The goal of these notes is to explain why any elliptic curve over $\boldsymbol{C}$ has a Weierstrass uniformization, up to obvious changes of coordinates. These notes are sketchy and they wade into topics that are beyond the scope of the class – invariance of domain, moduli spaces, extremal length, and conformal metrics. Even so, I hope that they are of some use.

1 Outline

The construction of the Weierstrass uniformizing map gives us a map from the set of all lattices to the set of Weierstrass elliptic curves. The idea is to define these sets precisely and analyze what the map does to them. Here is an outline of the notes.

- We will explain what Invariance of Domain means. I like to think of Invariance of Domain as a continuous version of the Pidgeonhole principle. It says that, under the right circumstances, a continuous, injective, and proper map is surjective. (*Properness* is defined below.)

- We will define a space Y of certain representatives of Weierstrass elliptic curves. Every Weierstrass elliptic curve will be equivalent to one of our representatives up to projective transformations. The space Y is known as the *moduli space of elliptic curves*.

- We will define a space X of certain representatives of lattices. Every lattice will be equivalent to a lattice in X up to scaling. The space X is known as *the moduli space of lattices*.

- We will show that the Weierstrass uniformization constructs a well-defined map $f : X \to Y$ that is both continuous and surjective. Invariance of Domain reduces the question of whether f is surjective to the question of whether f is proper.

- We will define the concepts of *extremal length* and *conformal metrics* and sketch some technical lemmas about them.

- Using the concepts of extremal length and conformal metrics, we will prove that f is proper. Invariance of Domain allows us to conclude that f is surjective, and in fact a homeomorphism.

2 Invariance of Domain

Say that an *unbounded sequence* in $\boldsymbol{R}^k$ is a sequence $\{x_n\}$ such $\|x_n\| \to \infty$. A map $f : \boldsymbol{R}^k \to \boldsymbol{R}^k$ is called *proper* if it carries unbounded sequences to unbounded sequences. That is, if $\{x_n\}$ is unbounded then so is $\{f(x_n)\}$.

Lemma 2.1 (Invariance of Domain) *Suppose that $f : \boldsymbol{R}^k \to \boldsymbol{R}^k$ is continuous, injective, and proper. Then f is a homeomorphism.*

A proof of this result can be found in any book on algebraic topology, including Allen Hatcher's online book. All we need is the case $k = 2$. For convenience, we will prove this case under an additional hypothesis. When the time comes, we will verify that the extra hypothesis holds. Let $C_r(u)$ denote the circle of radius r centered at $u \in \boldsymbol{R}^2$.

Lemma 2.2 *Suppose that $f : \boldsymbol{R}^2 \to \boldsymbol{R}^2$ is continuous, injective, and proper. Suppose additionally that there is some point $u \in \boldsymbol{R}^2$ such that $f(C_r(u))$ winds a nonzero number of times around $f(u)$ for all sufficiently small r. Then f is a homeomorphism.*

Proof: We translate so that $u = 0$ and $f(0) = 0$. Let $p \in \boldsymbol{R}^2$ be any point. Consider the image $D_r = f(C_r)$. Since f is injective, D_r does not contain 0 for $r > 0$. By hypothesis, D_r winds a nonzero number of times around 0, for r small enough. But then D_r winds a nonzero number of times around the origin for all r, because the winding number is a continuous function of r, and also integer valued. If D_r winds 0 times around p, then D_r winds a different number of times around p than it does around 0. But then D_r must intersect the line segment joining 0 to p. Once r is large enough, this contradicts the fact that f is proper. Hence D_r winds a nonzero number of times around p for r large. But D_r winds 0 times around p when r is sufficiently small. This is only possible if the winding number is not defined for some r. That is, $p \in D_r$ for some r. Hence f is surjective.

To finish the proof, we just have to show that f^{-1} is continuous. If not, then we can find some $p \in \boldsymbol{R}^2$ and some sequence $\{q_n\} \to p$ such that $f^{-1}(q_n)$ does not converge to $f^{-1}(p)$ on any subsequence. Since f is proper, the sequence $\{f^{-1}(q_n)\}$ has a convergent subsequence. Let r be some limit of this sequence. Since f is continuous, we must have $f(r) = \lim q_n = p$. Hence $r = f^{-1}(p)$. Hence, some subsequence of $f^{-1}(q_n)$ converges to $f^{-1}(p)$. This is a contradiction. Hence f^{-1} is continuous. ♠

3 The Space of Elliptic Curves

Say that a *canonical form* for a Weierstrass elliptic curve is either

$$C_\infty : \qquad y^2 = x^3 + 1, \tag{1}$$

or

$$C_b : \qquad y^2 = x^3 + x + b; \tag{2}$$

There are 2 choices of b for which C_b is singular. Namely b should satisfy $4 + 27b^2 = 0$. That is

$$b_\pm = \pm 2i/\sqrt{27}. \tag{3}$$

Some coordinate change of the form $x \to \alpha x$ and $y \to \beta y$ converts an arbitrary Weierstrass elliptic curve into one in canonical form. The same kind of coordinate change maps C_b to C_{-b}. It is an exercise to show that C_a and C_b are projectively equivalent if and only if $a = \pm b$. For this reason, the space

$$Y = \Big((\boldsymbol{C} \cup \infty) - b_+ - b_- \Big) / \pm \tag{4}$$

parametrizes the set of all equivalence classes of Weierstrass elliptic curves. Any Weierstrass elliptic curve is projectively equivalent to a curve indexed by a unique point in Y. For this reason, Y is the space of projective equivalence classes of Weierstrass elliptic curves.

Topologically, the space $(C \cup \infty)/\pm$ is still a sphere. Hence the space Y is topologically a sphere with one point removed, namely $[b_\pm]$. A sphere with one point removed is homeomorphic to a plane. So, in short, Y is homeomorphic to a plane.

4 The Space of Lattices

Recall that a lattice is a set of the form

$$\Lambda(\alpha, \beta) = \{m\alpha + n\beta | m, n \in \boldsymbol{Z}\}. \tag{5}$$

Here α and β are two complex numbers with α/β non-real. We say that two lattices Λ_1 and Λ_2 are *equivalent* if there is a complex number w such that $\Lambda_2 = w\Lambda_1$. Here is the significance of this definition.

Lemma 4.1 *Two lattices Λ_1 and Λ_2 are equivalent if and only if there is a CA homeomorphism from $\boldsymbol{C}/\Lambda_1$ to $\boldsymbol{C}/\Lambda_2$.*

Proof: If $\Lambda_2 = w\Lambda_1$ then the map $f(z) = wz$ induces the CA homeomorphism from $\boldsymbol{C}/\Lambda_1$ to $\boldsymbol{C}/\Lambda_2$. That is the easy direction.

Suppose that $f : \boldsymbol{C}/\Lambda_1 \to \boldsymbol{C}/\Lambda_2$ is a CA homeomorphism. We can adjust by a translation so that $f(0) = 0$. Let $\pi_j : \boldsymbol{C} \to \boldsymbol{C}/\Lambda_j$ be the quotient map. Let $g = f \circ \pi_1$. Then g is a map from $\boldsymbol{C}$ to $\boldsymbol{C}/\Lambda_2$. Note that g' makes sense as a map from $\boldsymbol{C}$ to $\boldsymbol{C}$. The map g' is bounded since g' is completely determined by what g does on a single parallelogram in $\boldsymbol{C}$. Since g' is both CA and bounded, g' is constant. So, g must have the form

$$g(z) = \pi_2(wz). \tag{6}$$

Here $w = g'$. For $\lambda \in \Lambda_1$ we have

$$\pi_2(w\lambda) = f(\pi_1(\lambda)) = f(0) = 0.$$

Therefore $w\lambda \in \Lambda_2$. So, $w\Lambda_1 \subset \Lambda_2$. Reversing the roles of Λ_1 and Λ_2, we see that $(1/w)\Lambda_2 \subset \Lambda_1$. These two containments show that $w\Lambda_1 = \Lambda_2$. ♠

For now on, we always order α and β so that $\{\alpha, \beta\}$ makes a positive basis. That is β/α has positive imaginary part. Let $SL_2(\boldsymbol{Z})$ denote the set of matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}; \qquad ad - bc = 1. \tag{7}$$

That is, the determinant is 1. We write $(\alpha', \beta') = M(\alpha, \beta)$ if $\alpha = a\alpha' + b\beta'$ and $\beta' = c\alpha + d\beta$.

Lemma 4.2 $\Lambda(\alpha, \beta) = \Lambda(\alpha', \beta')$ *if and only if* $(\alpha', \beta') = M(\alpha, \beta)$ *for some* $M \in SL_2(\boldsymbol{Z})$.

Proof: The "if" direction is obvious. Suppose $\Lambda(\alpha, \beta) = \Lambda(\alpha', \beta')$. Since $\alpha', \beta' \in \Lambda(\alpha, \beta)$, we can write $\alpha' = a\alpha + b\beta$ and $\beta' = c\alpha + d\alpha$. At the same time, we can write $\alpha = a'\alpha' + b'\beta'$ and $\beta = c'\alpha' + d'\beta'$. The corresponding matrices M and M' are inverses of each other, and both are integer matrices. Hence, they both must have determinant ± 1. The condition on the ordering forces the determinant to be 1. ♠

Every lattice is certainly equivalent to one of the form $\Lambda(1,z)$ where $\mathrm{Im}(z) > 0$. Letting $\boldsymbol{H}^2$ denote the set of such z, we can say that every lattice is equivalent to one of the form $\Lambda(1,z)$, with $z \in \boldsymbol{H}^2$.

Lemma 4.3 *$\Lambda(1,z)$ and $\Lambda(1,z')$ are equivalent if and only if*

$$z' = \frac{az+b}{cz+d}; \qquad a,b,c,d \in \boldsymbol{Z}; \qquad ad-bc=1. \tag{8}$$

Proof: The "if" direction follows from Lemma 4.2. Suppose that $\Lambda(1,z)$ and $\Lambda(1,z')$ are equivalent. Then there is some complex number w such that $\Lambda(1,z') = w\Lambda(1,z)$. That is $\Lambda(1,z') = \Lambda(w,wz)$. But then $(1,z') = M(w,wz)$, where M is as in Equation 7. So, $z' = M(wz)/M(w)$. Writing this out and cancelling the extra factor of w in both the numerator and denominator gives Equation 8. ♠

We now see that the space X is the same as the quotient $\boldsymbol{H}^2/SL_2(\boldsymbol{Z})$, where the equivalence relation is as in Equation 8.

5 The Weierstrass Map

Now we define the map $f: X \to Y$. We choose some lattice $\Lambda = \Lambda(1,z)$ and form the Weierstrass function P. Next, we define $\Psi = (P,P')$. We have already seen that Ψ maps $\boldsymbol{C}/\Lambda$ onto an elliptic curve E, given by the equation

$$y^2 = 4x^3 + g_2 x + g_3.$$

Here g_2 and g_3 are such that $(P')^2 = 4P^3 + g_2 P + g_3$. We then take the elliptic curve in Y that is equivalent to this elliptic curve.

We need to see that f is well defined. The problem is that points in X are represented by more than one lattice. If we use the lattice $\Lambda(1,z^*)$ instead, with $z^* \sim z$, we get a different elliptic curve

$$y^2 = 4x^3 + g_2^* x + g_3^*.$$

We want to see that the two elliptic curves give the same point in Y.

There is a constant $w \in \boldsymbol{C}$ such that $\Lambda(1,z^*) = w\Lambda(1,z)$. Below, we will show that $g_2^* = w^{-4} g_2$ and $g_3^* = w^{-6} g_3$. From this information, it is an easy exercise to show that our two elliptic curves correspond to the same point in Y.

Lemma 5.1 *$g_2^* = w^{-4}g_2$ and $g_3^* = w^{-6}g_3$.*

Proof: Let P and P^* be the Weierstrass functions defined relative to Λ and Λ^* respectively. Consider the new function $Q(z) = P^*(wz)$. The functions P and Q are both Λ-periodic. Near 0, we have

$$P(z) = 1/z^2 + z^2 a(z); \qquad Q(z) = 1/(wz)^2 + z^2 b(z),$$

where $a(z)$ and $b(z)$ are CA functions. So, $P(z) - w^2 Q(z)$ is a bounded CA function. Hence $P(z) - w^2 Q(z)$ is constant. But we also know that $P(0) = Q(0) = 0$. Hence $Q(z) = w^{-2}P(z)$.

Now we know that $P^*(wz) = w^{-2}P(z)$. We can equally well write

$$P^*(z) = w^{-2}P(z/w). \tag{9}$$

By the chain rule,

$$(P^*)'(z) = w^{-3}P'(z/w). \tag{10}$$

Now we can see that

$$((P^*)'(z))^2 = w^{-6}(P'(z/w))^2 =$$

$$w^{-6}(P(z/w)^3 + g_2 P(z/w) + g_3) =$$

$$P^*(z)^3 + w^{-4}g_2 P^*(z) + w^{-6}g_3.$$

This shows that $g_2^* = w^{-4}g_2$ and $g_3^* = w^{-6}g_3$, as claimed. ♠

Lemma 5.2 *f is continuous and injective.*

Proof: To prove continuity, one just has to obvserve that the differential equation satisfied by the Weierstrass function pretty clearly depends continuously on the lattice. For injectivity, suppose that $f(x_1) = f(x_2)$. Then the map $\Psi_2^{-1} \circ \Psi_1$ gives a CA homeomorphism from $\boldsymbol{C}/\Lambda_1$ to $\boldsymbol{C}/\Lambda_2$. But then Λ_1 and Λ_2 are equivalent by Lemma 4.1. ♠

We want to use Lemma 2.2, so we need to verify the extra hypothesis. Let u be any point of $\boldsymbol{H}^2$ so that no two points of $\boldsymbol{C}$ sufficiently close to u are equivalent to each other in the sense of Equation 8. Only countably many points in $\boldsymbol{H}^2$ fail to have this property. For instance $u = 1/2 + i/2$ has the desired property. We also assume that $f(u) \neq 0$.

In a neighborhood of u, the space X is just a copy of an open set of $\boldsymbol{C}$. Likewise, in a neighborhood of $f(u)$, the space Y is just a copy of an open subset of $\boldsymbol{C}$. For this reason, it makes sense to discuss f as a CA function in a neighborhood of u.

Let $C_r(u)$ denote the set of points X representing lattices $\Lambda(1, z)$, where $|z - u| = r$. For r small, no two points of $C_r(u)$ are equivalent to each other. That is $C_r(u)$ is a loop in X.

Lemma 5.3 *For r sufficiently small, $f(C_r(u))$ winds a nonzero number of times around $f(u)$ in Y.*

Proof: An examination of construction of P and its differential equation shows that the coefficients g_2 and g_3 are complex analytic functions of the parameter z when they are constructed from the lattice $\Lambda(1, z)$. But then, the map f is CA in a neighborhood of u. Hence there is some integer m such that

$$f(z + u) - f(u) = z^m g(z) = z^m g(0) + z^{m+1} k(z) = z^m g(0) + \text{H.O.T.}.$$

Here g and k are CA in a neighborhood of 0 and $g(0) \neq 0$. This equation shows that $f(C_r(u))$ winds m times around $f(u)$. ♠

Suppose we knew that f was also proper. Then we could conclude from Lemma 2.2 that f is a homeomorphism from X to Y. The rest of these notes are devoted to showing that f is proper. Before giving the details, I'll explain the idea. If $\{p_n\}$ is an unbounded sequence in X, the corresponding quotients $\boldsymbol{C}/\Lambda_n$ are becoming increasingly long and skinny. The elliptic curves corresponding to $f(p_n)$ are also becoming long and skinny, in a certain sense, and therefore $f(p_n)$ must be an unbounded sequence in Y. In order to make this argument work, we need to somehow quantify what we mean by "long and skinny". The concept of extremal length does the job for us. Now for the details...

6 Extremal Length

Let $\Lambda = \Lambda(1,z)$ be a lattice. Suppose that $\rho : \boldsymbol{C}/\Lambda \to \boldsymbol{R}^+$ is a function, normalized so that

$$\int_{\boldsymbol{C}/\Lambda} \rho^2 \; dxdy = 1. \tag{11}$$

For each $y \in \boldsymbol{R}$, we define

$$f(y) = \int_0^1 \rho(x+iy)dx \tag{12}$$

We define

$$\mu(\Lambda,\rho) = \inf_{y \in \boldsymbol{R}} f(y). \tag{13}$$

So far, these definitions pertain to a specific choice of ρ. Finally, we define

$$\mu(\Lambda) = \sup_{\rho} \mu(\Lambda,\rho). \tag{14}$$

For this last equation, we are extremizing over all choices of ρ.

The function ρ is known as a *conformal metric* on $\boldsymbol{C}/\Lambda$. The first integral expresses the condition that the total area in this metric is 1. The integral $f(y)$ measures the length of the horizontal loop at height y relative to this metric. The quantity $\mu(\Lambda,\rho)$ measures the length of the shortest horizontal loop relative to this metric. The final quantity maximizes the length of the shortest loop, over all possible unit area conformal metrics. This quantity is known as the *extremal length* of a horizontal loop in $\boldsymbol{C}/\Lambda$.

Here is the basic result.

Lemma 6.1 *Let $\{p_n\}$ be a sequence of points in X that has no convergent subsequence. Let Λ_n be the lattice corresponding to p_n. Then $\mu(\Lambda_n) \to 0$.*

Proof: Let z_n be such that $\Lambda(1,z_n)$ corresponds to p_n. Replacing z_n by $z_n \pm 1$, we can assume that $z_n = x_n + y_n$ where $x_n \in [0,1]$. For ease of exposition, we will assume that $x_n = 0$. The general case requires small but slightly tedious modifications.

Since $\{p_n\}$ has no convergent subsequence, we have $y_n \to \infty$. We might as well re-index our sequence so that $y_n > n$. If this lemma is false, we can find some $a > 0$ and a function ρ_n so that $\mu(\Lambda_n,\rho_n) > a$ for all n.

Let R_n be the rectangle $[0,1] \times [0,n]$. The rectangle R_n consists of n unit squares stacked on top of each other. One of these squares has less than $(1/n)$ times the ρ_n-area. We can restrict ρ_n to this square and then rescale to get a new function $\alpha : R_1 \to \boldsymbol{R}^+$ such that

$$\int_{R_1} \alpha^2(x,y)\ dxdy < \epsilon; \qquad \int_0^1 \alpha(x+iy)\ dx \geq 2,$$

for all $y \in [0,1]$. Here we can make ϵ as small as we like by taking n large and suitably rescaling.

We can break R_1 into a $k \times k$ grid of squares so that α is constant on each square up to a factor of 2. Let α_{ij} be the minimum value of α on the ijth square on the grid. By hypothesis, we have

$$\sum_{i,j} \alpha_{ij}^2 \leq \epsilon; \qquad \sum_{i,j} \alpha_{ij} \geq k.$$

But the first quantity is minimized when $\alpha_{ij} = 1/k$, and the minimum is 1. This is a contradiction. ♠

7 Conformal Metrics on an Elliptic Curve

We already mentioned that a conformal metric on $\boldsymbol{C}/\Lambda$ is just a choice of a positive function ρ. We want to define something similar on an elliptic curve. Now the situation is more complicated, because elliptic curves are subsets of $P^2(\boldsymbol{C})$. This section is going to be a crash course on a bit of Riemannian geometry.

Let E be an elliptic curve. The important feature of E is that it is nonsingular. For each $P \in E$ there is a tangent line, $T_P(E)$, which is a copy of $\boldsymbol{C}$. Some of you may recognize the nonsingularity condition as saying that E is a *manifold*.

A *conformal metric* on E is a choice of nontrivial function

$$\rho_P : T_P(E) \to \boldsymbol{R}$$

for each $P \in E$. The function ρ_P should have the property that

$$\rho_P(az) = |a|\rho_P(z) \tag{15}$$

for all $a \in \boldsymbol{C}$ and all $z \in T_P(E)$. Also, the function should always assign positive numbers to nonzero elements of $T_P(E)$. A conformal metric on E is a special case of a *Riemannian metric* on E.

Given a conformal metric on E we can use it to measure the speeds of curves on E. If we have a curve $\gamma(t)$ on E, the derivative $\gamma'(t)$ is naturally an element of $T_{\gamma(t)}(P)$. So, we can use $\rho_{\gamma(t)}$ to define the speed of $\gamma(t)$. Namely

$$|\gamma'(t)| = \rho_{\gamma(t)}(\gamma'(t)). \tag{16}$$

Once we have the notion of speed, we can integrate it to obtain the notion of arc length. That is, the length of the portion of γ joining $\gamma(a)$ to $\gamma(b)$ is

$$\int_a^b |\gamma'(t)|\; dt.$$

The notion of a conformal metric ties in nicely to the concept we introduced in the previous section. Let $\Psi : \boldsymbol{C}/\Lambda \to E$ be the Weierstrass map and suppose E comes with a conformal metric. There is a function $\rho : \boldsymbol{C}/\Lambda \to \boldsymbol{R}$ such that Ψ is an *isometry*: The length of any curve γ on $\boldsymbol{C}/\Lambda$ with respect to ρ is the same as the length of $\Psi(\gamma)$ with respect to the conformal metric on E. This works because the Weierstrass map is complex analytic. We say that the conformal metric on E has *unit area* if ρ has unit area in the sense of the previous section.

8 Properness

Now we prove that f is proper.

Let $\{p_n\}$ be a sequence of points in X that has no convergent subsequence. Let Λ_n be the lattice corresponding to p_n. We have $\mu(\Lambda_n) \to 0$, by Lemma 6.1.

Let E_n be the elliptic curve corresponding to $f(p_n)$. Suppose that $\{E_n\}$ has a convergent subsequence. Passing to a subsequence, we can assume that $\{E_n\}$ converges to some limit elliptic curve E. We can choose a unit area conformal metric γ_n on E_n, and we can arrange that these metrics converge to a unit area conformal metric γ on the limit E. There is some $\epsilon > 0$ so that every loop on E has length at least 2ϵ relative to γ. Hence, once n is large, every closed loop on E_n has length at least ϵ relative to γ_n.

Let ρ_n be the function on $\boldsymbol{C}/\Lambda$ so that the Weierstrass map is an isometry from $\boldsymbol{C}/\Lambda_n$ to E_n relative to ρ_n and γ_n. Referring to our notation of extremal length, we would have $\mu(\Lambda_n, \rho_n) \geq \epsilon$. But this contradicts that fact that $\mu(\Lambda_n, \rho_n) \leq \mu(\Lambda_n)$ and $\mu(\Lambda_n) \to 0$.

Hence f is proper. Just to summarize, we now know that $f : X \to Y$ is injective, continuous, and proper. So, by Invariance of Domain, f is a homeomorphism. In particular, f is surjective. So, up to projective equivalence, every Weierstrass elliptic curve has a Weierstrass uniformization.