Tori, Weierstrass $\wp$, and Elliptic Curves Over $\mathbb{C}$
Math 414 Final Project

Christopher Raastad

March 12th, 2010

Abstract

This paper explores the structure of Elliptic Curves over $\mathbb{C}$ and equivalence classification under homothetic complex latticeswith the intent to show that tori are elliptic curves. The paper will give an overview of advanced results contributing to understanding of the topic. Although the results will attempt to be self-contained, a background in Complex Analysis will greatly contribute to comprehending the the subject matter, refer to Gamelin [1] for such an introduction. The paper is mainly based on the discussions given in Knapp [2] and Washington [5] with Husemöller [4] and [3] as an external reference.

For a given complex lattice $\Lambda = \{n_1 w_1 + n_2 w_2 : w_i \in \mathbb{C}, n_i \in \mathbb{Z}\}$ where w_1 and w_2 are linearly independent in $\mathbb{R}$, we can define a doubly periodic or Elliptic Function $f : \mathbb{C} \to \mathbb{C}$ such that $f(z+w) = f(z)$ for all $z \in \mathbb{C}$ and $w \in \Lambda$. Topologically, a Torus can be identified by a parallelogram with opposite sides identified, and hence follows the equivalence of Λ with a torus. After exploring general useful complex analytic properties of lattices and Elliptic functions we introduce a non-trivial Elliptic Function, the Weierstrass $\wp$ -function over a give lattice Λ. Then we sketch the proof that the set of Elliptic Functions for lattice Λ is $\mathbb{C}(\wp, \wp')$, that is, a complex rational function of $\wp$ and $\wp'$.

Next we show that a given lattice Λ generates an Elliptic Curve over $\mathbb{C}$. The equation of an elliptic curve falls out of deriving a differential equation with respect to $\wp$, $\wp'$, and G_k, the Einstein series with $k = 4, 6$, from the Laurent series expansions of these quantities and then proving the map $\varphi : \mathbb{C}/\Lambda \to E(\mathbb{C})$ sending $z \mapsto (\wp(z), \wp'(z))$ and $0 \mapsto \infty$ is indeed a group isomorphism.

The converse, to show that a non-singular Elliptic Curve can be associated to a $\mathbb{C}$-lattice Λ unique under homothetic equivalence, is much more tricky. There are two general approaches to prove the equivalence, one hinges on defining a special j-function invariant and proving useful relations amongst complex lattices. The other combines Riemannn surfaces, Γ functions, and winding numbers into proving a biholomorphic map. Theoretically we will state the results of the first approach but ignore the complicated details. Computationally, finding generators for a lattice Λ given an elliptic curve E reduces to computing an elliptic integral using the Gauss Arithmetic Geometric Mean. We will outline this derivation and then end with a computation of a lattice given a particular elliptic curve.

Contents

1 Lattices and Elliptic Functions **4**

1.1 Lattices over $\mathbb{C}$ 4

1.2 Equivalence of Torus and $\mathbb{C}/\Lambda$ 4

1.3 Elliptic Functions 5

1.4 The Weierstrass $\wp$-function 6

2 $\mathbb{C}/\Lambda \to E(\mathbb{C})$: Tori are Elliptic Curves **7**

2.1 Einstein Series 8

2.2 The Elliptic Curve Differential Equation 8

2.3 $\mathbb{C}/\Lambda$ and $E(\mathbb{C})$ are Isomorphic 9

3 $E(\mathbb{C}) \to \mathbb{C}/\Lambda$: Elliptic Curves come from a Torus **10**

3.1 Homothetic Lattices 10

3.2 The j-function 11

3.3 Elliptic Integrals 12

3.3.1 Definition 12

3.3.2 Gauss Arithmetic Geometric Mean 13

3.3.3 Computing Periods w_1 and w_2 14

4 Conclusion **15**

1 Lattices and Elliptic Functions

1.1 Lattices over $\mathbb{C}$

Let $w_1, w_2 \in \mathbb{C}$ such that $w_1 \neq \lambda w_2$ for any $\lambda \in \mathbb{R}$, we say w_1 and w_2 are linearly independent in $\mathbb{R}$. Then we define the complex **lattice** Λ generated by w_1 and w_2 as

$$\Lambda = \mathbb{Z}\, w_1 + \mathbb{Z}\, w_2 = \{n_1 w_1 + n_2 w_2 : n_1, n_2 \in \mathbb{Z}\}.$$

We define Π the **fundamental parallelogram** of Λ by

$$\Pi = \{a_1 w_1 + a_2 w_2 : 0 \leq a_i < 1, i = 1, 2\}.$$

We can generate the lattice Λ by simply translating the verticies of Π in any integral linear combination of w_1 and w_2.

1.2 Equivalence of Torus and $\mathbb{C}/\Lambda$

As a revealing diversion, it is straightforward to show the topological equivalence under homeomorphism of a **Torus** and $\mathbb{C}/\Lambda$, the space of complex numbers modded out by a lattice Λ. We can think of the fundamental parallelogram Π as a representative of the set $\mathbb{C}/\Lambda$, since $\mathbb{C}/\Lambda = \{z : z \equiv z'$ if and only if $z' = z + n_1 w_1 + n_2 w_2,\ n_1, n_2 \in \mathbb{Z}\}$. Hence using Π as a representative of $\mathbb{C}/\Lambda$, we can identify the aw_1 edge with the $w_2 + aw_2$ edge and likewise the bw_2 edge with the $w_1 + bw_2$ edge where $0 \leq a, b < 1$. And hence with a sequence of gluings we get the following derivation of a torus from $\mathbb{C}/\Lambda$, that is, $\mathbb{C}/\Lambda \to \Pi \to$ cylinder $C \to$ torus T^2.

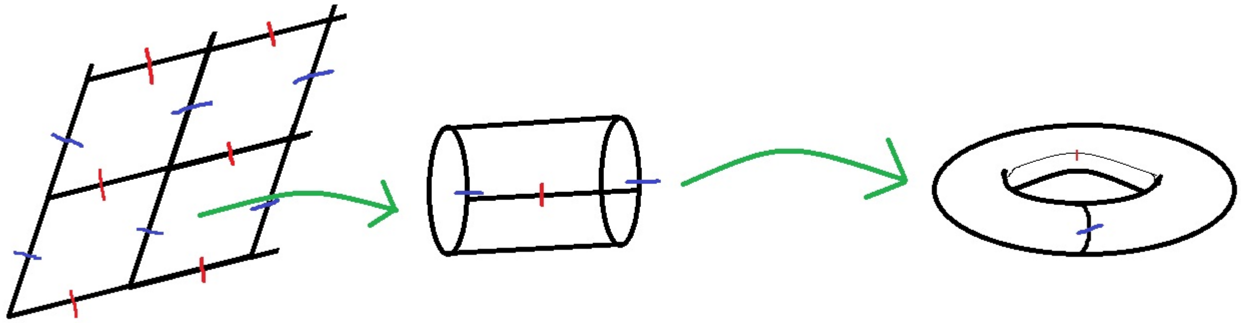

Figure 1: Identifying a Lattice to a Torus via transformations: Lattice → Fundamental Parallelogram → Cylinder → Torus

1.3 Elliptic Functions

An **Elliptic Function**, or double periodic function, over a complex lattice Λ is a complex analytic (continuous in the complex sense) function $f : \mathbb{C} \to \mathbb{C}^*$ (where $\mathbb{C}^* = \mathbb{C} \cup \infty$) such that $f(z + w) = f(z)$ for any $z \in \mathbb{C}$ and $w \in \Lambda$. It follows that $f(z + w_1) = f(z + w_2) = f(z)$, and we call w_1, w_2 the **periods**. of f.

If $f \not\equiv 0$, i.e identified to be zero, then since f is analytic we can write f as a Laurent series expansion around z $w \in \Lambda$ as

$$f(z) = a_r(z - w)^r + a_{r+1}(z - w)^{r+1} + \cdots$$

with $a_r \neq 0$. We define the **order** of f at w as $\mathrm{ord}_w f = r$ and the **residue** of f at w as $\mathrm{Res}_w f = a_{-1}$. It's clear that since f is doubly periodic, $\mathrm{Res}_{w+w} f = \mathrm{Res}_w f$ and likewise $\mathrm{ord}_{w+w} f = \mathrm{ord}_w f$.

Theorem: 1 Let f be an elliptic function for the lattice Λ and let Π be a fundamental parallelogram for Λ.

1. If f has no poles, then f is constant.
2. $\sum_{w\in\Pi} \mathrm{Res}_w f = 0$.
3. If f is not identically 0, that is $\displaystyle\sum_{w\in\Pi} w \cdot \mathrm{ord}_w f = 0$
4. If f is not constant then $f : \mathbb{C} \to \mathbb{C} \cup \infty$ is surjective. If n is the sum of the orders of the poles of f in Π and $z_0 \in \mathbb{C}$, then $f(z) = z_0$ has n solutions (counting multiplicities).
5. If f has only one pole in Π, then this pole cannot be a simple pole.

Where all of the above sums over $w \in \Pi$ have finitely many nonzero terms.

Proof. is given in Washington [5] p259. By definition f has a **pole** at z_0, if $\lim_{z\to z_0} f(z) = \pm\infty$ (this implies the Laurent series of f (as above) has negative order around $z = z_0$. Statement (1) stems from the analyticity of f, and the fact an analytic function and the general statement that an analytic function can only have finitely many zeros and poles in any compact. This implies f is bounded on any Π and hence all of $\mathbb{C}$ andby Liouville's theorem, a bounded entire function is constant, proving (1).

Statement (2) and (3) proven using some clever line integrals and Residue calculations. Statement (4) is proven by considering $h(z) = f(z) - z_0$, a doubly periodic function with poles the same as f. Statemetn (5) is simple, suppose f ahs only a simple pole, sat at w , and no others. Then $\mathrm{Res}_w f \neq 0$ (otherwise, the pole doesn't exist). Thus the sum in the second statement only has on nonzero term, a contradiction. Hence there are no other poles, or a **simple pole**, meaning a pole of single order. □

1.4 The Weierstrass $\wp$-function

A non-trival example of an Elliptic Function is the **Weierstrass $\wp$-function**. Given a lattice Λ we define the Weierstrass $\wp$-function by

$$\wp(z) = \wp(z;\Lambda) = \frac{1}{z^2} + \sum_{w\in L\ \{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

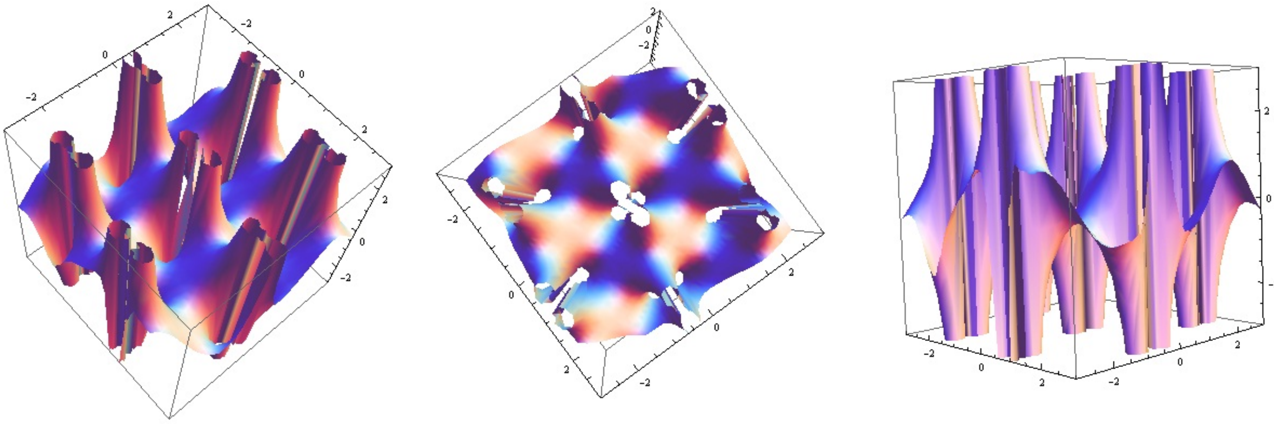

Figure 2: Various angles of a plot in Mathematica of a $\wp$-function on a lattice Λ generated by complex number $w_1 = 1 + i$ and $w_2 = 1 + 2i$. Notice the periodicity of the function and poles.

Theorem: 2 The $\wp$ function satisfies the following properties:

1. $\wp(z)$ is well defined in the sense that the sum converges absolutely and uniformly on compact sets Ω such that $\Omega \cap \Lambda = \emptyset$.

2. $\wp(z)$ is meromorphic in $\mathbb{C}$ and has a double pole at each $w \in \Lambda$.

3. $\wp(-z) = \wp(z)$ for all $z \in \mathbb{C}$.

4. $\wp(z + w) = \wp(z)$ for all $w \in \Lambda$.

5. The set of elliptic periodic function for Λ if $\mathbb{C}\ (\wp, \wp')$. In other words the every elliptic function is a rational function of $\wp$ and its derivative $\wp'$.

I will just sketch the proofs. For (1) it is convenient to prove the following lemma.

Lemma: If $k > 2$ then the following converges,

$$\sum_{w\in\Lambda/\{0\}} \frac{1}{|w|^k}.$$

where the sum converges over the entire lattice Λ. The convergence of the series is proven using an integral comparison test and estimates on the diagonal of the fundamental parallelogram Π. Then the absolute and uniform convergence is a consequence of another estimate and the exclusion of finitely many terms.

(2) is proven using the complex analytic fact a uniform limit of analytic functions is analytic, $\wp(z)$ is analytic for $z \notin \Lambda$. If $z \in \Lambda$ then the sum of terms for $w \neq z$ is analytic near z, so the term $1/(z-w)^2$ forces $\wp$ to have a double pole at z, hence (2).

(3) is fairly straightforward. If $w \in \Lambda$ then it is also true that $-w \in \Lambda$ by multiplying by -1, hence, in the sum for $\wp(-z)$ we can sum over $-w \in \Lambda$, hence the terms are in the form

$$\frac{1}{(-z+w)^2} - \frac{1}{(-2)^2} = \frac{1}{(z-w)^2} - \frac{1}{w^2}$$

hence not changing the sum, hence $\wp(-z) = \wp(z)$.

The proof of (4), we differenitate and conclude

$$\wp'(z) = -2 \sum_{w \in L} \frac{1}{(z-w)^3}.$$

The sum converges uniformly and absolutely by the lemma with simple comparison to $\frac{1}{|w|^3}$. When $z \notin w$, then swapping $z \leftrightarrow z + w$ only shifts terms, hence $\wp'(z+w) = \wp'(z)$. By calculus, this implies there exists a constant c_w such that $\wp(z+w) - \wp(z) = c_w$ for all $z \notin L$. Letting $z = \frac{w}{2}$ we have $c_w = \wp(-w/2) - \wp(w/2) = \wp(w/2) - \wp(w/2) = 0$, thus $\wp(z+w) = \wp(z)$.

Husemöller [4] gives a very slick proof of part (5) which i reproduce below. First, we write every elliptic function $f(z)$ as the sum of an even and odd elliptic function

$$f(z) = \frac{f(z) + f(-z)}{2} + \frac{f(z) - f(-z)}{2}.$$

Using the derivative computed above for $\wp'(z) = -2 \sum_{w \in L} \frac{1}{(z-w)^3}$, then $\wp'(z)$ times an odd elliptic function is an even elliptic function. Hence it suffices to show that $\mathbb{C}\,(\wp(z))$ is the field of even elliptic functions. If $f(z)$ is even, then $\mathrm{ord}_0 f(z) = 2m$ is even and $f(z) = \wp(z)^{-m} g(z)$, where elliptic $g(z)$ is even with no zeros or poles on Λ. If a is a zero of $\wp(z) - c = 0$ then so is $w - a$ for all $w \in L$ and if a is zero or a pole of $g(z)$ then so is $w - a$. If $2a \in L$, then the zero (or pole) is of order at least 2 since $g'(-z) = -g'(z)$ and so $g'(a) = g'(-a) = -g'(a)$, thus

$$g(z) = c \cdot \frac{\prod_i (\wp(z) - \wp(a_i))}{\prod_i (\wp(z) - \wp(b_i))}$$

where $\{a_i, w - a_i\}$ are zeros of $g(z)$ and $\{b_i, w - b_i\}$ are the poles of $g(z)$ in a fixed fundamental domain, Π^*. Hence proving the theorem. □

2 $\mathbb{C}\,/\Lambda \to E(\mathbb{C}\,)$: Tori are Elliptic Curves

In this section we show that given a complex lattice Λ we can generate an elliptic curve $E(\mathbb{C}\,)$.

2.1 Einstein Series

On a lattice Λ, for an integer $k \geq 3$ we define the **Einstein series**

$$G_k = G_k(\Lambda) = \sum_{w \in \Lambda/\{0\}} w^{-k}.$$

Notice this series converges by the lemma proved in the $\wp$-function section. Note that when $2k+1$ is odd, then $G_{2k+1} = 0$ since terms of w and $-w$ cancel out!

Proposition: For $0 < |z| < \min(|w|)$ such that $0 \neq w \in \Lambda$ then

$$\wp(z) = \frac{1}{z^2} + \sum_{j=1}^{\infty} (2j+1) G_{2j+2} z^{2j}.$$

Proof. Notice

$$\frac{1}{(z-w)^2} - \frac{1}{w^2} = w^{-2}\left(\frac{1}{(1-(z/w))^2} - 1\right) = w^{-2}\left(\sum_{n=1}^{\infty}(n+1)\frac{z^n}{w^n}\right).$$

Thus

$$\wp(z) = \frac{1}{z^2} + \sum_{w \neq 0} \sum_{n=1}^{\infty} (n+1) \frac{z^n}{w^{n+2}}.$$

which yields the result after taking the double sum over w then n.

2.2 The Elliptic Curve Differential Equation

Theorem: 3 Let $\wp(z)$ be the Wierstrass $\wp$-function for a lattice Λ, then

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_r\wp(z) - 140G_6.$$

Proof. We use the series expansions of $\wp$ and $\wp'$ from the previous proposition, we see

$$\wp(z) = z^{-2} + 3G_4z^2 + 5G_6z^4 + 7g_8z^6 + O(z^7)$$
$$\wp'(z) = -2z^{-3} + 6G_4z + 20G_6z^3 + 42G_8z^5 + O(z^4),$$

and taking the cube and the square we have

$$\wp(z)^3 = z^{-6} + 9G_4z^{-2} + 15G_6 + (21G_8 + 27G_4^2)z^2 + O(z^4)$$
$$\wp'(z)^2 = 4z^{-6} - 24G_4z^{-2} - 80G_6 + (36G_4^2 - 168)z^2 + O(z^4).$$

hence, we let $f(z)$ be defined as follows,

$$f(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6 = O(z^3).$$

Thank Knapp [2] for the slick proof idea. Notice that left side of higher order terms have no poles nor a constant term, hence since f is an elliptic function (as a polynomial of $\wp(z)$ and $\wp'(z)$) by the Theorem in the Elliptic Function section, $f(z) \equiv 0$. □

Now making the substitutions $g_2 = 60G_4$, $g_3 = 140G_6$ we have

$$\wp'(z)^2 = 4\wp(z)^3 = g_2\wp(z) - g_3.$$

Proposition: The discriminant $\Delta = 16(g_2^3 - 27g^3) \neq 0$.

Proof. Since $\wp'(z)$ is doubly periodic, $\wp'(w_i/2) = \wp'(-w_i/2)$, since $\wp'(-z) = -\wp'(z)$ it follows $\wp'(w_i/2) = 0$ for $i = 1, 2, 3$. Hence each $\wp(w_i/2)$ is a root of $4x^3 - g_2x - g_3$. Showing that these roots are distinct proves the discriminate is nonzero. Letting $h_i(z) = \wp(z) - \wp(w_i/2)$. Since $h_i(w_i/2) = 0 = h_i'(w_i/2)$, then h_i vanishes to order at least 2 at $w_i/2$. Since $h_i(z)$ has only one pole in Π, the double pole at $z = 0$, then Theorem 1 part (5) implies that $w_i/2$ is the only zero of $h_i(z)$, so $h_i(w_j/2) \neq 0$ when $j \neq i$ hence the values of $\wp(w_i/2)$ are distinct and the discriminant is non-zero. □

Hence making the substitution $(x, y) = (\wp(z), \wp'(z))$ we get a non-singular elliptic curve

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

As discussed in Knapp [2] and Koblitz [3], letting $w = \wp(z)$, the cubic polynomial $4w^3 - g_2w - g_3$ factors into

$$4w^3 - g_2w - g_3 = 4(w - e_1)(w - e_2)(w - e_3)$$

where $e_1 = \wp(w_1/2), e_2 = \wp(w_2/2)$, and $e_3 = \wp((w_1 + w_2)/2)$. The factorization hence proves the non-singularity of $E : y^2 = 4x^3 - g_2x - g_3$ since the factors are unique.

2.3 $\mathbb{C}/\Lambda$ and $E(\mathbb{C})$ are Isomorphic

Using our nice looking formula, we now need to prove the highly non-trivial but intuitively promising isomorphism.

Theorem: 4 Let Λ be a lattice on $\mathbb{C}$ and E be the elliptic curve $y^2 = 4x^3 - g_2x - g_3$. Then the map φ defined by

$$\begin{aligned} \varphi : \mathbb{C}/L &\to E(\mathbb{C}) \\ z &\to (\wp(z), \wp'(z)) \\ 0 &\to \infty \end{aligned}$$

is a group isomorphism under addition "modulo Λ" in $\mathbb{C}/\Lambda$ = and standard elliptic curve operations in $E(\mathbb{C})$.

Proof Sketch. Surjectivity and Injectivity are fairly easy (basically from Washington [5]). Take $(x, y) \in E(\mathbb{C})$. Since $\wp(z) - x$ has a double pole, Theorem 1 implies it has zeros, hence there exists

$z \in \mathbb{C}$ such that $\wp(z) = x$. The elliptic equation in Theorem 3 implies that $\wp'(x)^2 = y^2$, so $\wp'(z) = \pm y$. If $\wp'(z) = y$ we are done. If $\wp'(z) = -y$, then by the evenness formula in Theorem 2 on the $\wp$ function, $\wp'(-z) = y$ and $\wp(-z) = x$, so $-z \mapsto (x, y)$, hence φ is onto.

For Injectiviy suppose $\wp(z_1) = \wp(z_2)$ and $\wp'(z_1) = \wp'(z_2)$, and $z_1 \not\equiv z_2 \pmod \Lambda$. The only poles of $\wp(z)$ are for $z \in \Lambda$. Thus if z_1 is a pole of $\wp$, then $z_1 \in \Lambda$ and $z_2 \in \Lambda$ implies $z_1 \equiv z_2$ (mod Λ). Now suppose z_1 is not a pole of $\wp$, i.e., $z_1 \notin \Lambda$. Then $\wp(z) - \wp(z_1)$ has a double pole at $z = 0$ and no other poles in Π. By Theorem 1, $h(z)$ has exactly two zeros. Suppose $z_1 = w_i/2$ for some i. From the proof of the discriminant we know that $\wp'(w_i/2) = 0$ so z_1 is a double root of $h(z)$ hence the only root. Thus $z_2 = z_1$. Suppose z_1 is not of the form $w_i/2$. Since $h(-z_1) = h(z_1) = 0$ and since $z_1 \not\equiv -z_2 \pmod \Lambda$, two zeros of h are z_1 and $z_2 \equiv -z_1 \pmod \Lambda$. But $y = \wp'(z_2) = \wp'(-z_1) = -\wp'(z_1) = -y$. Hence $\wp'(z_1) = y = 0$. But $\wp'(z)$ has only a triple pole, thus has only three zeros in Π. But from the discriminent proof, we know that these zeros occur at $w_i/2$, hence a contradiction since $z \neq w_i/2$. Thus $z_1 \equiv z_2 \pmod \Lambda$ and φ is injective.

Proving φ is a homomorphism is much more tricky. Knapp [2] approaches the proof quite abstractly and complex algebraically. He proves the continuity of the inverse map $f(z_1, z_2) = \varphi^{-1}(\varphi(z_1) + \varphi(z_2)) \pmod \Lambda$ and then proves the general result that an analytic map $f : \mathbb{C}/\Lambda \times \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ can be expressed as $f(z_1, z_2) \equiv az_1 + bz_2 + c \pmod \Lambda$ for all $z_1, z_2 \in \mathbb{C}$. Then he derives that $a = b = 1, c = 0$ and hence $f(z_1, z_2) = z_1 + z_2$ hence $\varphi(z_1 + z_2) = \varphi(z_1) + \varphi(z_2)$.

Washington [5] approaches the problem by algebraically proving for each coordinate using some complicated analytic and algebraic techniques.

As Knapp [2] points out, if we didn't know that $E(\mathbb{C})$ was associative, then proving that φ is a group isomorphism would in fact prove the associativity of rational points on an Elliptic Curve since $\mathbb{Q} \subset \mathbb{C}$. Supposedly this was Poincare's approach. □

Notice after proving this isomorphism, then a corollary is every Torus generates an Elliptic curve, as given by the equation given in Theorem 4!

3 $E(\mathbb{C}) \to \mathbb{C}/\Lambda$: Elliptic Curves come from a Torus

In this section we outline that every elliptic curve over $\mathbb{C}$ comes from a torus. That is, given an elliptic curve $E(\mathbb{C})$, then we can produce a lattice Λ unique up to some homothetic equivalence. The subject is full of "deep" theorems in the sense that the proofs are long, complicated, and involved (that is more than a page), hence I will mostly be stating results.

3.1 Homothetic Lattices

Let $\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2$ be a lattice in $\mathbb{C}$. We define $\tau = \frac{w_1}{w_2}$. Since w_1 and w_2 are linearly independent over $\mathbb{R}$, τ cannot be real. Hence, by switching w_1 and w_2 if necessary, we can assume the imaginary part $\Im(\tau) > 0$, i.e., τ lies in the upper half plain $\mathcal{H} = \{x + iy \in \mathbb{C} \ : y > 0\}$. Now if we let $\Lambda_\tau = \mathbb{Z}\,\tau + \mathbb{Z}$, then Λ is **homothetic** to Λ_τ, that is

$$\Lambda = \lambda\Lambda_\tau$$

for some $\lambda \in \mathbb{C}$. In this case $\lambda = w_2$.

Now the main result of this section is,

Theorem: 5 Let $y^2 = 4x^3 - Ax + b$ define an elliptic curve E over $\mathbb{C}$. Then there exists a lattice Λ such that $g_2(\Lambda) = A$ and $g_3(\Lambda) = B$ and there is an isomorphism of groups $\mathbb{C}/\Lambda \cong E(\mathbb{C})$.

Here the elements of Λ are called the **periods** of Λ. Moreover this existence is a homothetic equivalence, that is, if we find Λ that works, then any $\Lambda' = \lambda\Lambda$ for $\lambda \in \mathbb{C}$ will suffice. There are two general approaches to proving the statement.

3.2 The *j*-function

This ironically named function (based on it's definition) which classifies elliptic curves under isomorphism, that is two elliptic curves E and E' over $\mathbb{C}$ are isomorphic if and only if $j(E) = j(E')$ [4]. The j function is defined as

$$1728(\tau) = 1728\frac{g_2^3}{g_2^3 - 27g_3^2}$$

or in long ridiculous computational form

$$j(\tau) = 1728\frac{\left(1 + 240\sum_{j=1}^{\infty}\frac{j^3q^j}{1-q^j}\right)^3}{\left(1 + 240\sum_{j=1}^{\infty}\frac{j^3q^j}{1-q^j}\right)^3 - \left(1 + 504\sum_{j=1}^{\infty}\frac{j^5q^j}{1-q^j}\right)^2}$$

where $q = e^{w\pi i\tau}$ with τ defined as above.

Studying j-functions[5], a few results follow that are used in the proof of the main equivalence statement of the section, Theorem 5.

Proposition: If Λ_1 and Λ_2 are lattices in $\mathbb{C}$. Then $j(\Lambda_1) = j(\Lambda_2)$ if and only if there exists $0 \neq \lambda \in \mathbb{C}$ such that $\lambda\Lambda_1 = \Lambda_2$.

Proposition: Let $\tau_1, \tau_2 \in \mathcal{H}$, then $j(\tau_1) = j(\tau_2)$ if and only if there exists $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_w(\mathbb{Z})$ (the group of invertible matrices in the integers) such that

$$\frac{a\tau_1 + b}{c\tau_1 + d} = \tau_2.$$

3.3 Elliptic Integrals

3.3.1 Definition

Finally, another approach to the inverse problem is given an Elliptic curve E, simply directly compute periods w_1 and w_2 of some lattice. We do this by transforming the $\wp$-function differential equation into an elliptic integral. Letting $x = \wp(z)$ we attempt to find the inverse $x = f(w)$. Using the factorization of the elliptic differential equation, we have the following transformation, with $e_1 < e_2 < e_3$ [5][2]

$$\begin{aligned}\left(\frac{dw}{dz}\right)^2 &= 4(x-e_1)(x-e_2)(x-e_3)\\ dz &= \frac{dw}{2\sqrt{(x-e_1)(x-e_2)(x-e_3)}}\\ z(w) &= \int_{e_3}^{\infty} \frac{dx}{2\sqrt{(x-e_1)(x-e_2)(x-e_3)}}\end{aligned}$$

with the change of variables $x = \wp(z)$, then the denominator becomes $\sqrt{\wp'(z)^2} = -\wp'(z)$ and the limits transform to $z = w_2/2$ to 0. So we have (with a direction reverse)

$$\int_0^{w_2/2} dz = \frac{w_2}{2}.$$

Hence

$$w_2 = \int_{e_3}^{\infty} \frac{dx}{\sqrt{(x-e_1)(x-e_2)(x-e_3)}}$$

which with the highly nontrivial change of coordinates

$$x = \frac{(e_3 - \sqrt{(e_3-e_1)(e_3-e_2)})t + (e_3 + \sqrt{(e_3-e_1)(e_3-e_2)}}{t+1} \qquad k = \frac{\sqrt{e_3-e_1} - \sqrt{e_3-e_2}}{\sqrt{e_3-e_2} + \sqrt{e_3-e_2}}$$

we get

$$w_2 = \frac{2}{\sqrt{e_3-e_1} + \sqrt{e_3-e_2}} \int_{-1}^{1} \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}}$$

and taking advantage of the evenness of the integral

$$w_2 = \frac{4}{\sqrt{e_3-e_1} + \sqrt{e_3-e_2}} \int_{0}^{1} \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}}.$$

Similarly we find

$$w_1 = \frac{2i}{\sqrt{e_3-e_1} + \sqrt{e_3-e_2}} \int_{1}^{1/k} \frac{dt}{\sqrt{(t^2-1)(1-k^2t^2)}}$$

and with the substitutions $k' = \sqrt{1-k^2}$ and $t = (1-k'^2u^2)^{-1/2}$ we have

$$w_1 = \frac{2i}{\sqrt{e_3-e_1}+\sqrt{e_3-e_2}}\int_1^{1/k}\frac{dt}{\sqrt{(1-t^2)(1-' k^2t^2)}}.$$

Now, we define the **Elliptic Integral** as follows

$$K(k) = \int_0^1 \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}}$$

and hence our periods become

$$w_1 = \frac{2i}{\sqrt{e_3-e_1}+\sqrt{e_3-e_2}}K(\sqrt{1-k^2}) \qquad w_2 = \frac{4}{\sqrt{e_3-e_1}+\sqrt{e_3-e_2}}K(k).$$

3.3.2 Gauss Arithmetic Geometric Mean

The **Gauss Arithmetic-Geometric Mean** (AMGM for short) can be thought of as a formal combination of the two means. Beginning with two positive real number $a, b \in \mathbb{R}$ we define a_n and b_n by

$$\begin{aligned} a_0 &= a, \quad b_0 = b \\ a_n &= \frac{1}{2}(a_{n-1}+b_{n-1}) \\ b_n &= \sqrt{a_{n-1}b_{n-1}} \end{aligned}$$

Proposition: the main result of the AMGM . Suppose $a \geq b > 0$, then

$$b_{n-1} \leq b_n \leq a_n \leq a_{n-1},$$

$$0 \leq a_n - b_n \leq \frac{1}{2}(a_{n-1}-b_{n-1}).$$

Thus

$$M(a,b) = \lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n$$

exists and if $b \geq 1$ then for all $n \geq 0$,

$$a_{n+m} - b_{n+m} \leq 8\left(\frac{a_n-b_n}{8}\right)^{2^m}.$$

Proof. From the fact that $a_n \geq b_n$ it follows from the basic equality

$$a_n - b_n = \frac{1}{2}(\sqrt{a_{n-1}} - \sqrt{b_{n-1}})^2 \geq 0.$$

From the definition of a_n, since $a_{n-1} \geq b_{n-1}$ then

$$a_n \leq \frac{1}{2}(a_{n-1} + a_{n-1}) = a_{n-1} \quad \text{and} \quad b_n = \sqrt{b_{n-1}b_{n-1}} = b_{n-1}.$$

Also,

$$a_n - b_n = \frac{1}{2}(\sqrt{a_{n-1}} - \sqrt{b_{n-1}})^2 \leq \frac{1}{2}(\sqrt{a_{n-1}} - \sqrt{b_{n-1}})(\sqrt{a_{n-1}} + \sqrt{b_{n-1}}) = \frac{1}{2}(a_{n-1} - b_{n-1}).$$

Therefore, $a_n - b_n \leq (1/2)^n(a - b)$, so $a_n - b_n \to 0$ as $n \to \infty$. Since the a_n's are decreasing and bounded below by the increasing sequence o b_n's it follows that the two sequences converge to the same limit, thus $M(a, b)$ exists. If $b_{n-1} \geq 1$ then $\sqrt{a_{n-1}} + \sqrt{b_{n-1}} \geq 2$, so

$$\frac{a_n - b_n}{8} = \frac{1}{16}\left(\sqrt{a_{n-1}} - \sqrt{b_{n-1}}\right)^2 \leq f116\left(\sqrt{a_{n-1}} - \sqrt{b_{n-1}}\right)^2 \frac{(\sqrt{a_{n-1}} + \sqrt{b_{n-1}})^2}{4} = \left(\frac{a_{n-1} - b_{n-1}}{8}\right)^2.$$

and hence the final inequality follows by induction. □

An interesting application of the AMGM occurs in the next section.

3.3.3 Computing Periods w_1 and w_2

The main computational result is as follows:

Theorem: 6 Suppose E is given by

$$y^2 = rx^3 - g_2x - g_3 = 2(x - e_1)(x - e_2)(x - e_3)$$

with real numbers $e_1 < e_2 < e_3$. Then $\mathbb{Z}\, w_1 + \mathbb{Z}\, w_2$ is a lattice for E, where

$$w_1 = \frac{\pi i}{M(\sqrt{e_3 - e_1}, \sqrt{e_2 - e_1})}$$
$$w_2 = \frac{\pi}{M(\sqrt{e_3 - e_1}, \sqrt{e_2 - e_1})}$$

Proof. Sketch: The use of the AMGM in the calculation was, of course, first discovered by Gauss. If we define the following Elliptic Integral

$$I(a, b) = \int_0^{\pi/2} \frac{d\theta}{\sqrt{a^2 \cos^2\theta + b^2 \sin^2\theta}}$$

then it can be shown with a trig substitution, $u = b\tan\theta$ that and taking limits that

$$I\left(\frac{a+b}{2}, \sqrt{ab}\right) = I(a, b) \qquad I(a, b) = \frac{\pi/2}{M(a, b)}.$$

Moreover, it is easily seen (with the substitution $t = \sin\theta$) that the elliptic integral defined above can be written as

$$K(k) = I(1, \sqrt{1 - k^2}) = I(1 + k, 1 - k).$$

which can be easily put these facts together with previous formulas for w_1 and w_2 to complete the proof sketch.

4 Conclusion

Considering the importance, interest, and prominence of Elliptic Curves in Number Theory, I find the connections between elliptic curves and tori, complex lattices, and the $\wp$-function a enlightening curiosity. I also see the practicality and existence of the AMGM as a tool for computing Elliptic Integrals and periods a real numerical treat. In the future I wish to consider giving more concrete examples of calculations on interesting elliptic curves, and seeing how elliptic curve periods relate to interesting properties of the curves.

References

[1] Gamelin, Theodore W. (2000). “Complex Analysis”, Springer

[2] Knapp, Anthony W. (1992). “Elliptic Curves”, Princeton Univeristy Press.

[3] Koblitz, Neal (1984). “Introduction to Elliptic Curves and Modular Forms”, Springer.

[4] Hosemöller, Dale (2004). “Elliptic Curves”, Springer.

[5] Washington, Larence C. (2008). “Elliptic Curves: Number Theory and Cryptography”, CRC Press.