CHAPTER 7

Gauss Sums and Quadratic Reciprocity

7.1. Gauss Sums

Recall the Law of quadratic reciprocity, that if p and q are distinct odd primes, then

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

There are many proofs of this – Gauss alone discovered six. Our aim here, however, is to give a second proof of this result, a proof discovered by Dirichlet and based on ideas from Fourier series.

Throughout this chapter, we use the notation that $e(y)=\mathrm{e}^{2\pi\mathrm{i}y}$ for every $y\in\mathbb{R}$.

Suppose that $q\in\mathbb{N}$ and $a\in\mathbb{Z}$ satisfy $(a,q)=1$. The Gauss sum

$$S(q,a)=\sum_{x=1}^{q}e\left(\frac{ax^2}{q}\right)$$

has many interesting properties, the first of which is a multiplicative property which simplifies its evaluation to cases when q is a prime power.

THEOREM 7.1. *Suppose that $q_1,q_2\in\mathbb{N}$ satisfy $(q_1,q_2)=1$. Suppose further that $a\in\mathbb{Z}$ satisfies $(a,q_1q_2)=1$. Then*

$$S(q_1q_2,a)=S(q_1,q_2a)S(q_2,q_1a).$$

PROOF. Since $(q_1,q_2)=1$, it follows from Theorem 3.5 that as x_1 and x_2 run through complete sets of residues modulo q_1 and q_2 respectively, $q_2x_1+q_1x_2$ runs through a complete set of residues modulo q_1q_2. Hence

$$S(q_1q_2,a)=\sum_{z=1}^{q_1q_2}e\left(\frac{az^2}{q_1q_2}\right)=\sum_{x_1=1}^{q_1}\sum_{x_2=1}^{q_2}e\left(\frac{a(q_2x_1+q_1x_2)^2}{q_1q_2}\right).$$

Note now that $(q_2x_1+q_1x_2)^2\equiv q_2^2x_1^2+q_1^2x_2^2 \bmod q_1q_2$. It follows that

$$S(q_1q_2,a)=\sum_{x_1=1}^{q_1}\sum_{x_2=1}^{q_2}e\left(\frac{aq_2x_1^2}{q_1}+\frac{aq_1x_2^2}{q_2}\right)=\sum_{x_1=1}^{q_1}e\left(\frac{aq_2x_1^2}{q_1}\right)\sum_{x_2=1}^{q_2}e\left(\frac{aq_1x_2^2}{q_2}\right).$$

The result follows. ○

The Law of quadratic reciprocity can be deduced from Theorem 7.1 and the two results below.

THEOREM 7.2. *Suppose that $p\in\mathbb{N}$ is an odd prime, and $a\in\mathbb{Z}$ satisfies $(a,p)=1$. Then*

$$S(p,a)=\left(\frac{a}{p}\right)_L S(p,1). \tag{7.1}$$

Theorem 7.3. *Suppose that $q \in \mathbb{N}$ is odd. Then $S(q,1) = \epsilon_q q^{\frac{1}{2}}$, where*

$$\epsilon_q = \begin{cases} 1, & \text{if } q \equiv 1 \bmod 4, \\ \mathrm{i}, & \text{if } q \equiv -1 \bmod 4. \end{cases}$$

To deduce the Law of quadratic reciprocity, note that by Theorems 7.1 and 7.2, we have, for distinct primes $p, q \in \mathbb{N}$, that

$$S(pq,1) = S(p,q)S(q,p) = \left(\frac{q}{p}\right)_L S(p,1) \left(\frac{p}{q}\right)_L S(q,1).$$

It follows from Theorem 7.3 that

$$\left(\frac{q}{p}\right)_L \left(\frac{p}{q}\right)_L = \frac{S(pq,1)}{S(p,1)S(q,1)} = \frac{\epsilon_{pq}}{\epsilon_p \epsilon_q}.$$

Note now that the right hand side has value -1 if $p \equiv q \equiv -1 \bmod 4$ and value 1 otherwise. The Law of quadratic reciprocity follows.

Proof of Theorem 7.2. Consider the congruence $x^2 \equiv n \bmod p$. Clearly the number of solutions of this congruence is given by $1 + (n/p)_L$, so that

$$S(p,a) = \sum_{x=1}^{p} e\left(\frac{ax^2}{p}\right) = \sum_{n=1}^{p} \left(1 + \left(\frac{n}{p}\right)_L\right) e\left(\frac{an}{p}\right) = \sum_{n=1}^{p} \left(\frac{n}{p}\right)_L e\left(\frac{an}{p}\right),$$

since

$$\sum_{n=1}^{p} e\left(\frac{an}{p}\right) = 0.$$

We now make the substitution $an \equiv m \bmod p$, and note that as n runs through a complete set of residues modulo p, so does m. Hence, denoting by a^{-1} the natural number satisfying $1 \leqslant a^{-1} < p$ and $aa^{-1} \equiv 1 \bmod p$, we have

$$S(p,a) = \sum_{m=1}^{p} \left(\frac{a^{-1}m}{p}\right)_L e\left(\frac{m}{p}\right) = \left(\frac{a^{-1}}{p}\right)_L \sum_{m=1}^{p} \left(\frac{m}{p}\right)_L e\left(\frac{m}{p}\right) = \left(\frac{a}{p}\right)_L \sum_{m=1}^{p} \left(\frac{m}{p}\right)_L e\left(\frac{m}{p}\right). \tag{7.2}$$

In particular, putting $a = 1$ in (7.2), we obtain

$$S(p,1) = \sum_{m=1}^{p} \left(\frac{m}{p}\right)_L e\left(\frac{m}{p}\right). \tag{7.3}$$

The identity (7.1) now follows on combining (7.2) and (7.3). ○

To complete the proof of the Law of quadratic reciprocity, it remains to establish Theorem 7.3, which we do in Section 7.3. As the proof involves ideas concerning the convergence of Fourier series, we first make a very brief study of this in the next section.

7.2. Convergence of Fourier Series

Suppose that a function $f : \mathbb{R} \to \mathbb{C}$ is Riemann integrable over the interval $[0,1]$ and is periodic with period 1. We define the Fourier coefficient c_h, for every $h \in \mathbb{Z}$, by

$$c_h = c_h(f) = \int_0^1 f(y)e(-hy)\,\mathrm{d}y.$$

The formal series

$$\sum_{h=-\infty}^{\infty} c_h(f)e(hy)$$

is called the Fourier series of the function f.

Our task here is to obtain sufficient conditions for the Fourier series of a given function f to converge to f, or at least some function closely related to f. The basic theorem in this study is the following result.

Theorem 7.4 (Riemann–Lebesgue lemma). *Suppose that $a,b\in\mathbb{R}$ and $a<b$. Suppose further that the function $f:[a,b]\to\mathbb{R}$ is Riemann integrable over the interval $[a,b]$. For any number $\lambda\in\mathbb{R}$, let*

$$I(\lambda,f)=\int_a^b f(y)\mathrm{e}^{\mathrm{i}\lambda y}\,\mathrm{d}y.$$

Then $I(\lambda,f)\to 0$ as $\lambda\to\infty$.

Proof. Our first task is to approximate f in $[a,b]$ by a step function. Let $\epsilon>0$ be given. For any sufficiently large $k\in\mathbb{N}$, there exists a dissection

$$\Delta_k : a=y_0<y_1<\ldots<y_k=b$$

of $[a,b]$ such that the upper sum $S(f,\Delta_k)$ and the lower sum $s(f,\Delta_k)$ satisfy

$$0\leqslant S(f,\Delta_k)-s(f,\Delta_k)<\epsilon.$$

For every $y\in[a,b]$, define

$$f_k(y)=\begin{cases}\sup\{f(y):y\in[y_{j-1},y_j]\}, & \text{if } y\in(y_{j-1},y_j],\\ f_k(y_1), & \text{if } y=y_0.\end{cases}$$

Clearly f_k is a step function in, and hence Riemann integrable over, the interval $[a,b]$. Furthermore, $f(y)\leqslant f_k(y)$ for all $y\in[a,b]$. It follows that f_k-f is Riemann integrable over $[a,b]$, and

$$|f_k(y)-f(y)|=f_k(y)-f(y)$$

for all $y\in[a,b]$. Hence

$$|I(\lambda,f_k)-I(\lambda,f)|=\int_a^b|f_k(y)-f(y)|\,\mathrm{d}y=\int_a^b(f_k(y)-f(y))\,\mathrm{d}y=S(f,\Delta_k)-\int_a^b f(y)\,\mathrm{d}y<\epsilon.$$

On the other hand,

$$I(\lambda,f_k)=\sum_{j=1}^k\int_{y_{j-1}}^{y_j}f_k(y_j)\mathrm{e}^{\mathrm{i}\lambda y}\,\mathrm{d}y=\sum_{j=1}^k f_k(y_j)\frac{\mathrm{e}^{\mathrm{i}\lambda y_j}-\mathrm{e}^{\mathrm{i}\lambda y_{j-1}}}{\mathrm{i}\lambda}\to 0$$

as $\lambda\to\infty$, so that $|I(\lambda,f_k)|<\epsilon$ for all sufficiently large λ. Then $|I(\lambda,f)|<2\epsilon$ for all sufficiently large λ. ○

We now establish a result concerning the convergence of a Fourier series.

Theorem 7.5. *Suppose that a function $f:\mathbb{R}\to\mathbb{C}$ is Riemann integrable over the interval $[0,1]$ and is periodic with period 1. Let $y\in\mathbb{R}$. Suppose that the limits*

$$f(y\pm)=\lim_{\delta\to 0\pm}f(y+\delta)\quad\textit{and}\quad f'_\pm(y)=\lim_{\delta\to 0\pm}\frac{f(y+\delta)-f(y\pm)}{\delta}$$

all exist, and the functions

$$g_\pm(u)=\begin{cases}\dfrac{f(u)-f(y\pm)}{u-y}-f'_\pm(y), & \textit{if } u\neq y,\\[2ex] 0, & \textit{if } u=y,\end{cases}\tag{7.4}$$

are Riemann integrable over $[y,y+\frac{1}{2}]$ and $[y-\frac{1}{2},y]$ respectively. Then

$$\lim_{H\to\infty}\sum_{n=-H}^{H}c_h(f)e(hy)=\frac{f(y+)+f(y-)}{2}.$$

Proof. In view of periodicity, we can write

$$c_h(f)=\int_{y-\frac{1}{2}}^{y+\frac{1}{2}}f(u)e(-hu)\,\mathrm{d}u.$$

For every $H\in\mathbb{N}$, let

$$S_H=\sum_{n=-H}^{H}c_h(f)e(hy).$$

Then

$$S_H = \int_{y-\frac{1}{2}}^{y+\frac{1}{2}} f(u) \sum_{n=-H}^{H} e(h(y-u))\,\mathrm{d}u.$$

Simple calculations give

$$\sum_{n=-H}^{H} e(h(y-u)) = \begin{cases} \dfrac{\sin \pi(2H+1)(y-u)}{\sin \pi(y-u)}, & \text{if } u \neq y, \\ 2H+1, & \text{if } u = y. \end{cases} \tag{7.5}$$

Note that the right hand side of (7.5) is continuous and Riemann integrable. Hence $S_H = I_1 + I_2$, where

$$I_1 = \int_{-\frac{1}{2}}^{0} f(y+v)\frac{\sin \pi(2H+1)v}{\sin \pi v}\,\mathrm{d}v \quad \text{and} \quad I_2 = \int_{0}^{\frac{1}{2}} f(y+v)\frac{\sin \pi(2H+1)v}{\sin \pi v}\,\mathrm{d}v.$$

Consider now the integral I_1. Clearly it follows from (7.4) that

$$\begin{aligned} I_1 = {} & \int_{-\frac{1}{2}}^{0} g_-(y+v)\frac{v}{\sin \pi v}\sin \pi(2H+1)v\,\mathrm{d}v \\ & + f'_-(y)\int_{-\frac{1}{2}}^{0} \frac{v}{\sin \pi v}\sin \pi(2H+1)v\,\mathrm{d}v + f(y-)\int_{-\frac{1}{2}}^{0} \frac{\sin \pi(2H+1)v}{\sin \pi v}\,\mathrm{d}v. \end{aligned}$$

By Theorem 7.4, the first two integrals on the right hand side both converge to 0 as $H \to \infty$. The last term is equal to

$$f(y-)\int_{-\frac{1}{2}}^{0} \sum_{h=-H}^{H} e(hv)\,\mathrm{d}v = f(y-)\left(\frac{1}{2} + \sum_{\substack{h=-H \\ h\neq 0}}^{H} \frac{1-(-1)^h}{2\pi \mathrm{i} h}\right) = \frac{1}{2}f(y-).$$

Similarly $I_2 \to \frac{1}{2}f(y+)$ as $H \to \infty$. ○

7.3. Proof of Theorem 7.3

Let $q \in \mathbb{N}$ be odd. For every real number $\theta \in [0,1]$, let

$$f(\theta) = \sum_{n=0}^{q-1} e\left(\frac{(n+\theta)^2}{q}\right),$$

and note that $S(q,1) = f(0) = f(1)$. The function f has the Fourier series

$$\sum_{h=-\infty}^{\infty} c_h e(hy),$$

where, for every $h \in \mathbb{Z}$, the coefficient

$$\begin{aligned} c_h &= \int_0^1 \sum_{n=0}^{q-1} e\left(\frac{(n+\theta)^2}{q}\right) e(-h\theta)\,\mathrm{d}\theta = \sum_{n=0}^{q-1} \int_n^{n+1} e\left(\frac{\phi^2}{q} - h\phi\right) e(hn)\,\mathrm{d}\phi = \int_0^q e\left(\frac{\phi^2}{q} - h\phi\right)\mathrm{d}\phi \\ &= q\int_0^1 e(q\theta^2 - qh\theta)\,\mathrm{d}\theta = qe\left(-\frac{qh^2}{4}\right)\int_0^1 e\left(q\left(\theta - \frac{h}{2}\right)^2\right)\mathrm{d}\theta = qe\left(-\frac{qh^2}{4}\right)\int_{-\frac{h}{2}}^{1-\frac{h}{2}} e(q\theta^2)\,\mathrm{d}\theta. \end{aligned}$$

By Theorem 7.5, the Fourier series converges to f in $[0,1]$, so that

$$S(q,1) = \lim_{N\to\infty} \sum_{h=-N}^{N} c_h e(h0) = \lim_{N\to\infty} \sum_{h=-N}^{N} c_h. \tag{7.6}$$

If h is even, then $-qh^2/4 \in \mathbb{Z}$. It follows that as $N \to \infty$, we have

$$\begin{aligned}(7.7)\qquad \sum_{\substack{h=-2N\\ h \text{ even}}}^{2N} c_h &= \sum_{\substack{h=-2N\\ h \text{ even}}}^{2N} qe\left(-\frac{qh^2}{4}\right)\int_{-\frac{h}{2}}^{1-\frac{h}{2}} e(q\theta^2)\,\mathrm{d}\theta = \sum_{\substack{h=-2N\\ h \text{ even}}}^{2N} q\int_{-\frac{h}{2}}^{1-\frac{h}{2}} e(q\theta^2)\,\mathrm{d}\theta \\ &= q\int_{-N}^{N+1} e(q\theta^2)\,\mathrm{d}\theta \to q\int_{-\infty}^{\infty} e(q\theta^2)\,\mathrm{d}\theta = q^{\frac{1}{2}} I,\end{aligned}$$

where

$$I = \int_{-\infty}^{\infty} e(\theta^2)\,\mathrm{d}\theta.$$

If h is odd, then $h^2 \equiv 1 \bmod 4$, and so $qh^2 \equiv q \bmod 4$. It follows that as $N \to \infty$, we have

$$\begin{aligned}(7.8)\qquad \sum_{\substack{h=-2N\\ h \text{ odd}}}^{2N} c_h &= \sum_{\substack{h=-2N\\ h \text{ odd}}}^{2N} qe\left(-\frac{qh^2}{4}\right)\int_{-\frac{h}{2}}^{1-\frac{h}{2}} e(q\theta^2)\,\mathrm{d}\theta = qe\left(-\frac{q}{4}\right)\sum_{\substack{h=-2N\\ h \text{ odd}}}^{2N} \int_{-\frac{h}{2}}^{1-\frac{h}{2}} e(q\theta^2)\,\mathrm{d}\theta \\ &= qe\left(-\frac{q}{4}\right)\int_{-N+\frac{1}{2}}^{N+\frac{1}{2}} e(q\theta^2)\,\mathrm{d}\theta \to q^{\frac{1}{2}} e\left(-\frac{q}{4}\right) I.\end{aligned}$$

Combining (7.6)–(7.8), we have

$$(7.9)\qquad S(q,1) = q^{\frac{1}{2}}\left(1 + e\left(-\frac{q}{4}\right)\right) I.$$

Putting $q = 1$ in (7.9), we have $1 = (1 - \mathrm{i})I$. Hence

$$S(q,1) = \frac{q^{\frac{1}{2}}(1 + e(-q/4))}{1-\mathrm{i}}.$$

Theorem 7.3 follows easily.