UNIFORMIZATION THEOREM FOR ELLIPTIC CURVES OVER $\mathbb{C}$

PETER S. PARK

1. Introduction

Every lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subset \mathbb{C}$ (with ω_1, ω_2 linearly independent over $\mathbb{R}$) corresponds to an elliptic curve

$$E_\Lambda : y^2 = 4x^3 - g_2 x - g_3,$$

where

$$g_2 = 60G_4(\Lambda) = 60 \sum_{\omega \in \Lambda^*} \frac{1}{\omega^4} \quad \text{and} \quad g_3 = 140G_6(\Lambda) = 140 \sum_{\omega \in \Lambda^*} \frac{1}{\omega^6}, \tag{1.1}$$

(in the above expressions, Λ^* denotes $\Lambda \setminus \{0\}$). This correspondence is given by the biholomorphic mapping $\varphi : \mathbb{C}/\Lambda \to E_\Lambda(\mathbb{C})$ defined by

$$\varphi(z) = \begin{cases} [\wp(z), \wp'(z), 1] & \text{if } z \notin \Lambda \\ [0, 1, 0] & \text{if } z \in \Lambda, \end{cases} \tag{1.2}$$

where

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda^*} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) \tag{1.3}$$

is the Weierstrass $\wp$-function for Λ. Moreover, φ is a group isomorphism. For detailed proofs of these facts, see [3, Sections 6.1-6.4], and for an overview of the theory of elliptic functions (of which $\wp(z)$ is one), see [1, Chapter 7] or [9, Chapter 9].

In this exposition[1], we consider the converse problem. Any elliptic curve over $\mathbb{C}$ can, after a linear change of variables, be written in the form $E : y^2 = 4(x-a)(x-b)(x-c)$, with $a, b, c \in \mathbb{C}$ distinct. By another linear change of variables, we can further assume that $a + b + c = 0$, i.e., that the x^2 term vanishes from the right hand side. For such an elliptic curve E, does there exist a lattice Λ such that the correspondence described above associates Λ to E?

A simple application of the uniformization theorem for Riemann surfaces shows that this is indeed the case. In this exposition, however, we will take a lengthier and more productive approach to proving this converse result, which we call *the uniformization theorem for elliptic curves over* $\mathbb{C}$. First, we will obtain explicit formulas for the generators ω_1 and ω_2 of our desired lattice Λ. Then, we will derive an expression for what is essentially the inverse of $\wp(z)$, the Weierstrass $\wp$-function for the lattice Λ we have constructed. This will allow us to show that $\wp$ satisfies the differential equation $\wp'^2 = 4(\wp - a)(\wp - b)(\wp - c)$, which shows that Λ indeed does give rise to our elliptic curve E by the correspondence described above.

For an intuitive sketch of our strategy, let us suppose that we have constructed a lattice Λ that corresponds to E. Then, $p = \wp(z)$ associated to Λ must satisfy

$$\left(\frac{dp}{dz} \right)^2 = 4(p-a)(p-b)(p-c)$$

[1]This exposition is based on Sections 6.5-6.8 of [3]. For other proofs of the uniformization theorem for elliptic curves over $\mathbb{C}$, see [2, Theorem 2.9], [4, I.3.13], [5, VII Proposition 5], [6, Section 4.2], or [7, I.4.3]; this selection of references is from [8, VI.5.1].

$$\frac{1}{2\sqrt{(p-a)(p-b)(p-c)}}\,dp = dz$$

$$z(w) = \int^{w} \frac{1}{2\sqrt{(p-a)(p-b)(p-c)}}\,dp. \tag{1.4}$$

An integral of this form is called an *elliptic integral of the first kind*. We wish to show that (1.4), which should essentially be $\wp^{-1}$, has a locally defined inverse that extends to a global meromorphic function, which must then essentially be $\wp$.

In order to accomplish this, however, we have to be precise about the definition of (1.4). Our first concern is that the integrand of (1.4) is double-valued, since one has to choose from two branches of the square root. Thus, in order to make (1.4) well-defined, we need to analytically continue a chosen determination of the square root to a global meromorphic function on a compact Riemann surface that is essentially the elliptic curve E. To this end, we will present an overview of the theory of analytic continuation in Section 2, then use this theory to make (1.4) well-defined in Section 3, where we construct the compact Riemann surface on which we will be integrating.

Our second concern is that the choice of the path of integration in (1.4) affects the value of the integral. However, we will show in Section 4 that different values of the integral arising from different choices of the path (with the same endpoints) will in fact be equal modulo some lattice Λ, which makes the integral well-defined in $\mathbb{C}/\Lambda$ as needed. Finally, in Section 5, we show that (1.4) has a global inverse that is essentially $\wp$, which by our previous discussion completes the proof of the uniformization theorem for elliptic curves over $\mathbb{C}$.

2. Overview of Analytic Continuation

For $\xi \in \mathbb{C}$, let a *function element at* ξ be an analytic function on an open disc centered at $z = \xi$. In this section, we will define the notion of an analytic continuation of a function element along a path. To this end, let f be a function element at $\xi_0 \in \mathbb{C}$, and let its Taylor series expansion at $z = \xi_0$ be given by

$$f(z) = \sum_{j=0}^{\infty} a_j (z-\xi_0)^j \qquad \text{for } |z-\xi_0| < r(\xi_0), \tag{2.1}$$

where $r(\xi_0)$ denotes the (maximal) radius of convergence of the Taylor series of f at ξ_0.

Suppose $\xi_1 \in \mathbb{C}$ is contained in the disc $|z-\xi_0| < r(\xi_0)$, so that the disc

$$|z-\xi_1| < r(\xi_0) - |\xi_1 - \xi_0|$$

is contained in the disc $|z-\xi_0| < r(\xi_0)$. Then, one can take the derivatives of $f(z)$ at $z = \xi_1$ to obtain the Taylor series expansion at that point.

$$f(z) = \sum_{j=0}^{\infty} b_j (z-\xi_1)^j \tag{2.2}$$

In fact, we can explicitly compute the Taylor coefficients b_j by using the relation

$$(z-\xi_0)^j = \left((z-\xi_1) + (\xi_1 - \xi_0)\right)^j,$$

which we can substitute into (2.1) and rearrange into a power series in $z - \xi_1$. It follows that (2.2) is a convergent power series with radius of convergence at least $r(\xi_0) - |\xi_1 - \xi_0|$.

We say that a second function element g at ξ_1 is a *direct analytic continuation* of a given function element f at ξ_0 if $|\xi_1 - \xi_0| < r(\xi_0)$ and if the Taylor series for g arises from rearranging the series of f at $z = \xi_1$ (i.e., if the Taylor coefficients of g are precisely b_j, in the above language). It may be the case that the radius of convergence $r(\xi_1)$ of the second function element g is larger than the

immediate lower bound of $r(\xi_0) - |\xi_1 - \xi_0|$. In fact, this is precisely the case of interest, because this permits the notion of analytic continuation along a path.

Let f be a function element at ξ_0, and let $C = \{C(t) : t \in [T_0, T_1]\} \in \mathbb{C}$ be a path from ξ_0 to ξ_1. A function element g at ξ_1 is an *analytic continuation of f along C* if there exists a partition

$$T_0 = t_0 < t_1 < \cdots < t_k = T_1$$

and function elements f_j on open discs D_j centered at $C(t_j)$ (respectively) for $0 \leq j \leq k$, such that

(1) $f_0 = f$
(2) $f_k = g$
(3) $C([t_{j-1}, t_j]) \subset D_{j-1}$ for $1 \leq j \leq n$
(4) f_j is a direct analytic continuation of f_{j-1} for $1 \leq j \leq n$.

Example 2.1. Let C denote the unit circle $C(t) = e^{it}$ for $t \in [0, 2\pi]$. Consider the function element $f(z) = \sqrt{z}$ (for one of the two choices of the branch of the square root) on the disc $|z - 1| < 1$. One can then check that the function element $-f$ on the same disc $|z - 1| < 1$ is an analytic continuation of f along C; indeed, the discs of the analytic continuation can be taken to be the unit discs centered at $e^{j\pi i/2}$ for $0 \leq j \leq 4$.

Analytic continuation respects translation and multiplication, so we can generalize the above observation in the following way. Let $\xi \in \mathbb{C}$ and C be a loop with winding number 1 about ξ. Let g be a function element on a disc $D \subset \mathbb{C}$ (centered at the base point of C) that can be analytically continued along C to itself. Then, if there exists a function element $f(z) = \sqrt{z - \xi}$ on D (where we take one of the two possible choices of the square root), it follows from above that $-fg$ is an analytic continuation of fg along C. This fact will be used a number of times throughout our proof.

The following are basic facts about analytic continuation that will be useful in our proof.

Proposition 2.2. *Let f be a function element at $\xi_0 \in \mathbb{C}$, and let C be a path from ξ_0 to $\xi_1 \in \mathbb{C}$. Suppose function elements g and h at ξ_1 are analytic continuations of f along C. Then, the Taylor expansions of g and h at $z = \xi_1$ are equal (i.e.: have the same coefficients).*

Proof. See [3, Proposition 6.20]. □

Proposition 2.3. *Let f be a function element at $\xi_0 \in \mathbb{C}$, and let C be a path from ξ_0 to $\xi_1 \in \mathbb{C}$. Suppose g is a function element at ξ_1 that is an analytic continuation of f along C. Then, f is an analytic continuation of g along the opposite path C^{-1}.*

Proof. See [3, Proposition 6.22]. □

Proposition 2.4. *Let $\xi_0, \xi_1 \in \mathbb{C}$, and let $C = \{C(t) : t \in [T_0, T_1]\}$ be a path from ξ_0 to ξ_1. Let f be a function element at ξ_0, and suppose that g is a function element at ξ_1 that is an analytic continuation of f along C. Then, there exists $\varepsilon > 0$ such that the following holds: for any path $C' = \{C'(t) : t \in [T_0, T_1]\}$ from ξ_0 to ξ_1 such that $C'(t)$ is within ε of $C(t)$ for all $t \in [T_0, T_1]$, g is an analytic continuation of f along C.*

Proof. See [3, Proposition 6.21]. □

3. The Riemann Surface of the Integrand

In this section, we would like to make $\sqrt{(z-a)(z-b)(z-c)}$ globally well-defined in some sense, but this is impossible when the domain is $\mathbb{C} \setminus \{a, b, c\}$. Indeed, given $z_0 \in \mathbb{C} \setminus \{a, b, c\}$ and a choice of square root $q_0 = \sqrt{(z_0 - a)(z_0 - b)(z_0 - c)}$ (among two possible choices), $\sqrt{(z-a)(z-b)(z-c)}$ can be extended to an analytic function on at least any disc $D_0 \subset \mathbb{C} \setminus \{a, b, c\}$ about z_0 (in fact, on any simply connected open set); however, it follows from our discussion in Example 2.1 that this ceases to be true if the domain contains a path that has winding number 1 about a, b, or c.

To remedy this problem, we construct a double covering $\mathcal{R}$ of $\mathbb{C} \setminus \{a, b, c\}$ such that roughly speaking, $\sqrt{(z-a)(z-b)(z-c)}$ extends to a well-defined analytic function on all of $\mathcal{R}$. Then, we compactify $\mathcal{R}$ by adding four points α, β, γ, and ∞ that are the respective preimages of a, b, c, and ∞; we denote the new compact space as $\mathcal{R}^*$. It turns out that $\mathcal{R}^*$ is a compact Riemann surface, and also that roughly speaking, $\sqrt{(z-a)(z-b)(z-c)}$ extends to be a global meromorphic function on $\mathcal{R}^*$ with simple zeros at α, β, and γ and an order 3 pole at ∞.

For $z_0 \in \mathbb{C} \setminus \{a, b, c\}$, consider a loop $C \subset \mathbb{C} \setminus \{a, b, c\}$ based at z_0. If C is piecewise smooth, then denoting its winding numbers about each of a, b, c as

$$n(C, a) = \frac{1}{2\pi i} \oint \frac{dz}{z-a}, \qquad n(C, b) = \frac{1}{2\pi i} \oint \frac{dz}{z-b}, \quad \text{and} \quad n(C, c) = \frac{1}{2\pi i} \oint \frac{dz}{z-c},$$

we define its *total winding number* (about a, b, and c) by

$$n(C) = n(C, a) + n(C, b) + n(C, c).$$

Even if C is not piecewise smooth, it is evident that all piecewise smooth loops that are sufficiently close uniformly to C must have the same total winding number as each other, and we define this to be $n(C)$ in this case. Homotopic loops based at z_0 share the same total winding number, so $n : \pi_1(\mathbb{C} \setminus \{a, b, c\}, z_0) \to \mathbb{Z}$ is a group homomorphism. As generators for $\pi_1(\mathbb{C} \setminus \{a, b, c\}, z_0)$, we can take simple piecewise smooth loops $\Gamma_a, \Gamma_b, \Gamma_c$ in $\mathbb{C} \setminus \{a, b, c\}$ based at z_0 that pairwise intersect only at z_0 and that satisfy

$$\begin{aligned} n(\Gamma_a, a) &= 1, \qquad & n(\Gamma_a, b) &= n(\Gamma_a, c) = 0 \\ n(\Gamma_b, b) &= 1, \qquad & n(\Gamma_b, c) &= n(\Gamma_b, a) = 0 \\ n(\Gamma_c, c) &= 1, \qquad & n(\Gamma_c, a) &= n(\Gamma_c, b) = 0. \end{aligned}$$

Since $n(\Gamma_a) = n(\Gamma_b) = n(\Gamma_c) = 1$, we note that $n(\cdot)$ is in fact surjective onto $\mathbb{Z}$. Thus, the *subgroup of even total winding number*, defined by

$$H = \{C \in \pi_1(\mathbb{C} \setminus \{a, b, c\}, z_0) : n(C) \in 2\mathbb{Z}\}, \tag{3.1}$$

has index 2. The following generators for H will be useful in our main proof.

Proposition 3.1. *The subgroup H defined in (3.1) is generated by the equivalence classes of $\Gamma_a^2, \Gamma_b^2, \Gamma_c^2, \Gamma_1$, and Γ_2, where*

$$\Gamma_1 = \Gamma_a \Gamma_b \qquad \text{and} \qquad \Gamma_2 = \Gamma_b \Gamma_c.$$

Proof. An arbitrary $C \in H$ can be written as a word in $\Gamma_a, \Gamma_b, \Gamma_c$, and their inverses, such that the number of factors in the word is even. So, it suffices to show that every pair made from these factors is generated by $\Gamma_a^2, \Gamma_b^2, \Gamma_c^2, \Gamma_1$, and Γ_2. This is immediate for $\Gamma_a^2, \Gamma_b^2, \Gamma_c^2, \Gamma_a\Gamma_b$, and $\Gamma_b\Gamma_c$, and we further have

$$\begin{aligned} \Gamma_b\Gamma_a &= \Gamma_b^2(\Gamma_a\Gamma_b)^{-1}\Gamma_a^2 \\ \Gamma_c\Gamma_b &= \Gamma_c^2(\Gamma_b\Gamma_c)^{-1}\Gamma_b^2 \\ \Gamma_a\Gamma_c &= (\Gamma_a\Gamma_b)(\Gamma_b^2)^{-1}(\Gamma_b\Gamma_c) \\ \Gamma_c\Gamma_a &= \Gamma_c^2(\Gamma_b\Gamma_c)^{-1}(\Gamma_b)^2(\Gamma_a\Gamma_b)^{-1}\Gamma_a^2. \end{aligned}$$

Finally, note that the remaining pairs are precisely the ones with at least one inverse factor. For these, note that if the left symbol of the pair is $\Gamma_\square^{-1}$ for $\square \in \{a, b, c\}$, then attaching $\Gamma_\square^2$ to the left of the pair results in a new pair where $\Gamma_\square^{-1}$ is replaced with $\Gamma_\square$. We apply an analogous process if the right symbol of the pair is an inverse. The resulting pair is among the above pairs that

we have already shown to be generated by our choice of five generators. This overall proves our proposition. □

Let $\mathcal{R}$ be the covering space of $\mathbb{C} \setminus \{a, b, c\}$ associated to H, and let $e : \mathcal{R} \to \mathbb{C} \setminus \{a, b, c\}$ be the covering map. $\mathcal{R}$ can naturally be given the structure of a Riemann surface. To this end, consider an arbitrary open disc $D \subset \mathbb{C} \setminus \{a, b, c\}$. Then, D is simply connected, so it is evenly covered. Thus, $e^{-1}(D)$ is a disjoint union of two open sets $\Delta_1 \cup \Delta_2$ that are each homeomorphic to D by the map e. For each $j \in \{1, 2\}$, we can take e as a local coordinate in Δ_j, making (e, Δ_j) a chart. So $\mathcal{R}$ is a Riemann surface, although it is noncompact.

We will eventually complete $\mathcal{R}$ into a compact Riemann surface $\mathcal{R}^*$. Note that we will use Greek letters to denote points in $\mathcal{R}$ (and later, in $\mathcal{R}^*$), and we will use their Latin counterparts to denote the point in $\mathbb{C}$ to which e maps the point denoted by the Greek letter. For example, for a point ζ in $\mathcal{R}$ (or in $\mathcal{R}^*$), we will denote $e(\zeta) = z \in \mathbb{C}$.

Recall that we have fixed a base point $z_0 \in \mathbb{C}$. Adhering to the convention set above, fix a base point $\zeta_0 \in \mathcal{R}$ so that $e(\zeta_0) = z_0$ (there are two possible choices). Let $D_0 \subset \mathbb{C} \setminus \{a, b, c\}$ be a disc centered at z_0, and let Δ_0 be the component of $e^{-1}(D)$ that contains ζ_0. Recall from the beginning of the section that $\sqrt{(z-a)(z-b)(z-c)}$ is an analytic function on D_0 such that $\sqrt{(z_0-a)(z_0-b)(z_0-c)} = q_0$, where q_0 is the choice of the square root we have taken. We will now show that this function can be analytically continued to be well-defined on the whole space $\mathcal{R}$.

Proposition 3.2. *There exists a unique analytic function $F : \mathcal{R} \to \mathbb{C}$ such that $F(\zeta_0) = q_0$ and the following holds: for any $\zeta_1 \in \mathcal{R}$, any path $C \subset \mathcal{R}$ from ζ_0 to ζ_1, and any open disc $D \subset \mathbb{C} \setminus \{a, b, c\}$ containing $z_1 = e(\zeta_1)$, if e^{-1} is regarded as a map from D to the component Δ of $e^{-1}(D)$ that contains ζ_1, then $(F \circ e^{-1}, D)$ is an analytic continuation of*

$$(\sqrt{(z-a)(z-b)(z-c)}, D_0) \tag{3.2}$$

along $e(C)$.

Proof. $\mathcal{R}$ is path-connected, so uniqueness immediately follows from Proposition 2.2. So, it suffices to prove existence. Let f_0 be the function element (3.2). f_0 can clearly be analytically continued along any path $C' \subset \mathbb{C} \setminus \{a, b, c\}$, since $f_0(z)^2$ extends to a globally defined analytic function on $\mathbb{C} \setminus \{a, b, c\}$, and squaring is preserved by analytic continuation. Let function element f_1 on a disc D_1 centered at z_1 be an analytic continuation of f_0 along $e(C)$, and let Δ_1 be the component of $e^{-1}(D_1)$ that contains ζ_1. Using the local inverse $e^{-1} : D_1 \to \Delta_1$, we can define an analytic function $F = f_1 \circ e^{-1}$ on Δ_1.

It now suffices to show that F is well-defined, since then it is immediately a global analytic function with the desired properties. To this end, let $C^\#$ be another path from ζ_0 to ζ_1, and let $f_1^\#$ denote a function element at z_1 that is an analytic continuation of f_0 along $e(C^\#)$. We will show that f_1 and $f_1^\#$ have the same Taylor expansions at z_1, which will prove that F does not depend on the choice of path from ζ_0 to ζ_1.

It follows from our discussion in Example 2.1 that for any $\square \in \{a, b, c\}$, the analytic continuation of f_0 along the loop $\Gamma_\square$ yields $-f_0$. So, the analytic continuation of f_0 along a loop $\gamma \subset \mathbb{C} \setminus \{a, b, c\}$ yields $(-1)^{n(\gamma)} f_0$. Note that $CC^{\#-1}$ is a loop in $\mathcal{R}$ based at ζ_0, so $e(CC^{\#-1}) = f_0$. Since analytic continuation of f_0 along $e(C)$ yields f_1, it follows that analytic continuation of f_1 along $e(C^{\#-1}) = e(C^\#)^{-1}$ yields f_0. We can apply Proposition 2.3 to see that analytic continuation of f_0 along $e(C^\#)$ yields f_1. Then, by Proposition 2.2, the Taylor expansions of f_1 and $f_1^\#$ at $z = z_1$ are equal, thus proving that F is well-defined.

□

We now construct a compact Riemann surface $\mathcal{R}^*$ by adding to $\mathcal{R}$ four additional points: α, β, γ, and ∞. Concordantly, we extend our map e by defining $e(\alpha) = a, e(\beta) = b, e(\gamma) = c$, and $e(\infty) = \infty$,

so that $e : \mathcal{R}^* \to \mathbb{C} \cup \{\infty\}$. To endow $\mathcal{R}$ with a topology, we let it inherit the topology of our original noncompact $\mathcal{R}$, and additionally define the following basic open discs. A basic open disc of α is given precisely by $\{\alpha\} \cup e^{-1}(D_a^\times)$, where $D_a^\times \subset \mathbb{C} \setminus \{a, b, c\}$ is a punctured disc centered at a. The basic open discs of β and γ are defined analogously. Finally, a basic open disc of ∞ is given precisely by $\{\infty\} \cup (D_\infty^\times)$, where $D_\infty^\times \subset \mathbb{C} \setminus \{a, b, c\}$ is of the form $\{z > R\}$ for some $R \geq \max\{|a|, |b|, |c|\}$. Under this topology, one sees that our new $\mathcal{R}^*$ is a Hausdorff regular space with a countable basis, and thus a separable metric space. Furthermore, $\mathcal{R}^*$ is sequentially compact, and thus compact. Note that with this notation, it makes sense to write the function F defined in Proposition 3.2 as

$$F(z) = \sqrt{(\zeta - \alpha)(\zeta - \beta)(\zeta - \gamma)}. \tag{3.3}$$

We now give $\mathcal{R}^*$ the structure of a (compact) Riemann surface. Since we have already defined charts for $\mathcal{R}$, it suffices to construct compatible charts about α, β, γ, and ∞. Consider a basic open disc of α given by $\{\alpha\} \cup e^{-1}(D_a^\times)$ for some punctured disc $D_a^\times \subset \mathbb{C} \setminus \{a, b, c\}$ centered at a. Recall that $e^{-1}(D_a^\times)$ is a two-to-one cover of $D_a^\times$. Moreover, for a point $z \in D_a^\times$, the lift of a loop with base point z and winding number 1 around a is not a loop, but in fact a path from one of the two preimage points of z to the other. So, $e^{-1}(D_a^\times)$ is connected, which shows that it is a covering space of $D_a^\times$ for the map e. By an argument analogous to the proof of Proposition 3.2, we can define a function $\sqrt{\zeta - \alpha}$ on $e^{-1}(D_a^\times)$ so that $\sqrt{e^{-1}(z) - \alpha}$ is an analytic continuation of $\sqrt{z - a}$ (where the square root is taken to be consistent with the earlier choice of $\sqrt{\zeta_0} = z_0$).

Naturally, we define $\sqrt{\zeta - \alpha} = 0$ for $\zeta = \alpha$. This ensures that $\sqrt{\zeta - \alpha}$ is continuous in $e^{-1}(D_a^\times)$. Moreover, $\sqrt{\zeta - \alpha}$ maps small open discs to open sets, so it is an open map. I further claim that it is injective. Indeed, suppose that $\sqrt{\zeta_1 - \alpha} = \sqrt{\zeta_2 - \alpha}$. Then, we have $z_1 - a = z_2 - a$, so $z_1 = z_2$, i.e., ζ_1 and ζ_2 lie over the same point z. If $z = a$, then $\zeta_1 = \zeta_2 = \alpha$. On the other hand, if $z \neq a$, then $\sqrt{\zeta - \alpha}$ takes on distinct nonzero values (differing by a factor of -1) at the two preimage points of $e^{-1}(z)$, so $\sqrt{\zeta_1 - \alpha} = \sqrt{\zeta_2 - \alpha}$ implies that $\zeta_1 = \zeta_2$. Since $\sqrt{\zeta - \alpha}$ is a continuous, open, and injective map into $\mathbb{C}$, we have that $(\sqrt{\zeta - \alpha}, \{\alpha\} \cup e^{-1}(D_a^\times))$ is a chart, one that can easily be seen to be compatible with the charts on $\mathcal{R}$. By a similar argument as above, we can define compatible charts $(\sqrt{\zeta - \beta}, \{\beta\} \cup e^{-1}(D_b^\times))$ and $(\sqrt{\zeta - \gamma}, \{\gamma\} \cup e^{-1}(D_c^\times))$.

We are left with the task of defining a chart about ∞. Consider a basic open disc of ∞ given by $\{\infty\} \cup e^{-1}(D_\infty^\times)$, where $D_\infty^\times \subset \mathbb{C} \setminus \{a, b, c\}$ is of the form $\{z > R\}$ for some $R \geq \max\{|a|, |b|, |c|\}$. Then, $e^{-1}(D_\infty^\times)$ is a two-to-one cover of $D_\infty^\times$. For a point $z \in D_\infty^\times$, the lift of a loop with base point z and winding number 1 around ∞ (i.e., winding number -1 around 0) is a path from one of the two preimage points of z to the other. Thus, $e^{-1}(D_\infty^\times)$ is connected, which shows that it is a covering space of $D_\infty^\times$ for the map e. Arguing again as in Proposition 3.2, we can define a function $\dfrac{1}{\sqrt{\zeta}}$ on $e^{-1}(D_\infty^\times)$ so that $\dfrac{1}{\sqrt{\zeta}}$ is an analytic continuation of $\dfrac{1}{\sqrt{z}}$ (where the square root is taken to be consistent with the earlier choice of $\sqrt{\zeta_0} = z_0$), and that $\dfrac{1}{\sqrt{\zeta}} = 0$ for $\zeta = \infty$. Similarly as before, we check that $\left(\dfrac{1}{\sqrt{\zeta}}, \{\infty\} \cup e^{-1}(D_\infty^\times)\right)$ is a chart that can easily be seen to be compatible with the charts on $\mathcal{R}$ by construction. This overall gives $\mathcal{R}^*$ the structure of a compact Riemann surface, as desired.

The reciprocal of (3.3), given by

$$F(\zeta)^{-1} = \frac{1}{\sqrt{(\zeta - \alpha)(\zeta - \beta)(\zeta - \gamma)}}, \tag{3.4}$$

satisfies $F(\zeta_0)^{-1} = 1/q_0$, is analytic in $\mathcal{R}$, and is continuous in $\mathcal{R}^*$ as a map into $\mathbb{C} \cup \{\infty\}$. By Riemann's removable singularity theorem, $F(\zeta)^{-1}$ a meromorphic function on $\mathcal{R}^*$. We now inspect its behavior near each of α, β, γ, and ∞.

The local coordinate near α is $s = \sqrt{\zeta - \alpha}$. Using the complex variable z to write $F(\zeta)^{-1}$ in terms of s, we have $s^2 = z - a$, i.e., $z = s^2 + a$. This gives us

$$(z-b)(z-c) = (s^2 + a - b)(s^2 + a - c).$$

As a result, we have

$$F(\zeta)^{-1} = s^{-1} \frac{1}{\sqrt{(s^2 + a - b)(s^2 + a - c)}} \tag{3.5}$$

for one of the two possible branches of the square root. The square root is analytic and nonvanishing at $s = 0$, so $F(\zeta)^{-1}$ has a simple pole at $\zeta = \alpha$. By an analogous argument, $F(\zeta)^{-1}$ also has simple poles at $\zeta = \beta$ and $\zeta = \gamma$.

The local coordinate near ∞ is $s = \dfrac{1}{\sqrt{\zeta}}$. Using the complex variable z as before, we have $z = s^{-2}$, which means

$$\begin{aligned}(z-a)(z-b)(z-c) &= z^3 \left(1 - \frac{a}{z}\right)\left(1 - \frac{b}{z}\right)\left(1 - \frac{c}{z}\right) \\ &= s^{-6}(1 - as^2)(1 - bs^2)(1 - cs^2).\end{aligned}$$

As a result, we have

$$F(\zeta)^{-1} = s^3 \frac{1}{\sqrt{(1 - as^2)(1 - bs^2)(1 - cs^2)}} \tag{3.6}$$

for one of the two possible branches of the square root. The square root is analytic and nonvanishing at $s = 0$, so $F(\zeta)^{-1}$ has a triple zero at $\zeta = \infty$.

4. Lemmas for the Elliptic Integral

With the notation of Section 3, we can write the integral of (1.4) (with the choice of a piecewise smooth path $C \subset \mathcal{R}^*$) as

$$w(C) = \int_C \frac{1}{2} F(\zeta)^{-1} d\zeta, \tag{4.1}$$

but the notation of this elliptic integral still needs to be made more precise. To this end, parametrize the piecewise smooth path C as $\{C(t) : t \in I\}$ for some domain interval I, and consider the path $e(C) \in \mathbb{C} \cup \infty$ parametrized by $\{e(C(t)) : t \in I\}$. Then, we formally define the integral (4.1) by

$$w(C) = \int_{t \in I} \frac{1}{2} F(C(t))^{-1} e(C)'(t) dt. \tag{4.2}$$

We now show that the integral (4.2) is convergent for any choice of C. The denominator of the integrand is clearly bounded away from 0 when C is bounded away from α, β, γ, and ∞, so we only need to consider the cases when C is contained in a (sufficiently small) basic open disc of α, β, γ, or ∞, since any piecewise continuous path in $\mathcal{R}^*$ can be decomposed into subpaths that each fit one of the above descriptions.

Suppose C is confined to a basic open disc of α. The local parameter near α is $s = \sqrt{\zeta - \alpha}$, so if we denote $s(t)$ to be the coordinate path corresponding to C, we have $s(t)^2 = e(C(t)) - a$, which gives $e(C(t)) = s(t)^2 + a$. Taking derivatives, we get

$$e(C)'(t)dt = 2s(t)s'(t)dt,$$

and substituting this expression and (3.5) into (4.2) yields

$$w(C) = \int_{t \in I} \frac{s'(t)}{\sqrt{(s(t)^2 + a - b)(s(t)^2 + a - c)}}\, dt. \tag{4.3}$$

As long as our basic open disc of α is sufficiently small, the denominator is bounded away from 0, and thus the integral is convergent. Analogously, we can show that (4.2) is convergent when C is contained in a sufficiently small basic open disc of β or γ.

Finally, suppose C is confined to a basic open disc of ∞. The local parameter near ∞ is $s = \dfrac{1}{\sqrt{\zeta}}$, so if we denote $s(t)$ to be the coordinate path corresponding to C, we have $s(t)^2 = 1/e(C(t))$, which gives $e(C(t)) = s(t)^{-2}$. Taking derivatives, we get

$$e(C)'(t)dt = -2s(t)^{-3}s'(t)dt$$

and substituting this expression and (3.6) into (4.2) yields

$$w(C) = \int_{t\in I} -\frac{s'(t)}{\sqrt{(1-as(t)^2)(1-bs(t)^2)(1-cs(t)^2)}}\,dt. \tag{4.4}$$

Again, as long as our basic open disc of ∞ is sufficiently small, the denominator is bounded away from 0, and thus the integral is convergent.

Therefore, the integral (4.2) is convergent, which justifies our definition of $w(C)$ by (4.2). We now show the following lemma, which allows us to evaluate $w(C)$.

Lemma 4.1. *Let $C \subset \mathcal{R}^*$ be a piecewise smooth path contained in a basic open disc with local parameter s, such that in this local parameter, C goes from s_1 to s_2. Then,*

$$w(C) = \int_{s_1}^{s_2} \frac{1}{2}F(\zeta(s))^{-1}\frac{dz}{ds}\,ds. \tag{4.5}$$

Proof. If the basic open disc is in $\mathcal{R}$ with local parameter z, then we immediately obtain the lemma by applying the Cauchy integral theorem to the integrand, which is equal to $\dfrac{1}{2\sqrt{(z-a)(z-b)(z-c)}}$ for one of the two choices of branch for the square root.

If the basic open disc is centered at α with local parameter $s = \sqrt{\zeta - \alpha}$, then it follows from (4.3) that $w(C)$ is given by

$$\int \frac{1}{\sqrt{(s^2+a-b)(s^2+a-c)}}\,ds, \tag{4.6}$$

where the path of integration is given by the coordinate path $s(t) = \sqrt{C(t) - \alpha}$ corresponding to C. The integrand of (4.6) is analytic in a disc containing the path $s(t)$, so the lemma follows from the Cauchy integral theorem. Analogous remarks apply when the basic open disc is centered at β or γ.

Finally, suppose that the basic open disc is centered at ∞ with local parameter $s = \dfrac{1}{\sqrt{\zeta}}$. Then, it follows from (4.4) that $w(C)$ is given by

$$\int -\frac{1}{\sqrt{(1-as^2)(1-bs^2)(1-cs^2)}}\,ds, \tag{4.7}$$

where the path of integration is given by the coordinate path $s(t) = \dfrac{1}{\sqrt{C(t)}}$ corresponding to C. The integrand of (4.7) is analytic in a disc containing the path $s(t)$, so the lemma follows from the Cauchy integral theorem.

□

We note that (4.5) only depends on the endpoints; taking the integral over different paths with the same endpoints yields the same value for $w(C)$. In fact, the following more general result holds.

Lemma 4.2. *Let $C, C' \subset \mathcal{R}^*$ be piecewise smooth paths from ζ_1 to ζ_2. If C and C' are homotopic in $\mathcal{R}^*$, then $w(C) = w(C')$.*

Proof. Denote the homotopy as $\{C_r : r \in [0,1]\}$, where $C_0 = C$ and $C_1 = C'$, and each C_r is a path from ζ_1 to ζ_2. Without loss of generality, we can assume that each C_r is piecewise smooth and has the same interval I as its domain. To prove our lemma, it suffices to show that for each $r_0 \in [0,1]$, the value of $w(C_r)$ is invariant for r in a neighborhood of r_0. For this purpose, it is enough to prove that $w(C_{r_0}) = w(C'')$ for any piecewise smooth path C'' that is sufficiently close to C_{r_0} uniformly for $t \in I$.

At each point in the image of C_{r_0}, choose a basic open disc Δ and an open basic subdisc $\Delta'' \subsetneq \Delta$, both centered at the point. The discs Δ'' form an open cover of the image of C_{r_0}, which is compact. So, there exists a finite subcover $\Delta''_1, \ldots, \Delta''_n$. Let $\Delta_1, \ldots, \Delta_n$ be the corresponding discs Δ, and choose intermediate basic open discs $\Delta'_1, \ldots, \Delta'_n$ satisfying

$$\Delta''_i \subset \bar{\Delta}''_i \subset \Delta'_i \subset \bar{\Delta}'_i \subset \Delta_i \qquad \text{for } 1 \le i \le n.$$

C_{r_0} is uniformly continuous as a map, so there exists some $\delta > 0$ such that $C_{r_0}(t) \in \Delta''_i$ implies $C_{r_0}(t) \in \Delta'_i$ for $|t' - t| < \delta$. Let $t_0 < \cdots < t_m$ be a partition of I such that $t_j - t_{j-1} < \delta$ for $1 \le j \le m$. For each $j \in \{0, \ldots, m\}$, choose $\imath(j)$ so that $C_{r_0}(t_j) \in \Delta''_{\imath(j)}$. Then, since the mesh of our partition is $< \delta$, it follows that $C_{r_0}([t_{j-1}, t_j]) \subset \Delta'_{\imath(j-1)}$ for $1 \le j \le m$.

Choose $\varepsilon > 0$ so that $\mathrm{dist}_i(\bar{\Delta}'_i, \Delta_i^C) \ge \varepsilon$ for $1 \le i \le n$, where $\mathrm{dist}_i(\cdot)$ denotes the pullback distance given by the chart on Δ_i. Let C'' be a piecewise smooth path from ζ_1 to ζ_2 that is uniformly within ε of C_{r_0}. Then, $C''([t_{j-1}, t_j]) \subset \Delta_{\imath(j-1)}$ for $1 \le j \le m$. In fact, for $1 \le j \le m-1$, $C_{r_0}(t_j)$ and $C''(t_j)$ are both in $\Delta_{\imath(j-1)} \cap \Delta_{\imath(j)}$, which is easily seen to be connected. So, for $1 \le j \le m-1$, there exists a piecewise smooth path S_j from $C_{r_0}(t_j)$ to $C''(t_j)$ in $\Delta_{\imath(j-1)} \cap \Delta_{\imath(j)}$. Additionally, denote by S_0 the constant path at $C_{r_0}(t_0) = \zeta_1$, and denote by S_m the constant path at $C_{r_0}(t_m) = \zeta_2$. Then, by canceling the subintegrals along opposite paths, we have

$$w(C'') = \sum_{j=1}^{m} w(S_{j-1} C''|_{[t_{j-1}, t_j]} S_j^{-1}). \tag{4.8}$$

But $S_{j-1} C''|_{[t_{j-1}, t_j]} S_j^{-1}$ is a path lying in the basic open disc $\Delta_{\imath(j-1)}$ with the same endpoints as $C_{r_0}|_{[t_{j-1}, t_j]}$. Thus, by Lemma 4.1, it follows that (4.8) is

$$= \sum_{j=1}^{m} w(C_{r_0}|_{[t_{j-1}, t_j]}) = w(C_{r_0}),$$

which proves our lemma. □

We have shown in Proposition 3.3 that the equivalence classes of $\Gamma_a^2, \Gamma_b^2, \Gamma_c^2, \Gamma_1$, and Γ_2 generate the subgroup H of $\pi_1(\mathbb{C} \setminus \{a, b, c\}, z_0)$. We can lift these five loops to the respective loops $\Gamma_\alpha, \Gamma_\beta, \Gamma_\gamma, \bar{\Gamma}_1$, and $\bar{\Gamma}_2$ in $\mathcal{R} \subset \mathcal{R}^*$ with base point ζ_0. It is natural to compute the integral (4.1) over these five loops.

Lemma 4.3. *For $\Gamma_\alpha, \Gamma_\beta$, and Γ_γ defined above, we have*

$$\int_{\Gamma_\alpha} \frac{1}{2} F(\zeta)^{-1} d\zeta = \int_{\Gamma_\beta} \frac{1}{2} F(\zeta)^{-1} d\zeta = \int_{\Gamma_\gamma} \frac{1}{2} F(\zeta)^{-1} d\zeta = 0.$$

Proof. Applying Lemma 4.2 to just within $\mathcal{R}$, computing the integral $\int_{\Gamma_\alpha} \frac{1}{2} F(\zeta)^{-1} d\zeta$ reduces to taking the same integral over a loop around α (with the same winding number) in a basic open disc of $\mathcal{R}^*$ about α. Then, by Lemma 4.1, this integral is 0. Similarly, the analogous integrals over Γ_β and Γ_γ are also 0. □

As for the analogous integrals over the other two loops $\bar{\Gamma}_1$ and $\bar{\Gamma}_2$, we denote them by

$$\omega_1 = \int_{\bar{\Gamma}_1} \frac{1}{2} F(\zeta)^{-1} d\zeta \qquad \text{and} \qquad \omega_2 = \int_{\bar{\Gamma}_2} \frac{1}{2} F(\zeta)^{-1} d\zeta, \tag{4.9}$$

and we let $\Lambda \subset \mathbb{C}$ denote

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2. \tag{4.10}$$

We take the quotient space $\mathbb{C}/\Lambda$ and endow it with the quotient topology. It turns out we can project the aforementioned map w into $\mathbb{C}/\Lambda$ in a well-defined manner.

Proposition 4.4. *Let $w : \mathcal{R}^* \to \mathbb{C}/\Lambda$ be defined by*

$$w(\zeta) = w(C) \pmod{\Lambda}$$

for any piecewise smooth path $C \subset \mathcal{R}^*$ from ζ_0 to ζ. The map w is well-defined (i.e.: the above definition doesn't depend on the specific path C), and is in fact continuous and open.

Proof. Fix $\zeta \in \mathcal{R}^*$, and let $C, C' \subset \mathcal{R}^*$ be piecewise smooth paths from ζ_0 to ζ. We need to show that $w(C') - w(C) \in \Lambda$. By homotopically perturbing C' if necessary, we can without loss of generality assume the following: if $\zeta \notin \{\alpha, \beta, \gamma, \infty\}$, then neither C or C' meets any point in $\{\alpha, \beta, \gamma, \infty\}$, whereas if $\zeta \in \{\alpha, \beta, \gamma, \infty\}$, then C and C' meet $\{\alpha, \beta, \gamma, \infty\}$ only at their final endpoints. Note that

$$w(C') - w(C) = w(C'C^{-1}),$$

where $C'C^{-1}$ is a loop with base point ζ_0. By Lemma 4.2, we can homotopically perturb $C'C^{-1}$ near ζ, if necessary, so that $C'C^{-1}$ doesn't meet any point in $\{\alpha, \beta, \gamma, \infty\}$. Afterwards, by Lemma 4.2, $w(C'C^{-1})$ depends only on the equivalence class of $C'C^{-1}$ in $\mathcal{R}$. It follows from Proposition 3.1 that the equivalence classes of loops in $\mathcal{R}$ are generated by $\Gamma_\alpha, \Gamma_\beta, \Gamma_\gamma, \bar{\Gamma}_1$, and $\bar{\Gamma}_2$, so $w(C'C^{-1})$ is equal to an integer combination of $w(\Gamma_\alpha), w(\Gamma_\beta), w(\Gamma_\gamma), w(\bar{\Gamma}_1)$, and $w(\bar{\Gamma}_2)$. But we have shown in Lemma 4.3 that $w(\Gamma_\alpha) = w(\Gamma_\beta) = w(\Gamma_\gamma) = 0$. Thus, $w(C'C^{-1})$ is an integer combination of $w(\bar{\Gamma}_1)$ and $w(\bar{\Gamma}_2)$. This shows that $w(C') - w(C) \in \Lambda$, proving that $w : \mathcal{R}^* \to \mathbb{C}/\Lambda$ is well-defined.

Now, we show that w is continuous and open. To this end, we fix $\zeta_1 \in \mathcal{R}^*$ and a path C_1 from ζ_0 to ζ_1, then observe how w varies as the path of integration that start with C_1 and continue completely inside a basic open disc about ζ_1. Let C_2 be this continuation path within the basic disc, let ζ be the final endpoint of C_2, and let ζ_1 and ζ correspond to s_1 and s, respectively, in the local coordinate. Then, by Lemma 4.1,

$$w(\zeta) = w(C_1) + w(C_2) = w(C_1) + \int_{s_1}^{s} \frac{1}{2} F(\zeta(s))^{-1} \frac{dz}{ds} ds. \tag{4.11}$$

The integral of the last term can be made arbitrarily small by having s arbitrarily close to s_1, so w is continuous. Furthermore, the integral of the last term is nonconstant analytic as a function of s, which implies that w is open. □

The above result allows us to show that ω_1 and ω_2, as defined in (4.9), do in fact generate a lattice that gives rise to an elliptic curve over $\mathbb{C}$.

Corollary 4.5. *Λ is not contained in $\mathbb{R}\omega$ for any $\omega \in \mathbb{C}^\times$. Therefore, ω_1 and ω_2 are nonzero complex numbers that are linearly independent over $\mathbb{R}$.*

Proof. Suppose for the sake of a contradiction that $\Lambda \subset \mathbb{R}\omega$ for some $\omega \in \mathbb{C}^\times$. The natural map $\mu : \mathbb{C}/\Lambda \to \mathbb{C}/(\mathbb{R}\omega)$ is necessarily continuous and open. It follows that the composition $\mu \circ w : \mathcal{R}^* \to \mathbb{C}/(\mathbb{R}\omega)$, where w is the map defined in Proposition 4.4, is continuous and open. Note that $\mathcal{R}^*$ is compact and $\mathbb{C}/(\mathbb{R}\omega)$ is Hausdorff, which implies that the image $\mu \circ w(\mathcal{R}^*)$ is compact, and moreover that $\mu \circ w$ is a closed map. Thus, $\mu \circ w(\mathcal{R}^*)$ is open and closed, and since $\mathbb{C}/(\mathbb{R}\omega)$ is connected, we in fact have $\mu \circ w(\mathcal{R}^*) = \mathbb{C}/(\mathbb{R}\omega)$. But $\mathbb{C}/(\mathbb{R}\omega)$ is noncompact. Contradiction. □

It thus follows that Λ is a lattice, and that $\mathbb{C}/\Lambda$ is a complex torus.

5. The Main Proof

The map w defined in Proposition 4.4 maps the compact Riemann surface $\mathcal{R}^*$ into $\mathbb{C}/\Lambda$, which we have also shown to have the structure of a compact Riemann surface (in fact, a complex torus). Given our sketch argument in Section 1, w should essentially be the inverse of the Weierstrass $\wp$-function for Λ. Thus, it makes sense to investigate the invertibility of w, and afterwards, the holomorphicity of w^{-1}. To this end, we prove the following.

Theorem 5.1. *The map $w : \mathcal{R}^* \to \mathbb{C}/\Lambda$ defined in Proposition 4.4 is biholomorphic.*

Proof. (4.11) shows that w is holomorphic and has derivative (in terms of the local coordinate)

$$\frac{1}{2}F(\zeta(s))^{-1}\frac{dz}{ds}. \tag{5.1}$$

For $\zeta \in \mathcal{R}$, the local parameter is $s = z$, and so the derivative (5.1) is given in this case by

$$\frac{1}{2\sqrt{(s-a)(s-b)(s-c)}},$$

which is nonzero. At $\zeta = \alpha$, (5.1) is given by the integrand of (4.6), which is also nonzero. Analogous results hold for $\zeta = \beta$ and $\zeta = \gamma$. Finally, at $\zeta = \infty$, (5.1) is given by the integrand of (4.7), which is again nonzero. Since the derivative is nowhere vanishing, w is an immersion. An immersion from a compact manifold to a manifold of the same dimension is necessarily a covering map, so $w : \mathcal{R}^* \to \mathbb{C}/\Lambda$ is a covering map. Thus, if we show that w is injective, then w is a bijective holomorphic map, so there exists a holomorphic inverse map w^{-1} by the holomorphic inverse function theorem for Riemann surfaces.

So, it suffices to show that w is injective. Suppose $w(\zeta_1) = w(\zeta_2)$ for $\zeta_1, \zeta_2 \in \mathcal{R}^*$. Then, for piecewise smooth paths C_1 and C_2 from ζ_0 to ζ_1 and ζ_0 to ζ_1, respectively, we have

$$w(C_1) = w(C_2) + \omega$$

for some integer combination $\omega = m\omega_1 + n\omega_2$ in Λ. Let $\Gamma = \bar{\Gamma}_1^m \bar{\Gamma}_2^n$, so that $w(\Gamma) = \omega$. Then, $C_3 = \Gamma C_2$ is a path that goes from ζ_0 to ζ_2 and satisfies $w(C_3) = w(C_2) + \omega$. Thus,

$$w(C_1) = w(C_3) \tag{5.2}$$

Let us parametrize C_1 and C_3 to have domain interval $[0, 1]$, so that the paths are respectively denoted by $\{C_1(t) : t \in [0,1]\}$ and $\{C_3(t) : t \in [0,1]\}$. For $t \in [0,1]$, define

$$C_1^{\#}(t) = w(C_1|_{[0,t]}) \qquad \text{and} \qquad C_3^{\#}(t) = w(C_3|_{[0,t]})$$

as piecewise smooth paths in $\mathbb{C}$. We also define

$$C_1^{\#\#} = w \circ C_1 \qquad \text{and} \qquad C_3^{\#\#} = w \circ C_3 \tag{5.3}$$

as piecewise smooth paths in $\mathbb{C}/\Lambda$. By Proposition 4.4, we have

$$C_1^{\#}(t) = w(C_1|_{[0,t]}) \equiv w(C_1(t)) \pmod{\Lambda},$$

so $C_1^{\#}$ is the lift of $C_1^{\#\#}$ based at 0. By an analogous argument, we also conclude that $C_3^{\#}$ is the lift of $C_3^{\#\#}$ based at 0.

By (5.2), we have $C_1^{\#}(1) = C_3^{\#}(1)$, from which it follows that $C_1^{\#} C_3^{\#-1}$ is a contractible loop in $\mathbb{C}$. Thus, $C_1^{\#\#} C_3^{\#\#-1}$ is a contractible loop in $\mathbb{C}/\Lambda$. Since w is a covering map, it follows from the definition (5.3) that $C_1 C_3^{-1}$ is a contractible loop in $\mathcal{R}^*$. Thus, the final endpoints of C_1 and C_2 are equal, i.e., $\zeta_1 = \zeta_2$. This completes our proof that w is injective, and thus biholomorphic by our previous argument.

□

We have constructed a lattice Λ and a bioholomorphic map $w(\zeta)$ that should essentially be the Weierstrass $\wp$-function associated to Λ. To make the necessary modification for this to work, we translate the map $w(\zeta)$ by $\int_\infty^{\zeta_0} \frac{1}{2}F(\zeta)^{-1}d\zeta + \Lambda \in \mathbb{C}/\Lambda$, which is well-defined as a result of (4.2) and Proposition 4.4. The ensuing new map $w : \mathcal{R}^* \to \mathbb{C}/\Lambda$, given by

$$w(\zeta) = \int_\infty^\zeta \frac{1}{2}F(\lambda)^{-1}d\lambda + \Lambda, \tag{5.4}$$

is still biholomorphic. Let $w^{-1} : \mathbb{C}/\Lambda \to \mathcal{R}^*$ denote its holomorphic inverse. Let $\mu : \mathbb{C} \to \mathbb{C}/\Lambda$ be the quotient map, which is trivially holomorphic. Then, we can define $P : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ as the meromorphic function

$$P(z) = e \circ w^{-1} \circ \mu(z), \tag{5.5}$$

where the map $e : \mathcal{R}^* \to \mathbb{C} \cup \{\infty\}$ is defined in Section 2. We will see that this map P is essentially the Weierstrass $\wp$-function associated to Λ.

Theorem 5.2. *The map $P(z)$ defined in (5.5) is in fact*

$$P(z) = \wp(z) + \frac{1}{3}(a + b + c),$$

where $\wp(z)$ is the Weierstrass $\wp$-function associated to the lattice Λ defined in (4.10).

Proof. The function P is meromorphic and double periodic with respect to Λ, so it is an elliptic function. Note that $w(\{\infty\}) = 0 + \Lambda$ by (5.4), so we have

$$\begin{aligned} P^{-1}(\{\infty\}) = \mu^{-1}(w(e^{-1}(\{\infty\}))) &= \mu^{-1}(w(\{\infty\})) \\ &= \mu^{-1}(0 + \Lambda) \\ &= \Lambda, \end{aligned}$$

i.e., the poles are precisely at Λ. To compute the order of these poles, we observe the behavior of $P(z)$ near $z = 0$. Since μ and w^{-1} are locally invertible maps, the order of the pole of P at $z = 0$ is the same as the order of the pole of e at ∞ in $\mathbb{C}$. The local parameter of $\mathcal{R}^*$ near ∞ is $s = \dfrac{1}{\sqrt{\zeta}}$, from which we get that $w(\zeta) = z = s^{-2}$. So, the order of the pole is 2.

I further claim that P is an even function, i.e., that $P(z) = P(-z)$ for all $z \in \mathbb{C}$. Indeed, fix $z \in \mathbb{C}$, and let $\psi = w^{-1} \circ \mu(z) \in \mathcal{R}^*$. Let $C \subset \mathcal{R}^*$ be a piecewise smooth path from ∞ to ψ. Note that $\mathcal{R}^*$ has a holomorphic involution that interchanges the two sheets. Let $C' \subset \mathcal{R}^*$ be the image of C under this involution. Then, C' is a piecewise smooth curve from ∞ to some point $\psi' \in \mathcal{R}^*$, where ψ' is the point to which the involution maps ψ. We have

$$\begin{aligned} w(\psi') \equiv \int_{C'} \frac{1}{2}F(\zeta)^{-1}d\zeta \pmod{\Lambda} &= -\int_C \frac{1}{2}F(\zeta)^{-1}d\zeta \\ &\equiv -w(\psi) \pmod{\Lambda}, \end{aligned}$$

where the middle equality holds because the integrands, as defined in (4.2), differ precisely by a factor of -1. It follows that $\psi' = w^{-1}(-w(\psi) + \Lambda)$, from which we have

$$\begin{aligned} P(z) = e(w^{-1}(\mu(z))) = e(\psi) = e(\psi') &= e(w^{-1}(-w(\psi) + \Lambda)) \\ &= e(w^{-1}(-w(w^{-1}(\mu(z))) + \Lambda)) \\ &= e(w^{-1}(-\mu(z) + \Lambda)) \\ &= e(w^{-1}(\mu(-z) + \Lambda)) = P(-z). \end{aligned}$$

Since P only has one order 2 pole mod Λ, it is an order 2 elliptic function. It thus follows from the proof of the classification theorem for even elliptic functions (see the proof of [8, VI.3.2]) that

$$P(z) = k_1(\wp(z) + k_2) \tag{5.6}$$

for some $k_1 \in \mathbb{C}^\times$ and $k_2 \in \mathbb{C}$.

We now show that P satisfies the differential equation for $\wp$. As before, let $\psi = w^{-1} \circ \mu(z) \in \mathcal{R}^*$. It suffices to show that P satisfies the differential equation in $\mathcal{R}$, so we can suppose that $\psi \in \mathcal{R}$. Then, we take $p = e(\psi)$ as a local parameter in $\mathbb{C}$, which gives

$$P(z) = e \circ w^{-1} \circ \mu(z) = e(\psi) = p.$$

Moreover, $w(\psi) = \mu(z)$, so it follows from (5.4) that

$$z \in \int_\infty^\psi \frac{1}{2} F(\zeta)^{-1} d\zeta + \Lambda.$$

This allows us to use the equality (4.5), take derivatives of both side with respect to the parameter p, and apply the fundamental theorem of calculus to obtain

$$\frac{dz}{dp} = \frac{1}{2} F(p)^{-1} = \frac{1}{2\sqrt{(p-a)(p-b)(p-c)}}$$

for one of the two branches of the square root. It follows that

$$\frac{dp}{dz} = 2\sqrt{(p-a)(p-b)(p-c)}.$$

Substituting $p = P(z)$ and taking squares, we get the differential equation

$$P'^2 = 4(P-a)(P-b)(P-c). \tag{5.7}$$

This relationship allows us to evaluate k_1 and k_2 in (5.6). Since P is an even meromorphic function with a double pole at $z = 0$, we have the following as $z \to 0$:

$$P(z) = \frac{c_{-2}}{z^2} + c_0 + O(z^2)$$

$$P'(z) = -\frac{2c_{-2}}{z^3} + O(z)$$

$$P'(z)^2 = \frac{4c_{-2}^2}{z^6} + O(z^{-2})$$

$$\begin{aligned}(P(z)-a)(P(z)-b)(P(z)-c) &= \left(\frac{c_{-2}}{z^2} + O(1)\right)\left(\frac{c_{-2}}{z^2} + O(1)\right)\left(\frac{c_{-2}}{z^2} + O(1)\right) \\ &= \frac{c_{-2}^3}{z^6} + O(z^{-4}).\end{aligned}$$

By our work above, it follows from (5.7) that $\dfrac{4c_{-2}^2}{z^6} = \dfrac{4c_{-2}^3}{z^6}$, which gives us $c_{-2} = 1$. Recall from (1.3) that the coefficient of z^{-2} in the Laurent series for $\wp(z)$ is 1, which overall implies that $k_1 = 1$. The differential equation (5.7) thus gives us

$$\begin{aligned}\wp'^2 &= 4(\wp + k_2 - a)(\wp + k_2 - b)(\wp + k_2 - c) \\ &= 4\wp^3 + 4(3k_2 - a - b - c)\wp^2 + (\text{lower-order terms in } \wp).\end{aligned}$$

But recall from (1.1) that we also have

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3$$

for $g_2 = 60G_4(\Lambda)$ and $g_3 = 140G_6(\Lambda)$. This overall implies that

$$4(3k_2 - a - b - c)\wp^2 + (\text{lower-order terms in } \wp) = 0.$$

But $\wp$ takes on more than two distinct values in $\mathbb{C}$, which contradicts the above equality unless the left-hand side is uniformly 0. So, it follows that

$$3k_2 - a - b - c = 0,$$

which proves the theorem. □

Recall from our discussion in Section 1 that by a linear change of variables, we have assumed that our elliptic curve $E : y^2 = 4(x-a)(x-b)(x-c)$ satisfies $a+b+c = 0$. This means that the Weierstrass $\wp$-function for the lattice Λ constructed in (4.10) satisfies the differential equation given by the affine equation for E. Thus, we conclude that the correspondence described in (1.2) in fact associates Λ to E. In summary, we have proven the following main result.

Theorem 5.3 (Uniformization)**.** *For every nonsingular curve*

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

over $\mathbb{C}$, there exists a lattice Λ such that E can be written as $\mathbb{C}/\Lambda$, i.e., such that

$$g_2 = 60G_4(\Lambda), \qquad g_3 = 140G_6(\Lambda),$$

and the map (1.2) is both a biholomorphism and a group isomorphism from $\mathbb{C}/\Lambda$ to $E(\mathbb{C})$.

Acknowledgments

The author would like to thank Professor Manjul Bhargava for providing many valuable suggestions on the writing of this report.

References

[1] Lars V. Ahlfors, *Complex analysis*, Third, McGraw-Hill Book Co., New York, 1978. An introduction to the theory of analytic functions of one complex variable, International Series in Pure and Applied Mathematics. MR510197 (80c:30001)

[2] Tom M. Apostol, *Modular functions and Dirichlet series in number theory*, Second, Graduate Texts in Mathematics, vol. 41, Springer-Verlag, New York, 1990. MR1027834 (90j:11001)

[3] Anthony W. Knapp, *Elliptic curves*, Mathematical Notes, vol. 40, Princeton University Press, Princeton, NJ, 1992. MR1193029 (93j:11032)

[4] Alain Robert, *Elliptic curves*, Lecture Notes in Mathematics, Vol. 326, Springer-Verlag, Berlin-New York, 1973. Notes from postgraduate lectures given in Lausanne 1971/72. MR0352107 (50 #4594)

[5] J.-P. Serre, *A course in arithmetic*, Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7. MR0344216 (49 #8956)

[6] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1. MR1291394 (95e:11048)

[7] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR1312368 (96b:11074)

[8] ———, *The arithmetic of elliptic curves*, Second, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094 (2010i:11005)

[9] Elias M. Stein and Rami Shakarchi, *Complex analysis*, Princeton Lectures in Analysis, II, Princeton University Press, Princeton, NJ, 2003. MR1976398 (2004d:30002)

Department of Mathematics, Princeton University, Princeton, NJ 08544
E-mail address: pspark@math.princeton.edu