Notes on Weierstrass Uniformization

Rich Schwartz

April 25, 2011

1 Introduction

In the Spring of 2011, I taught Math 1540 at Brown. This is the second semester of our undergraduate algebra sequence. As a portion of the class, I taught about elliptic curves, using Silverman and Tate's *rational points on elliptic curves* as a text. In particular, I wanted to verify all the claims made in the book about Weierstrass uniformization. I wrote these notes so that someone with essentially no background in complex analysis could see all the main results after about 30 pages of not-too-hard reading. The notes are divided into 3 sections:

- **A primer on complex analysis:** This explains all the results in complex analysis you need to know in order to understand Weierstrass Uniformization and why it works.
- **Weierstrass Uniformization:** This explains how one starts with a lattice Λ in the plane and produces a bihilomorphic group isomorphism from $\boldsymbol{C}/\Lambda$ to some elliptic curve in Weierstrass form.
- **Global Properties:** This explains why, up to projective equivalence, every elliptic curve in Weierstrass form is obtained from the Weierstrass Uniformization construction. This part is somewhat sketchy, and wades into the deeper waters of moduli space.

While I made a decent effort to proof-read the notes, I did not try to polish them to the extent that they could appear in a book. In particular, I didn't worry too much about things like the fine points of grammar and punctuation. Nonetheless, I hope that all the math is essentially correct.

2 A Primer on Complex Analysis

2.1 A Resume of Results

Let U be an open set in $\boldsymbol{C}$, the complex plane. Let $f : U \to \boldsymbol{C}$ be a continuous map. We say that f *has a complex derivative* at $z \in U$ if the quotient

$$f'(z) = \lim_{h \to 0} \frac{f(z+h) - f(z)}{h}$$

exists and is finite. Note that h is allowed to be a complex number. f is said to be *complex analytic* (or CA for short) in U if $f'(z)$ exists for all $z \in U$ and the function $z \to f'(z)$ varies continuously in U. Here is everything you need to know from complex analysis to understand Weierstrass uniformization.

1. **Bounded Implies Constant:** Suppose $f : \boldsymbol{C} \to \boldsymbol{C}$ is is CA and bounded, then f is constant.

2. **Removable Singularities:** Let U be an open set and let $b \in U$ be a point. Suppose that $f : U - \{b\} \to \boldsymbol{C}$ is CA and f is bounded in a neighborhood of b. Then f extends to all of U and is CA on U.

3. **Non-Vanishing:** Suppose that f is CA in a neighborhood of $a \in \boldsymbol{C}$, and not identically 0. Then there is some m such that $f(z+a) = z^m g(z)$ where g is CA in a neighborhood of 0 and $g(0) \neq 0$.

4. **Local Homeomorphism:** Let $f : U \to \boldsymbol{C}$ be a CA map. If $f'(a) \neq 0$ then there is some open disk Δ about a such that $f : \Delta \to f(\Delta)$ is a homeomorphism.

In general, a *homeomorphism* $f : X \to Y$ is a bijection $f : X \to Y$ such that f and f^{-1} are both continuous. Here X and Y are spaces in which continuity makes sense, e.g., metric spaces or topological spaces.

2.2 Cauchy–Riemann Equations

We can think of a CA function f as a map from $\boldsymbol{R}^2$ to $\boldsymbol{R}^2$ by writing

$$f(x+iy) = u(x+iy) + iv(x+iy).$$

To say that the complex derivative of f exists is the same as saying that f is differentiable and $df|_p$ (the differential at p) is the composition of a rotation and a dilation. That is

$$\begin{bmatrix} u_x & u_y \\ v_x & v_y \end{bmatrix} = \begin{bmatrix} r\cos(\theta) & r\sin(\theta) \\ -r\sin(\theta) & r\cos(\theta) \end{bmatrix}, \qquad r \in \boldsymbol{R}, \quad \theta \in [0, 2\pi).$$

Equating terms, we get

$$u_x = v_y; \qquad u_y = -v_x. \tag{1}$$

These are called the *Cauchy–Riemann equations*.

2.3 Complex Line Integrals

Suppose γ is a smooth oriented arc in $\boldsymbol{C}$ and f is a complex valued function defined in a neighborhood of γ. We define a complex line integral along γ as follows. Letting $g : [a, b] \to \gamma$ be a smooth parametrization of γ that respects the orientation of γ, we define

$$\int_\gamma f \; dz = \int_a^b f(g(t)) \frac{dg}{dt} \; dt. \tag{2}$$

From the change of variables formula for integration, the answer only depends on the orientation and not the parametrization. Were we to switch the orientation, the value of the line integral would switch signs.

If we have a finite union $\gamma = \{\gamma_j\}$ of smooth oriented arcs, we define

$$\int_\gamma f \; dz = \sum_j \int_{\gamma_j} f.$$

Theorem 2.1 (Cauchy) *Let γ be a loop made from finitely many smooth arcs. Suppose that f is CA in a neighborhood of the domain bounded by γ. Then $\int_\gamma f \; dz = 0$.*

Proof: Let $f = u + iv$. Letting dx and dy be the usual line elements, we can write

$$\int_{\partial D} f \; dz = \int_{\partial D} (u + iv)(dx + idy) = \int_{\partial D} (udx - vdy) + i \int_{\partial D} (vdx + udy).$$

By Green's theorem, the integral on the right-hand side equals

$$\int_D (u_y + v_x) dxdy + i \int_D (u_x - v_y) dxdy.$$

Both pieces vanish, due to the Cauchy–Riemann equations. ♠

2.4 The Cauchy Integral Formula

Here is the main technical tool we will use.

Theorem 2.2 (Cauchy Integral Formula) *Let γ be loop oriented counterclockwise around the domain D that it bounds. Let $a \in D - \gamma$. Suppose that f is CA in a neighborhood U of D. Then*

$$f(a) = \frac{1}{2\pi i} \int_\gamma \frac{f(z)}{z-a} dz. \tag{3}$$

Proof: We translate the whole picture and consider without loss of generality the case when $a = 0$. The function $g(z) = f(z)/z$ is CA in $U - \{0\}$. Let β be the circular polygon shown in Figure 1.

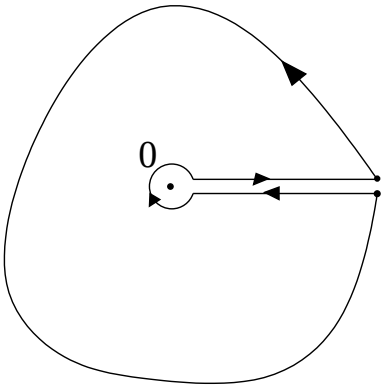

Figure 1.

We have

$$\int_\beta g \; dz = 0 \tag{4}$$

by Cauchy's Theorem. We allow the two oppositely oriented vertical segments in β to approach each other. In the limit, the contributions from the two vertical segments cancel out, and equation (4) yields

$$\int_\gamma g(z)dz = \int_\lambda g(z)dz. \tag{5}$$

Here λ is a counterclockwise circle centered at 0. But

$$\int_\lambda g(z)dz \approx f(0) \int_\lambda \frac{dz}{z} = 2\pi i f(0). \tag{6}$$

The approximation becomes exact as the radius of λ shrinks to 0. ♠

2.5 Bounded Functions

Suppose that $f : \boldsymbol{C} \to \boldsymbol{C}$ is a CA bounded function. We will show that $f'(a) = 0$ for all $a \in \boldsymbol{C}$.

Using the Cauchy Integral Formula, we compute

$$\lim_{h\to 0} \frac{f(a+h)-f(a)}{h} = \lim_{h\to 0} \frac{1}{2\pi i h}\Big(\int_\gamma \frac{f(z)}{z-a-h}dz - \int_\gamma \frac{f(z)}{z-a}dz\Big) =$$

$$\lim_{h\to 0} \frac{1}{2\pi i}\int_\gamma \frac{f(z)}{(z-a)(z-a-h)}dz = \frac{1}{2\pi i}\int_\gamma \frac{f(z)}{(z-a)^2}dz. \tag{7}$$

Equation 7 tells us that

$$f'(a) = \frac{1}{2\pi i}\int_\gamma \frac{f(z)}{(z-a)^2}dz. \tag{8}$$

Let N be the radius of γ. The length of γ is $2\pi N$. The numerator in Equation 8 is at most C. The denominator is at least $|N-a|^2$. Hence,

$$|f'(a)| \le \frac{CN}{|N-a|^2}. \tag{9}$$

Letting N tend to ∞, we see that $|f'(a)| = 0$. But a is arbitrary. Hence $f'(a) = 0$ for all $a \in \boldsymbol{C}$.

2.6 Removable Singularities

Here we will prove the following result:

Theorem 2.3 *Let U be an open set that contains a point b. Suppose that f is CA and bounded on $U - \{b\}$. Then $f(b)$ can be (uniquely) defined so that f is CA in U.*

Proof: Let γ and β and λ be the loops used to prove the Cauchy Integral Formula. So, λ is a small loop surrounding b and γ is a big loop surrounding b. Let $|\lambda|$ denote the radius of λ. Let D be the open domain bounded by γ. We define $g : D \to \boldsymbol{C}$ by the integral

$$g(a) = \frac{1}{2\pi i}\int_\gamma \frac{f(z)}{z-a}dz.$$

The same derivation used for Equation 7 shows that g is CA on all of D. We will show that $f(a) = g(a)$ for all $a \in D - \{b\}$. Once we know this, we set $f(b) = g(b)$ and we are done.

Now suppose that $a \neq b$. Since $f(z)$ is bounded in a neighborhood of b we have

$$\lim_{|\lambda| \to 0} \int_\lambda \frac{f(z)}{z-a} dz = 0.$$

But, by the Cauchy Integral Formula,

$$f(a) = \frac{1}{2\pi i} \int_\beta \frac{f(z)}{z-a} dz$$

no matter which choice of λ we make. Therefore

$$f(a) = \lim_{|\lambda| \to 0} \frac{1}{2\pi i} \int_\beta \frac{f(z)}{z-a} dz = \frac{1}{2\pi i} \int_\gamma \frac{f(z)}{z-a} dz = g(a).$$

So $f(a) = g(a)$ for all $a \in D - \{b\}$. ♠

2.7 The Maximum Principle

Let f be a complex analytic function in a connected open set U. Here we will show that f cannot take on its maximum value at a point in U unless f is constant. We will assume that f takes on a maximum at some point $a \in U$, and we will derive a contradiction. If f has an interior maximum, we can compose f with translations and dilations and arrange the following properties.

- $|f(0)| = 1$.
- U contains the unit disk.
- $|F(z)| \leq 1$ for all $|z| = 1$.
- $|F(z)| < 1$ for some z such that $|z| = 1$.

Let γ be the unit circle. By the Cauchy Integral Formula we have

$$1 = |f(0)| = \frac{1}{2\pi} \left| \int_\gamma \frac{f(z)}{z} \right| \leq^* \frac{1}{2\pi} \int_\gamma |f(z)| dz < 1.$$

This is a contradiction. The starred inequality is essentially the triangle inequality.

2.8 Non-Vanishing

Lemma 2.4 *Suppose, for all n, that the function $f(z)/z^n$ is well defined at 0 and complex analytic in a neighborhood of the unit disk. Then f is identically 0 on the unit disk.*

Proof: Let $g_n(z) = f(z)/z^n$. Let M be the maximum of f on the unit disk. Note that $|g_n(z)| = |f(z)|$ for $|z| = 1$. But the maximum principle, $|g_n(z)| \leq M$ for all z in the unit disk. Hence $|f(z)| \leq M|z|^n$. If $|z| < 1$, then

$$\lim_{n\to\infty} M|z|^n = 0.$$

Hence $|f(z)| = 0$ if $|z| < 1$. By continuity, $|f(z)| = 0$ if $|z| \leq 1$. ♠

Now we prove Item 3. We want to see that $f(a + z) = z^n g(a)$ for some CA function g such that $g(a) \neq 0$. We can translate the picture so that $a = 0$. Then we can dilate the picture so that f is defined and CA in a neighborhood of the closed unit disk Δ. If $f(0) \neq 0$, then we are done. If $f(0) = 0$, then the existence of $f'(0)$ guarantees that the function $f(z)/z$ is bounded on $\Delta - \{0\}$. But then $f(z)/z$ is CA in Δ. Hence $f(z) = zg_1(z)$, where $g_1(z)$ is CA in Δ.

If $g_1(a) \neq 0$ we are done. Otherwise, by the same argument, we can write $f(z) = z^2 g_2(z)$. And so on. The only way Item 3 could fail is that there is a sequence of CA functions $\{g_n\}$ such that $f(z) = z^n g_n(z)$ for all n. But then f satisfies the hypotheses of Lemma 2.4. Hence f vanishes identically in the unit disk. This is a contradiction.

2.9 Local Homeomorphism

Now we prove Item 4. Let $f : U \to \boldsymbol{C}$ be a CA function. We call f *normalized* if f is defined at 0 and $f(0) = 0$ and $f'(0) = 1$.

Lemma 2.5 *When f is normalized, we have a small disk Δ centered at 0 and an estimate*

$$\Big|(f(a) - f(b)) - (a - b)\Big| \leq \frac{|a - b|}{10}, \tag{10}$$

which holds for all $a, b \in \Delta$.

Proof: f' exists and is continuous. Hence, there is some small neighborhood Δ about 0 with the property that

$$|f'(z) - 1| < 10^{-100} \tag{11}$$

for all $z \in \Delta$. If γ is any curve in Δ, then the velocity of γ at z and the velocity of $f(\gamma)$ at $f(z)$ are nearly the same, by Equation 11. To get our result, we compare the straight unit speed line segment γ connecting a to b with the nearly straight, nearly unit speed, curve $f(\gamma)$ connecting $f(a)$ to $f(b)$. ♠

In what follows, we always take Δ to be as in Lemma 2.5 when we are talking about normalized functions.

Lemma 2.6 *Suppose f is normalized. Then f is one to one on Δ and f^{-1} is continuous on $f(\Delta)$.*

Proof: The fact that f is one to one follows immediately from Equation 10. Equation 10 also gives us the bound $|f(a) - f(b)| > |a - b|/2$ for all $a, b \in \Delta$. But then we have $f^{-1}(a) - f^{-1}(b)| < 2|a - b|$ for all $a, b \in f(\Delta)$. This bound obviously does the job. ♠

The next result has many different kinds of proofs, but none of the proofs is really easy. We'll give a geometrical proof. As you read this proof, you should think about a bad game of golf: The player hits the ball towards the hole but misses slightly. The next put comes closer, etc. In the limit, the ball goes in the hole.

Lemma 2.7 *Suppose f is normalized Then $f(\Delta)$ contains a neighborhood of 0.*

Proof: Let r be the radius of Δ. Suppose $\alpha \in \boldsymbol{C}$ satisfies $|\alpha| < r/10$. Let $a_0 = \alpha$. We have

$$|a_0| < r/10; \qquad |\alpha - f(a_0)| < r/100.$$

The second bound comes from Equation 10. In general, suppose that

$$|a_n| < r/10 + r/100 + ... + r/10^n < r; \qquad |f(a_n) - \alpha| < r/10^{n+1},$$

we define

$$a_{n+1} = a_n + \alpha - f(a_n).$$

Note that

$$|a_{n+1}| < r/10 + r/100 + ... + r/10^{n+1} < r.$$

Hence $a_n, a_{n+1} \in \Delta$. Equation 10 then gives

$$|f(a_{n+1}) - \alpha| = |(f(a_{n+1}) - f(a_n)) - (a_{n+1} - a_n)| \leq$$

$$\frac{|a_{n+1} - a_n|}{10} = \frac{|f(a_n) - \alpha|}{10} < r/10^{n+2}.$$

So, we can define $a_1, a_2, ...$ inductively. By construction $|\alpha - f(a_n)| \to 0$ as $n \to \infty$. By continuity $f(a) = \alpha$ where $a = \lim a_n$. ♠

Lemma 2.8 *Suppose that $f : U \to \boldsymbol{C}$ is CA and $f'(a) \neq 0$ for some $a \in U$. Then*

- *f is one to one in a neighborhood Δ of a.*
- *$f(\Delta)$ contains an open neighborhood of $f(a)$.*
- *$f^{-1} : f(\Delta) \to \Delta$ is continuous.*

Proof: We can scale f so that $a = 0$ and f is normalized. This scaling does not change the conclusions of the lemma. This result now follows from everything we have proved about normalized functions. ♠

We are almost to the point of proving the first part of Item 4. Here is the last step.

Lemma 2.9 *Suppose that $f : U \to \boldsymbol{C}$ is CA and $f'(a) \neq 0$ for some $a \in U$. Then, for all sufficiently small open sets V containing a, the set $f(V)$ is open.*

Proof: V just has to be small enough so that $f'(b) \neq 0$ for all $b \in V$. But then the previous result shows that $f(V)$ contains an open set that contains $f(b)$, for all $b \in V$. This proves that $f(V)$ is open. ♠

3 Weierstrass Uniformization

3.1 Lattices

Say that 2 complex numbers α and β are *independent* of α/β is not real. For instance 1 and i are independent.

A *lattice* in $\boldsymbol{C}$ is a set of points of the form

$$\Lambda = \{m\alpha + n\beta \quad m, n \in \boldsymbol{Z}\}, \tag{12}$$

where α and β are independent numbers. The set of points in Λ forms a grid of parallelograms. The classic case is when $\alpha = 1$ and $\beta = i$. In this case $\Lambda = \boldsymbol{Z}[i]$, the Gaussian integers.

The quotient $\boldsymbol{C}/\Lambda$ has several nice properties.

1. $\boldsymbol{C}/\Lambda$ is homeomorphic to a torus – namely, a single parallelogram with its sides identified.

2. $\boldsymbol{C}/\Lambda$ abelian group under addition, since both $\boldsymbol{C}$ and Λ are abelian groups under addition.

A map $f : \Lambda \to \boldsymbol{C}$ is called Λ-*periodic* if $f(\lambda + z) = f(z)$ for all $z \in \boldsymbol{C}$ and all $\lambda \in \Lambda$. In this case, f induces a map from $\boldsymbol{C}/\Lambda$ into $\boldsymbol{C}$. This new map is usually also denoted by f. We can also talk about Λ-periodicity when f is not defined at all points of $\boldsymbol{C}$. In the case of interest, we will be able to interpret f as a map from $\boldsymbol{C}$ to $\boldsymbol{C} \cup \infty$.

3.2 The Weierstrass Function

Let Λ be any lattice. Informally, the function we are interested in is

$$\sum_{\lambda \in \Lambda} \frac{1}{(z-\lambda)^2} \tag{13}$$

The nice thing about this "function" is that it is clearly Λ-periodic. The bad thing is that the series above does not converge, so the "function" does not exist.

The Weierstrass function is the function that the expression in Equation 13 wants to be. Here is the definition.

$$P(z) = \frac{1}{z^2} + \sum_{\lambda \neq 0} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right) = \frac{1}{z^2} + \sum_{\lambda \neq 0} \frac{2z\lambda - z^2}{\lambda^2 (z - \lambda^2)}. \tag{14}$$

To study the convergence of this series, choose $z \notin \Lambda$. For all λ sufficiently large, we have the estimate

$$\Big|\frac{z^2 - 2z\lambda}{\lambda^2(z-\lambda^2)}\Big| < \frac{C_z}{|\lambda|^3}. \tag{15}$$

Here C_z is a constant that depends on z in a way that we don't care about. The series in Equation 14 does converge because the corresponding series

$$\sum_{\lambda \neq 0} \frac{1}{|\lambda|^3}$$

converges.

The Weierstrass function $P(z)$ is defined for all $z \in \boldsymbol{C} - \Lambda$. As $z \to \lambda \in \Lambda$, the quantity $|P(z)|$ tends to ∞. One says that $P(z)$ has *poles* at points of Λ.

3.3 Differentiability

In this subsection we'll prove that the function P is complex analytic on $\boldsymbol{C} - \Lambda$ and that

$$P'(z) = \sum_{\lambda \in \Lambda} \frac{-2}{(z-\lambda)^3}, \qquad \forall z \in \boldsymbol{C} - \Lambda. \tag{16}$$

This is the standard proof that term-by-term differentiation works.

For any N we can write $P = P_N + R_N$, where

$$P_N(z) = \frac{1}{z^2} + \sum_{0<|\lambda|<N} \Big(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\Big). \tag{17}$$

and R_N is the remainder. In other words, P_N is defined just like P, except we only sum over the lattice points inside the disk of radius N.

Since P_N just involves a finite number of terms, we have

$$dP_N/dz = \lim_{h \to 0} \frac{P_N(z+h) - P_N(h)}{h} = \sum_{|\lambda|<N} \frac{-2}{(z-\lambda)^3} \tag{18}$$

Note that the case $\lambda = 0$ is included in the sum.

To understand what happens to the remainder, we write

$$R_N = \sum_{|\lambda \geq N} f_\lambda(z); \qquad f_\lambda(z) = \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}. \tag{19}$$

We have

$$\frac{f_\lambda(z+h)-f_\lambda(z)}{h}=\frac{2\lambda-h-2z}{(z-\lambda)^2(z-\lambda-h)^2}. \tag{20}$$

For now on, we suppose $|h|<1$. Also, we fix z. Once $|\lambda|$ is large ebough we have

$$\left|\frac{f_\lambda(z+h)-f_\lambda(z)}{h}\right|<\frac{C_z}{|z-\lambda|^3}. \tag{21}$$

Again, the constant C_z depends on z in a way that we don't care about. For any $\epsilon_1>0$ we can choose N large enough so that

$$\left|\frac{R_N(z+h)-R_N(z)}{h}\right|<C_z\sum_{|\lambda\geq N}\frac{1}{|z-\lambda|^3}<\epsilon_1. \tag{22}$$

From Equation 22 we have

$$\begin{aligned}\left|\frac{P(z+h)-P(z)}{h}-\sum_\lambda\frac{-2}{(z-\lambda)^3}\right|\leq\\ \epsilon_1+\left|\frac{P_N(z+h)-P_N(z)}{h}-\sum_\lambda\frac{-2}{(z-\lambda)^3}\right|\leq\\ \epsilon_1+\epsilon_2+\left|\frac{P_N(z+h)-P_N(z)}{h}-\sum_{|\lambda|<N}\frac{-2}{(z-\lambda)^3}\right|\leq\\ \epsilon_1+\epsilon_2+\epsilon_3\end{aligned} \tag{23}$$

The terms ϵ_1 and ϵ_2 tend to 0 as $N\to\infty$, and the term ϵ_3, which comes from Equation 18, tends to 0 as $h\to 0$. This proves that

$$\lim_{h\to 0}\left|\frac{P(z+h)-P(z)}{h}-\sum_\lambda\frac{-2}{(z-\lambda)^3}\right|=0. \tag{24}$$

3.4 The Differential Equation

In this subsection we'll establish the differential equation

$$(P')^2=4P^3+g_2P+g_3. \tag{25}$$

A function f is called *even* if $f(-z)=f(z)$ for all z. Also, f is called *odd* if $f(-z)=-f(z)$ for all z.

Lemma 3.1 *P is even and Λ-periodic.*

Proof: Since $1/z^2$ is even, it suffices to prove that $Q(z) = P(z) - 1/z^2$ is even. Since P' is odd, so is Q'. Also, $Q(0) = 0$. Since Q' is odd and $Q(0) = 0$, we get that Q is even. Hence P is even.

Now we show periodicity. Let $\lambda \in \Lambda$ be any point. Let $Q(z) = P(z+\lambda) - P(z)$. From Equation 16 we see that $P'(z)$ is clearly Λ-periodic. Therefore $Q'(z) = 0$. Hence $Q(z) = C_\lambda$, a constant that perhaps depends on λ. We just have to show that $C_\lambda = 0$. But

$$C_\lambda = P(-\lambda/2 + \lambda) - P(-\lambda/2) = P(\lambda/2) - P(-\lambda/2) = 0,$$

since P is even. ♠

Lemma 3.2 *In a neighborhood of* 0 *we have*

$$P(z) = \frac{1}{z^2} + z^2 m_1(z); \qquad P'(z) = \frac{-2}{z^3} + z m_2(z).$$

Here m_1 *and* m_2 *are CA in a neighborhood of* 0.

Proof: Let $Q(z) = P(z) - 1/z^2$. $Q(z)$ is even and $Q(0) = 0$. Since $Q(0) = 0$ and Q is CA, the quotient $Q(z)/z$ is bounded in a neighborhood of 0. So, we can write $Q(z) = zR(z)$ where $R(z)$ is CA in a neighborhood of 0. Note that $R(z)$ is odd. Hence $R(0) = 0$. The same argument now shows that $R(z) = zm_1(z)$. Hence $Q(z) = z^2 m_1(z)$. This gives the first equation. The second equation comes from differentiating the first one. ♠

Lemma 3.2 tells us that

$$A(z) = 4P^3 - g_2 P - g_3 - (P')^2 = \frac{m_3(z) + g_2}{z^2} + g_3 + m_4(z), \qquad (26)$$

where m_3 and m_4 are CA in a neighborhood of 0. We choose g_2 so that $m_3(0) + g_2 = 0$. We choose g_3 so that A vanishes at some point.

Lemma 3.3 $A(z)$ *is bounded in a neighborhood of* 0.

Proof: Consider the function $q(z) = m_3(z) + q_2$. Is suffices to prove that $q(z)/z^2$ is bounded in a neighborhood of 0. The function $q(z)$ is even and $q(0) = 0$. The same argument as in Lemma 3.2 shows that $q(z) = z^2 s(z)$,

where $s(z)$ is CA in a neighborhood of 0. This does it. ♠

The function $A(z)$ is Λ-periodic. Hence $A(z)$ is bounded in a neighborhood of each lattice point. On the other hand, $A(z)$ is CA in $\boldsymbol{C} - \Lambda$. So, A is bounded in the complement of any neighborhood of Λ. Hence A is bounded. All the singularities of A are removable, so A extends to a bounded CA function on $\boldsymbol{C}$. But then A is constant. Our choice of g_3 gives $A = 0$. This establishes Equation 25.

Remark: With a bit of effort, one can trace through the proof below and prove that

$$g_2 = \sum_{\lambda \neq 0} \frac{-60}{\lambda^4}; \qquad g_3 = \sum_{\lambda \neq 0} \frac{-140}{\lambda^6}. \tag{27}$$

3.5 Map to the Elliptic Curve

Let E be the elliptic curve

$$y^2 = 4x^3 + g_2 x + g_3. \tag{28}$$

We will assume that this elliptic curve is nonsingular, meaning that

$$4g_2^3 + 27g_3^2 \neq 0.$$

In fact, all choices of Λ have this property, but this is a bit of a digression to prove.

There is a map from $\boldsymbol{C}$ into E, given by

$$\Psi(z) = (P(z), P'(z)). \tag{29}$$

Equation 25 tells us that this map actually lands in E. When $z \in \Lambda$, we define $\Psi(z) = [0:1:0]$, the infinite point.

Since Ψ is Λ-periodic, Ψ induces a map (with the same name)

$$\Psi : \boldsymbol{C}/\Lambda \to E. \tag{30}$$

The map Ψ is called the *Weierstrass uniformizing map*.

3.6 Branch Points

As a prelude to understanding the map Ψ, we need some information about the derivatives of P. A *branch point* of P is a point z such that $P'(z) = 0$. In this subsection we characterize the branch points. Let $\frac{1}{2}\Lambda$ denote the set of points of the form $\lambda/2$ where $\lambda \in \Lambda$. Let $\Lambda' = \frac{1}{2}\Lambda - \Lambda$. We will prove:

- $P'(z) = 0$ if $z \in \Lambda'$.
- $P'(z) = 0$ only if $z \in \Lambda'$.
- $P''(z) \neq 0$ if $z \in \Lambda'$.

Suppose that $z \in \Lambda'$. Then

$$P(z+h) = P(z+h-2z) = P(-z+h) = P(z-h). \tag{31}$$

The first equality comes from the fact that $2z \in \Lambda$ and that P is Λ-periodic. The last equality comes from the fact that Λ is even. Since P' is continuous,

$$2P'(z) = \lim_{h \to 0} \frac{P(z+h) - P(z-h)}{h} = 0.$$

It is convenient to define $Q = P'$. Suppose that $Q(a) = 0$. We can write $Q(a+z) = z^m g(z)$, where $g(0) \neq 0$ and m is some integer. We define m to be the *multiplicity* of a. This notion of multiplicity coincides with the notion of the multiplicity of a root of a polynomial. If both $Q(a)$ and $Q'(a)$ are 0 then a has multiplicity greater than 1. So, either of the remaining claims above fails, the equation $Q = 0$ has at least 4 solutions in $\boldsymbol{C}/\Lambda$, counting multiplicity.

The multiplicity has the following topological interpretation. Suppose that C is a loop that surrounds a and no other roots of Q. Then the multiplicity of a counts the number of times $Q(C)$ winds around 0. More generally, if C is a loop that surrounds the roots $a_1, ..., a_k$ of Q, then the sum of multiplicities of $a_1, ..., a_k$ counts the number of times $Q(C)$ winds around 0. The multi-root case can be deduced from the single root case by considering pictures of the kind shown in Figure 1. The idea is that the winding number of the outer loop, the loop we care about, is the same as the winding number of the inner loop, and the winding number of the inner loop is the sum of the winding numbers of the 3 small loops surrounding the individual roots.

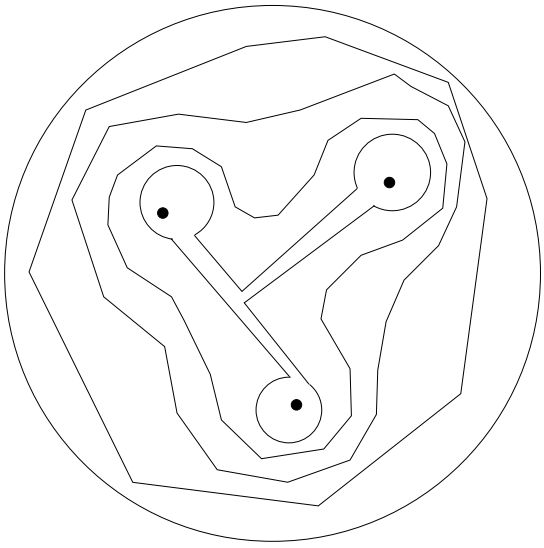

Figure 1.

For any $u \in \boldsymbol{C}$ we define $N(u)$ to be the number of solutions to the equation $Q(z) - u = 0$, counting multiplicity. We suppose that $N(0) \geq 4$. By Equation 16, we have

$$Q(z) = \frac{1}{z^3} + g(z),$$

where $g(z)$ is CA in a neighborhood of 0. From this equation we see that $Q(z) - u = 0$ only has solutions near lattice points when $|u|$ is large, and moreover that $N(u) = 3$ when $|u|$ is large.

It follows from the topological interpretation of multiplicity that the function $u \to N(u)$ varies continuously. On the other hand, this function is integer-valued. Hence, it is impossible for $N(0) > 3$. This is a contradiction. This completes our proofs of the claims.

3.7 Regularity of the Map

In this subsection we will show that Ψ is a regular map. This is to say that Ψ' never vanishes. First, suppose that $z \in \boldsymbol{C} - \Lambda$. We have $\Psi'(z) = (P'(z), P''(z))$. Note that $P'(z)$ and $P''(z)$ are not both zero, by the result in §3.6.

It remains to consider the case when $z \in \Lambda$. Since Ψ is Λ-periodic, it suffices to consider the case $z = 0$. The secret in this case is to change

coordinates to that we are still dealing with a map into $\boldsymbol{C}^2$. We can't use the usual copy of $\boldsymbol{C}^2$ sitting inside $P^2(\boldsymbol{C})$, so we will use one of the other copies. We have $\Psi(0) = [0:1:0]$. To analyze the derivative, we consider the picture in the plane $\boldsymbol{C}^2$ consisting of points $y = 1$. For points $z \in \boldsymbol{C}$ near 0,

$$\Psi(z) = [P(z), P'(z) : 1] = [P(z)/P'(z) : 1 : 1/P'(z)].$$

Consider the first coordinate, $g(z) = P(z)/P'(z)$. From Lemma 3.2, the function $g(z)$ is bounded in a neighborhood of 0. Also, $\lim_{z\to 0} |g(z)| = 0$. So, we can write $g(z) = zh(z)$. If $h(0) = 0$ then $g(z) = z^2 m(z)$, where $m(z)$ is CA in a neighborhood of 0. This contradicts Lemma 3.2. So, $h(0) \neq 0$. But then $g'(0) \neq 0$. Hence $\Psi'(0) \neq 0$.

3.8 Surjectivity of the Map

Now we'll show that $\Psi : \boldsymbol{C}/\Lambda \to E$ is onto. Be warned that this subsection requires a bit of background in real analysis. The main result we will use is that a nonempty subset of E, which is both open and closed, must be all of E. This follows from the fact that E is connected. Obviously $\Psi(\boldsymbol{C}/\Lambda)$ is nonempty. So, we just need to show that this set is open and closed.

Closed: This follows from the fact that $\boldsymbol{C}/\Lambda$ is compact, and Ψ is continuous. The continuous image of a compact set is always closed. Here is a more elementary argument, which explains the meaning of "compactness". Choose some point w that lies in the closure of $\Psi(\boldsymbol{C}/\Lambda)$. By definition, there is a sequence $\{z_i\}$ in $\boldsymbol{C}/\Lambda$ such that $\Psi(z_i)$ converges to w. Since $\boldsymbol{C}/\Lambda$ is compact, we can pass to a subsequence so that $\{z_i\}$ is a convergent subsequence. Let $z = \lim z_i$. By continuity $\Psi(z) = w$. Hence $w \in \Psi(\boldsymbol{C}/\Lambda)$. Since w was an arbitrary point in the closure of $\Psi(\boldsymbol{C}/\Lambda)$, we see that $\Psi(\boldsymbol{C}/\Lambda)$ contains its closure. Hence $\Psi(\boldsymbol{C}/\Lambda)$ is closed.

Open: Let $a \in \boldsymbol{C}$. Let L be the tangent line to E at a. Let π be the projection map from E onto L. Since E is a nonsingular elliptic curve, π is a local homeomorphism from a neighborhood of $\Psi(a)$ in E to an open set in L.

Consider the auxilliary map

$$\pi \circ \Psi : \boldsymbol{C} \to L.$$

This is a C.A. map from $\boldsymbol{C}$ to L, and L is just a copy of $\boldsymbol{C}$. The map $\pi \circ \Psi$ is C.A. Since Ψ is regular, the derivative of $\pi \circ \Psi$ does not vanish at a. Hence, $\pi \circ \Psi$ is a local homeomorphism. Hence $\pi \circ \Psi$ maps an open neighborhood U of a in $\boldsymbol{C}$ onto an open neighborhood of $\pi \circ \Psi(a)$ in L. Given what we have already said about π, we see that $\Psi(U)$ is an open set in E which contains $\Psi(a)$. This shows that every point of $\Psi(\boldsymbol{C})$ is contained in an open subset of $\Psi(\boldsymbol{C})$. Hence $\Psi(\boldsymbol{C})$ is open in E.

Remark: We actually didn't need to know that Ψ is a regular map. It always happens that the image of an open set under a non-trivial CA map is open.

3.9 Injectivity of the Map

Here we will show that Ψ is injective. Let $X \subset \boldsymbol{C}/\Lambda$ denote those points where Ψ is not injective. That is, each $a \in X$ is such that there is some distinct $b \in X$ such that $\Psi(a) \neq \Psi(b)$. Note that $[0] \notin X$ since $[0]$ is the only point of $\boldsymbol{C}/\Lambda$ which Ψ maps to the line at infinity. So, X is not all of $\boldsymbol{C}/\Lambda$. We will show that X is both open and closed. Since $\boldsymbol{C}/\Lambda$ is connected, this shows that X is empty!

Closed: Suppose a lies in the closure of X. Let $\{a_n\}$ be a sequence in X converging to a. Let $\{b_n\}$ be a sequence so that $\Psi(a_n) = \Psi(b_n)$. Passing to a subsequence, we can assume that $b_n \to b$. By continuity, we have $\Psi(a) = \Psi(b)$. We just have to prove that $a \neq b$. Since Ψ is regular, Ψ is a homeomorphism from a neighborhood U of a into E. The restriction of Ψ to U is injective. But $a_n \in U$ for n large. Hence $b_n \notin U$ for n large. Hence $b \notin U$. Hence $a \neq b$. This proves that $a \in X$. Hence X is closed.

Open: Suppose that $a \in X$. Let $b \in X$ be such that $\Psi(a) = \Psi(b)$ and $a \neq b$. Since Ψ is regular, there are small disks U_a and U_b about a and b such that $\Psi(U_a)$ and $\Psi(U_b)$ are both open sets containing the common point $w = \Psi(a) = \Psi(b)$. We can take U_a and U_b so small that they are disjoint, and we can shrink U_a to be so small that $\Psi(U_a) \subset \Psi(U_b)$. But then $U_a \subset X$. Hence X contains an open set which contains a. Since a was an arbitrary point of X, this shows that X is open.

3.10 Crash Course on Riemann Surfaces

It only remains to show that Ψ is a group isomorphism. Before we do this, we need to make a little digression. We would like to say when a map $f : E \to E$ is complex analytic. This doesn't quite make sense, because E is not really $\boldsymbol{C}$. However, E is nonsingular, and there is a projection from E to each of its tangent planes. We will use these projections to talk about CA maps of E. Essentially, we are treating E as a Riemann surface, but we are doing to do it without making a big fuss about a formal definition of a Riemann surface.

Given $a \in E$ let $\pi_a : E \to L$ be the projection from E to the tangent line at a. We have already considered these maps. Suppose that $\phi : E \to E$ is a map of E and $b = \phi(a)$. We say that f is CA at a if

$$\pi_b \circ f \circ \pi_a^{-1} \tag{32}$$

is CA in a neighborhood of $\pi_a(a)$. The map π_a^{-1} makes sense at least in a neighborhood of $\pi_a(a)$.

Lemma 3.4 *$f : E \to E$ is CA if and only if $\Psi^{-1} \circ f \circ \Psi$ is a CA map of $\boldsymbol{C}/\Lambda$.*

Proof: The point is that the coordinates of Ψ are CA maps. So, this is just an exercise in the chain rule. ♠

Here is the main example of interest to us. Let $T_A : E \to E$ denote addition by A. That is $T_A(P) = A + P$ for all $P \in E$.

Lemma 3.5 *T_A is a CA map of E.*

Proof: Recall that there are rational functions describing the group law on E. Hence, the coordinates of T_A are rational functions. The compositions in Equation 32 are rational functions on $\boldsymbol{C}$. (Here we are thinking of the tangent lines as copies of $\boldsymbol{C}$.) Hence, the compositions in Equation 32 are all CA. So, by definition T_A is CA. ♠

3.11 Group Isomorphism

Now we will show that $\Psi : \boldsymbol{C}/\Lambda \to E$ is a group isomorphism. We want to show that $\Psi(a+b) = \Psi(a) + \Psi(b)$ for any $a, b \in \boldsymbol{C}/\Lambda$. Let $A = \Psi(a)$ and $B = \Psi(b)$. Let $T_A : E \to E$ denote addition by A. This is a CA map of E. Define

$$\tau_A = \Psi^{-1} \circ T_A \circ \Psi \tag{33}$$

Lemma 3.6 *τ_A is a translation.*

Proof: T_A is a CA map of E. At the same time, T_A is a homeomorphism with no fixed points. Hence τ_A is a CA homeomorphism of $\boldsymbol{C}/\Lambda$ with no fixed points. Let $\tau = \tau_A$. We have the quotient map $\pi : \boldsymbol{C} \to \boldsymbol{C}/\Lambda$. Let $g = \pi \circ \tau : \boldsymbol{C} \to \boldsymbol{C}/\Lambda$. The derivative g' makes sense as a map from $\boldsymbol{C} \to \boldsymbol{C}$. Since g' is continuous and Λ-periodic, there is some M such that $|g'| < M$. But then g' is both bounded and CA. Hence g' is constant. Hence τ' is constant. Since τ preserves the area of $\boldsymbol{C}/\Lambda$, we must have $|\tau'| = 1$. If τ had any rotational component, it would have a fixed point. Hence $\tau' = 1$. This implies that τ is a translation. ♠

We have

$$\tau_A(0) = \Psi^{-1} \circ T_A \circ \Psi(0) = \Psi^{-1} \circ T_A([0:1:0]) = \Psi^{-1}(A) = a. \tag{34}$$

Likewise $\tau_B(0) = b$. Since τ_A is a translation and $\tau_A(0) = a$,

$$\tau_A(b) = a + b. \tag{35}$$

But then

$$\tau_A \circ \tau_B(0) = \tau_A(b) = a + b. \tag{36}$$

On the other hand.

$$\tau_A \circ \tau_B(0) = (\Psi^{-1} \circ T_A \circ \Psi) \circ (\Psi^{-1} \circ T_B \circ \Psi)(0) =$$

$$\Psi^{-1} \circ T_A \circ T_B \circ \Psi(0) =$$

$$\Psi^{-1} \circ T_A \circ T_B([0:1:0]) = \Psi^{-1}(A + B).$$

In short

$$a + b = \tau_A \circ \tau_B(0) = \Psi^{-1}(A + B) \tag{37}$$

Applying Ψ, we see that $\Psi(a+b) = \Psi(a) + \Psi(b)$, as claimed.

4 Global Properties

The goal of this chapter is to explain why any elliptic curve over $\boldsymbol{C}$ has a Weierstrass uniformization, up to projective transformations. These notes are sketchy and they wade into topics that are beyond the scope of the class – moduli spaces, extremal length, and conformal metrics.

4.1 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.

4.2 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 4.1 (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 4.2 *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. ♠

4.3 The Space of Elliptic Curves

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

$$C_\infty : \qquad y^2 = x^3 + 1, \tag{38}$$

or

$$C_b : \qquad y^2 = x^3 + x + b; \tag{39}$$

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

$$b_\pm = \pm 2i/\sqrt{27}. \tag{40}$$

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

$$Y = \Big((\boldsymbol{C} \cup \infty) - b_+ - b_-\Big)/\pm \tag{41}$$

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.

4.4 The Space of Lattices

Recall that a lattice is a set of the form

$$\Lambda(\alpha, \beta) = \{m\alpha + n\beta | m, n \in \boldsymbol{Z}\}. \tag{42}$$

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 4.3 *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

$$g(z) = \pi_2(wz). \tag{43}$$

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

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}; \qquad ad - bc = 1. \tag{44}$$

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 4.4 *$\Lambda(\alpha, \beta) = \Lambda(\alpha', \beta')$ 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 4.5 *$\Lambda(1,z)$ and $\Lambda(1,z')$ are equivalent if and only if*

$$z' = \frac{az+b}{cz+d}; \qquad a,b,c,d \in \boldsymbol{Z}; \qquad ad-bc=1. \tag{45}$$

Proof: The "if" direction follows from Lemma 4.4. 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 44. So, $z' = M(wz)/M(w)$. Writing this out and cancelling the extra factor of w in both the numerator and denominator gives Equation 45. ♠

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 45.

4.5 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 4.6 *$g_2^* = w^{-4} g_2$ 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

$$P^*(z) = w^{-2} P(z/w). \tag{46}$$

By the chain rule,

$$(P^*)'(z) = w^{-3} P'(z/w). \tag{47}$$

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 4.7 *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 4.3. ♠

We want to use Lemma 4.2, 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 45. 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 4.8 *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 $f(u)$ for r small. ♠

Suppose we knew that f was also proper. Then we could conclude from Lemma 4.2 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...

4.6 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

$$\int_{\boldsymbol{C}/\Lambda}\rho^2\,dxdy=1. \tag{48}$$

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

$$f(y) = \int_0^1 \rho(x + iy) dx \tag{49}$$

We define

$$\mu(\Lambda, \rho) = \inf_{y \in \boldsymbol{R}} f(y). \tag{50}$$

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

$$\mu(\Lambda) = \sup_{\rho} \mu(\Lambda, \rho). \tag{51}$$

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 4.9 *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. ♠

4.7 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 subsection 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

$$\rho_P(az) = |a|\rho_P(z) \tag{52}$$

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

$$|\gamma'(t)| = \rho_{\gamma(t)}(\gamma'(t)). \tag{53}$$

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 subsection. 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 subsection.

4.8 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 4.9.

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.