Quadratic Reciprocity and the Sign of the Gauss Sum via the Finite Weil Representation

Shamgar Gurevich¹, Ronny Hadani², and Roger Howe³
¹School of Mathematics, Institute for Advanced Study, Princeton, NJ 08540, USA, ²Department of Mathematics, The University of Texas at Austin, Texas 78712, USA, and ³Department of Mathematics, Yale University, New Haven, CT 06520-8283, USA

Correspondence to be sent to: shamgar@math.ias.edu

We give new proofs of two basic results in number theory: the law of quadratic reciprocity and the sign of the Gauss sum. We show that these results are encoded in the relation between the discrete Fourier transform and the action of the Weyl element in the Weil representation modulo \( p \), \( q \), and \( pq \).

1 Introduction

Two basic results due to Gauss are the quadratic reciprocity law and the sign of the Gauss sum [8]. The first concerns the identity

\[
\left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}, \tag{1.1}
\]

where \( p \) and \( q \) are two distinct odd prime numbers and \((·/p)\) (respectively, \((·/q)\)) is the Legendre symbol modulo \( p \) (respectively, \( q \)), i.e. \((x/p) = 1\) if \( x \) is a square modulo \( p \) and \(-1\), otherwise. The latter result asserts that

\[
G_p = \sum_{x \in \mathbb{F}_p} e^{\frac{2\pi i x^2}{p}} = \begin{cases} 
\sqrt{p}, & p \equiv 1 \pmod{4}, \\
i\sqrt{p}, & p \equiv 3 \pmod{4}.
\end{cases} \tag{1.2}
\]
In fact, it is easy to show that \( G_p^2 = (-1/p) \cdot p \). Hence, the problem is to determine the exact sign in the evaluation of \( G_p \).

In this work, we will explain how these results follow from the proportionality relations

\[
F_n = C_n \cdot \rho_n \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \text{ for } n = p, q, \text{ and } pq,
\]

where \( F_n \) is the discrete Fourier transform (DFT), \( \rho_n \) is the Weil representation of the group \( SL_2(\mathbb{Z}/n\mathbb{Z}) \), both acting on the Hilbert space \( C(\mathbb{Z}/n\mathbb{Z}) \) of complex-valued functions on the finite ring \( \mathbb{Z}/n\mathbb{Z} \), and \( C_n \) is the proportionality constant. More specifically, the law of quadratic reciprocity follows from basic properties of the Weil representation and group theoretic considerations, while the calculation of the sign of the Gauss sum is a bit more delicate and it uses a formula for the character of the Weil representation. The fact that the DFT can be normalized so that it becomes a part of a representation plays a crucial role in our proof of both statements.

The main technical computation that we carry in this paper is of the determinant of the DFT \( F_n \). Interestingly, in this specific calculation, we use the concrete model of the ring \( \mathbb{Z}/n\mathbb{Z} \) as the set \( 0, 1, \ldots, n-1 \) with the standard addition and multiplication operations, while in the rest of the calculations, we do not use any specific model of \( \mathbb{Z}/n\mathbb{Z} \).

In his seminal work [10], André Weil recasts several known proofs of the law of quadratic reciprocity in terms of the Weil representation of some cover of the group \( SL_2(\mathbb{A}_Q) \), where \( \mathbb{A}_Q \) denotes the adele ring of \( \mathbb{Q} \). The main contribution of this short note is showing that quadratic reciprocity already follows from the Weil representation over finite rings and, moreover, establishing a conceptual mechanism, different from that of Weil, which produces the law of quadratic reciprocity.

1.1 Structure of the paper

In Section 2, we recall the Weil representation over the finite ring \( \mathbb{Z}/n\mathbb{Z} \). We then describe the relation between the Weil representations associated with the rings \( \mathbb{Z}/n_1\mathbb{Z} \), \( \mathbb{Z}/n_2\mathbb{Z} \), and \( \mathbb{Z}/n_1n_2\mathbb{Z} \), for \( n_1 \) and \( n_2 \) coprime. Finally, we describe some properties and write the formula of its character in the case \( n \) is an odd prime number. In Section 3, we define the DFT, compute its determinant, and explain its relation to the Weil representation.
In Section 4, we prove the quadratic reciprocity law, and in Section 5, we compute the Gauss sum. Finally, in the Appendix, we supply the proofs of the main technical claims that appear in the body of the paper.

2 The Weil Representation

2.1 The Heisenberg group

Let \((V, \omega)\) be a symplectic free module of rank 2 over the finite ring \(\mathbb{Z}/n\mathbb{Z}\), where \(n\) is an odd number. The reader should think of \(V\) as \(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\) equipped with the standard skew-symmetric form \(\omega((t, w), (t', w')) = tw' - wt'\). Considering \(V\) as an abelian group, it admits a non-trivial central extension \(H\) called the Heisenberg group. Concretely, the group \(H\) can be presented as the set \(H = V \times \mathbb{Z}/n\mathbb{Z}\) with the multiplication given by

\[(v, z) \cdot (v', z') = (v + v', z + z' + \frac{1}{2} \omega(v, v')).\]

The center of \(H\) is \(Z = Z(H) = \{(0, z) : z \in \mathbb{Z}/n\mathbb{Z}\}\). The symplectic group \(\text{Sp}(V, \omega)\), which in this case is isomorphic to \(\text{SL}_2(\mathbb{Z}/n\mathbb{Z})\), acts by automorphisms of \(H\) through its action on the \(V\)-coordinate.

2.2 The Heisenberg representation

One of the most important attributes of the group \(H\) is that it admits a special family of irreducible representations. The precise statement goes as follows. Let \(\psi : \mathbb{Z} \to \mathbb{C}^\times\) be a faithful character of the center (i.e. an imbedding of \(\mathbb{Z}\) into \(\mathbb{C}^\times\)). It is not hard to show

**Theorem 2.1 (Stone–von Neuman).** There exists a unique (up to isomorphism) irreducible representation \((\pi, H, \mathcal{H})\) with the center acting by \(\psi\), i.e. \(\pi|_Z = \psi \cdot 1_{\mathcal{H}}\).

The representation \(\pi\) which appears in the above theorem will be called the Heisenberg representation associated with the central character \(\psi\).

We denote by \(\psi_1(z) = e^{\frac{2\pi i}{n} z}\) the standard additive character, and for every invertible element \(a \in (\mathbb{Z}/n\mathbb{Z})^\times\), we denote \(\psi_a(z) = e^{\frac{2\pi i}{n} az}\).
2.2.1 Standard realization of the Heisenberg representation

The Heisenberg representation \((\pi, H, \mathcal{H})\) can be realized as follows: the Hilbert space is the space \(F_n = \mathbb{C}(\mathbb{Z}/n\mathbb{Z})\) of complex-valued functions on the finite field, with the standard Hermitian product. The action \(\pi\) is given by

- \(\pi(t, 0)[f](x) = f(x + t);\)
- \(\pi(0, w)[f](x) = \psi(wx) f(x);\)
- \(\pi(z)[f](x) = \psi(z) f(x), z \in \mathbb{Z}.

Here, we are using \(t\) to indicate the first coordinate of a typical element \(v \in V \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\) and \(w\) to indicate the second coordinate.

We call this explicit realization the standard realization.

2.3 The Weil representation

A direct consequence of Theorem 2.1 is the existence of a projective representation \(\tilde{\rho}_n: SL_2(\mathbb{Z}/n\mathbb{Z}) \rightarrow PGL(\mathcal{H})\). The construction of \(\tilde{\rho}_n\) out of the Heisenberg representation \(\pi\) is due to Weil [10], and it goes as follows: considering the Heisenberg representation \(\pi\) and an element \(g \in SL_2(\mathbb{Z}/n\mathbb{Z})\), one can define a new representation \(\pi^g\) acting on the same Hilbert space via \(\pi^g(h) = \pi(g(h))\). Clearly, both \(\pi\) and \(\pi^g\) have the same central character \(\psi\); hence, by Theorem 2.1, they are isomorphic. Since the space \(\text{Hom}_H(\pi, \pi^g)\) is one-dimensional, choosing for every \(g \in SL_2(\mathbb{Z}/n\mathbb{Z})\) a non-zero representative \(\tilde{\rho}_n(g) \in \text{Hom}_H(\pi, \pi^g)\) gives the required projective Weil representation. In more concrete terms, the projective representation \(\tilde{\rho}\) is characterized by the formula

\[
\tilde{\rho}_n(g) \pi(h) \tilde{\rho}_n(g)^{-1} = \pi(g(h)),
\]

for every \(g \in SL_2(\mathbb{Z}/n\mathbb{Z})\) and \(h \in H\). A more delicate statement is that there exists a lifting of \(\tilde{\rho}_n\) into a linear representation; this is the content of the following theorem

**Theorem 2.2.** The projective Weil representation \(\tilde{\rho}_n\) can be linearized into an honest representation

\[\rho_n: SL_2(\mathbb{Z}/n\mathbb{Z}) \rightarrow GL(\mathcal{H})\]

that satisfies equation (2.1).
The existence of a linearization $\rho_n$ follows from a known fact [1] that any projective representation of $SL_2(\mathbb{Z}/n\mathbb{Z})$ can be linearized (in case $n = p$ is a prime number, see also [5, 6] for an explicit construction of a canonical linearization).

Clearly, any two linearizations differ by a character $\chi$ of $SL_2(\mathbb{Z}/n\mathbb{Z})$. In addition, we have the following simple lemma:

**Lemma 2.3.** Let $\chi$ be a character of the group $SL_2(\mathbb{Z}/n\mathbb{Z})$, then $\chi^n = 1$. □

For a proof, see Section A.1.

**Remark 2.4.** In the case when $n$ is not divisible by 3, the group $SL_2(\mathbb{Z}/n\mathbb{Z})$ is perfect—i.e. does not have non-trivial characters—therefore, the representation $\rho_n$ is unique. The perfectness of $SL_2(\mathbb{Z}/n\mathbb{Z})$ can be proved as follows: Let $pr : SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/n\mathbb{Z})$ denote the canonical projection. Given a character $\chi : SL_2(\mathbb{Z}/n\mathbb{Z}) \to \mathbb{C}^\times$, its pull-back $\chi \circ pr$ satisfies $(\chi \circ pr)^{12} = 1$ since the group of characters of $SL_2(\mathbb{Z})$ is isomorphic to $\mathbb{Z}/12\mathbb{Z}$ [3]. Since $pr$ is surjective, this implies that $\chi^{12} = 1$. This combined with the facts that $\chi^n = 1$ (Lemma 2.3) and $\gcd(12, n) = 1$ implies that $\chi = 1$. □

**Notation 2.5.** The Weil representation $\rho_n$ depends on the central character $\psi$; hence, sometimes we will write $\rho_n[\psi]$ to emphasize this point. We will denote by $\rho_n$ the Weil representation associated with the standard character $\psi_1$. □

Let $n_1$ and $n_2$ be coprime odd integers. Consider the natural homomorphism

$$\mathbb{Z}/n_1n_2\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z},$$

which, by the Chinese reminder theorem, is an isomorphism. This isomorphism induces an isomorphism of Hilbert spaces $F_{n_1n_2} \xrightarrow{\sim} F_{n_1} \otimes F_{n_2}$ and an isomorphism of groups $SL_2(\mathbb{Z}/n_1n_2\mathbb{Z}) \xrightarrow{\sim} SL_2(\mathbb{Z}/n_1\mathbb{Z}) \times SL_2(\mathbb{Z}/n_2\mathbb{Z})$. In addition, the character $\psi_1 \otimes \psi_1$ of $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ transforms to the character $\psi_{n_1+n_2}$ of $\mathbb{Z}/n_1n_2\mathbb{Z}$. Under these identifications, it is not difficult to show

**Claim 2.6.** The representations $\rho_{n_1} \otimes \rho_{n_2}$ and $\rho_{n_1n_2}[\psi_{n_1+n_2}]$, realized on the Hilbert spaces $F_{n_1} \otimes F_{n_2}$ and $F_{n_1+n_2}$, coincide as projective representations of $SL_2(\mathbb{Z}/n_1n_2\mathbb{Z})$. □

**Remark 2.7.** The element $n_1 + n_2 \in (\mathbb{Z}/n_1n_2\mathbb{Z})^\times$, hence, the character $\psi_{n_1+n_2}$ is faithful. □
Remark 2.8. In the case \( n_1 \) and \( n_2 \) are in addition not divisible by 3, Claim 2.6 and Remark 2.4 imply that the representations \( \rho_{n_1 n_2} [\psi_{n_1 + n_2}] \) and \( \rho_{n_1} [\psi_1] \otimes \rho_{n_2} [\psi_1] \) coincide. \( \square \)

2.4 The character of the Weil representation

We denote by \( \text{ch}_\rho : SL_2(\mathbb{F}_p) \to \mathbb{C} \) the character of the Weil representation \( \rho = \rho_p [\psi] \) associated with the non-trivial additive character \( \psi \).

2.4.1 The dependence on the additive character

The character \( \text{ch}_\rho \) depends on the choice of \( \psi \); however, we have

Proposition 2.9. The characters \( \text{ch}_{\rho[\psi]} \) and \( \text{ch}_{\tilde{\rho}[\tilde{\psi}]} \), associated with two non-trivial additive characters \( \psi \) and \( \tilde{\psi} \), agree on regular semisimple elements of \( SL_2(\mathbb{F}_p) \) if \( p \neq 3 \) and differ by a character of \( SL_2(\mathbb{F}_p) \) if \( p = 3 \). \( \square \)

For a proof, see Section A.2.

2.4.2 Formula

In the case \( n = p \) is a prime number, the absolute value of the character \( \text{ch}_\rho \) was described in [7], but the phases have been made explicit only recently in [5]. The following formula is taken from [5]:

\[
\text{ch}_\rho(g) = \left( \frac{-\det(\kappa(g) + I)}{p} \right),
\]

(2.2)

for every \( g \in SL_2(\mathbb{F}_p) \) such that \( g - I \) is invertible, where \(( \cdot / p)\) is the Legendre symbol modulo \( p \) and \( \kappa(g) = (g + I)/(g - I) \) is the Cayley transform. Using the identity \( \kappa(g) + I = (2g)/(g - I) \), one can write (2.2) in the simpler form

\[
\text{ch}_\rho(g) = \left( \frac{-\det(g - I)}{p} \right).
\]

Remark 2.10. Sketch of the proof of (2.2) (see details in [5]). First observation is that the Heisenberg representation \( \pi \) and the Weil representation \( \rho = \rho_p \) combine to give
a representation of the semi-direct product $\tau = \rho \ltimes \pi : SL_2(\mathbb{F}_p) \ltimes H \to GL(H)$. Second observation is that the character of $\tau$, $ch_\tau : SL_2(\mathbb{F}_p) \ltimes H \to \mathbb{C}$, satisfies the following multiplicativity property

$$ch_\tau (g_1 \cdot g_2) = \frac{1}{\dim H} ch_\tau (g_1) * ch_\tau (g_2),$$

(2.3)

where $ch_\tau (g)$ denotes the function on $H$ given by $ch_\tau (g, \cdot)$ and the $*$ operation denotes convolution with respect to the Heisenberg group action. Now, one can easily show that

$$ch_\tau (g) (v, z) = \mu_g \cdot \psi \left( \frac{1}{4} \omega (\kappa (g) v, v) + z \right),$$

for $g \in SL_2(\mathbb{F}_p)$ with $g - I$ invertible and for some $\mu_g \in \mathbb{C}$. Finally, a direct calculation reveals that $\mu_g$ must equal $(- \det(\kappa(g) + I)/p)$ for (2.3) to hold. Restricting $ch_\tau$ to $SL_2(\mathbb{F}_p) \subset SL_2(\mathbb{F}_p) \ltimes H$, we obtain (2.2). □

**Remark 2.11.** Using similar methods to those developed in [5], we can show that

$$ch_{\rho_n} (g) = \left( \frac{- \det (g - I)}{n} \right),$$

where $\rho_n$ is the Weil representation of the group $SL_2(\mathbb{Z}/n\mathbb{Z})$, the element $g$ is such that $\det (g - I) \in (\mathbb{Z}/n\mathbb{Z})^*$, and $(\cdot / n)$ is the Jacobi symbol modulo $n$ (see Section 4.1). □

3 The DFT

3.1 The DFT

Given an additive character $\psi$, there is a DFT operator $F_n[\psi]$ acting on the Hilbert space $F_n = \mathbb{C}(\mathbb{Z}/n\mathbb{Z})$ by the formula (Usually, the DFT operator appears in its normalized form $\Phi_n = (1/\sqrt{n})F_n$, which makes it a unitary operator. However, the non-normalized form is better suited to our purposes.)

$$F_n[\psi] (f) (y) = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \psi (yx) f (x).$$
It is easy to show that $F_n[\psi]^2(f)(y) = n \cdot f(-y)$ and, hence, $F_n[\psi]^4 = n^2 \cdot \text{Id}$. 

**Notation 3.1.** We will denote by $F_n$ the DFT operator associated with the standard character $\psi_1$. □

It is not difficult to show that under the isomorphism $F_{n_1 n_2} \simeq F_{n_1} \otimes F_{n_2}$, we have

**Lemma 3.2.** The operators $F_{n_1} \otimes F_{n_2}$ and $F_{n_1 n_2} [\psi_{n_1 + n_2}]$ coincide. □

The main technical statement that we will require concerns the explicit evaluation of the determinant of the DFT operator which is associated with the standard character $\psi_1$.

**Proposition 3.3 (Main technical statement).** For any odd natural number $n$, we have

$$
\det (F_n) = i^{\frac{n(n-1)}{2}} n^\frac{n}{2}.
$$

(3.1)

□

For a proof, see Section A.3.

### 3.2 Relation between the DFT and the Weil representation

We will show that for an odd $n$, the operator $F_n$ is proportional to the operator $\rho_n(w)$ in the Weil representation, where $w \in SL_2(\mathbb{Z}/n\mathbb{Z})$ is the Weyl element

$$
w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.
$$

**Lemma 3.4 (Key lemma).** The operator $\rho_n(w)$ does not depend on the choice of linearization $\rho_n$. Moreover,

$$
F_n = C_n \cdot \rho_n(w),
$$

(3.2)

where $C_n = i^{\frac{n-1}{2}} \sqrt{n}$. □

For a proof, see Section A.4.
4 The Quadratic Reciprocity Law

We are ready to prove the quadratic reciprocity law. For a natural number \( n \), we define the Gauss sums [8]

\[
G_n(a) = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} e^{\frac{2\pi i}{n} ax^2},
\]

where \( a \in (\mathbb{Z}/n\mathbb{Z})^\times \), and we denote \( G_n = G_n(1) \).

Consider two distinct odd prime numbers \( p \) and \( q \). Using known identities of Gauss sums, we deduce that

**Lemma 4.1.** We have

\[
\left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = \frac{G_p \cdot G_q}{G_{pq}}.
\]

For a proof, see Section A.5.

The Gauss sum is related to the DFT by

\[
G_n = \text{Tr}(F_n). \tag{4.1}
\]

Hence, we can write

\[
\left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = \frac{\text{Tr}(F_p) \cdot \text{Tr}(F_q)}{\text{Tr}(F_{pq})} = \frac{C_p \cdot C_q}{C_{pq}} \cdot \frac{\text{Tr}(\rho_p(w)) \cdot \text{Tr}(\rho_q(w))}{\text{Tr}(\rho_{pq}(w))}
\]

\[
= \frac{C_p \cdot C_q}{C_{pq}} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}, \tag{4.2}
\]

where in the first equality, we used Equation (4.1) and Lemma 4.1; in the second and fourth equalities, we used Lemma 3.4. Finally, the third equality follows from the following crucial identity

**Proposition 4.2.** We have

\[
\text{Tr}(\rho_{pq}(w)) = \text{Tr}(\rho_p(w)) \cdot \text{Tr}(\rho_q(w)).
\]

For a proof, see Section A.6.
This completes our proof of Equation (1.1)—the Quadratic Reciprocity Law.

4.1 Quadratic reciprocity law for the Jacobi symbol

For an odd number \( n \in \mathbb{N} \), let \((\cdot/n)\) denote the Jacobi symbol of the multiplicative group \((\mathbb{Z}/n\mathbb{Z})^\times\), which can be characterized [2] by the condition

\[
G_n(a) = \left(\frac{a}{n}\right) G_n(1),
\]

(4.3)

for every \( a \in (\mathbb{Z}/n\mathbb{Z})^\times\).

**Remark 4.3.** The Jacobi symbol admits the following explicit description: when \( n = p \) is an odd prime number, the Jacobi symbol coincides with the Legendre character (Lemma A.3). If \( n = p_1^{k_1} \times \ldots \times p_l^{k_l} \) is the decomposition of \( n \) into a product of prime numbers, then it is easy to show that for \( a \in (\mathbb{Z}/n\mathbb{Z})^\times \),

\[
\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{k_1} \times \ldots \times \left(\frac{a}{p_l}\right)^{k_l}.
\]

In particular, this implies that the Jacobi symbol is a character of the multiplicative group \((\mathbb{Z}/n\mathbb{Z})^\times\), and it takes the values \( \pm 1 \).

The quadratic reciprocity law can be formulated in terms of the Jacobi symbol, for any two coprime odd numbers \( n_1, n_2 \); the general law is

\[
\left(\frac{n_1}{n_2}\right) \left(\frac{n_2}{n_1}\right) = (-1)^{\frac{n_1-1}{2} \cdot \frac{n_2-1}{2}}
\]

(4.4)

The proof we just described for the quadratic reciprocity law gives also the more general identity (4.4) without changes: using Equation (4.3), it is not hard to realize that the statement of Lemma 4.1 can be formulated more generally as

\[
\left(\frac{n_1}{n_2}\right) \left(\frac{n_2}{n_1}\right) = \frac{G_{n_1} \cdot G_{n_2}}{G_{n_1 n_2}}.
\]
Then applying the same derivation as in (4.2), one obtains

\[
\left( \frac{n_1}{n_2} \right) \left( \frac{n_2}{n_1} \right) = \frac{C_{n_1} \cdot C_{n_2}}{C_{n_1 n_2}} = (-1)^{\frac{n_1 - 1}{2} \frac{n_2 - 1}{2}}.
\]

4.2 Alternative interpretation

A slightly more transparent interpretation of the above argument proceeds as follows:

\[
1 = \frac{\operatorname{Tr}(F_{n_1}) \operatorname{Tr}(F_{n_2})}{\operatorname{Tr}(F_{n_1 n_2} \psi_{n_1 + n_2})} = \frac{C_{n_1} C_{n_2}}{C_{n_1 n_2} \psi_{n_1 + n_2}} \cdot \frac{\operatorname{Tr}(\rho_{n_1}(w)) \operatorname{Tr}(\rho_{n_2}(w))}{\operatorname{Tr}(\rho_{n_1 n_2}(\psi_{n_1 + n_2}))(w)},
\]

where the first equality follows from Lemma 3.2 and the second equality appears by substituting

- \( F_{n_1} = C_{n_1} \rho_{n_1}(w) \),
- \( F_{n_2} = C_{n_2} \rho_{n_2}(w) \),
- \( F_{n_1 n_2} \psi_{n_1 + n_2} = C_{n_1 n_2} \psi_{n_1 + n_2} \rho_{n_1 n_2} \psi_{n_1 + n_2}(w) \).

Now, by Claim 2.6, we have

\[
\frac{\operatorname{Tr}(\rho_{n_1}(w)) \operatorname{Tr}(\rho_{n_2}(w))}{\operatorname{Tr}(\rho_{n_1 n_2}(\psi_{n_1 + n_2}))(w)} = 1.
\]

Hence, the quadratic reciprocity law follows from the equivariance property of the proportionality constant \( C \):

**Proposition 4.4.** Let \( n \in \mathbb{N} \) be an odd number. We have

\[
C_n[\psi_a] = \left( \frac{a}{n} \right) C_n[\psi_1],
\]

for every \( a \in (\mathbb{Z}/n\mathbb{Z})^\times \). \( \square \)

**Remark 4.5.** In our approach, the above identity is a non-trivial corollary of the proof of the quadratic reciprocity law. \( \square \)
5 The Sign of the Gauss Sum

The exact evaluation of $G_p$ for an odd prime $p$ uses an additional fact about the Weil representation, i.e. the evaluation

$$\text{Tr}(\rho_p(w)) = \text{ch}_{\rho_p}(w) = \left(\frac{-2}{p}\right).$$

which follows directly from formula (2.2). The explicit evaluation of the Legendre symbol at $-2$ is a simple and well-known computation (see [9]) which gives $(-2/p) = (-1/p)(2/p) = (-1)^{p-1} (-1)^{p^2-1}$. Now using (4.1), we conclude that

$$G_p = \text{Tr}(F_p) = C_p \cdot \text{Tr}(\rho_p(w))
= i^{p-1} \sqrt{p} \cdot \left(\frac{-2}{p}\right) = \begin{cases} \sqrt{p}, & p \equiv 1 \pmod{4}, \\ i\sqrt{p}, & p \equiv 3 \pmod{4}. \end{cases}$$

This completes our proof of equation (1.2)—the Sign of Gauss Sum.

5.1 The sign of the Gauss sum modulo $n$

The exact evaluation of the Gauss sum for a general odd natural number $n$ can also be derived using the above formalism and the more general formula for the character of the Weil representation given in Remark 2.11. We obtain

$$G_n = \text{Tr}(F_n) = C_n \cdot \text{Tr}(\rho_n(w))
= i^{n-1} \sqrt{n} \cdot \left(\frac{-2}{n}\right) = \begin{cases} \sqrt{n}, & n \equiv 1 \pmod{4}, \\ i\sqrt{n}, & n \equiv 3 \pmod{4}. \end{cases}$$

Acknowledgements

The first two authors would like to thank their teacher J. Bernstein for his interest and guidance. They would also like to acknowledge M. Nori for the encouragement to write this paper. They thank C.P. Mok for explaining parts from the known proofs of quadratic reciprocity and T. Schedler for helping with various of the computations. We appreciate the time T.Y. Lam spent with us teaching math and history. Finally, we thank M. Baruch, P. Diaconis, M. Haiman, B. Poonen, and K. Ribet for the opportunities to present this work at the Technion, Israel, and the Mathematical Sciences Research Institute, Research Training Group in Representation Theory, Geometry and Combinatorics, and Number Theory Seminars at Berkeley during February 2008.
A Proof of Statements

A.1 Proof of Lemma 2.3

Let $\chi$ be a character of $SL_2(\mathbb{Z}/n\mathbb{Z})$. The condition $\chi^n = 1$ follows from the basic fact that the group $SL_2(\mathbb{Z}/n\mathbb{Z})$ is generated by the unipotent elements [3]:

$$u_+ = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad u_- = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

which satisfy $u_+^n = u_-^n = Id$.

A.2 Proof of Proposition 2.9

Let $\psi$ and $\tilde{\psi}$ be two non-trivial additive characters of the finite field $\mathbb{F}_p$. There exists an element $a \in \mathbb{F}_p^*$ such that $\tilde{\psi}(x) = \psi(ax)$ for every $x \in \mathbb{F}_p$. Let $A \in GL_2(\mathbb{F}_p)$ with $\det(A) = a$, and consider the conjugate representation $Ad_A[\psi]$ given by $Ad_A[\psi](g) = \rho(d_Ag)$. Using the identity (2.1), it is easy to see that $Ad_A[\psi]$ and $\rho[\tilde{\psi}]$ differ by a character of $SL_2(\mathbb{F}_p)$. Moreover, the group of characters of $SL_2(\mathbb{F}_p)$ is trivial when $p \neq 3$ (Remark 2.4).

It is enough to show that for a regular semisimple element $s \in SL_2(\mathbb{F}_p)$, there exist $g \in SL_2(\mathbb{F}_p)$ such that $Ad_g s = Ad_s$. This follows from the following general statement about conjugacy classes of regular semisimple elements in $SL_2(\mathbb{F}_p)$:

**Claim A.1.** Let $s$ and $s' \in SL_2(\mathbb{F}_p)$ be regular semisimple elements. Assume that there exists an element $A \in GL_2(\mathbb{F}_p)$ such that $Ad_A s = s'$. Then there exists an element $g \in SL_2(\mathbb{F}_p)$ such that $Ad_g s = s'$.

This concludes the proof of the proposition.

A.2.1 Proof of Claim A.1.

Find $A \in GL_2(\mathbb{F}_p)$ such that $As = s'A$. Let $d = \det(A)$. It is enough to find a matrix $B$ in the centralizer of $s$ such that $\det(B) = d^{-1}$. The centralizer of $s$ is a semisimple commutative algebra $K$ over $\mathbb{F}_p$, and hence, it is isomorphic either to $\mathbb{F}_p \times \mathbb{F}_p$ or to $\mathbb{F}_{p^2}$. So we use the following standard lemma:

**Lemma A.2.** The norm map $N : K \to \mathbb{F}_p^*$ is onto. \qed
This concludes the proof of the claim.

A.3 Proof of Proposition 3.3

We work with the model of $\mathbb{Z}/n\mathbb{Z}$ as the set $0, 1, 2, \ldots, n-1$ with addition and multiplication modulo $n$. If we write $\psi$ in the form $\psi(x) = \zeta^x$, $x = 0, \ldots, n-1$, and $\zeta = e^{2\pi i/n}$, then the matrix of $F_n$ takes the form $(\zeta^{xy} : x, y \in \{0, 1, \ldots, n-1\})$; hence, it is a Vandermonde matrix. Applying the standard formula \cite{4} for the determinant of a Vandermonde matrix, we get

$$\det(F_n) = \prod_{0 \leq x < y \leq n-1} (\zeta^y - \zeta^x) \tag{A.1}$$

where the equality $\prod_{0 \leq x < y \leq n-1} \zeta^{x+y/2} = \zeta^0$ follows from the fact that

$$\sum_{0 \leq x < y \leq n-1} (x + y) = \frac{1}{2} \left( \sum_{x, y \in \mathbb{Z}/n\mathbb{Z}} (x + y) - \sum_{x = y \in \mathbb{Z}/n\mathbb{Z}} (x + y) \right) = 0 - 0 = 0.$$

Now, taking the absolute value on both sides of (A.1), using $F_n^4 = n^2 \cdot Id$ and the positivity of $\prod_{j=1}^{n-1} (\sin(\tau j/n))^{n-j}$, gives us

$$n^2 = 2^{\frac{mn-1}{2}} \prod_{j=1}^{n-1} (\sin(\tau j/n))^{n-j};$$

hence, $\det(F_n) = i^{\frac{mn-1}{2}} n^2$.

This concludes the proof of the proposition. $\blacksquare$

A.4 Proof of Lemma 3.4

First, we explain why the operator $\rho_n(w)$ does not depend on the choice of linearization $\rho_n$. Any two linearization differ by a character $\chi$ of $SL_2(\mathbb{Z}/n\mathbb{Z})$; therefore, it is
enough to show that $\chi(w) = 1$. By Lemma 2.3, $\chi^n = 1$; hence, $\chi(w) = 1$ since $w^4 = 1$ and $\gcd(4, n) = 1$.

Next, we explain the relation $F_n = C_n \cdot \rho_n(w)$. The operator $\rho_n(w)$ is characterized up to a unitary scalar by the identity (see formula (2.1)) $\rho_n(w) \pi(h) \rho_n(w)^{-1} = \pi(w(h))$ for every $h \in H$. Explicit computation reveals that for every $h \in H$, $F_n \circ \pi(h) \circ F_n^{-1} = \pi(w(h))$, which implies that

$$F_n = C_n \cdot \rho_n(w).$$

Finally, we evaluate the proportionality coefficient $C_n$. Computing determinants, one obtains $\det(F_n) = C_n^\ast \cdot \det(\rho_n(w))$. Arguing as above, the character $\chi = \det \circ \rho_n$ satisfies $\chi(w) = 1$. Hence,

$$\det(F_n) = C_n^\ast. \tag{A.2}$$

The relations $F_n^4 = n^2 \cdot \text{Id}$ and $\rho_n(w)^4 = \text{Id}$ imply that $C_n^4 = n^2$. By Proposition 3.3, Equation (A.2) and using $\gcd(4, n) = 1$, one obtains that $C_n = i^{\frac{n-1}{2}} \sqrt{n}$.

This concludes the proof of the Theorem. \hfill \blacksquare

A.5 Proof of Lemma 4.1

Consider the isomorphism $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \rightarrow \mathbb{Z}/pq\mathbb{Z}$, given by $(x, y) \mapsto x \cdot q + y \cdot p$. Now write

$$G_{pq} = \sum_{z \in \mathbb{Z}/pq\mathbb{Z}} e^{2\pi i z^2} = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \sum_{y \in \mathbb{Z}/q\mathbb{Z}} e^{2\pi i (xq + yp)^2}$$

$$= \sum_{x \in \mathbb{F}_p} e^{2\pi i qx^2} \sum_{y \in \mathbb{F}_q} e^{2\pi i py^2} = \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) G_p \cdot G_q,$$

where in the last equality, we used

**Lemma A.3.** For every $a \in \mathbb{F}_p^*$

$$\sum_{x \in \mathbb{F}_p} e^{2\pi i ax^2} = \left(\frac{a}{p}\right) \sum_{x \in \mathbb{F}_p} e^{2\pi i x^2}. \tag{□}$$

This concludes the proof of the Lemma 4.1.
A.5.1 Proof of Lemma A.3

The statement follows from the following basic identity

\[ \sum_{x \in \mathbb{F}_p} e^{\frac{2\pi i}{p} ax^2} = \sum_{x \in \mathbb{F}_p} e^{\frac{2\pi i}{p} ax} \left( \frac{x}{p} \right), \]  

which can be explained by observing that both sides are equal to \( \sum_{x \in \mathbb{F}_p} e^{\frac{2\pi i}{p} ax} (1 + (x/p)) \).

Now using (A.3), we can write

\[ \sum_{x \in \mathbb{F}_p} e^{\frac{2\pi i}{p} ax^2} = \sum_{x \in \mathbb{F}_p} e^{\frac{2\pi i}{p} a \cdot x} = \sum_{x \in \mathbb{F}_p} e^{\frac{2\pi i}{p} a^{-1} \cdot x} \]

\[ = \left( \frac{a^{-1}}{p} \right) \sum_{x \in \mathbb{F}_p} e^{\frac{2\pi i}{p} a^{-1} \cdot x} = \left( \frac{a}{p} \right) \sum_{x \in \mathbb{F}_p} e^{\frac{2\pi i}{p} x^2}, \]

where, in the second equality, we applied a change of variables \( x \mapsto ax \). This concludes the proof of the lemma. \( \blacksquare \)

A.6 Proof of Proposition 4.2

We proceed as in Claim 2.6. For any characters \( \psi \) and \( \psi' \) of \( \mathbb{Z}/p\mathbb{Z} \) and \( \mathbb{Z}/q\mathbb{Z} \), the representations \( \rho_p[\psi] \otimes \rho_q[\psi'] \) and \( \rho_{pq}[\varphi] \), where \( \varphi \) is a corresponding character of \( \mathbb{Z}/pq\mathbb{Z} \), differ by a character \( \chi \) of the group \( SL_2(\mathbb{Z}/pq\mathbb{Z}) \). Since \( \chi \) is of odd order (see Lemma 2.3) and \( w^4 = 1 \), we have \( \chi(w) = 1 \). Consequently, we get

\[ Tr(\rho_{pq}[\varphi](w)) = Tr(\rho_p[\psi](w)) \cdot Tr(\rho_q[\psi'](w)). \]  

(A.4)

Since \( w \) is regular semisimple, by Proposition 2.9, the right-hand side of (A.4) does not depend on \( \psi \) and \( \psi' \). Running over all pairs \( \psi \) and \( \psi' \), we recover all faithful characters \( \varphi \). Hence, the left-hand side is independent of the specific additive character \( \varphi \).

This concludes the proof of the proposition. \( \blacksquare \)

References


