# Modular Forms and Sums of Squares

Ng Chung Lok Andrew

## 1 Introduction

This expository essay will introduce modular forms, with a view to their application to the problem of deciding which positive integers can be written as a sum of squares. The material closely follows that of [1].
The first sections will introduce the necessary background from analysis and lay the groundwork for later sections by proving the requisite properties about functions of number-theoretic interest. The rest of the essay will use these tools to answer the question of how many ways can an integer be written as a sum of two or four squares, a question that has attracted attention from many great mathematicians over the past hundreds of years.

## 2 Some complex analysis

As this essay aims to be as self-contained as possible, we begin by proving some technical results needed later. The general principle will be that basic facts about complex analysis (those appearing in the schedules for the undergraduate Cambridge Mathematical Tripos) will be assumed, but of the further results, as many as possible will be proved (or sketched if the details aren't important).We begin by dealing with infinite products.

The product $\prod_{n=1}^{\infty}(1+a_n)$ is said to converge if $\lim_{N\to\infty}\prod_{n=1}^{N}(1+a_n)$ exists.

**Proposition 1.** *Let $\{a_n\}_{n=1}^{\infty}$ be a sequence of complex numbers such that $\sum_{n=1}^{\infty}|a_n|$ converges. Then the infinite product $\prod_{n=1}^{\infty}(1+a_n)$ converges. Furthermore, it is 0 if and only if one of the factors is 0.*

*Proof.* Since the sum converges, there is some integer $k$ such that for all $n > k, |a_n| < \frac{1}{2}$. Then, after this point, the sequence $1+a_n$ is contained in the right half plane, so it is possible to define a continuous logarithm for all terms in the sequence. Let $b_n = \log(1+a_n)$. Writing $\prod_{n=k}^{N}(1+a_n) = \prod_{n=k}^{N} e^{b_n} = e^{\sum b_n}$, the infinite product converges if and only if the infinite sum $\sum b_n$ does. In the real case, we would be done by the well known fact $1+x \le e^x$. Unfortunately, $x = 2\pi i$ means more care is needed over $\mathbb{C}$. Nevertheless, for $|z| < 1/2$, the Taylor series and triangle inequality show that $|\log(1+z)| \le \sum_{n=1}^{\infty}\frac{|z|^n}{n} \le |z|\sum_{n=1}^{\infty}|0.5|^{n-1} = 2|z|$, so the hypothesis that $\sum|a_n|$ converges implies that $\sum b_n$ converges absolutely, hence the product converges. Finally, $\prod_{n=k}^{\infty}(1+a_n) = e^b \neq 0$ for some $b \in \mathbb{C}$, so the product is 0 if and only $1+a_n = 0$ for some $1 \le n \le k-1$. □

This generalises to functions which 'behave like constants':

**Proposition 2.** *Let $\{F_n\}$ be a sequence of holomorphic functions on an open set $U$. Suppose there are constants $c_n > 0$ such that $\sum c_n < \infty$ and $|F_n(z) - 1| \leq c_n$ for all $z \in U$. Then*

*i The product $\prod_{n=1}^{\infty} F_n(z)$ converges uniformly in $U$ to a holomorphic function $F$.*

*ii If all the $F_n$ never vanish, then $\frac{F'(z)}{F(z)} = \sum_{n=1}^{\infty} \frac{F_n'(z)}{F_n(z)}$*

*Proof.* Trying to use the previous proposition quickly leads to the idea of letting $a_n(z) = F_n(z) - 1$ so that $|a_n(z)| \leq c_n$. Then all estimates are uniform in $z$ because the $c_n$ are constants, so the product converges uniformly to a holomorphic function $F$.
For (ii), define $G_N(z) = \prod_{n=1}^{N} F_n(z)$. $G_N \to F$ uniformly in $U$, so the derivatives converge uniformly as well, i.e. $G_N' \to F'$ uniformly. Let $K$ be a compact subset of $U$. $G_N$ never vanishes, so $|G_N|$ is bounded below away from 0 on $K$ by compactness. Hence $\frac{G_N'}{G_N} \to \frac{F'}{F}$ uniformly on $K$, and since $K$ was arbitrary, the limit holds for all $z$ $inU$. Finally, the product rule shows $\frac{G_N'}{G_N} = \sum_{n=1}^{N} \frac{F_n'}{F_n}$, which completes the proof. □

Next, a cute relation between a function $f$ and its Fourier transform $\hat{f}$.

**Theorem 3** (Poisson summation)**.** *Let $f$ be a function holomorphic on $S_a = \{z : Im(z) < a\}$ for some $a > 0$, such that there is a constant $A > 0$ satisfying $|f(z)| \leq \frac{A}{1+Re(z)^2}$ for all $z \in S_a$. Then $\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(n)$.*

*Sketch proof.* Consider $\frac{f(z)}{e^{2\pi i z}-1}$. This has simple poles at the integers, with residue $\frac{f(n)}{2\pi i}$ at $z = n$.Let $\gamma_N$ be the rectangular contour with vertices at $\pm N + 0.5 \pm ib$ for some $0 \leq b \leq a$. By the residue theorem, $\sum_{|n|<N} f(n) = \int_{\gamma_N} \frac{f(z)dz}{e^{2\pi i}-1}$. The decay condition means that the integral along the vertical edges goes to 0 as $N \to \infty$, and along the horizontal edges, expanding into a geometric series and interchanging order of summation, which is valid by uniform convergence, followed by applying Cauchy's theorem on each of the summands to move back to the real line, gives the result. □

This is an invaluable tool for proving that all sorts of infinite sums are equal, as demonstrated below.

**Application 1** We sketch a proof that

$$I = \int_{-\infty}^{\infty} \frac{e^{-2\pi i x z} dx}{\cosh \pi x} = \frac{1}{\cosh \pi z}$$

, i.e. $\frac{1}{\cosh \pi z}$ is its own Fourier transform.
Consider the integral of $\frac{e^{-2\pi i x z} dx}{\cosh \pi x}$ along the contour with vertices at $\pm R, \pm R + 2i$. As $R \to \infty$, one can show that the integral along the vertical sides disappears, and apply periodicity of cosh to show that the integral along the top is $e^{-4\pi z} I$. Computing the residues at the poles $i/2, 3i/2$ and applying the residue theorem gives the result.

Some algebra then gives that, if $t > 0$ so that no signs are flipped, the Fourier transform of $f(x) = \frac{e^{-2\pi iax}}{\cosh \frac{\pi x}{t}}$ is $\hat{f}(z) = \frac{t}{\cosh \pi(z+a)t}$, and Poisson summation gives

$$\sum_{n=-\infty}^{\infty} \frac{e^{-2\pi ian}}{\cosh \frac{\pi n}{t}} = \sum_{n=-\infty}^{\infty} \frac{t}{\cosh \pi(n+a)t} \tag{1}$$

**Application 2** We sketch a proof that

$$\int_{-\infty}^{\infty} e^{-2\pi ixz} e^{-\pi x^2} dx = e^{-\pi z^2}$$

, i.e. $e^{-\pi z^2}$ is its own Fourier transform.
Let $\gamma_R$ be the rectangular contour with vertices at $\pm R, \pm R + iz$. $e^{-\pi z^2}$ is holomorphic, so $\int_{\gamma_R} e^{-\pi z^2} dz = 0$. As $\mathbb{R} \to \infty$, simple estimates show the integral along the vertical sides tends to 0.
The integral along the real axis tends to $\int_{-\infty}^{\infty} e^{-\pi x^2} dx$, which equals 1 as a consequence of the well-known Gaussian integral.
The integral along the other horizontal side tends to $-e^{\pi z^2} \int_{-\infty}^{\infty} e^{-2\pi ixz} e^{-\pi x^2} dx$.
Since the sum of these is 0, the result follows.
For $t > 0, a \in \mathbb{R}$, the change of variables $x \mapsto t^{1/2}(x + a)$ shows that $f(x) = e^{-\pi t(x+a)^2}$ has Fourier transform $\hat{f}(z) = t^{-1/2} e^{-\pi z^2/t} e^{2\pi iaz}$. Applying Poisson summation then gives

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

**Application 3** Consider the function $f(z) = \frac{1}{(z+\tau)^k}$, for $Im(\tau) > 0$. This has Fourier transform $\hat{f}(t) = \int_{-\infty}^{\infty} \frac{e^{2\pi itz} dz}{(z+\tau)^k} = \frac{(-2\pi it)^{k-1}}{(k-1)!} \int_{-\infty}^{\infty} \frac{e^{2\pi itz} dz}{(z+\tau)}$ by repeated integration by parts.
Now consider $g(t) = e^{2\pi it\tau}, t > 0, 0$ otherwise. $\int_{-\infty}^{\infty} g(t) e^{2\pi ixt} dt = \int_0^{\infty} e^{2\pi it(\tau+x)} dt = \frac{-1}{2\pi i(x+\tau)}$, where the boundary term disappears since $|e^{2\pi it(\tau+x)}| = e^{-2\pi t Im(\tau)} \to 0$ as $t \to \infty$.
Hence by the Fourier inversion formula, $-2\pi i g(t)$ is the Fourier transform of $\frac{1}{x+\tau}$, so $\hat{f}(t) = \frac{(-2\pi i)^k}{(k-1)!} t^{k-1} e^{2\pi it\tau}, t > 0$, 0 otherwise. Applying Poisson summation then gives

$$\sum_{n=-\infty}^{\infty} \frac{1}{(n+\tau)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{t=1}^{\infty} t^{k-1} e^{2\pi it\tau} \tag{3}$$

It may shock the reader to learn that these aren't just three randomly chosen results that can be proved by Poisson summation. If later on a result is magically proved by reference to an earlier equation that doesn't come to mind, chances are it will be one of these.

# 3 Modular Forms

Let $SL_2(\mathbb{Z})$ be the group of matrices with integer entries and determinant 1. This acts on the complex plane by Mobius maps. Since $-I$ acts trivially, we then consider $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I\}$, which is sometimes called the modular group (others define $SL_2(\mathbb{Z})$ to be the modular group).
For the rest of this essay, let $\mathbb{H} = \{z : Im(z) > 0\}$. Also let $\mathbb{D} = \{\tau \in \mathbb{H} | Re(\tau) \leq 1/2 \text{ and } |\tau| \geq 1\}$, known as the fundamental domain of the modular group.

**Lemma 4.** *Every point in $\mathbb{H}$ can be mapped to a point in $\mathbb{D}$ by finitely many applications of one of the following Mobius maps or their inverses:*

*i* $T : \tau \mapsto \tau + 1$

*ii* $S : \tau \mapsto -\frac{1}{\tau}$

Geometrically, this should be quite believable: if $Im(\tau) \geq 1$, just translate it into the strip. If $Im(\tau) < 1$ and the point lands in the unit disc after translation, just use $S$ to throw it up the plane far enough so that more translations does the job.

*Proof.* Let $G$ be the group generated by T and S, and consider the corresponding Mobius maps. It is not particularly difficult to show that $G \equiv SL_2(\mathbb{Z})$ algebraically; alternatively, one can consider the action of $G$ on $\mathbb{D}$ to give a geometric proof, but the proof is omitted. Every Mobius map M is represented by some matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, and since both T and S are represented by matrices in $SL_2(\mathbb{Z})$, every transformation in G is as well. In particular, for all $M \in G, Im(M(\tau)) = \frac{(ad-bc)Im(\tau)}{|c\tau+d|^2} = \frac{Im(\tau)}{|c\tau+d|^2}$, since $ad - bc = 1, a, b, c, d \in \mathbb{Z}$. This also shows that $SL_2(\mathbb{Z})$ acts on $\mathbb{H}$.
Moreover, $c, d \in \mathbb{Z}$ means that, for every $\tau \in \mathbb{H}$, there is some $M_0 \in G$ such that $|c\tau + d|$ is minimal, hence $Im(M_0(\tau))$ is maximal. Since applying $T$ doesn't affect the imaginary part, we can further assume that $|Re(M_\tau)| \leq 1/2$. Finally, $\frac{Im(M_0(\tau))}{|M_0(\tau)|} = Im(S(M_0(\tau))) \leq Im(M_0(\tau))$ by maximality, so $|M_0(\tau)| \geq 1$, i.e. $M_0(\tau) \in \mathbb{D}$. □

**Definition.** Let $k$ be an integer. A function $f$ is said to be weakly modular of weight $k$ if it is meromorphic in $\mathbb{H}$ and satisfies

$$f(z) = (cz + d)^{-k} f(\frac{az + b}{cz + d})$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$.

Combined with the previous lemma, a function $f$ is weakly modular of weight $k$ if and only if for all $z \in \mathbb{C}$, $f(z + 1) = f(z)$ and $f(-1/z) = z^k f(z)$. In particular, $f$ is periodic so has a Fourier series, i.e. can be written as a function of $q = e^{2\pi i z}$ (also known as the nome). This gives a function $g(q)$ on the punctured unit disc. If $g$ extends to a meromorphic (resp. holomorphic) function at the origin, then $f$ is said to be meromorphic (resp. holomorphic) at infinity.
A weakly modular function is called modular if it is meromorphic at infinity, and called a *modular form* if it is holomorphic at infinity.

We will not develop any general theory of modular forms; this is done in [2] and [3]. Instead, we will study some explicit examples of modular forms and functions which have similar properties.

## 3.1 Eisenstein Series

An urban legend tells the story of a researcher who studied anti-metric spaces: ones where the inequality sign in the triangle inequality is reversed. He managed to prove many amazing properties about such spaces, until it was pointed out that such a space can contain at most one point.
The definition of modular forms forces such functions to exhibit a lot of symmetry, which will be useful in later calculations. However, to avoid repeating others' mistakes, it would be prudent to first exhibit a non-trivial example of a modular form after giving the definition. Eisenstein series give some of the simplest examples of modular forms.
Let $k \geq 3$ be an integer and $\tau \in \mathbb{H}$. Define the Eisenstein series of order $k$ to be $E_k(\tau) = \sum_{(n,m)\in\mathbb{Z}^2\setminus(0,0)} \frac{1}{(n+m\tau)^k}$.

**Theorem 5.** *Eisenstein series have the following properties:*

*i* $E_k(\tau)$ *converges absolutely for* $k \geq 3$ *and is a holomorphic function of* $\tau$

*ii* $E_k(\tau) \equiv 0$ *if* $k$ *is odd*

*iii* $E_k(\tau)$ *satisfies* $E_k(\tau+1) = E_k(\tau)$ *and* $E_k(\tau) = \tau^{-k}E_k(-1/\tau)$,

(ii) is in fact a special case of a more general phenomenon: setting $c = -1, d = 0$ shows that the only modular form of weight $k$ when $k$ is odd is the zero function. Note that absolute convergence means changing the order of summation is valid, which gives the rest of the properties. Pairing up the $(n, m)$ term with the $(-n, -m)$ term gives (ii), and doing some algebra gives (iii). Hence it suffices to prove (i). To this end, we sketch a proof of the following:

**Lemma 6.** *The two series*

$$\sum_{(n,m)\in\mathbb{Z}^2\setminus(0,0)} \frac{1}{(|n|+|m|)^r} \text{ and } \sum_{(n,m)\in\mathbb{Z}^2\setminus(0,0)} \frac{1}{|n+m\tau|^r}$$

*converge for* $r > 2$

*Sketch Proof.* We sum the first series in $m$ and then $n$ to show it is convergent, and hence absolutely convergent since all the terms are positive reals. For $n \neq 0$

$$\begin{aligned}
\sum_{m\in\mathbb{Z}} \frac{1}{(|n|+|m|)^r} &= \frac{1}{|n|^r} + 2\sum_{m\geq 1} \frac{1}{(|n|+|m|)^r} \\
&= \frac{1}{|n|^r} + 2\sum_{k\geq |n|+1} \frac{1}{k^r} \\
&\leq \frac{1}{|n|^r} + 2\int_{|n|}^{\infty} \frac{dx}{x^r} \\
&\leq \frac{1}{|n|^r} + \frac{C}{|n|^{r-1}}
\end{aligned}$$

for some constant $C$. Then for $r > 2$, noting that the series $\sum_n \frac{1}{n^s}$ converges if and only if $Re(s) > 1$,

$$\sum_{(n,m)\in\mathbb{Z}^2\setminus(0,0)} \frac{1}{(|n|+|m|)^r} \leq \sum_{m\neq 0} \frac{1}{|m|^r} + \sum_{n\neq 0} \frac{1}{|n|^r} + \frac{C}{|n|^{r-1}} < \infty$$

Hence the first series converges. To show the second series converges, it suffices to show there exists positive constants $c_1, c_2$ such that $c_1|n+m\tau| \leq |n|+|m| \leq c_2|n+m\tau|$ for all $n, m \in \mathbb{Z}$. The main observation used is for any positive numbers $A$ and $B$, $\sqrt{A^2+B^2} < A+B < 2\sqrt{A^2+B^2}$. The rest of the proof is not interesting so is omitted for ease of exposition. □

This gives absolute convergence. Moreover, this gives uniform convergence in every half-plane $Im(\tau) \geq \delta > 0$, so $E_2(\tau)$ is holomorphic. This finishes the proof of the theorem. As $\tau \to \infty, E_k \to \sum_{n\neq 0} \frac{1}{n^k}$, which converges, so $E_k$ is holomorphic at infinity and is a modular form of weight $k$.

Define $\sigma_k(r) = \sum_{d|r} d^k$, the sum of the $kth$ powers of the divisors of $r$. Note that $\sigma_k(r) < \sum_{d|r} r^k < r^{k+1}$. Let $\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}$ be the infamous Riemann zeta function. The next theorem highlights a connection of Eisenstein series to these much studied functions in number theory.

**Theorem 7.** *Let $k \geq 4$ be even and $\tau \in \mathbb{H}$. Then*

$$E_k(\tau) = 2\zeta(k) + \frac{2(-1)^{k/2}(2\pi)^k}{(k-1)!} \sum_{r=1}^{\infty} \sigma_{k-1}(r) e^{2\pi i \tau r}$$

*Proof.* For all $\tau$ such that $Im(\tau) = t \geq t_0$, $|e^{2\pi i \tau r}| \leq e^{-2\pi t_0 r}$. Together with the bound for $\sigma_k$ given earlier, this shows the series on the right is absolutely convergent in every half plane $t \geq t_0$ by comparison with $\sum_{r=1}^{\infty} r^k e^{-2\pi t_0 r}$. Then,

$$\begin{aligned} E_k(\tau) &= \sum_{n\neq 0} \frac{1}{n^k} + \sum_{m\neq 0} \sum_{n=-\infty}^{\infty} \frac{1}{(n+m\tau)^k} \\ &= 2\zeta(k) + 2\sum_{m>0} \sum_{n=-\infty}^{\infty} \frac{1}{(n+m\tau)^k} \end{aligned}$$

Now recall equation 3. Substituting this in with $m\tau$ in place of $\tau$ gives

$$\begin{aligned} E_k(\tau) &= 2\zeta(k) + 2\sum_{m>0} \frac{(-2\pi i)^k}{(k-1)!} \sum_{l=1}^{\infty} l^{k-1} e^{2\pi i m \tau l} \\ &= 2\zeta(k) + 2\frac{(-1)^{k/2}(2\pi)^k}{(k-1)!} \sum_{m>0} \sum_{l=1}^{\infty} l^{k-1} e^{2\pi i m \tau l} \end{aligned}$$

Finally, changing the order of summation to fix the value of the product $r = ml$ first and then summing over the divisors of $r$ shows this last series is equal to $2\zeta(k) + 2\frac{(-1)^{k/2}(2\pi)^k}{(k-1)!} \sum_{r=1}^{\infty} \sigma_{k-1}(r) e^{2\pi i \tau r}$, as desired. □

For $k = 2$, the series in the definition of $E_2$ doesn't converge absolutely, so more care is needed. Define $F(\tau) = \sum_m \sum_n \frac{1}{(n+m\tau)^2}$, which goes by the scary

sounding name of the *forbidden* Eisenstein series. The argument given above can be adapted to show that

$$F(\tau) = 2\zeta(2) - 8\pi^2 \sum_{r=1}^{\infty} \sigma_1(r) e^{2\pi i \tau r} \tag{4}$$

The reader is advised to keep the series $F$ and the above result in mind as these will be quite important later. Next, we demonstrate some properties of the functions that will appear later.

## 3.2 The Jacobi theta function

For $z \in \mathbb{C}$ and $\tau \in \mathbb{H}$, the Jacobi theta function is defined as

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

**Proposition 8.** $\Theta$ *has the following properties:*

*i* $\Theta$ *is entire in* $z$ *and holomorphic in* $\tau \in \mathbb{H}$

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

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

*iv* $\Theta(z, \tau) = 0$ *whenever* $z = 1/2 + \tau/2 + n + m\tau$ *for any integers* $n, m$.

*Proof.* (i) follows from checking the absolute uniform convergence for $z$ in bounded sets and $\tau$ in half planes. Similar calculations are done at many points in the essay so this one is omitted.
(ii) is immediate from the definition, and (iii) comes from completing the square in the exponents.
Using the previous periodicity properties, to prove (iv) it suffices to check that $\Theta(1/2 + \tau/2, \tau) = 0$.

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

Pairing up $n$ with $-(n+1)$, noting that the difference $2n+1$ is odd so they have different parity, and $(-(n+1))^2 + (-n-1) = n^2 + n$ so the exponential terms match up, gives that the sum is 0. □

Let $q = e^{i\pi\tau}$. Consider the infinite product, sometimes known as the triple-product:

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

This turns out to have many of the same properties as $\Theta$:

**Proposition 9.** $\Pi$ *has the following properties:*

*i* $\Pi$ *is entire in* $z$ *and holomorphic in* $\tau \in \mathbb{H}$

*ii* $\Pi(z+1,\tau) = \Pi(z,\tau)$

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

*iv* *For a fixed* $\tau$, $\Pi(z,\tau) = 0$ *whenever* $z = 1/2 + \tau/2 + n + m\tau$ *for any integers* $n, m$. *These are zeros of order 1, and* $\Pi$ *has no other zeros.*

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

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

$\sum |q|^{2n-1}$ converges, so by the result for infinite products at the start, (i) holds. (ii) is clear from the definition.
To prove (iii), note that $q^2 = e^{2\pi i\tau}$, so $\Pi(z+\tau,\tau) = \prod_{n=1}^{\infty}(1-q^{2n})(1+q^{2n+1}e^{2\pi iz})(1+q^{2n-3}e^{-2\pi iz})$. Comparing with $\Pi(z,\tau)$ and adding in the factors which are missing on either side gives

$$\Pi(z,\tau)(1+(qe^{2\pi iz})^{-1}) = \Pi(z+\tau,\tau)(1+qe^{2\pi iz})$$

Noting that none of the factors are zero because $|q| < 1$ implies $qe^{2\pi iz} \neq -1$, this simplifies to (iii)
Finally, an infinite product vanishes if and only if one of the factors is 0. $|q| < 1$ so $1 - q^{2n} \neq 0$. Suppose $1 + q^{2n-1}e^{2\pi iz} = 0$. Then $e^{(\pi i\tau)(2n-1)}e^{2\pi iz} = e^{\pi i}$. This simplifies to $(2n-1)\tau + 2z = 1 + 2m$ for some integer $m$. This gives zeros of the form $z = 1/2 + \tau/2 - n + m\tau, n \geq 1$. The other zeros come from the other factor, where the argument is essentially the same. Also, each zero is simple since $e^w - 1$ has a simple zero at the origin. □

Readers who, staring at how similar the previous results look, guess that $\Pi$ is $\Theta$ in disguise are right. The proof technique will be one that is used again later, i.e. that these properties define a unique holomorphic function by appealing to Liouville's theorem somehow. First, we prove a lemma.

**Lemma 10.** *Suppose* $f(z)$ *is an entire function, and* $\tau \in \mathbb{C}$ *with* $Im(\tau) > 0$ *that satisfies* $f(z+1) = f(z)$ *and* $f(z+\tau) = f(z)$ *for all* $z \in C$. *(Such functions are called doubly periodic.) Then* $f$ *is constant.*

*Proof.* Consider the set $P = \{a + b\tau, 0 \leq a, b < 1\}$. This is known as the fundamental parallelogram, and it should be geometrically obvious that the plane can be tiled with these, so $f$ is completely determined by its values on $P$. The closure of $P$ is compact, so $f$ attains its bounds on $P$. Hence $f$ is a bounded entire function, so is constant by Liouville's theorem. □

Now the main result.

**Theorem 11.** *For all* $z \in \mathbb{C}, \tau \in \mathbb{H}$, $\Pi$=$\Theta$

*Proof.* Consider $F(z) = \frac{\Theta}{\Pi}$. By the previous propositions, $F$ is entire and has periods 1 and $\tau$. By the previous lemma $F$ is constant. Call this constant $c(\tau)$.

**Claim.** $c(\tau) = c(4\tau)$

*Proof.* Letting $z = 1/2$ gives

$$\sum_{n=-\infty}^{\infty} (-1)^n q^{n^2} = c(\tau) \prod_{n=1}^{\infty} (1-q^{2n})(1-q^{2n-1})(1-q^{2n-1})$$
$$= c(\tau) \prod_{n=1}^{\infty} [(1-q^{2n})(1-q^{2n-1})](1-q^{2n-1})$$

As $n$ runs over the natural numbers, the terms in square brackets together give a factor of $(1-q^k)$ for every natural number $k$, so $c(\tau)\prod_{n=1}^{\infty}[(1-q^{2n})(1-q^{2n-1})](1-q^{2n-1}) = c(\tau)\prod_{n=1}^{\infty}(1-q^n)(1-q^{2n-1})$, and

$$c(\tau) = \frac{\sum_{n=-\infty}^{\infty}(-1)^n q^{n^2}}{\prod_{n=1}^{\infty}(1-q^n)(1-q^{2n-1})} \tag{5}$$

Now let $z = 1/4$. $\Theta(1/4,\tau) = \sum_{n=-\infty}^{\infty}(i)^n q^{n^2}$. Since $\frac{1}{i} = -i$, the terms for odd $n$ cancel, so $\Theta(1/4,\tau) = \sum_{m=-\infty}^{\infty}(-1)^m q^{4m^2}$. On the other side,

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

This mysterious last line demands explanation. Consider the first factor when $m = 2n-1$ is odd. This can then be paired with the second factor from the $m = n$ term to give $(1-q^{8n-4})$. When $m = 2n$, leave the first factor untouched. Putting these together and reordering the product gives the last equality. Hence,

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

Equation 5 implies that the right hand side is $c(4\tau)$ which gives the result. □

Repeatedly applying this gives $c(\tau) = c(4^k\tau)$, and $q^{4^k} = e^{i\pi 4^k\tau} \to 0$ as $k \to \infty$. As $q \to 0$, both $\Pi$ and $\Theta$, and hence $F$, tend to 1, which shows $c(\tau) = 1$. □

Next we consider transformations in the $\tau$ variable. Note that $\Theta(z,\tau+2) = \Theta(z,\tau)$. Also,

**Theorem 12.** $\Theta(z,-1/\tau) = \sqrt{\frac{\tau}{i}}e^{\pi i\tau z^2}\Theta(z\tau,\tau)$

The branch of the square root is taken such that $\sqrt{\frac{\tau}{i}} > 0$ when $\tau = it, t > 0$.

*Proof.* It suffices to prove this for real $z$ and $\tau$ on the imaginary axis, since the identity theorem does the rest of the work. For $x$ real, $\tau = it$, substituting these into the series definition of $\Theta$ and rearranging shows that it suffices to prove

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

This last equation is now just equation 2 with $a$ replaced by $x$. □

Next, we turn to the 'children' of the Jacobi theta function

## 3.3 The (little) theta function

Define $\theta(\tau) = \Theta(0,\tau) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau}$. This naturally inherits a lot of properties from the Jacobi theta function and will be used a lot in the next two sections, so readers are advised to familiarise themselves with the next few results.
A consequence of the product formula for $\Theta$ is $\theta(\tau) = \prod_{n=1}^{\infty}(1-q^{2n})(1+q^{2n-1})^2$, so $\theta$ is never 0. Moreover, as a consequence of Theorem 12, if $Im(\tau) > 0$

$$\theta(\frac{-1}{\tau}) = \sqrt{\frac{\tau}{i}}\theta(\tau) \tag{6}$$

**Proposition 13.**

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

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

*Proof.* Since $n, n^2$ have the same parity, $\theta(1+\tau) = \sum_{n=-\infty}^{\infty}(-1)^n q^{n^2} = \Theta(1/2,\tau)$. Then, together with theorem 12,

$$\begin{aligned}\theta(1-1/\tau) &= \Theta(1/2, -1/\tau) \\ &= \sqrt{\frac{\tau}{i}} e^{\pi i \tau/4} \Theta(\tau/2, \tau) \\ &= \sqrt{\frac{\tau}{i}} \sum_{n=-\infty}^{\infty} e^{\pi i (n+1/2)^2 \tau} \\ &= 2\sqrt{\frac{\tau}{i}} \sum_{n=0}^{\infty} e^{\pi i (n+1/2)^2 \tau}\end{aligned}$$

Let $Im(\tau) = t$. The sum of the $k \neq 0$ terms is of order $O(\sum_{k=1}^{\infty} e^{\pi i (k+1/2)^2 \tau}) = O(e^{-9\pi t/4})$ □

## 3.4 Dedekind eta function

The last function to consider is the Dedekind eta function, which will be used in the proof of the four squares theorem. For $Im(\tau) > 0$, define

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

**Proposition 14.** *For* $Im(\tau) > 0, \eta(\frac{-1}{\tau}) = \sqrt{\frac{\tau}{i}}\eta(\tau)$

*Proof.* Using the product formula for the Jacobi theta function and shifting the third factor,

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

Note that the first factor vanishes at $z_0 = 1/2 + \tau/2$.
Define $H(\tau) = \prod_{n=1}^{\infty}(1-e^{2\pi in\tau})^3$. Differentiating $\Theta$ with respect to $z$ gives

$$\begin{aligned}\Theta'(z,\tau) = (1+qe^{-2\pi iz})\frac{\mathrm{d}}{\mathrm{d}z}(\prod_{n=1}^{\infty}(1-q^{2n})(1+q^{2n-1}e^{2\pi iz})(1+q^{2n-1}e^{-2\pi iz}))\\ + \frac{\mathrm{d}((1+qe^{-2\pi iz}))}{\mathrm{d}z}(\prod_{n=1}^{\infty}(1-q^{2n})(1+q^{2n-1}e^{2\pi iz})(1+q^{2n-1}e^{-2\pi iz}))\end{aligned}$$

Substituting $z = z_0$ makes the first term disappear, and we are left with

$$\Theta'(z_0,\tau) = 2\pi i H(\tau)$$

Replace $-1/\tau$ by $\tau$ in Theorem 12 then gives

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

Differentiating this, evaluating at $z_0$ and simplifying then gives

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

When $\tau = it, t > 0$, $\eta(\tau)$ is a positive real number, as are all the terms in the above equation. Hence, taking cube roots, the claim in the proposition is true on the imaginary axis, and by the identity theorem it is true everywhere in $\mathbb{H}$. □

These are all the preliminary results, and the fruits of our labour will soon be seen in the next sections, which illustrate the utility of modular forms in number theory.

# 4 Sum of two squares theorem

The question to be answered in this section is the following: Given a positive integer $n$, how many ordered pairs $(a,b) \in \mathbb{Z}^2$ are there such that $n = a^2 + b^2$? Denote this number by $r_2(n)$. By considering squares modulo 4, one can quickly see that $r_2(n) = 0$ if $n \equiv 3 \mod 4$, but then one quickly becomes stuck when trying to find all $n$ with $r_2(n) > 0$ using this approach. The correct result is:

**Theorem 15.** *A positive integer $n$ is representable (as a sum of two squares) if and only if every prime $p \equiv 3 \mod 4$ appears with an even exponent in the prime factorization of $n$.*

The legendary mathematician Pál Erdős believed that God keeps a book of the most elegant proofs of every theorem in mathematics, and many Book

proofs of this theorem have appeared over the years since Fermat first claimed that an odd prime $p$ can be written as the sum of two squares if and only if $p \equiv 1 \mod 4$.[1] Interested readers should see [4]. One might ask why we went through the great trouble of the past sections when a much simpler proof of the exact same result is available. The cynic might suggest it is to show off our knowledge of complex analysis: when the only tool you have is a hammer, every problem seems like a nail. Less facetiously, a new proof of an known result is never a bad thing, and often sheds new light on the problem. Crucially, many of these proofs have the disadvantage that no indication of the actual value of $r_2(n)$ is given (in the cases where it is non-zero). As we shall see, an approach based on complex analysis, while arguably not as beautiful, gives an exact formula in the case of two and four squares.[2] With the historical and philosophical remarks aside, we turn our attention to the mathematics.

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

$$\theta(\tau)^2 = (\sum_{n_1=-\infty}^{\infty} q^{n^2})(\sum_{n_2=-\infty}^{\infty} q^{n^2}) = \sum_{(n_1,n_2)\in\mathbb{Z}^2} q^{n_1^2+n_2^2} = \sum_{n=0}^{\infty} r_2(n)q^n \qquad (7)$$

where absolute convergence allows us to change the order of summation and $r_2(0) = 1$, and as a sanity check the last sum converges for $|q| < 1$ since $r_2(n) < 4n + 2$: the first number in the ordered pair must have modulus at most $n$, and the second number can take two possibilities (if any). Similar remarks will apply to other sums which appear later. Thus, $\theta(\tau)^2$ is the generating function for the sequence $\{r_2(n)\}$. This much is motivatable.
Let $d_1(n)$ be the number of divisors of $n$ which are $\equiv 1 \mod 4$, and $d_3(n)$ be the number of divisors of $n$ which are $\equiv 3 \mod 4$. In the source material, the correct result

**Theorem 16.** $r_2(n) = 4(d_1(n) - d_3(n)), n \geq 1$

is given, and the entire section is devoted solely to proving it. However, a couple of remarks are in order. The first is very minor: we could have defined $r_2(n)$ to be the number of unordered pairs of positive integers whose sum of squares is $n$, which at first sight is a simplification, but then computing its generating function would be messier.
The second is the question of how one might come up with this formula if one didn't already know it. If one believes Fermat's result for odd primes, it suggests a connection between $r_2(n)$ and the mod 4 properties of a numbers divisors. Noting the identity $(a^2 + b^2)(c^2 + d^2) = (ad + bc)^2 + (ac - bd)^2$ [3], which in turn comes from looking at $(a+ib)(c+id) = (ac-bd)+i(ad+bc)$ and taking norms, and the well-known fact that $2 = 1^2 + 1^2$, one could decide to consider the odd divisors only. Small cases would then give the conjecture, which can be verified

[1] Characteristically, Fermat gave no proof, hence the use of the word 'claimed'. This author thinks that he should have used paper with larger margins.

[2] A great many powerful results in analytic number theory are proved by exploiting the amazing properties of holomorphic functions, but some have criticised this approach as not really shedding light on the number-theoretic aspect of the results. Sadly, a detailed discussion of this topic, and the alternative viewpoints, would be well beyond the scope of this essay.

[3] Sometimes known as the Brahmagupta-Fibonacci identity, which is a bit unnecessary since it takes about as much ink to just write out the identity.

directly for primes. If $x^2+y^2=p\equiv 1 \mod 4$, then $p=(x+iy)(x-iy)$ in $\mathbb{Z}[i]$, which is a unique factorization domain, so the representation is 'unique', giving $r_2(p)=8$. One could then make a conjecture, and set about proving it with the machinery of generating functions and complex analysis, which is what follows. However, the reader is advised to remember this point, as we will return to it.

$r_2(n)=4(d_1(n)-d_3(n))$ is equivalent to the statement that they have the same generating function, so consider the generating function of $d_1(n), d_3(n)$.

$$\sum_{k=1}^{\infty} d_1(k)q^k=\sum_{n=1}^{\infty}\sum_{m=0}^{\infty} q^{n(4m+1)}=\sum_{n=1}^{\infty}\frac{q^n}{1-q^{4n}} \tag{8}$$

and similarly $d_3(n)$ has generating function $\sum_{n=1}^{\infty}\frac{q^{3n}}{1-q^{4n}}$, so $4(d_1(n)-d_3(n))$ has generating function $4\sum_{n=1}^{\infty}\frac{q^n}{1-q^{4n}}-\frac{q^{3n}}{1-q^{4n}}=4\sum_{n=1}^{\infty}\frac{q^n}{1+q^{2n}}$. Hence, the problem now becomes showing that

$$\theta(\tau)^2=1+4\sum_{n=1}^{\infty}\frac{q^n}{1+q^{2n}}=2\sum_{n=-\infty}^{\infty}\frac{1}{q^n+q^{-n}}=\sum_{n=-\infty}^{\infty}\frac{1}{\cos n\pi\tau} \tag{9}$$

where the last equality follows from remembering that $q=e^{i\pi\tau}$. This should seem promising, since the cosine function displays periodicity, and the symmetry of the range of summation could give other properties that match those of $\theta$. One could then hope to find enough properties to force the two (generating) functions to be equal, exploiting the fact that far weaker conditions are necessary for holomorphic functions to be equal compared to differentiable functions over the reals. Indeed, this is what comes next.

Call the last series, the sum of cosines, $C(\tau)$. Clearly, $C(\tau+2)=C(\tau)$. Also, as $Im(\tau)\to\infty, |\cos n\tau\pi|\to\infty$, just by looking at the definition in terms of exponentials, so $C(\tau)\to 1$ (only the $n=0$ term is left). We now abuse equation 1.

Setting $a=0$, we get $\sum_{n=-\infty}^{\infty}\frac{1}{\cosh\frac{\pi n}{t}}=\sum_{n=-\infty}^{\infty}\frac{t}{\cosh\pi nt}$, and letting $t=\frac{\tau}{i}$, noting the definition of cosh and cos in terms of exponentials, gives that $C(\tau)=\frac{i}{\tau}C(\frac{-1}{\tau})$ for all $\tau$ on the positive imaginary axis. It is then true for all $\tau$ in $\mathbb{H}$ by the identity theorem.

At this point, we know that $C$ and $\tau$ have the same quasi-modular properties, and display the same behaviour for large values of $Im(\tau)$. The last part of $\mathbb{H}$ which is of interest, i.e. where there might be pathological behaviour, is when $\tau$ gets close to the real axis. Since the map $z\mapsto\frac{-1}{z}$ fixes the unit circle and swaps the regions inside and outside the circle, applying the periodicity and the Mobius map should determine the behaviour, except for when $\tau$ is near 1. Hence one more result is needed.

Setting $a=0.5$ in equation 1 this time, $\sum_{n=-\infty}^{\infty}\frac{(-1)^n}{\cosh\frac{\pi n}{t}}=\sum_{n=-\infty}^{\infty}\frac{t}{\cosh\pi(n+\frac{1}{2})t}$. Again setting $t=\frac{\tau}{i}$, and noting that $\cos(x+n\pi)=(-1)^n\cos x$, we get that $C(1-\frac{1}{\tau})=\sum_{-\infty}^{\infty}\frac{\tau}{i}\frac{1}{\cos\pi(n+\frac{1}{2})\tau}=2\frac{\tau}{i}\sum_{0}^{\infty}\frac{1}{\cos\pi(n+\frac{1}{2})\tau}$ on the positive imaginary axis, and hence everywhere in $\mathbb{H}$ by the identity theorem again. Writing $\frac{1}{\cos\pi(n+\frac{1}{2})\tau}=\frac{2e^{i\pi(n+\frac{1}{2})\tau}}{1+e^{i\pi(2n+1)\tau}}$, we see that as $Im(\tau)\to\infty$, $n=0$ is the dominant term, i.e. $C(1-\frac{1}{\tau})\sim 4\frac{\tau}{i}e^{\pi i\tau/2}$ as $Im(\tau)\to\infty$. Hence the following theorem has been proved:

**Theorem 17.** *$C$ satisfies the following properties:*

*i* $C(\tau+2) = C(\tau)$

*ii* $C(\tau) = \frac{i}{\tau} C(\frac{-1}{\tau})$

*iii* $C(\tau) \to 1$ *as* $Im(\tau) \to \infty$

*iv* $C(1-\frac{1}{\tau}) \sim 4\frac{\tau}{i} e^{\pi i \tau/2}$ *as* $Im(\tau) \to \infty$

These are the exact same properties that $\theta^2$ has (c.f. equation 6 and proposition 13). Furthermore, $\theta^2$ has no zeros in $\mathbb{H}$ by the product formula, so $f = \frac{C}{\theta^2}$ is a holomorphic function of $\tau$ in $\mathbb{H}$. Since the goal is to show that this is identically 1, we need some sort of result that says the conditions we have force $f$ to be constant. First note that $f(\frac{-1}{\tau}) = f(\tau) = f(\tau+2)$. Next, by an analogous argument to that given in the section on modular forms, the following is true:

**Lemma 18.** *Every point in $\mathbb{H}$ can be mapped to a point in $\mathbb{F} = \{\tau \in \mathbb{H} | Re(\tau) \leq 1 and |\tau| \geq 1\}$ by finitely many applications of one of the following Mobius maps or their inverses:*

*i* $T : \tau \mapsto \tau + 2$

*ii* $S : \tau \mapsto -\frac{1}{\tau}$.

Note that this is the general construction for any finite index subgroup of the modular group: it is possible to consider functions obeying the equation for any element of the finite index subgroup, and is determined by its values on the corresponding fundamental domain.
With this result, we now see that $f$ is bounded: the open unit disc can be conformally mapped to $\mathbb{H}$ by some function $g$, and the preimage of $\mathbb{F}$ only approaches three points on the boundary of the unit disc. $f \circ g$ defines a function on $g^{-1}(\mathbb{F})$ which is bounded near the boundary of the unit disc, and after removing some suitable neighbourhood of those points, the rest of the domain is compact, so $f \circ g$ must be bounded. Hence $f$ is bounded on $\mathbb{F}$, and therefore on $\mathbb{H}$.
The asymptotics of $C$ and $\theta^2$ imply that $f \to 1$ as $\tau \to \pm 1$ (known as the cusps), and as $Im(\tau) \to \infty$. Since we want to show that $f$ is identically 1, and know it tends to 1 at the boundary, it suggests we try some sort of maximum modulus principle argument.
Suppose $f$ is not constant. Define $g(e^{i\pi\tau}) = f(\tau)$, noting this is well defined by the periodicity of $f$, $g$ is a non-constant holomorphic function on the punctured unit disc. $f(\tau) \to 1$ as $Im(\tau) \to \infty$, so the singularity at $z = 0$ is removable. Then by the maximum modulus principle applied to $g$, there is some $w$ such that $|g(w)| > |g(0)|$, so there is some $\tau_0 \in \mathbb{F}$ such that $|f(\tau_0)| > 1$. Since $f(\tau) \to 1$ as $\tau \to \pm 1$, $|f|$ attains its maximum in the interior of $\mathbb{H}$, which contradicts the maximum modulus principle. Hence $f$ must be a constant, and asymptotics force the constant to be 1, as desired.

The theorem given at the beginning of the section can now be deduced as a corollary: suppose $q_{a_1} \dots q_{a_k}$ are the primes $\equiv 3 \mod 4$ dividing $n$. Then if $2 \nmid d | n$, $d \equiv 1 \mod 4$ if and only if the sum of the exponents of the $q_{a_i}$ is even. If any $q_{a_i}$ appears with odd exponent in $n$, then multiplying by powers of this prime gives a bijection between odd divisors $\equiv 1 \mod 4$ and $\equiv 3 \mod 4$. If

every $q_{a_i}$ appears with even exponent, then $r_2(n) > 0$.

We now revisit the connection with the Gaussian integers. $(d_1(n) - d_3(n)) = \sum_{d|n, 2\nmid d}(-1)^{\frac{d-1}{2}} = c(n)$. This latter function is in fact multiplicative: $c(mn) = c(m)c(n)$ for $m, n$ coprime. To see this,

$$c(m)c(n) = (\sum_{c|m, 2\nmid c}(-1)^{\frac{c-1}{2}})(\sum_{d|n, 2\nmid d}(-1)^{\frac{d-1}{2}}) = \sum_{c|m, d|n 2\nmid c,d}(-1)^{\frac{c-1+d-1}{2}}$$

Now, $\frac{cd-1}{2} - \frac{c-1+d-1}{2} = \frac{(c-1)(d-1)}{2}$, which is even since both $c$ and $d$ are odd. Also, every divisor $cd$ of $mn$ arises uniquely as the product of a divisor of $m$ and a divisor of $n$ if $m, n$ are coprime, so $c(m)c(n) = \sum_{cd|mn, 2\nmid cd}(-1)^{\frac{cd-1}{2}} = c(mn)$. One can then check that $r_2(n) = 4c(n)$ holds for all prime powers, with the main case being $p^k$ when $p \equiv 1 \mod 4$. Note that $p$ uniquely factorises as $(a + ib)(a - ib)$, and writing $n = x^2 + y^2$ is equivalent to specifying, up to multiplication by units, $n = (x + iy)(x - iy)$. For $p^k$, the factor $(x + iy)$ can arise in $c(p^k) = k + 1$ ways, corresponding to the number of times the factor of $(a + ib)$ is taken (as opposed to its conjugate). The factor of 4 appears because $\mathbb{Z}[i]$ has 4 units: $\pm 1, \pm i$. This draws out the multiplicative nature and some sort of connection to the whether the primes in the factorization are representable. In fact, multiplicative functions have become an active area of modern research, particularly as an alternative to the complex analysis based approach alluded to in a previous footnote. Interested readers should see for example the works of Granville and Soundararajan.
The next section covers the four squares theorem, in which the reader should notice how much the argument resembles that given for the two squares theorem.

# 5 Four squares theorem

Knowing the result and proof for the case of two squares, we now do the analogous calculations for the four squares case.
The generating function for $r_4(n)$ is given by $\theta(\tau)^4$. In the previous section a nice sum of cosines was found. No such luck this time. Define

$$E_2^*(\tau) = \sum_m \sum_n \frac{1}{\frac{m\tau}{2} + n} - \sum_m \sum_n \frac{1}{\frac{n}{2} + m\tau} \tag{10}$$

ignoring the terms where $m = 0 = n$. This is basically a couple of Eisenstein series: $E_2^*(\tau) = F(\frac{\tau}{2}) - 4F(2\tau)$.

Also define $\sigma_1^*(n) = \sum_{4\nmid d|n} d$. Then $\sigma_1^*(n) = \begin{cases} \sigma_1(n), 4 \nmid n \\ \sigma_1(n) - 4\sigma(n/4), 4|n \end{cases}$

Let $q = e^{i\pi\tau}$. We claim now that

$$-\frac{1}{\pi^2}E_2^*(\tau) = 1 + \sum_{k=1}^{\infty} 8\sigma_1^*(k)q^k \tag{11}$$

But remembering the following fact proved at the end of the section on Eisenstein series, $F(\tau) = \frac{\pi^2}{3} - 8\pi^2 \sum_{k=1}^{\infty} \sigma_1(k)e^{2\pi ik\tau}$ and substituting in gives the result. We will abuse this equation some more in what follows.

By the periodicity of $F$, it is immediate that $E_2^*(\tau+2) = E_2^*(\tau)$. Letting $Im(\tau) \to \infty$ in the above series for $F$ also shows that $F \to \frac{\pi^2}{3}$, so $E_2^* \to -\pi^2$. Comparing with the two squares theorem, the next step is to show that $E_2^*$ has the same modular properties as $-\pi^2\theta^4$.
Next on the list of properties is the following: $E_2^*(\tau) = -\tau^{-2}E_2^*(-1/\tau)$. For that, we need to consider $F(-1/\tau)$. Define $\tilde{F}(\tau) = \sum_n \sum_m \frac{1}{m\tau+n}$, omitting the $m = 0 = n$ term. Note that the series defining $F$ isn't absolutely convergent, so the order of summation matters. Now we prove:

**Lemma 19.** *$F, \tilde{F}$ satisfy*

*i* $F(-1/\tau) = \tau^2\tilde{F}(\tau)$

*ii* $F(\tau) - \tilde{F}(\tau) = \frac{2\pi i}{\tau}$ *(note this proves to any skeptical readers that the series doesn't converge absolutely, since it turns out the order of summation does matter)*

*iii* $F(-1/\tau) = \tau^2 F(\tau) - 2\pi i\tau$

*Proof.* The first property follows from simple algebra.
Consider the Dedekind eta function $\eta(\tau) = q^{\frac{1}{12}}\prod_{n=1}^{\infty}(1-q^{2n})$. Taking logarithmic derivatives gives

$$\frac{\eta'}{\eta} = \frac{\pi i}{12} - 2\pi i\sum_{n=1}^{\infty}\frac{nq^{2n}}{1-q^{2n}} \tag{12}$$

But

$$\sum_{n=1}^{\infty}\frac{nq^{2n}}{1-q^{2n}} = \sum_{n=1}^{\infty}\sum_{l=0}^{\infty} nq^{2n}q^{2ln} = \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} nq^{2mn} = \sum_{n=1}^{\infty}\sigma_1(k)q^{2k} \tag{13}$$

where the last equality comes from fixing the value $k$ of the product $mn$ and then allowing $n$ to run over the divisors of $k$. This amounts to changing the order of summation, which is once again valid due to absolute convergence. Comparing with the series for $F$ then gives

$$\frac{\eta'}{\eta} = \frac{i}{4\pi}F(\tau)$$

We have also proved that $\eta(\tau)$ satisfies $\eta(-1/\tau) = \sqrt{\frac{\tau}{i}}\eta(\tau)$, and taking logarithmic derivatives and rearranging the resulting equation gives (ii).
Putting (i) and (ii) together gives (iii). □

Applying (iii) to $E_2^*(\tau) = F(\frac{\tau}{2}) - 4F(2\tau)$ gives the desired property for $E_2^*(\tau)$.

Finally, we have to study the behaviour at the cusp. $E_2^*(1-1/\tau) = F(\frac{1}{2}(1-1/\tau)) - 4F(2(1-1/\tau))$, so we deal with each term in turn (repeatedly) using the last lemma. For the first term,

$$F(\frac{1}{2}(1-1/\tau)) = (\frac{2\tau}{\tau-1})^2 F(\frac{2\tau}{\tau-1}) - 2\pi i\frac{2\tau}{\tau-1},$$

and

$$F(\frac{2\tau}{\tau-1}) = F(-2+\frac{2}{1-\tau}) = F(\frac{2}{1-\tau}) = (\frac{1-\tau}{2})^2 F(\frac{\tau-1}{2}) - 2\pi i(\frac{\tau-1}{2})$$

For the second term,

$$F(2(1-1/\tau)) = F(-2/\tau) = (\frac{\tau}{2})^2 F(\frac{\tau}{2}) - 2\pi i \frac{\tau}{2}$$

Substituting all of these into the expression for $E_2^*$ gives

$$E_2^*(1-1/\tau) = \tau^2(F(\frac{\tau-1}{2}) - F(\frac{\tau}{2})) \tag{14}$$

Using the series expansion for $F$, we have thus proved the following:

**Proposition 20.** *$E_2^*$ satisfies the following properties:*

*i* $E_2^*(\tau+2) = E_2^*(\tau)$

*ii* $E_2^*(\tau) = \frac{-1}{\tau^2} E_2^*(\frac{-1}{\tau})$

*iii* $E_2^*(\tau) \to -\pi^2$ *as* $Im(\tau) \to \infty$

*iv* $|E_2^*(1-\frac{1}{\tau})| = O(|\tau^2 e^{\pi i \tau}|)$ *as* $Im(\tau) \to \infty$

$-\pi^2\theta^4$ also satisfies these properties (c.f. equation 6 and proposition 13). Unfortunately, we are not done yet. Defining $f = \frac{E_2^*}{-\pi^2\theta^4}$, which we would like to be identically 1 in $\mathbb{H}$, (iv) only says $f$ is bounded near the cusp, but not what value it tends to. We could try and compute it, in the hope it turns out to be 1, then we could apply the same maximum modulus principle argument. However, it turns out the following is true:

**Theorem 21.** *Suppose $f$ is a holomorphic function on $\mathbb{H}$ satisfying*

*i* $f(\tau+2) = f(\tau)$

*ii* $f(\tau) = f(-1/\tau)$

*iii* $f$ *is bounded*

*Then $f$ is constant.*

*Proof.* The argument follows the one we gave for the two squares theorem, except now more machinery is needed to handle the point at the cusp. However, the idea is the same, as one could potentially guess from the mapping to the unit disc, since in the extended complex plane (or Riemann sphere) there is not really anything special about infinity, and for example in half-plane model of hyperbolic geometry, points on the real line are basically the same as the point at infinity.

Consider $F(\tau) = f(1-\frac{1}{\tau})$. This interchanges the roles of 1 and $\infty$, so if we can show that $|F|$ doesn't tend to its supremum as $Im(\tau) \to \infty$ then $f$ wouldn't attain its maximum near the cusp, so it would attain its maximum modulus in the interior of $\mathbb{H}$ and we reach the same contradiction as before. In particular, the contradiction arose last time from defining a function on the unit disc so that we could apply the maximum modulus principle.

We prove that $F$ is periodic. Define functions $u_n(\tau) = \frac{(1-n)\tau+n}{-n\tau+(1+n)}, \mu(\tau) = \frac{1}{1-\tau}, T_n(\tau)$. Then $u_n = \mu^{-1}T_n\mu$, so $u_n u_m = u_{n+m}$ and $u_{-1} = T_2 S$. Hence any $u_n$ can be obtained by finitely many applications of $T_2, S$, or their inverses.

Since $f$ is invariant $T_2, S$, it is invariant under $u_n$, so $f(\mu^{-1}T_n\mu(\tau)) = f(\tau)$. Since $F(\tau) = f(\mu^{-1}(\tau), F(T_n(\tau)) = F(\tau)$ for all $n \in \mathbb{Z}$. In particular, $F$ has period 1, so $h(e^{2\pi i\tau}) = F(\tau)$ is the function on the disc, which completes the proof. □

Using this result, $f \equiv 1$ in $\mathbb{H}$, so we have proved that $r_4(n) = 8\sigma_1^*(n)$. In particular, this is always $\geq 1$ since 1 is always a divisor, so every number can be written as a sum of 4 squares.

# 6 What next?

The case for 8 squares follows the exact same argument and is given as an exercise in [1]. In chapter 7 of [3], the increasingly complicated formulae for $r_{2k}, 1 \leq k \leq 12$ are listed. The explanation for why the answers get messier is that the space of modular forms of a given weight is a vector space over $\mathbb{C}$, whose dimension can be calculated. For small $k$, this dimension is 1, and studying the Eisenstein series suffices, but when the dimension increases, other forms have to be studied.
The reader may be wondering what of sums of an odd number of squares, which aren't covered in [3]. This is a much tougher question to answer, which we will not go into, but make two observations which might suggest why this is more difficult.
The first is $(1^2 + 1^2 + 1^2)(2^2 + 1^2 + 0^2) = 15$, which can't be written as the sum of 3 squares. This illustrates that unlike in the cases of 2 and 4 squares, there is no identity guaranteeing that the product of a sum of 3 squares is a sum of 3 squares (there are very deep reasons why no such identity can exist: see [5]). Legendre's three square theorem states a number is a sum of 3 squares if and only if it is not of the form $4^a(8b + 7)$ for nonnegative integers $a, b$.
The second is equation 6. The generating function for the sum of $k$ squares is $\theta^k$. When $k$ is even this obeys a modular form type relation, but when $k$ is odd, this contains a square root, and requires developing the theory of modular forms of non-integer weights.

# References


[1] Elias M. Stein and Rami Shakarchi, Complex analysis, Princeton Lectures in Analysis, vol. 2, Princeton University Press, Princeton, NJ, 2003.

[2] Serre, J.P. A Course in Arithmetic. Springer, 1996

[3] Rankin, R. (1977). Modular Forms and Functions. Cambridge: Cambridge University Press. doi:10.1017/CBO9780511566035

[4] Aigner, Martin; Ziegler, Günter (2009). Proofs from THE BOOK (4th ed.). Berlin, New York: Springer-Verlag. ISBN 978-3-642-00855-9.

[5] https://en.wikipedia.org/wiki/Hurwitz_problem