10 Applications of Theta Functions

> The problem of the representation of an integer n as the sum of a given number k of integral squares is one of the most celebrated in the theory of numbers. Its history may be traced back to Diophantus, but begins effectively with Girard's (or Fermat's) theorem that a prime $4m + 1$ is the sum of two squares. Almost every arithmetician of note since Fermat has contributed to the solution of the problem, and it has its puzzles for us still.
>
> *G. H. Hardy,* 1940

This chapter is devoted to a closer look at the theory of theta functions and some of its applications to combinatorics and number theory.

The theta function is given by the series

$$\Theta(z|\tau) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau} e^{2\pi i n z},$$

which converges for all $z \in \mathbb{C}$, and τ in the upper half-plane.

A remarkable feature of the theta function is its dual nature. When viewed as a function of z, we see it in the arena of elliptic functions, since Θ is periodic with period 1 and "quasi-period" τ. When considered as a function of τ, Θ reveals its modular nature and close connection with the partition function and the problem of representation of integers as sums of squares.

The two main tools allowing us to exploit these links are the triple-product for Θ and its transformation law. Once we have proved these theorems, we give a brief introduction to the connection with partitions, and then pass to proofs of the celebrated theorems about representation of integers as sums of two or four squares.

1 Product formula for the Jacobi theta function

In its most elaborate form, Jacobi's **theta function** is defined for $z \in \mathbb{C}$ and $\tau \in \mathbb{H}$ by

$$\Theta(z|\tau) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau} e^{2\pi i n z}. \tag{1}$$

Two significant special cases (or variants) are $\theta(\tau)$ and $\vartheta(t)$, which are defined by

$$\theta(\tau) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau}, \qquad \tau \in \mathbb{H},$$
$$\vartheta(t) = \sum_{n=-\infty}^{\infty} e^{-\pi n^2 t}, \qquad t > 0.$$

In fact, the relation between these various functions is given by $\theta(\tau) = \Theta(0|\tau)$ and $\vartheta(t) = \theta(it)$, with of course, $t > 0$.

We have already encountered these functions several times. For example, in the study of the heat diffusion equation for the circle, in Chapter 4 of Book I, we found that the heat kernel was given by

$$H_t(x) = \sum_{n=-\infty}^{\infty} e^{-4\pi^2 n^2 t} e^{2\pi i n x},$$

and therefore $H_t(x) = \Theta(x|4\pi i t)$.

Another instance was the occurence of ϑ in the study of the zeta function. In fact, we proved in Chapter 6 that the functional equation of ϑ implied that of ζ, which then led to the analytic continuation of the zeta function.

We begin our closer look at Θ as a function of z, with τ fixed, by recording its basic structural properties, which to a large extent characterize it.

Proposition 1.1 *The function Θ satisfies the following properties:*

(i) *Θ is entire in $z \in \mathbb{C}$ and holomorphic in $\tau \in \mathbb{H}$.*

(ii) *$\Theta(z+1|\tau) = \Theta(z|\tau)$.*

(iii) *$\Theta(z+\tau|\tau) = \Theta(z|\tau)e^{-\pi i\tau}e^{-2\pi i z}$.*

(iv) *$\Theta(z|\tau) = 0$ whenever $z = 1/2 + \tau/2 + n + m\tau$ and $n, m \in \mathbb{Z}$.*

Proof. Suppose that $\mathrm{Im}(\tau) = t \geq t_0 > 0$ and $z = x + iy$ belongs to a bounded set in $\mathbb{C}$, say $|z| \leq M$. Then, the series defining Θ is absolutely and uniformly convergent, since

$$\sum_{n=-\infty}^{\infty} |e^{\pi i n^2 \tau} e^{2\pi i n z}| \leq C \sum_{n \geq 0} e^{-\pi n^2 t_0} e^{2\pi n M} < \infty.$$

Therefore, for each fixed $\tau \in \mathbb{H}$ the function $\Theta(\cdot|\tau)$ is entire, and for each fixed $z \in \mathbb{C}$ the function $\Theta(z|\cdot)$ is holomorphic in the upper half-plane.

Since the exponential $e^{2\pi i n z}$ is periodic of period 1, property (ii) is immediate from the definition of Θ.

To show the third property we may complete the squares in the expression for $\Theta(z + \tau|\tau)$. In detail, we have

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

Thus we see that $\Theta(z|\tau)$, as a function of z, is periodic with period 1 and "quasi-periodic" with period τ.

To establish the last property it suffices, by what was just shown, to prove that $\Theta(1/2 + \tau/2|\tau) = 0$. Again, we use the interplay between n and n^2 to get

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

To see that this last sum is identically zero, it suffices to match $n \geq 0$ with $-n-1$, and to observe that they have opposite parity, and that $(-n-1)^2 + (-n-1) = n^2 + n$. This completes the proof of the proposition.

We consider next a product $\Pi(z|\tau)$ that enjoys the same structural properties as $\Theta(z|\tau)$ as a function of z. This product is defined for $z \in \mathbb{C}$ and $\tau \in \mathbb{H}$ by

$$\Pi(z|\tau) = \prod_{n=1}^{\infty}(1-q^{2n})(1+q^{2n-1}e^{2\pi iz})(1+q^{2n-1}e^{-2\pi iz}),$$

where we have used the notation that is standard in the subject, namely $q = e^{\pi i\tau}$. The function $\Pi(z|\tau)$ is sometimes referred to as the **triple-product**.

Proposition 1.2 *The function* $\Pi(z|\tau)$ *satisfies the following properties:*

(i) $\Pi(z, \tau)$ *is entire in* $z \in \mathbb{C}$ *and holomorphic for* $\tau \in \mathbb{H}$.

(ii) $\Pi(z+1|\tau) = \Pi(z|\tau)$.

(iii) $\Pi(z+\tau|\tau) = \Pi(z|\tau)e^{-\pi i\tau}e^{-2\pi iz}$.

(iv) $\Pi(z|\tau) = 0$ *whenever* $z = 1/2 + \tau/2 + n + m\tau$ *and* $n, m \in \mathbb{Z}$. *Moreover, these points are simple zeros of* $\Pi(\cdot|\tau)$, *and* $\Pi(\cdot|\tau)$ *has no other zeros.*

Proof. If $\mathrm{Im}(\tau) = t \geq t_0 > 0$ and $z = x+iy$, then $|q| \leq e^{-\pi t_0} < 1$ and

$$(1-q^{2n})(1+q^{2n-1}e^{2\pi iz})(1+q^{2n-1}e^{-2\pi iz}) = 1 + O\left(|q|^{2n-1}e^{2\pi|z|}\right).$$

Since the series $\sum |q|^{2n-1}$ converges, the results for infinite products in Chapter 5 guarantee that $\Pi(z|\tau)$ defines an entire function of z with $\tau \in \mathbb{H}$ fixed, and a holomorphic function for $\tau \in \mathbb{H}$ with $z \in \mathbb{C}$ fixed.

Also, it is clear from the definition that $\Pi(z|\tau)$ is periodic of period 1 in the z variable.

To prove the third property, we first observe that since $q^2 = e^{2\pi i\tau}$ we have

$$\begin{aligned}\Pi(z+\tau|\tau) &= \prod_{n=1}^{\infty}(1-q^{2n})(1+q^{2n-1}e^{2\pi i(z+\tau)})(1+q^{2n-1}e^{-2\pi i(z+\tau)}) \\ &= \prod_{n=1}^{\infty}(1-q^{2n})(1+q^{2n+1}e^{2\pi iz})(1+q^{2n-3}e^{-2\pi iz}).\end{aligned}$$

Comparing this last product with $\Pi(z|\tau)$, and isolating the factors that are either missing or extra leads to

$$\Pi(z+\tau|\tau) = \Pi(z|\tau)\left(\frac{1+q^{-1}e^{-2\pi iz}}{1+qe^{2\pi iz}}\right).$$

Hence (iii) follows because $(1 + x)/(1 + x^{-1}) = x$, whenever $x \neq -1$.

Finally, to find the zeros of $\Pi(z|\tau)$ we recall that a product that converges vanishes only if at least one of its factors is zero. Clearly, the factor $(1 - q^n)$ never vanishes since $|q| < 1$. The second factor $(1 + q^{2n-1}e^{2\pi iz})$ vanishes when $q^{2n-1}e^{2\pi iz} = -1 = e^{\pi i}$. Since $q = e^{\pi i\tau}$, we then have[1]

$$(2n - 1)\tau + 2z = 1 \pmod 2.$$

Hence,

$$z = 1/2 + \tau/2 - n\tau \pmod 1,$$

and this takes care of the zeros of the type $1/2 + \tau/2 - n\tau + m$ with $n \geq 1$ and $m \in \mathbb{Z}$. Similarly, the third factor vanishes if

$$(2n - 1)\tau - 2z = 1 \pmod 2$$

which implies that

$$\begin{aligned} z &= -1/2 - \tau/2 + n\tau \pmod 1 \\ &= 1/2 + \tau/2 + n'\tau \pmod 1, \end{aligned}$$

where $n' \geq 0$. This exhausts the zeros of $\Pi(\cdot|\tau)$. Finally, these zeros are simple, since the function $e^w - 1$ vanishes at the origin to order 1 (a fact obvious from a power series expansion or a simple differentiation).

The importance of the product Π comes from the following theorem, called the product formula for the theta function. The fact that $\Theta(z|\tau)$ and $\Pi(z|\tau)$ satisfy similar properties hints at a close connection between the two. This is indeed the case.

Theorem 1.3 (Product formula) *For all $z \in \mathbb{C}$ and $\tau \in \mathbb{H}$ we have the identity $\Theta(z|\tau) = \Pi(z|\tau)$.*

Proof. Fix $\tau \in \mathbb{H}$. We claim first that there exists a constant $c(\tau)$ such that

$$\Theta(z|\tau) = c(\tau)\Pi(z|\tau). \tag{2}$$

In fact, consider the quotient $F(z) = \Theta(z|\tau)/\Pi(z|\tau)$, and note that by the previous two propositions, the function F is entire and doubly periodic with periods 1 and τ. This implies that F is constant as claimed.

[1]We use the standard short-hand, $a = b \pmod c$, to mean that $a - b$ is an integral multiple of c.

We must now prove that $c(\tau) = 1$ for all τ, and the main point is to establish that $c(\tau) = c(4\tau)$. If we put $z = 1/2$ in (2), so that $e^{2i\pi z} = e^{-2i\pi z} = -1$, we obtain

$$\begin{aligned}\sum_{n=-\infty}^{\infty} (-1)^n q^{n^2} &= c(\tau) \prod_{n=1}^{\infty} (1-q^{2n})(1-q^{2n-1})(1-q^{2n-1}) \\ &= c(\tau) \prod_{n=1}^{\infty} \left[(1-q^{2n-1})(1-q^{2n})\right](1-q^{2n-1}) \\ &= c(\tau) \prod_{n=1}^{\infty} (1-q^n)(1-q^{2n-1}).\end{aligned}$$

Hence

$$c(\tau) = \frac{\sum_{n=-\infty}^{\infty} (-1)^n q^{n^2}}{\prod_{n=1}^{\infty} (1-q^n)(1-q^{2n-1})}. \tag{3}$$

Next, we put $z = 1/4$ in (2), so that $e^{2i\pi z} = i$. On the one hand, we have

$$\Theta(1/4|\tau) = \sum_{n=-\infty}^{\infty} q^{n^2} i^n,$$

and due to the fact that $1/i = -i$, only the terms corresponding to $n =$ even $= 2m$ are not cancelled; thus

$$\Theta(1/4|\tau) = \sum_{m=-\infty}^{\infty} q^{4m^2} (-1)^m.$$

On the other hand,

$$\begin{aligned}\Pi(1/4|\tau) &= \prod_{m=1}^{\infty} (1-q^{2m})(1+iq^{2m-1})(1-iq^{2m-1}) \\ &= \prod_{m=1}^{\infty} (1-q^{2m})(1+q^{4m-2}) \\ &= \prod_{n=1}^{\infty} (1-q^{4n})(1-q^{8n-4}),\end{aligned}$$

where the last line is obtained by considering separately the two cases $2m = 4n-4$ and $2m = 4n-2$ in the first factor. Hence

$$c(\tau) = \frac{\sum_{n=-\infty}^{\infty} (-1)^n q^{4n^2}}{\prod_{n=1}^{\infty} (1-q^{4n})(1-q^{8n-4})}, \tag{4}$$

and combining (3) and (4) establishes our claim that $c(\tau) = c(4\tau)$. Successive applications of this identity give $c(\tau) = c(4^k\tau)$, and since $q^{4^k} = e^{i\pi 4^k \tau} \to 0$ as $k \to \infty$, we conclude from (2) that $c(\tau) = 1$. This proves the theorem.

The product formula for the function Θ specializes to its variant $\theta(\tau) = \Theta(0|\tau)$, and this provides a proof that θ is non-vanishing in the upper half-plane.

Corollary 1.4 *If* $\mathrm{Im}(\tau) > 0$ *and* $q = e^{\pi i \tau}$, *then*

$$\theta(\tau) = \prod_{n=1}^{\infty}(1 - q^{2n})(1 + q^{2n-1})^2.$$

Thus $\theta(\tau) \neq 0$ *for* $\tau \in \mathbb{H}$.

The next corollary shows that the properties of the function Θ now yield the construction of an elliptic function (which is in fact closely related to the Weierstrass $\wp$ function).

Corollary 1.5 *For each fixed* $\tau \in \mathbb{H}$, *the quotient*

$$(\log \Theta(z|\tau))'' = \frac{\Theta(z|\tau)\Theta''(z|\tau) - (\Theta'(z|\tau))^2}{\Theta(z|\tau)^2}$$

is an elliptic function of order 2 *with periods* 1 *and* τ, *and with a double pole at* $z = 1/2 + \tau/2$.

In the above, the primes $'$ denote differentiation with respect to the z variable.

Proof. Let $F(z) = (\log \Theta(z|\tau))' = \Theta(z|\tau)'/\Theta(z|\tau)$. Differentiating the identities (ii) and (iii) of Proposition 1.1 gives $F(z+1) = F(z)$, $F(z+\tau) = F(z) - 2\pi i$, and differentiating again shows that $F'(z)$ is doubly periodic. Since $\Theta(z|\tau)$ vanishes only at $z = 1/2 + \tau/2$ in the fundamental parallelogram, the function $F(z)$ has only a single pole, and thus $F'(z)$ has only a double pole there.

The precise connection between $(\log \Theta(z|\tau))''$ and $\wp_\tau(z)$ is stated in Exercise 1.

For an analogy between Θ and the Weierstrass σ function, see Exercise 5 of the previous chapter.

1.1 Further transformation laws

We now come to the study of the transformation relations in the τ-variable, that is, to the modular character of Θ.

Recall that in the previous chapter, the modular character of the Weierstrass $\wp$ function and Eisenstein series E_k was reflected by the two transformations

$$\tau \mapsto \tau + 1 \quad \text{and} \quad \tau \mapsto -1/\tau,$$

which preserve the upper half-plane. In what follows, we shall denote these two transformations by T_1 and S, respectively.

When looking at the Θ function, however, it will be natural to consider instead the transformations

$$T_2 : \tau \mapsto \tau + 2 \quad \text{and} \quad S : \tau \mapsto -1/\tau,$$

since $\Theta(z|\tau + 2) = \Theta(z|\tau)$, but $\Theta(z|\tau + 1) \neq \Theta(z|\tau)$.

Our first task is to study the transformation of $\Theta(z|\tau)$ under the mapping $\tau \mapsto -1/\tau$.

Theorem 1.6 *If $\tau \in \mathbb{H}$, then*

$$\Theta(z| - 1/\tau) = \sqrt{\frac{\tau}{i}} e^{\pi i \tau z^2} \Theta(z\tau|\tau) \quad \textit{for all } z \in \mathbb{C}. \tag{5}$$

Here $\sqrt{\tau/i}$ denotes the branch of the square root defined on the upper half-plane, that is positive when $\tau = it$, $t > 0$.

Proof. It suffices to prove this formula for $z = x$ real and $\tau = it$ with $t > 0$, since for each fixed $x \in \mathbb{R}$, the two sides of equation (5) are holomorphic functions in the upper half-plane which then agree on the positive imaginary axis, and hence must be equal everywhere. Also, for a fixed $\tau \in \mathbb{H}$ the two sides define holomorphic functions in z that agree on the real axis, and hence must be equal everywhere.

With x real and $\tau = it$ the formula becomes

$$\sum_{n=-\infty}^{\infty} e^{-\pi n^2/t} e^{2\pi i n x} = t^{1/2} e^{-\pi t x^2} \sum_{n=-\infty}^{\infty} e^{-\pi n^2 t} e^{-2\pi n x t}.$$

Replacing x by a, we find that we must prove

$$\sum_{n=-\infty}^{\infty} e^{-\pi t (n+a)^2} = \sum_{n=-\infty}^{\infty} t^{-1/2} e^{-\pi n^2/t} e^{2\pi i n a}.$$

However, this is precisely equation (3) in Chapter 4, which was derived from the Poisson summation formula.

In particular, by setting $z = 0$ in the theorem, we find the following.

Corollary 1.7 *If* $\mathrm{Im}(\tau) > 0$*, then* $\theta(-1/\tau) = \sqrt{\tau/i}\,\theta(\tau)$.

Note that if $\tau = it$, then $\theta(\tau) = \vartheta(t)$, and the above relation is precisely the functional equation for ϑ which appeared in Chapter 4.

The transformation law $\theta(-1/\tau) = (\tau/i)^{1/2}\theta(\tau)$ gives us very precise information about the behavior when $\tau \to 0$. The next corollary will be used later, when we need to analyze the behavior of $\theta(\tau)$ as $\tau \to 1$.

Corollary 1.8 *If* $\tau \in \mathbb{H}$*, then*

$$\begin{aligned}\theta(1-1/\tau) &= \sqrt{\frac{\tau}{i}}\sum_{n=-\infty}^{\infty} e^{\pi i(n+1/2)^2\tau} \\ &= \sqrt{\frac{\tau}{i}}\left(2e^{\pi i\tau/4} + \cdots\right).\end{aligned}$$

The second identity means that $\theta(1-1/\tau) \sim \sqrt{\tau/i}2e^{i\pi\tau/4}$ *as* $\mathrm{Im}(\tau) \to \infty$.

Proof. First, we note that n and n^2 have the same parity, so

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

hence $\theta(1-1/\tau) = \Theta(1/2|-1/\tau)$. Next, we use Theorem 1.6 with $z = 1/2$, and the result is

$$\begin{aligned}\theta(1-1/\tau) &= \sqrt{\frac{\tau}{i}}e^{\pi i\tau/4}\Theta(\tau/2|\tau) \\ &= \sqrt{\frac{\tau}{i}}e^{\pi i\tau/4}\sum_{n=-\infty}^{\infty} e^{\pi i n^2\tau}e^{\pi i n\tau} \\ &= \sqrt{\frac{\tau}{i}}\sum_{n=-\infty}^{\infty} e^{\pi i(n+1/2)^2\tau}.\end{aligned}$$

The terms corresponding to $n = 0$ and $n = -1$ contribute $2e^{\pi i\tau/4}$, which has absolute value $2e^{-\pi t/4}$ where $\tau = \sigma + it$. Finally, the sum of the other terms $n \neq 0, -1$ is of order

$$O\left(\sum_{k=1}^{\infty} e^{-(k+1/2)^2\pi t}\right) = O\left(e^{-9\pi t/4}\right).$$

Our final corollary of the transformation law pertains to the **Dedekind eta function**, which is defined for $\mathrm{Im}(\tau) > 0$ by

$$\eta(\tau) = e^{\frac{\pi i \tau}{12}} \prod_{n=1}^{\infty} (1 - e^{2\pi i n \tau}).$$

The functional equation for η given below will be relevant to our discussion of the four-square theorem, and in the theory of partitions.

Proposition 1.9 *If* $\mathrm{Im}(\tau) > 0$*, then* $\eta(-1/\tau) = \sqrt{\tau/i}\ \eta(\tau)$.

This identity is deduced by differentiating the relation in Theorem 1.6 and evaluating it at $z_0 = 1/2 + \tau/2$. The details are as follows.

Proof. From the product formula for the theta function, we may write with $q = e^{\pi i \tau}$,

$$\Theta(z|\tau) = (1 + qe^{-2\pi i z}) \prod_{n=1}^{\infty} (1 - q^{2n})(1 + q^{2n-1} e^{2\pi i z})(1 + q^{2n+1} e^{-2\pi i z}),$$

and since the first factor vanishes at $z_0 = 1/2 + \tau/2$, we see that

$$\Theta'(z_0|\tau) = 2\pi i H(\tau), \qquad \text{where } H(\tau) = \textstyle\prod_{n=1}^{\infty} (1 - e^{2\pi i n \tau})^3.$$

Next, we observe that with $-1/\tau$ replaced by τ in (5), we obtain

$$\Theta(z|\tau) = \sqrt{i/\tau} e^{-\pi i z^2/\tau} \Theta(-z/\tau| - 1/\tau).$$

If we differentiate this expression and then evaluate it at the point $z_0 = 1/2 + \tau/2$, we find

$$2\pi i H(\tau) = \sqrt{i/\tau} e^{-\frac{\pi i}{4\tau}} e^{-\frac{\pi i}{2}} e^{-\frac{\pi i \tau}{4}} \left(\frac{-2\pi i}{\tau} \right) H(-1/\tau).$$

Hence

$$e^{\frac{\pi i \tau}{4}} H(\tau) = \left(\frac{i}{\tau} \right)^{3/2} e^{-\frac{\pi i}{4\tau}} H(-1/\tau).$$

We note that when $\tau = it$, with $t > 0$, the function $\eta(\tau)$ is positive, and thus taking the cube root of the above gives $\eta(\tau) = \sqrt{i/\tau}\ \eta(-1/\tau)$; therefore this identity holds for all $\tau \in \mathbb{H}$ by analytic continuation.

A connection between the function η and the theory of elliptic functions is given in Problem 5.

2 Generating functions

Given a sequence $\{F_n\}_{n=0}^{\infty}$, which may arise either combinatorially, recursively, or in terms of some number-theoretic law, an important tool in its study is the passage to its **generating function**, defined by

$$F(x) = \sum_{n=0}^{\infty} F_n x^n.$$

Often times, the defining properties of the sequence $\{F_n\}$ imply interesting algebraic or analytic properties of the function $F(x)$, and exploiting these can eventually lead us back to new insights about the sequence $\{F_n\}$. A very simple-minded example is given by the Fibonacci sequence. (See Exercise 2). Here we want to study less elementary examples of this idea, related to the Θ function.

We shall first discuss very briefly the theory of partitions.

The **partition function** is defined as follows: if n is a positive integer, we let $p(n)$ denote the numbers of ways n can be written as a sum of positive integers. For instance, $p(1) = 1$, and $p(2) = 2$ since $2 = 2 + 0 = 1 + 1$. Also, $p(3) = 3$ since $3 = 3 + 0 = 2 + 1 = 1 + 1 + 1$. We set $p(0) = 1$ and collect some further values of $p(n)$ in the following table.

n	0	1	2	3	4	5	6	7	8	$\cdots$	12
$p(n)$	1	1	2	3	5	7	11	15	22	$\cdots$	77

The first theorem is Euler's identity for the generating function of the partition sequence $\{p(n)\}$, which is reminiscent of the product formula for the zeta function.

Theorem 2.1 *If* $|x| < 1$, *then* $\displaystyle\sum_{n=0}^{\infty} p(n)x^n = \prod_{k=1}^{\infty} \frac{1}{1-x^k}$.

Formally, we can write each fraction as

$$\frac{1}{1-x^k} = \sum_{m=0}^{\infty} x^{km},$$

and multiply these out together to obtain $p(n)$ as the coefficient of x^n. Indeed, when we group together equal integers in a partition of n, this partition can be written as

$$n = m_1 k_1 + \cdots + m_r k_r,$$

where $k_1, \dots, k_r$ are distinct positive integers. This partition corresponds to the term

$$(x^{k_1})^{m_1} \cdots (x^{k_r})^{m_r}$$

that arises in the product.

The justification of this formal argument proceeds as in the proof of the product formula for the zeta function (Section 1, Chapter 7); this is based on the convergence of the product $\prod 1/(1-x^k)$. This convergence in turn follows from the fact that for each fixed $|x| < 1$ one has

$$\frac{1}{1-x^k} = 1 + O(x^k).$$

A similar argument shows that the product $\prod 1/(1-x^{2n-1})$ is equal to the generating function for $p_o(n)$, the number of partitions of n into odd parts. Also, $\prod(1+x^n)$ is the generating function for $p_u(n)$, the number of partitions of n into unequal parts. Remarkably, $p_o(n) = p_u(n)$ for all n, and this translates into the identity

$$\prod_{n=1}^{\infty} \left(\frac{1}{1-x^{2n-1}} \right) = \prod_{n=1}^{\infty} (1+x^n).$$

To prove this note that $(1+x^n)(1-x^n) = 1-x^{2n}$, and therefore

$$\prod_{n=1}^{\infty}(1+x^n) \prod_{n=1}^{\infty}(1-x^n) = \prod_{n=1}^{\infty}(1-x^{2n}).$$

Moreover, taking into account the parity of integers, we have

$$\prod_{n=1}^{\infty}(1-x^{2n}) \prod_{n=1}^{\infty}(1-x^{2n-1}) = \prod_{n=1}^{\infty}(1-x^n),$$

which combined with the above proves the desired identity.

The proposition that follows is deeper, and in fact involves the Θ function directly. Let $p_{e,u}(n)$ denote the number of partitions of n into an even number of unequal parts, and $p_{o,u}(n)$ the number of partitions of n into an odd number of unequal parts. Then, Euler proved that, unless n is a pentagonal number, one has $p_{e,u}(n) = p_{o,u}(n)$. By definition, **pentagonal numbers**[2] are integers n of the form $k(3k+1)/2$, with $k \in \mathbb{Z}$. For

[2] The traditional definition is as follows. Integers of the form $n = k(k-1)/2$, $k \in \mathbb{Z}$, are "triangular numbers"; those of the form $n = k^2$ are "squares"; and those of the form $k(3k+1)/2$ are "pentagonal numbers." In general, numbers of the form $(k/2)((\ell-2)k + \ell - 4)$ are associated with an ℓ-sided polygon.

example, the first few pentagonal numbers are $1, 2, 5, 7, 12, 15, 22, 26, \ldots$. In fact, if n is pentagonal, then

$$p_{e,u}(n) - p_{o,u}(n) = (-1)^k, \qquad \text{if } n = k(3k+1)/2.$$

To prove this result, we first observe that

$$\prod_{n=1}^{\infty}(1-x^n) = \sum_{n=1}^{\infty}[p_{e,u}(n) - p_{o,u}(n)]x^n.$$

This follows since multiplying the terms in the product, we obtain terms of the form $(-1)^r x^{n_1+\cdots+n_r}$ where the integers $n_1, \ldots, n_r$ are distinct. Hence in the coefficient of x^n, each partition $n_1 + \cdots + n_r$ of n into an even number of unequal parts contributes for $+1$ (r is even), and each partition into an odd number of unequal parts contributes -1 (r is odd). This gives precisely the coefficient $p_{e,u}(n) - p_{o,u}(n)$.

With the above identity, we see that Euler's theorem is a consequence of the following proposition.

Proposition 2.2 $\displaystyle\prod_{n=1}^{\infty}(1-x^n) = \sum_{k=-\infty}^{\infty}(-1)^k x^{\frac{k(3k+1)}{2}}$.

Proof. If we set $x = e^{2\pi i u}$, then we can write

$$\prod_{n=1}^{\infty}(1-x^n) = \prod_{n=1}^{\infty}(1-e^{2\pi i n u})$$

in terms of the triple product

$$\prod_{n=1}^{\infty}(1-q^{2n})(1+q^{2n-1}e^{2\pi i z})(1+q^{2n-1}e^{-2\pi i z})$$

by letting $q = e^{3\pi i u}$ and $z = 1/2 + u/2$. This is because

$$\prod_{n=1}^{\infty}(1-e^{2\pi i 3nu})(1-e^{2\pi i(3n-1)u})(1-e^{2\pi i(3n-2)u}) = \prod_{n=1}^{\infty}(1-e^{2\pi i n u}).$$

By Theorem 1.3 the product equals

$$\sum_{n=-\infty}^{\infty} e^{3\pi i n^2 u}(-1)^n e^{2\pi i n u/2} = \sum_{n=-\infty}^{\infty}(-1)^n e^{\pi i n(3n+1)u}$$

$$= \sum_{n=-\infty}^{\infty} (-1)^n x^{n(3n+1)/2},$$

which was to be proved.

We make a final comment about the partition function $p(n)$. The nature of its growth as $n \to \infty$ can be analyzed in terms of the behavior of $1/\prod_{n=1}^{\infty}(1-x)^n$ as $|x| \to 1$. In fact, by elementary considerations, we can get a rough order of growth of $p(n)$ from the growth of the generating function as $x \to 1$; see Exercises 5 and 6. A more refined analysis requires the transformation properties of the generating function which goes back to the corresponding Proposition 1.9 about η. This leads to a very good asymptotic formula for $p(n)$. It may be found in Appendix A.

3 The theorems about sums of squares

The ancient Greeks were fascinated by triples of integers (a, b, c) that occurred as sides of right triangles. These are the "Pythagorean triples," which satisfy $a^2 + b^2 = c^2$. According to Diophantus of Alexandria (ca. 250 AD), if c is an integer of the above kind, and a and b have no common factors (a case to which one may easily reduce), then c is the sum of two squares, that is, $c = m^2 + n^2$ with $m, n \in \mathbb{Z}$; and conversely, any such c arises as the hypotenuse of a triangle whose sides are given by a Pythagorean triple (a, b, c). (See Exercise 8.) Therefore, it is natural to ask the following question: which integers can be written as the sum of two squares? It is easy to see that no number of the form $4k+3$ can be so written, but to determine which integers can be expressed in this way is not obvious.

Let us pose the question in a more quantitative form. We define $r_2(n)$ to be the number of ways n can be written as the sum of two squares, counting obvious repetitions; that is, $r_2(n)$ is the number of pairs (x, y), $x, y \in \mathbb{Z}$, so that

$$n = x^2 + y^2.$$

For example, $r_2(3) = 0$, but $r_2(5) = 8$ because $5 = (\pm 2)^2 + (\pm 1)^2$, and also $5 = (\pm 1)^2 + (\pm 2)^2$. Hence, our first problem can be posed as follows:

> **Sum of two squares:** Which integers can be written as a sum of two squares? More precisely, can one determine an expression for $r_2(n)$?

Next, since not every positive integer can be expressed as the sum of two squares, we may ask if three squares, or possibly four squares suffice.

However, the fact is that there are infinitely many integers that cannot be written as the sum of three squares, since it is easy to check that no integer of the form $8k + 7$ can be so written. So we turn to the question of four squares and define, in analogy with $r_2(n)$, the function $r_4(n)$ to be the number of ways of expressing n as a sum of four squares. Therefore, a second problem that arises is:

> **Sum of four squares:** Can every positive integer be written as a sum of four squares? More precisely, determine a formula for $r_4(n)$.

It turns out that the problems of two squares and four squares, which go back to the third century, were not resolved until about 1500 years later, and their full solution was first given by the use of Jacobi's theory of theta functions!

3.1 The two-squares theorem

The problem of representing an integer as the sum of two squares, while obviously additive in nature, has a nice multiplicative aspect: if n and m are two integers that can be written as the sum of two squares, then so can their product nm. Indeed, suppose $n = a^2 + b^2$, $m = c^2 + d^2$, and consider the complex number

$$x + iy = (a + ib)(c + id).$$

Clearly, x and y are integers since $a, b, c, d \in \mathbb{Z}$, and by taking absolute values on both sides we see that

$$x^2 + y^2 = (a^2 + b^2)(c^2 + d^2),$$

and it follows that $nm = x^2 + y^2$.

For these reasons the divisibility properties of n play a crucial role in determining $r_2(n)$. To state the basic result we define two new **divisor functions**: we let $d_1(n)$ denote the number of divisors of n of the form $4k + 1$, and $d_3(n)$ the number of divisors of n of the form $4k + 3$. The main result of this section provides a complete answer to the two-squares problem:

Theorem 3.1 *If* $n \geq 1$, *then* $r_2(n) = 4(d_1(n) - d_3(n))$.

A direct consequence of the above formula for $r_2(n)$ may be stated as follows. If $n = p_1^{a_1} \cdots p_r^{a_r}$ is the prime factorization of n where $p_1, \ldots, p_r$ are distinct, then:

> *The positive integer n can be represented as the sum of two squares if and only if every prime p_j of the form $4k+3$ that occurs in the factorization of n has an even exponent a_j.*

The proof of this deduction is outlined in Exercise 9.

To prove the theorem, we first establish a crucial relationship that identifies the generating function of the sequence $\{r_2(n)\}_{n=1}^{\infty}$ with the square of the θ function, namely

$$\theta(\tau)^2 = \sum_{n=0}^{\infty} r_2(n) q^n, \tag{6}$$

whenever $q = e^{\pi i \tau}$ with $\tau \in \mathbb{H}$. The proof of this identity relies simply on the definition of r_2 and θ. Indeed, if we first recall that $\theta(\tau) = \sum_{-\infty}^{\infty} q^{n^2}$, then we obtain

$$\begin{aligned}
\theta(\tau)^2 &= \left(\sum_{n_1=-\infty}^{\infty} q^{n_1^2} \right) \left(\sum_{n_2=-\infty}^{\infty} q^{n_2^2} \right) \\
&= \sum_{(n_1,n_2)\in\mathbb{Z}\times\mathbb{Z}} q^{n_1^2+n_2^2} \\
&= \sum_{n=0}^{\infty} r_2(n) q^n,
\end{aligned}$$

since $r_2(n)$ counts the number of pairs (n_1, n_2) with $n_1^2 + n_2^2 = n$.

Proposition 3.2 *The identity $r_2(n) = 4(d_1(n) - d_3(n))$, $n \geq 1$, is equivalent to the identities*

$$\theta(\tau)^2 = 2 \sum_{n=-\infty}^{\infty} \frac{1}{q^n + q^{-n}} = 1 + 4 \sum_{n=1}^{\infty} \frac{q^n}{1+q^{2n}}, \tag{7}$$

whenever $q = e^{\pi i \tau}$ and $\tau \in \mathbb{H}$.

Proof. We note first that both series converge absolutely since $|q| < 1$, and the first equals the second, because $1/(q^n + q^{-n}) = q^{|n|}/(1 + q^{2|n|})$.

Since $(1+q^{2n})^{-1} = (1-q^{2n})/(1-q^{4n})$, the right-hand side of (7) equals

$$1 + 4 \sum_{n=1}^{\infty} \left(\frac{q^n}{1-q^{4n}} - \frac{q^{3n}}{1-q^{4n}} \right).$$

However, since $1/(1-q^{4n}) = \sum_{m=0}^{\infty} q^{4nm}$, we have

$$\sum_{n=1}^{\infty} \frac{q^n}{1-q^{4n}} = \sum_{n=1}^{\infty}\sum_{m=0}^{\infty} q^{n(4m+1)} = \sum_{k=1}^{\infty} d_1(k) q^k,$$

because $d_1(k)$ counts the number of divisors of k that are of the form $4m+1$. Observe that the series $\sum d_1(k)q^k$ converges since $d_1(k) \leq k$.

A similar argument shows that

$$\sum_{n=1}^{\infty} \frac{q^{3n}}{1-q^{4n}} = \sum_{k=1}^{\infty} d_3(k) q^k,$$

and the proof of the proposition is complete.

In effect, we see that the identity (6) links the original problem in arithmetic with the problem in complex analysis of establishing the relation (7).

We shall now find it convenient to use $\mathcal{C}(\tau)$ to denote[3]

$$\text{(8)} \qquad \mathcal{C}(\tau) = 2\sum_{n=-\infty}^{\infty} \frac{1}{q^n + q^{-n}} = \sum_{n=-\infty}^{\infty} \frac{1}{\cos(n\pi\tau)},$$

where $q = e^{\pi i \tau}$ and $\tau \in \mathbb{H}$. Our work then becomes to prove the identity $\theta(\tau)^2 = \mathcal{C}(\tau)$.

What is truly remarkable are the different yet parallel ways that the functions θ and $\mathcal{C}$ arise. The genesis of the function θ may be thought to be the heat diffusion equation on the real line; the corresponding heat kernel is given in terms of the Gaussian $e^{-\pi x^2}$ which is its own Fourier transform; and finally the transformation rule for θ results from the Poisson summation formula.

The parallel with $\mathcal{C}$ is that it arises from another differential equation: the steady-state heat equation in a strip; there, the corresponding kernel is $1/\cosh \pi x$ (Section 1.3, Chapter 8), which again is its own Fourier transform (Example 3, Chapter 3). The transformation rule for $\mathcal{C}$ results, once again, from the Poisson summation formula.

To prove the identity $\theta^2 = \mathcal{C}$ we will first show that these two functions satisfy the same structural properties. For θ^2 we had the transformation law $\theta(\tau)^2 = (i/\tau)\theta(-1/\tau)^2$ (Corollary 1.7).

[3]We denote the function by $\mathcal{C}$ because we are summing a series of cosines.