ELLIPTIC CURVES OVER C

MICHAEL TRAVIS

Abstract. Elliptic curves are an exciting example of mathematics that is at the intersection of numerous fields of study. This paper begins by introducing elliptic curves over **R** but is more concerned with the field of complex numbers, continuing through basic theory to showing that complex tori are isomorphic to complex elliptic curves. I will take a mostly analytic approach, and only a basic knowledge of complex variables and analysis should suffice to understand the material.

Contents

1. What Is An Elliptic Curve?

It is perhaps easiest to begin with the most simple definition of an elliptic curve. The name "elliptic curve" comes from elliptic integrals, which originally arose in order to find the arclength of an ellipse. Let's first consider a general field, K of characteristic not 2, then later consider **R** and **C**. Let $f(x) \in K[x]$ be a cubic polynomial with distinct roots, and x and y in the algebraic closure of K. Then our definition is:

Definition 1.1. An *elliptic curve* is the locus of points satisfying

$$y^2 = f(x) \tag{1.2}$$

We will also add the point at infinity (∞, ∞) to the curve, which will be discussed later. The condition that the roots be distinct is required so that the curve is smooth everywhere. In **R**, elliptic curves generally look like this:

Date: DEADLINE AUGUST 22, 2008.

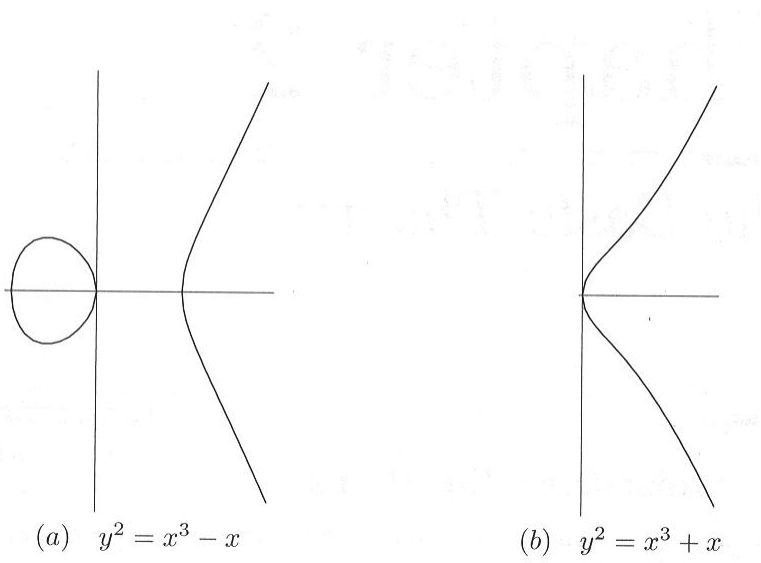

FIGURE 1. Two typical elliptic curves over $\mathbf{R}$

1.1. **The Group Law.** The first interesting results we run into is that the set of points of an elliptic curve (and the point at infinity, recall) coupled with a certain addition creates a group. Consider two points, M_1 and M_2 on an elliptic curve E. If you draw a line through these points, it will intersect the curve at a third point which[1], when reflected about the x-axis, we will call M_3. It isn't geometrically obvious that this method will always yield a third point, but consider that in this addition a point plus another distinct point can equal the original point. In other words, the points need not all be distinct. This process gives the sum of two points on an elliptic curve. In the following figure, $M_1 + M_2 := M_3$:

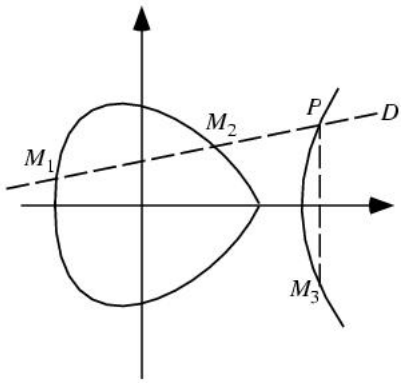

FIGURE 2. The Sum of Two Points on an Elliptic Curve

[1]In the study of algebraic curves, this is a consequence of *Bezout's Theorem*, which states that the number of intersection points of two curves is equal to the product of their degrees

Definition 1.3. For E an elliptic curve in a field of characteristic not 2 or 3, let E be defined as

$$y^2 = x^3 + ax + b$$

Let $M_1 = (x_1, y_1)$ and $M_2 = (x_2, y_2)$ (neither infinity) be on E. Define $M_1 + M_2 = M_3 = (x_3, y_3)$ in one of four cases:
(i) If $x_1 \neq x_2$, then $x_3 = m^2 - x_1 - x_2$, $y_3 = m(x_1 - x_2) - y_1$, where $m = \frac{y_2 - y_1}{x_2 - x_1}$
(ii) If $x_1 = x_2$ but $y_1 \neq y_2$ or $y_1 = y_2 = 0$, then $x_3 = \infty$, $y_3 = \infty$
(iii) If $x_1 = x_2$, $y_1 = y_2 \neq 0$, then $x_3 = m^2 - 2x_1$, $y_3 = m(x_1 - x_3) - y_1$, where $m = \frac{3x_1^2 + a}{2y_1}$
(iv) $M_i + \infty = M_i$ for any M_i

Remark 1.4. The definition of this operation seems quite cumbersome, but understanding the geometric definition described previously is more important. Furthermore, it is beyond the scope of this paper to prove that the set of all points on E together with this addition defines a group, but it is nevertheless worth noting that this is, in fact, an abelian group with ∞ as the identity and $-M = (x, -y)$ as the inverse of M. This inverse is only correct if E is defined as in Definition (1.3). More general elliptic curves aren't so simple.

This is really all the introductory material required to understand elliptic curves over the complex numbers, so let's move straight to it. These new curves should be similarly easy to grasp.

2. Elliptic Curves Over **C**

2.1. **Lattices and the Fundamental Parallelogram.** To understand elliptic curves over the complex numbers, we must first investigate lattices. A **lattice** is the set of all integral linear combinations of two given complex numbers:

Definition 2.1. Let ω_1,ω_2 be two linearly independent (considered as two vectors in $\mathbf{R}^2$) complex numbers such that $\frac{\omega_1}{\omega_2}$ has a positive imaginary part–that is, they're taken clockwise, heuristically speaking. Then the **lattice** L associated with ω_1, ω_2 is defined to be

$$L = \{m\omega_1 + n\omega_2 | m, n \in Z\} \tag{2.2}$$

Associated with each lattice is a **fundamental parallelogram**, Π.

Definition 2.3. The fundamental parallelogram for L and α a complex number[2] is defined as

$$\Pi = \alpha + \{a\omega_1 + b\omega_2 | 0 \leq a \leq 1, 0 \leq b \leq 1\} \tag{2.4}$$

We are interested in functions on $\mathbf{C}/L$, which can be thought of as functions on C with a certain periodicity condition. These are the doubly periodic functions. For the next section, recall that the *Riemann Sphere* is just the complex numbers **C** unioned with the point at infinity, considered to be sitting "on top" (and bottom) of the imaginary axis.

[2]After this definition through the end of the paper, α will be set as equal to 0 without loss of generality

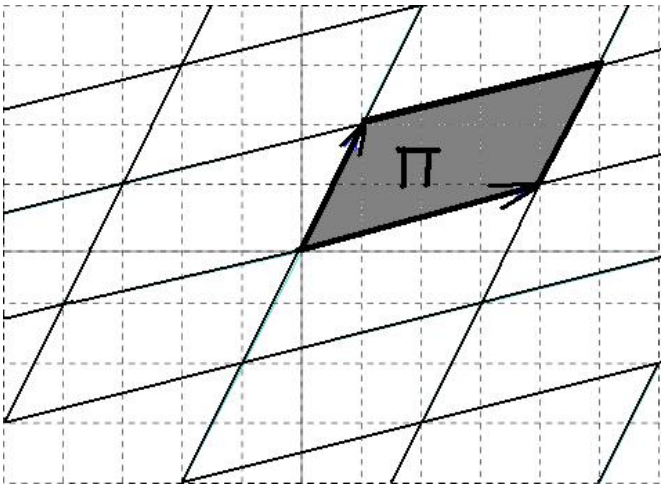

FIGURE 3. The fundamental parallelogram Π of a lattice L is periodic

2.2. **Doubly Periodic Functions.** Given a lattice L and its generating ω_i, we can now define a meromorphic function f from the complex numbers to the Riemann Sphere such that

$$f(z+\omega_i) = f(z);\ z \in \mathbf{C} \tag{2.5}$$

Note that ω_1 and ω_2 are the two periods of this function, hence the name *doubly periodic*. These doubly periodic, meromorphic functions are called **elliptic**, and this term will be used primarily from here on out. This function is defined by its values in Π and opposite sides of the fundamental parallelogram have equal values– to foreshadow things to come–if you think of gluing opposite edges together this fundamental parallelogram can be though of as a torus. These functions have many properties recognizable from complex analysis. The following all assume f, L, and Π to be defined as above.

Theorem 2.6. *If f has no poles on its boundary $\partial\Pi$, then the sum of the residues in Π is 0.*

Proof. By the residue theorem, $2\pi i \sum Res f = \int f$ over $\partial\Pi$. Since f is doubly periodic, the integrals on opposite sides of $\partial\Pi$ cancel and the sum is 0. □

Theorem 2.7. *If f has no poles in the interior of Π, then f is constant.*

Proof. Π is a compact domain, so f is bounded on Π, and since f is doubly periodic f is bounded in all $\mathbf{C}$. By Liouville's theorem, f is thus constant since it is a bounded meromorphic function over $\mathbf{C}$. □

Remark 2.8. An elliptic function can be non-trivial, it simply requires at least two poles (including multiplicity) by the residue theorem.

Theorem 2.9. *If f has no poles or zeroes on the boundary of Π, and $\{a_i\}$ are the singular points of f in Π where f has order m_i at a_i, then $\sum m_i = 0$.*

Proof. If f is elliptic, then so are f' and f'/f. Then by the residue formula for quotient functions we have $0 = \int f'/f = 2\pi i \sum Res f = 2\pi i \sum m_i$. □

Let $\mathbf{C}/L$ denote the quotient of the additive group of complex numbers by the lattice L (a subgroup). A simple group isomorphism from C/L to the unit circle in the complex plane can be given by $f(a+ib) = (e^{2\pi ia}, e^{2\pi ib})$. So far we've learned about basic complex elliptic functions, but have no concrete examples. The following function is just what we need.

2.3. **Weierstrass $\wp$-Function.** The most important example of a non-constant elliptic function in $\mathbf{C}$ is the following curious function defined with respect to L:

$$\wp(z) = \wp(z; L) = \frac{1}{z^2} + \sum_{0 \neq \omega \in L} \left(\frac{1}{z-\omega^2} - \frac{1}{\omega^2}\right) \tag{2.10}$$

The Weierstrass $\wp$-function alone gives rise to many of the most important results of elliptic curves in the complex numbers. We will use it to investigate our most powerful results in elliptic functions. First, let's make sure it's an elliptic function.

Theorem 2.11. *$\wp(z)$ converges absolutely and uniformly on compact sets not intersecting L.*

Lemma 2.12. *$\sum |\omega|^{-k}$ converges if $k > 2$.*

Proof. Let A_n be the annulus defined by $n-1 \leq |z| < n$. Now let $m > 0$ be an integer such that the maximum distance between any two points in Π is less than or equal to d. Then A_n is contained within

$$n - 1 - d \leq |z| \leq n + d \tag{2.13}$$

The area of this annulus is $C \cdot n$ for some C. If k_n is the number of fundamental parallelograms (as in Figure 3) of the lattice L which intersect the annulus A_n, then the number of lattice points in A_n is bounded by k_n. Then for Π, we have the following equation:

$$k_n \cdot (\text{Area of } \Pi) \leq (\text{Area of } 2.13) \leq C_1 \cdot n$$

where $C_1 = C \cdot (\text{Area of } \Pi) > 0$, such that the number of lattice points in $A_n \leq C \cdot n$. Then we have for n less than an arbitrarily large N

$$\sum_{|\omega| \leq N} \frac{1}{|\omega|^k} \ll \sum_1^\infty \frac{n}{n^k} = \sum_1^\infty \frac{1}{n^{k-1}} \tag{2.14}$$

which converges for $k > 2$. □

Proof of Theorem 2.11. Now rewrite the $\wp$-function as one fraction

$$\wp(z) = \frac{z(2\omega - z)}{(z-\omega)^2 (w)^2} \tag{2.15}$$

Now on a compact set C, let $M = \text{Max}\{|z| \ | z \in C\}$ and $|\omega| \geq 2M$. Then $|z - \omega| \geq |\omega|/2$ and $|2\omega - z| \leq 5|\omega|/2$, so we have

$$\left| \frac{1}{z^2} + \sum_{0 \neq \omega \in L} \left(\frac{1}{z-\omega^2} - \frac{1}{\omega^2}\right) \right| = \left| \frac{z(2\omega - z)}{(z-\omega)^2 (w)^2} \right| \leq \frac{M(5|\omega|/2)}{|\omega|^4/4} = \frac{10M}{|\omega|^3} \tag{2.16}$$

By the preceding lemma, this sum converges so the theorem is proven. □

Inspecting our function more carefully, we see that $\wp(z) - (z-\omega)^{-2}$ is continuous for all z except at lattice points $z = \omega_i$, thus $\wp(z)$ is meromorphic with a double pole at each lattice point. Replacing ω by $-\omega$ and z by $-z$ in the equation leaves the sum the same and thus $\wp(z) = \wp(-z)$ so the Weierstrass function is even. Next, we take the derivative (term-by-term)

$$\wp'(z) = -2\sum_{\omega\in L}\frac{1}{(z-\omega)^3} \tag{2.17}$$

The derivative function is doubly periodic since replacing z by $z+\omega_0$ just rearranges the sum and in fact it is odd, which is even easier to spot. Then $\wp'(z)$ is an elliptic function.

Theorem 2.18. *$\wp(z)$ is doubly periodic.*

Proof. We know that the derivative is doubly periodic, so for $i = 1, 2$ we have $\wp'(z+\omega_i) - \wp'(z) = 0$, so therefore $\wp(z+\omega_i) - \wp(z) = C$ for some constant C. Let $z = -\frac{1}{2}\omega_i$ and we have $\wp(\frac{\omega_i}{2}) = \wp(\frac{(\omega_i}{2)}) + C$, but since $\wp$ is even $C = 0$. □

One of the truly superb properties of the Weierstrass function is that it and its derivative generate any and all elliptic functions in $\mathbf{C}$. Since $\wp'(z)$ is odd, for any odd f the product $f \cdot \wp'(z)$ is a new even elliptic function. Then we want to show that any elliptic function f can be represented as a rational function of $\wp$ and $\wp'$ using the fact that any function can be written as the sum of an even and an odd function:

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

Theorem 2.19. *If f is any elliptic function periodic with respect to a lattice L, then f can be expressed as a rational function of $\wp$ and $\wp'$.*

Proof. As described above, it is sufficient to prove that if f is even, it is a rational function of $\wp$. For this proof, we must define a modified fundamental paralellogram with two sides removed, Π'.

$$\Pi' = \{a\omega_1 + b\omega_2 \mid 0 \le a < 1, 0 \le b < 1\} \tag{2.20}$$

Every point in $\mathbf{C}$ differs by a lattice element from exactly one point in Π'. Now, we are interested in the zeroes and poles of f in order to generate a new function in terms of $\wp$, so let's list those in a special way. If 0 is a zero or pole of f, it will be omitted, and each other zero or pole will be listed as many times as its multiplicity.

Suppose that $a \neq 0$ is in Π' and a zero of $f(z)$, but is not half of a lattice point. That is, $a \neq \frac{\omega_1}{2}$, $\frac{\omega_2}{2}$, or $\frac{(\omega_1+\omega_2)}{2}$. Define a^* to be $a^* = \omega_1 + \omega_2 - a$ if a is in the interior of Π', or $a^* = \omega_1 - a$ or $a^* = \omega_2 - a$, respectively, if a is on one of the two sides of Π'. By double periodicity and the evenness of f, if a is a zero of order m, then so is a^*. This is seen because

$$f(a^* - z) = f(-a - z) = f(a + z)$$

and then writing f as a power series implies that a^* is a zero of order m as well. Now suppose a is a zero of $f(z)$ in Π' but is half a lattice point. Without loss of generality, let $a = \frac{\omega_1}{2}$. Then $f(a+z) = f(\frac{1}{2}\omega_1 + z) = a_m z^m +$ higher terms, and $f(\frac{1}{2}\omega_1 - z) = f(-\frac{1}{2}\omega_1 + z) = f(\frac{1}{2}\omega_1 + z)$ by double periodicity and evenness. Thus, the order of the zero m is even. Let a_i be the list of the zeroes of $f(z)$ in Π' which are not half-lattice points, each listed as many times as its multiplicity, but only

one taken from each pair a, a^*. If one of the three possible half-lattice points is a zero, include it in the list half as many times as its multiplicity. Let b_j be the list of nonzero poles of $f(z)$ in Π', counted in the same way as the zeroes so that only "half" of them appear. Since all the elements of these two lists are nonzero, $\wp(a_i)$ and $\wp(b_j)$ are finite and we can define a new elliptic function

$$g(z) = \frac{\prod_i \wp(z) - \wp(a_i)}{\prod_i \wp(z) - \wp(b_j)} \tag{2.21}$$

Then $g(z)$ has the same zeroes and poles of $f(z)$, counting multiplicity. To see this, let's examine the nonzero points in Π'. Since 0 is the only pole in the numerator or denominator of $g(z)$ we have that the zeroes of $g(z)$ come from the zeroes of $\wp(z) - \wp(a_i)$, while the nonzero poles must come from the zeroes of $\wp(z) - \wp(b_j)$. Since $\wp(z) - u$ for a constant u has a double zero at $z = u$ if u is a half-lattice point or a pair of simple zeroes at u and u^*, these are the only zeroes of $\wp(z) - u$ in Π'. Then by construction $f(z)$ and $g(z)$ have the same zeroes and poles with the same orders everywhere in Π' with the possible exception of 0. But since we can choose our α wisely as in (2.3), the point at 0 can be disregarded.

Now then we have that $f(z) = cg(z)$ for some constant c, but by Theorem 2.7 the ratio of two elliptic functions with no poles in the fundamental parallelogram is constant, so $g(z)$ is defined entirely in terms of $\wp(z)$: we have proved the theorem. □

This theorem tells us some useful things about any elliptic function we choose, but let's focus on $\wp'(z)$. Recall from (2.17) that $\wp'(z)$ has a triple pole at 0 and three simple zeroes, so that a corollary of this theorem is that $\wp'(z)^2$ is a cubic polynomial in $\wp(z)$. Now the double zeroes of $\wp'(z)^2$ are $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$, and $\frac{(\omega_1+\omega_2)}{2}$; these are the a_i's. Now calling these e_1, e_2, and e_3, respectively, yields a pretty equation expressible in terms only of a constant C, $\wp(z)$, and the e_i's.

$$\wp'(z)^2 = C(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3) \tag{2.22}$$

Now we want to find what C is. The way to do this is to compare powers of z near the origin, but first recall that $\wp(z) - z^{-2}$ and $\wp'(z) + 2z^{-3}$ are both continuous at the orgin. So the leading term on the left of (2.22) is $(-2z^{-3})^2 = 4z^6$, while on the right it is $C(z^{-2})^3 = Cz^{-6}$, so $C = 4$. Now we can rewrite (2.22) as a more general differential equation:

$$\wp'(z)^2 = f(\wp(z)), \text{where } f(x) = 4(x - e_1)(x - e_2)(x - e_3) \in \mathbf{C}[x] \tag{2.23}$$

Another common way to write this cubic function f is

$$f(x) = 4x^3 - g_2x - g_3. \tag{2.24}$$

The g_i's depend on L but deriving them requires some truly hideous algebra, so one should check my sources for a very in-depth discussion on the subject.

3. Complex Elliptic Curves are Tori

3.1. **Complex Projective Space.** We need one final concept before reaching our ultimate goal of equating elliptic functions with tori. This is the complex projective space, often notated $\mathbf{CP}^n$. We've actually been working in a projective space–the Riemann sphere is $\mathbf{CP}^1$–but now to more precisely give the isomorphism we seek, it is necessary to switch to $\mathbf{CP}^2$.

Definition 3.1. The Complex Projective Plane, $\mathbf{CP}^2$ is a set of equivalence classes $[z_1, z_2, z_3]$ of ordered triples $(z_1, z_2, z_3) \in \mathbf{C}^3 \backslash (0,0,0)$ under the equivalence relation $(z_1, z_2, z_3) \sim (z_1', z_2', z_3')$ if $(z_1, z_2, z_3) = (\lambda z_1, \lambda z_2, \lambda z_3)$ for some nonzero complex λ.

This space is not too hard to visualize. As stated before, $\mathbf{CP}$ is the Riemann sphere. Dividing each z_i by z_3 gives the equivalent coordinates $(\frac{z_1}{z_3}, \frac{z_2}{z_3}, 1)$ for $z_3 \neq 0$ and the point at infinity introduced in the beginning is $(0,1,0)$. Going back to the definition of the group law and the result of Bezout's Theorem, it is perhaps now more clear why a line through any two points will intersect a third point on the curve counting multiplicities.

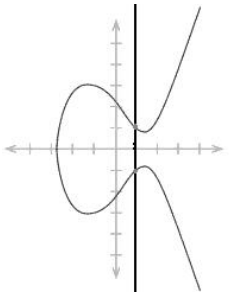

FIGURE 4. The sum of the two intersection points of the line x=1 with the curve is the point at infinity

3.2. **The Isomorphism.** We now have all the tools we need to see that there is an analytic one-to-one correspondence between the complex torus $\mathbf{C}/L$ and $y^2 = 4x^3 - g_2(L)x - g_3(L)$ in $\mathbf{CP}^2$, though I will not prove it. The map that gives this wonderful correspondence can be written as

$$z \mapsto (\wp(z), \wp'(z), 1) \text{ for } z \neq 0;\ 0 \mapsto (0,1,0). \tag{3.2}$$

By our equation (2.24) we know that the image of any nonzero z is in the xy-plane satisfying $y^2 = f(x)$, and the point $z = 0$ maps to the point at infinity. In fact, every x-value except for the e_i's and infinity have exactly two z's such that $\wp(z) = x$. The values $y = \wp'(z)$ coming from these z's are the square roots of $f(x) = f(\wp(z))$. If x_i is a root of $f(x)$, then there is only one z such that $\wp(z) = x_i$ and $y_i = \wp'(z) = 0$ so this map is one-to-one. The inverse map is constructed by taking path integrals from a fixed starting point to a variable endpoint. The integrals change only by a lattice element if the path changes, so the map is well-defined. For more information on this mapping, see one of my sources (or google it).

REFERENCES

[1] Lawrence C. Washington. Elliptic Curves: Number Theory and Cryptography. Chapman & Hall. 2003.
[2] Serge Lang. Complex Analysis, 4th Edition. Springer-Verlag. 1999.
[3] Neil Koblitz. Introduction to Elliptic Curves and Modular Forms, 2nd Edition. Springer-Verlag. 1993.
[4] Joseph H. Silverman. Advanced Topics in the Arithmetic of Elliptic Curves. Springer-Verlag. 1994.