Theta functions and their applications

Håvard Damm-Johnsen 2019

Contents

1 Certain Theta Functions **1**
1.1 Introduction 1
1.2 The Jacobi theta functions 3
1.3 The transformation formula 4

2 Applications to Number Theory **6**
2.1 Jacobi's four-square theorem 6
2.2 Quadratic reciprocity 7

3 Epilogue **11**

Bibliography **11**

1 Certain Theta Functions

1.1 Introduction

The classical theta function,

$$\theta(\tau) := \sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau} = 1 + 2\sum_{n=1}^{\infty} e^{\pi i n^2 \tau}$$

was introduced by Euler in a letter to Goldbach, as a tool in the study of representation of integers as sums of squares. Observe that

$$\theta^2(\tau) = \left(\sum_{m=-\infty}^{\infty} e^{\pi i m^2 \tau}\right)\left(\sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau}\right) = \sum_{k=1}^{\infty} r_2(k) e^{\pi i k \tau},$$

where $r_2(k)$ is the number of ways in which k can be written as a sum of two squares, since we get one contribution from each ordered pair (m,n) such that $e^{\pi i m^2 \tau} e^{\pi i n^2 \tau} = e^{\pi i k \tau}$, or equivalently, $k = n^2 + m^2$. This line of inquiry was taken up by Jacobi, who first proved the fundamental transformation formula for θ, and the four-square theorem of section 2.1. Our point of departure will be slightly more general.

Definition 1.1. For $z \in \mathbb{C}$ and $\tau \in \mathfrak{H} := \{\tau \in \mathbb{C} : \operatorname{Im}\tau > 0\}$, we define the **theta function** to be

$$\theta(z,\tau) = \sum_{n=-\infty}^{\infty} e^{2\pi i n z + \pi i n^2 \tau}.$$

Remark. Our notation follows Riemann and Mumford [Mum83], but there is no shortage of alternative conventions.

We see that $\theta(\tau) = \theta(0,\tau)$. The condition that $\tau \in \mathfrak{H}$ ensures that by the ratio test, $\theta(z,\tau)$ converges absolutely, and moreover uniformly on compact sets in the first variable, hence is an entire function in z. A fundamental property of the theta function is the following:

Proposition 1.2. *The theta function satisfies the transformation equations*

$$\theta(z+1,\tau) = \theta(z,\tau) \quad \textit{and} \quad \theta(z+\tau,\tau) = e^{-2\pi i z} e^{-\pi i \tau} \theta(z,\tau).$$

Proof. The first is immediate from the definition, the second follows from the quick computation

$$\begin{aligned}\theta(z+\tau,\tau) &= \sum_{n=-\infty}^{\infty} e^{2\pi i n z + 2\pi i n \tau + \pi i n^2 \tau} = e^{-2\pi i z} e^{-\pi i \tau} \sum_{n=-\infty}^{\infty} e^{2\pi i (n+1) z + 2\pi i (n+1)^2 \tau} \\ &= e^{-2\pi i z} e^{-\pi i \tau} \theta(z,\tau).\end{aligned}$$

□

Recall that by Liouville's theorem, every entire doubly periodic function is constant. One might ask what happens if we weaken the periodicity condition slightly. The above proposition can be interpreted as saying that when viewed as a function of z, θ has period 1, and a *quasi-period* τ with *periodicity factor* $e^{-2\pi i z} e^{-\pi \tau}$. In other words, it is a *quasi-periodic function* with respect to the lattice $\Lambda := \mathbb{Z} + \tau\mathbb{Z}$. Conversely, considering quasi-periodic functions of this sort naturally gives rise to the theta function:

Theorem 1.3 (Functional equation for θ)**.** *Suppose $f\colon \mathbb{C} \to \mathbb{C}$ is entire and non-constant, $f(z) = f(z+1)$ and $f(z+\tau) = e^{az+b} f(z)$ for some fixed $a, b \in \mathbb{C}$ and any $z \in \mathbb{C}$. If $a = 0$, then $f(z) = e^{2\pi i z}$, and if $a = -2\pi i$, then*

$$f(z) = a_0 \theta\left(-z - \frac{1}{2}\tau - \frac{b}{2\pi i}, \tau\right),$$

for some $a_0 \in \mathbb{C}$.

Proof [Mum83]. Expanding f in terms of its Fourier series, we have that

$$f(z) = \sum_{n=-\infty}^{\infty} a_n e^{2\pi i n z} \qquad \text{for some } a_n \in \mathbb{C}.$$

Using the periodicity relations, we compute $f(z+\tau+1)$ in two ways, namely

$$f(z+\tau+1) = f(z+\tau) = e^{az+b} f(z)$$

and

$$f(z+\tau+1) = e^{a(z+1)+b} f(z+1) = e^{a(z+1)+b} f(z) = e^{a} e^{az+b} f(z),$$

so $a = 2\pi i k$ for some $k \in \mathbb{Z}$. Substituting in the Fourier series of f, we find that

$$f(z+\tau) = e^{2\pi i k z + b} f(z) = \sum_{n=-\infty}^{\infty} a_n e^{2\pi i k z + b + 2\pi i n z} = \sum_{n=-\infty}^{\infty} a_{n-k} e^{2\pi i n z + b},$$

which gives a recurrence relation for the Fourier coefficients, $a_n = a_{n-k} e^{b - 2\pi n i \tau}$. If $k = 0$, then $a_n = 0$ for all n but possibly $n = 0$, so $f(z) = e^{2\pi i z}$. Taking $k = -1$, we readily see that

$$a_n = a_0 e^{-nb + \pi i n(n-1)\tau} \qquad \text{for all } n \in \mathbb{Z},$$

and so

$$f(z) = a_0 \sum_{n=-\infty}^{\infty} e^{-nb + \pi i n(n-1)\tau + 2\pi i n z} = a_0 \theta\left(-z - \frac{1}{2}\tau - \frac{b}{2\pi i}, \tau\right). \qquad \square$$

Suppose we take $k \geq 1$ in the proof above; then the Fourier coefficients grow rapidly, and so the corresponding function f is not entire. On the other hand, for $k < -1$, one can show that the solutions of the functional equations form a vector space of dimension $|k|$.

1.2 The Jacobi theta functions

Returning to the lattice $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$, we define the following:

Definition 1.4. Let $\tau \in \mathfrak{H}$ and $z \in \mathbb{C}$. The **Jacobi theta functions** are

$$\theta_{00}(z,\tau) := \theta(z,\tau), \qquad \theta_{10}(z,\tau) := e^{\pi i \tau/4 + \pi i z} \theta(z + \tau/2, \tau),$$
$$\theta_{01}(z,\tau) := \theta(z + 1/2, \tau), \qquad \theta_{11}(z,\tau) := e^{\pi i \tau/4 + \pi i (z + 1/2)} \theta(z + (1+\tau)/2, \tau).$$

If $\tau \in \mathfrak{H}$ is fixed, we write $\theta_{ab}(z) := \theta_{ab}(z,\tau)$. The value $\theta_{ab}(0)$ is traditionally called the *theta-nullwerte* of $\theta_{ab}(z,\tau)$.

These functions were studied in great detail by Jacobi. Note that the Jacobi theta functions are simply θ shifted by the half-periods of Λ, modulo a certain scaling factor. This is explained in the more general theory of *theta functions with characteristic*, which is unfortunately beyond the scope of this essay. The Jacobi theta functions are also quasi-elliptic with respect to the same lattice Λ. An astonishing number of formulae involving these functions exist, but we will limit our attention to the following identity:

Theorem 1.5 (Jacobi's identity)**.** *For $\tau \in \mathfrak{H}$ fixed, we have*

$$\theta_{00}^4(0) = \theta_{01}^4(0) + \theta_{10}^4(0).$$

It is easily seen that for any $z \in \mathbb{C}$, $\theta_{11}(-z) = -\theta_{11}(z)$, so that $\theta_{11}(0) = 0$, which explains why θ_{11} is absent from the identity. The identity is particularly interesting from an algebro-geometric point of view, since it gives a parameterisation of the *Fermat quartic* $X^4 + Y^4 = Z^4$ in terms of theta functions.

Let $q := e^{\pi i \tau}$. Using Jacobi's triple product identity,[1] one can prove that

$$\theta_{11}(z,q) = -2q^{1/4}\sin\pi z \prod_{n=1}^{\infty}(1-q^{2n})(1-2q^{2n}\cos 2\pi z + q^{4n}),$$
$$\theta_{10}(z,q) = 2q^{1/4}\cos\pi z \prod_{n=1}^{\infty}(1-q^{2n})(1+2q^{2n}\cos 2\pi z + q^{4n}),$$

and from these we readily compute

$$\lim_{q\to 0}\frac{\theta_{11}(z,q)}{-2q^{1/4}} = \sin\pi z \quad \text{and} \quad \lim_{q\to 0}\frac{\theta_{10}(z,q)}{2q^{1/4}} = \cos\pi z.$$

Therefore, Jacobi's theta functions can be considered as natural one-parameter deformations of sin and cos. For more details, see [GR04], section 1.6.

1.3 The transformation formula

The transformation formula for the theta function is arguably its most useful property in applications. Without further ado:

Theorem 1.6. *The theta function satisfies the following identity:*

$$\theta\left(\frac{1}{z},-\frac{1}{\tau}\right) = \sqrt{-i\tau}\, e^{\pi i z^2/\tau}\theta(z,\tau).$$

The theorem is not "optimal", since there exists a more general transformation formula, cf. Thm. 7.1 in [Mum83]. However, that one follows without too much effort from the ours, which is quite sufficient for our purposes. We start off with two lemmata:

Lemma 1.7. *We have that*

$$\int_{-\infty}^{\infty} e^{-x^2}\,dx = \sqrt{\pi}.$$

Proof (Poisson). Let I denote the integral on the left. We can consider I^2 as an integral in two variables x and y, and introduce polar coordinates r and ϕ in the (x,y)-plane to yield

$$I^2 = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-x^2-y^2}\,dx\,dy = \int_0^{2\pi}\int_0^{\infty} e^{-r^2} r\,dr\,d\phi = 2\pi\int_0^{\infty}\frac{e^{-u}}{2}\,du = \frac{2\pi}{2} = \pi,$$

so $I = \sqrt{\pi}$. □

Lemma 1.8 (Poisson summation formula)**.** *Suppose $f\colon \mathbb{R}\to\mathbb{C}$ is a Schwarz function. Then*

$$\sum_{n=-\infty}^{\infty} f(x+n) = \sum_{n=-\infty}^{\infty} e^{2\pi i n x}\hat{f}(n),$$

where $\hat{f}$ denotes the Fourier transform of f.

[1] Not to be confused with the above identity.

Proof (sketch). Recognise the left-hand side as a periodic function, write out its Fourier series and re-index after a change of variables in the integral. □

Remark. The condition that f be Schwarz is very far from optimal, but sufficient for our purposes. The classical statement of the Poisson formula is obtained by taking $x = 0$.

Proof of theorem 1.6. Fixing $t \in \mathbb{C}$ with $\operatorname{Re} t > 0$, for $x \in \mathbb{R}$ we define $f(x) := e^{-\pi t x^2}$ and compute

$$\hat{f}(y) = \int_{-\infty}^{\infty} e^{\pi i x y - \pi t x^2} dx = \frac{e^{-\pi y^2/t}}{\sqrt{t}\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-u^2} du = \frac{e^{-\pi y^2/t}}{\sqrt{t}}$$

by the substitution $u = \pi\sqrt{t}(x - iy/t)$ and lemma 1.7. Now by Poisson summation (lemma 1.8), we obtain

$$\sum_{n=-\infty}^{\infty} f(x+n) = \sum_{n=-\infty}^{\infty} e^{-\pi t(x+n)^2} = \sum_{n=-\infty}^{\infty} e^{2\pi i n x} \hat{f}(n) = \frac{1}{\sqrt{t}} \sum_{n=-\infty}^{\infty} e^{2\pi i n x - \pi n^2/t}. \tag{1}$$

Taking $\tau = it$, we have that $\tau \in \mathfrak{H}$, and we see that

$$\sum_{n=-\infty}^{\infty} e^{\pi i \tau (x+n)^2} = e^{\pi i \tau x^2} \sum_{n=-\infty}^{\infty} e^{2\pi i \tau x n + \pi i n^2 \tau} = e^{\pi i \tau x^2} \theta(\tau x, \tau).$$

But now, by eq. (1),

$$e^{\pi i \tau x^2} \theta(\tau x, \tau) = \frac{1}{\sqrt{-i\tau}} \sum_{n=-\infty}^{\infty} e^{2\pi i n x - \pi i n^2/\tau} = \frac{1}{\sqrt{-i\tau}} \theta\left(x, -\frac{1}{\tau}\right),$$

and by analytic continuation, this is valid for any $x \in \mathbb{C}$. Setting $z = \tau x$ and rearranging, we obtain

$$\theta\left(\frac{1}{z}, -\frac{1}{\tau}\right) = \sqrt{-i\tau}\, e^{\pi i z^2/\tau} \theta(z, \tau),$$

as required. □

Corollary 1.9. *Euler's theta function is a modular form of weight* $1/2$ *and level* 2.

Proof. In addition to the regular growth and analyticity conditions, this means that θ transforms like a modular form under $\tau \mapsto \tau + 2$ and $\tau \mapsto -1/\tau$. The first two conditions hold because the series defining θ converges absolutely and uniformly on compact sets. As for the final one, we easily check that $\theta(\tau + 2) = \theta(\tau)$, and setting $z = 0$ in the transformation formula gives

$$\theta\left(-\frac{1}{\tau}\right) = \sqrt{-i\tau}\, \theta(\tau).$$ □

2 Applications to Number Theory

The fact that θ is a modular form allows us to effortlessly derive some of the most famous number-theoretic results of the 17th and 18th centuries. Taking up the thread from the introduction with $\theta^2(z) = \sum_{n=1}^{\infty} r_2(n) e^{\pi i n z}$, we have the following:

Theorem 2.1 (Fermat)**.** *An odd prime p can be written as a sum of two squares if and only if $p \equiv 1 \pmod 4$.*

Proof [BvHZ08]. It follows from corollary 1.9 that θ^2 is a modular form of weight 1 and level 4. It can be shown (cf. Prop. 1.3 in [BvHZ08]) that the vector space of such functions is one-dimensional with basis

$$G_{1,\chi}(z) := \frac{1}{4} + \sum_{n=1}^{\infty} \left(\sum_{d \mid n} \chi(d) \right) e^{\pi i z n}$$

where $\chi(n)$ is the Dirichlet character defined by $\chi(n) = 1$ if $n \equiv 1 \pmod 4$, $\chi(n) = -1$ if $n \equiv 3 \pmod 4$, and 0 otherwise. Comparing constant terms, $\theta^2 = 4G_{1,\chi}$, so by equating the coefficients we find that

$$r_2(n) = 4 \sum_{d \mid n} \chi(d) = 4 \sum_{d \mid n,\, d \text{ odd}} (-1)^{(d-1)/2}.$$

In particular, if $p \equiv 1 \pmod 4$, we have that $r_2(p) = 4(1 + (-1)^{(p-1)/2}) = 8$, and if $p \equiv 3 \pmod 4$ we have $r_2(p) = 0$. □

2.1 Jacobi's four-square theorem

Theorem 2.2 (Jacobi's four-square theorem)**.** *Let $r_4(n)$ denote the number of distinct ways in which n can be represented as a sum of four squares of integers. Then*

$$r_4(n) = \begin{cases} 8 \sum_{m \mid n} m & \text{if } n \text{ is odd,} \\ 24 \sum_{m \mid n,\, m \text{ odd}} m & \text{if } n \text{ is even.} \end{cases}$$

Proof [Mum83]. Note that θ^4 satisfies $\theta^4(-1/\tau) = -\tau^2 \theta^4(\tau)$ and is a modular form. We claim that the space of functions which transform as θ^4 and are entire in $\mathfrak{H}$ and finite at $i\infty$, denoted by $\mathscr{M}_{2,4}$, is spanned by

$$E_2^{\theta}(\tau) := \sum_{m=-\infty}^{\infty} \sum_{n=-\infty}^{\infty} \left(\frac{1}{(2m\tau + (2n+1))^2} - \frac{1}{((2m+1)\tau + 2n)^2} \right).$$

Unlike G_2, this is in fact absolutely convergent. We leave the details out here, but the standard arguments show that it is entire in $\mathfrak{H}$ and bounded at $i\infty$. Moreover, one easily checks that it transforms as θ, and that $\mathscr{M}_{2,4}$ is one-dimensional. We

can compute the Fourier expansion of E_2^θ in the manner of that of G_k in [Apo90] – being slightly cavalier with details, which can be found in [Mum83] – to give

$$\begin{aligned} E_2^\theta(\tau) &= \frac{\pi^2}{4} - 2\pi^2 \sum_{m=1}^{\infty} \left(\sum_{n=1}^{\infty} (-1)^n n e^{2\pi i n m \tau} \right) + 2\pi^2 \sum_{m=0}^{\infty} \left(\sum_{n=1}^{\infty} n e^{\pi i n (2m+1)\tau} \right) \\ &= \frac{\pi^2}{4} - 2\pi^2 \sum_{m=1}^{\infty} \sum_{\substack{n \mid m \\ m/n \text{ even}}} (-1)^n n e^{2\pi i m \tau} + 2\pi^2 \sum_{m=1}^{\infty} \sum_{\substack{n \mid m \\ m/n \text{ odd}}} n e^{\pi i m \tau} \\ &= \frac{\pi^2}{4} \left(1 + 24 \sum_{\substack{m \in \mathbb{N} \\ m \text{ even}}} \sum_{\substack{n \mid m \\ n \text{ odd}}} n e^{2\pi i n \tau} + 8 \sum_{\substack{m \in \mathbb{N} \\ m \text{ odd}}} \sum_{n \mid m} n e^{2\pi i n \tau} \right). \end{aligned}$$

By comparing constant terms, we see that $\theta^4 = 4E_2^\theta/\pi^2$, and so we read off the Fourier coefficients

$$r_4(n) = \begin{cases} 8 \sum_{m \mid n} m & \text{if } n \text{ is odd,} \\ 24 \sum_{m \mid n,\, m \text{ odd}} m & \text{if } n \text{ is even.} \end{cases}$$

□

Since $r_4(n) > 0$ for any $n \in \mathbb{N}$, we immediately obtain:

Corollary 2.3 (Lagrange's theorem)**.** *Every positive integer can be written as a sum of four squares.*

2.2 Quadratic reciprocity

The law of quadratic reciprocity was first established by Gauß, who referred to it in his diary as his *theorema aureum*, the golden theorem, and who published six proofs of it in the course of his career. The fourth proof made use of the following finite sums, which will also be the starting point of our proof:

Definition 2.4. Let p and q be coprime integers. We define the **Gauß sum** of p and q as

$$S(p,q) = \sum_{r=0}^{q-1} e^{-\pi i r^2 p/q}.$$

The theta function lets us compute Gauß sums via the following theorem:

Theorem 2.5 (Landsberg-Schaar)**.** *Let p and q be coprime integers. Then $\frac{1}{\sqrt{q}} S(p,q) = \frac{e^{-\pi i/4}}{\sqrt{p}} \overline{S(q,p)}$, where the bar denotes complex conjugation. Explicitly,*

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

Proof [Bel61]. Set

$$f(t) := \theta\left(\frac{it}{\pi}\right) = \sum_{n=-\infty}^{\infty} e^{-n^2 t}.$$

In short, we will consider the asymptotic behaviours of f before and after applying the transformation formula, and conclude that the asymptotic expressions are equal. Let $t := \varepsilon + \pi i p/q$ for $\varepsilon > 0$ small. Then

$$f(\varepsilon + \pi i p/q) = 1 + 2\sum_{n=1}^{\infty} e^{-n^2\varepsilon} e^{-\pi i n^2 p/q} = 1 + 2\sum_{r=1}^{q} e^{-\pi i r^2 p/q}\left(\sum_{s=0}^{\infty} e^{-(r+sq)^2\varepsilon}\right)$$

by the periodicity of $e^{-\pi i n^2 p/q}$. Now as $\varepsilon \to 0$, $\sum_{s=0}^{\infty} e^{-(r+sq)^2\varepsilon}$ behaves, up to a constant, like the Riemann sum of

$$\int_0^{\infty} e^{-(r+sq)^2\varepsilon} = \int_r^{\infty} e^{-u^2\varepsilon}\frac{du}{q} \sim \frac{1}{q\sqrt{\varepsilon}}\int_0^{\infty} e^{-u^2}du = \frac{\sqrt{\pi}}{2q\sqrt{\varepsilon}}.$$

Therefore, noting that

$$S(p,q) = \sum_{r=0}^{q-1} e^{-\pi i r^2 p/q} = \sum_{r=1}^{q} e^{-\pi i r^2 p/q}$$

by periodicity, we obtain

$$f\left(\varepsilon + \frac{\pi i p}{q}\right) \sim \frac{\sqrt{\pi}}{q\sqrt{\varepsilon}} S(p,q) \quad \text{as} \quad \varepsilon \to 0.$$

Next, applying the transformation formula, we have that

$$f(t) = \sqrt{\frac{\pi}{t}} f\left(\frac{\pi^2}{t}\right),$$

and we see that

$$\frac{\pi^2}{t} = \frac{\pi^2}{\varepsilon + \pi i p/q} = \frac{\pi^2(\varepsilon - \pi i p/q)}{\varepsilon^2 + \pi^2 p^2/q^2} = \frac{\varepsilon q^2}{p^2} - \frac{\pi i q}{p} + O(\varepsilon^2),$$

so

$$f\left(\frac{\pi^2}{t}\right) \sim \frac{\sqrt{\pi}}{q\sqrt{\varepsilon}} S(-q,p) \quad \text{as} \quad \varepsilon \to 0.$$

As for the transformation factor, we see that

$$\lim_{\varepsilon\to 0} \frac{\sqrt{\pi}}{\sqrt{\varepsilon + \pi i p/q}} = \sqrt{\frac{q}{ip}} = e^{-\pi i/4}\sqrt{\frac{q}{p}},$$

so that we obtain

$$f(t) = \sqrt{\frac{\pi}{t}} f\left(\frac{\pi^2}{t}\right) \sim e^{-\pi i/4}\sqrt{\frac{q}{p}}\left(\frac{\sqrt{\pi}}{q\sqrt{\varepsilon}}\right) S(-q,p) \quad \text{as} \quad \varepsilon \to 0.$$

Equating the two asymptotic expressions, we finally get that

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

as required. □

We shall also need the following lemma:

Lemma 2.6. *Let $G(n,m) := \overline{S(2n,m)}$. Then for distinct primes p and q,*

$$G(1,pq) = G(p,q)G(q,p).$$

Proof. We have that

$$\begin{aligned} G(p,q)G(q,p) &= \sum_{k=0}^{q-1} e^{i2\pi k^2 p/q} \sum_{l=0}^{p-1} e^{2\pi i l^2 q/p} = \sum_{k=0}^{q-1}\sum_{l=0}^{p-1} e^{2\pi i k^2 p/q + 2\pi i l^2 q/p} \\ &= \sum_{k=0}^{q-1}\sum_{l=0}^{p-1} e^{2\pi i (k^2 p^2 + l^2 q^2)/pq} = G(1,pq), \end{aligned}$$

since $k^2p^2 + l^2q^2 \equiv (kp+lq)^2 \pmod{pq}$ and $kp+lq$ runs through all the values in $\mathbb{Z}/pq\mathbb{Z}$ exactly once. □

Definition 2.7. Let p and q be distinct primes. The **Legendre symbol** is defined as follows:

$$\left(\frac{p}{q}\right) := \begin{cases} 1 & \text{if } x^2 \equiv p \pmod{q} \text{ has a solution for } x \in \mathbb{Z}, \\ -1 & \text{otherwise.} \end{cases}$$

Lemma 2.8. *Let p and q be distinct primes. Then*

$$G(q,p) = \left(\frac{q}{p}\right) G(1,p).$$

Proof. Note that as r runs from 1 to $p-1$, $r^2 \pmod{p}$ goes through the set Q of quadratic residues of $\mathbb{Z}/p\mathbb{Z}$ exactly twice since $(r-p)^2 \equiv r^2 \pmod{p}$. Therefore,

$$G(q,p) = 1 + 2\sum_{k\in Q} e^{2\pi i k q/p}.$$

One easily checks that if q is a quadratic residue, then so is kq for kq, hence

$$G(q,p) = 1 + 2\sum_{l\in Q} e^{2\pi i l/p} = G(1,p) = \left(\frac{q}{p}\right) G(1,p).$$

If q is not a quadratic residue of p, then kq runs through the non-quadratic residues Q'. Noting that

$$1 + \sum_{m\in Q} e^{2\pi i m/p} + \sum_{m\in Q'} e^{2\pi i m/p} = \sum_{m=0}^{p-1} e^{2\pi i m/p} = 0$$

by evaluating the geometric series, we find that

$$G(q,p) = 1 + 2\sum_{m\in Q'} e^{2\pi i m/p} = -1 - 2\sum_{n\in Q} e^{2\pi i n/p} = \left(\frac{q}{p}\right) G(1,p),$$

as required. □

We are now ready to state and prove our theorem:

Theorem 2.9 (Law of Quadratic Reciprocity)**.** *Let p and q be distinct odd primes. Then*

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

Proof. By theorem 2.5 we see that $G(1,p) = \overline{S(2,p)} = e^{\pi i/4}S(2,p)$, so

$$S(2,p) = \frac{\sqrt{p}}{\sqrt{2}}\sum_{r=0}^{1} e^{-\pi i r^2 p/2} = \frac{\sqrt{p}}{\sqrt{2}}\left(1 + e^{-\pi i p/2}\right) = \sqrt{p}e^{\pi i/4}\frac{1+(-i)^p}{\sqrt{2}}.$$

If $p \equiv 1 \pmod 4$, then this equals $\sqrt{p}e^{\pi i/4}(1-i)/\sqrt{2} = \sqrt{p}e^{\pi i/4}e^{-\pi i/4} = \sqrt{p}$, and if $p \equiv 3 \pmod 4$, we obtain $\sqrt{p}e^{2\pi i/4} = i\sqrt{p}$. It is easily checked that this can be written in a single equation as $G(1,p) = \sqrt{p}i^{(p-1)^2/4}$. Now, using the two lemmata above, this yields

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \frac{G(p,q)}{G(1,q)}\frac{G(q,p)}{G(1,p)} = \frac{G(1,pq)}{G(1,p)G(1,q)} = \frac{\sqrt{pq}\,i^{(pq-1)^2/4}}{\sqrt{pq}\,i^{(p-1)^2/4+(q-1)^2/4}}.$$

The square roots cancel, and the remaining term is easily computed to yield -1 if $p \equiv q \equiv 3 \pmod 4$ and 1 otherwise, hence is equal to $(-1)^{(p-1)(q-1)/4}$, for which the same holds. But this is precisely what we wanted to show. □

We can also use this method for the case where one of the primes is even:

Proposition 2.10. *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod 8, \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod 8. \end{cases}$$

Proof. By lemma 2.8, the Landsberg-Schaar relation (theorem 2.5) and our previous computation of $G(1,p)$, we find that

$$\left(\frac{2}{p}\right) = \frac{G(2,p)}{G(1,p)} = \frac{\frac{\sqrt{p}}{2}e^{\pi i/4}\sum_{r=0}^{3} e^{\pi i r^2 p/4}}{\sqrt{p}i^{(p-1)^2/4}} = \frac{e^{\pi i(p+1)/4} + e^{\pi i(9p+1)/4}}{2i^{(p-1)^2/4}},$$

and by comparing the various residues in $\mathbb{Z}/8\mathbb{Z}$ we see that this equals $(-1)^{\frac{p^2-1}{8}}$, as required. □

Our method of computing Gauß sums using theta functions is extended to great generality in a very deep theorem due to Hecke ([Hec13]), which is far beyond the scope of this text. In Chap. 8 of the text, he proves quadratic reciprocity for arbitrary number fields, having defined corresponding theta functions.

3 Epilogue

In closing we make a few reflections on the significance of these theorems: The proof of quadratic reciprocity shows that like zeta functions, theta functions carry deep information about the structure of the primes in a number field. The proof of the four-square theorem suggests that θ also "knows" about the combinatorial structure of the integers.

From a different point of view, Fermat's theorem is classically proved by looking at primes splitting in $\mathbb{Z}[i]$, and an analogous proof due to Hurwitz ([Hur19]) runs a similar argument with the Hurwitz quaternions to prove the four-square theorem. These are both lattices over $\mathbb{Z}$, so alternatively we can argue that the properties of θ ought to interpreted from, say, a representation-theoretic point of view. Indeed, one of the most fruitful extensions of the classical theory is the *theta correspondence*, which very roughly realises θ as a (still conjectural) correspondence between representations of the metaplectic group of order $2n$ and the special orthogonal group of order $2n+1$. That, however, is another story for another essay.

Bibliography

[Apo90] Tom M. Apostol. *Modular Functions and Dirichlet Series in Number Theory*. Graduate Texts in Mathematics. Springer-Verlag, New York, 2 edition, 1990.

[Bel61] Richard Bellman. *A Brief Introduction to Theta Functions*. Athena Series: Selected Topics in Mathematics. Holt, Rinehart and Winston, New York, 1961.

[BvHZ08] Jan Hendrik Bruinier, Gerard van der Geer, Günter Harder, and Don Zagier. *The 1-2-3 of Modular Forms*. Universitext. Springer-Verlag, Berlin, 2008.

[GR04] George Gasper and Mizan Rahman. *Basic Hypergeometric Series*, volume 96 of *Encyclopedia of Mathematics and Its Applications*. Cambridge University Press, Cambridge, second edition, 2004.

[Hec13] E. T. Hecke. *Lectures on the Theory of Algebraic Numbers*. Springer Science & Business Media, March 2013.

[Hur19] Adolf Hurwitz. *Vorlesungen Über die Zahlentheorie der Quaternionen*. Springer-Verlag, Berlin Heidelberg, 1919.

[Mum83] David Mumford. *Tata Lectures on Theta. I*, volume 28 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, 1983.