Proc. Int. Conf. – Number Theory No. 1, 2004, pp. 107–116.

Quadratic Reciprocity Via Theta Functions

M. Ram Murty[1]*and Allison Pacelli[2]

[1]Department of Mathematics, Queen's University, Kingston K7L 3N6, Ontario, Canada
e-mail: murty@mast.queensu.ca
[2]Department of Mathematics, Williams College, Williamstown, MA 01267
e-mail: Allison.Pacelli@williams.edu

1. Introduction

The celebrated law of quadratic reciprocity has had numerous proofs. Gauss, who first discovered the law, gave several proofs in his famous book, *Disquitiones Arithmeticae*. A proof, not widely known, is due to Hecke and it uses θ-functions in number fields. In Chapter 8 of his classical text [H], the complete proof using θ-functions of several variables is given in its full generality. Among the experts, it is widely believed that this proof is conceptually significant and leads to natural generalizations in the higher dimensional context (see for example [Kub]). From a didactic standpoint, it seems desirable to make Hecke's proof accessible to the undergraduate. This is the purpose of this paper.

In this task, we are simply not going to follow Hecke and merely specialize to the case of the rational number field. Rather, we expose the underlying idea and simplify considerably much of his derivation.

Let us recall the statement of the law of quadratic reciprocity. If p and q are distinct odd primes, we define the Legendre symbol $\left(\frac{p}{q}\right)$ to be $+1$ if the congruence $x^2 \equiv p \pmod{q}$ has a solution; we define it to be -1 if the congruence has no solution.

Theorem 1 (The Law of Quadratic Reciprocity).

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

The theorem is remarkable in many ways, the most notable being the relationship between the solvability of $x^2 \equiv p \pmod{q}$ to the solvability of $x^2 \equiv q \pmod{p}$.

Hecke's proof makes use of the classical θ-function:

$$\theta(t) = \sum_{n=-\infty}^{\infty} e^{-n^2\pi t} \tag{2}$$

*Research partially supported by NSERC.

and its functional equation

$$\theta\left(\frac{1}{t}\right) = t^{1/2}\theta(t). \tag{3}$$

In fact, the central point of Hecke is that (3) implies (1), and it is this feature we will expose in this paper.

Historically, there seems to be some precedence for Hecke's proof. In his famous paper of 1860, Riemann used (3) to derive the analytic continuation and functional equation of the ζ-function, defined as

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{4}$$

for $\Re(s) > 1$. Shortly thereafter, θ-functions became more widely used in other contexts. But the idea that (3) implies (1) seems to originate with Landsberg [Lan] in 1893. By a complicated process, he derives using (3), the amazing identity

$$\frac{1}{\sqrt{p}} \sum_{r=0}^{p-1} e^{2\pi i r^2 q/p} = \frac{e^{\pi i/4}}{\sqrt{2q}} \sum_{r=0}^{2q-1} e^{\frac{-\pi i r^2 p}{2q}} \tag{5}$$

valid for any two coprime numbers p and q. Apparently, this identity was first discovered by Schaar [Sc] by another method. Recently, the authors in [AR] give a new proof of this identity using quantum mechanics.

Experts will recognize the left hand side of (5) as a Gauss sum and that the identity immediately leads to:

Theorem 2. *Let b be any odd number. Then,*

$$\sum_{r=0}^{b-1} e^{2\pi i r^2/b} = \begin{cases} \sqrt{b} & \text{if } b \equiv 1 \pmod 4 \\ i\sqrt{b} & \text{if } b \equiv 3 \pmod 4 \end{cases}. \tag{6}$$

Proof. We set $q = 1$ in (5) and the result is immediate. □

The method of deriving Theorem 1 from Theorem 2 is well-known. However, for the sake of completeness, we review it below.

2. Gauss sums

For any natural number q, consider the group $(\mathbb{Z}/q\mathbb{Z})^*$ of coprime residue classes (mod q). A homomorphism

$$\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$$

is called a **Dirichlet character**. The **Gauss sum** attached to χ and the residue class n (mod q) is by definition

$$G(\chi, n) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \chi(a) e^{2\pi i a n/q}. \tag{7}$$

Observe that when $(n, q) = 1$, we have

$$\begin{aligned}\chi(n)G(\chi, n) &= \sum_{\substack{a=1\\(a,q)=1}}^{q} \chi(n)\chi(a)e^{2\pi ian/q}\\ &= \sum_{\substack{b=1\\(b,q)=1}}^{q} \chi(b)e^{2\pi ib/q} \\ &= G(\chi, 1),\end{aligned} \tag{8}$$

because χ is a homomorphism and as a runs through the coprime residue classes, so does an. In the special case that q is prime and χ is the Legendre symbol, observe that:

$$\sum_{\substack{b=1\\(b,q)=1}}^{q} (1 + \chi(b))e^{2\pi ib/q} = \sum_{j=1}^{q-1} e^{2\pi ij^2/q} \tag{9}$$

as $\chi(b) = \pm 1$ according as b is a square (mod q) or not. Since

$$1 + \sum_{b=1}^{q-1} e^{2\pi ib/q} = 0,$$

we deduce

$$\sum_{\substack{b=1\\(b,q)=1}}^{q} \chi(b)e^{2\pi ib/q} = \sum_{j=0}^{q-1} e^{2\pi ij^2/q}. \tag{10}$$

More generally, if $(a, q) = 1$, then

$$\sum_{\substack{b=1\\(b,q)=1}}^{q} (1 + \chi(b))e^{2\pi iba/q} = \sum_{j=1}^{q-1} e^{2\pi ij^2a/q} \tag{11}$$

from which we deduce

$$\sum_{\substack{b=1\\(b,q)=1}}^{q} \chi(b)e^{2\pi iba/q} = \sum_{j=0}^{q-1} e^{2\pi ij^2a/q}. \tag{12}$$

From Theorem 2, we deduce:

Theorem 3. *Let q be prime. Then*

$$\sum_{\substack{b=1\\(b,q)=1}}^{q} \left(\frac{b}{q}\right)e^{2\pi ib/q} = \begin{cases}\sqrt{q} & \text{if } q \equiv 1 (\text{mod } 4)\\ i\sqrt{q} & \text{if } q \equiv 3 (\text{mod } 4)\end{cases} \tag{13}$$

The left hand side of the equation in Theorem 3 is a Gauss sum, and the theorem provides an explicit determination of it.

If we define for any natural number b,

$$S(b,a) = \sum_{j=0}^{b-1} e^{2\pi i j^2 a/b} \tag{14}$$

then

$$S(ab,1) = S(a,b)S(b,a). \tag{15}$$

To see this, observe that

$$S(ab,1) = \sum_{j=0}^{ab-1} e^{\frac{2\pi i j^2}{ab}} = \sum_{j_1=0}^{a-1}\sum_{j_2=0}^{b-1} e^{\frac{2\pi i (bj_1+aj_2)^2}{ab}} \tag{16}$$

since every residue class j (mod ab) can be written as $bj_1 + aj_2$ with $0 \le j_1 \le a-1$ and $0 \le j_2 \le b-1$. Expanding the square and simplifying the identity (15) is immediate.

We are now in a position to deduce Theorem 1. From (12), we have for a quadratic character χ,

$$S(q,a) = \sum_{\substack{b=1\\(b,q)=1}}^{q} \chi(b)e^{2\pi i ba/q} = \chi(a)\sum_{\substack{b=1\\(b,q)=1}}^{q} \chi(b)\chi(a)e^{2\pi i ba/q} \tag{17}$$

as $\chi^2(a) = 1$. The sum on the right hand side is

$$\chi(a)\sum_{\substack{b=1\\(b,q)=1}}^{q} \chi(ba)e^{2\pi i ba/q} = \chi(a)G(\chi,1). \tag{18}$$

Therefore, by Theorem 3,

$$S(q,a) = \left(\frac{a}{q}\right)\epsilon(q)\sqrt{q}$$

where $\epsilon(q) = 1$ or i according as $q \equiv 1$ (mod 4) or 3 (mod 4). By (15),

$$S(pq,1) = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)\epsilon(p)\epsilon(q)\sqrt{pq}. \tag{19}$$

By Theorem 2, the left hand side is $\epsilon(pq)\sqrt{pq}$. Thus,

$$\epsilon(pq) = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)\epsilon(p)\epsilon(q), \tag{20}$$

from which Theorem 1 is immediate.

3. Poisson's summation formula

It remains to prove the θ-function identity (3) and deduce (5) from it. The usual tool for deriving (3) is Poisson's summation formula.

Recall Féjer's fundamental theorem [Mur, 69–72] concerning Fourier series. Let $f(x)$ be a function of a real variable which is bounded, measurable, and periodic with period 1. The Fourier coefficients of f are, by definition, given by

$$c_n = \int_0^1 f(x)e^{-2\pi inx}dx, \tag{21}$$

for each n in $\mathbb{Z}$. The partial sums of the Fourier series of f are defined as

$$S_N(x) = \sum_{|n|\leq N} c_n e^{2\pi inx}. \tag{22}$$

Let $x_0 \in \mathbb{R}$ be such that $f(x)$ admits left and right limits there:

$$f(x_0 \pm 0) = \lim_{h\to 0^+} f(x_0 \pm h). \tag{23}$$

Then Féjer proved

$$\frac{f(x_0+0)+f(x_0-0)}{2} = \lim_{N\to\infty} \frac{S_0(x)+S_1(x)+\cdots+S_N(x)}{N+1}. \tag{24}$$

If $f(x)$ is continuous at x_0, and the partial sums $S_N(x_0)$ converge, then

$$f(x_0) = c_0 + \sum_{n=1}^{\infty}(c_n e^{2\pi inx} + c_{-n}e^{-2\pi inx}). \tag{25}$$

When $f(x)$ is continuous and $\sum_{n=-\infty}^{\infty} |c_n| < \infty$, then the function is represented by the absolutely convergent Fourier series:

$$f(x) = \sum_{n=-\infty}^{\infty} c_n e^{2\pi inx}. \tag{26}$$

If $F(x)$ is continuous such that

$$\int_{-\infty}^{\infty} |F(x)|dx < \infty, \tag{27}$$

then we define its Fourier transform by

$$\hat{F}(u) = \int_{-\infty}^{\infty} F(x)e^{-2\pi ixu}dx. \tag{28}$$

It is also a continuous function of u, and if

$$\int_{-\infty}^{\infty} |\hat{F}(u)|du < \infty, \tag{29}$$

then we have the Fourier inversion formula:

$$F(x) = \int_{-\infty}^{\infty} \hat{F}(u)e^{2\pi ixu}du. \tag{30}$$

Lemma 1.

$$\int_{-\infty}^{\infty} e^{-\pi x^2} dx = 1. \tag{31}$$

Proof. We have upon squaring the left hand side

$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-\pi(x^2+y^2)}\, dx\, dy.$$

Switching to polar coordinates ($x = r\cos\theta$, $y = r\sin\theta$) and evaluating the Jacobian, the above integral becomes

$$\int_0^{\infty}\int_0^{2\pi} e^{-\pi r^2} r\, d\theta\, dr = 2\pi \int_0^{\infty} e^{-\pi r^2} r dr = 1, \tag{32}$$

as desired. □

Lemma 2. *For any $u \in \mathbb{R}$,*

$$\int_{-\infty}^{\infty} e^{-\pi(x+iu)^2} dx = 1. \tag{33}$$

Proof. Observe that

$$\begin{aligned}\frac{\partial}{\partial u}\int_0^{\infty} e^{-\pi(x+iu)^2} dx &= \int_{-\infty}^{\infty}\Big(\frac{\partial}{\partial u} e^{-\pi(x+iu)^2}\Big) dx\\ &= 2\pi i \int_{-\infty}^{\infty} (x+iu) e^{-\pi(x+iu)^2} dx\\ &= i\int_{-\infty}^{\infty} \frac{\partial}{\partial x} e^{-\pi(x+iu)^2} dx\\ &= \Big[ie^{-\pi(x+iu)^2}\Big]_{x=-\infty}^{x=+\infty} = 0,\end{aligned} \tag{34}$$

so that the integral is independent of u. Setting $u = 0$ and using Lemma 1 gives the desired result. □

We now derive:

Theorem 4. *Let $F \in L^1(\mathbb{R})$. Suppose that the series $\sum_{n\in\mathbb{Z}} F(n+v)$ converges absolutely and uniformly in v and that $\sum_{m\in\mathbb{Z}} |\hat{F}(m)| < \infty$. Then*

$$\sum_{n\in\mathbb{Z}} F(n+v) = \sum_{n\in\mathbb{Z}} \hat{F}(n) e^{2\pi i n v}. \tag{35}$$

Proof. The function

$$G(v) = \sum_{n\in\mathbb{Z}} F(n+v) \tag{36}$$

is a continuous function of v and of period 1. The Fourier coefficients of G are given by

$$\begin{aligned} c_m &= \int_0^1 G(v)e^{-2\pi imv}dv \\ &= \sum_{n\in\mathbb{Z}}\int_0^1 F(n+v)e^{-2\pi imv}dv \\ &= \sum_{n\in\mathbb{Z}}\int_n^{n+1} F(x)e^{-2\pi imx}dx \qquad (37) \\ &= \int_{-\infty}^{\infty} F(x)e^{-2\pi imx}dx \\ &= \hat{F}(m). \end{aligned}$$

Since $\sum_{m\in\mathbb{Z}}|\hat{F}(m)| < \infty$, we can represent G by its Fourier series:

$$\sum_{n\in\mathbb{Z}} F(n+v) = \sum_{n\in\mathbb{Z}} \hat{F}(n)e^{2\pi inv}, \qquad (38)$$

as desired. □

Corollary 1 (Poisson's summation formula). With F as in Theorem 4, we have

$$\sum_{n\in\mathbb{Z}} F(n) = \sum_{n\in\mathbb{Z}} \hat{F}(n). \qquad (39)$$

Proof. Set $v = 0$ in the Theorem. □

Now we can deduce the functional equations of the θ-function.

Theorem 5. *For $t > 0$,*

$$\sum_{n\in\mathbb{Z}} e^{-n^2\pi/t} = t^{\frac{1}{2}} \sum_{n\in\mathbb{Z}} e^{-n^2\pi t}. \qquad (40)$$

Proof. We apply Corollary 1 to the function $F(x) = e^{-\pi x^2 t}$. It clearly is an element of $L^1(\mathbb{R})$ and the series

$$\sum_{n\in\mathbb{Z}} e^{-\pi(n+v)^2 t}$$

converges absolutely and uniformly in v. Moreover,

$$\begin{aligned} \hat{F}(m) &= \int_{-\infty}^{\infty} e^{-\pi x^2 t}e^{-2\pi ixm}dx \\ &= e^{-\pi m^2/t}\int_{-\infty}^{\infty} e^{-\pi(x\sqrt{t}+im/\sqrt{t})^2}dx \qquad (41) \\ &= t^{-1/2}e^{-\pi m^2/t}, \end{aligned}$$

by Lemma 2. Thus $\sum_{m\in\mathbb{Z}}|\hat{F}(m)| < \infty$, and we can apply Corollary 1 to deduce the result. □

If we define for $z \in \mathbb{C}$, with $\Im(z) > 0$,

$$\Theta(z) = \sum_{n \in \mathbb{Z}} e^{i\pi n^2 z},$$

then (40) says that

$$\Theta\Big(-\frac{1}{it}\Big) = t^{1/2}\Theta(it).$$

By analytic continuation, we deduce

$$\Theta\Big(-\frac{1}{z}\Big) = \Big(\frac{z}{i}\Big)^{1/2}\Theta(z). \tag{40$'$}$$

4. The Landsberg–Schaar identity

It now only remains to prove (5). In addition to Theorem 5, we will need:

Lemma 3. *Let $a, b \in \mathbb{Z}$. Let $f(x)$ be a differentiable function on $[a, b]$. Then*

$$\frac{1}{2}f(a) + f(a+1) + \cdots + f(b-1) + \frac{1}{2}f(b) = \int_a^b f(t)dt + O\Big(\int_a^b |f'(t)|dt\Big). \tag{42}$$

Remark. This is a special case of the well-known Euler-Maclaurin summation formula (see for example, [Mur, 21]).

Proof. We have

$$\int_n^{n+1}\Big(t - n - \frac{1}{2}\Big) f'(t)dt = \frac{f(n) + f(n+1)}{2} - \int_n^{n+1} f(t)dt. \tag{43}$$

Summing this identity over the range $a \le n \le b-1$ and noting that $|t - n - \frac{1}{2}| \le 1$ for $t \in [n, n+1]$ gives the desired result. □

As a corollary, we deduce:

Lemma 4.

$$\sum_{t=-\infty}^{\infty} e^{-(b+tp)^2\epsilon} \sim \frac{1}{p}\sqrt{\frac{\pi}{\epsilon}} \tag{44}$$

as $\epsilon \to 0$.

Proof. We apply Lemma 3 to $f(t) = e^{-(b+tp)^2\epsilon}$ for $t \in [-N, N]$ and let $N \to \infty$, to deduce

$$\sum_{t=-\infty}^{\infty} e^{-(b+tp)^2\epsilon} = \int_{-\infty}^{\infty} e^{-(b+tp)^2\epsilon}dt + O(\epsilon). \tag{45}$$

By Lemma 1, the integral equals $\frac{\sqrt{\pi}}{p\sqrt{\epsilon}}$ from which the lemma follows. □

Remark. Notice that the lemma is valid for complex values of ϵ provided that $-\frac{\pi}{2} < \arg\epsilon < \frac{\pi}{2}$, that is for $\Re(\epsilon) > 0$.

Now consider

$$\theta\left(\epsilon - \frac{2iq}{p}\right) = \sum_{n=-\infty}^{\infty} e^{-\pi n^2(\epsilon - 2iq/p)} = \sum_{b=0}^{p-1} e^{2\pi i b^2 q/p}\left(\sum_{n\equiv b (\text{mod } p)} e^{-\pi n^2 \epsilon}\right). \tag{46}$$

By Lemma 4, the inner sum on the right hand side of (46) is asymptotic to $\frac{\sqrt{\pi}}{p\sqrt{\epsilon}}$ as $\epsilon \to 0^+$. Therefore, as $\epsilon \to 0^+$,

$$\theta\left(\epsilon - \frac{2iq}{p}\right) \sim \frac{\sqrt{\pi}S(p,q)}{p\sqrt{\epsilon}} \tag{47}$$

in the notation of (14). By (40$'$),

$$\theta\left(\frac{1}{\epsilon - \frac{2iq}{p}}\right) = \left(\epsilon - \frac{2iq}{p}\right)^{1/2}\theta\left(\epsilon - \frac{2iq}{p}\right)$$

so that

$$\frac{\sqrt{\pi}S(p,q)}{p\sqrt{\epsilon}} \sim \left(\epsilon - \frac{2iq}{p}\right)^{-1/2}\theta\left(\frac{1}{\epsilon - \frac{2iq}{p}}\right) \tag{48}$$

as $\epsilon \to 0^+$. If we define τ by the equation

$$\frac{1}{\epsilon - 2iq/p} = \frac{\epsilon + 2iq/p}{\epsilon^2 + 4q^2/p^2} = \tau + \frac{ip}{2q}, \tag{49}$$

then $\tau \to 0$ as $\epsilon \to 0^+$. Moreover, $\Re(\tau) > 0$, for $\epsilon > 0$. We have

$$\begin{aligned}\theta\left(\frac{1}{\epsilon - \frac{2iq}{p}}\right) &= \theta\left(\tau + \frac{ip}{2q}\right) \\ &= \sum_{n=-\infty}^{\infty} e^{-\pi n^2(\tau + ip/2q)} \\ &= \sum_{b=0}^{4q-1} e^{-2\pi i b^2 p/4q}\left(\sum_{n\equiv b\ (\text{mod } 4q)} e^{-\pi n^2 \tau}\right).\end{aligned} \tag{50}$$

Notice that as $\tau \to 0$, the inner sum on the right hand side of (50) can be treated as in (46) and we deduce

$$\theta\left(\frac{1}{\epsilon - 2iq/p}\right) \sim \frac{S(4q,-p)\sqrt{\pi}}{4q\sqrt{\tau}} \tag{51}$$

as $\epsilon \to 0^+$. From (49),

$$\frac{\tau}{\epsilon} = -\frac{ip}{2q(\epsilon - 2iq/p)}$$

so that from (48), we obtain

$$\frac{S(p,q)}{p}\sqrt{\frac{-ip}{2q}} = \frac{S(4q,-p)}{4q}. \tag{52}$$

Now $\sqrt{-i} = e^{-i\pi/4}$, the determination being ascertained in several ways. (For example, take $p = q = 1$ in (52) to determine it.) Upon noting that

$$\sum_{b=o}^{4q-1} e^{\frac{-2\pi i p b^2}{4q}} = 2\sum_{b=0}^{2q-1} e^{\frac{-\pi i b^2 p}{2q}}$$

we immediately obtain (5). This completes the proof of the Landsberg – Schaar identity.

5. Concluding remarks

It is possible to give an elementary derivation of the θ-function transformation law by Polya [Po] (see also [Be]).

The proof given above appears with very few details in two places. The first is [DM] and the second is [Be]. It is also mentioned in several places such as [Te], [BEW], and [BE]. We hope that our exposition makes this idea more widely known and supplies the relevant details of the proof which are omitted in the literature.

We also refer the reader to the website: http://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html for an extensive history and references of the proofs of the law of quadratic reciprocity.

References

[AR] V. Armitage and A. Rogers, Gauss sums and quantum mechanics, *J. Phys. A.* **33** no. 34 (2000) 5993–6002

[Be] R. Bellman, *A Brief Introduction to Theta Functions*, (Rinehart & Winston) (1961)

[BE] B. Berndt and R. Evans, Determination of Gauss sums, *Bulletin of the Amer. Math. Society.* **5** no. 2 (1981) 107–129

[BEW] B. Berndt, R. Evans and K. S. Williams, Gauss and Jacobi Sums, *Canadian Mathematical Society Series of Monographs and Advanced Texts* **21**, (Wiley Interscience, New York) (1998)

[DM] H. Dym and H. P. McKean Jr., Fourier Series and Integrals, *Probability and Mathematical Statistics*, (Academic Press) no. 14 (1972)

[H] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Springer-Verlag, (1981)

[Kub] T. Kubota, On Automorphic Functions and the Reciprocity Law in a Number Field, *Lectures in Mathematics*, 2 (1969)

[Lan] G. Landsberg, Zur Theorie der Gausschen Summen und der linearen Transformation der Thetafunctionen, *J. Reine Angew Math.* **111** (1893) 234–253

[Mur] R. Murty, Problems in Analytic Number Theory, *Graduate Texts in Mathematics*, Springer-Verlag, (2001)

[Po] G. Polya, Elementarer Beweis einer Thetaformel, Sitz. der *Phys-Math Klasse*, (Berlin) (1927) 158–161 (see also Collected Papers, vol. 1 303–306, MIT Press, 1974)

[Sc] M. Schaar, Mémoire sur la théorie des résidus quadratiques, *Acad. Roy. Sci. Lettres Beaux Arts Belgique* **24** (1850) 14p

[Te] A. Terras, *Harmonic Analysis on Symmetric Spaces and Applications*, vol. 1, Springer-Verlag, (New York) (1985)