ANALYTIC APPROACH TO QUADRATIC RECIPROCITY

We apply Jacobi's theta functions to give an analytic proof of quadratic reciprocity.

For an odd prime p, the Legendre symbol $\left(\frac{m}{p}\right)$ is 1 if p does not divide m and m is quadratic residue modulo p in the sense that m is congruent to the square of an integer modulo p. The Legendre symbol $\left(\frac{m}{p}\right)$ is -1 if p does not divide m and m is not a quadratic residue modulo p. The Legendre symbol $\left(\frac{m}{p}\right)$ is 0 if p divides m. Because r^2 is congruent to $(p-r)^2$ modulo p, we know that there are $\frac{p-1}{2}$ quadratic residues modulo p and $\frac{p-1}{2}$ quadratic nonresidues modulo p among the numbers between 1 and $p-1$. The statement of quadratic reciprocity is that for any unequal odd primes m and n we have

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}.$$

As an application of the Jacobian theta functions, we are going to prove the quadratic reciprocity as a consequence of the following relation between $\vartheta_3(w,\tau)$ and $\vartheta_3\left(\frac{w}{\tau}, -\frac{1}{\tau}\right)$.

$$\exp\left(\frac{iw^2}{\pi\tau}\right)\vartheta_3(w,\tau) = \sqrt{\frac{i}{\tau}}\vartheta_3\left(\frac{w}{\tau}, -\frac{1}{\tau}\right).$$

Using

$$\vartheta_3(w) = 1 + 2\sum_{n=1}^{\infty} q^{n^2}\cos 2nw = \sum_{n=-\infty}^{\infty}\exp\left(\pi i\tau n^2 + 2niw\right),$$

we rewrite the relation as

$$(\dagger)\qquad \begin{aligned}&\exp\left(\frac{iw^2}{\pi\tau}\right)\sum_{n=-\infty}^{\infty}\exp\left(\pi i\tau n^2 + 2niw\right)\\ =&\sqrt{\frac{i}{\tau}}\sum_{n=-\infty}^{\infty}\exp\left(-\frac{\pi i n^2}{\tau} + \frac{2niw}{\tau}\right).\end{aligned}$$

Completion of Squares in Exponent of Left-Hand Side of (†). In the equation (†) we would like to absorb the first factor on the left-hand into the infinite

sum to complete the square in the exponent of the terms of the infinite sum. Since

$$\frac{iw^2}{\pi\tau} + \pi i\tau n^2 + 2niw = i\pi\tau\left(\frac{w}{\pi\tau} + n\right)^2,$$

we can set $w = \pi v\tau$ with v as the new variable to get

$$\frac{iw^2}{\pi\tau} + \pi i\tau n^2 + 2niw = i\pi\tau v^2 + \pi i\tau n^2 + 2ni\pi\tau v = i\pi\tau(v+n)^2$$

so that

$$\sum_{n=-\infty}^{\infty} \exp(\pi i\tau(n+v)^2) = \sqrt{\frac{i}{\tau}} \sum_{n=-\infty}^{\infty} \exp(-\pi i n^2/\tau + 2\pi i n v) \tag{1}$$

after we set $w = \pi v\tau$. This identity is the basis for the quadratic reciprocity. In order to get

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

We are going to take advantage of τ appearing in the exponent on the left-hand side of (1) and $\frac{1}{\tau}$ appearing in the exponent of the right-hand side of (1) and attempt to make τ behave like $\frac{a}{b}$ and $\frac{1}{\tau}$ behave like $\frac{b}{a}$. Since the imaginary part of τ must be positive, our best choice will be to set $\tau = \frac{a}{b} + \varepsilon i$ with $\varepsilon > 0$ and then to let ε approach 0 at the end. We are going to cancel the limits of the contributions on the left-hand side and the right-hand side of (1), as $\varepsilon \to 0$, to end up with an identity of finite sums on both sides of the equation. This cancellation relies on finite sums of periods a and b and we will proceed to do it now.

Use of Periodicity to Go from Identity for Infinite Series to Identity for Finite Series. First we explain in a general setting the technique of using periodicity to go from an identity for infinite series to an identity for finite series. Then we will apply this technique to get an identity for finite series (known as the theorem of Cauchy-Kronecker) from the identity for the infinite series

$$\sum_{n=-\infty}^{\infty} \exp(\pi i\tau(n+v)^2) = \sqrt{\frac{i}{\tau}} \sum_{n=-\infty}^{\infty} \exp(-\pi i n^2/\tau + 2\pi i n v) \tag{1}$$

with the substitution $\tau = \frac{a}{b} + \varepsilon i$. Here a and b are just two integers without any assumption of either being an odd prime.

Consider an infinite series

$$\sum_n \varphi(n)\psi_\varepsilon(n)$$

with $\varphi(n)$ being periodic in n with period b. We can use the decomposition $m = nb + h$ with $0 \le h \le b-1$ and the periodicity of $\varphi(n)$ in n with period b to rewrite the series as

$$\sum_{h=1}^{b} \varphi(h) \sum_n \psi_\varepsilon(h+nb).$$

We introduce

$$\Psi_\varepsilon(h) = \sum_n \psi_\varepsilon(h+nb)$$

for $1 \le h \le b$. When we have a similar setup

$$\sum_n \hat{\varphi}(n)\hat{\psi}_\varepsilon(n)$$

with $\hat{\varphi}(n)$ being periodic in n with period a, we can rewrite

$$\sum_n \hat{\varphi}(n)\hat{\psi}_\varepsilon(n) = \sum_{h=1}^{a} \hat{\varphi}(h) \sum_n \hat{\psi}_\varepsilon(h+na)$$

and introduce

$$\hat{\Psi}_\varepsilon(h) = \sum_n \hat{\psi}_\varepsilon(h+na)$$

for $1 \le h \le a$. Suppose we start out with

$$\sum_n \varphi(n)\psi_\varepsilon(n) = \sum_n \hat{\varphi}(n)\hat{\psi}_\varepsilon(n).$$

If we know that there exist a function θ_ε and a constant γ such that $\Psi_\varepsilon(h)$ is asymptotically the same as θ_ε and $\hat{\Psi}_\varepsilon(h)$ is asymptotically the same as $\gamma\theta_\varepsilon$ as $\varepsilon \to 0^+$ for all h, then we obtain the following identity for finite sums.

$$\sum_{h=1}^{b} \varphi(n) = \gamma \sum_{h=1}^{a} \hat{\varphi}(n)$$

We now apply this general setup to our situation at hand.

Application of Technique of Construction of Identity for Finite Series to Identity of the Third Jacobian Theta Function. The term $\varphi(n)$ is going to be

$$\exp\left(\pi i\frac{a}{b}(n+v)^2\right)$$

and we would like to make it periodic in n with period b. It would be the case if

$$\pi i\frac{a}{b}(n+v+b)^2-\pi i\frac{a}{b}(n+v)^2\in 2\pi i\mathbb{Z}$$

which is the same as

$$\frac{a}{b}(n+v+b)^2-\frac{a}{b}(n+v)^2\in 2\mathbb{Z}$$

Now,

$$\frac{a}{b}(n+v+b)^2-\frac{a}{b}(n+v)^2=2an+2av+ab$$

which belongs to $2\mathbb{Z}$ if and only if $2av+ab\in 2\mathbb{Z}$. Recall that the variable v comes from $w=\pi v\tau$ and we are free to choose a value for the variable w. We now make the decision to choose v as a rational number with the property that $2av+ab\in 2\mathbb{Z}$.

The term $\hat{\varphi}(n)$ is going to be

$$\exp\left(-\pi i n^2\frac{b}{a}+2\pi i n v\right)$$

and we would like to make it periodic in n with period a. It would be the case if

$$\left(-\pi i(n+a)^2\frac{b}{a}+2\pi i(n+a)v\right)-\left(-\pi i n^2\frac{b}{a}+2\pi i n v\right)\in 2\pi i\mathbb{Z}$$

which is the same as

$$\left(-(n+a)^2\frac{b}{a}+2(n+a)v\right)-\left(-n^2\frac{b}{a}+2nv\right)\in 2\mathbb{Z}.$$

Since

$$\left(-(n+a)^2\frac{b}{a}+2(n+a)v\right)-\left(-n^2\frac{b}{a}+2nv\right)=-2nb-ab+2av$$

and we know that $-2nb-2ab\in 2\mathbb{Z}$, it follows that $-2nb-ab+2av$ is in $2\mathbb{Z}$ if and only if $2av+ab\in 2\mathbb{Z}$, but the choice of v as explained above already satisfies the condition $2av+ab\in 2\mathbb{Z}$.

We now look at the functions $\psi_\varepsilon(n)$ and $\hat{\psi}_\varepsilon(n)$ we will get when we set $\tau = \frac{a}{b} + \varepsilon i$ in the identity

$$(1) \qquad \sum_{n=-\infty}^{\infty} \exp(\pi i \tau (n+v)^2) = \sqrt{\frac{i}{\tau}} \sum_{n=-\infty}^{\infty} \exp(-\pi i n^2/\tau + 2\pi i n v)$$

from the identity for the third Jacobian theta function.

Asymptotic Behavior as $\operatorname{Im}\tau \to 0^+$. Recall that we set $\tau = \frac{a}{b} + i\,\varepsilon$ for some $\varepsilon > 0$ which later will approach zero. Also recall that we let v be a rational number such that $ab + 2av$ is an even integer. As we have seen earlier, this condition on v is to make that the following two statements hold.

(i) $\exp\left(\pi i \frac{a}{b}(n+v)^2\right)$ is periodic in n with period b.

(ii) $\exp\left(-\pi i n^2 \frac{b}{a} + 2\pi i n v\right)$ is periodic in n with period a.

The substitution of $\tau = \frac{a}{b} + i\,\varepsilon$ is done in the identity

$$(1) \qquad \sum_{n=-\infty}^{\infty} \exp(\pi i \tau (n+v)^2) = \sqrt{\frac{i}{\tau}} \sum_{n=-\infty}^{\infty} \exp(-\pi i n^2/\tau + 2\pi i n v).$$

The left-hand side of (1) now becomes

$$\sum_{n=-\infty}^{\infty} \exp\left(\pi i \frac{a}{b}(n+v)^2 - \pi\,\varepsilon (n+v)^2\right) = \sum_{n=-\infty}^{\infty} \exp\left(\pi i \frac{a}{b}(n+v)^2\right) \exp\left(-\pi\,\varepsilon (n+v)^2\right).$$

In terms of the notations we introduced earlier, we have

$$\varphi(n) = \exp\left(\pi i \frac{a}{b}(n+v)^2\right)$$

and

$$\psi_\varepsilon(n) = \exp\left(-\pi\,\varepsilon (n+v)^2\right)$$

so that

$$\Psi_\varepsilon(h) = \sum_{n=-\infty}^{\infty} \exp\left(-\pi\,\varepsilon (nb+h+v)^2\right) = \sum_{n=-\infty}^{\infty} \exp\left(-\pi\,\varepsilon\, b^2 \left(n + \frac{v+h}{b}\right)^2\right).$$

The right-hand side of (1) now becomes

$$\sqrt{\frac{i}{\frac{a}{b}+i\varepsilon}}\sum_{n=-\infty}^{\infty}\exp\left(-\frac{\pi i n^2}{\frac{a}{b}+i\varepsilon}+2\pi i n v\right)$$

which can be written as

$$\sqrt{\frac{i}{\frac{a}{b}+i\varepsilon}}\sum_{n=-\infty}^{\infty}\exp\left(-\pi i n^2\frac{b}{a}-\frac{\pi\, n^2\frac{b}{a}\varepsilon}{\frac{a}{b}+i\varepsilon}+2\pi i n v\right)$$

after we rewrite

$$\frac{1}{\frac{a}{b}+i\varepsilon}$$

as

$$\frac{b}{a}-\frac{b}{a}\frac{i\varepsilon}{\frac{a}{b}+i\varepsilon}$$

inside the exponent in order to more readily see its limit as $\varepsilon\to 0$. We put it in the form

$$\sum_{n=-\infty}^{\infty}\exp\left(-\pi i n^2\frac{b}{a}+2\pi i n v\right)\sqrt{\frac{i}{\frac{a}{b}+i\varepsilon}}\exp\left(-\frac{\pi\, n^2\frac{b}{a}\varepsilon}{\frac{a}{b}+i\varepsilon}\right)$$

so that in terms of the notations we introduced earlier, we have

$$\hat{\varphi}(n)=\exp\left(-\pi i n^2\frac{b}{a}+2\pi i n v\right)$$

and

$$\hat{\psi}_\varepsilon(n)=\sqrt{\frac{i}{\frac{a}{b}+i\varepsilon}}\exp\left(-\frac{\pi\, n^2\frac{b}{a}\varepsilon}{\frac{a}{b}+i\varepsilon}\right)$$

and

$$\hat{\Psi}_\varepsilon(h)=\sqrt{\frac{i}{\frac{a}{b}+i\varepsilon}}\sum_{n=-\infty}^{\infty}\exp\left(-\frac{\pi\,(h+na)^2\frac{b}{a}\varepsilon}{\frac{a}{b}+i\varepsilon}\right).$$

Determination of Asymptotic Behavior of $\Psi_\varepsilon(h)$ *as* $\varepsilon\to 0^+$. We now determine the asymptotic behavior of

$$\Psi_\varepsilon(h)=\sum_{n=-\infty}^{\infty}\exp\left(-\pi\,\varepsilon\, b^2\left(n+\frac{v+h}{b}\right)^2\right)$$

as $\varepsilon \to 0^+$. Each term becomes 1 as $\varepsilon \to 0$ and we know that the sum blows up. To determine how it blows up, we use once more the identity

$$(1) \qquad \sum_{n=-\infty}^{\infty} \exp\left(\pi i \tau (n+v)^2\right) = \sqrt{\frac{i}{\tau}} \sum_{n=-\infty}^{\infty} \exp\left(-\frac{\pi i n^2}{\tau} + 2\pi i n v\right)$$

and replace τ by $\varepsilon i b^2$ and replace v by $\frac{v+h}{b}$. Then we get

$$\sum_{n=-\infty}^{\infty} \exp\left(-\pi\, \varepsilon\, b^2 \left(n + \frac{v+h}{b}\right)^2\right)$$
$$= \sqrt{\frac{1}{\varepsilon b^2}} \sum_{n=-\infty}^{\infty} \exp\left(-\frac{\pi n^2}{\varepsilon b^2} + 2\pi i n \frac{v+h}{b}\right).$$

Now each term in the sum

$$\sum_{n=-\infty}^{\infty} \exp\left(-\frac{\pi n^2}{\varepsilon b^2} + 2\pi i n \frac{v+h}{b}\right)$$

goes to zero as $\varepsilon \to 0$ except when $n = 0$. We can also estimate the rate at which each term (with $n \neq 0$) goes to zero and we conclude that

$$\sum_{n=-\infty}^{\infty} \exp\left(-\frac{\pi n^2}{\varepsilon b^2} + 2\pi i n \frac{v+h}{b}\right)$$

approaches 1 as $\varepsilon \to 0$. The estimation comes from the inequality

$$\sum_{n=1}^{\infty} \exp(-cn^2) \leq \sum_{n=1}^{\infty} \exp(-cn) = \frac{e^{-c}}{1-e^{-c}}$$

which approaches 0 as $c \to \infty$. Thus $\Psi_\varepsilon(h)$ is asymptotically the same as

$$\frac{1}{\sqrt{\varepsilon} b}$$

as $\varepsilon \to 0$. In the notations introduced earlier, the function θ_ε is

$$\frac{1}{\sqrt{\varepsilon} b}.$$

Determination of Asymptotic Behavior of $\hat{\Psi}_\varepsilon(h)$ *as* $\varepsilon \to 0^+$. Write

$$\begin{aligned}\sqrt{\frac{\frac{a}{b}+i\varepsilon}{i}}\hat{\Psi}_\varepsilon(h) &= \sum_{n=-\infty}^{\infty} \exp\left(-\frac{\pi\,(h+na)^2\frac{b}{a}\varepsilon}{\frac{a}{b}+i\varepsilon}\right)\\ &= \sum_{n=-\infty}^{\infty} \exp\left(-\pi\left(\frac{h}{a}+n\right)^2\frac{b^2\varepsilon}{1+i\varepsilon\frac{b}{a}}\right)\end{aligned}$$

As before, each term in the infinite sum

$$\sum_{n=-\infty}^{\infty} \exp\left(-\pi\left(\frac{h}{a}+n\right)^2\frac{b^2\varepsilon}{1+i\varepsilon\frac{b}{a}}\right)$$

becomes 1 as $\varepsilon \to 0$ and we have to get a more precise asymptotic behavior by using the identity

$$(1)\qquad \sum_{n=-\infty}^{\infty} \exp\left(\pi i\tau(n+v)^2\right) = \sqrt{\frac{i}{\tau}}\sum_{n=-\infty}^{\infty} \exp\left(-\frac{\pi i n^2}{\tau}+2\pi i n v\right)$$

with

$$\tau = \frac{ib^2\varepsilon}{1+i\varepsilon\frac{b}{a}}$$

and $v = \frac{h}{a}$. We have

$$\begin{aligned}&\sum_{n=-\infty}^{\infty} \exp\left(\frac{-\pi(\frac{h}{a}+n)^2b^2\varepsilon}{1+i\varepsilon\frac{b}{a}}\right)\\ =&\sqrt{\frac{1+i\varepsilon\frac{b}{a}}{b^2\varepsilon}}\sum_{n=-\infty}^{\infty} \exp\left(\frac{-\pi n^2\left(1+i\varepsilon\frac{b}{a}\right)}{b^2\varepsilon}+\frac{2\pi i n h}{a}\right)\\ =&\sqrt{\frac{1+i\varepsilon\frac{b}{a}}{b^2\varepsilon}}\sum_{n=-\infty}^{\infty} \exp\left(\frac{-\pi n^2}{b^2\varepsilon}-\frac{\pi n^2 i}{ab}+\frac{2\pi i n h}{a}\right).\end{aligned}$$

As before, the sum

$$\sum_{n=-\infty}^{\infty} \exp\left(-\frac{\pi n^2}{b^2\varepsilon}-\frac{\pi n^2 i}{ab}+\frac{2\pi i n h}{a}\right)$$

approaches 1 as $\varepsilon \to 0$. Thus asymptotically $\hat{\Psi}_\varepsilon(h)$ is the same as

$$\sqrt{\frac{i}{\frac{a}{b}+i\varepsilon}}\sqrt{\frac{1+i\varepsilon\frac{b}{a}}{b^2\varepsilon}}$$

which is the same as

$$e^{\frac{\pi i}{4}}\sqrt{\frac{b}{a}}\,\frac{1}{\sqrt{\varepsilon}b}$$

as $\varepsilon \to 0$. In the notations introduced earlier, the function θ_ε is

$$\frac{1}{\sqrt{\varepsilon}b}$$

and

$$\gamma = e^{\frac{\pi i}{4}}\sqrt{\frac{b}{a}}.$$

From our earlier statement

$$\sum_{h=1}^{b}\varphi(n) = \gamma\sum_{h=1}^{a}\hat{\varphi}(n),$$

we obtain the following theorem.

Theorem (Cauchy-Kronecker). Let a and b be positive integers and v be a rational number such that $ab+2av$ is an even integer. Then

$$\frac{1}{\sqrt{b}}\sum_{h=1}^{b}\exp\left(\pi i\frac{a}{b}(h+v)^2\right) = \frac{e^{\frac{\pi i}{4}}}{\sqrt{a}}\sum_{h=1}^{a}\exp\left(-\pi i h^2\frac{b}{a}+2\pi i h v\right). \tag{2}$$

Expanding the square in the exponents of the terms on the left-hand side of (2), we get

$$\frac{1}{\sqrt{b}}\sum_{h=1}^{b}\exp\left(\pi i\frac{a}{b}h^2+\pi i\frac{a}{b}2hv+\pi i\frac{a}{b}v^2\right) = \frac{e^{\frac{\pi i}{4}}}{\sqrt{a}}\sum_{h=1}^{a}\exp\left(-\pi i h^2\frac{b}{a}+2\pi i h v\right).$$

We would like the exponents of the terms on the left-hand side to be like those on the right-hand side after interchanging a and b. A comparison of the first terms in the exponents from sides suggests setting $v=b$. Actually setting $v=\frac{b}{2}$ will do the same thing and will turn out to more useful in the

next step because of the factor 4 in the denominator of the exponent in the statement of quadratic reciprocity

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}.$$

So with $v = \frac{b}{2}$ we get from (2)
(3)

$$\frac{1}{\sqrt{b}}\sum_{h=1}^{b}\exp\left(\pi i\frac{a}{b}h^2 + \pi iah + \frac{\pi iab}{4}\right) = \frac{e^{\frac{\pi i}{4}}}{\sqrt{a}}\sum_{h=1}^{a}\exp\left(-\pi ih^2\frac{b}{a} + \pi ihb\right).$$

We can move the third term in the exponent on the left-hand side of (3) to the right-hand side of (3) to yield

$$\frac{1}{\sqrt{b}}\sum_{h=1}^{b}\exp\left(\pi i\frac{a}{b}h^2 + \pi iah\right) = e^{\frac{(1-ab)\pi i}{4}}\frac{1}{\sqrt{a}}\sum_{h=1}^{a}\exp\left(-\pi ih^2\frac{b}{a} - \pi ihb\right). \tag{4}$$

Gauss Sum and its Relation to Legendre Symbol. We introduce the *Gauss sum*

$$G(m,n) = \sum_{h=1}^{n}\exp\left(\pi i\frac{m}{n}h^2 + \pi imh\right) \tag{5}$$

so that we can rewrite the above expression (4) in the form

$$\frac{1}{\sqrt{b}}\,G(a,b) = e^{\frac{(1-ab)\pi i}{4}}\frac{1}{\sqrt{a}}\,G(-b,a). \tag{6}$$

The quadratic reciprocity will follow from this identity involving Gauss sums.

The first important observation is that, independent of the identity from the third theta function of Jacobi, we have the following *relation between the Gauss sum and the Legendre symbol*

$$G(m,n) = \left(\frac{m}{n}\right)G(1,n). \tag{7}$$

This comes just from the definition of quadratic residue and $G(m,n)$. Let us assume this first and use the identity from the third theta function of Jacobi to verify the law of quadratic reciprocity.

Proof of Quadratic Reciprocity under Assumption of Relation between Gauss Sum and Legendre Symbol. Let $\rho = e^{\frac{\pi i}{4}}$. From the identity (6) (with $a = 1$ and $b = n$) we get

$$\frac{1}{\sqrt{n}}\, G(1,n) = G(-n,1)\rho^{1-n}. \tag{8}$$

From the definition of $G(m,n)$ in (5) we have $G(-n,1) = 1$. Thus (8) yields

$$\frac{1}{\sqrt{n}}\, G(1,n) = \rho^{1-n} \tag{9}$$

and (7) yields

$$\frac{1}{\sqrt{n}}\, G(m,n) = \left(\frac{m}{n}\right)\rho^{1-n}. \tag{10}$$

Relabelling the variables, from (10) we get

$$\frac{1}{\sqrt{m}}\, G(-n,m) = \left(\frac{-n}{m}\right)\rho^{1-m}. \tag{11}$$

We now use the identity (6) (with $a = m$ and $b = n$) to get

$$\frac{1}{\sqrt{n}}\, G(m,n) = \rho^{1-mn}\,\frac{1}{\sqrt{m}}\, G(-n,m),$$

which by (10) and (12) can be rewritten as

$$\left(\frac{m}{n}\right)\rho^{1-n} = \left(\frac{-n}{m}\right)\rho^{1-m}\rho^{1-mn}. \tag{12}$$

At this point we need to compute the Legendre symbol $\left(\frac{-1}{p}\right)$ for an odd prime p.

Computation of Legendre Symbol $\left(\frac{-1}{p}\right)$ for Odd Prime p. We claim that

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

for any odd prime p. The proof of the claim is as follows.

From the order $p-1$ of the multiplicative group of nonzero elements of $\mathbb{Z}/\mathbb{Z}p$ we have

$$x^{p-1} \equiv 1 \bmod p,$$

which implies either

$$x^{\frac{p-1}{2}} \equiv 1 \bmod p$$

or

$$x^{\frac{p-1}{2}} \equiv -1 \bmod p.$$

If a is a quadratic residue, then $a \equiv x^2 \bmod p$ and

$$a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \bmod p.$$

Since there are precisely $\frac{p-1}{2}$ quadratic residues and there are precisely $\frac{p-1}{2}$ solutions of

$$a^{\frac{p-1}{2}} \equiv 1 \bmod p$$

among the numbers a between 1 and $p-1$ and also precisely $\frac{p-1}{2}$ solutions of

$$a^{\frac{p-1}{2}} \equiv -1 \bmod p$$

among the numbers a between 1 and $p-1$, we have

$$m^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right) \bmod p$$

for any $m \in \mathbb{Z}$. The special case $m = -1$ yields

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \bmod p.$$

Since the absolute value of $\left(\frac{-1}{p}\right)$ is no more than 1, we must have

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

for any odd prime p. This means that

$$\left(\frac{-m}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{-1}{p}\right) = \left(\frac{m}{p}\right)(-1)^{\frac{p-1}{2}} = \left(\frac{m}{p}\right)\rho^{2(p-1)} \tag{13}$$

for any odd prime p and any $m \in \mathbb{Z}$.

We now continue with our proof of quadratic reciprocity under the assumption of the relation

$$G(m,n) = \left(\frac{m}{n}\right) G(1,n). \tag{7}$$

between the Gauss sum and the Legendre symbol. Putting together (12) and (13), we get

$$\left(\frac{p}{q}\right)\left(\frac{-q}{p}\right) = \rho^{pq-1}\rho^{p-1}\rho^{1-q}$$

and

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \rho^{2(1-p)}\rho^{pq-1}\rho^{p-1}\rho^{1-q} = \rho^{(p-1)(q-1)},$$

which is the statement of quadratic reciprocity.

Proof of Relation between Gauss Sum and Legendre Symbol. Finally we prove the the relation between Gauss sum and Legendre symbol

$$G(m,n) = \left(\frac{m}{n}\right) G(1,n) \tag{7}.$$

Since $h^2 - h = h(h-1) \in 2\mathbb{Z}$ so that $e^{\pi imh} = e^{\pi imh^2}$ for $m \in \mathbb{Z}$, we can rewrite

$$\begin{aligned} G(m,n) &= 1 + \sum_{h=1}^{n-1} \exp\left(\pi i \frac{m}{n} h^2 + \pi imh\right) \\ &= 1 + \sum_{h=1}^{n-1} \exp\left(\pi i \frac{m}{n}(n+1)h^2\right). \end{aligned}$$

Since $(n-h)^2 \equiv h^2 \bmod n$, the $n-1$ elements h^2 with $1 \le h \le n-1$ are the same as the $\frac{n-1}{2}$ quadratic residues λ with each one counted twice, we can rewrite

$$\begin{aligned} G(m,n) &= 1 + \sum_{h=1}^{n-1} \exp\left(\pi i \frac{m}{n}(n+1)h^2\right) \\ &= 1 + 2\sum_{\lambda} \exp\left(\pi i \frac{m}{n}(n+1)\lambda\right) \end{aligned}$$

where λ runs through the set of all quadratic residues. Let μ run through the set of all quadratic nonresidues. Let $\xi = \exp(\pi i \frac{m}{n}(n+1))$. Since

$$1 + \sum_{\lambda} \exp\left(\pi i \frac{m}{n}(n+1)\lambda\right) + \sum_{\mu} \exp\left(\pi i \frac{m}{n}(n+1)\mu\right) = \sum_{h=0}^{n-1} \xi^h = 0,$$

it follows that

$$G(m,n) = 1 + 2\sum_{\lambda} \exp\left(\pi i \frac{m}{n}(n+1)\lambda\right) \tag{14}$$
$$= \sum_{\lambda} \exp\left(\pi i \frac{m}{n}(n+1)\lambda\right) - \sum_{\mu} \exp\left(\pi i \frac{m}{n}(n+1)\mu\right).$$

Suppose m is a quadratic residue. When λ runs through the set of all quadratic residues, $m\lambda$ runs through also the set of all quadratic residues. When μ runs through the set of all quadratic nonresidues, $m\mu$ runs through also the set of all quadratic nonresidues. Thus, if m is a quadratic residue, then (14) implies that

$$G(m,n) = \sum_{\lambda} \exp\left(\pi i \frac{1}{n}(n+1)\lambda\right) - \sum_{\mu} \exp\left(\pi i \frac{1}{n}(n+1)\lambda\right)$$

which is equal to $G(1,n)$ or $(\frac{m}{n})G(1,n)$. In the case when m is not a quadratic residue, $m\lambda$ (respectively $m\mu$) runs through the set of all quadratic nonresidues (respectively residues) when λ runs through the set of all quadratic residues (respectively nonresidues). Hence if m is a quadratic nonresidue, then (14) implies that

$$G(m,n) = -\sum_{\lambda} \exp\left(\frac{\pi i}{n}(n+1)\lambda\right) + \sum_{\mu} \exp\left(\frac{\pi i}{n}(n+1)\lambda\right) = \left(\frac{m}{n}\right) G(1,n).$$

In both cases, we have

$$G(m,n) = \left(\frac{m}{n}\right) G(1,n),$$

which is the relation between Gauss sum and Legendre symbol.