MODULAR FORMS LECTURE 1: INTRODUCTION AND MOTIVATING EXAMPLES

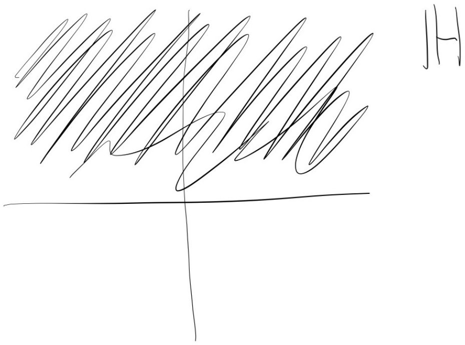
LARRY ROLEN, VANDERBILT UNIVERSITY, FALL 2020

> Modular forms are everywhere.
>
> Don Zagier

Before diving into the general theory of modular forms, let's first ask a basic question: what **is** a modular form? There are many possible answers to this question depending on how technical you want to be.

Modular forms are functions which live on the **upper half plane**,

$$\mathbb{H} := \{\tau \in \mathbb{C} : \Im(\tau) > 0\}.$$



Convention. $\tau =: u + iv$ where $u, v \in \mathbb{R}$.

Definition. The **modular group** is $\Gamma = \mathrm{SL}_2(\mathbb{Z}) := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : a, b, c, d \in \mathbb{Z},\ ad - bc = 1\}$.

There is a special group action

$$\mathrm{SL}_2(\mathbb{Z}) \circlearrowleft \mathbb{H}$$

given by **Möbius transformations** (fractional linear transformations):

$$\gamma \cdot \tau := \frac{a\tau + b}{c\tau + d},$$

where $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$.

Exercise 1. *Show that this is indeed a group action. That is, show that*

(1) *If $\tau \in \mathbb{H}$ and $\gamma \in \Gamma$, then $\gamma \cdot \tau \in \mathbb{H}$.*
(2) *$I_2 \cdot \tau = \tau$ for all $\tau \in \mathbb{H}$, where I_2 is the identity matrix.*

(3) $\gamma_1 \cdot (\gamma_2 \cdot \tau) = (\gamma_1\gamma_2) \cdot \tau$ *for all* $\gamma_1, \gamma_2 \in \Gamma$ *and all* $\tau \in \mathbb{H}$.

We are now ready to give our first approximation of what modular forms are.

"Definition". *A* **modular form of weight** k *is a function* $f\colon \mathbb{H} \to \mathbb{C}$ *such that the following hold.*

(1) *For all* $\gamma \in \Gamma, \tau \in \mathbb{H}$, *we have the* **modularity transformation**

$$f(\gamma \cdot \tau) = (c\tau + d)^k f(\tau).$$

(2) $f(\tau)$ *has nice analytic conditions (for example, holomorphic, meromorphic, or real-analytic).*

(3) $f(\tau)$ *has nice growth conditions as* $\tau \to i\infty$ *along the imaginary axis.*

Remarks. (1) *This seems like a strange definition! We will see more later about where this comes from, but for now we'll take a leap of faith that it is useful.*

(2) *Condition (1) is the most important symmetry property of modular forms; (2) and (3) can change depending on context. This flexibility gives modular form theory a lot of power. As Martin Raum once quipped, there is a "free group" of adjectives that can be put before the word modular; indeed, these adjectives aren't always commutative! E.g., nearly, quasi, almost, weakly, mock, false, partial. . . .*

Thus modular forms are functions with infinitely many symmetries. As Mazur said, they have so many symmetries they seem like they might not exist, but they do.

Exercise 2. *Show that the set of modular forms of weight k (with any reasonable choice of "nice" in (2) and (3)) is a* **vector space**.

One of the ways you can think about Mazur's summary is that most spaces of functions are infinite dimensional, but nice spaces of modular forms are finite dimensional. So the infinitely many symmetries are restrictive enough to cut down spaces to finite dimensional situations, but not so much so that the spaces are empty. A lot of the beautiful number theory arises from this finite dimensionality, as identities and rationality pop up from this.

Example. *The matrix* $S := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ *gives the modular relation*

$$f\left(-\frac{1}{\tau}\right) = \tau^k f(\tau).$$

This transformation is called **inversion**.

The matrix $T := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ *gives the modular relation*

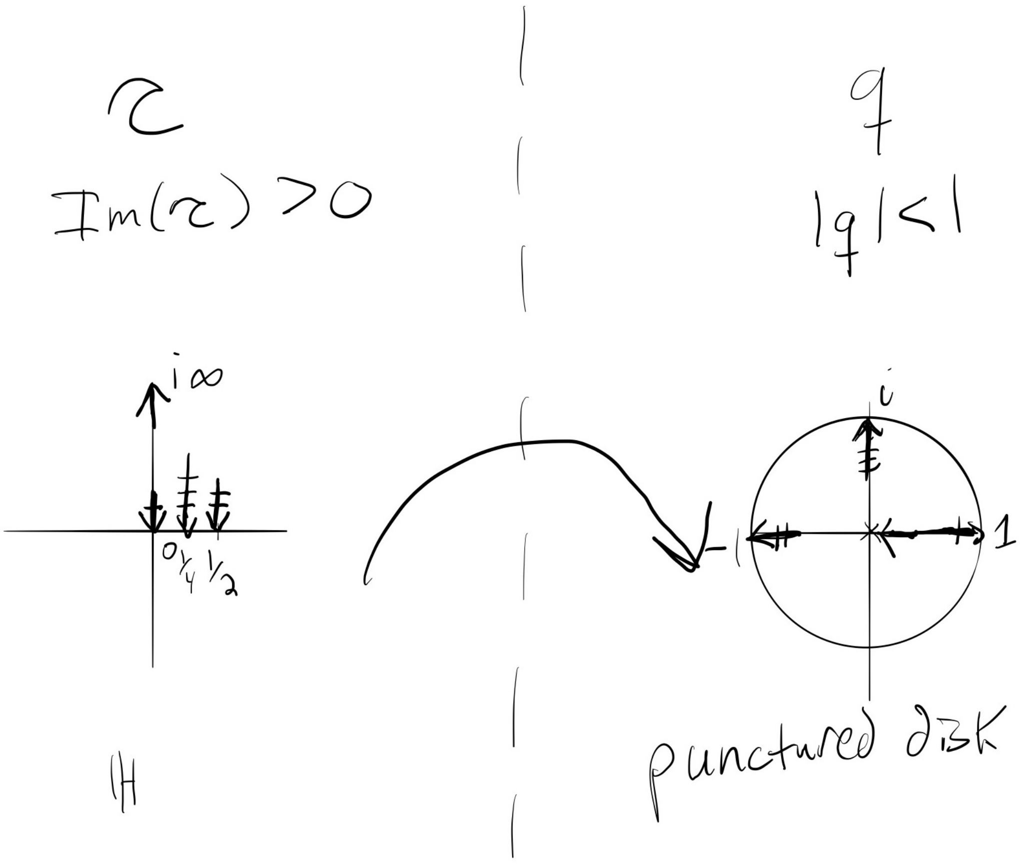
$$f(\tau + 1) = f(\tau).$$

Thus modular forms are **translation invariant**.

From complex analysis, we have that "nice" functions satisfying $f(\tau+1) = f(\tau)$ have **Fourier expansions** in terms of

$$q := e^{2\pi i\tau}.$$

If you have seen Fourier series using sines and cosines, think of this as a complexified version. We will frequently move back and forth between the τ and q perspectives, so its useful to look at what this change of variables does to the upper half plane.



The existence of Fourier series gives the connection to many applications. It turns out that many interesting sequences of numbers, when you stick them in a generating function, are, or nearly are, coefficients of modular forms.

I want to conclude the intro with a whirlwind tour of a few notable applications of modular forms. These are only for illustrative purposes, so if you don't understand the details of these (and you likely won't until we are much further in the class), just take them as motivating examples.

Example (Divisor sums)**.** *Let* $\sigma_k(n) := \sum_{d|n} d^k$*. We will give an "easy" (one line) proof of the following identity:*

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{0<k<n} \sigma_3(k)\sigma_3(n-k).$$

By taking generating functions of the generating functions (using two variable modular objects), we can even prove an infinite family of these identities all at once! As Don Zagier likes to say, if you have a sequence you want to study, its always best to stick things into a generating function, whether those be numbers or functions themselves!

Example (Representations of integers by sums of squares)**.** *Let* $r_k(n)$ *be the number of ways to write* n *as a sum of* k *squares of integers. Most elementary number theory classes prove the following.*

Theorem (Lagrange)**.** *For all* $n \in \mathbb{N}$*, we have* $r_4(n) > 0$*.*

Modular forms show much more. In fact, we have

$$r_4(n) = 8\sigma_1(n) - 32\sigma_1(n/4).$$

(N.B.: Whenever I write a fraction inside of a function only defined on integers, I always mean that it takes the value zero if the argument isn't an integer). Again, the proof of this refined version of Lagrange's Theorem is only 1 line using modular forms, or a really trivial computer check!

Example (Representation theory)**.** *(Linear combinations of) dimensions of irreducible representations of the* **Monster group** *are counted by a weight* 0 *modular form. This is the theory of Monstrous Moonshine, so-called by Conway as you'd have to be drinking moonshine to conjecture something so crazy (in the general English sense, moonshine means a crackpot theory). This arose as a series of strange "coincidences", such as McKay's observation that* $196884 = 196883 + 1$*, leading to Borcherds proof of what was going on, for which he won the Fields Medal.*

Example (Physics)**.** *Many counting functions in physics, especially string theory are related to modularity. These often involve exotic modular forms and provide inspiration to the number theorists as well. For instance, in mirror symmetry, modular transformations arise naturally. A lot of the time, modular symmetry doesn't have to be exactly satisfied in the physics applications, but only nearly. For instance, if you have a function defined on a certain space, and want to extend it to a larger space, you can use symmetry to do so. If you know what modular transformations do up to something else explicit enough to write down, that may be good enough.*

Example (Combinatorics)**.** *Many, many combinatorial functions have modular properties. For instance, we have* **integer partitions***.*

Definition. The partition function $p(n)$ counts the number of ways to write n as a sum of natural numbers.

For instance, $p(4) = 5$ *as the ways are:*

$$4, 3+1, 2+2, 2+1+1, 1+1+1+1.$$

These sorts of functions are also important in statistic mechanics, where "partition functions" count states of large ensembles of particles. Modular forms are a strong tool in combinatorics for things like

- *Automatic identity proving.*
- *Automatic congruence proving, such as Ramanujan's famous:*

$$p(5n+4) \equiv 0 \pmod{5}.$$

- *Proving asymptotic growth rates/inequalities.*

Example (Arithmetic Geometry)**.** *The most famous theorem in modular forms, and the biggest result of number theory in this generation, is the following:*

Theorem 0.1 (Modularity Theorem of Wiles,Taylor-Wiles, et al)**.** *For each elliptic curve over* $\mathbb{Q}$*, there is a special modular form which coefficients determine the number of points of* E *over all finite fields.*

This implies **Fermat's Last Theorem***!*

Example. *My favorite number is* $e^{\pi\sqrt{163}} = 262537412640768743.99999999999925\ldots$. *Why is this so very nearly an integer? Stay tuned! It requires a theory which Hilbert called the most beautiful in not only all of mathematics but all of* **science***.*

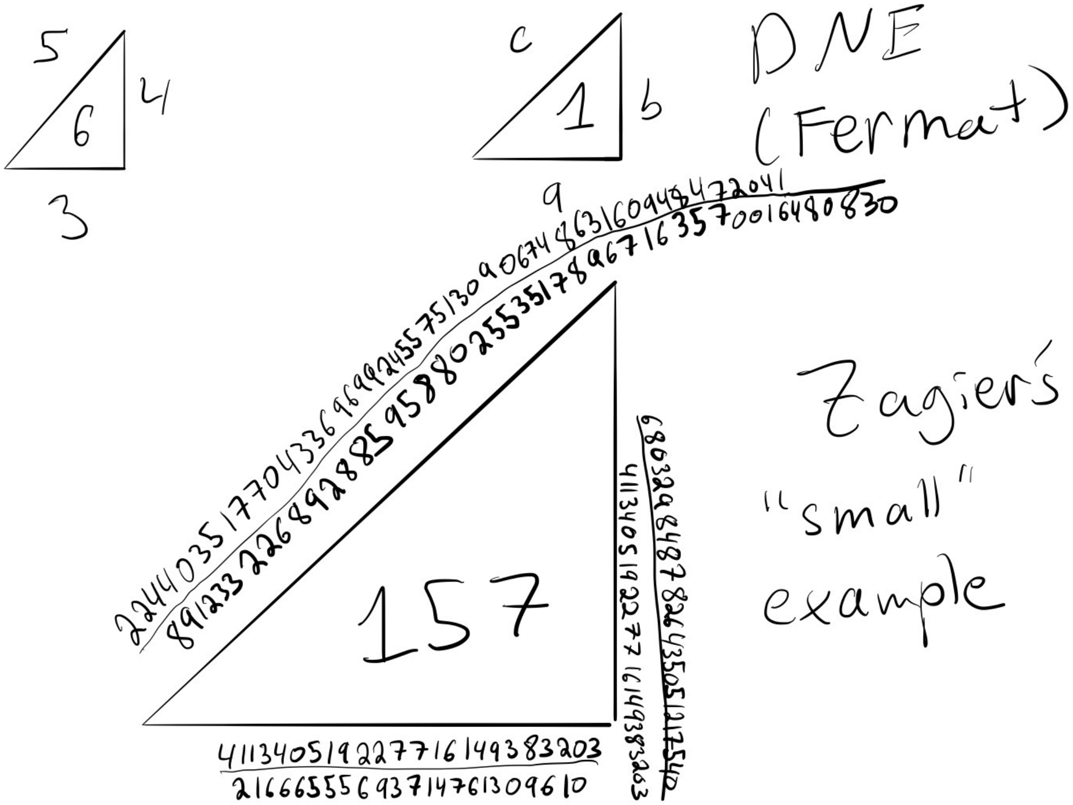
Example. *A motivating example for us will be the following. Which numbers are* **congruent***, that is, the areas of rational right triangles? For instance,* 6 *is the area of a* $3-4-5$ *triangle, so* 6 *is congruent. As an example, we have the following.*

Theorem 0.2 (Fermat, though essentially known to Fibonacci)**.** 1 *isn't congruent.*

Theorem 0.3 (Zagier)**.** 157 *is congruent, and the "smallest" example has*

$$\textit{hypotenuse } = \frac{48 \textit{ digit } \#}{46 \textit{ digit } \#}$$

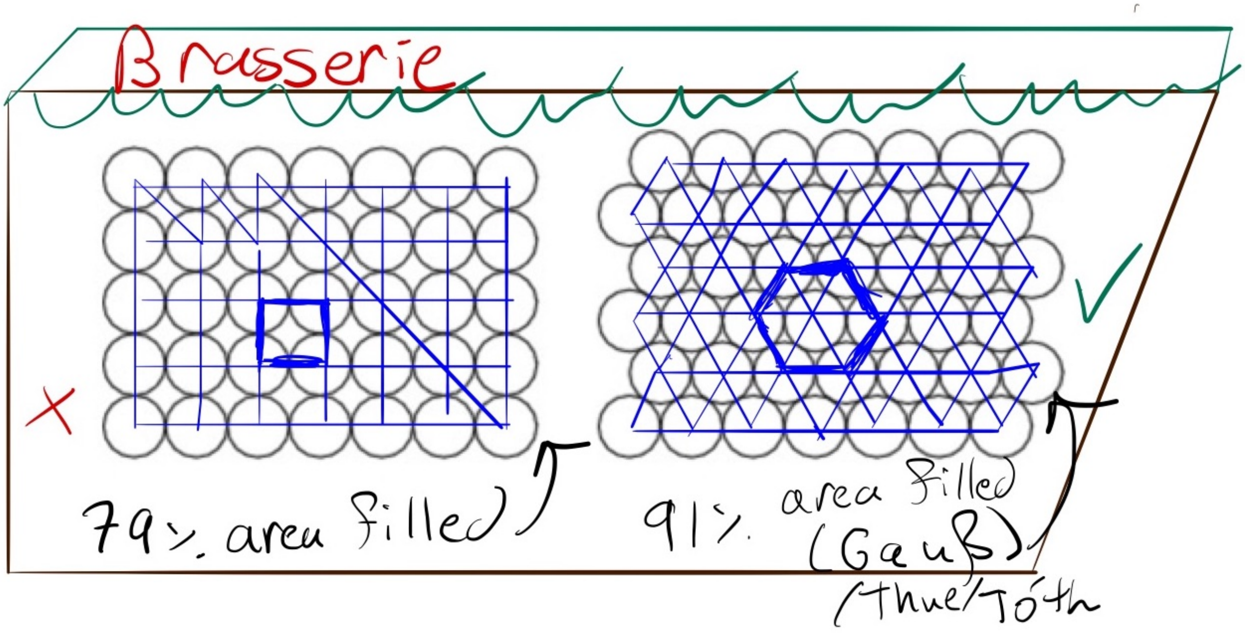
(assuming I counted right!). A naive computer search has no real limit on how long it may take to find a triangle if it exists, and you would not find Zagier's numbers this way (search space not far off from a googol).



There is a stunning result we will be able to understand at the end of this semester.

Theorem 0.4 (Tunnell). *There is a super fast test for which numbers are congruent (assuming the Birch and Swinnerton-Dyer conjecture).*

Example (Sphere packing). *During the pandemic, some restaurants now have indoor seating again. If they want to maximize the number of customers they can serve while adhering to social distancing guidelines, how should they arrange the tables? I have peeked in a number of restaurants to see, but I have yet to see one use the mathematically correct way! Rather than a rectangular grid, it is much better to place the tables on the vertices of a hexagonal lattice!*



What about optimal packing in other dimensions? In 3 dimensions, you have seen "grocery store orange" packings, which also involve hexagons. In higher dimensions, namely 8 and 24, there has been a recent series of breakthroughs by Viazovska and her collaborators, using modular forms. We will be able to understand these proofs with a little more background.

Modular forms are functions with loads of symmetry, and this symmetry causes things like spaces of modular forms to have finite dimensionality and nice congruences and arithmetic to happen. We will also see that modular inversion and translation invariance are very natural from an analytic point of view, in the sense that if you have a sequence of numbers which has some near-modularity under S and is translation invariant, then you have a very good shot of being able to determine the growth properties of that sequence from general theorems in complex analysis (and these asymptotic properties are really important limiting factors in physics). In short, as Ken Ono says, not all sequences of numbers are related to modular forms, but when they are, we know so much more about them that we can prove cool results about them.