# Elliptic curves over $\mathbb{C}$

We now consider elliptic curves over the complex numbers. Our main tool will be the correspondence between elliptic curves over $\mathbb{C}$ and tori $\mathbb{C}/L$ defined by lattices $L$ in $\mathbb{C}$ (see Definition 16.1). We will proceed to show the following:

1. Every lattice $L$ can be used to define an elliptic curve $E/\mathbb{C}$.
2. Every elliptic curve $E/\mathbb{C}$ arises from a lattice $L$.
3. If $E/\mathbb{C}$ is the elliptic curve corresponding to the lattice $L$, then there is an isomorphism

$$\mathbb{C}/L \xrightarrow{\Phi} E/\mathbb{C}$$

that is both analytic (as a mapping of complex manifolds) and algebraic: addition of points in $E(\mathbb{C})$ corresponds to addition in $\mathbb{C}$ modulo the lattice $L$.

This correspondence between lattices and elliptic curves over $\mathbb{C}$ is known as the *Uniformization Theorem*; we will spend this lecture and part of the next proving it.

To make the correspondence explicit, we need to specify the map $\Phi$ from $\mathbb{C}/L$ and an elliptic curve $E/\mathbb{C}$. This map is parameterized by *elliptic functions*, specifically the Weierstrass $\wp$-function. We will introduce general properties of elliptic functions in Section 16.1, specialize to the $\wp$-function in Section 16.3, and then construct the map $\Phi$ in Section 16.4.

Once we have fleshed out this correspondence, we obtain a powerful method to construct elliptic curves with desired properties. The arithmetic properties of lattices over $\mathbb{C}$ are usually easier to understand than those of the corresponding elliptic curve. In particular, by choosing an appropriate lattice, we can construct an elliptic curve with a given endomorphism ring. In the case of elliptic curves over $\mathbb{C}$, the endomorphism ring must either be $\mathbb{Z}$ or an order $\mathcal{O}$ in an imaginary quadratic field (a fact we will prove). The order $\mathcal{O}$ may be viewed as a lattice, and we will see that the elliptic curve corresponding to the torus $\mathbb{C}/\mathcal{O}$ has endomorphism ring $\mathcal{O}$.

This has important implications for elliptic curves over finite fields. If we choose a suitable prime $p$, we can reduce an elliptic curve $E/\mathbb{C}$ with complex multiplication to a curve $\bar{E}/\mathbb{F}_p$ with the same endomorphism ring $\mathcal{O}$. The endomorphism ring determines, in particular, the trace of the Frobenius endomorphism $\pi$ (up to a sign), which in turn determines the group order $\#E(\mathbb{F}_p) = p + 1 - \mathrm{tr}(\pi)$. This allows us to construct elliptic curves over finite fields that have a prescribed group order, using what is known as the *CM method*. As we will see, this has many practical applications, including cryptography and primality proving.

## 16.1 Elliptic functions

We begin with the definition of a lattice in the complex plane.

**Definition 16.1.** A *lattice* $L = [\omega_1, \omega_2]$ is an additive subgroup $= \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ of $\mathbb{C}$ generated by complex numbers $\omega_1$ and $\omega_2$ that are independent over $\mathbb{R}$.

**Example 16.2.** Let $\tau$ be the root of a monic quadratic equation $x^2 + bx + c$ with integer coefficients and negative discriminant. Then the lattice $[1, \tau]$ is the additive group of an imaginary quadratic order $\mathcal{O} = \mathbb{Z}[\tau]$. Conversely, if $\mathcal{O}$ is an imaginary quadratic order $\mathbb{Z}[\tau]$, then the additive group of $\mathcal{O}$ is the lattice $[1, \tau]$.

If we take the quotient of the complex plane $\mathbb{C}$ modulo a lattice $L$, we get a torus $\mathbb{C}/L$.

**Definition 16.3.** A *fundamental parallelogram* for $L = [\omega_1, \omega_2]$ is a set of the form

$$\mathcal{F}_\alpha = \{\alpha + t_1\omega_1 + t_2\omega_2 : \alpha \in \mathbb{C},\ 0 \le t_1, t_2 < 1\}.$$

We can identify the points in a fundamental parallelogram with the points of $\mathbb{C}/L$.

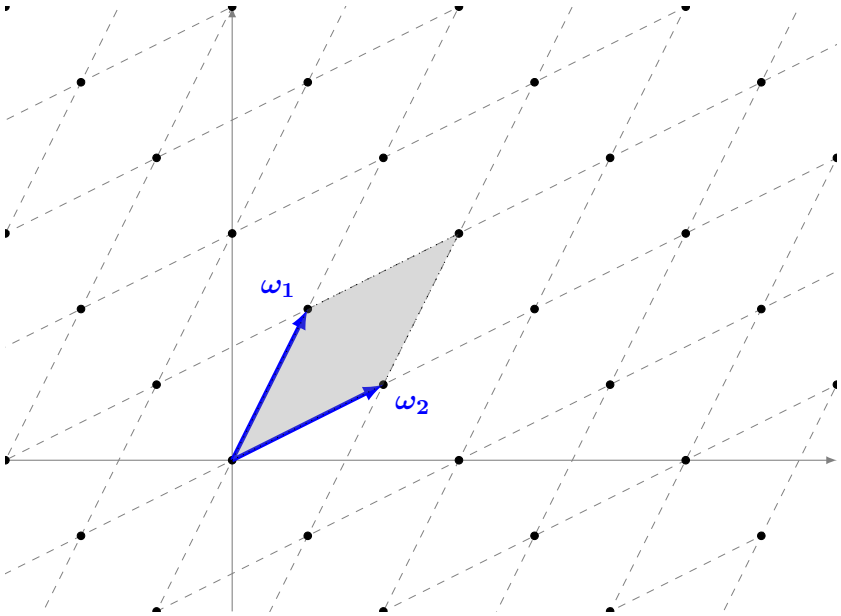



Figure 1: A lattice $[\omega_1, \omega_2]$ with a fundamental parallelogram shaded.

In order to define the correspondence between complex tori and elliptic curves over $\mathbb{C}$, we need to define the notion of an *elliptic function* on $\mathbb{C}$. As complex analysis is not a prerequisite for this course, we first define the terminology we need, which can be found in any standard textbook on the subject, including [1, 3].[1]

A function $f(z)$ defined on some open neighborhood of a point $z_0 \in \mathbb{C}$ is said to be *holomorphic* at $z_0$ if the complex derivative

$$f'(z_0) = \lim_{h \to 0} \frac{f(z_0 + h) - f(z_0)}{h}$$

exists.[2] We say that $f$ is holomorphic on an open set $\Omega$ if it is holomorphic at every $z_0 \in \Omega$, and we say that $f$ is holomorphic on a closed set $C$ if it is holomorphic on some open set $\Omega$ containing $C$. Functions that are holomorphic on all of $\mathbb{C}$ are said to be *entire*.

[1] We will occasionally appeal to some standard theorems of complex analysis which are covered in any first course on the subject. We will note when we do and provide references to proofs.

[2] The limit must take the same value no matter how the complex number $h$ approaches 0; this makes differentiability a very strong condition for a complex function to satisfy.

Examples of holomorphic functions include polynomials and convergent power series. Functions that admit a power series expansion about a point $z_0$ are said to be *analytic* at $z_0$. It is a theorem ([1, Thm. 5.3], [3, Thm. 2.4.4]) that in fact any function that is holomorphic at $z_0$ has a power series expansion about $z_0$, thus the terms *analytic* and *holomorphic* are often used interchangeably.

A complex function $f(z)$ has a *zero of order* $k$ at $z_0$ if an equation of the form

$$f(z) = (z - z_0)^k g(z)$$

holds in some neighborhood of $z_0$ in which $g$ is holomorphic and $g(z_0) \neq 0$. We say that $f(z)$ has a *pole of order* $k$ at $z_0$ precisely when the function $1/f(z)$ has a zero of order $k$ at $z_0$. Note that $f$ cannot be holomorphic at $z_0$ if it has a pole at $z_0$, but we say that $f$ is *meromorphic* if it is holomorphic everywhere except for a discrete set of poles (this means that there exists a neighborhood about each pole that contains no other poles).

**Definition 16.4.** An *elliptic function* for a lattice $L$ is a complex function $f(z)$ such that

1. $f$ is meromorphic.
2. $f$ is periodic with respect to $L$. This means that $f(z + \omega) = f(z)$ for all $\omega \in L$.[3]

Note that if $f$ is an elliptic function for $L$ then it is also an elliptic function for every sub-lattice of $L$. For a fixed lattice $L$, the set of elliptic functions for $L$ form a field $\mathbb{C}(L)$ that is an extension of $\mathbb{C}$ (every constant function is an elliptic function).

**Definition 16.5.** The *order* of an elliptic function is the number of poles it has in a fundamental parallelogram, each counted with multiplicity equal to its order.

Whenever we count poles or zeros, we do so with multiplicity.

**Theorem 16.6.** *For any nonzero elliptic function $f(z)$ the number of zeros of $f$ in any fundamental parallelogram is equal to the order of $f$.*

To prove this we rely on the following theorem, known as Cauchy's argument principle.

**Theorem 16.7** (Argument Principle)**.** *Let $f$ be a meromorphic function and let $F$ be a region whose boundary $\partial F$ is a simple closed curve*[4] *that contains no zeros or poles of $f$. Then*

$$\frac{1}{2\pi i}\int_{\partial F} \frac{f'(z)}{f(z)}\,dz = \textit{(number of zeros of } f \textit{ in } F) - \textit{(number of poles of } f \textit{ in } F),$$

*where each zero and each pole is counted with multiplicity equal to its order.*

*Proof.* See [1, Thm. 4.20] or [3, Thm. 3.4.1]. □

[3] Equivalently, when $L = [\omega_1, \omega_2]$ the function $f$ is also called *doubly periodic*, with *periods* $\omega_1$ and $\omega_2$, since $f(z + m\omega_1) = f(z + n\omega_2) = f(z)$ for all $m, n \in \mathbb{Z}$.

[4] A curve in the complex plane is the image of a continuous function $u(t)$ from the unit interval to $\mathbb{C}$, subject to some additional conditions (at a minimum, we require curves to have finite length). All the curves we shall consider consist of a finite number of line segments and arcs (a "toy contour" in [3]). A curve is simple if $u(t)$ is injective, except possibly $u(0) = u(1)$, in which case the curve is closed.

*Proof of Theorem 16.6.* The zeros and poles of $f$ are all isolated, so we can pick a fundamental parallelogram $\mathcal{F}$ such that $f(z)$ has no zeros or poles on the boundary $\partial\mathcal{F}$, which we orient counterclockwise. By periodicity the integrals along opposite sides of $\partial\mathcal{F}$ cancel each other out, because $f(z)$ (and $f'(z)$) takes on the same values but we are integrating in opposite directions. Hence

$$\frac{1}{2\pi i}\int_{\partial\mathcal{F}} \frac{f'(z)}{f(z)}\,dz = 0.$$

We then apply the argument principle (Theorem 16.7). □

## 16.2 Eisenstein series

Before giving some non-trivial examples of elliptic functions, we first define the Eisenstein series of a lattice.

**Definition 16.8.** Let $L$ be a lattice and let $k > 2$ be an integer. The *weight-$k$ Eisenstein series* for $L$ is the sum

$$G_k(L) = \sum_{\omega\in L}{}' \frac{1}{\omega^k}.$$

where the notation $\sum'$ means that we exclude the lattice point $\omega = 0$.

**Remark 16.9.** $G_k(L)$ is a function of the lattice $L$, so for any fixed lattice, it is a constant. If we consider lattices $L = [1, \tau]$ parameterized by a complex number $\tau$ in the *upper half plane* $\mathbb{H} = \{z \in \mathbb{C} : \operatorname{im} z > 0\}$, we can view $G_k(L)$ as a function of $\tau$:

$$G_k(\tau) := G_k([1,\tau]) = \sum_{m,n\in\mathbb{Z}}{}' \frac{1}{(m+n\tau)^k}.$$

Because it comes from function defined over a lattice, the function $G_k(\tau)$ has some very nice transformation properties. In particular, $G_k(\tau+1) = G_k(\tau)$ and $G_k(\tau) = \tau^{-k}G_k(-1/\tau)$. It is the simplest example of a *modular form*, which we will see later in the course. Some authors use $E_k$ to denote Eisenstein series, rather than $G_k$, but since we are already using the (often sub-scripted) symbol $E$ for elliptic curves, we will stick with $G_k$.

**Remark 16.10.** $G_k(L) = 0$ for all odd integers $k$, since the terms $\frac{1}{\omega^k}$ and $\frac{1}{(-\omega)^k}$ then cancel. Thus we are only interested in Eisenstein series of even weight.

**Lemma 16.11.** *For any latice $L$, the sum $\sum'_{\omega\in L} \frac{1}{\omega_k}$ converges absolutely for all $k > 2$.*

*Proof.* Let $\delta$ be the minimum distance between points in $L$. Consider an annulus $A$ of inner radius $r$ and width $\frac{\delta}{2}$.

Any two distinct lattice points in $A$ must be separated by an arc length of at least $\delta/2$, measured along the inner rim of $A$. It follows that $A$ contains at most $4\pi r/\delta$ lattice points. The number of lattice points in the annulus $\{\omega : n \le |\omega| < n+1\}$ is therefore bounded by $cn$, where $c \le 8\pi/\delta^2$. We then have

$$\sum_{\omega\in L,\,|\omega|\ge 1} \frac{1}{|\omega|^k} \;\le\; \sum_{n=1}^{\infty} \frac{cn}{n^k} \;=\; c\sum_{n=1}^{\infty} \frac{1}{n^{k-1}} \;<\infty,$$

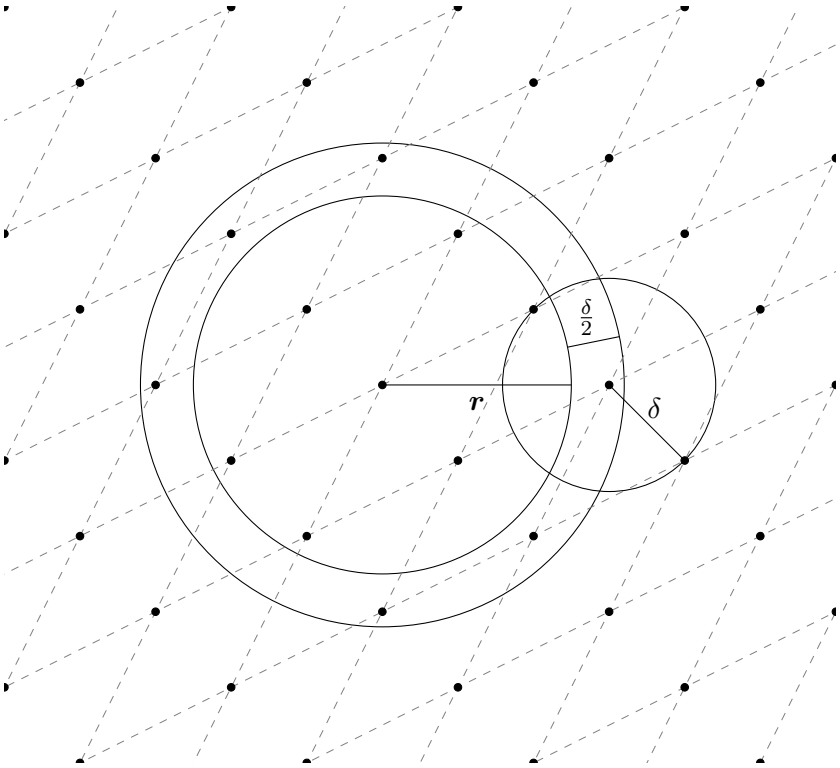



Figure 2: Annulus of radius $\delta/2$.

since $k > 2$. The finite sum $\sum_{\omega\in L,\, 0<|\omega|<1} \frac{1}{|\omega|^k}$ is clearly bounded, thus

$$\sum_{\omega\in L}{}' \frac{1}{|\omega|^k} \;=\; \sum_{\omega\in L,\, 0<|\omega|<1} \frac{1}{|\omega|^k} \;+\; \sum_{\omega\in L,\, |\omega|\geq 1} \frac{1}{|\omega|^k} \;<\; \infty,$$

so $G_k(L)$ converges absolutely. □

## 16.3 The Weierstrass $\wp$-function

We now give our first example of a non-constant elliptic function. It may be regarded as *the* elliptic function in the sense that it can be used to construct every other non-constant elliptic function, a fact we will prove in the next lecture (or see [2, Thm. VI.3.2]).

**Definition 16.12.** The *Weierstrass $\wp$-function* of a lattice $L$ is defined by

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

When the lattice $L$ is fixed or clear from context we typically just write $\wp(z)$, but we should keep in mind that this function depends on $L$. It is clear from the definition that $\wp(z)$ has a pole of order 2 at each point in $L$; we will show that it has no other poles and is in fact holomorphic at every point not in $L$. To do so we rely on the following theorem from complex analysis.

**Theorem 16.13.** *Suppose $\{f_n\}$ is a sequence of functions holomorphic in a region $\Omega$, and that $\{f_n\}$ converges to a function $f$, uniformly on every compact subset of $\Omega$. Then $f$ is holomorphic on $\Omega$.*

*Proof.* See [1, Thm. 5.1] or [3, Thm. 2.5.2]. □

**Theorem 16.14.** *For any lattice $L$, the function $\wp(z;L)$ is holomorphic at every $z \notin L$.*

*Proof.* For each positive integer $n$, we define the function

$$f_n(z) = \frac{1}{z^2} + \sum_{\omega \in L, 0 \le |\omega| < n} \left[ \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right].$$

Each $f_n(z)$ is clearly holomorphic at any $z \notin L$, since we can differentiate term by term. We will show that the sequence of functions $\{f_n\}$ converges uniformly to $\wp$ on all compact sets $S$ disjoint from $L$. Theorem 16.13 then implies that $\wp(z)$ is holomorphic at all $z \notin L$.

So let $S$ be a compact subset of $\mathbb{C}$ disjoint from $L$. Then $S$ is bounded, so we may fix a positive real number $r$ such that $|z| \le r$ for all $z \in S$. For all but finitely many $\omega \in L$, we have $|\omega| \ge 2r$. By the triangle inequality, $|\omega - z| + |z| \ge |\omega|$, so $|\omega| \ge 2r$ implies the following inequalities:

$$|\omega - z| \ge |\omega| - |z| \ge \frac{1}{2}|\omega|;$$
$$|2\omega - z| \le |2\omega| + |-z| \le \frac{5}{2}|\omega|.$$

Thus the bound

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{z(2\omega - z)}{\omega^2 (z-\omega)^2} \right| \le \frac{r\frac{5}{2}|\omega|}{|\omega|^2 (\frac{1}{2}|\omega|)^2} = \frac{10r}{|\omega|^3}$$

holds for all $z \in S$ (with the same fixed $r$). The series $\sum'_{\omega \in L} \frac{1}{|\omega|^3}$ converges, by Lemma 16.11, so $\sum'_{\omega \in L} \left( \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$ converges absolutely for all $z \in S$, and the rate of convergence can be bounded in terms of $r$ and $L$, independent of $z$. It follows that $\{f_n\}$ converges uniformly to $\wp$ on $S$, since for every $\epsilon > 0$ there exists an $N$ such that for all $n \ge N$ we have $|\wp(z) - f_n(z)| < \epsilon$ for all $z \in S$. □

With Theorem 16.14 in hand, we can now summarize the key properties of $\wp(z)$.

**Theorem 16.15.** *For any lattice $L$, the function $\wp(z) = \wp(z;L)$ satisfies the following:*

(i) *$\wp(z)$ is a meromorphic even function whose only poles are double poles at points in $L$.*

(ii) *$\wp'(z) = -2\sum_{\omega \in L} (z-\omega)^{-3}$ is a meromorphic odd function whose only poles are triple poles at each lattice point.*

*Proof.* Clearly $\wp(z)$ has a double pole at each lattice point, and (i) then follows from Theorem 16.13 and the fact that $\wp(z) = \wp(-z)$. For part (ii), note that the partial sums of $\wp(z)$ converge uniformly to a meromorphic function, so we can differentiate term by term, and clearly $\wp'(z)$ has a triple pole at each lattice point and satisfies $\wp'(-z) = -\wp'(z)$. □

**Corollary 16.16.** *The function $\wp(z;L)$ is an elliptic function of order 2 for the lattice $L$.*

*Proof.* We've just shown that $\wp$ is meromorphic, and it has exactly 2 poles in any fundamental region of $L$. We only need to show that it is periodic. Let $L = [\omega_1, \omega_2]$. It suffices to show that

$$\wp(z + \omega_i) = \wp(z), \quad \text{for } i = 1, 2.$$

Now $\wp'(z)$ is clearly periodic, so $\wp'(z + \omega_i) = \wp'(z)$. Integrating gives

$$\wp(z + \omega_i) - \wp(z) = c_i.$$

for some constant $c_i$ and for all $z \notin L$. To find $c_i$, plug in $z = -\omega_i/2$. We have

$$\wp(\omega_i/2) - \wp(-\omega_i/2) = c_i.$$

But $\wp(z)$ is an even function, so $c_i = 0$. □

The study of elliptic functions dates back to Gauss, who discovered them as solutions to elliptic integrals $\int \sqrt{f(z)}dz$, where $f(z)$ is a cubic or quartic polynomial (they were later rediscovered by Abel and Jacobi). We will show that $\wp(z)$ satisfies a differential equation of the form $\wp'(z)^2 = f(\wp(z))$, where $f(x)$ is a cubic polynomial over $\mathbb{C}$. Notice that if one views $(\wp(z), \wp'(z))$ as a pair $(x, y)$, this is exactly the equation of an elliptic curve! This explains our interest in $\wp(z)$.

To derive the differential equation satisfied by the Weierstrass $\wp$-function, we first need to compute its Laurent series.

**Theorem 16.17.** *The Laurent series expansion for $\wp(z; L)$ at $z = 0$ is*

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

*where $G_k(L)$ denotes the Eisenstien series of weight $k$.*

*Proof.* For all $|x| < 1$ we have the power series expansion

$$\frac{1}{(1-x)^2} = (1 + x + x^2 + \cdots)^2 = \sum_{n=0}^{\infty} (n + 1)x^n.$$

Applying this to $x = \frac{z}{w}$ with $|x| < 1$,

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left(\frac{1}{(1-x)^2} - 1\right) = \frac{1}{\omega^2}\sum_{n=1}^{\infty}(n + 1)x^n = \sum_{n=1}^{\infty}\frac{(n + 1)z^n}{\omega^{n+2}}$$

Summing over $\omega$ and changing the order of summation (valid, since we have already proved

absolute convergence) gives

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + \sum_{\omega\in L}{}' \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right] \\
&= \frac{1}{z^2} + \sum_{\omega\in L}{}' \sum_{n=1}^{\infty} \frac{(n+1)z^n}{\omega^{n+2}} \\
&= \frac{1}{z^2} + \sum_{n=1}^{\infty} (n+1)z^n \sum_{\omega\in L}{}' \frac{1}{\omega^{n+2}} \\
&= \frac{1}{z^2} + \sum_{n=1}^{\infty} (n+1)G_{n+2}(L)z^n \\
&= \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1)G_{2n+2}(L)z^{2n}.
\end{aligned}$$

In the last step we used the fact that $\wp$ is an even function, so the coefficients of the odd terms are 0, and we can take the sum over just even integers $2n$. □

## 16.4 Lattices define elliptic curves

The key link between $\wp(z)$ and elliptic curves is given by the following differential equation.

**Theorem 16.18.** *The function $\wp(z;L)$ satisfies the differential equation*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L) \tag{1}$$

*where $g_2(L) = 60G_4(L)$ and $g_3(L) = 140G_6(L)$.*

*Proof.* We use Theorem 16.17 to compute the first few terms of the Laurent series for $\wp$ and $\wp'$:

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + 3G_4(L)z^2 + 5G_6(L)z^4 + \cdots \\
\wp'(z) &= -\frac{2}{z^3} + 6G_4(L)z + 20G_6(L)z^3 + \cdots \\
\wp(z)^3 &= \frac{1}{z^6} + \frac{9G_4(L)}{z^2} + 15G_6(L) + \cdots \\
\wp'(z)^2 &= \frac{4}{z^6} - \frac{24G_4(L)}{z^2} - 80G_6(L) + \cdots
\end{aligned}$$

Now let $f(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4(L)\wp(z) + 140G_6(L)$. The terms with non-positive powers of $z$ cancel, and we have $f(0) = 0$. Because $\wp$ and $\wp'$ have poles only at points of $L$, the function $f(z)$ is holomorphic over the entire complex plane. Note that $f(z)$ is bounded because all values attained by $f$ are attained on the closure of a fundamental parallelogram, which is a compact set. It then follows from Liouville's Theorem (see Theorem 16.19 below) that $f$ is a constant function and hence identically zero. □

**Theorem 16.19** (Liouville's Theorem)**.** *A function that is bounded and holomorphic on all of $\mathbb{C}$ must be constant.*

*Proof.* See [1, p. 122] or [3, Cor. 2.4.5]. □

With $y = \wp'(z)$ and $x = \wp(z)$, the equation (1) corresponds to the curve

$$y^2 = 4x^3 - g_2(L)x - g_3(L), \tag{2}$$

This curve can easily be put into Weierstrass form with $g_2(L) = -4A$ and $g_3(L) = -4B$, thus every lattice $L$ gives us an equation we can use to define an elliptic curve over $\mathbb{C}$, provided we can show that the projective curve defined by (2) is not singular. If the partial derivatives of $zy^2 = 4x^3 - g_2(L)xz^2 - g_3(L)z^3$ simultaneously vanish at some point, then there must be a projective solution to the system of equations

$$0 = 12x^2 - g_2(L)z^2, \qquad 2zy = 0, \qquad y^2 = -2g_2(L)xz - 3g_3(L)z^2.$$

We cannot have $z = 0$ (this would force $x = y = 0$), thus thus we may assume $z = 1$, and the second equation then implies $y = 0$. The first equation requires $x = -3g_3(L)/(2g_2(L))$, and plugging this into the third equation yields $g_2(L)^3 - 27g_3(L)^2 = 0$. Thus so long as the *discriminant*

$$\Delta(L) = g_2(L)^3 - 27g_3(L)^2$$

of the lattice $L$ is nonzero, equation (2) defines an elliptic curve over $\mathbb{C}$. We will prove that $\Delta(L) \neq 0$, for every lattice $L$. For this we need the following lemma.

**Lemma 16.20.** *A point $z \notin L$ is a zero of $\wp'(z; L)$ if and only if $2z \in L$.*

*Proof.* Suppose $2z \in L$ for some $z \notin L$. Then

$$\wp'(z) = \wp'(z - 2z) = \wp'(-z) = -\wp'(z) = 0,$$

where we have used the fact that $\wp'$ is both periodic and odd. If $L = [\omega_1, \omega_2]$, then $\omega_1/2, \omega_2/2, (\omega_1 + \omega)/2$ are the only points in $\mathcal{F}_0$ that are not in $L$ and satisfy $2z \in L$. Since $\wp'$ is an elliptic function of order 3, it has only these three zeros in $\mathcal{F}_0$, by Theorem 16.6. Thus for any $z \notin$ Ł, we have $\wp'(z) = 0$ if only if $2z \in L$. □

This lemma is analogous to the fact that the points of order 2 on the elliptic curve (2) are precisely the points $(x, y) = (\wp(z), \wp'(z))$ with $y = 0$. The requirement that $z \notin L$ simply means that $(x, y)$ is not the point at infinity.

**Lemma 16.21.** *For any lattice $L$, the discriminant $\Delta(L)$ is nonzero.*

*Proof.* Let $L = [\omega_1, \omega_2]$. Let

$$r_1 = \frac{\omega_1}{2}, \quad r_2 = \frac{\omega_2}{2}, \quad r_3 = \frac{\omega_1 + \omega_2}{2}.$$

Then $2r_i \in L$ for $i = 1, 2, 3$. So $\wp'(r_i) = 0$ by Lemma 16.20. Thus from (2) we see that $\wp(r_1), \wp(r_2)$, and $\wp(r_3)$ are the zeros of the cubic $f(x) = 4x^3 - g_2(L)x - g_3(L)$. Now the discriminant $\Delta(f)$ of $f(x)$ is equal to $16\Delta(L)$, thus

$$\Delta(L) = \frac{1}{16} \prod_{i<j} (\wp(r_i) - \wp(r_j))^2,$$

and it suffices to show that the $\wp(r_i)$ are distinct.

Let $g(z) = \wp(z) - \wp(r_1)$. Then $g(z)$ is an elliptic function of order 2 (its poles are the poles of $\wp$), so it has exactly 2 zeros, by Theorem 16.6. Now $r_1$ is a double zero because $\wp'(r_1) = 0$, by Lemma 16.20. Thus $g(z)$ has no other zeros, and therefore

$$\wp(r_2) \neq \wp(r_1) \text{ and } \wp(r_3) \neq \wp(r_1).$$

Similarly, $\wp(r_2) \neq \wp(r_3)$, as desired. □

We have now shown that every lattice $L$ gives rise to an elliptic curve $E/\mathbb{C}$ defined by $y^2 = 4x^3 - g_2(L)x - g_3(L)$, and that the map

$$\begin{aligned} \Phi\colon \mathbb{C}/L &\longrightarrow E(\mathbb{C}) \\ z &\longrightarrow (\wp(z), \wp'(z)) \end{aligned}$$

maps points on $\mathbb{C}/L$ to points on the elliptic curve. We will show in the next lecture that $\Phi$ is an isomorphism and that every elliptic curve $E/\mathbb{C}$ arises from some lattice $L$.

## References


[1] Lars Ahlfors, *Complex analysis*, third edition, McGraw Hill, 1979.

[2] Joseph H. Silveman, *The arithmetic of elliptic curves*, second edition, Springer, 2009.

[3] Elias M. Stein and Rami Shakarchi, *Complex analysis*, Princeton University Press, 2003.