ELLIPTIC CURVES, THE GROUP LAW, AND THE J INVARIANT

RAIANN RAHMAN

Abstract. Elliptic curves play an important role in many areas of mathematics. In just the last few decades, elliptic curves have found important applications in cryptography and were famously related to modular forms by Andrew Wiles, who then used this relation to prove Fermat's last theorem. In this paper, we introduce elliptic curves over $\mathbb{C}$. We show how the j-invariant characterizes classes of elliptic curves, we introduce the group law and briefly talk about some of the cryptographic applications that arise from it. Finally, we introduce modular functions, and modular forms. While Fermat's theorem is well beyond the scope of this paper, we show how the j-invariant shows up as a modular function.

Contents

1. Projective Space and the Projective Plane

A comprehensive understanding of elliptic curves requires some background in algebraic geometry. To understand the most general definition of an elliptic curve, we need to know what a 'genus' is, and we need to know the Riemann-Roch theorem. My aim is for this paper to take an approach that makes things accessible to those who have not yet had a class in algebraic geometry. I will work with Elliptic curves in Weierstrass normal form, and for a more in depth treatment I defer to textbooks on the subject (see references). We begin by defining the projective space:

Definition 1.1. Projective space: Given a field K, the projective space $\mathbb{P}^n(K)$ is the set

$$\{(x_0, \ldots, x_n) \in K^{n+1}\} \setminus \{\mathbf{0}\}$$

endowed with the equivalence relation

$$(x_0, \ldots, x_n) \simeq (y_0, \ldots, y_n) \iff \text{there exists } \lambda \in K \text{ such that } (x_0, \ldots, x_n) = (\lambda y_1, \ldots, \lambda y_n)$$

Date: August 15th, 2016.

For a discussion regarding elliptic curves, we are concerned mainly with the projective plane $\mathbb{P}^2(K)$. By convention, we denote the equivalence class of (x,y,z) as [x : y : z]. When we discuss elliptic curves in the next section we will need to understand a certain "point at infinity." We lay the groundwork for that by splitting $\mathbb{P}^2(K)$ into two disjoint subsets:

$$A = \{[x : y : z] \in \mathbb{P}^2 \mid z \neq 0\}$$

and

$$B = \{[x : y : z] \in \mathbb{P}^2 \mid z = 0\}$$

Note that $A \cup B = \mathbb{P}^2$. $A = \{[x : y : z] \in \mathbb{P}^2 \mid z \neq 0\}$ is isomorphic to K^2 (we take $(x, y) \in K^2$ to [x : y : 1] in A), and $B = \{[x : y : z] \in \mathbb{P}^2 \mid z = 0\}$ is isomorphic to the projective line, $\mathbb{P}^1$ (we take $[x : y]$ in $\mathbb{P}^1$ to $[x : y : 0] \in B$). So we have divided $\mathbb{P}^2$. One part is isomorphic to K^2, and the other part is called the "line at infinity." This line at infinity will be important for understanding the "point at infinity" in the section below.

2. elliptic curves/weierstrass equations

Definition 2.1. A polynomial function P is said to be **homogeneous** of degree j if given a scalar λ

$$P(\lambda \mathbf{v}) = \lambda^j P(\mathbf{v})$$

Definition 2.2. Given a homogenous polynomial of three variables in the field K (call this polynomial P(x,y,z)), we define a **projective plane curve** C_P as the points in the projective plane that yield zeroes to the polynomial back in K^3

$$C_p = \{[x : y : z] \in \mathbb{P}^2(K) \mid P(x, y, z) = 0\}$$

Definition 2.3. A plane curve is **nonsingular** if one of its partial derivatives is nonzero at any point).

Definition 2.4. We now turn to **elliptic curves**. Elliptic curves are smooth nonsingular projective curves of genus 1 with a specified base point. But, as we stated above, we will not work with this definition in the interest of avoiding an exposition in algebraic geometry. Instead, for us, elliptic curves will be defined according to the following equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

such an equation is called a Weierstrass equation. As stated above, an elliptic curve ought to be a nonsingular projective plane curve. Note that each term in the equation above is degree three, so if we move all terms to one side we get an equation that describes the zeroes of a homogenous polynomial of degree three:

$$P(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3)$$

Thus, we can define a projective plane curve accordingly from the above equation. We require that this curve be nonsingular.

Note that the only place where $Z = 0$ is when $X = 0$. Recall the 'line at infinity' is the set of all [X : Y : Z] where $Z = 0$. Thus any Weierstrass elliptic curve intersects the 'line at infinity at [0 : 1 : 0]. This point $O = [0 : 1 : 0]$ is called the 'point at infinity.' In the following section (group law) it will become clear why this point is important.

If we are working an a field, we can remember the 'point at infinity' $O = [0 : 1 : 0]$ and then divide by $Z = 1$ (because we have a homogenous polynomial), and get

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Next, we want to show that if we are working a field of not characteristic 2 or 3, we can use a linear change of variables to simplify the Weierstrass equation. Recall that K is a field. Let $\overline{K}$ be an algebraic closure of K.

Theorem 2.5. *If the characteristic of $\overline{K}$ is not 2 (alternatively we can just assume that K is algebraically closed and not of characteristic 2), we can use an invertible linear change of variables to simplify the general Weierstrass equation to one of the form*

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

Proof. We substitute y with

$$\frac{1}{2}(y - a_1x - a_3)$$

And then we get:

$$(\frac{1}{2}(y-a_1x-a_3))^2+a_1x(\frac{1}{2}(y-a_1x-a_3))+a_3\frac{1}{2}(y-a_1x-a_3) = x^3+a_2x^2+a_4x+a_6$$

which implies:

$$\frac{1}{4}(y^2-2a_1xy-2a_3y+a_1^2x^2+2a_1a_3x+a_3^2)+a_1x(\frac{1}{2}(y-a_1x-a_3))+a_3\frac{1}{2}(y-a_1x-a_3) = x^3+a_2x^2+a_4x+a_6$$

which implies:

$$\frac{1}{4}y^2 - \frac{1}{4}a_3^2 - \frac{1}{4}a_1^2x^2 - \frac{1}{2}a_3a_1x = x^3 + a_2x^2 + a_4x + a_6$$

and then we multiply both sides by 4 to get

$$y^2 - a_3^2 - a_1^2x^2 - 2a_3a_1x = 4x^3 + 4a_2x^2 + 4a_4x + 4a_6$$

and move things over to get

$$y^2 = 4x^3 + (a_1^2 + 4a_2x^2) + 2(a_4 + a_1a_3)x + (a_3^2 + 4a_6)$$

and if we write

$$b_2 = a_1^2 + 4a_4$$

and

$$b_4 = 2a_4 + a_1a_3$$

and

$$b_6 = a_3^2 + 4a_6$$

we get

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

where did we make use of the fact that the characteristic is not 2? Right at the beginning, when we substituted $\frac{1}{2}(y - a_1x - a_3)$. If we had a characteristic of 2, we wouldn't be able to use $\frac{1}{2}$, as we would have $\frac{1}{2} = \frac{1}{1+1} = \frac{1}{0}$, which is ill-defined.

□

Theorem 2.6. *If the characteristic of $\overline{K}$ is neither 2 nor 3 (alternatively we can just assume that K is algebraically closed and not of characteristic 2 or three), we can use a invertible linear change of variables to simplify the general Weierstrass equation to one of the form*

$$y^2 = x^3 + 27c_4x + 54c_6$$

Proof. here I won't bother with tedious algebra, but I will instead tell the steps and the result. Substitute $\frac{x-3b_2}{36}$ with b_2 (defined as above), and then substitute $y/108$ for y. We will find that

$$c_4 = b_2^2 - 24b_4$$

and

$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6$$

with b_2, b_4, and b_6 defined as above. We use the fact that the characteristic is neither two nor three because we can write factorizations of both 36 and 108 that consist of only two and three. Note that $36 = 2^23^2$, so

$$\frac{1}{36} = \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{3} \cdot \frac{1}{3}$$

and none of the denominators of any term on the right hand side is zero, so $1/36$ is well defined. Similar logic for $\frac{1}{108}$. □

Here are some examples of graphs of elliptic curves over the field $\mathbb{R}$, graphed in $\mathbb{R}^2$ (so not including the 'point at infinity')

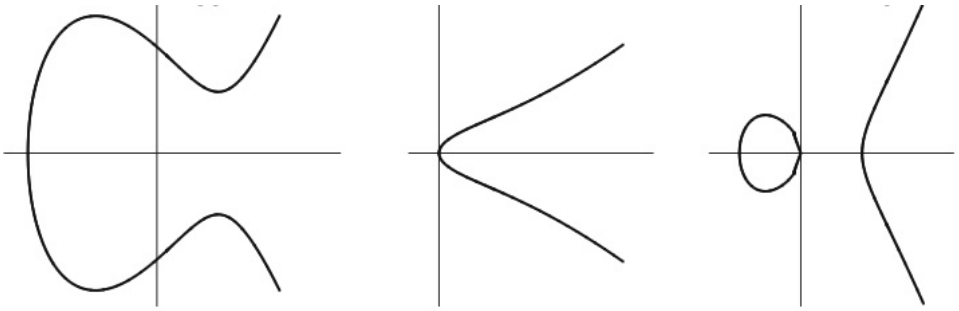

FIGURE 1. [1]

from left to right, the curves are described by the equations $y^2 = x^3 - 3x + 3$, then $y^2 = x^3 + x$, and then $y^2 = x^3 - x$.

Given an elliptic curve

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

I will compile a list of constants:

$$b_2 = a_1^2 + 4a_4$$
$$b_4 = 2a_4 + a_1a_3$$
$$b_6 = a_3^2 + 4a_6$$

[1]Silverman, Joseph H, The Arithmetic of Elliptic curves. Springer. 1986. pg 43

$$b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \quad \text{or} \quad 4b_8 = b_2 b_6 - b_4^2$$
$$c_4 = b_2^2 - 24 b_4$$
$$c_6 = -b_2^3 + 36 b_2 b_4 - 216 b_6$$
$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27 b_6^2 + 9 b_2 b_4 b_6$$

and

$$j = c_4^3/\Delta$$

the last two quantities, Δ and j (we call this the 'j-invariant') are particularly important. If we have characteristic not 2 or 3 and our equation takes the form

$$y^2 = x^3 + Ax + B$$

then it turns out

$$\Delta = -16(4A^3 + 27B^2)$$

and

$$j = -1728 \frac{(4A)^3}{\Delta}$$

Theorem 2.7. *A Curve described by a Weierstrass equation is singular if and only if* $\Delta = 0$

Proof. Recall our Weierstrass equation:

$$Y^2 Z + a_1 XYZ + a_3 YZ^2 = X^3 + a_2 X^2 Z + a_4 XZ^2 + a_6 Z^3$$

we put it into the form of a polynomial:

$$F(X, Y, Z) = Y^2 Z + a_1 XYZ + a_3 YZ^2 - (X^3 + a_2 X^2 Z + a_4 XZ^2 + a_6 Z^3)$$

and for the curve to be nonsingular we require that at all the zeroes of the polynomial at least one of the partial derivatives is nonzero. We start with the point at infinity, $O = [0 : 1 : 0]$, and show this is never singular, regardless of the discriminant. Note that

$$\frac{\partial F}{\partial Z} = Y^2 = 1$$

at $O = [0 : 1 : 0]$ so we are not singular at this point. Moving on, we assume that we have some singular point. Because we have already taken care of the point at infinity, we can divide by Z and work in the affine plane:

$$f(x, y) = y^2 + a_1 xy + a_3 y - (x^3 + a_2 x^2 + a_4 x + a_6)$$

say at x_0, y_0. Well we may as well assume without loss of generality that the singular point is at $(0, 0)$ because otherwise we could just shift with a change of variables $x = x' + x_0$ and $y = y' + y_0$. If we do this shift, a computation shows that Δ and c_4 invariant. But then

$$a_6 = f(0, 0) = 0$$

and

$$a_4 = \frac{\partial f}{\partial x} = 0$$

and

$$a_3 = \frac{\partial f}{\partial y} = 0$$

so we have

$$f(x, y) = y^2 + a_1 xy - a_2 x^2 - x^3 = 0$$

in which case $\Delta = 0$.

Now for the other way. To simplify computation we assume characteristic not 2. While we will not prove the result for characteristic 2, it is still true. Then

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

the partial derivatives are both zero if and only if there is x', y' such that

$$2y' = 12x'^2 + 2b_2x' + 2b_4 = 0$$

then any singular point is along the line $y = 0$ (in the affine plane), and has derivative 0, which means it is a double root (it is tangent to the x axis). But this can only happen if the discriminant 16Δ is 0. □

Theorem 2.8. *If K is an algebraically closed field, two elliptic curves in Weierstrass form have the same j-invariant if and only if there is an invertible linear change of variables between them of the form*

$$(x, y) = (u^2x' + r, u^3y' + u^2sx' + t)$$

with $u, r, s, t \in K$ and $u \neq 0$. If the characteristic is not 2 or 3, the change of variables is of the form

$$(x, y) = (u^2x', u^3y')$$

Proof. We will prove this fully for the case where the characteristic is not 2 or 3, although it holds true in general.

We begin first by showing that if we can choose $u, r, s, t \in K$ and $u \neq 0$, and we perform the substitution

$$(x, y) = (u^2x' + r, u^3y' + u^2sx' + t)$$

to the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

some computation and simplification reveals that such a substitution results in a new Weierstrass equation with new coefficients:

$$y'^2 + a_1'x'y' + a_3'y' = x'^3 + a_2'x'^2 + a_4'x' + a_6'$$

the new 'prime' coefficients $a_1', a_2', a_3', a_4', a_6'$ are related to the old coefficients as follows:

$$ua_1' = a_1 + 2s$$
$$u^2a_2' = a_2 - sa_1 + 3r - s^2$$
$$u^3a_3' = a_3 + ra_1 + 2t$$
$$u^4a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st$$
$$u^2b_2' = b_2 + 12r$$
$$u^4b_4' = b_4 + rb_2 + 6r^2$$
$$u^6b_6' = b_6 + 2rb_4 + r^2b_2 + 4r^3$$
$$u^8b_8' = b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4$$
$$u^4c_4' = c_4$$
$$u^6c_6' = c_6$$
$$u^{12}\Delta' = \Delta$$
$$j' = j$$

So, we have one way. If two Weierstrass equations can be related by the change of variables described above, then they have the same j-invariant. Now for the other way. Assume characteristic not 2 or 3. Then are elliptic curves are described by:

$$E : y^2 = x^3 + Ax + B$$

and

$$E' : y'^2 = x'^3 + A'x' + B'$$

Because we are assuming the j invariants are the same,

$$j = \frac{(4A)^3}{4A^3 + 27B^2} = \frac{(4A')^3}{4A'^3 + 27B'^2}$$

which means that

$$4A^3A'3 + 27A^3B'^2 = 4A^3A'3 + 27A'^3B^2$$

or

$$A^3B'^2 = A'^3B^2$$

Note that $\Delta \neq 0$ otherwise we would have a singular point. If $A = 0$, then $B \neq 0$ otherwise we would have $\Delta = 0$, so $A' = 0$, which means that $B' \neq 0$. Then we write

$$u = (\frac{B}{B'})^{1/6}$$

And then substituting into E yields:

$$u^6y^2 = u^6x^3 + Au^2x + B = u^6x^3 + B = \frac{B}{B'}y^2 = \frac{B}{B'}x^3 + B \implies y^2 = x^3 + B' = x^3 + A' + B'$$

If $B = 0$, then $A \neq 0$ and consequently $B' = 0$, and we write

$$u = (\frac{A}{A'})^{1/4}$$

and substituting into E yields

$$u^6y^2 = u^6x^3 + Au^2x + B = u^6x^3 + Au^2x = (\frac{A}{A'})^{6/4}y^2 = (\frac{A}{A'})^{6/4}x^3 + A(\frac{A}{A'})^{2/4}x \implies$$

(multiplying by the inverse of $(\frac{A}{A'})^{6/4}$

$$y^2 = x^3 + A'x = x^3 + A'x + B'$$

Finally, there is the case where $AB \neq 0$. Then we also have $A'B' \neq 0$, and we write

$$u = (\frac{A}{A'})^{1/4} = (\frac{B}{B'})^{1/6}$$

which gives us the desired result.

□

In the above theorem, why did we only consider substitutions of the form $(x, y) = (u^2x' + r, u^3y' + u^2sx' + t)$, or $(x, y) = (u^2x', u^3y')$ for characteristic not 2 and 3? The reason is that we wanted to keep things in Weierstrass form. As far as linear changes of variables go, it is clear that if we have an equation such as

$$y^2 = x^3 + Ax + B$$

we must substitute (u^2x', u^3y') if we want to keep the coefficients for the y^2 and x^3 terms 1, without introducing new terms (such as an xy or x^2 term). If we are not in characteristic 2 or three, our equation is more complicated:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

but if we have a linear change of variable not of the form $(x, y) = (u^2x' + r, u^3y' + u^2sx' + t)$ with $u \neq 0$, we run the risk of introducing new terms, making it so the coefficients of y^2 and x^3 are not 1, or even changing the 'point at infinity' This would result in a curve not in Weierstrass form. As it turn out, if we use the general definition of an elliptic curve (a nonsingular projectve curve of genus 1...) we can obtain things that are not in Weierstrass form:

$$y^2 = 3x^4 - 2$$

Furthermore, any elliptic curve can be transformed into Weierstrass form through a linear change of variables, although the Weierstrass representation is not necessarily unique. While there may be many Weierstrass forms for an elliptic curve (such as the one above), it turns out that they will all have the same j-invariant.

3. The Group Law

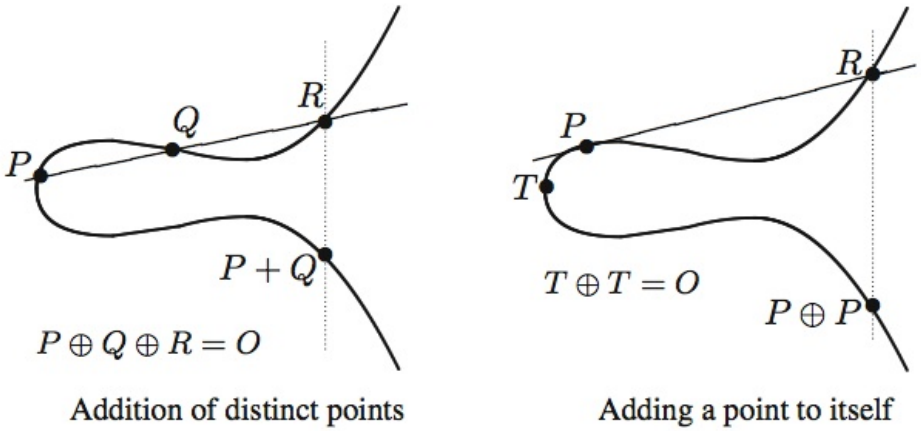

Figure 2. [2]

It may seem that I have gone through the trouble of introducing the projective plane, describing an elliptic curve as the set of points in the projective plane satisfying a Weierstrass equation, but then immediately dividing out by Z and just telling you to remember that the 'point at infinity' is there. Why not just start with regular old plane curves instead of dealing with the projective plane? It turns out that if we consider the set of points on an elliptic curve, we can define a binary operation on the set that turns the elliptic curve into an abelian group. This is also one place where the fact that the curve must be non-singular comes into play. If the curve has a singular point, the group structure breaks down. The 'point at infinity' (which for Weierstrass equations is $[0 : 1 : 0]$) serves as the additive identity.

[2]Silverman, pg 51

Roughly speaking, given two points P and Q on an elliptic curve, we take the line connecting P and Q (or if P=Q, the tangent line to the elliptic curve at P) and we note that this line intersects the curve again at some point R. We then have another line L' connecting R and $O = [0 : 1 : 0]$. The line L' intersects the elliptic curve at $P \oplus Q$. Given an explicit Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

we define group addition $\oplus$ and the additive inverse as follows:

Definition 3.1. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on the elliptic curve. If P_1 is the 'point at infinity,' it is the additive identity so it's additive inverse is itself. Otherwise define the additive inverse by:

$$-P_1 = (x_1, -y_1 - a_1x_1 - a_3)$$

and then if $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$ then

$$P_1 \oplus P_2 = O$$

Otherwise, we have $P_3 = P_1 \oplus P_2$, with $P_3 = (x_3, y_3)$, where

$$x_3 = \lambda^2 + a_1\lambda - a_2 - a_1 - x_2$$

and

$$y_3 = -(\lambda + a_1)x_3 - v - a_3$$

where if $x_1 \neq x_2$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

and

$$v = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$$

and otherwise $x_1 = x_2$ and

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$$

and

$$v = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$$

the group axioms can then be verified by computation.

Finally, we also include the duplication formula for the x coordinate, as this makes computing an integer multiple of a group element significantly quicker. If $(x', y') = (x, y) \oplus (x, y)$, then

$$x' = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}$$

Now that there is a group law, we can very briefly mention some cryptographic applications:

Definition 3.2. The **elliptic curve discrete logarithm problem** (ECDLP) gives some points P and Q on an elliptic curve and the objective is to find m such that $[m]P = Q$ ([m]P is P plus itself M times).

As it turns out, solving the ECDLP is quite hard and the best known algorithms are quite slow. The advantage of using ECDLP, as opposed to, say, RSA is that theoretically the key and message sizes can be 5 to 10 times smaller for the same time to solve.

Definition 3.3. Another application of elliptic curves to cryptography is secure key exchange. Here we describe the **Diffie − Hellman key exchange**:

(1) Persons A and B agree on a finite field $\mathbb{F}$, an elliptic curve E and a point P.
(2) Person A selects a secret integer a and computes $N = [a]P$, while person B does similarly for their secret integer b and computes $M = [b]P$.
(3) Persons A and B exchange the value of N and M over a potentially insecure channel.
(4) Person A computes $[a]M$ and person B computes $[b]N$. They both get $[ab]P$.

In the end, $[ab]P$ can be used as some secret key that only person A and person B will know. This is useful because for now, nobody knows how to compute $[ab]P$ from P, $[a]P$ and $[b]P$ without knowing a or b. Note that this key exchange method can be used for any group. However, if we are using elliptic curves, discovering a or b requires that one solve the ECDLP (at least at present), which is hard (alternatively, one could interrogate or blackmail person A or person B).

4. The j-invariant as a modular function

Above we saw how the j-invariant determines the isomorphism class of an elliptic curve. Here, we study the j-invariant in a different context, in the context of modular functions and modular forms. First we introduce the idea of a lattice.

Definition 4.1. We define a **lattice** as follows, given two linearly independent complex numbers ω_1 and ω_2 such that $Im(\omega_1/\omega_2) > 0$ (this means that the vectors are taken 'clockwise') the lattice $L(\omega_1, \omega_2)$ defined according to these vectors is

$$L(\omega_1, \omega_2) = \{n\omega_1 + n\omega_2 \mid n, m \in \mathbb{Z}\}$$

Definition 4.2. A **holomorphic** function is a complex function that takes in any number of complex variables and is complex differentiable in some neighborhood of every point

Definition 4.3. A **meromorphic** function is a complex function that is holomorphic save for a set of isolated points which are called poles

Definition 4.4. We call $\mathbb{H} = \{x \in \mathbb{C} \mid Im(x) > \mathbb{C}\}$ the upper half plane.

Definition 4.5. We define

$$SL_2(\mathbb{Z}) = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid ad - bc = 1 \text{ and } a, b, c, d \in \mathbb{Z}\}$$

Definition 4.6. A function f is called **weakly modular** of weight 2k if it is meromorphic on $\mathbb{H}$ and

$$f(z) = (cz + d)^{-2k} f(\frac{az + b}{cz + d})$$

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

If f is meromorphic at infinity it is a **modular function**, and if it is holomorphic everywhere (including infinity, meaning as $z \to i\infty$) it is a **modular form**.

Definition 4.7. We define a function on the upper half plane $G_{2k}(\tau)$, the Eisenstein series of weight 2k, by

$$G_{2k}(\tau) = \sum_{\omega \in L(\tau,1) | \omega \neq 0} \omega^{-2k} = \sum_{(m,n) \neq (0,0)} \frac{1}{(m+n\tau)^{2k}}$$

Theorem 4.8. *For $k \geq 1$, the Eisenstein series is a modular form of weight 2k*

Proof. First we ought to show that the function is well-defined (that the series converges). We will just show that the series converges absolutely We can find some constant c such that for $n \geq 1$

$$\#\{\omega \in L(\tau,1) \mid N < |\omega| < N+1\} < cN$$

which means that

$$\sum_{\omega \in L(\tau,1), \omega \geq 1} \leq \sum_{N=1}^{\infty} \frac{\#\{\omega \in L(\tau,1) \mid N < |\omega| < N+1\}}{N^{2k}} < \sum_{n=1}^{\infty} \frac{c}{N^{2k-1}}$$

and that is all we need to show the function is well-defined.

Note that

$$G_{2k}(\frac{a\tau+b}{c\tau+d}) = \sum_{(m,n) \neq (0,0)} \frac{1}{(m+n\frac{a\tau+b}{c\tau+d})^{2k}} = \sum_{(m,n) \neq (0,0)} \frac{(c\tau+d)^{2k}}{(md+nb+\tau(mc+na))^{2k}} =$$

$$\sum_{(m',n')=(m,n)\begin{bmatrix} d & c \\ b & a \end{bmatrix}, (m,n) \neq (0,0)} \frac{(c\tau+d)^{2k}}{m'+n'\tau}^{2k}$$

but the inverse of $\begin{bmatrix} d & c \\ b & a \end{bmatrix}$ is $\begin{bmatrix} a & -c \\ -b & d \end{bmatrix}$ which has determinant 1 so $\begin{bmatrix} d & c \\ b & a \end{bmatrix}$ is rank 2 and therefore a bijection so continuing the chain of equalities from above

$$\sum_{(m',n')=(m,n)\begin{bmatrix} d & c \\ b & a \end{bmatrix}, (m,n) \neq (0,0)} \frac{(c\tau+d)^{2k}}{m'+n'\tau}^{2k} = \sum_{(m',n') \neq (0,0)} \frac{1}{(m'+n'\tau)^{2k}} = G_{2k}(\tau)$$

which means that

$$G_{2k}(\tau) = (c\tau+d)^{-2k} G_{2k}(\frac{a\tau+b}{c\tau+d})$$

which gets rid of the 'weight 2k' part. Now we just need to show the function is holomorphic.

Let us show that the function is holomorphic on the half-plane first. Note that for any m, n $f(\tau) = \frac{1}{(m+n\tau)^{2k}}$ is holomorphic. Recall that $G_{2k}(\tau)$ is an infinite series which is absolutely convergent, and this means that it is uniformly convergent on any compact (or closed and bounded) domain. If a sequence of holomorphic functions is uniformly convergent on every compact subset of the domain, it is holomorphic on the domain, so G_{2k} is holomorphic on $\mathbb{H}$. The last thing to do

is to show that the function is holomorphic at infinity. We must prove that as $Im(\tau) \to \infty$, there is a limit. But as $\tau \in \mathbb{H}$, $|\tau| \to \infty$ is the same as $Im(\tau) \to \infty$. Thus

$$\lim_{\tau\to\infty} \sum_{(m,n)\neq(0,0)} (m+n\tau)^{-2k} = \lim_{\tau\to\infty} \sum n^{-2k} + \lim_{\tau\to\infty} \sum_m \sum_n (m+n\tau)^{-2k} = \lim_{\tau\to\infty} \sum n^{-2k}$$

which is 2 times the Riemann zeta function value for 2k. This proves the function is holomorphic at infinity. Thus, G_{2k} is a modular form of weight 2k.

□

We write $g_2 = 60G_{2(2)}$ and $g_3 = 140G_{2(3)}$, then consider the elliptic curve

$$y^2 = 4x^3 - g_2x - g_3$$

note that this equation is not in Weierstrass form. Either way, from here we can define Δ and j as a function of $\tau \in \mathbb{H}$ by writing

$$\Delta(\tau) = g_2^3 - 27g_3^2$$

and

$$j(\tau) = 1728\frac{g_2^3}{\Delta}$$

because sums and products of holomorphic functions are holomorphic, and quotients when the denominator is 0, it is easily verified that Δ is a modular form of weight 12. This, combined with the fact that g_2^3 is also weight 12, allows us to conclude that j is a modular function of weight 0.

Acknowledgments. It is a pleasure to thank my mentors, Jingren Chi and Jonathan Wang, for guiding me through this

References

[1] Joseph H Silverman. The Arithmetic of Elliptic curves. Springer. 1986.
[2] J. S. Milne. Elliptic Curves. BookSurge Publishers. 2006.
[3] Dale Husemoller. Elliptic Curves, Second Edition. Springer. 2004.
[4] Ian Connel. Elliptic Curve Handbook. http://www.math.mcgill.ca/connell/
[5] Bonaccorso Salvatore. Modular Forms, Eisenstein Series and a Short Introduction to elliptic functions.