Elliptic Functions
with a view toward elliptic curves

Daniel Hirsbrunner

August 6, 2013

Abstract

An elliptic curve over $\mathbb{C}$ can be described either by an equation of the form $y^2 = x^3 + ax + b$ where a and b are complex constants satisfying $4a^3 + 27b^3 \neq 0$, or as a torus $\mathbb{C}/L$, where L is some lattice. The connection between these two ways of viewing an elliptic curve is explained through the theory of elliptic functions. Some concepts from complex analysis are recalled when needed.

These notes correspond to two talks given by the author on July 18 and 25, 2013, accounting for some helpful comments by Jim Morrow and Jerry Li. The original purpose was to make another project, which exclusively uses the torus form of elliptic curves, less impenetrable. Although that project ran into trouble, this material is still worth presenting, even if only as a demonstration of some beautiful complex analysis.

1 Liouville's Theorems

We give a basic, but non-trivial, introduction to elliptic functions through Joseph Liouville's three theorems about the behavior of a general elliptic function. Before presenting these, we define elliptic functions and two ancillary concepts.

1.1 Definition. A subset $L \subset \mathbb{C}$ is a *lattice* if there exist independent ω_1 and ω_2 such that L can be written as $\{m\omega_1 + n\omega_2 : n, m \in \mathbb{Z}\}$. The *torus* $\mathbb{C}/L$ corresponding to the lattice L is formally the quotient of $\mathbb{C}$ by the additive subgroup L.

The terminology "torus" comes from considering a parallelogram such as P in Figure 1 and identifying the two edges in each pair of opposite edges with one another. A common visualization aid is forming a piece of paper into a cylinder, and then connecting the two boundary circles together.

1.2 Definition. A function $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ is *meromorphic* if $f^{-1}(\infty)$, the set of points where f is infinite, is discrete; f is complex differentiable when restricted to $\mathbb{C} \setminus f^{-1}(\infty)$; and the points in $f^{-1}(\infty)$ are poles of this restriction, rather than essential singularities.

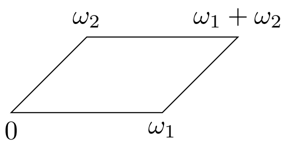

Figure 1: The parallelogram $P = \{\omega_1 t_1 + \omega_2 t_2 : t_1, t_2 \in [0,1]\}$.

The meromorphic functions on $\mathbb{C}$ form a field.

1.3 Definition. A function $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ is an *elliptic function* if it is meromorphic and there exists a lattice L such that $f(z+\omega) = f(z)$ for all $z \in \mathbb{C}$ and all $\omega \in L$. The domain of such a function can also be considered $\mathbb{C}/L$.

The elliptic functions for a given lattice L also form a field.

1.4 Theorem (First Liouville Theorem)**.** If an elliptic function has no poles, then it is constant.

Proof. Let f be such an elliptic function, in which case it is complex differentiable, and therefore continuous, on all of $\mathbb{C}$. A continuous function on the closed bounded region P must be bounded. Since f takes on each of its values at least once in this region, f is bounded on all of $\mathbb{C}$. Finally, Liouville's theorem from complex analysis says that any function that is both complex differentiable on all of $\mathbb{C}$ and bounded must be constant. □

The Liouville's theorem used in the preceding proof is originally due to Augustin–Louis Cauchy, and Liouville's name became attached to it precisely because of his interest in it through Theorem 1.4 [3, 1].

The statement of the next theorem involves residues.

1.5 Definition. The *residue* $\operatorname{Res}(f, z_0)$ of a function f at a pole z_0 is the complex number given by

$$\frac{1}{2\pi i} \oint_\gamma f(z) dz,$$

where γ is a contour that winds once around z_0 counterclockwise and encloses no other poles of f. In complex analysis, it is shown that this is also equal to the coefficient a_{-1} in the series for f around z_0,

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

1.6 Theorem (Second Liouville Theorem)**.** An elliptic function f always has finitely many poles modulo its associated lattice L, and the sum of their residues is zero.

Proof. For the first half, simply note that the intersection of a discrete set with a compact set must be finite. For the second half, consider the parallelogram $Q = \{z_0 + \omega_1 t_1 + \omega_2 t_2 : t_1, t_2 \in [0,1)\}$, where z_0 is chosen so that there are no poles of f on the boundary of Q. By evaluating

$$\oint_{\partial Q} f(z)dz$$

in two different ways, we will show that the sum of the residues of f is zero. First, this integral is the sum of the residues of the poles inside Q due to the residue theorem from complex analysis, and second, it is zero simply due to symmetry. □

1.7 Theorem (Third Liouville Theorem)**.** A non-constant elliptic function f always has the same number of zeros modulo its associated lattice L as it does poles, counting multiplicites of zeros and orders of poles.

Proof. Consider the function f'/f, which is also an elliptic function with associated lattice L. We will evaluate the sum of the residues of this function in two different ways. By Theorem 1.6, this sum is zero, and by the argument principle from complex analysis, it is precisely the number of zeros of f counting multiplicities minus the number of poles of f counting orders. □

1.8 Corollary. A non-constant elliptic function f always takes on every value in $\mathbb{C} \cup \{\infty\}$ the same number of times modulo L, counting multiplicities in the appropriate sense.

Proof. Given a complex value b, consider the function $f - b$. This function is also an elliptic function, and one with the same poles as f. By Theorem 1.6, it therefore has the same number of zeros as f. Thus, f must take on the value b as many times as it does 0. □

1.9 Definition. If $f - b$ in the previous proof has a multiple root, then b is called a *ramification point* of f.

1.10 Corollary. A non-constant elliptic function f always has finitely many ramification points.

Proof. Ramification points correspond to zeros of f', which is also an elliptic function, and therefore has finitely many zeros by Theorems 1.6 and 1.7. □

2 The Weierstrass $\wp$ Function

We explicitly show how to get from the description of an elliptic curve as a torus $\mathbb{C}/L$ to the description as an equation $y^2 = x^3 + ax + b$. The basic idea is to construct an elliptic function whose associated lattice is L, and which satisfies a differential equation that essentially looks like $y^2 = x^3 + ax + b$.

2.1 Definition. The *order* of an elliptic function is the number of poles counting orders, modulo its lattice.

By Theorems 1.6 and 1.7, the order is also the number of zeros counting multiplicities, and also the number of times any other value is taken on, accounting for ramification points.

What do elliptic functions of low orders look like? An elliptic function has order 0 if and only if it is a constant function, according to Theorem 1.4. Next, there are no elliptic functions of order 1, since that would entail having a residue that is both zero because of Theorem 1.6 and non-zero because it's at a pole of order one. For order 2, there are two possibilities— one pole of order 1 with residue 0 or two poles of order 1 with residues that are additive inverses of one another. By Mittag-Leffler's theorem, functions satisfying both cases exist.

For the first case, it is tempting to guess

$$\sum_{\omega \in L} \frac{1}{(z-\omega)^2},$$

but this series is neither absolutely nor uniformly convergent on compact subsets of $\mathbb{C} \setminus L$, which means it is not necessarily periodic nor meromorphic. This guess can be salvaged by introducing some correcting terms, and in fact this is what Weierstrass himself did [2]. The correcting terms are analogous to those found in the partial fraction decompositions of functions such as the secant.

2.2 Definition. The *Weierstrass $\wp$ function* with associated lattice L is given by the following equation for $z \notin L$:

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in L \setminus \{0\}} \left[\frac{1}{(z-\omega)^2} + \frac{1}{\omega^2} \right].$$

2.3 Theorem. The Weierstrass $\wp$ function is an even elliptic function.

Proof. It can be shown that the series is absolutely convergent and that the series is uniformly convergent on compact subsets of $\mathbb{C} \setminus L$. One method uses estimation techniques from analysis and comparison with an integral. Absolute convergence shows that the function is even, since replacing z with $-z$ simply rearranges the terms. Uniform continuity shows that the function is meromorphic, since the individual terms are meromorphic.

For periodicity on L, we first look at the derivative,

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

which is clearly periodic. We know that $\wp(z)$ and $\wp(z+\omega_1)$ differ by a constant because they have the same derivative, and this constant can be seen to be 0 by taking $z = \frac{1}{2}\omega_1$. Repeating this with ω_2 completes the proof. □

2.4 Definition. The *Eisenstein series* with associated lattice L is given by the following equation for integers $n \geqslant 3$:

$$G_n = \sum_{\omega \in L \setminus \{0\}} \omega^{-n}.$$

2.5 Theorem ([2, V.2.11])**.** The power series for $\wp$ centered at the origin is

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

Proof. Using Taylor's theorem on $\wp(z) - z^{-2}$ gives the following coefficients:

$$c_n = \frac{f^n(0)}{n!} = (-1)^n \frac{(n+1)!}{n!} \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega^{n+2}},$$

and those with an odd index are known to be zero because $\wp$ is even. □

The region of convergence of this series is the largest disk centered at the origin that does not contain any lattice points, with the origin removed.

2.6 Theorem (Representation Theorem, [2, V.3.1–3])**.** Every elliptic function can be written as $R(\wp) + \wp' S(\wp)$ for some rational functions R and S.

Proof. We divide the proof into three cases of increasing generality.

1. If f is an even elliptic function whose poles are contained in L, then f can be written as polynomial in $\wp$ in the following way. Use the series expansions $f(z) = a_{-2n} z^{-2n} + \cdots$ and $\wp(z) = z^{-2} + \cdots$ to see that $f - a_{-2n}\wp^n$ is an elliptic function with strictly smaller order than f. Repeat this process on the new elliptic function until the order is reduced to zero.

2. If f is an even elliptic function with arbitrary poles, then f can be written as a rational function of $\wp$ in the following way. For each pole $z_j \notin L$, consider the map $z \mapsto f(z)(\wp(z) - \wp(z_j))^{N_j}$, where N_j is an integer large enough to remove the pole at z_j. Doing this for each pole $z_j \notin L$ leads to an elliptic function whose poles are contained in L, namely

$$f(z) \prod_j (\wp(z) - \wp(z_j))^{N_j}.$$

Part (1) shows that this new elliptic function can be written as a polynomial in $\wp$, and dividing by the product explicitly gives f as a rational function of $\wp$.

3. If f is a completely arbitrary elliptic function, then it can be written as $R(\wp) + \wp' S(\wp)$ for some rational functions R and S in the following way. In general, any function $\mathbb{C} \to \mathbb{C}$ can be decomposed into its even and odd parts as

$$\begin{aligned} f(z) &= f_{\text{even}}(z) + f_{\text{odd}}(z) \\ &= \tfrac{1}{2}(f(z) + f(-z)) + \tfrac{1}{2}(f(z) - f(-z)). \end{aligned}$$

So we have $f_{\text{even}} = R(\wp)$ by part (2), and we want $f_{\text{odd}} = \wp' S(\wp)$. Since f_{odd} and $\wp'$ are both even functions, their quotient is even, and therefore can be given as $S(\wp)$. □

This theorem has analogues in the theory of Fourier series.

2.7 Theorem (Differential Equation for $\wp$, [2, V.3.4])**.** The $\wp$ function satisfies

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

where g_2 and g_3 are complex constants depending on the lattice.

Proof. We apply the algorithm described in part (1) of the proof of Theorem 2.6 to the elliptic function $(\wp'(z))^2$, and we start by listing all the necessary ingredients.

$$\begin{aligned} \wp(z) &= z^{-2} + 3G_4z^2 + 5G_6z^4 + \cdots \\ \wp'(z) &= -2z^{-3} + 6G_4z + 20G_6z^3 + \cdots \\ (\wp(z))^2 &= z^{-4} + 6G_4 + 10G_6z^2 + \cdots \\ (\wp(z))^3 &= z^{-6} + 9G_4z^{-2} + 15G_6 + \cdots \\ (\wp'(z))^2 &= 4z^{-6} - 24G_4z^{-2} - 80G_6 + \cdots \end{aligned}$$

Clearly subtracting $4(\wp(z)^3)$ from $(\wp'(z))^2$ will give an elliptic function with lower order,

$$(\wp'(z))^2 - 4(\wp(z)^3) = -60G_4z^{-2} - 140G_6 + \cdots,$$

and then adding $60G_4\wp(z)$ will give an elliptic function with order zero,

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

Since the right-hand side is an elliptic function with no poles, it is constant, and therefore equal to simply $-140G_6$. Taking $g_2 = 60G_4$ and $g_3 = 140G_6$ completes the proof. □

This proves one direction between the two representations of elliptic curves. The other direction is much more difficult to prove and amounts to showing that g_2 and g_3 can be specified arbitrarily, as long as $g_2^3 \neq 27g_3^2$. See [5, §21·73].

Furthermore, not all meromorphic functions satisfy an algebraic differential equation such as this. One well known example is the gamma function Γ, and the proof of that is originally due to Otto Hölder in 1887.

There is much more to the theory of elliptic functions, so we conclude by stating some further theorems without proof.

2.8 Theorem (Addition Theorem, [2, V.4.1])**.** For any $z, w \notin L$,

$$\wp(z+w) = \frac{1}{4}\left(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)}\right)^2 - \wp(z) - \wp(w).$$

This addition of inputs to $\wp$ corresponds to the addition of points on an elliptic curve. Also, the addition theorems of elliptic functions are analogous to those for circular functions. The first instance of such a theorem was discovered by Fagnano in 1718, and this was generalized somewhat by Leonhard Euler in 1751 [4, 12.5].

2.9 Theorem ([2, V.4.4])**.** If $x + y + z = 0$, then

$$\begin{vmatrix} \wp(x) & \wp'(x) & 1 \\ \wp(y) & \wp'(y) & 1 \\ \wp(z) & \wp'(z) & 1 \end{vmatrix} = 0.$$

This implies Theorem 2.8, but is not implied by it.

2.10 Theorem (Abel's Existence Theorem, [2, V.6.1])**.** There exists an elliptic function with a prescribed lattice, poles, and zeros if and only if the sum of the orders of the poles is equal to the sum of the multiplicities of the zeros, both modulo the lattice.

References

[1] Cauchy, Augustin–Louis. *Mémoires sur les fonctions complémentaires.* Œuvres complètes d'Augustin Cauchy, 1882.

[2] Freitag, Eberhard, Rolf Busam. *Complex Analysis.* Springer, 2009.

[3] Liouville, Joseph. *Leçons sur les fonctions doublement périodiques.* Journal für die Reine und Angewandte Mathematik, 1879.

[4] Stillwell, John. *Mathematics and its History.* Springer, 2010.

[5] Whittaker, E. T., G. N. Watson. *A Course of Modern Analysis.* Cambridge, 1963.