The law of quadratic reciprocity

Loïc Dobler, Paul Mangers

October 2021

Definition. An integer q is a quadratic residue modulo p if it is congruent to a perfect square modulo p and is a quadratic nonresidue modulo otherwise.

Definition. Let p be an odd prime and q an integer such that p and q are coprime. Then the Legendre symbol is defined as follows

$$\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } q \text{ is a quadratic residue modulo } p \text{ and } q \not\equiv 0 \pmod{p}, \\ -1 & \text{if } q \text{ is a non-quadratic residue modulo } p, \\ 0 & \text{if } q \equiv 0 \pmod{p}. \end{cases}$$

Legendre's original definition was by means of the explicit formula

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p} \quad \text{and} \quad \left(\frac{a}{p}\right) \in \{-1, 0, 1\}.$$

We now want to know if $\left(\frac{p}{q}\right)$ can be determined if $\left(\frac{q}{p}\right)$ is known. Gauss's law of quadratic reciprocity shows that this is indeed possible.

We are now going to state the main Theorem of this lecture.

Theorem 1. (GAUSS) If p and q are distinct odd primes, then

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

Since $\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)$ is odd if and only if $p \equiv q \equiv 3 \pmod 4$, Theorem 1 can be restated as follows:

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right), \quad \text{if } p \equiv q \equiv 3 \pmod 4$$

and

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right), \quad \text{otherwise}$$

We will try to prove this Theorem in a two different ways. The first one will be a more algebraic proof and the second one a more analytic.

Theorem 2. (Fermat's little Theorem) Let p be a prime number. For any integer a, the number $a^p - a$ is an integer multiple of p. So

$$a^p \equiv a \pmod{p}$$

If a is not divisible by p, we get

$$a^{p-1} \equiv 1 \pmod{p}$$

Since this Theorem is not in the book we don't do a proof of it.

Theorem 3. (Euler's criterion). Let p be an odd prime. Then for all n we have

$$\left(\frac{n}{p}\right) \equiv n^{(p-1)/2} \pmod{p}.$$

Proof. If $n \equiv 0 \pmod{p}$ the result is trivial, because both members are congruent to 0 mod p. Now suppose that $\left(\frac{n}{p}\right) = 1$. Then there is an x such that $x^2 \equiv n \pmod{p}$ and hence

$$n^{(p-1)/2} \equiv (x^2)^{(p-1)/2} = x^{p-1} \equiv 1 = \left(\frac{n}{p}\right) \pmod{p}$$

(here we used Fermat's little Theorem)

This proves the Theorem if $\left(\frac{n}{p}\right) = 1$.
Now suppose that $\left(\frac{n}{p}\right) = -1$ and consider the polynomial

$$f(x) = x^{(p-1)/2} - 1.$$

Since $f(x)$ has degree $(p-1)/2$ the congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most $(p-1)/2$ solutions. But the $(p-1)/2$ quadratic residues mod p are solutions so the nonresidues are not. Hence

$$n^{(p-1)/2} \not\equiv 1 \pmod{p} \quad \text{if } \left(\frac{n}{p}\right) = -1.$$

But $n^{(p-1)/2} \equiv \pm 1 \pmod{p}$ so $n^{(p-1)/2} \equiv -1 \equiv \left(\frac{n}{p}\right) \pmod{p}$. This completes the proof. □

Theorem 4. (Gauss' Lemma) Assume $n \not\equiv 0 \pmod{p}$ and consider the least positive residues mod p of the following $(p-1)/2$ multiples of n:

$$n, 2n, 3n, ..., \frac{p-1}{2}n.$$

If m denotes the number of these residues which exceed $p/2$, then

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

Example. Let $p = 17$ and $a = 7$. There are 16 nonzero elements $[1, 16]$. We consider the first half $[1, 8]$ and multiply all the numbers from there by 7 to get 7,14,4,11,1,8,15,5. We see that 14,11 and 15 are greater than $p/2$ so Gauss' Lemma tells us that

$$\left(\frac{7}{17}\right) = (-1)^3 = -1$$

Proof. The multiples of n above are incongruent mod p. We consider their least positive residues and distribute them into two disjoint sets A and B, according as the residues are $< p/2$ or $> p/2$. Thus

$$A = \{a_1, a_2, ..., a_k\}$$

where each $a_i \equiv tn \pmod{p}$ for some $t \leq (p-1)/2$, $\quad 0 < a_i < p/2$ and

$$B = \{b_1, b_2, ..., b_m\}$$

where each $b_i \equiv sn \pmod{p}$ for some $s \leq (p-1)/2$ and $p/2 < b_i < p$. Note that $m + k = (p-1)/2$ since A and B are disjoint. Form a new set C of m elements by subtracting each b_i from p. Thus

$$C = \{c_1, c_2, ..., c_m\}, \text{where } c_i = p - b_i$$

Now $0 < c_i < p/2$ so the elements of C lie in the same interval as the elements of A. We show next that the sets A and C are disjoint.
Assume that $c_i = a_j$ for some pair i and j. Then $p - b_i = a_j$ or $a_j + b_i \equiv 0 \pmod{p}$. Therefore

$$tn + sn = (t+s)n \equiv 0 \pmod{p}$$

for some s and t with $1 \leq t < p/2$, $1 \leq s < p/2$. But this is impossible since $p \not| \; n$ (because $n \not\equiv \pmod{p}$) and $0 < s + t < p$. Therefore A and C are disjoint, so their union $A \cup C$ contains $m + k = (p-1)/2$ integers in the interval $[1, (p-1)/2]$. Hence

$$A \cup C = \{a_1, a_2, ..., a_k, c_1, c_2, ..., c_m\} = \{1, 2, ..., \frac{p-1}{2}\}.$$

Now form the product of all the elements in $A \cup B$ to optain

$$a_1 a_2 ... a_k c_1 c_2 ... c_m = \left(\frac{p-1}{2}\right)!$$

since $c_i = p - b_i$ this gives us

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &= a_1...a_k(p-b_1)...(p-b_m)\\ &\equiv (-1)^m a_1...a_k b_1...b_m \pmod p\\ &\equiv (-1)^m n(2n)...\left(\frac{p-1}{2}n\right) \pmod p\\ &\equiv (-1)^m n^{(p-1)/2}\left(\frac{p-1}{2}\right)! \pmod p.\end{aligned}$$

(we have exactly $(p-1)/2$ n's, that's why we obtain $n^{(p-1)/2}$)
Canceling the factorial we obtain

$$n^{(p-1)/2} \equiv (-1)^m \pmod p.$$

Euler's criterion shows that $(-1)^m \equiv \left(\frac{n}{p}\right) \pmod p$ hence $(-1)^m \equiv \left(\frac{n}{p}\right)$ and the proof of Gauss' Lemma is complete. □

Theorem 5. Let m be the number defined in Gauss' lemma. Then

$$m \equiv \sum_{t=1}^{(p-1)/2}\left[\frac{tn}{p}\right] + (n-1)\frac{p^2-1}{8} \pmod 2$$

In particular, if n is odd we have

$$m \equiv \sum_{t=1}^{(p-1)/2}\left[\frac{tn}{p}\right] \pmod 2$$

where $[x]$ denotes the integer part of a number x.

Proof. Recall that m is the number of least positive residues of the numbers

$$n, 2n, 3n, ..., \frac{p-1}{2}n$$

which exceed $p/2$. Take a typical number, say tn, divide it by p and examine the size of the remainder. We have

$$\frac{tn}{p} = \left[\frac{tn}{p}\right] + \left\{\frac{tn}{p}\right\}, \text{ where } 0 < \left\{\frac{tn}{p}\right\} < 1,$$

so

$$tn = p\left[\frac{tn}{p}\right] + p\left\{\frac{tn}{p}\right\} = p\left[\frac{tn}{p}\right] + r_t,$$

say, where $0 < r_t < p$. The number $r_t = tn - p\left[\frac{tn}{p}\right]$ is the least positive residue of tn modulo p. Referring again to the sets A and B used in the proof of Gauss' lemma we have

$$\{r_1, r_2, ..., r_{(p-1)/2}\} = \{a_1, a_2, ..., a_k, b_1, ..., b_m\}.$$

Recall also that

$$\left\{1, 2, ..., \frac{p-1}{2}\right\} = \{a_1, a_2, ..., a_k, c_1, ..., c_m\}$$

where each $c_i = p - b_i$. Now we compute the sums of the elements in these sets to obtain the two equations

$$\sum_{t=1}^{(p-1)/2} r_t = \sum_{i=1}^{k} a_i + \sum_{j=1}^{m} b_j$$

and

$$\sum_{t=1}^{(p-1)/2} t = \sum_{i=1}^{k} a_i + \sum_{j=1}^{m} c_j = \sum_{i=1}^{k} a_i + mp - \sum_{j=1}^{m} b_j.$$

In the first equation we replace r_t by its definition to obtain

$$\sum_{i=1}^{k} a_i + \sum_{j=1}^{m} b_j = n\left(\sum_{t=1}^{(p-1)/2} t\right) - p\left(\sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p}\right]\right).$$

The second equation is

$$mp + \sum_{i=1}^{k} a_i - \sum_{j=1}^{n} b_j = \sum_{t=1}^{(p-1)/2} t$$

Adding this to the previous equation we get

$$\begin{aligned} mp + 2\sum_{i=1}^{k} a_i &= (n+1)\left(\sum_{t=1}^{(p-1)/2} t\right) - p\left(\sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p}\right]\right) \\ &= (n+1)\frac{p^2-1}{8} - p\left(\sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p}\right]\right) \end{aligned}$$

Now we reduce this modulo 2, noting that $n + 1 \equiv n - 1 \pmod 2$ and $p \equiv 1 \pmod 2$ since p is odd, and we obtain

$$m \equiv (n-1)\frac{p^2-1}{8} + \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p}\right] \pmod 2,$$

which completes the proof (in the last step we added twice the sum). □

Proof. of Theorem 1 (second proof). By Gauss' lemma and Theorem 9.7 we have

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

where

$$m \equiv \sum_{t=1}^{(p-1)/2} \left[\frac{tq}{p}\right] \pmod 2.$$

since q is odd. Similarly,

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

with

$$n \equiv \sum_{s=1}^{(q-1)/2} \left[\frac{sp}{q}\right] \pmod 2.$$

since p is odd. Hence $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{m+n}$, and Theorem 1 follows at once from the identity

$$\sum_{t=1}^{(p-1)/2} \left[\frac{tq}{p}\right] + \sum_{s=1}^{(q-1)/2} \left[\frac{sp}{q}\right] = \frac{p-1}{2}\frac{q-1}{2} \tag{1}$$

To prove (22) we consider the function

$$f(x,y) = qx - py.$$

If x and y are nonzero integers then $f(x,y)$ is a nonzero integer (because p and q are coprime). Moreover, as x takes the values $1, 2, ..., (p-1)/2$ and y takes the values $1, 2, ..., (q-1)/2$ then $f(x,y)$ takes

$$\frac{p-1}{2}\frac{q-1}{2}$$

values, no two of wich are equal because

$$f(x,y) - f(x',y') = f(x-x', y-y') \neq 0.$$

Now we count the number of values of $f(x,y)$ wich are positive and the number wich are negative.

For each fixed x we have $f(x,y) > 0$ if and only if $y < \frac{qx}{p}$, or $y \leq \left[\frac{qx}{p}\right]$. Hence the total number of positive values is

$$\sum_{t=1}^{(p-1)/2} \left[\frac{tq}{p}\right]$$

And similarly the number of negative values is

$$\sum_{s=1}^{(p-1)/2} \left[\frac{sp}{q}\right]$$

Since the number of positive and negative values together is

$$\frac{p-1}{2}\frac{q-1}{2}$$

(just the whole number of elements) this proves (22) and so Theorem 1. □

Now we will do a second proof of Theorem 1. For this we need a few more statements and definitions.

Definition. (Gaussian sums) Let m and n be two non-zero integers. Then a generalized Gaussian sum is defined as

$$g(m,n) := \sum_{k=1}^{|n|} e^{\pi i \frac{m}{n} k^2 + \pi i m k} \tag{2}$$

Remark. When m is even, this reduces to a Gaussian sum (sum of n-th unity roots).

Theorem 1 can be deduced from a formula connecting $g(m,n)$ and $g(-n,m)$, wich we state as

Theorem 6. If m and n are non-zero integers, then

$$\frac{1}{\sqrt{|n|}} g(m,n) = e^{\frac{\pi i}{4}(1-|mn|)\mathrm{sgn}(mn)} \frac{1}{\sqrt{|m|}} g(-n,m), \tag{3}$$

where $\mathrm{sgn}(r) = \frac{r}{|r|}$ if $r \neq 0$, and $\mathrm{sgn}(r) = 0$ if $r = 0$.

Proof. We shall use complex integration for the proof. Consider the integral

$$f(X,\tau) = \int_C \Phi(u,X,\tau) du \tag{4}$$

where

$$\Phi(u,X,\tau) = \frac{e^{\pi i \tau u^2 + 2\pi X u}}{e^{2\pi i u} - 1} \tag{5}$$

with u a complex variable, X an arbitrary complex number, τ a complex number with positive real part, and C a line in the complex u-plane through the point $u = \frac{1}{2}$ wich is inclined at an angle $\frac{\pi}{4}$ to the positive real axis. We will first show that the integral converges by estimating the function Φ in any strip of finite width, which is bounded by two lines parallel to C. If we set

$$u = c + r e^{\frac{i\pi}{4}}$$

where c and r are real, c bounded and r variable, and

$$\tau = \mathrm{Re}(\tau) + i\mathrm{Im}(\tau)$$

We rewrite u like this because we will integrate along C so we will be able integrate only using the variable r.

We now get

$$\left| e^{\pi i \tau u^2 + 2\pi i X u} \right| = e^{-\pi \mathrm{Im}(\tau u^2 + 2Xu)},$$

and

$$\tau u^2 + 2Xu = i\tau r^2 + 2e^{\frac{\pi i}{4}}(\tau c + X)r + (\tau c + 2X)c,$$

so that

$$\mathrm{Im}(\tau u^2 + 2Xu) \geq \mathrm{Re}(\tau) \cdot r^2 - 2|\tau c + X| \cdot |r| - |(\tau c + 2X)c|$$

Hence

$$\left| e^{\pi i \tau u^2 + 2\pi i X u} \right| \leq e^{-\pi r^2 \mathrm{Re}(\tau) + \pi |\tau| (c^2 + 2|cr|) + 2\pi |X| (|c| + |r|)} \leq A e^{-\pi r^2 \mathrm{Re}(\tau) + B|r|}, \quad (6)$$

where A and B are constants independent of r. Further

$$|e^{2\pi i u} - 1| \geq \left| 1 - |e^{2\pi i u}| \right| = |1 - e^{-\sqrt{2}\pi r}|$$

Now we let $r \to \pm\infty$ as $|u| \to \infty$ in the strip, so that if $|u|$ is large enough, then

$$|e^{2\pi i u} - 1| \geq \frac{1}{2} > 0. \quad (7)$$

After some calculations we find that

$$|\Phi(u, X, \tau)| \leq A_1 \cdot e^{-\pi r^2 n \mathrm{Re}(\tau) + B|r|}, \quad (8)$$

(where A_1 and B are real constants) in the chosen strip, for $|u|$ large enough. Since e^{-r^2} goes faster to 0 than e^r goes to ∞ we have that the integral

$$\int_C \Phi(u, X, \tau) du$$

converges. We now prove for $n > 0$ that $g(m, n)$ is the value of the integral

$$\int_\gamma \Phi(u, X, \tau) du$$

where γ is the parallelogram formed by the line C, the line C_n (the line parallel to C wich cuts the real axis at the point $n + \frac{1}{2}, n \in \mathbb{N}$) and the lines L_1, L_2 which are parallel to the real axis (and are at a positive distance from it) and connect C and C_n (see picture).

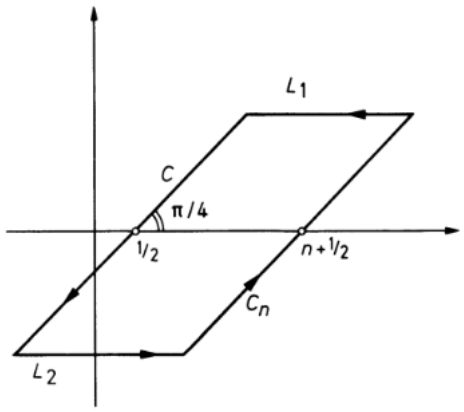

Fig. 1

Recap: A meromorphic function on an open subset D of the complex plane is a function that is holomorphic on all of D except for a set of isolated points, which are poles of the function.

Now $\Phi(u, X, \tau)$ is a meromorphic function of u, and if γ is taken in the positive sense, then by Cauchy's theorem of residues, we have

$$\int_\gamma \Phi(u, X, \tau)du = \sum_{k=1}^{n} e^{\pi i\tau k^2 + 2\pi iXk} \tag{9}$$

Because of our approximation (7) above we clearly have $\Phi(u, X, \tau) \to 0$ uniformly as $|u| \to \infty$ in the strip. Now since the two sides of γ that are parallel to the real axis have constant length the path integral on these two vanishes when the sides are infinitly far away from the real axis. So we are left with

$$\int_{C_n} \Phi(u, X, \tau)du - \int_C \Phi(u, X, \tau)du = \sum_{k=1}^{n} e^{\pi i\tau k^2 + 2\pi iXk}. \tag{10}$$

Starting with (4) and doing some simple calculations we find that

$$\Phi(u + n, X, \tau) = e^{\pi i\tau n^2 + 2\pi iXn}\Phi(u, X + \tau n, \tau),$$

and thus by integrating both sides along C we get

$$\int_{C_n} \Phi(u, X, \tau)du = e^{\pi i\tau n^2 + 2\pi iXn} f(X + \tau n, \tau)$$

for f defined as above (we have C_n instead of C because of the shift $u \mapsto u + n$). So the equation (9) becomes

$$e^{\pi i\tau n^2 + 2\pi iXn} f(X + \tau n, \tau) - f(X, \tau) = \sum_{k=1}^{n} e^{\pi i\tau k^2 + 2\pi iXk} \tag{11}$$

wich gives us a relation between $f(X,\tau)$ and $f(X+\tau n)$ (we just replaced the integral over C_n and Φ).

We now need a second relation like this one to compare the two. With the definition of f we find that

$$\begin{aligned} f(X+1,\tau)-f(X,\tau) &= \int_C \frac{e^{\pi i\tau u^2}}{e^{2\pi iu}-1}\left(e^{2\pi i(X+1)u}-e^{2\pi iXu}\right)du \\ &= \int_C e^{\pi i\tau u^2+2\pi iXu}du \\ &= e^{-\pi i\frac{X^2}{\tau}}\int_C e^{\pi i\tau\left(u+\frac{X}{\tau}\right)^2}du. \end{aligned}$$

We completed the square in the last step.

We write C' for the line parallel to C, obtained by the translation $u\mapsto u+\frac{X}{\tau}$. Then

$$f(X+1,\tau)-f(X,\tau) = e^{-\pi i\frac{X^2}{\tau}}\int_{C'} e^{\pi i\tau u^2}du.$$

This integral converges for the same reasons as above. Now we will integrate around a parallelogramm as before using our estimations with $X=0$ (we do this to find a relation between $\int_{C'}$ and $\int_{C_0}$), we can see that

$$\int_{C'} e^{\pi i\tau u^2}du = \int_{C_0} e^{\pi i\tau u^2}du$$

where C_0 is the line parallel to C' through the origin (these to integrals are the same since for $X=0$ and $n=0$ the sum over the residues in (10) is just 0 and so we get the equality).

Remark. The notation is a little redundent, the C_0 used here has nothing to do with the C_n's we defined before (we defined them for $n>0$).

On C_0 we have $u=re^{\frac{\pi i}{4}}$, with r real ($c=0$ on C_0 because we go through the origin). Therefore

$$\int_{C_0} e^{\pi i\tau u^2}du = e^{\frac{\pi i}{4}}\int_{-\infty}^{\infty} e^{-\pi\tau r^2}dr = e^{\frac{\pi i}{4}}I_\tau$$

We only integrate $e^{-\pi\tau r^2}$ along the real axis and we keep $e^{\frac{\pi i}{4}}$ so that it's still in the complex plane. Hence

$$f(X+1,\tau)-f(X,\tau) = e^{\pi i\left(\frac{1}{4}-\frac{X^2}{\tau}\right)}I_\tau.$$

Here we replaced the integral over C' with the integral over C_0 (since they are the same) and replaced this with a real integral. If we iterate this formula m

times we get

$$f(X+m,\tau)-f(X,\tau)=I_\tau\sum_{k=0}^{m-1}e^{\pi i\left(\frac{1}{4}-\frac{(X+k)^2}{\tau}\right)},$$

where m is a positive integer. If we replace X by $X+\tau n-m$ (we do a shift), we get the second relation we are seeking, namely

$$f(X+\tau n,\tau)-f(X+\tau n-m,\tau)=I_\tau\sum_{k=0}^{m-1}e^{\pi i\left(\frac{1}{4}-\frac{(X+\tau n-m+k)^2}{\tau}\right)} \tag{12}$$

Now from (11) and (12) we get

$$\begin{aligned}e^{\pi i\tau n^2+2\pi iXn}f(X+\tau n-m,\tau)-f(X,\tau)&=\sum_{k=1}^{n}e^{\pi i\tau k^2+2\pi iXk}-I_\tau e^{\pi i\tau n^2+2\pi iXn}\sum_{j=1}^{m}e^{\pi i\left(\frac{1}{4}-\frac{(X+\tau n-j)^2}{\tau}\right)}\\&=\sum_{k=1}^{n}e^{\pi i\tau k^2+2\pi iXk}-I_\tau\sum_{j=1}^{m}e^{\pi i\left(\frac{1}{4}-\frac{(X-j)^2}{\tau}\right)}\end{aligned}$$

(We obtain this by doing (11) - $e^{\pi i\tau n^2+2\pi iXm}$(12) and we do a shift)

If we set $X=\frac{m}{2}$ and $\tau=\frac{m}{n},m>0,n>0$ (in the formula we found), we have

$$\sum_{k=1}^{n}e^{\pi ik^2\frac{m}{n}+\pi imk}=I_{\frac{m}{n}}e^{\frac{\pi i}{4}(1-mn)}\sum_{k=1}^{m}e^{\pi ikn-k^2\pi i\frac{n}{m}} \tag{13}$$

Here if we set $m=n=1$, we get $I_1=1$, that is

$$\int_{-\infty}^{\infty}e^{-\pi t^2}dt=1$$

If we make the substitution $t\mapsto t\sqrt{\tau}$, where τ is real and positive, we get

$$I_t=\int_{-\infty}^{\infty}e^{-\pi\tau t^2}dt=\frac{1}{\sqrt{\tau}} \tag{14}$$

If in (14) we set $\tau=\frac{m}{n}$, and use this in formula (13) we will get

$$\begin{aligned}\frac{1}{\sqrt{n}}\sum_{k=1}^{n}e^{\pi ik^2\frac{m}{n}+\pi imk}&=\frac{1}{\sqrt{m}}e^{\frac{\pi i}{4}(1-mn)}\sum_{k=1}^{m}e^{\pi ikn-k^2\pi i\frac{n}{m}}\\&=\frac{1}{\sqrt{m}}e^{\frac{\pi i}{4}(1-mn)}\sum_{k=1}^{m}e^{-\pi ikn-k^2\pi i\frac{n}{m}}\end{aligned}$$

With the definition of $g(m,n)$ we get

$$\frac{1}{\sqrt{n}}g(m,n)=\frac{1}{\sqrt{m}}e^{\frac{\pi i}{4}(1-mn)}g(-n,m) \tag{15}$$

So the theorem is proven for $m > 0, n > 0$. Now if $m > 0$ and $n < 0$ then $-n, m > 0$ and thus (15) gives us

$$\frac{1}{\sqrt{m}} g(-n, m) = \frac{1}{\sqrt{-n}} e^{\frac{\pi i}{4}(1+mn)} g(-m, -n)$$

or

$$\frac{1}{\sqrt{|n|}} g(-m, -n) = \frac{1}{\sqrt{m}} e^{-\frac{\pi i}{4}(1-|mn|)} g(-n, m)$$

But by definition we have $g(-m, -n) = g(m, n)$ and therefore

$$\frac{1}{\sqrt{|n|}} g(m, n) = \frac{1}{\sqrt{m}} e^{\frac{\pi i}{4}(1-|mn|)\mathrm{sgn}(mn)} g(-n, m)$$

If $m < 0, n < 0$ the statement of the theorem still holds since $g(-m, -n) = g(m, n)$, $g(n, -m) = g(-n, m)$ and $(1 - |mn|)\mathrm{sgn}(mn)$ remains unchanged if m, n are replaced by $-m, -n$ respectively. □

Before we begin with the proof of Theorem 1, we state a corollary we will need. We will not prove this one since it is treated in another chapter.

Corollary. We have for m, n integers and p an odd prime

$$\left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = \left(\frac{mn}{p}\right)$$

which means that the product of two quadratic residues, or non-residues, modulo p, is again a quadratic residue, but the product of a quadratic residue with a quadratic non-residue, modulo p, is again a quadratic non-residue.

Proof. We can now deduce the law of quadratic reciprocity (Theorem 1) using the formula for generalized Gaussian sums proved in Theorem 2.

Since $k^2 \equiv k \pmod 2$, we can replace k by k^2 in the definition of $g(m, n)$ given in (1) and write

$$g(m, n) = \sum_{k=1}^{|n|} e^{\pi i k^2 \frac{m}{n}(n+1)}$$

We are able to do this because of the periodicity of the exponential function.

Now let n be an odd prime and m some integer prime to n. We then have

$$g(m, n) = 1 + \sum_{k=1}^{n-1} e^{\pi i k^2 \frac{m}{n}(n+1)}.$$

If $k^2 \equiv \rho \pmod n$, then we can see that

$$e^{\pi i k^2 \frac{m}{n}(n+1)} = e^{\pi i \rho \frac{m}{n}(n+1)}.$$

If $k^2 \equiv \rho \pmod{n}$, and $1 \leq k \leq n-1$, then ρ is a quadratic residue modulo n and $(n-k)^2 \equiv k^2 \equiv \rho \pmod{n}$. Thus if k runs through the integers $1, 2, ..., n-1$, then k^2 (taken modulo n) runs twice through the set of quadratic residues modulo n. Hence

$$g(m,n) = 1 + 2\sum_{\rho} e^{\pi i \rho \frac{m}{n}(n+1)}, \tag{16}$$

where ρ runs through the set of quadratic residues modulo an odd prime n (we have a 2 because ρ runs twice through the quadratic residues).

We will now consider the sum

$$\sum_{\nu} e^{\pi i \nu \frac{m}{n}(n+1)}$$

where ν runs through the quadratic non-residues modulo n. So we have

$$1 + \sum_{\rho} e^{\pi i \rho \frac{m}{n}(n+1)} + \sum_{\nu} e^{\pi i \nu \frac{m}{n}(n+1)} = \sum_{k=0}^{n-1} e^{\pi i k \frac{m}{n}(n+1)}.$$

(here residues and non residues together give all the numbers between 0 and $n-1$).

But $n+1$ is even and therefore $e^{\pi i k \frac{m}{n}(n+1)}$ is the k^{th} power of an n^{th} root of unity, say η and $\eta \neq 1$ since n does not divide m. Thus

$$1 + \sum_{\rho} e^{\pi i \rho \frac{m}{n}(n+1)} + \sum_{\nu} e^{\pi i \nu \frac{m}{n}(n+1)} = 1 + \sum_{\rho} \eta^{\rho} + \sum_{\nu} \eta^{\nu} = \sum_{p=0}^{n-1} \eta^p = \frac{1-\eta^n}{1-\eta} = 0 \tag{17}$$

This gives us 0 since η is the n-th root of unity.

With (16) and (17) ((17) - (16)) we get

$$g(m,n) = \sum_{\rho} e^{\pi i \rho \frac{m}{n}(n+1)} - \sum_{\nu} e^{\pi i \nu \frac{m}{n}(n+1)} \tag{18}$$

We now consider the two possibilities $\left(\frac{m}{n}\right) = 1$ and $\left(\frac{m}{n}\right) = -1$.

First case $\left(\frac{m}{n}\right) = 1$ then m is a quadratic residue modulo n and ρ runs through all quadratic residues modulo n, then by the Corollary of Theorem 3 of chapter IV, ρm likewise runs through all the quadratic residues (because a quadratic residue times a quadratic residue gives a quadratic residue, so summing over ρ is the same as summing over ρm). And if ν runs through all the non-residues, so does νm. Hence

$$\begin{aligned} g(m,n) &= \sum_{\rho} e^{\pi i \rho \left(\frac{n+1}{n}\right)} - \sum_{\nu} e^{\pi i \nu \left(\frac{n+1}{n}\right)} \\ &= g(1,n) \qquad \text{(by (18))} \\ &= \left(\frac{m}{n}\right) g(1,n). \end{aligned}$$

Now we consider the second case. If m is a quadratic non-residue modulo n, then by reasoning again as in the first case, we have

$$\begin{aligned} g(m,n) &= \sum_{\nu} e^{\pi i \nu \left(\frac{n+1}{n}\right)} - \sum_{\rho} e^{\pi i \rho \left(\frac{n+1}{n}\right)} \\ &= -g(1,n) \\ &= \left(\frac{m}{n}\right) g(1,n). \end{aligned}$$

So we proved that if n is an odd prime and $(m,n) = 1$ (where $(\cdot,\cdot)$ denotes the gcd), then

$$g(m,n) = \left(\frac{m}{n}\right) g(1,n) \tag{19}$$

From Theorem 2 (with $m = 1$) we also have

$$\frac{1}{\sqrt{n}} g(1,n) = e^{\frac{\pi i}{4}(1-n)} g(-n,1),$$

and by definition $g(-n,1) = e^{-2\pi n} = 1$ holds. Thus we have

$$g(1,n) = \sqrt{n} e^{\frac{\pi i}{4}(1-n)} \tag{20}$$

Combining (19) and (20) (we plug $g(1,n)$ in) we obtain

$$\left(\frac{m}{n}\right) = \frac{1}{\sqrt{n}} e^{\frac{\pi i}{4}(n-1)} g(m,n) \tag{21}$$

where n is an odd prime, and m is an integer such that $(m,n) = 1$. Now if $m = -1$ this formula gives us

$$\left(\frac{-1}{n}\right) = \frac{1}{\sqrt{n}} e^{\frac{\pi i}{4}(n-1)} g(-1,n)$$

But from Theorem 2 we have

$$\frac{1}{\sqrt{n}} g(-1,n) = e^{\frac{\pi i}{4}(n-1)} g(-n,-1) = e^{\frac{\pi i}{4}(n-1)}$$

since $g(-n,-1) = 1$ (for the same reason as above). Therefore by combining the two equations we just found we get

$$\left(\frac{-1}{n}\right) = e^{\frac{\pi i}{2}(n-1)} = (-1)^{\frac{n-1}{2}} \tag{22}$$

Here n is an odd prime. We now assume that m is also an odd prime. Then with Theorem 2 and (21) we get

$$\left(\frac{m}{n}\right) = e^{\frac{\pi i}{4}(n-1)} \cdot e^{\frac{\pi i}{4}(1-mn)} \frac{1}{\sqrt{m}} g(-n,m).$$

If we use (21) again we have

$$\left(\frac{m}{n}\right) = e^{\frac{\pi i}{4}(n-1)} \cdot e^{\frac{\pi i}{4}(1-mn)} e^{\frac{-\pi i}{4}(m-1)} \left(\frac{-n}{m}\right).$$

But (with corollary 3 again)

$$\left(\frac{-n}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}} \left(\frac{n}{m}\right) = e^{\frac{2\pi i}{4}(m-1)} \left(\frac{n}{m}\right)$$

because of (22). So

$$\left(\frac{m}{n}\right) = e^{\frac{-\pi i}{4}(n-1)(m-1)} \left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}} \left(\frac{n}{m}\right),$$

Since $\left(\frac{n}{m}\right)^2 = 1$ we can multiply both sides with $\left(\frac{n}{m}\right)$ and we get

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}$$

And therefore Theorem 1 is proven. □

References

◦ Introduction to Analytic Number Theory by T.M. Apostol (Springer 1976), chapter 9

◦ Introduction to Analytic Number Theory by K. Chandrasekharan (Springer 1968), chapter 5