14 Elliptic curves over $\mathbb{C}$ (part I)

We now consider elliptic curves over the complex numbers. Our first goal is to prove the Uniformization Theorem, which establishes an explicit correspondence between elliptic curves over $\mathbb{C}$ and tori $\mathbb{C}/L$ defined by lattices L in $\mathbb{C}$:

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.

To make the correspondence explicit, we need to specify the map Φ. This map is parameterized by *elliptic functions*, specifically the Weierstrass $\wp$-function and its derivative. We will begin by studying general properties of elliptic functions in §14.1 and Eisenstein series in §14.3, then specialize to the Weierstrass $\wp$-function in §14.4 and construct the map Φ in §14.5. Our presentation generally follows that in [2, Ch. 3, §10], but we will fill in some more details for the benefit of those who have not taken a course in complex analysis.

Once we have fleshed out this correspondence, we will have 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 an elliptic curve $E_p/\mathbb{F}_p$ with the same endomorphism ring $\mathcal{O}$. The endomorphism ring determines, in particular, the trace of the Frobenius endomorphism π_{E_p} (up to a sign), which in turn determines $\#E_p(\mathbb{F}_p) = p + 1 - \mathrm{tr}(\pi_{E_p})$. This allows us to construct elliptic curves over finite fields that have a prescribed number of rational points, using what is known as the *CM method*. As we will see, this has many practical applications, including cryptography and a faster version of elliptic curve primality proving.

14.1 Elliptic functions

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

Definition 14.1. A *lattice* $L = [\omega_1, \omega_2]$ in $\mathbb{C}$ is an additive subgroup $\omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ of $\mathbb{C}$ generated by complex numbers ω_1 and ω_2 that are linearly independent over $\mathbb{R}$.

Example 14.2. Let τ 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 $\mathbb{C}/L$. Note that this quotient makes sense not just as a quotient of abelian groups, but also as a quotient of topological spaces (where $\mathbb{C}$ has its usual Euclidean topology and L has the discrete topology); the torus $\mathbb{C}/L$ is a compact topological group.

Definition 14.3. A *fundamental parallelogram* for $L = [\omega_1, \omega_2]$ is any set of the form

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

for some $\alpha \in \mathbb{C}$. We can identify the points in any $\mathcal{F}_\alpha$ with the points of $\mathbb{C}/L$.

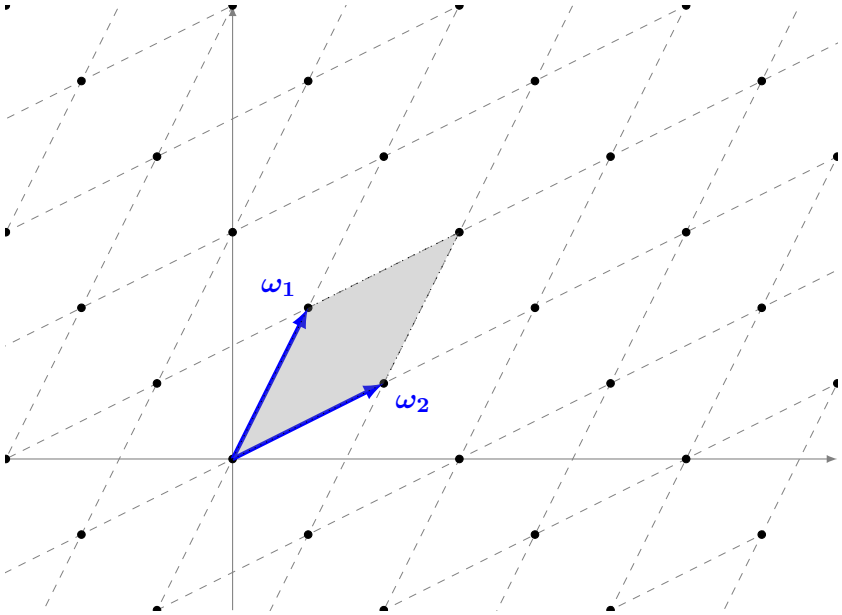


Figure 1: A lattice $[\omega_1, \omega_2]$ with a fundamental parallelogram shaded.

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 an official prerequisite for this course, we will take a moment to define the terminology we need and recall some elementary results that can be found in standard textbooks such as [1, 4, 6].

Definition 14.4. A function $f\colon \Omega \to \mathbb{C}$ defined on an open neighborhood Ω of a point $z_0 \in \mathbb{C}$ is said to be *holomorphic* at z_0 if the derivative

$$f'(z_0) := \lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0}$$

exists.[1] We say that f is holomorphic on an open set Ω if it is holomorphic at every $z_0 \in \Omega$. Functions that are holomorphic on all of $\mathbb{C}$ are simply said to be holomorphic or *entire*.

Examples of holomorphic functions include polynomials and convergent power series. Functions that admit a power series expansion with a positive radius of convergence about a point z_0 are said to be *analytic* at z_0. Remarkably, any function that is holomorphic at z_0 is also analytic at z_0 (see [1, Thm. 5.3] or [6, Thm. 2.4.4]), so the terms analytic and holomorphic may be used interchangeably (modern usage favors holomorphic).

[1]The limit must take the same value no matter how the complex number z approaches z_0; this makes differentiability a much stronger condition on a complex function than it is on a real function.

Definition 14.5. Let k be a positive integer. 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 open neighborhood of z_0 in which $g(z)$ is holomorphic and $g(z_0) \neq 0$. We say that $f(z)$ has a *pole of order k* at z_0 if the function $1/f(z)$ has a zero of order k at z_0. A pole or zero of order 1 is called a *simple pole* or a *simple zero*.

Definition 14.6. A complex function f is *meromorphic* on an open set Ω if it is holomorphic at every point on Ω except for a discrete set of poles.[2]

Definition 14.7. For any nonzero complex function $f(z)$ that is meromorphic on an open neighborhood of a point $z_0 \in \mathbb{C}$ we define

$$\operatorname{ord}_{z_0}(f) := \begin{cases} n & \text{if } f \text{ has a zero of order } n \text{ at } z_0, \\ -n & \text{if } f \text{ has a pole of order } n \text{ at } z_0, \\ 0 & \text{otherwise.} \end{cases}$$

For any open set $\Omega \subseteq \mathbb{C}$, the set of complex functions that are meromorphic on Ω forms a field $\mathbb{C}(\Omega)$ that we view as an extension of $\mathbb{C}$ (the constant functions). For each fixed $z_0 \in \Omega$, we then have a *discrete valuation* $\operatorname{ord}_{z_0} \colon \mathbb{C}(\Omega)^\times \to \mathbb{Z}$, which has the following properties:

1. $\operatorname{ord}_{z_0}(fg) = \operatorname{ord}_{z_0}(f) + \operatorname{ord}_{z_0}(g)$ for all $f, g \in \mathbb{C}(\Omega)^\times$;
2. $\operatorname{ord}_{z_0}(f + g)) \geq \min(\operatorname{ord}_{z_0}(f), \operatorname{ord}_{z_0}(g))$ for all $f, g \in \mathbb{C}(\Omega)^\times$.

We note that the second inequality is in fact an equality whenever $\operatorname{ord}_{z_0}(f) \neq \operatorname{ord}_{z_0}(g)$. It is customary to extend ord_{z_0} to all of $\mathbb{C}(\Omega)$ by defining $\operatorname{ord}_{z_0}(0) := \infty$, with addition and comparisons in $\mathbb{Z} \cup \{\infty\}$ defined in the obvious way.

Definition 14.8. An *elliptic function* for a lattice L is a complex function $f(z)$ such that

1. f is meromorphic on $\mathbb{C}$.
2. f is periodic with respect to L; this means that $f(z + \omega) = f(z)$ for all $\omega \in L$.[3]

The fact that an elliptic function is periodic with respect to L means that it can also be viewed as a function on $\mathbb{C}/L$. Note that if f is an elliptic function for L then it is also an elliptic function for every sub-lattice of L. Sums, differences, products, and quotients of elliptic functions for a lattice L are also elliptic functions for L; thus the set of elliptic functions for a fixed lattice L form a field that we denote $\mathbb{C}(L)$; note that constant functions are elliptic functions for every lattice L.

Definition 14.9. The *order* of an elliptic function is the number of poles it has in any fundamental parallelogram, where each pole is counted with multiplicity equal to its order (this is a finite number because the poles in a fundamental parallelogram are a discrete subset of its closure, which is compact).

As a general rule, whenever we count the poles or zeros of a meromorphic function, we always count them with multiplicity.

Remark 14.10. The elliptic functions of order zero are precisely the constant functions. This follows from Liouville's theorem (see Theorem 14.30 below), since a holomorphic elliptic function is necessarily bounded (as a continuous function it must achieve a maximum value on any compact set, including the closure of a fundamental parallelogram), hence constant.

[2] This means that each pole lies in an open subset of Ω that contains no other poles.

[3] If $L = [\omega_1, \omega_2]$ the function f is also said to be *doubly periodic*, with *periods* ω_1 and ω_2.

14.2 Contour integrals and the residue formula

In order to count poles and zeros of meromorphic functions (and elliptic functions in particular), we need a few standard tools from complex analysis that we briefly recall here. Those who are familiar with this material can skip ahead to Theorem 14.18, which uses Cauchy's argument principle to deduce that an elliptic function has the same number of zeros as poles in any fundamental parallelogram.

Definition 14.11. A *smooth curve* in $\mathbb{C}$ is a continuously differentiable function

$$\gamma\colon [a,b] \to \mathbb{C},$$

where $[a,b]$ is a closed interval in $\mathbb{R}$. A *piecewise smooth curve* $\gamma\colon [a,b] \to \mathbb{C}$ is defined by a finite sequence of n smooth curves $\gamma_i\colon [a_i,b_i] \to \mathbb{C}$ with $a_0 = a$, $a_{i+1} = b_i$, and $b_n = b$. We will simply use the term *curve* to refer to a piecewise smooth curve.[4] A curve is *simple* if its restriction to the open interval (a,b) is injective, and it is *closed* if $\gamma(a) = \gamma(b)$.

For simple closed curves γ the Jordan curve theorem (see [1, §4.2 Ex. 3] or [6, Appendix B, Thm. 2.1]) gives a well-defined notion of interior and exterior, as well as a notion of positive and negative orientation. Loosely speaking, we that a simple closed curve is *positively oriented* if the interior is on the left as we travel along the curve (if γ is a circle, this means counter-clockwise). The notion of orientation can be made completely precise using *winding numbers*, but this is overkill for our purposes here; the simple closed curves we will use (circles and parallelograms) all have obvious interiors and orientation.

Definition 14.12. For a smooth curve $\gamma\colon [a,b] \to \mathbb{C}$ and a complex function $f(z)$ defined on an open set containing γ the *contour integral* of f along γ is defined by

$$\int_\gamma f(z)dz := \int_a^b f(\gamma(t))\gamma'(t)dt.$$

This definition extends to piecewise smooth curves in the obvious way (sum the contour integrals on each smooth piece).

Theorem 14.13. *Let Ω be an open set containing a curve $\gamma\colon [a,b] \to \mathbb{C}$, and let $F(z)$ be a holomorphic function on Ω and let $f(z) = F'(z)$. Then*

$$\int_\gamma f(z)dz = F(\gamma(b)) - F(\gamma(a)).$$

Proof. If γ is smooth then

$$\int_\gamma f(z)dz = \int_a^b F'(\gamma(t))\gamma'(t)dt = \int_a^b \left(\frac{d}{dt}F(\gamma(t))\right)dt = F(\gamma(b)) - F(\gamma(a)).$$

The piecewise smooth case follows by taking summing over smooth pieces. □

It is a non-trivial fact that if $f(z)$ is holomorphic on a simply connected open set Ω then there exists a holomorphic function[5] $F(z)$ for which $f(z) = F'(z)$ (this is obvious locally,

[4] More generally one can define *rectifiable curves* that are defined by continuous (but not necessarily differentiable) functions and have finite length, but we will not need these.

[5] The function $F(z)$ is called a *primitive* of $f(z)$.

since in a neighborhood of each $z_0 \in \Omega$ there is a power series expansion of $f(z)$ about z_0 that we can integrate term by term, but we want a single $F(z)$ that works for all $z_0 \in \Omega$); see [1, §4.1 Thm. 4] or [6, §2 Thm. 2.1] for a proof in the case that Ω is a disc. An important consequence of this fact is Cauchy's theorem.

Theorem 14.14 (Cauchy's theorem)**.** *Let f be a function that is holomorphic on an open set containing a closed curve γ and its interior. Then*

$$\int_\gamma f(z)dz = 0.$$

Proof. See [6, Appendix B Thm. 2.9]. □

A corollary of this theorem is that the countour integral of a holomorphic function depends only on the end points $(\gamma(a), \gamma(b))$ of the curve γ, not the path taken from $\gamma(a)$ to $\gamma(b)$.

We now want to consider countour integrals of functions that are meromorphic but not necessarily holomorphic. Note that a function $f(z)$ that is meromorphic on an open set Ω has a Laurent series expansion

$$f(z) = \sum_{n \geq n_0} a_n (z - z_0)^n$$

about any point $z_0 \in \Omega$. Here $n_0 = \operatorname{ord}_{z_0}(f)$ can be any integer (positive or negative), and we define $a_n = 0$ for all $n < n_0$.

Definition 14.15. The *residue* at z_0 of a function $f(z) = \sum_{n \geq n_0} a_n (z - z_0)^n$ that is meromorphic on an open neighborhood of z_0 is

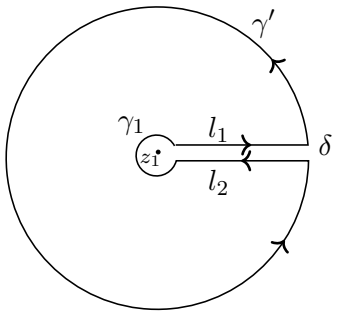
$$\operatorname{res}_{z_0}(f) := a_{-1}.$$

If f is holomorphic at z_0 then $\operatorname{res}_{z_0}(f) = 0$. Even if f has a pole at z_0 it is still possible to have $\operatorname{res}_{z_0}(f) = 0$ when the order of the pole is greater than 1, but if f has a simple pole at z_0 then $\operatorname{res}_{z_0}(f)$ must be nonzero. This definition may look strange at first glance, but it is motivated by the following theorem.

Theorem 14.16 (Residue formula)**.** *Let γ be a simple closed curve with positive orientation and let $f(z)$ be a function that is meromorphic on an open set containing γ and its interior with no poles on γ. Let $z_1, \ldots, z_N$ be the poles of $f(z)$ that lie in the interior of γ. Then*

$$\int_\gamma f(z)dz = 2\pi i \sum_{k=1}^{N} \operatorname{res}_{z_k}(f).$$

Proof. Let us first suppose that γ is a circle and that $f(z)$ has a single pole at z_1 inside γ. We now consider a *keyhole contour* $\tilde{\gamma}$ that approximates γ but whose interior does not contain z_1, as shown below. The function $f(z)$ is holomorphic on an open set that contains $\tilde{\gamma}$ and its interior, but not z_1; thus $\int_{\tilde{\gamma}} f(z)dz = 0$, by Cauchy's theorem.



As the distance δ between the horizontal segments l_1 and l_2 goes to zero, the sum $\int_{l_1} f(z)dz) + \int_{l_2} f(z)dz$ approaches zero while $\int_{\gamma'} f(z)dz$ approaches $\int_\gamma f(z)dz$. In the limit we have

$$\int_{\tilde{\gamma}} f(z)dz = 0 = \int_\gamma f(z)dz - \int_{c_1} f(z)dz,$$

where c_1 is a positively oriented circle with the same radius as the arc γ_1 (which is oriented in the opposite direction; this explains the minus sign in the equation above). Thus

$$\int_\gamma f(z)dz = \int_{c_1} f(z)dz.$$

If $f(z) = \sum_{n\geq n_0} a_n(z-z_1)^n$ is the Laurent series for $f(z)$ about z_1, then

$$\int_{c_1} f(z)dz = \int_{c_1} \left(\sum_{n=n_0}^{-1} a_n(z-z_0)^n + \sum_{n\geq 0} a_n(z-z_0)^n \right) dz.$$

The infinite sum on the right is holomorphic in an open neighborhood of z_0 that we can assume contains c_1, since we can make the radius of c_1 as small as we wish, thus the integral of this sum is zero. It thus suffices to compute the integrals $\int_{c_1}(z-z_0)^n dz$ for negative n. After replacing $z-z_0$ with u and dz by du we can assume c_1 is a circle about 0 parameterized by re^{it}, where r is the radius of c_1. For $n<0$ we then have

$$\int_{c_1} u^n du = \int_0^{2\pi} (re^{it})^n (ire^{it})dt = \int_0^{2\pi} ir^{n+1}e^{(n+1)it}dt = \begin{cases} 0 & \text{if } n<-1, \\ 2\pi i & \text{if } n=-1. \end{cases}$$

Thus

$$\int_\gamma f(z)dz = \int_{c_1} f(z)dz = 2\pi i a_{-1} = 2\pi i \operatorname{res}_{z_1}(f)$$

as desired. The case where $f(z)$ has N poles inside γ is similar; we now approximate γ with a contour $\tilde{\gamma}$ that has N keyholes, one about each z_k, each of which has an inner arc with negative (clockwise) orientation. We then obtain

$$\int_\gamma f(z)dz = 2\pi i \sum_{k=1}^N \operatorname{res}_{z_k}(f).$$

The same argument applies when γ is not a circle, it just requires approximating γ with a more complicated contour $\tilde{\gamma}$. □

We can now use the residue formula to derive a generalization of Cauchy's *argument principle*, which is our main tool for counting the zeros and poles of a meromorphic function.

Theorem 14.17. *Let γ be a simple closed curve with positive orientation, let $f(z)$ be a function that is meromorphic on an open set Ω containing γ and its interior Γ, with no zeros or poles on γ, and let $g(z)$ be a nonzero function that is holomorphic on Ω.*

$$\frac{1}{2\pi i}\int_\gamma g(z)\frac{f'(z)}{f(z)}\,dz = \sum_{w\in\Gamma} g(w)\mathrm{ord}_w(f).$$

When $g(z) = 1$, the RHS is the difference between the number of zeros and poles that $f(z)$ has in Γ (counted with multiplicity), which is the usual argument principle.

Proof. For any $z_0 \in \Gamma$ that is a zero or pole of $f(z)$, we consider the Laurent series expansions

$$f(z) = \sum_{n\ge n_0} a_n(z-z_0)^n, \qquad g(z) = \sum_{n\ge 0} b_n(z-z_0)^n$$

where $n_0 = \mathrm{ord}_{z_0}(f)$ is chosen so that $a_{n_0} \neq 0$ and we note that $g(z_0) = b_0$. Then

$$f'(z) = \sum_{n\ge n_0} n a_n (z-z_0)^{n-1}$$

and we have

$$\frac{f'(z)}{f(z)} = n_0(z-z_0)^{-1} + h_1(z), \qquad g(z)\frac{f'(z)}{f(z)} = b_0 n_0 (z-z_0)^{-1} + h_2(z),$$

where $h_1(z)$ and $h_2(z)$ denote functions that are holomorphic on an open neighborhood of z_0. Thus $g(z)f'(z)/f(z)$ has a simple pole with residue $b_0 n_0 = g(z_0)\mathrm{ord}_{z_0}(f)$ at each zero or pole z_0 of $f(z)$, and no other poles. The theorem follows from the residue formula. □

Applying Theorem 14.17 with $g(z) = 1$ to an elliptic function $f(z)$ yields the following.

Theorem 14.18. *Let $f(z)$ be a nonzero elliptic function for a lattice L. When counted with multiplicity, the number of zeros of $f(z)$ in any fundamental parallelogram $\mathcal{F}_\alpha$ for L is equal to the number of poles of $f(z)$ in $\mathcal{F}_\alpha$.*

Proof. We first note that by the periodicity of $f(z)$, it suffices to prove this for any particular fundamental parallelogram $\mathcal{F}_\alpha$. The zeros and poles of $f(z)$ are discrete (note that $1/f(z)$ is also a meromorphic function), so we can pick an α for which the boundary $\partial\mathcal{F}_\alpha$ of $\mathcal{F}_\alpha$ does not contain any zeros or poles of $f(z)$. We now consider the contour integral

$$\int_{\partial\mathcal{F}_\alpha} \frac{f'(z)}{f(z)}dz,$$

where the simple closed curve $\partial\mathcal{F}_\alpha$ is positively oriented. The fact that $f(z)$ is periodic with respect to L implies that $f'(z)$ is also periodic with respect to L, as is $f'(z)/f(z)$, and it follows that the sum of the integral of $f'(z)/f(z)dz$ along opposite sides of the parallelogram ∂F_α is zero, since $f'(z)/f(z)$ takes on the same values on both sides (because it is periodic) but the oriented curve ∂F_α traverses them in opposite directions. We thus have

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

and the theorem then follows from Theorem 14.17. □

14.3 Eisenstein series

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

Definition 14.19. Let L be a lattice in $\mathbb{C}$ 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 $L^* = L - \{0\}$.

Remark 14.20. $G_k(L)$ 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 τ in the *upper half plane* $\mathcal{H} := \{z \in \mathbb{C} : \operatorname{im} z > 0\}$, we can view $G_k(L)$ as a function of τ:

$$G_k(\tau) := G_k([1,\tau]) = \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(m+n\tau)^k}.$$

Because it comes from a function defined over a lattice, the function $G_k(\tau)$ has some very nice properties. In particular, we have

$$G_k(\tau + 1) = G_k(\tau) \qquad \text{and} \qquad G_k(-1/\tau) = \tau^k G_k(\tau)$$

for all $\tau \in \mathcal{H}$. Eisenstein series are the simplest example of *modular forms*, which we will see later in the course.[6]

Remark 14.21. If k is odd then $G_k(L) = 0$ for any lattice L, since the terms $\frac{1}{\omega^k}$ and $\frac{1}{(-\omega)^k}$ in the sum cancel (note that L is an additive group, so $\omega \in L \implies -\omega \in L$, and in the sum over L^*, each ω is distinct from $-\omega$). Thus the only interesting Eisenstein series are those of even weight.

Lemma 14.22. *For any lattice L, the sum $\sum_{\omega \in L^*} \frac{1}{\omega^k}$ converges absolutely for all $k > 2$.*

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

Any two distinct lattice points in A must be separated by an arc of length at least $\delta/2$ when measured along the inner rim of A. It follows that A contains at most $4\pi r/\delta$ lattice points. If we put $r = n$ and $\delta = 2$ then the number of lattice points in the annulus $\{\omega : n \le |\omega| < n+1\}$ is bounded by $4\pi n/2 = 2\pi n$. We then have

$$\sum_{\omega \in L,\, |\omega| \ge 1} \frac{1}{|\omega|^k} \;\le\; \sum_{n=1}^{\infty} \frac{2\pi n}{n^k} \;=\; 2\pi \sum_{n=1}^{\infty} \frac{1}{n^{k-1}} \;< \infty,$$

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

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

so the sum converges absolutely as claimed. □

[6] Many authors use E_k to denote Eisenstein series, rather than G_k, but since we are already using the (often subscripted) symbol E for elliptic curves, we will stick with G_k.

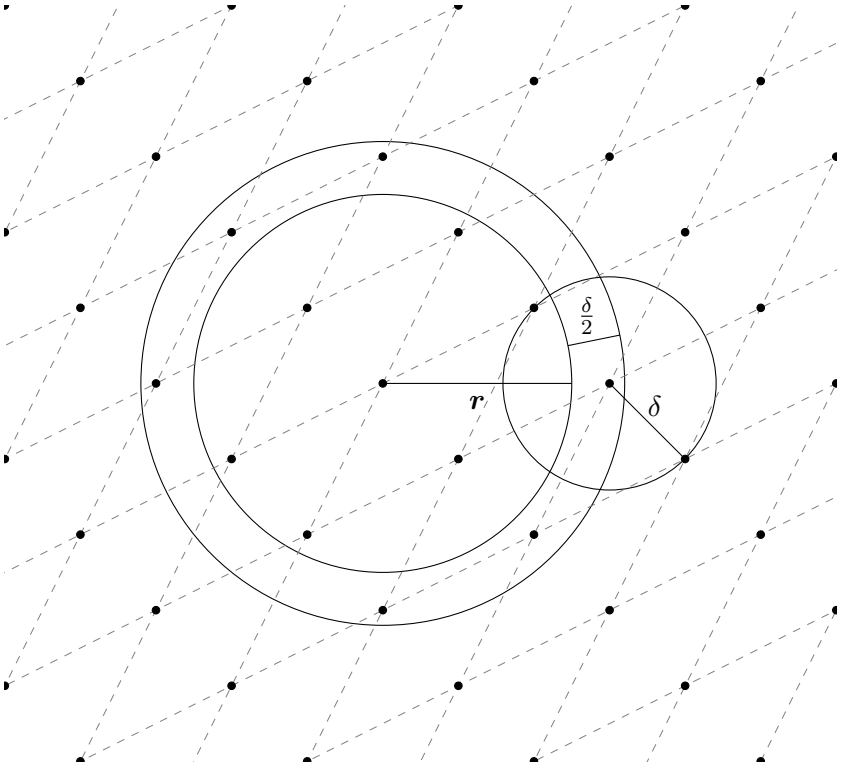


Figure 2: Annulus of radius r and width $\delta/2$.

14.4 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 [5, Thm. VI.3.2]).

Definition 14.23. The *Weierstrass $\wp$-function* of a lattice L in $\mathbb{C}$ 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 $z \in L$ (including $z = 0$); 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 14.24. *Suppose $\{f_n\}$ is a sequence of functions holomorphic on an open set Ω, and that $\{f_n\}$ converges to a function f uniformly on every compact subset of Ω. Then f is holomorphic on Ω, and $\{f_n'\}$ converges uniformly to f' on every compact subset of Ω.*

Proof. See [1, §5 Thm. 1] or [6, §2 Thm. 5.2-3]. □

Theorem 14.25. *The function $\wp(z; L)$ is holomorphic at every $z_0 \notin L$.*

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

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

Each $f_n(z)$ is clearly holomorphic at any $z \notin L$, since we can differentiate the finite sum 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 14.24 will then imply that $\wp(z)$ is holomorphic on the open set $\mathbb{C} - L$.

So let S be a compact subset of $\mathbb{C}$ disjoint from L. Then S is bounded and we may fix $r \in \mathbb{R}_{>0}$ 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 $z \in S$. The series $\sum_{\omega \in L^*} \frac{1}{|\omega|^3}$ converges, by Lemma 14.22, 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 is an N such that for all $n \ge N$ we have $|\wp(z) - f_n(z)| < \epsilon$ for all $z \in S$. □

With Theorem 14.25 in hand, we can now summarize the key properties of $\wp(z)$.

Theorem 14.26. *The function $\wp(z) = \wp(z; L)$ and its derivative*

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

satisfy the following:

(i) *$\wp(z)$ is a meromorphic even function whose poles consist of double poles at each $z \in L$.*

(ii) *$\wp'(z)$ is a meromorphic odd function whose poles consist of triple poles at each $z \in L$.*

Proof. We first note that the sequence of functions $\{f_n\}$ defined in the proof of Theorem 14.25 consist of finite partial sums that converge uniformly to $\wp(z)$ on compact subsets of $\mathbb{C} - L$, and Theorem 14.24 implies that the sequence $\{f_n'\}$ converges uniformly to $\wp'(z)$, thus we can therefore differentiate $\wp(z)$ term by term to obtain $\wp'(z)$ (the sum for $\wp'(z)$ includes $\omega = 0$ due to the leading $1/z^2$ term in $\wp(z)$). It is clear that $\wp(z)$ has a double pole at each lattice point, and (i) then follows from Theorem 14.25 and the fact that $\wp(z) = \wp(-z)$. Part (ii) is clear from the formula for $\wp'(z)$ and the fact that the derivative of a function that is holomorphic on an open neighborhood of a point z is also holomorphic on that neighborhood (so $\wp'(z)$ is holomorphic at all $z \notin L$ since $\wp(z)$ is). □

Corollary 14.27. *The function $\wp(z) = \wp(z; L)$ is an elliptic function of order 2 for L, and its derivative $\wp'(z)$ is an elliptic function of order 3 for L.*

Proof. We've just shown that $\wp(z)$ and $\wp'(z)$ are meromorphic. Every fundamental region of L contains exactly one lattice point, so $\wp(z)$ has two poles in each fundamental region, while $\wp'(z)$ has three. It is clear from the formula for $\wp'(z)$ that $\wp'(z)$ is periodic with respect to L, we just need to show that $\wp(z)$ 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 periodic, so $\wp'(z + \omega_i) = \wp'(z)$. Integrating then 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 $c_i = 0$ and $\wp(z + \omega_i) = \wp(z)$ as desired. □

The study of elliptic functions dates back to Gauss, who discovered them as solutions to elliptic integrals (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 14.28. *The Laurent series expansion of $\wp(z) = \wp(z; L)$ at $z = 0$ is given by*

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

where $G_k(L)$ denotes the Eisenstein 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 $x = \frac{z}{\omega}$ with $|x| < 1$ (which we can assume holds for all $\omega \in L^*$ provided we keep z close to 0),

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

Summing over ω and changing the order of summation (via 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 $\wp(z)$ is an even function, so the coefficients of the odd terms are 0 and we can sum over $2n$ rather than n. □

14.5 Lattices define elliptic curves

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

Theorem 14.29. *The function $\wp(z) = \wp(z; L)$ satisfies the differential equation*

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

where $g_2(L) \coloneqq 60G_4(L)$ and $g_3(L) \coloneqq 140G_6(L)$.

Proof. We may apply Theorem 14.28 to compute the first few terms of the Laurent series expansions for $\wp(z)$ and $\wp'(z)$ at $z_0 = 0$:

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

Now let

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

We can compute the Laurent series expansion for $f(z)$ at $z_0 = 0$ as a linear combination of those computed above, and one finds that the non-positive powers of z all cancel; we thus have $f(0) = 0$.

Because $\wp$ and $\wp'$ have poles only at points of L, the function $f(z)$ is holomorphic on the fundamental parallelogram $\mathcal{F}_0$. The function $f(z)$ is periodic with respect to L, since $\wp(z)$ and $\wp'(z)$ are, thus it is holomorphic on 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 14.30 below) that f is a constant function, hence identically zero. □

Theorem 14.30 (Liouville's Theorem)**.** *The only functions that are bounded and holomorphic on $\mathbb{C}$ are constant functions.*

Proof. See [1, p. 122] or [6, §2 Cor. 4.5]. □

With $y = \wp'(z)$ and $x = \wp(z)$, the differential equation in (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

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

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

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

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 14.31. *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 $\wp'(z)$ is both periodic with respect to L and an odd function. If $L = [\omega_1, \omega_2]$, then

$$\frac{\omega_1}{2}, \quad \frac{\omega_2}{2}, \quad \frac{\omega_1 + \omega_2}{2}$$

are the only points $z \in \mathcal{F}_0$ that are not in L and also satisfy $2z \in L$. Since $\wp'(z)$ is an elliptic function of order 3, it has only these three zeros in $\mathcal{F}_0$, by Theorem 14.18. Thus for any $z \notin L$ 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 $y = \wp'(z) = 0$. The requirement that $z \notin L$ simply means that (x, y) is not the point at infinity.

Remark 14.32. Having shown that the zeros of $\wp'(z)$ correspond to 2-torsion point of $\mathbb{C}/L$ you might wonder about the zeros of $\wp(z)$. As shown by Eichler and Zagier, the zeros of $\wp(z)$ in the fundamental region $\mathcal{F}_0$ for $L = [1, \tau]$ are

$$\frac{1}{2} \pm \left(\frac{\log(5 + 2\sqrt{6})}{2\pi i} + 144\pi i\sqrt{6} \int_\tau^{i\infty} (x - \tau) \frac{\Delta(x)}{G_6(x)^{3/2}} dx \right),$$

a fact that does not appear to have any obvious arithmetic significance.

Lemma 14.33. *For any lattice L, the discriminant $\Delta(L)$ is nonzero.*

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

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

Then $r_i \notin L$ and $2r_i \in L$ for $i = 1, 2, 3$. So $\wp'(r_i) = 0$ by Lemma 14.31. 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 $g_i(z) = \wp(z) - \wp(r_i)$. Then $g_i(z)$ is an elliptic function of order 2 (its poles are the poles of $\wp(z)$), so it has exactly 2 zeros, by Theorem 14.18. Now r_i is a double zero because $g_i'(r_i) = \wp'(r_i) = 0$, by Lemma 14.31. Thus $g_i(z)$ has no other zeros, and therefore $\wp(r_j) \neq \wp(r_i)$ for $i \neq j$. □

We have shown that every lattice L in $\mathbb{C}$ 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

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

sends points on $\mathbb{C}/L$ to points on the elliptic curve. This is the first step in proving the Uniformization Theorem. In the next lecture we will show that Φ is a group isomorphism and that every elliptic curve $E/\mathbb{C}$ arises from some lattice L.

References

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

[2] David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, second edition, Wiley, 2013.

[3] Martin Eichler and Don Zagier, *On the zeros of the Weierstrass $\wp$-function*, Math. Annalen **258** (1982), 399-407.

[4] Serge Lang, *Complex analysis*, fourth edition, Springer, 1999.

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

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