# Introduction to Modular Forms

Lecture Notes

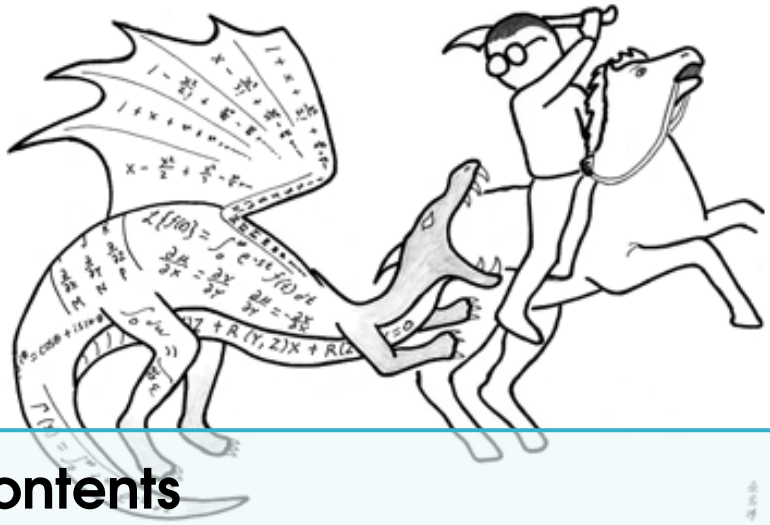
*Alexander J. Barrios*

2021 ARIZONA WINTER SCHOOL

These are the lecture notes for the Arizona Winter School's Introduction to Modular Forms

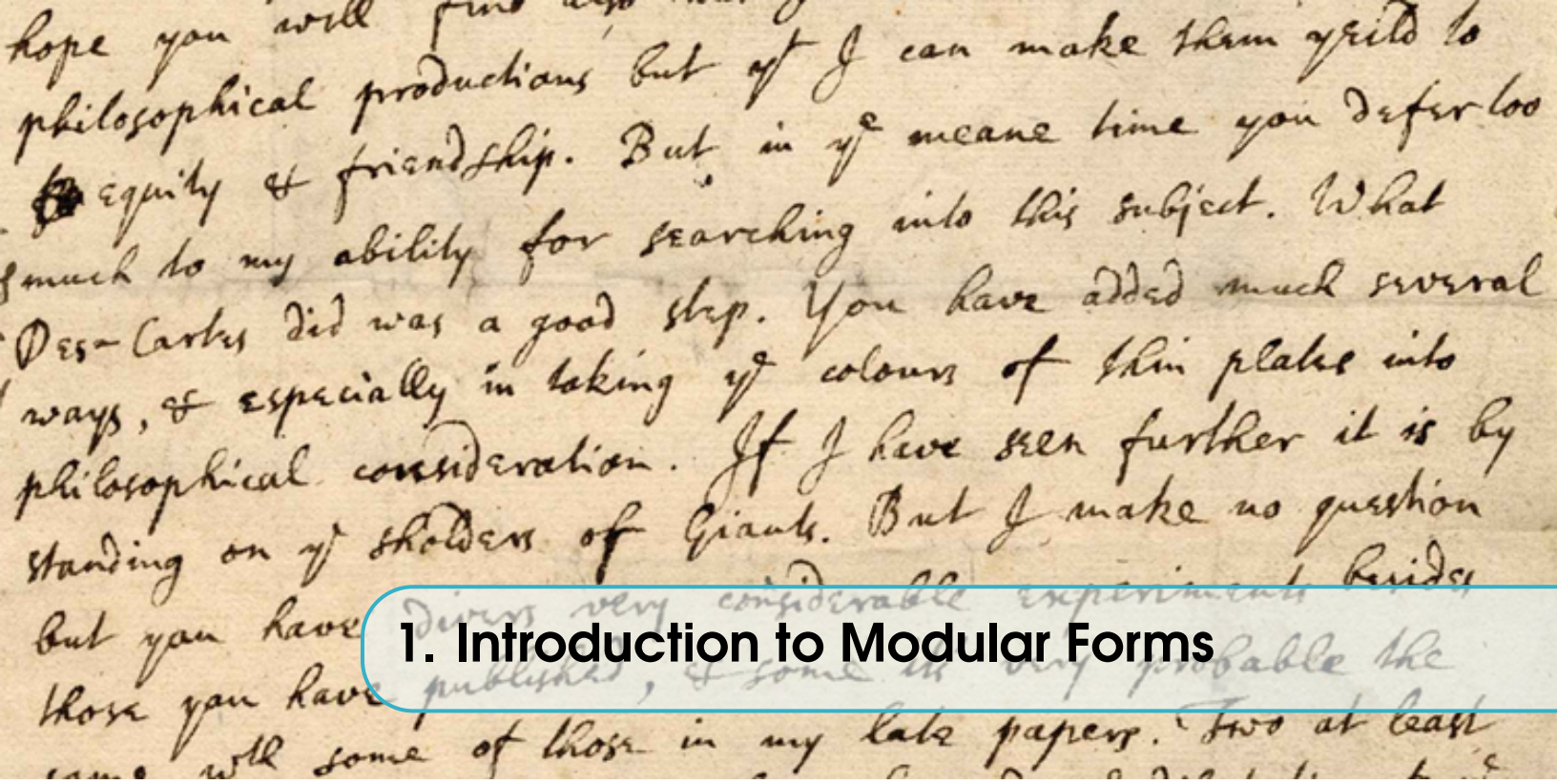
*Last Updated, January 30, 2021*

HOW TO STUDY MATH



# Contents

**Don't just read it; fight it!**
— *Paul R. Halmos*



# 1. Introduction to Modular Forms

## 1.1 Euler and $q$-Series

### 1.1.1 Sums of Two and Four Squares

In the third century of the common era, Diophantus of Alexandria published a series of books called *Arithmetica*. Unfortunately, most of these books were lost, but those that remained would inspire mathematicians a millennia later to found the modern branch of number theory. Our story begins with Claude Gaspard Bachet de Méziriac, who, in 1621, published a Latin translation with extensive commentary of the surviving books which composed the *Arithmetica*. In this work, Bachet notes that Diophantus had assumed in two of the surviving problems that every positive integer can be expressed as a sum of four squares. Unfortunately, no proof was provided, and it is unclear whether Diophantus had a proof or based this assumption on experimental evidence. That being said, upon the publication of Bachet's translation, mathematicians worked at proving this claim. But, it would take over a century until Joseph-Louis Lagrange settled the claim:

**Theorem 1.1 — Lagrange's Four-Square Theorem, 1770.** If $n$ is a positive integer, then there exists integers $a, b, c$, and $d$ such that $n = a^2 + b^2 + c^2 + d^2$.

As part of our course, we will follow Carl Gustav Jacob Jacobi's footsteps and prove Theorem 1.1. Related to Theorem 1.1 is the question of which positive integers are expressible as a sum of two squares. As with Theorem 1.1, this question was inspired by Diophantus's *Arithmetica*.

In 1636, Pierre de Fermat purchased a copy of Bachet's translation of Diophantus's *Arithmetica*. This began a life-long obsession for Fermat with the theory of numbers. In fact, throughout his lifetime, he would write forty-eight marginal notes in his copy of *Arithmetica*. In these notes, Fermat wrote down mathematical statements which he claimed to have proven. Of these claims, only one had a sketch of a proof, namely what is known today as Fermat's Right Triangle Theorem. Five years after his passing, his son, Clément-Samuel de Fermat, published a new edition of *Arithmetica* with his father's marginal notes. These notes would go on to galvanize mathematicians to prove

Fermat's remaining forty-seven claims. One of these claims is the infamous Fermat's Last Theorem[1], which will be discussed at length in the second half of the Arizona Winter School. Our focus for this course will be on another famous marginal note of Fermat, namely his Sums of Squares Theorem:

**Theorem 1.2 — Fermat's Sum of Two Squares Theorem, 1749.** Let $p$ be an odd prime number. Then $p = a^2 + b^2$ for some integers $a$ and $b$ if and only if $p \equiv 1 \mod 4$.

Unlike Fermat's Last Theorem, Fermat corresponded with mathematicians to inform them that he had a solid proof of his Sums of Squares Theorem and challenged them to find their own proof of this statement. The first of these correspondences dates to December 25, 1640, when Fermat wrote to Marin Mersenne. For the next century mathematicians worked at Establishing Fermat's claim, which Leonhard Euler finally settled in 1749. Immediately after completing his proof, Euler wrote to Christian Goldbach: "Now have I finally found a valid proof [of Fermat's Sum of Squares Theorem]." Euler's work on Fermat's Sums of Squares laid the foundation for what is now known as the Law of Quadratic Reciprocity, established by Carl Friedrich Gauss in 1796. [For those who have seen the Law of Quadratic Reciprocity, Euler conjectured [Cox13] the following which is equivalent to the law of quadratic reciprocity:

**Conjecture 1.3 — Euler's Conjecture, 1744.** Let $p$ and $q$ be distinct odd primes. Then $q \equiv a^2 \mod p$ for some integer $a$ if and only if $p \equiv \pm b^2 \mod 4q$ for some odd integer $b$.

For homework, you will have the opportunity to prove that Euler's Conjecture is equivalent to the Law of Quadratic Reciprocity.]

In addition to proving Fermat's claim, Euler established the following generalization:

**Theorem 1.4 — Sum of Two Squares Theorem, 1749.** Let $n$ be a positive integer. Then $n = a^2 + b^2$ for some integers $a$ and $b$ if and only if each prime $q \equiv 3 \mod 4$ that appears in the prime factorization of $n$ appears with an even exponent.

The following exercise will have you deduce the Sum of Squares Theorem by assuming Fermat's Sum of Squares Theorem. We note that the forward direction of the Sum of Squares Theorem can be attained without assuming Fermat's result.

**Exercise 1.1** (1) Prove the following proposition of Diophantus (250 C.E.): If $m$ and $n$ can be expressed as a sum of two squares, then $mn$ can also be expressed as a sum of squares.

(2) Assume Fermat's Sums of Squares Theorem and let $n$ be a positive integer. Show that $n = a^2 + b^2$ for some integers $a$ and $b$ if and only if each prime $q \equiv 3 \mod 4$ that appears in the prime factorization of $n$ appears with an even exponent.

In 1750, Euler wrote to Goldbach with a roadmap for deducing a new proof of the sums of

[1] The reason for it being called the last theorem is that in the 20th-century, it was the last of Fermat's claims which remained open. In 1994, Andrew Wiles and Richard Taylor settled a special case of the Taniyama-Shimura Conjecture. This settled Fermat's Last Theorem, as Ken Ribet showed in 1987 that if the Taniyama-Shimura Conjecture is true, then Fermat's Last Theorem is true. If you are interested in learning more on this recent development, I recommend the following documentary on the Proof of Fermat's Last Theorem, which discusses the Taniyama-Shimura Conjecture and its connection to Fermat's Last Theorem: https://www.dailymotion.com/video/x1btavd.

squares theorem and Theorem 1.1. Euler's plan was to consider the following infinite series

$$\theta(q) = \sum_{n\in\mathbb{Z}} q^{n^2} = 1 + 2q + 2q^4 + 2q^9 + \cdots$$

where $q \in \mathbb{C}$ with $|q| < 1$. Euler then showed the following results:

**Lemma 1.5 — Euler, 1750.** Let $k$ be a positive integer and define

$$r_k(n) = \#\left\{(a_1, a_2, \ldots, a_k) \in \mathbb{Z}^k \mid \sum_{j=1}^{k} a_j^2 = n\right\}.$$

Then $\theta(q)^k = \sum_{n=0}^{\infty} r_k(n)\, q^n$.

*Proof.* This is left as an exercise. ■

Consequently, Theorem 1.1 is equivalent to proving that $r_4(n)$ is a positive integer for each positive integer $n$. While Euler was unable to prove Theorem 1.1 via this methodology, he did simplify Lagrange's proof in 1772. Euler's approach was eventually completed by Carl Gustav Jacob Jacobi, who in 1834 proved that $r_4(n) > 0$ for each positive integer $n$. In fact, he found a closed formula for $r_4(n)$:

**Theorem 1.6 — Jacobi's Four Square Theorem, 1834.** Let $n$ be a nonnegative integer. Then

$$r_4(n) = 8 \sum_{\substack{d \mid n \\ d \not\equiv 0 \bmod 4}} d.$$

■ **Example 1.7** By Theorem 1.6, then $r_4(3) = 8(1+3) = 32$. Indeed, $3 = (\pm 1)^2 + (\pm 1)^2 + (\pm 1)^2 + (0)^2$, and a combinatorial argument now shows that this leads to 32 different ways of writing 3 as a sum of squares. Keep in mind that we mean that there are 32 different 4-tupes $(a_1, a_2, a_3, a_4)$ such that $3 = a_1^2 + a_2^2 + a_3^2 + a_4^2$.

The goal for this course is to prove Theorem 1.6. Doing so will lead us into the realm of modular forms as the crucial ingredient of the proof is that $\theta(q)^4$ is a modular form. To motivate this further, let $n$ be an integer and define

$$\chi_4(n) = \begin{cases} 1 & \text{if } n \equiv 1 \bmod 4, \\ -1 & \text{if } n \equiv 3 \bmod 4, \\ 0 & \text{if } n \text{ is even.} \end{cases}$$

Next, let $\mathbb{H} = \{a + bi \mid a, b \in \mathbb{R}, b > 0\}$ denote the upper half plane and set $q = e^{2\pi i z}$. With this in mind, we define $\theta(z) = \theta(q)$. We will show in a future lesson that if $z \in \mathbb{H}$, then the following infinite series are convergent in a subset of $\mathbb{H}$:

$$\begin{aligned} \mathbb{G}_1(z) &= \frac{1}{4} + \sum_{n=1}^{\infty} \left(\sum_{d\mid n} \chi_4(d)\right) q^n = \frac{1}{4} + q + q^2 + q^4 + 2q^5 + q^8 + \cdots, \\ \mathbb{G}_2(z) &= \frac{-1}{24} + \sum_{n=1}^{\infty} \left(\sum_{d\mid n} d\right) q^n = -\frac{1}{24} + q + 3q^2 + 4q^3 + 7q^4 + \cdots. \end{aligned}$$

Using these series, we define the following $\mathbb{C}$-vector spaces:

$$\begin{aligned} M_1 &= \{a\mathbb{G}_1(z) \mid a \in \mathbb{C}\}, \\ M_2 &= \{a(\mathbb{G}_2(z) - 2\mathbb{G}_2(2z)) + b(\mathbb{G}_2(2z) - 2\mathbb{G}_2(4z)) \mid a,b \in \mathbb{C}\}. \end{aligned}$$

The elements of these vector spaces are examples of modular forms, and in fact, the dimension of $M_j$ as a $\mathbb{C}$-vector space is $j$. Our proof of Theorems 1.4 and 1.1 will rely on showing that $\theta(z)^2 \in M_1$ and $\theta(z)^4 \in M_2$, respectively. The next exercise, will have you use this fact to deduce Theorems 1.4 and 1.1.

**Exercise 1.2** Use the fact that

$$\theta(z)^2 = 4\mathbb{G}_1(z) \qquad \text{and} \qquad \theta(z)^4 = 8(\mathbb{G}_2(z) - 2\mathbb{G}_2(2z)) + 16(\mathbb{G}_2(2z) - 2\mathbb{G}_2(4z)) \quad (1.1)$$

to deduce Theorems 1.4 and 1.1. Specifically, show that

$$r_2(n) = 4\sum_{d|n} \chi_4(d) \qquad \text{and} \qquad r_4(n) = 8 \sum_{\substack{d|n \\ d \not\equiv 0 \bmod 4}} d.$$

Over the next three lessons, we will construct vector spaces of modular forms with the goal of establishing (1.1).

### 1.1.2 Naudé's Question to Euler

Let us return to Euler's observation that the sum of two and four squares is related to studying $\sum_{n\in\mathbb{Z}} q^{n^2}$. For our purposes, we will refer to an infinite series of the form $\sum_{n\in\mathbb{Z}} a_n q^n$ as a (formal) $q$-series with $a_n \in \mathbb{Z}$. The reason for the word formal is that we will not concern ourselves in this lesson with convergence. In fact, the notion of convergence of an infinite series was not established until 1768, when Jean le Rond d'Alembert introduced the comparison tests and the ratio test. That being said, if we take $q \in \mathbb{C}$ with $|q| < 1$, then we will have convergence for the $q$-series considered in this lesson. Euler pioneered the use of $q$-series to answer number-theoretic questions. On September 4, 1740, Philip Naudé the younger wrote to Euler to ask "how many ways can the number 50 be written as a sum of seven different positive integers." Two weeks after receiving Naudé's letter, Euler responded that the answer is 522. Euler went one step further, and gave a method for answer how deducing how many ways a positive integer $n$ can be written as a sum of $m$ different positive integers. He presented his findings on this generalization on April 6, 1741 at the St. Petersburg Academy. However, the publication with the result would not appear until 1751. So how did Euler solve Naudé's question? Euler's approach was to consider the following product:

$$\begin{aligned} \prod_{n=1}^{\infty}(1+q^n x) &= (1+qx)(1+q^2x)(1+q^3x)(1+q^4x)\cdots \qquad (1.2) \\ &= 1 + x(q+q^2+q^3+\cdots) + x^2(q^3+q^4+2q^5+\cdots) + \cdots. \end{aligned}$$

Euler reduced Naudé's question to finding the coefficient of $q^{50}x^7$. To see why this is the case, observe that there are 3 different ways of writing 9 as a sum of 3 distinct positive integers:

$$9 = 1+2+6 = 1+3+5 = 2+3+4.$$

Now observe that the coefficient of $q^9x^3$ in (1.2) is 3 since expanding (1.2) shows that term $q^9x^3$ occurs from multiplying the following terms:

$$q^9x^3 = qx\cdot q^2x\cdot q^6x = qx\cdot q^3x\cdot q^5x = q^2x\cdot q^3x\cdot q^4x.$$

In particular, if $s(n,m)$ denotes the number of ways a nonnegative integer $n$ can be written as a sum of $m$ distinct positive integers, then

$$\prod_{n=1}^{\infty}(1+q^nx) = \sum_{n,m\geq 0} s(n,m)\,q^nx^m.$$

Euler's response to Naudé that $s(50,7) = 522$ relied on the following recursive formula: $s(n,m) = s(n-m,m)+s(n-m,m-1)$. Using this recursive formula, it is not too difficult to deduce Euler's answer.

**Exercise 1.3** Use Euler's recursive formula $s(n,m) = s(n-m,m)+s(n-m,m-1)$ to show that $s(50,7) = 522$.

### 1.1.3 Euler's Pentagonal Number Theorem

Naudé's question led Euler to stumble into the realm of modular forms. Shortly after responding to Naudé, Euler came across the following expansion:

$$\prod_{n=1}^{\infty}(1-q^n) = 1-q-q^2+q^5+q^7-q^{12}-q^{15}+\cdots.$$

After computing the first fifteen or so terms, Euler realized that it appeared that the following equality should hold:

$$\prod_{n=1}^{\infty}(1-q^n) = \sum_{n\in\mathbb{Z}}(-1)^n q^{\frac{n(3n-1)}{2}}.$$

In our study of modular forms, we will see that the left-hand side is closely related to the Dedekind $\eta$-function. On September 15, 1740, Euler corresponded with Daniel Bernoulli to inform him of his conjecture and asked whether he had any idea for establishing the equality. On January 28, 1741, Bernoulli replied, "This can be shown in a most pleasant investigation, together with tranquil pastime and the endurance of pertinacious labor, all three of which I lack." Thankfully, Euler did not lack these three, and he succeeded in proving his conjecture in 1750. In what follows, we establish the necessary tools for proving Euler's Pentagonal Number Theorem. We note that the proof covered here is not the one deduced by Euler, as we use Jacobi's Triple Product Formula, which was established in 1829. To learn more on Euler's work on $q$-series, specifically, his work towards Naudé's problem and the Pentagonal Number Theorem, consult the following references: [Bel10], [San07], [HW07], [Wil08].

In what follows, we will set $\prod_{j=1}^{0}\left(1-q^j\right) = 1$. We will refer to this as an empty product.

**Lemma 1.8 — Euler, 1740.** Let $q \in \mathbb{C}$ such that $|q| < 1$. Then

$$\prod_{n=1}^{\infty}(1+q^n x) = 1 + \sum_{n=1}^{\infty} \frac{q^{\frac{n(n+1)}{2}} x^n}{\prod_{j=1}^{n}(1-q^j)} = \sum_{n=0}^{\infty} \frac{q^{\frac{n(n+1)}{2}} x^n}{\prod_{j=1}^{n}(1-q^j)}.$$

*Proof.* Observe that

$$\begin{aligned}
\sum_{n=0}^{\infty} \frac{q^{\frac{n(n+1)}{2}} x^n}{\prod_{j=1}^{n}(1-q^j)} - \sum_{n=0}^{\infty} \frac{q^{\frac{n(n+1)}{2}} (qx)^n}{\prod_{j=1}^{n}(1-q^j)} &= \sum_{n=0}^{\infty} \frac{q^{\frac{n(n-1)}{2}} q^n \left(x^n - (qx)^n\right)}{\prod_{j=1}^{n}(1-q^j)} \\
&= \sum_{n=0}^{\infty} \frac{q^{\frac{n(n-1)}{2}} (qx)^n (1-q^n)}{\prod_{j=1}^{n}(1-q^j)} \\
&= qx \sum_{n=1}^{\infty} \frac{q^{\frac{n(n-1)}{2}} (qx)^{n-1}}{\prod_{j=1}^{n-1}(1-q^j)} \\
&= qx \sum_{n=0}^{\infty} \frac{q^{\frac{n(n+1)}{2}} (qx)^n}{\prod_{j=1}^{n}(1-q^j)}.
\end{aligned}$$

Consequently,

$$\begin{aligned}
f(x) = \sum_{n=0}^{\infty} \frac{q^{\frac{n(n+1)}{2}} x^n}{\prod_{j=1}^{n}(1-q^j)} &= (1+qx) \sum_{n=0}^{\infty} \frac{q^{\frac{n(n+1)}{2}} (qx)^n}{\prod_{j=1}^{n}(1-q^j)} \\
&= (1+qx) f(qx).
\end{aligned}$$

Iterating this relation yields

$$\begin{aligned}
f(x) &= \prod_{n=1}^{k}(1+q^n x) f\left(q^k x\right) \\
\implies \qquad & \lim_{k\to\infty} \prod_{n=1}^{k}(1+q^n x) f\left(q^k x\right) = \prod_{n=1}^{\infty}(1+q^n x).
\end{aligned}$$

For the last equality, note that

$$\lim_{k\to\infty} f\left(q^k x\right) = \lim_{k\to\infty} \left(1 + q^k \sum_{n=1}^{\infty} \frac{q^{\frac{n(n+1)}{2}} x^n q^{kn-k}}{\prod_{j=1}^{n}(1-q^j)}\right) = 1$$

since $|q| < 1$. ∎

**Corollary 1.9** Let $q \in \mathbb{C}$ such that $|q| < 1$. Then

$$\prod_{n=0}^{\infty}(1+q^n x) = \sum_{n=0}^{\infty} \frac{q^{\frac{n(n-1)}{2}} x^n}{\prod_{j=1}^{n}(1-q^j)}.$$

*Proof.* Let

$$f(x) = \sum_{n=0}^{\infty} \frac{q^{\frac{n(n+1)}{2}} x^n}{\prod_{j=1}^{n}(1-q^j)}.$$

By the proof of Lemma 1.8,

$$\begin{aligned}\sum_{n=0}^{\infty} \frac{q^{\frac{n(n-1)}{2}} x^n}{\prod_{j=1}^{n}(1-q^j)} &= f\left(\frac{x}{q}\right) \\ &= (1+x) f(x) \\ &= (1+x)\prod_{n=1}^{\infty}(1+q^n x) \\ &= \prod_{n=0}^{\infty}(1+q^n x).\end{aligned}$$

■

**Lemma 1.10** Let $q \in \mathbb{C}$ such that $|q| < 1$. Then

$$\prod_{n=0}^{\infty}(1+q^n x)^{-1} = \sum_{n=0}^{\infty} \frac{x^n}{\prod_{j=1}^{n}(q^j-1)}.$$

*Proof.* This is left as an exercise. ■

In our next lesson, we will use the previous results to prove Jocobi's Triple Product. As a consequence of this result, Jacobi attained a simpler proof of Euler's Pentagonal Number Theorem, which we cover below.

**Theorem 1.11 — Jacobi's Triple Product, 1829.** Let $q \in \mathbb{C}$ such that $|q| < 1$. If $x \neq 0$, then

$$\prod_{n=0}^{\infty}\left(1-q^{2n+2}\right)\left(1+q^{2n+1}x\right)\left(1+\frac{q^{2n+1}}{x}\right) = \sum_{n\in\mathbb{Z}} q^{n^2}x^n.$$

**Theorem 1.12 — Euler's Pentagonal Number Theorem, 1750.** Let $q \in \mathbb{C}$ such that $|q| < 1$. Then

$$\prod_{n=1}^{\infty}(1-q^n) = \sum_{n\in\mathbb{Z}} (-1)^n q^{\frac{n(3n-1)}{2}}.$$

*Proof.* Let $f(q,x) = \sum_{n\in\mathbb{Z}} q^{n^2}x^n$. Then by Theorem 1.11,

$$\begin{aligned}
f\left(q^{\frac{3}{2}}, -q^{\frac{-1}{2}}\right) &= \sum_{n\in\mathbb{Z}} (-1)^n q^{\frac{3}{2}n^2} q^{\frac{-n}{2}} \\
&= \sum_{n\in\mathbb{Z}} (-1)^n q^{\frac{n(3n-1)}{2}} \\
&= \prod_{n=0}^{\infty} \left(1-q^{3n+3}\right)\left(1-q^{3n+\frac{3}{2}-\frac{1}{2}}\right)\left(1-q^{3n+\frac{3}{2}+\frac{1}{2}}\right) \\
&= \prod_{n=0}^{\infty} \left(1-q^{3n+3}\right)\left(1-q^{3n+1}\right)\left(1-q^{3n+2}\right) \\
&= \prod_{n=1}^{\infty} \left(1-q^{3n}\right)\left(1-q^{3n-2}\right)\left(1-q^{3n-1}\right) \\
&= \prod_{n=1}^{\infty} (1-q^n).
\end{aligned}$$

■

## 1.2 Modular Forms for $\mathrm{SL}_2(\mathbb{Z})$

The goal of this lesson is to define modular forms over $\mathrm{SL}_2(\mathbb{Z})$. Before this, however, we will finish our discussion of Euler's Pentagonal Theorem.

### 1.2.1 Jacobi's Triple Product

At the end of the last lesson, we proved this result by assuming Jacobi's Triple Product, which Jacobi considered his "most important and fruitful" discovery in mathematics in a letter to Paul Heinrich Fuss in 1828. The Triple Product would appear a year later in Jacobi's book, *Fundamenta nova theoriae functionum ellipticarum* [Jac29]. In this book, Jacobi furthered the ongoing research on elliptic functions and used these to prove his famed triple product. However, the proof that we do below is not based on elliptic functions but on the two lemmas of Euler discussed at the end of our last lesson. While that makes the proof that we will cover was within reach of Euler, the short argument we provide for Jacobi's Triple Product is due to George Andrews [And65] in 1965. If you are interested in reading more on elliptic functions and Jacobi's original proofs, I highly recommend [Roy17], which does a modern faithful reproduction of Jacobi's original arguments through elliptic functions. In fact, elliptic functions are the rightful birthplace of both elliptic curves and modular forms, and while we won't cover these topics in our course, most of the results that we will see got their start in this theory.

**Theorem 2.1 — Jacobi's Triple Product, 1829.** Let $q \in \mathbb{C}$ such that $|q| < 1$. If $x \neq 0$, then

$$\prod_{n=0}^{\infty} \left(1-q^{2n+2}\right)\left(1+q^{2n+1}x\right)\left(1+\frac{q^{2n+1}}{x}\right) = \sum_{n\in\mathbb{Z}} q^{n^2}x^n.$$

*Proof.* Let

$$f(q,x) = \sum_{n=0}^{\infty} \frac{q^{\frac{n(n-1)}{2}}x^n}{\prod_{j=1}^{n}\left(1-q^j\right)} \qquad \text{and} \qquad g(q,x)I = \prod_{j=0}^{\infty}\left(1+q^j x\right).$$

Then Corollary 1.9 states that $f(q,x) = g(q,x)$. Now observe that

$$\begin{aligned}
g\left(q^2,xq\right) &= \sum_{n=0}^{\infty} \frac{q^{n^2}x^n}{\prod_{j=1}^{n}\left(1-q^{2j}\right)} \\
&= \sum_{n=0}^{\infty} \frac{q^{n^2}x^n\prod_{j=0}^{\infty}\left(1-q^{2n+2j+2}\right)}{\prod_{j=1}^{n}\left(1-q^{2j}\right)\prod_{j=n+1}^{\infty}\left(1-q^{2j}\right)} \\
&= \sum_{n=0}^{\infty} q^{n^2}x^n \frac{\prod_{j=0}^{\infty}\left(1-q^{2n+2j+2}\right)}{\prod_{j=0}^{\infty}\left(1-q^{2j+2}\right)} \\
&= \prod_{j=0}^{\infty}\left(1-q^{2j+2}\right)^{-1}\sum_{n=0}^{\infty}\left(q^{n^2}x^n\prod_{j=0}^{\infty}\left(1-q^{2n+2j+2}\right)\right) \\
&= \prod_{j=0}^{\infty}\left(1-q^{2j+2}\right)^{-1}\sum_{n\in\mathbb{Z}}\left(q^{n^2}x^n\prod_{j=0}^{\infty}\left(1-q^{2n+2j+2}\right)\right). \qquad (1.3)
\end{aligned}$$

For the last equality, note that $\prod_{j=0}^{\infty}\left(1-q^{2n+2j+2}\right) = 0$ for $n$ a negative integer. Another application

of Corollary 1.9 yields

$$\begin{aligned} g\left(q^2,-q^{2n+2}\right) &= \prod_{j=0}^{\infty}\left(1-q^{2n+2j+2}\right) \\ &= \sum_{m=0}^{\infty}\frac{(-1)^m q^{m(m-1)}q^{(2n+2)m}}{\prod_{j=1}^{m}\left(1-q^{2j}\right)} \\ &= \sum_{m=0}^{\infty}\frac{(-1)^m q^{m^2+2mn+m}}{\prod_{j=1}^{m}\left(1-q^{2j}\right)}. \end{aligned}$$

Substituting in (1.3) gives

$$\begin{aligned} \sum_{n\in\mathbb{Z}}\left(q^{n^2}x^n\prod_{j=0}^{\infty}\left(1-q^{2n+2j+2}\right)\right) &= \sum_{n\in\mathbb{Z}}\left(q^{n^2}x^n\sum_{m=0}^{\infty}\frac{(-1)^m q^{m^2+2mn+m}}{\prod_{j=1}^{m}\left(1-q^{2j}\right)}\right) \\ &= \sum_{m=0}^{\infty}\left(\frac{(-1)^m q^m}{\prod_{j=1}^{m}\left(1-q^{2j}\right)}\sum_{n\in\mathbb{Z}}q^{(n+m)^2}x^n\right) \\ &= \sum_{m=0}^{\infty}\left(\frac{(-1)^m \left(\frac{q}{x}\right)^m}{\prod_{j=1}^{m}\left(1-q^{2j}\right)}\sum_{n\in\mathbb{Z}}q^{(n+m)^2}x^{n+m}\right) \\ &= \sum_{m=0}^{\infty}\left(\frac{(-1)^m \left(\frac{q}{x}\right)^m}{\prod_{j=1}^{m}\left(1-q^{2j}\right)}\sum_{n\in\mathbb{Z}}q^{n^2}x^n\right). \end{aligned} \tag{1.4}$$

By Lemma 1.10,

$$\begin{aligned} h(q,x) &= \sum_{m=0}^{\infty}\frac{(-1)^m x^m}{\prod_{j=1}^{m}\left(1-q^j\right)} = \prod_{j=0}^{\infty}\left(1+q^j x\right)^{-1} \\ \Longrightarrow \quad h\left(q^2,\frac{q}{x}\right) &= \sum_{m=0}^{\infty}\frac{(-1)^m \left(\frac{q}{x}\right)^m}{\prod_{j=1}^{m}\left(1-q^{2j}\right)} = \prod_{j=0}^{\infty}\left(1+\frac{q^{2j+1}}{x}\right)^{-1}. \end{aligned}$$

Substituting in (1.4) completes the proof since

$$\begin{aligned} \prod_{j=0}^{\infty}\left(1+q^{2j+1}x\right) &= \prod_{j=0}^{\infty}\left(1-q^{2j+2}\right)^{-1}\prod_{j=0}^{\infty}\left(1+\frac{q^{2j+1}}{x}\right)^{-1}\sum_{n\in\mathbb{Z}}q^{n^2}x^n \\ \Longrightarrow \quad \sum_{n\in\mathbb{Z}}q^{n^2}x^n &= \prod_{j=0}^{\infty}\left(1+q^{2j+1}x\right)\left(1-q^{2j+2}\right)\left(1+\frac{q^{2j+1}}{x}\right). \end{aligned}$$

■

In addition to providing a new proof of Euler's Pentagonal Number Theorem, Jacobi used the Triple Product to attain what we call Jacobi's Triangular Number Theorem:

**Theorem 2.2 — Jacobi's Triangular Number Theorem, 1829.** Let $q \in \mathbb{C}$ such that $|q| < 1$. Then

$$\prod_{n=1}^{\infty}\left(1-q^n\right)^3 = \sum_{n=0}^{\infty}(-1)^n(2n+1)q^{\frac{n(n+1)}{2}}.$$

*Proof.* This is left as an exercise. ■

Next, let $n$ be a positive integer and let $p(n)$ denote the number of ways $n$ can be represented as a sum of any positive integers. That is, $p(n)$ denotes the *partitions* of $n$. For instance, $p(5) = 7$ since

$$\begin{aligned} 5 &= 1+1+1+1+1 = 1+1+1+2 = 1+1+3 \\ &= 1+4 = 2+3 = 2+2+1 = 3+1+1. \end{aligned}$$

Next, set $p(0) = 1$. Is it possible to find a formula for $p(n)$? This was a question that Leibniz's posed to Johann Bernoulli. While Johann was unable to answer Leibniz question, his former doctoral student, Euler, would provide the first such formula for computing $p(n)$. In fact, Euler presented his formula in 1741 at the St. Petersburg Academy along with his solution to Naudé's question. For homework, you will be tasked with proving this result of Euler, which reduces the finding of $p(n)$ to computing the coefficient of $q^n$ in the expansion $\prod_{n=1}^{\infty}(1-q^n)^{-1}$.

**Theorem 2.3 — Euler's Theorem on Partitions, 1740.** Let $q \in \mathbb{C}$ such that $|q| < 1$. Then

$$\prod_{n=1}^{\infty}(1-q^n)^{-1} = \sum_{n=0}^{\infty} p(n)\,q^n.$$

*Proof.* This is left as an exercise. ■

Consequently, we have the following corollary:

**Corollary 2.4** Let $q \in \mathbb{C}$ such that $|q| < 1$. Then

$$\left(\sum_{n\in\mathbb{Z}} (-1)^n q^{\frac{n(3n-1)}{2}}\right)\left(\sum_{n=0}^{\infty} p(n)\,q^n\right) = 1.$$

*Proof.* By Theorems 1.12 and 2.3,

$$\left(\sum_{n\in\mathbb{Z}} (-1)^n q^{\frac{n(3n-1)}{2}}\right)\left(\sum_{n=0}^{\infty} p(n)\,q^n\right) = \prod_{n=1}^{\infty}(1-q^n)\prod_{n=1}^{\infty}(1-q^n)^{-1} = 1.$$

■

### 1.2.2 Analytic Functions

We now transition towards defining modular forms. To this end, we need to briefly review functions over the complex numbers and their properties.

**Definition 2.5** Let $D \subseteq \mathbb{C}$ be an open set. We say a function $f : D \to \mathbb{C}$ is **holomorphic at the point** $z_0 \in D$ if

$$\lim_{h\to 0} \frac{f(z_0+h)-f(z_0)}{h}$$

converges. Here $h \in \mathbb{C}$ and $h \neq 0$ with $z_0 + h \in D$. If $f$ is *holomorphic* at $z_0$, we let

$$f'(z_0) = \lim_{h\to 0} \frac{f(z_0+h)-f(z_0)}{h}$$

and call it the *derivative* of $f$ at $z_0$. We say $f$ is **holomorphic** on $D$ if $f$ is *holomorphic* at every point of $D$.

What if we were to view a holomorphic function $f : D \to \mathbb{C}$ as a function from $\mathbb{R}^2 \to \mathbb{R}^2$? Specifically, write $z = x + iy$ for $x$ and $y$ real variables and $f(x) = \operatorname{Re} f(z) + i \operatorname{Im} f(z)$. Then we can view $f$ as a function $f : \mathbb{R}^2 \to \mathbb{R}^2$ defined by $f\,(x,y) = (\operatorname{Re} f(z), \operatorname{Im} f(z))$. From this perspective, Bernhard Riemann [BG13] discovered in his doctoral dissertation (1851) an important relationship between $\operatorname{Re} f(z)$ and $\operatorname{Im} f(z)$:

**Lemma 2.6 — The Cauchy-Riemann Equations, 1851.** Let $D \subseteq \mathbb{C}$ be an open set and let $z = x + iy$ where $x$ and $y$ denote the real and imaginary parts of $z$, respectively. If $f : D \to \mathbb{C}$ defined by $f(z) = u(x,y) + iv(x,y)$ is a holomorphic function, then the partial derivative of $u$ and $v$ satisfy the **Cauchy-Riemann equations** at each point in $D$:

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y} \qquad \text{and} \qquad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}.$$

*Proof.* This is left as an exercise. ■

Working independently from Riemann, Cauchy discovered the Cauchy-Riemann Equations in 1851 as well! While the Cauchy-Riemann equations can be attained as a special case of a work of Cauchy in 1814, he did not explicitly write these formulas down. In fact, starting in 1851, he began to reformulate many of his earlier results by adhering to the Cauchy-Riemann Equations.

What of the converse of the Cauchy-Riemann equations? Riemann incorrectly assumed that it held but did not pursue a proof of this result. In the years that followed, partial converses were proven, culminating with the work of Herman Looman and Dmitrii Menshov:

**Theorem 2.7 — The Looman-Menshov Theorem, 1923, 1936.** Let $D \subseteq \mathbb{C}$ be an open set and let $z = x + iy$ where $x$ and $y$ denote the real and imaginary parts of $z$, respectively. Let $f : D \to \mathbb{C}$ defined by $f(z) = u(x,y) + iv(x,y)$ be a continuous function. If the partial derivatives $\frac{\partial u}{\partial x}, \frac{\partial v}{\partial y}, \frac{\partial u}{\partial y}, -\frac{\partial v}{\partial x}$ exist and satisfy the Cauchy-Riemann Equations at each point in $D$, then $f$ is holomorphic on $D$.

**Definition 2.8** Let $D \subseteq \mathbb{C}$ be an open set. We say $f$ is **analytic at a point** $z_0 \in D$ if there exists a power series $\sum_{n=0}^{\infty} a_n (z - z_0)^n$ centered at $z_0$, with a positive radius of convergence, such that there exists an open set $D' \subseteq D$ with $z_0 \in D'$ and

$$f(z) = \sum_{n=0}^{\infty} a_n (z - z_0)^n$$

for all $z \in D'$. If $f$ has a power series expansion at every point in $D$, we say that $f$ is analytic on $D$.

In this course, we will assume the following theorem, which is proven in a complex analysis course:

**Theorem 2.9 — Cauchy, 1821.** Let $D \subseteq \mathbb{C}$ be an open set. Then $f$ is holomorphic on $D$ if and only if $f$ is analytic on $D$.

R This result of Cauchy settled a century-long conjecture at the time! Following Taylor's Theorem (1715), it was conjectured that every function could be represented by a Taylor series expansion about every point in its domain. The belief was so prevalent that in 1797, Lagrange sought to redo all of calculus with infinite series rather than with functions such as $\tan^{-1}x$ or $\sin x$. Cauchy's Theorem showed that the conjecture held if $f$ is holomorphic. However, Cauchy showed in 1823 that the theorem could not be extended to real-differentiable functions as demonstrated by his counterexample:

$$f(x) = \begin{cases} e^{-1/x^2} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

is infinitely differentiable yet has no power series expansion about 0. To make matters worse, there are infinitely many real-differentiable functions whose domain is the set of all real numbers but do not have a power series expansion about any point in their domain.

Next, let $\mathcal{H} = \{a+bi \in \mathbb{C} \mid a,b \in \mathbb{R}, b>0\} = \{z \in \mathbb{C} \mid \mathrm{Im}\, z > 0\}$ denote the *upper half plane*.

**Lemma 2.10** Let $D' = \{z \in \mathbb{C} \mid |z| < 1\} - \{0\}$ be the punctured unit disk.. Then $q : \mathcal{H} \to D'$ defined by $q(z) = e^{2\pi iz}$ is a surjective holomorphic function.

*Proof.* We show that $q$ is a surjective function, and leave that $q$ is holomorphic as an exercise. Let $z = x+yi$ with $x,y \in \mathbb{R}$. We first show that $f(D') \subseteq D'$. To this end, observe that

$$q(z) = e^{2\pi iz} = e^{2\pi i(x+yi)} = e^{-2y\pi}e^{2x\pi i} = e^{-2\pi y}\left(\cos 2x\pi + i \sin 2x\pi\right).$$

Since $y > 0$, we have that $\left|e^{-2\pi y}\right| < 1$ and thus $f(\mathcal{H}) \subseteq D'$. Let $z \in D'$, then $z = re^{i\theta}$ for some positive real number $r < 1$ and $0 \leq \theta < 2\pi$. Next, set $a = \frac{\theta}{2\pi}$ $b = \frac{-\log r}{2\pi}$. Then $q(x+yi) = re^{i\theta}$. ■

### 1.2.3 The Modular Group

Now that we have defined what it means to be holomorphic, we are ready to define modular forms! To this end, we will rely on the results covered in your first lesson with Dr. Watson, namely the modular group $\mathrm{SL}_2(\mathbb{Z})$. While the modular group can be deduced from Lagrange's 1775 work on quadratic forms, it would take a century until it was explicitly defined in the mathematics literature by Richard Dedekind in 1877. We define the *modular group* $\mathrm{SL}_2(\mathbb{Z})$ to be the group of invertible $2 \times 2$ matrices with integer entries and determinant 1. That is,

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in D,\ ad-bc = 1 \right\}.$$

The modular group is generated by the matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Next, let $\mathcal{H} = \{a+bi \in \mathbb{C} \mid a,b \in \mathbb{R}, b>0\}$ denotes *upper half plane*. In your problem set, you saw that $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{H}$ by *fractional linear transformations*:

$$\begin{array}{rcl} \mathrm{SL}_2(\mathbb{Z}) \times \mathcal{H} & \longrightarrow & \mathcal{H} \\ \gamma\tau = (\gamma, z) & \longmapsto & \dfrac{a\tau+b}{c\tau+d} \qquad \text{where } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \end{array}$$

It is standard to abuse notation and write $\gamma\tau$, where it is understood that if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathcal{H}$, then $\gamma\tau = \frac{a\tau+b}{c\tau+d} \in \mathcal{H}$.

### 1.2.4 Modular Forms for $\mathrm{SL}_2(\mathbb{Z})$

At first glance, our discussion of modular groups bears no resemblance to Euler and Jacobi's results in the last lesson and at the start of this lesson. Jacobi's work concerned itself with elliptic functions, which gave rise to the theory of modular forms. Dedekind and Felix Klein put forward the modern theory of modular forms. Their contribution shined a new light on the existing literature by uncovering the connection to the modular group and focusing on some of its subgroups of finite index. With this in mind, we now begin our coverage of modular forms, and our coverage follows [DS05].

**Definition 2.11** Let $k$ be an integer and let $f : \mathcal{H} \to \mathbb{C}$ be a holomorphic function. We say that $f$ satisfies the **modularity condition with weight $k$ for** $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ if

$$f(\gamma\tau) = (c\tau + d)^k f(\tau) \tag{1.5}$$

for each $\tau \in \mathcal{H}$.

**Lemma 2.12** Let $k$ be an integer. If $f : \mathcal{H} \to \mathbb{C}$ is a holomorphic function which satisfies the modularity condition with weight $k$ for each $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, then there exists a holomorphic function $g : D' \to \mathbb{C}$ such that $f(\tau) = g(q(\tau))$.

Moreover, if $\lim_{\mathrm{Im}\,\tau\to\infty} f(\tau)$ exists, then $g$ can be extended to a holomorphic function $g : D \to \mathbb{C}$. In particular, $g$ has a Taylor series about 0 with

$$g(q) = \sum_{n=0}^{\infty} a_n q^n$$

for each $q \in D$.

*Proof.* Since $f$ satisfies the modularity condition with weight $k$ for $T$, we have that $f(T\tau) = f(\tau+1) = f(\tau)$. Consequently, if $W = \left\{z \in \mathcal{H} \mid -\frac{1}{2} < \mathrm{Re}\,\tau \leq \frac{1}{2}\right\}$, then $f(W) = f(\mathcal{H})$. Now define $h : D' \to W$ by $h\left(re^{i\theta}\right) = \frac{\log r + i\theta}{2\pi i}$ with $-\pi < \theta \leq \pi$. Then if $\tau = x + iy \in W$ with $x, y \in \mathbb{R}$, then

$$\begin{aligned} h(q(\tau)) &= h\left(e^{-2\pi y}e^{2\pi xi}\right) = \frac{\log e^{-2\pi y} + 2\pi xi}{2\pi i} = \frac{-2\pi y + 2\pi xi}{2\pi i} = x + iy, \\ q\left(h\left(re^{i\theta}\right)\right) &= q\left(\frac{\log r + i\theta}{2\pi i}\right) = e^{-2\pi\left(\frac{\theta}{2\pi i}\right)} e^{2\pi i\left(\frac{\log r}{2\pi i}\right)} = re^{i\theta}. \end{aligned}$$

In particular, $h$ is the inverse function of $q|_W : W \to D'$. Now set $g = f \circ h$. By construction,

$$f(\tau) = g(q(\tau))$$

and we leave it as an exercise to show that this implies that $g$ is holomorphic for each $z \in D'$.

Next, observe that $\lim_{\mathrm{Im}\,\tau\to\infty} q(\tau) = 0$. Thus, if $\lim_{\mathrm{Im}\,\tau\to\infty} f(\tau)$ exists, then we can define

$$\lim_{\mathrm{Im}\,\tau\to\infty} f(\tau) = g\left(\lim_{\mathrm{Im}\,\tau\to\infty} q(\tau)\right) = g(0).$$

Then an application of Riemann's Removable Singularity Theorem shows that $g : D \to \mathbb{C}$ is a holomorphic function and has a Taylor series expansion about 0:

$$g(q) = \sum_{n=0}^{\infty} a_n q^n.$$

In fact, since $g$ is analytic on $D$, we have by a consequence of the Cauchy integral formula that taking $q = e^{2\pi i\tau}$ for $\tau \in \mathcal{H}$ leads to the Fourier expansion of $f$:

$$f(\tau) = \sum_{n=0}^{\infty} a_n q^n.$$

■

**Definition 2.13** Let $k$ be an integer and $f : \mathcal{H} \to \mathbb{C}$ be a holomorphic function which satisfies the modularity condition with weight $k$ for each $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. If $\lim_{\mathrm{Im}\,\tau\to\infty} f(\tau)$ exists, then we say that $f$ is **holomorphic at** $\infty$. In particular, and $f$ has a **Fourier expansion** (or **q-expansion**)

$$f(\tau) = \sum_{n=0}^{\infty} a_n q^n.$$

**Definition 2.14** Let $k$ be an integer. A holomorphic function $f : \mathcal{H} \to \mathbb{C}$ is said to be a **modular form of weight** $k$ **for** $\mathrm{SL}_2(\mathbb{Z})$ if $f$ is holomorphic at $\infty$ and $f$ satisfies the modularity condition with weight $k$. The set of modular forms of weight of weight $k$ with respect to $\mathrm{SL}_2(\mathbb{Z})$ is denoted $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$.

**Definition 2.15** A **cusp form** $f$ **of weight** $k$ **for** $\mathrm{SL}_2(\mathbb{Z})$ is a modular form of weight $k$ for $\mathrm{SL}_2(\mathbb{Z})$ whose Fourier expansion has leading coefficient $a_0 = 0$, i.e.,

$$f(\tau) = \sum_{n=1}^{\infty} a_n q^n.$$

The set of cusp forms is denoted $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$.

**Exercise 2.1** (1) $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ and $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$ are $\mathbb{C}$-vector spaces;
(2) $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z})) = \{0\}$ if $k$ is odd;
(3) If $f \in \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ and $g \in \mathcal{M}_l(\mathrm{SL}_2(\mathbb{Z}))$, then $fg \in \mathcal{M}_{k+l}(\mathrm{SL}_2(\mathbb{Z}))$;
(4) If $f \in \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ and $g \in \mathcal{S}_l(\mathrm{SL}_2(\mathbb{Z}))$, then $fg \in \mathcal{S}_{k+l}(\mathrm{SL}_2(\mathbb{Z}))$.
(5) $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z})) = \bigoplus_{k\in\mathbb{Z}} \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ is a ring;
(6) $\mathcal{S}(\mathrm{SL}_2(\mathbb{Z})) = \bigoplus_{k\in\mathbb{Z}} \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$ is an ideal of the ring $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))$.

*Proof.* This is left as an exercise. ■

R For those of you who have taken commutative algebra, observe that the lemma shows that $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))$ is a graded ring and $\mathcal{S}(\mathrm{SL}_2(\mathbb{Z}))$ is a graded ideal.

**Lemma 2.16** Let $k$ be an integer and let $\gamma, \delta \in \mathrm{SL}_2(\mathbb{Z})$. If $f : \mathcal{H} \to \mathbb{C}$ is a holomorphic function such that $f$ satisfies the modularity condition with weight $k$ for $\gamma$ and $\delta$. Then $f$ satisfies the modularity condition with weight $k$ for $\gamma\delta$ and $\gamma^{-1}$.

*Proof.* Let $\gamma = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ and $\delta = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$. Then $\gamma\delta = \begin{pmatrix} a_1a_2+b_1c_2 & a_1b_2+b_1d_2 \\ a_2c_1+c_2d_1 & b_2c_1+d_1d_2 \end{pmatrix}$ and $\gamma^{-1} = \begin{pmatrix} d_1 & -b_1 \\ -c_1 & a_1 \end{pmatrix}$. By assumption, $f(\gamma\tau) = (c_1+d_1)^k f(\tau)$ and $f(\delta\tau) = (c_2+d_2)^k f(\tau)$ for each $\tau \in \mathcal{H}$. Now observe that for $\tau \in \mathcal{H}$,

$$\begin{aligned} f(\tau) &= f\big(\gamma\big(\gamma^{-1}\tau\big)\big) = \big(c_1\gamma^{-1}\tau + d_1\big)^k f\big(\gamma^{-1}\tau\big) \\ \implies \quad f\big(\gamma^{-1}\tau\big) &= \big(c_1\gamma^{-1}\tau + d_1\big)^{-k} f(\tau) \\ &= \left(c_1\frac{d_1\tau - b_1}{-c_1\tau + a_1} + d_1\right)^{-k} f(\tau) \\ &= \left(\frac{a_1d_1 - b_1c_1}{-c_1\tau + a_1}\right)^{-k} f(\tau) \\ &= (-c_1\tau + a_1)^k f(\tau). \end{aligned}$$

Similarly, we have that for each $\tau \in \mathcal{H}$,

$$\begin{aligned} f((\gamma\delta)\,\tau) &= f(\gamma(\delta\tau)) \\ &= (c_1\delta\tau + d_1)^k f(\delta\tau) \\ &= \left(c_1\left(\frac{a_2\tau + b_2}{c_2\tau + d_2}\right) + d_1\right)^k (c_2\tau + d_2)^k f(\tau) \\ &= \left(\frac{\tau(a_2c_1 + c_2d_1) + b_2c_1 + d_1d_2}{c_2\tau + d_2}\right)^k (c_2\tau + d_2)^k f(\tau) \\ &= (\tau(a_2c_1 + c_2d_1) + b_2c_1 + d_1d_2)^k f(\tau). \end{aligned}$$

■

**Corollary 2.17** Let $f : \mathcal{H} \to \mathbb{C}$ be a holomorphic function which is holomorphic at $\infty$. Suppose further that $f(\tau+1) = f(\tau)$ and $f\left(\frac{-1}{\tau}\right) = \tau^k f(\tau)$ for each $\tau \in \mathcal{H}$. Then $f$ is a modular form of weight $k$ for $\mathrm{SL}_2(\mathbb{Z})$.

*Proof.* This is left as an exercise. ■

## 1.3 Lesson 3

## 1.4 Lesson 4

## 1.5 Lesson 5

## 1.6 Lesson 6

## 1.7 Appendix

### 1.7.1 Fermat's Only Known Proof

Only one of Fermat's has survived, namely his proof of the Right Triangle Theorem. From it, the $n = 4$ case of Fermat's Last Theorem follows, and for this reason, Fermat is credited with having proved the $n = 4$ case of Fermat's Last Theorem. The proof of the Right Triangle Theorem employs Fermat's method of infinite descent, which was used by Euler in his proof of Fermat's Sum of Two Squares Theorem. Fermat was extremely proud of his use of *infinite descent* and described it in various correspondences, including the letter to Mersenne. This is summarized in the following quote from Edwards's *Fermat's Last Theorem* [Edw77]:

> "Fermat invented the method of infinite descent and it was an invention of which he was extremely proud. In a long letter written toward the end of his life he summarized his discoveries in number theory and he stated very definitely that all of his proofs used this method. Briefly put, the method proves that certain properties or relations are impossible for [natural] numbers by proving that if they held for any numbers they would hold for some smaller numbers; then, by the same argument, they would hold for some numbers that were smaller still, and so forth ad infinitum, which is impossible because a sequence of [natural] numbers cannot decrease indefinitely."

Fermat's proof of the $n = 4$ case of Fermat's Last Theorem relies on the following result (which Fermat stated and proved in the margin of his copy of Arithmetica! It is also the only proof of Fermat that survived!):

**Theorem 7.1 — Fermat's Right Triangle Theorem, 1641.** The area of a right triangle with integer sides cannot be a perfect square.

*Proof.* The following is a translation of Fermat's proof as found in the margin of his copy of *Arithmetica*:

"If the area of a right-angled triangle were a square, there would exist two biquadrates[2] the difference of which would be a square number. Consequently there would exist two square numbers the sum and difference of which would both be squares. Therefore we should have a square number which would be equal to the sum of a square and the double of another square, while the squares of which this sum is made up would themselves have a square number for their sum. But if a square is made up of a square and the double of another square, its side, as I can very easily prove, is also similarly made up of a square and the double of another square. From this we conclude that the said side is the sum of the sides about the right angle in a right-angled triangle, and that the simple square contained in the sum is the base and the double of the other square is the perpendicular.

This right-angled triangle will thus be formed from two squares, the sum and differences of which will be squares. But both these squares can be shown to be smaller than the squares originally assumed to be such that both their sum and difference are squares. Thus if there exist two squares such that their sum and difference are both squares, there will also exist two other integer squares which have the same property but have a smaller sum. By the same reasoning we find a sum still smaller than that last found, and we can go on ad infinitum finding integer square numbers smaller

[2] A **biquadrate** is a perfect fourth power. For instance, 16 and 81 are biquadrates.

and smaller which have the same property. This is, however, impossible because there cannot be an infinite series of numbers smaller than any given integer we please. The margin is too small to enable me to give the proof completely and with all detail."[3] ■

**Theorem 7.2 — The $n = 4$ Case of Fermat's Last Theorem, 1641.** There do not exist natural numbers $x, y$, and $z$ such that $x^4 + y^4 = z^4$.

*Proof.* Towards a contradiction, suppose there are natural numbers $x, y, z$ satisfying $x^4 + y^4 = z^4$. We may assume $x, y, z$ are relatively prime. Indeed, if $d$ is the greatest common divisor of $x, y, z$, then

$$\left(\frac{x^2}{d^2}\right)^2 + \left(\frac{y^2}{d^2}\right)^2 = \left(\frac{z^2}{d^2}\right)^2.$$

Since $\frac{x}{d}, \frac{y}{d}, \frac{z}{d}$ are relatively prime, we may change our $x, y, z$ if necessary so that we can assume that $x, y, z$ are relatively prime natural numbers such that $x^4 + y^4 = z^4$. In particular, $\left(x^2, y^2, z^2\right)$ is a primitive Pythagorean triple. After a possible reordering of $x$ and $y$, we may assume by Diophantus's classification of Pythagorean Triples that

$$x^2 = 2pq \qquad y^2 = p^2 - q^2 \qquad z^2 = p^2 + q^2 \tag{1.6}$$

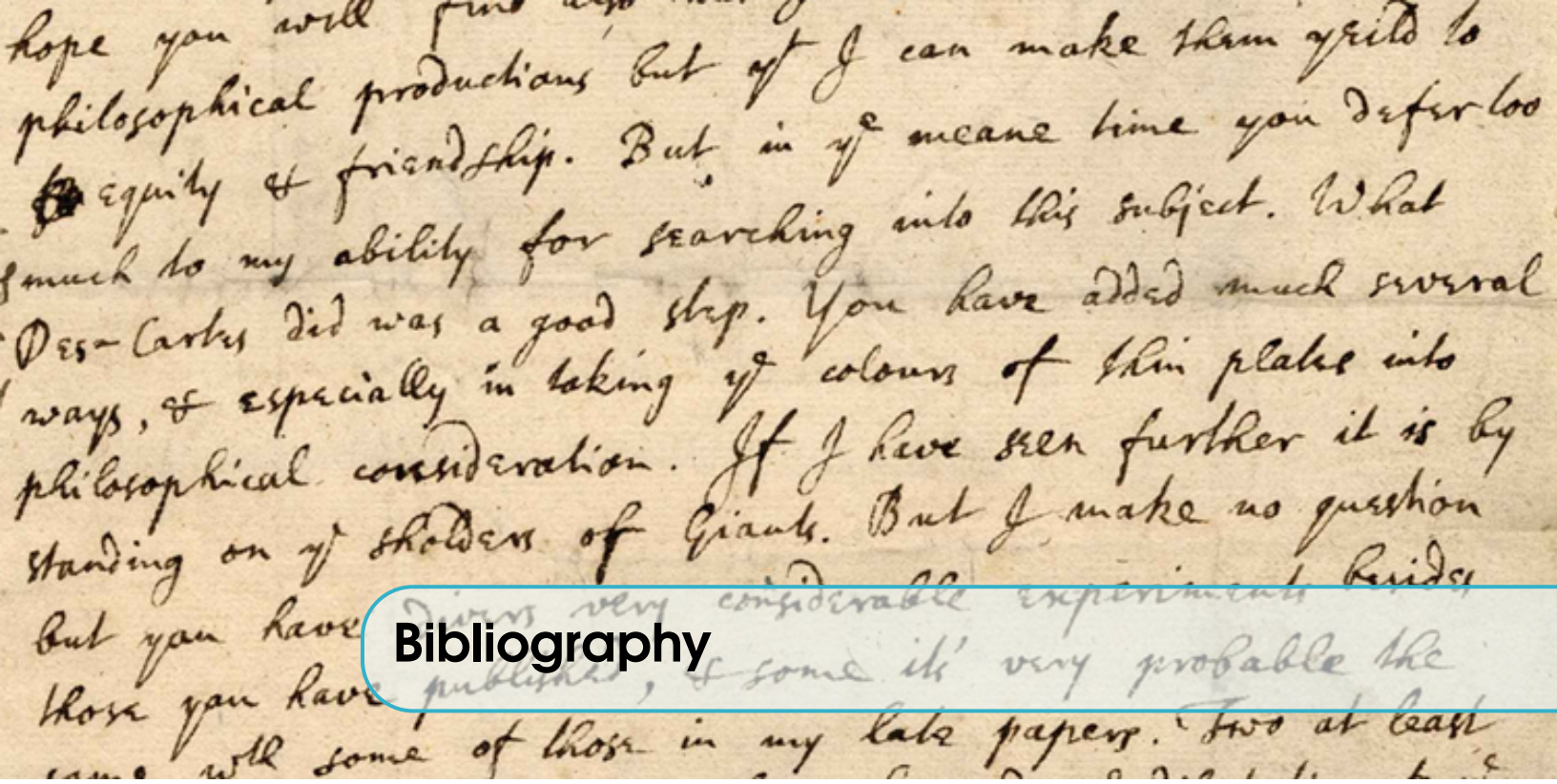
for some relatively prime natural numbers $p$ and $q$ of opposite parity such that $p > q$. Since $(p, q, z)$ is a Pythagorean triple, we have a right triangle with integer sides $p, q, z$. Since $z$ is the hypotenuse, we have that the area $A$ of this triangle is

$$A = \frac{pq}{2} = \left(\frac{\frac{x^2}{2}}{2}\right) = \left(\frac{x}{2}\right)^2 \qquad \text{by (1.6)}.$$

This is our desired contradiction, the area of the triangle is a perfect square, which contradicts Theorem 7.1. ■

$\mathcal{S}$

[3] Even in his only proof, the margin was too small for him to include all the details.



# Bibliography


[And65] George E. Andrews, *A simple proof of Jacobi's triple product identity*, Proc. Amer. Math. Soc. **16** (1965), 333–334. MR 171725

[Bel10] Jordan Bell, *A summary of Euler's work on the pentagonal number theorem*, Arch. Hist. Exact Sci. **64** (2010), no. 3, 301–373. MR 2651525

[BG13] Umberto Bottazzini and Jeremy Gray, *Hidden harmony—geometric fantasies*, Sources and Studies in the History of Mathematics and Physical Sciences, Springer, New York, 2013, The rise of complex function theory. MR 3099398

[Cox13] David A. Cox, *Primes of the form $x^2 + ny^2$*, second ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013, Fermat, class field theory, and complex multiplication. MR 3236783

[DS05] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005. MR 2112196

[Edw77] Harold M. Edwards, *Fermat's last theorem*, Graduate Texts in Mathematics, vol. 50, Springer-Verlag, New York-Berlin, 1977, A genetic introduction to algebraic number theory. MR 616635

[HW07] Brian Hopkins and Robin Wilson, *Euler's science of combinations*, Leonhard Euler: life, work and legacy, Stud. Hist. Philos. Math., vol. 5, Elsevier, Amsterdam, 2007, pp. 395–408. MR 3890500

[Jac29] Carl Gustav Jacob Jacobi, *Fundamenta nova theoriae functionum ellipticarum*, Borntraeger, 1829.

[Roy17] Ranjan Roy, *Elliptic and modular functions from Gauss to Dedekind to Hecke*, Cambridge University Press, Cambridge, 2017. MR 3702031

[San07] C. Edward Sandifer, *How Euler did it*, MAA Spectrum, Mathematical Association of America, Washington, DC, 2007. MR 2321397

[Wil08] Robin Wilson, *Euler's combinatorial mathematics*, BSHM Bull. **23** (2008), no. 1, 13–23. MR 2394576