chi \) is a primitive real character mod \( q \), i.e., \( \chi \) assumes its values in \( \mathbb{R} \), so in \( \{0, \pm 1\} \). There is no general efficient method known to compute \( \varepsilon_\chi \) for non-real characters \( \chi \) modulo large values of \( q \).

3.5 Character sums

For many purposes one needs good estimates for expressions \( \left| \sum_{a=M+1}^{M+N} \chi(a) \right| \), where \( \chi \) is a non-principal character modulo an integer \( q \geq 2 \). We prove the following classic result, which, apart from the constant 3 in front of \( \sqrt{q} \log q \), was obtained independently by Polyá and I.N. Vinogradov in 1918.

Theorem 3.5.1. Let \( q \) be an integer \( \geq 2 \), \( \chi \) a non-principal character modulo \( q \), and \( M, N \) integers with \( N \geq 1 \). Then

\[ \left| \sum_{a=M+1}^{M+N} \chi(a) \right| \leq 3\sqrt{q} \log q. \]
Of course, the left-hand side is at most $N$. So this estimate is non-trivial only if $N > 3\sqrt{q} \log q$.

We need the following simple exponential sum estimate.

**Lemma 3.5.2.** Let $0 < x < 1$. Then

$$\left| \sum_{a=M+1}^{M+N} e^{2\pi i ax} \right| \leq \frac{1}{2} \cdot \max \left( \frac{1}{x}, \frac{1}{1-x} \right).$$

**Proof.** By the sum formula for geometric series,

$$M+1 \sum_{a=M+1}^{M+N} e^{2\pi i ax} = e^{2(M+1)\pi i x} \frac{e^{2N\pi i x} - 1}{e^{2\pi i x} - 1} = e^{(2M+N+1)\pi i x} \frac{e^{N\pi i x} - e^{-N\pi i x}}{e^{\pi i x} - e^{-\pi i x}}$$

$$= e^{(2M+N+1)\pi i x} \frac{\sin(\pi N x)}{\sin(\pi x)}.$$

The lemma easily follows by taking absolute values, using $|e^{\pi iy}| = 1$ and $|\sin \pi y| \leq 1$ for every $y \in \mathbb{R}$, and $\sin \pi y \geq 2 \min(y, 1-y)$ for every $y$ with $0 \leq y \leq 1$ (check the graph of $\sin$).

**Proof of Theorem 3.5.1.** We give an elementary proof, due to Schur (1918). We first assume that $\chi$ is a primitive character modulo $q$. Then by Theorem 3.4.1,

$$\sum_{a=M+1}^{M+N} \chi(a) = \tau(1, \chi)^{-1} \sum_{a=M+1}^{M+N} \tau(a, \chi)$$

$$= \tau(1, \chi)^{-1} \sum_{a=M+1}^{M+N} \left( \sum_{n=1}^{q-1} \chi(n)e^{2\pi i a n / q} \right)$$

$$= \tau(1, \chi)^{-1} \sum_{n=1}^{q-1} \chi(n) \left( \sum_{a=M+1}^{M+N} e^{2\pi i a n / q} \right).$$

Now from Theorem 3.4.2, $|\chi(n)| \leq 1$ for all $n$ and Lemma 3.5.2, we infer

$$\left| \sum_{a=M+1}^{M+N} \chi(a) \right| \leq \sqrt{q} \sum_{n=1}^{q-1} \frac{1}{n} \cdot \max \left( \frac{1}{n/q}, \frac{1}{1 - (n/q)} \right)$$

$$\leq \sqrt{q} \sum_{n=1}^{[q/2]} \frac{1}{n} \leq \sqrt{q} \left( 1 + \int_{1}^{q/2} \frac{dx}{x} \right) = \sqrt{q} \left( 1 + \log(q/2) \right),$$

101
(clear from the graph of $1/x$) and thus, using $1 + \log(x/2) \leq \frac{3}{2} \log x$ for $x \geq 2$,

\[(3.5.2) \left| \sum_{a=M+1}^{M+N} \chi(a) \right| \leq \frac{3}{2} \sqrt{q} \log q.
\]

This proves our theorem for primitive characters $\chi$ modulo $q$.

We still have to prove our theorem for non-primitive characters. Let $\chi$ be a non-primitive, non-principal character modulo $q$, and let $f$ be the conductor of $\chi$. Then $\chi$ is induced by a primitive character $\chi^*$ modulo $f$. We write $q = f \cdot q'$. If $\gcd(a, q') = 1$ then $\gcd(a, f) = \gcd(a, q)$, hence $\chi(a) = \chi^*(a)$. If $\gcd(a, q') > 1$, then $\chi(a) = 0$. Thus,

\[
\sum_{a=M+1}^{M+N} \chi(a) = \sum_{a=M+1}^{M+N} \chi^*(a).
\]

The following trick is used quite often. Recall the property of the Möbius function

\[
\sum_{d|q', d|a} \mu(d) = \sum_{d|\gcd(a, q')} \mu(d) = \begin{cases} 1 & \text{if } \gcd(a, q') = 1, \\ 0 & \text{if } \gcd(a, q') > 1. \end{cases}
\]

By inserting this into the above identity and interchanging the summations, we obtain

\[
\sum_{a=M+1}^{M+N} \chi(a) = \sum_{a=M+1}^{M+N} \left( \sum_{d|q', d|a} \mu(d) \right) \chi^*(a)
\]

\[
= \sum_{d|q'} \mu(d) \left( \sum_{a=M+1}^{M+N} \chi^*(a) \right)
\]

\[
= \sum_{d|q'} \mu(d) \chi^*(d) \left( \sum_{(M+1)/d \leq b \leq (M+N)/d} \chi^*(b) \right),
\]

where we have written $a = db$ and used the multiplicativity of $\chi^*$. The inner sum has absolute value at most $\frac{3}{2} \sqrt{f} \log f$ by (3.5.2) with $\chi^*, f$ instead of $\chi, q$, the quantities $\mu(d)$ and $\chi^*(d)$ have absolute value at most 1 and the number of summands $d$ is precisely the number of divisors $\tau(q')$ of $q'$. Hence

\[
\left| \sum_{a=M+1}^{M+N} \chi(a) \right| \leq \frac{3}{2} \tau(q') \sqrt{f} \log f.
\]
Note that for each divisor \( d \) of \( q' \) with \( \sqrt{q'} \leq d \leq q \) there is a divisor \( q'/d \leq \sqrt{q'} \). Hence \( \tau(q') \leq 2\sqrt{q'} \) (of course there are much better estimates). Since also \( f \leq q \), we arrive at
\[
\left| \sum_{a=M+1}^{M+N} \chi(a) \right| \leq 3\sqrt{q'} \sqrt{f} \log f \leq 3\sqrt{q} \log q.
\]

We mention that the estimate in Theorem 3.5.1 can not be improved very much, since by a result of Schur, for every primitive character \( \chi \) modulo an integer \( q \geq 2 \) one has
\[
\max_N \left| \sum_{a=1}^{N} \chi(a) \right| > \frac{\sqrt{q}}{2\pi}.
\]
As mentioned above, Theorem 3.5.1 improves the trivial bound \( N \) only if \( N > 3\sqrt{q} \log q \). It would be important to have non-trivial estimates also for smaller values of \( N \). Burgess proved in 1962 that for every \( \varepsilon > 0 \) there is a number \( C(\varepsilon) > 0 \) such that for every integer \( q \geq 2 \), every primitive character \( \chi \) modulo \( q \), and every pair of integers \( M, N \) with \( N > 0 \),
\[
\left| \sum_{a=M+1}^{M+N} \chi(a) \right| \leq C(\varepsilon) N^{1/2} q^{(3/16)+\varepsilon}.
\]
This upper bound is non-trivial (smaller than \( N \)) if \( N \gg q^{(3/8)+2\varepsilon} \).

### 3.6 Quadratic reciprocity

We give an analytic proof of Gauss’ Quadratic Reciprocity Theorem, by computing certain special Gauss sums.

Let \( p > 2 \) be a prime number. An integer \( a \) is called a \textit{quadratic residue modulo} \( p \) if \( x^2 \equiv a \pmod{p} \) is solvable in \( x \in \mathbb{Z} \) and \( p \nmid a \), and a \textit{quadratic non-residue modulo} \( p \) if \( x^2 \equiv a \pmod{p} \) is not solvable in \( x \in \mathbb{Z} \). Further, a quadratic (non-)residue class modulo \( p \) is a residue class modulo \( p \) represented by a quadratic (non-)residue.
We define the Legendre symbol
\[
\left( \frac{a}{p} \right) := \begin{cases} 
1 & \text{if } a \text{ is a quadratic residue modulo } p; \\
-1 & \text{if } a \text{ is a quadratic non-residue modulo } p; \\
0 & \text{if } p \mid a.
\end{cases}
\]

Lemma 3.6.1. Let \( p \) be a prime > 2.
(i) \( \left( \frac{a}{p} \right) \) is a primitive character mod \( p \).
(ii) There are precisely \( \frac{1}{2}(p - 1) \) quadratic residue classes, and precisely \( \frac{1}{2}(p - 1) \) quadratic non-residue classes modulo \( p \).
(iii) \( \left( \frac{a}{p} \right) \equiv a^{(p-1)/2} \pmod{p} \) for \( a \in \mathbb{Z} \).

Proof. (i) The group \((\mathbb{Z}/p\mathbb{Z})^*\) is cyclic of order \( p - 1 \). Let \( g \pmod{p} \) be a generator of this group. Take \( a \in \mathbb{Z} \) with gcd\((a,p) = 1\). Then there is \( t \in \mathbb{Z} \) such that \( a \equiv g^t \pmod{p} \). Now clearly, \( x^2 \equiv a \pmod{p} \) is solvable in \( x \in \mathbb{Z} \) if and only if \( t \) is even. Hence \( \left( \frac{a}{p} \right) = (-1)^t \). This shows that \( \left( \frac{\cdot}{p} \right) \) is a character mod \( p \). It is not the principal character mod \( p \), since \( \left( \frac{g}{p} \right) = -1 \). Since \( p \) is a prime, it must be primitive.

(ii) The group \((\mathbb{Z}/p\mathbb{Z})^*\) consists of \( g^t \pmod{p} \) \( (t = 0, \ldots, p - 1) \). As we have seen, the quadratic residue classes are those with \( t \) even, and the quadratic non-residue classes those with \( t \) odd. This implies (ii).

(iii) The assertion is clearly true if \( p \mid a \). Assume that \( p \nmid a \). Then there is \( t \in \mathbb{Z} \) with \( a \equiv g^t \pmod{p} \). Note that \( (g^{(p-1)/2})^2 \equiv 1 \pmod{p} \), hence \( g^{(p-1)/2} \equiv \pm 1 \pmod{p} \). But \( g^{(p-1)/2} \not\equiv 1 \pmod{p} \) since \( g \pmod{p} \) is a generator of \((\mathbb{Z}/p\mathbb{Z})^*\). Hence \( g^{(p-1)/2} \equiv -1 \pmod{p} \). As a consequence,
\[
a^{(p-1)/2} \equiv (-1)^t \equiv \left( \frac{a}{p} \right) \pmod{p}.
\]

The following is immediate:

Corollary 3.6.2. Let \( p \) be a prime > 2. Then
\[
\left( \frac{-1}{p} \right) = (-1)^{(p-1)/2} = \begin{cases} 
1 & \text{if } p \equiv 1 \pmod{4}, \\
-1 & \text{if } p \equiv 3 \pmod{4}.
\end{cases}
\]

We now come to the formulation of Gauss’ Quadratic Reciprocity Theorem:
Theorem 3.6.3. Let $p, q$ be distinct primes $> 2$. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} = \begin{cases} -1 & \text{if } p \equiv q \equiv 3 \pmod{4}, \\ 1 & \text{otherwise.} \end{cases}$$

Furthermore, as a supplement we have:

Theorem 3.6.4. Let $p$ be a prime $> 2$. Then

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$$

Example. Check if $x^2 \equiv 33 \pmod{97}$ is solvable.

$$\left(\frac{33}{97}\right) = \left(\frac{3}{97}\right) \cdot \left(\frac{11}{97}\right) = \left(\frac{97}{3}\right) \cdot \left(\frac{97}{11}\right)$$

$$= \left(\frac{1}{3}\right) \cdot \left(-2\right) = \left(\frac{1}{3}\right) \cdot \left(-1\right) \cdot \left(\frac{2}{11}\right) = 1 \cdot (-1) \cdot (-1) = 1.$$
\[ \int_0^1 |f(t)| dt < \infty \] and \( f \) has bounded variation. The version we state and prove with a much more restrictive condition on \( f \) is amply sufficient for our purposes.

2. It may be that \( \lim_{N \to \infty} \sum_{n=-N}^{N} a_n \) converges, whereas the doubly infinite series \( \sum_{n=-\infty}^{\infty} a_n = \lim_{M,N \to \infty} \sum_{n=-M}^{N} a_n \) (with \( M, N \to \infty \) independently of each other) diverges. For instance, if \( a_{-n} = -a_n \) for \( n \in \mathbb{Z} \setminus \{0\} \), then \( \lim_{N \to \infty} \sum_{n=-N}^{N} a_n = a_0 \), but \( \sum_{n=-\infty}^{\infty} a_n \) may be horribly divergent.

**Proof.** We first consider some special cases. For the constant function \( f(z) = 1 \) we have \( c_0(f) = 1 \), while \( c_n(f) = 0 \) for \( n \neq 0 \), and so in this case, \( \sum_{n=-N}^{N} c_n(f) = 1 = \frac{1}{2}(f(0) + f(1)) \) for all \( N \). For the function \( f(z) = z \) we have \( c_0(f) = \frac{1}{2} \), while \( c_n(f) = -\frac{1}{2\pi i n} \) for \( n \neq 0 \). So also in this case, \( \sum_{n=-N}^{N} c_n(f) = \frac{1}{2} = \frac{1}{2}(f(0) + f(1)) \) for all \( N \).

We now take an arbitrary function \( f \) as in the statement of the theorem, say analytic on an open subset \( U \) of \( \mathbb{C} \) containing \([0, 1]\). Define the function \( f^*(z) := f(z) - f(0) + (f(0) - f(1))z \). Then \( f^* \) is analytic on \( U \) and \( f^*(0) = f^*(1) = 0 \). We prove that \( \lim_{N \to \infty} \sum_{n=-N}^{N} c_n(f^*) = 0 \). Together with the special cases just considered and the linearity of \( c_n(\cdot) \) over \( \mathbb{C} \) this implies \( \lim_{N \to \infty} \sum_{n=-N}^{N} c_n(f) = \frac{1}{2}(f(0) + f(1)) \).

From the identity
\[
\sum_{n=-N}^{N} e^{-2\pi i n t} = e^{2\pi i N t} \sum_{n=0}^{2N} e^{-2\pi i n t} = e^{2\pi i N t} \frac{e^{-2\pi i (2N+1) t} - 1}{e^{-2\pi i t} - 1} = \frac{e^{-\pi i (2N+1) t} - e^{\pi i (2N+1) t}}{e^{-\pi i t} - e^{\pi i t}} = \frac{\sin((2N+1)\pi t)}{\sin \pi t}
\]
we obtain
\[
\sum_{n=-N}^{N} c_n(f^*) = \int_0^1 f^*(t) \cdot \sin((2N+1)\pi t) \cdot dt = \int_0^1 g(t) \cdot \sin(h_N(t)) dt,
\]
where \( g(z) := \frac{f^*(z)}{\sin \pi z}, \quad h_N(z) := (2N+1)\pi z. \)

Assume that \( U \) is small enough, so that it does not contain any integers other than \( 0, 1 \). Then \( g \) is analytic on \( U \). Indeed, \( \sin \pi z \neq 0 \) on \( U \) except at \( z = 0, z = 1 \) where
it has simple zeros, but these are cancelled by the zeros of \( f^* \) at \( z = 0, z = 1 \). Now using integration by parts, we obtain

\[
\left| \sum_{n=-N}^{N} c_n(f^*) \right| = \left| \int_{0}^{1} g(t) \sin(h_N(t))dt \right| = \frac{1}{(2N+1)\pi} \left| \int_{0}^{1} g(t) d\cos(h_N(t)) \right|
\]

\[
= \frac{1}{(2N+1)\pi} \left| -g(1) - g(0) - \int_{0}^{1} g'(t) \cos(h_N(t))dt \right|
\]

\[
\leq \frac{1}{(2N+1)\pi} \left( \left| g(1) \right| + \left| g(0) \right| + \int_{0}^{1} \left| g'(t) \right| dt \right) \rightarrow 0 \text{ as } N \rightarrow \infty.
\]

Here we used that \( g' \) is analytic on \( U \), hence \( t \mapsto \left| g'(t) \right| \) is continuous and bounded on \([0,1]\). This completes our proof. \( \square \)

**Corollary 3.6.6** (Poisson’s summation formula for finite sums). Let \( a, b \) be integers with \( a < b \) and let \( f \) be a complex analytic function, defined on an open subset of \( \mathbb{C} \) containing the interval \([a,b]\). Then

\[
\sum_{m=a}^{b} f(m) = \frac{1}{2} \left( f(a) + f(b) \right) + \lim_{N \rightarrow \infty} \sum_{n=-N}^{N} \int_{a}^{b} f(t) e^{-2\pi i nt} dt
\]

\[
= \frac{1}{2} \left( f(a) + f(b) \right) + \int_{a}^{b} f(t) dt + 2 \sum_{n=1}^{\infty} \int_{a}^{b} f(t) \cos 2\pi nt \cdot dt.
\]

**Proof.** Pick \( m \in \{a, \ldots, b-1\} \). Then by Theorem 3.6.5, applied to \( z \mapsto f(z + m) \), using \( e^{2\pi im} = 1 \),

\[
\frac{1}{2} \left( f(m) + f(m + 1) \right) = \lim_{N \rightarrow \infty} \sum_{n=-N}^{N} \int_{0}^{1} f(t + m)e^{-2\pi i nt} dt
\]

\[
= \lim_{N \rightarrow \infty} \sum_{n=-N}^{N} \int_{m}^{m+1} f(t) e^{-2\pi i nt} dt
\]

\[
= \int_{m}^{m+1} f(t) dt + \lim_{N \rightarrow \infty} \sum_{n=1}^{N} \int_{m}^{m+1} f(t) \left( e^{2\pi i nt} + e^{-2\pi i nt} \right) dt
\]

\[
= \int_{m}^{m+1} f(t) dt + 2 \sum_{n=1}^{\infty} \int_{m}^{m+1} f(t) \cos 2\pi nt \cdot dt.
\]
Now take the sum over \( m = a, a + 1, \ldots, b - 1 \).

Let \( q \) be any integer \( \geq 1 \), and \( b \) any integer coprime with \( q \). Define the exponential sums

\[
S(b, q) := \sum_{a=0}^{q-1} e^{2\pi iba^2/q}, \quad S(q) := S(1, q).
\]

**Lemma 3.6.7.** Let \( q \) be an odd prime and \( b \) an integer coprime with \( q \). Then

\[
S(b, q) = \tau(b, \left( \frac{q}{b} \right)) = \left( \frac{b}{q} \right) S(q).
\]

**Proof.** Let \( Q := \sum_{a=0}^{q-1} e^{2\pi iba^2/q}, N := \sum_{a=0}^{q-1} e^{2\pi iba/q} \), where \( \sum_{a=0}^{q-1} \) denotes the summation over the quadratic residues \( a \in \{0, \ldots, q-1\} \) and \( \sum_{a=0}^{q-1} \) that over the quadratic non-residues \( a \in \{0, \ldots, q-1\} \). Then

\[
1 + Q + N = \sum_{a=0}^{q-1} e^{2\pi iba/q} = \frac{e^{2\pi ib} - 1}{e^{2\pi ib/q} - 1} = 0.
\]

If \( a \) runs through \( 1, \ldots, q-1 \), then \( a^2 \pmod{q} \) runs twice through the quadratic residue classes mod \( q \) (note that \( a^2 \) and \( (q-a)^2 \) give the same quadratic residue). So

\[
S(b, q) = 1 + 2Q = Q - N = \sum_{a=0}^{q-1} \left( \frac{a}{q} \right) e^{2\pi ba/q} = \tau(b, \left( \frac{q}{b} \right)).
\]

The second equality in the statement follows from Theorem 3.4.1. \( \square \)

**Lemma 3.6.8.** Let \( p, q \) be two distinct odd primes. Then

\[
S(pq) = S(q,p)S(p,q) = \left( \frac{q}{p} \right) \left( \frac{p}{q} \right) S(p)S(q).
\]

**Proof.** If \( a \) runs through \( 0, \ldots, p-1 \) and \( b \) through \( 0, \ldots, q-1 \), then \( qa + pb \) runs through a complete system of residues mod \( pq \). Thus,

\[
S(pq) = \sum_{a=0}^{p-1} \sum_{b=0}^{q-1} e^{2\pi i(qa + pb)^2/pq} = \sum_{a=0}^{p-1} \sum_{b=0}^{q-1} e^{2\pi i((qa^2/p) + pb^2/q) + 2abq)}
\]

\[
= \sum_{a=0}^{p-1} \sum_{b=0}^{q-1} e^{2\pi iqa^2/p} \cdot e^{2\pi ib^2/q} = \sum_{a=0}^{p-1} e^{2\pi iqa^2/p} \sum_{b=0}^{q-1} e^{2\pi ib^2/q} = S(q,p)S(p,q).
\]

By Lemma 3.6.7, the latter is \( \left( \frac{q}{p} \right) \left( \frac{p}{q} \right) S(p)S(q) \). \( \square \)
Lemma 3.6.9. Let $q$ be a positive integer. Then

$$S(q) = \begin{cases} 
(1 + i)\sqrt{q} & \text{if } q \equiv 0 \pmod{4}, \\
\sqrt{q} & \text{if } q \equiv 1 \pmod{4}, \\
0 & \text{if } q \equiv 2 \pmod{4}, \\
i\sqrt{q} & \text{if } q \equiv 3 \pmod{4}.
\end{cases}$$

Proof. By Corollary 3.6.6 we have

\[
S(q) = -1 + \sum_{a=0}^{q} e^{2\pi ia^2/q} = \lim_{N \to \infty} \sum_{n=-N}^{N} \int_{0}^{q} e^{(2\pi it^2/q) - 2\pi in t} dt
\]

\[
= \sqrt{q} \cdot \lim_{N \to \infty} \sum_{n=-N}^{N} \int_{0}^{q} e^{2\pi i u^2 - 2\pi n \sqrt{q} u} (\text{substituting } u = t/\sqrt{q})
\]

\[
= \sqrt{q} \cdot \lim_{N \to \infty} \sum_{n=-N}^{N} \int_{0}^{q} e^{2\pi i ((u-n\sqrt{q})^2-n^2 q/4)} du
\]

\[
= \sqrt{q} \cdot \lim_{N \to \infty} \sum_{n=-N}^{N} e^{-\pi n^2 q/2} \int_{0}^{q} e^{2\pi i (u-n \sqrt{q})^2} du.
\]

We split the summation into even $n$ and odd $n$. Note that $e^{-\pi i n^2 q/2} = 1$ if $n$ is even, and $e^{-\pi i n/2}$ if $n$ is odd. So

\[
\sum_{n=-N}^{N} e^{-\pi n^2 q/2} \int_{0}^{q} e^{2\pi i (u-n \sqrt{q})^2} du = \sum_{n=-N}^{N} \int_{-N(1/2) \sqrt{q}}^{-N(1/2) \sqrt{q}} e^{2\pi i u^2} du = \int_{-N(1/2) \sqrt{q}}^{N(1/2) \sqrt{q}} e^{2\pi i u^2} du,
\]

say, where we use that the intervals $[-\frac{1}{2}n \sqrt{q}, (1 - \frac{1}{2}n) \sqrt{q}]$ $(n \in \{-N, \ldots, N\}$ even) apart from their begin points and end points do not overlap and paste together to a single interval $[-N_1 \sqrt{q}, N_2 \sqrt{q}]$ where $|N_i - \frac{1}{2} N| \leq 1$ for $i = 1, 2$. Likewise, the sum over the odd values of $n$ in $\{-N, \ldots, N\}$ is

\[
e^{-\pi i q/2} \int_{-N_3 \sqrt{q}}^{N_3 \sqrt{q}} e^{2\pi i u^2} du,
\]

where $|N_i - \frac{1}{2} N| \leq 1$ for $i = 3, 4$. Taking for the moment for granted that the integral $C := \int_{-\infty}^{\infty} e^{2\pi i u^2} du$ converges, we get

\[
S(q) = \sqrt{q} \lim_{N \to \infty} \left( \int_{-N_1 \sqrt{q}}^{N_1 \sqrt{q}} e^{2\pi i u^2} du + e^{-\pi i q/2} \int_{-N_3 \sqrt{q}}^{N_3 \sqrt{q}} e^{2\pi i u^2} du \right) = \sqrt{q}(1 + e^{-\pi i q/2}) C.
\]
Substituting $q = 1$ and using $S(1) = 1$ we read off $C = (1 - i)^{-1}$. Thus we get $S(q) = \sqrt{q} \cdot (1 + e^{-\pi i/2})/(1 - i)$, which gives our lemma.

It remains to show that $\int_{-\infty}^{\infty} e^{2\pi i u^2} du$ converges. This integral is equal to $2 \int_{0}^{\infty} e^{2\pi i u^2} du$, provided the latter converges. But this is indeed the case, since for any $B > A > 0$,

$$
\left| \int_{A}^{B} e^{2\pi i u^2} du \right| = \left| \int_{A}^{B} (4\pi i u)^{-1} e^{2\pi i u^2} du \right|
= \left| e^{2\pi i B^2} - e^{2\pi i A^2} - \frac{1}{4\pi i} \int_{A}^{B} u^{-2} e^{2\pi i u^2} du \right|
\leq (4\pi)^{-1} \left( B^{-1} + A^{-1} + \int_{A}^{B} u^{-2} du \right) = (2\pi A)^{-1} \rightarrow 0 \text{ as } A, B \rightarrow \infty.
$$

This completes our proof. \qed

*Proof of Theorem 3.6.3.* Immediate from Lemmas 3.6.9 and 3.6.8. \qed

## 3.7 Exercises

**Exercise 3.1.** Compute the characters modulo 12 and determine the conductor of each character.

**Exercise 3.2.** Recall that a character $\chi \mod q$ is called real if $\chi(a) \in \mathbb{R}$ for every $a \in \mathbb{Z}$, i.e., if $\chi(a) \in \{-1, 1\}$ for every $a \in \mathbb{Z}$ with $\gcd(a, q) = 1$.

a) For a positive integer $q$ denote by $R(q)$ the number of real characters mod $q$. Prove that $R$ is a multiplicative arithmetic function, and compute $R(p^k)$ for every prime power $p^k$.

b) Determine those positive integers $q$ such that every character mod $q$ is real.

**Exercise 3.3.** For a positive integer $q$, denote by $F(q)$ the number of primitive characters mod $q$. Prove that $F = \mu \ast \varphi$ where $\varphi(n) = \# \{m \in \mathbb{Z} : 1 \leq m \leq n, \gcd(m, n) = 1 \}$.

*Hint.* Show that $F(f)$ is equal to the number of characters mod $q$ with conductor $f$. Use Theorem 3.2.2.
Exercise 3.4. Let \( q \) be a positive integer. The Gauss sum \( \tau(1, \chi_0^{(q)}) \) is defined by
\[
\sum_{a=0}^{q-1} \chi_0^{(q)}(a)e^{2\pi ia/q} = \sum_{\substack{a=0 \atop \gcd(a,q)=1}}^{q-1} e^{2\pi ia/q}.
\]
Prove that \( \tau(1, \chi_0^{(q)}) = \mu(q) \).

Exercise 3.5. 

a) Let \( p^k \) be a prime power with \( k \geq 2 \) and \( \chi \) a non-primitive character modulo \( p^k \). Prove that \( \tau(1, \chi) = 0 \).

b) Let \( q_1, q_2 \) be two coprime integers \( \geq 2 \), \( \chi_1 \) a character modulo \( q_1 \) and \( \chi_2 \) a character modulo \( q_2 \). Prove that \( \tau(1, \chi_1 \chi_2) = \chi_1(q_2) \chi_2(q_1) \tau(1, \chi_1) \tau(1, \chi_2) \).

Hint. If \( a \) runs through \( \{0, \ldots, q_1 - 1\} \) and \( b \) through \( \{0, \ldots, q_2 - 1\} \) then \( aq_2 + bq_1 \) runs through a complete residue system modulo \( q_1 q_2 \).

Exercise 3.6. Let \( p \) be a prime \( > 2 \) and \( m \) a divisor of \( p - 1 \) with \( m \geq 2 \). An integer \( a \) is called an \( m \)-th power residue modulo \( p \) if \( p \) does not divide \( a \) and if there is an integer \( b \) with \( a \equiv b^m \pmod{p} \). Let \( M, N \) be integers with \( 0 \leq M < M + N < p \). Denote by \( R_m \) the number of \( m \)-th power residues mod \( p \) in the interval \([M+1, M+N]\). The purpose of this exercise is to show that
\[
| R_m - \frac{N}{m} | \leq \frac{3(m-1)}{m} \sqrt{p \log p}.
\]

In case that \( p \) is a large prime and \( N \) is much larger than \( 3(m-1)\sqrt{p \log p} \) this implies that about a fraction of \( 1/m \) among the integers in \( \{M+1, \ldots, M+N\} \) is an \( m \)-th power residue modulo \( p \). To prove this, perform the following steps:

a) Recall that \((\mathbb{Z}/p\mathbb{Z})^*\) is a cyclic group of order \( p - 1 \). Choose an integer \( g \) such that \( g \mod p \) generates \((\mathbb{Z}/p\mathbb{Z})^*\). Choose a character \( \chi_1 \mod p \) such that \( \chi_1(g) = e^{2\pi i/(p-1)} \); then \( G(p) = \langle \chi_1 \rangle \). Let \( t := (p-1)/m \). Prove that
\[
\sum_{j=0}^{m-1} \chi_1^{tj}(a) = \begin{cases} m & \text{if } a \text{ is an } m \text{-th power residue mod } p, \\ 0 & \text{otherwise.} \end{cases}
\]

b) Compute \( \sum_{j=0}^{m-1} \sum_{a=M+1}^{M+N} \chi_1^{tj}(a) \) in two ways.

Exercise 3.7. Prove Theorem 3.6.4.

Hint. Prove an analogue of Lemma 3.6.8 with \( q = 8 \).
Exercise 3.8. For an integer $a$ and a positive odd integer $b$ we define the Jacobi-symbol

$$\left(\frac{a}{b}\right) := \prod_{i=1}^{t} \left(\frac{a}{p_i}\right)^{k_i},$$

where $b = p_1^{k_1} \cdots p_t^{k_t}$ is the unique prime factorization of $b$.

a) Let $b$ be a positive odd integer. Prove that

$$\left(\frac{-1}{b}\right) = (-1)^{(b-1)/2}, \quad \left(\frac{2}{b}\right) = (-1)^{(b^2-1)/8}.$$ 

b) Let $a, b$ be two odd, positive, coprime integers. Prove that

$$\left(\frac{a}{b}\right) \cdot \left(\frac{b}{a}\right) = (-1)^{(a-1)(b-1)/4}.$$ 

c) Let $n$ be a positive odd, square-free integer which is not a prime. Prove that there are integers $a$ such that $x^2 \equiv a \pmod{n}$ is not solvable, while $\left(\frac{a}{n}\right) = 1$. 

112