Chapter 1

Elliptic curves in a nutshell

1.1 Elliptic curves: elementary approach

Curves in the projective plane $\mathbb{P}^2_{\mathbb{C}}$ of degrees one and two are easy to understand. So the first interesting case is three. For historical reasons, these are called elliptic curves. More precisely, an elliptic curve is a nonsingular cubic in $\mathbb{P}^2$. We can ask how many "degrees of freedom" do we have to choose such a curve. First of all, a homogeneous cubic polynomial in x, y, z has 10 coefficients. However, any nonzero scalar multiple of a given polynomial determines the same curve. So the count should be reduced to $10-1$. Furthermore, we only care up to linear change of variables. More formally, we want to divide out by PGL_3, leaving only $1 = 10 - 1 - 8$ parameter for an elliptic curve. Of course, this discussion was not rigorous, but it can be made so.

Theorem 1.1.1. *After a linear change of variables, an elliptic curve (over $\mathbb{C}$) can be put into Weierstrass form, given by homogenizing*

$$y^2 = 4x^3 - ax - b \tag{1.1}$$

where a, b are constants such that

$$\Delta = a^3 - 27b^2 \neq 0$$

Proof. The reduction to

$$y^2 = x^3 + Ax + B$$

can be found in [Si, chap III, §1]. From here, a further linear change of the form $(x, y) \mapsto (cx, y)$, will put into Weierstrass form. □

The significance of the shape of the right side of (1.1) will be clear shortly. Note that Δ is the discriminant of the right side $4x^3 - ax - b$. So the condition $\Delta \neq 0$ is exactly the condition for this polynomial to have distinct roots. This is equivalent to the nonsingularity of the projective curve defined by (1.1). The Weierstrass form is not unique. If $a' = c^4 a$ and $b' = c^6 b$, then

$$y^2 = 4x^3 - a'x - b'$$

gives a curve isomorphic to (1.1) under the transformation $(x, y) \mapsto (c^2 x, c^3 x)$. This is in fact the only ambiguity. We can see that the quantity

$$j = 1728 \frac{a^3}{\Delta}$$

is invariant under such a transformation. (The normalization factor 1728 is there by tradition, although unimportant for our purposes.) In fact, we have

Theorem 1.1.2. *Two elliptic curves over $\mathbb{C}$ in Weierstrass form are isomorphic if and only if their j-invariants coincide.*

This makes precise what we said above.

1.2 Elliptic curves: analytic theory

We now give an analytic description. We recall that a lattice in $\mathbb{C}$ is a subgroup spanned by a real basis.

Theorem 1.2.1. *Any elliptic curve is isomorphic (as a Riemann surface) to the quotient of $\mathbb{C}$ by a lattice. Conversely, any such quotient is an elliptic curve.*

We will explain the idea of the proof of the converse statement in the last theorem, referring to [Si] for details. Let say that two tori $\mathbb{C}/L$ and $\mathbb{C}/L'$ are isomorphic if there exists a nonzero $c \in \mathbb{C}^*$ such that $cL = L'$.

Lemma 1.2.2. *Any elliptic curve is isomorphic to one of the form $E_\tau = \mathbb{C}/L_\tau, L_\tau = \mathbb{Z} + \mathbb{Z}\tau$, with $\operatorname{Im} \tau > 0$.*

This is elementary, but we give the proof, since we will need the notation anyway.

Proof. Let

$$B = \{(u, v) \in \mathbb{C}^2 \mid u, v \ \mathbb{R}\text{-linearly independent}\}$$

be the set of real bases for $\mathbb{C}$. It is easy to see that this has two connected components

$$B^+ = \{(u, v) \mid \operatorname{Im}(u/v) > 0\},\ B^- = \{(u, v) \mid \operatorname{Im}(u/v) < 0\}$$

which correspond to positively and negatively oriented bases. Clearly any lattice is given by $\mathbb{Z}u + \mathbb{Z}v$, where $(u, v) \in B$. By switching u, v, if necessary, we can assume $(u, v) \in B^+$. Then $\mathbb{Z}u + \mathbb{Z}v = v(\mathbb{Z} + \mathbb{Z}u/v)$ gives the desired isomorphism. □

We define the Weierstrass $\wp$-function by

$$\wp(z,\tau) = \wp(z) = \frac{1}{z^2} + \sum_{\lambda\in L,\,\lambda\neq 0}\left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right) \tag{1.2}$$

It is not hard to show that the terms are dominated by $Const|z|/|\lambda|^3$, and consequently that

Proposition 1.2.3. *The series converges uniformly on compact subsets to a holomorphic function on $\mathbb{C} - L$.*

Clearly, $\wp$ has poles at L.

Theorem 1.2.4. *The Weierstrass function is periodic with respect to L in the sense that*

$$\wp(z+\lambda) = \wp(z)$$

for $\lambda \in L$

Proof. By the previous proposition, we can differentiate (1.2) term by term to obtain

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

So clearly $\wp'$ is doubly periodic. Therefore

$$\wp(z+\lambda) = \wp(z) + c(\lambda)$$

for appropriate constants $c(\lambda)$. In particular, setting $z = -\lambda/2$ shows that

$$\wp(\lambda/2) = \wp(-\lambda/2) + c(\lambda)$$

However, we can see directly from (1.2), that $\wp(-z) = \wp(z)$. Therefore $c(\lambda) = 0$. □

An *elliptic function* (relative to L) is a meromorphic function on $\mathbb{C}$ which is periodic with respect to L. The theorem shows that $\wp$ is elliptic. An elliptic function can be viewed a meromorphic function on $\mathbb{C}/L$. From Liouville's theorem, we obtain

Proposition 1.2.5. *An entire elliptic function is constant.*

Theorem 1.2.6. *The Laurent expansion of $\wp$ at 0 is*

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

where the coefficients, called Eisenstein series, are

$$G_{2k} = \sum_{\lambda\in L-\{0\}}\frac{1}{\lambda^{2k}}$$

Proof. This results from substituting

$$(z-\lambda)^{-2} - \lambda^{-2} = \lambda^{-2}[(1-z/\lambda)^{-2} - 1]$$
$$= \sum_{1}^{\infty} \frac{(k+1)z^k}{\lambda^{k+2}}$$

into (1.2). □

Theorem 1.2.7.
$$(\wp')^2 = 4\wp^3 - g_2\wp^2 - g_3$$

where
$$g_2 = 60G_4,\ g_3 = 140G_6$$

Sketch. Let
$$f(z) = (\wp')^2 - 4\wp^3 - g_2\wp^2 - g_3$$

This is clearly elliptic, and the only possible poles are at points of L. However, using the previous theorem we can calculate enough terms of the Laurent series of f to conclude that f has no poles at 0 and $f(0) = 0$. It follows that f has no singularities at all, and is therefore constant. So it must be identically 0.

□

We can now define a map $\mathbb{C}/L \to \mathbb{P}^2$ given by

$$z \mapsto \begin{cases} [\wp(z), \wp'(z), 1] & \text{if } z \notin L \\ [0,1,0] & \text{otherwise} \end{cases}$$

Proposition 1.2.8. *This is an embedding.*

Proof. See [Si, pp 158-159]. □

Putting the above statements together, we see that $\mathbb{C}/L$ is a cubic in $\mathbb{P}^2$ as claimed earlier.

One consequence of this representation of an elliptic curve as a torus, is that we get a natural group law on it.

1.3 Analytic theory continued: theta functions

With an eye towards higher dimensions, we want to give a different method of realizing the elliptic curve $E = \mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$ as a projective curve. We need to construct functions $f_i : E \to \mathbb{C}$ such that $p \mapsto [f_0(p), \ldots, f_n(p)] \in \mathbb{P}^n$ is well defined and gives an embedding. If we regard f_i as functions from $\mathbb{C} \to \mathbb{C}$, these would be quasiperiodic, in the sense that

$$f_i(p+\lambda) = (\text{some factor}) f_i(p), \quad \forall \lambda \in \mathbb{Z} + \mathbb{Z}\tau$$

where the factor in front is the same for all i and nonzero. The basic example is Jacobi's θ-function. This is given by the Fourier series

$$\theta(z,\tau) = \sum_{n\in\mathbb{Z}} \exp(\pi i n^2\tau + 2\pi i n z) = \sum_{n\in\mathbb{Z}} \exp(\pi i n^2\tau)\exp(2\pi i n z)$$

Since τ is fixed, we just view it as function of z for now. Writing $\tau = x+iy$, with $y>0$, shows that on a compact subset of the z-plane the terms are bounded by $O(e^{-n^2y})$. So uniform convergence on compact sets is guaranteed, and we can conclude that θ holomorphic. This is clearly periodic

$$\theta(z+1) = \theta(z) \tag{1.3}$$

In addition it satifies the functional equation

$$\begin{aligned} \theta(z+\tau) &= \sum \exp(\pi i n^2\tau + 2\pi i n(z+\tau)) \\ &= \sum \exp(\pi i (n+1)^2\tau + 2\pi i (n+1)z - 2\pi i z - \pi i \tau) \\ &= \exp(-\pi i \tau - 2\pi i z)\theta(z) \end{aligned} \tag{1.4}$$

Conversely, if $f(z)$ is a holomorphic function satisfying these equations, then (1.3) yields a Fourier exansion

$$f(z) = \sum_n a_n \exp(2\pi i n z)$$

and (1.4) produces recurrence conditions on the coefficients. This can be used to show that $f(z) = a_0\theta(z)$. We get more solutions by relaxing these conditions. Let $N>0$ be an integer, and consider the space V_N of holomorphic functions satisfying

$$\begin{aligned} f(z+N) &= f(z) \\ f(z+N\tau) &= \exp(-\pi i N^2\tau - 2\pi i N z)f(z) \end{aligned} \tag{1.5}$$

By the first equation, any function in V_N can be expanded in a Fourier series (in powers of $\exp(2\pi i/N)$), and the second equation yields recurrences which shows that the coefficients are determined by N^2 of them. In other words:

Lemma 1.3.1. $\dim V_N = N^2$.

A proof of this lemma can be found on pp 8-10 of [MT]. The discussion there gives quite a bit more information that we recall. The conditions (1.5) can be expressed as invariance under the operators

$$S_a(f)(z) = f(z+a),$$

$$T_b(f)(z) = \exp(\pi i b^2\tau + 2\pi i b z)f(z+b\tau)$$

for $a,b\in N\mathbb{Z}$. For $a,b\in\mathbb{R}$, we have the following identities

$$S_aS_b = S_{a+b},\ T_aT_b = T_{a+b}$$

$$S_aT_b = \exp(2\pi iab)T_bS_a$$

So they generate a nonabelian group H, called a Heisenberg group, which fits into an exact sequence

$$1 \to U(1) \to H \to \mathbb{R}^2 \to 0$$

where the last map sends $S_aT_b \mapsto (a,b)$ and $U(1) \subset \mathbb{C}^*$ is the unit circle. A key fact is:

Lemma 1.3.2. *V_N is stable under the operators $S_{1/N}$ and $T_{1/N}$, and therefore under the subgroup H'_N of H generated by these operators. This subgroup fits into a sequence*

$$1 \to \mu_N \to H'_N \to (\frac{1}{N}\mathbb{Z})^2 \to 0$$

The action of H'_N on V_N is trivial on the preimage of $(N\mathbb{Z})^2$. Therefore the action factors through a finite quotient H_N of H'_N which, as an abstract group, fits into an exact sequence

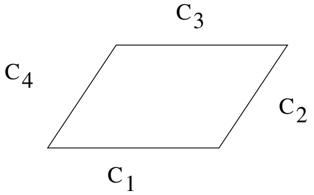
$$1 \to \mu_N \to H_N \to (\mathbb{Z}/N^2\mathbb{Z})^2 \to 0$$

Lemma 1.3.3. *Given nonzero $f \in V_N$, it has exactly N^2 zeros, counted with multiplicities, in the parallelogram with vertices $0, N, N\tau, N+\tau$ (where we translate if necessary so no zeros lie on the boundary).*

Proof. Complex analysis tells us that the number of zeros is given by the integral

$$\frac{1}{2\pi i}\int_{C_1+C_2+C_3+C_4} \frac{f'(z)dz}{f(z)}$$

over the boundary of the parallelogram.



Using $f(z+N) = f(z)$, we obtain

$$\int_{C_2+C_4} \frac{f'(z)dz}{f(z)} = 0$$

and from $f(z+N\tau) = Const.\exp(-2\pi iNz)f(z)$, we obtain

$$\int_{C_1+C_3} \frac{f'(z)dz}{f(z)} = 2\pi iN^2$$

□

A function $f \in V_N$ is quasi-periodic with respect to the lattice NL. If we transform it to $F(z) = f(Nz)$, then it become quasi-periodic with respect to L. Once we choose a basis f_i of V_N, the map $\phi : E \to \mathbb{P}^{N^2-1}$ given by $z \mapsto [F_i(z)]$ is well defined. Recall that we found a finite group H_N which acts on V_N, and therefore on $\mathbb{P}^{N^2-1}$. This group also acts on E where the image (a, b) under the homomorphism $H_N \to (\mathbb{Z}/N^2)^2$ sends $z \mapsto z + a/N^2 + b\tau/N^2$. One checks by a calculation [MT, p 13] that

Lemma 1.3.4. *ϕ is equivariant for these actions*

Theorem 1.3.5. *$\phi : E \to \mathbb{P}^{N^2-1}$ is an embedding.*

Proof. Suppose that ϕ is not one to one. Then $F(z_1) = \lambda F(z_1')$ for some $z_1 \neq z_1'$ in $\mathbb{C}/L$, some $\lambda \in \mathbb{C}^*$, and all $f \in V_N$. By translation by H_N, we can find another such pair z_2, z_2' with this property, such that z_1, z_1', z_2, z_2' are distinct. Choose $N^2 - 3$ additional points $z_3, \ldots z_{N^2-1}$ in $\mathbb{C}/L$ distinct from the previous choices. We define a map $V_N \to \mathbb{C}^{N^2-1}$ by $f \mapsto (F(z_i))$. Since $\dim V_N = N^2$, we can find a nonzero $f \in V_N$ so that

$$F(z_1) = F(z_2) = F(z_3) = \ldots F(z_{N^2-1}) = 0$$

Notice that we are forced to also have $F(z_1') = F(z_2') = 0$ which means that f has at least $N^2 + 1$ zeros which contradicts the lemma.

A similar argument shows that the derivative $d\phi$ is nowhere zero. Otherwise we would have a point z_1 such that F' has a zero at z_1 for every $f \in V_N$. Arguing as above, we would find a nonzero $f \in V_N$ and points $z_1, \ldots z_{N^2-1}$, such that F has zeros at the z_i and double zeros at z_1, z_2. This again yields a contradiction. □

The embeddings produced this way are different from the previous method. The smallest case is when $N = 2$. Then we get an embedding E into $\mathbb{P}^3$. One can show that it an intersection of two quadrics. In general, we can always guarantee that the image is algebraic by:

Theorem 1.3.6 (Chow)**.** *If $X \subset \mathbb{P}^n$ is a complex submanifold, then it automatically a nonsingular projective algebraic variety.*

1.4 Elliptic curves over arbitrary fields

Finally let us redo parts of the theory assuming Hartshorne level algebraic geometry.[1] We now work over an arbitrary field k, which is not necessarily algebraically closed. An elliptic curve over k, is a smooth projective curve E over k, of genus one, with a fixed k-rational point O. We will deduce the earlier description as a consequence. First, we should recall that the fundamental invariant of a smooth projective curve is its genus g. Suppose that k is algebraically closed.

[1] And if you haven't read it, don't worry about it too much. All of this material can be understood with only basic AG, as in [Si].

If $X \subset \mathbb{P}^N$ is a smooth projective curve, let X' be its image under a general linear projection $\mathbb{P}^N \dashrightarrow \mathbb{P}^2$. Then $X' \subset \mathbb{P}^2$ has only nodes as singularities. The genus is given by

$$g = \frac{(d-1)(d-2)}{2} - \delta$$

where d is the degree of X' and δ is the number of nodes. So $g = 1$ when $X = X'$ is smooth of degree 3. Although this gives a method for calculating g, it does not make a good definition, as it not obviously independent of the choice of embedding. A more intrinsic definition is via sheaf cohomology

$$g = \dim H^1(X, \mathcal{O}_X) = \dim H^0(X, \Omega^1_X)$$

where the last equality is a special case of Serre duality. This shows that $g \geq 0$, which wasn't obvious from the last formula. When $k = \mathbb{C}$, g can also be identified with one half the first Betti number. This can be seen from the Hodge decomposition.

Among other things, the genus enters into the statement of the Riemann-Roch theorem, which we will recall. Let us suppose that k is algebraically closed for simplicity, then a divisor D is a finite formal sum $D = \sum n_i p_i$, where p_i are points of X. Define the degree

$$\deg D = \sum n_i$$

The formalism works over nonalgebraically closed fields, but now p_i are closed points of X viewed as a scheme, and $\deg D = \sum n_i[k(p_i) : k]$, where $k(p_i)$ are the residue fields. If f is a nonzero rational function, the associated principal divisor

$$\operatorname{div} f = \sum ord_p(f)p$$

where $ord_p(f)$ is the discrete valuation attached to p. If ω is a nonzero rational differential form, the canonical divisor

$$\operatorname{div} \omega = \sum ord_p(\omega)$$

In spite of the formal similarity canonical divisors are usually not principal. In fact the degrees

$$\deg(\operatorname{div} f) = 0, \ \deg(\operatorname{div} \omega) = 2g - 2$$

are usually different. However, when $g = 1$, we do have equality. In fact, more is true.

Lemma 1.4.1. *When $g = 1$, $\Omega^1_X \cong \mathcal{O}_X$ and any canonical divisor is principal.*

Proof. Since $H^0(\Omega^1_X) \neq 0$, we have a nonzero regular 1-form ω. Note that ω has no poles, and since $\deg \operatorname{div} \omega = 0$, it has no zeros either. By identifying $H^0(X, \Omega^1_X) \cong Hom(\mathcal{O}_X, \Omega^1_X)$, we can view ω as a nonzero morphism $\mathcal{O}_X \to \Omega^1_X$. The map is injective, because the kernel consists of functions f such that $f\omega = 0$. Since for every $p \in X$, $\omega(p) \neq 0$, we can express dx as multiple of ω, where x is local uniformizer. This implies that ω is surjective as well. Therefore $\Omega^1_X \cong \mathcal{O}_X$, and the second statement is an immediate consequence. □

We define a sheaf $\mathcal{O}_X(D)$, sometimes denoted by $\mathcal{L}(D)$, whose global sections are

$$H^0(X, \mathcal{O}_X(D)) \cong \{f \text{ a rational function} \mid ord_{p_i} f + n_i \geq 0\}$$

This means that $\operatorname{div}(f) + D$ is effective in the sense that its coefficients are nonnegative. There are a few cases where this can be computed directly from the definition. If $D = 0$, then $H^0(\mathcal{O}_X(D)) = H^0(\mathcal{O}_X)$ consists of constant functions (because X is projective). If D is nonzero with positive coefficients, then $H^0(\mathcal{O}_X(-D))$, consists of constant functions vanishing somewhere, so that $H^0(\mathcal{O}_X(-D)) = 0$. For more general cases, we can use Riemann-Roch.

Theorem 1.4.2 (Riemann-Roch)**.**

$$h^0(\mathcal{O}_X(D)) - h^0(\mathcal{O}_X(K - D)) = \deg D + 1 - g$$

where K is any canonical divisor and $h^i = \dim H^i$.

This leads to another useful method for computing the genus.

Corollary 1.4.3. $\deg K = 2g - 2$

Proof. Apply Riemann-Roch when $D = K$. □

Let us return to the case of an elliptic curve (E, O). Take $D = nO$ (O not 0), where n is a positive integer. Then

$$h^0(\mathcal{O}_E(nO)) - h^0(\mathcal{O}_E(K - nO)) = 1$$

Since $K = 0$, we can write the second term on the left as $h^0(\mathcal{O}(-nO))$, but this is 0. Thus we can conclude that

$$h^0(\mathcal{O}_E(nO)) = n$$

It follows that $H^0(\mathcal{O}_E(O)) = H^0(\mathcal{O}_E)$ consists of just the constant functions. This also implies that there exists a nonconstant $f \in H^0(\mathcal{O}(2E))$ and a function $g \in H^0(\mathcal{O}(3O))$ not in $H^0(\mathcal{O}(2O))$. We can also conclude that the seven functions $1, f, f^2, f^3, g, g^2, gf \in H^0(\mathcal{O}(6O))$ are linearly dependent. Using these facts, it is not difficult to show that the map $p \mapsto (f(p), g(p))$ extends to embedding of E as a cubic in $\mathbb{P}^2_k$. More generally:

Theorem 1.4.4. *Suppose that D is a divisor of degree 3 or more, and $f_0, \dots f_n \in H^0(E, \mathcal{O}_E(D))$ is a basis. Then the map $\phi : E \to \mathbb{P}^n_k$ given $\phi(x) = [f_0(x), \dots, f_n(x)]$ is an embedding.*

Proof. This follows from [H, cor 3.2, p 308]. □

Recall that the class group $Cl(X)$ of a smooth projective curve is the quotient of the group of divisors by the subgroup of principal divisors. Since principal divisors have degree 0, the degree homomorphism factors through $Cl(X)$. Let $Cl^0(X) = \ker \deg Cl(X) \to \mathbb{Z}$.

Theorem 1.4.5. *Let (E, O) be an elliptic curve. The map $\alpha : E \to Cl^0(E)$ defined by $\alpha(p) = p - O$ is a bijection.*

Proof. Suppose D is divisor of degree 0. By Riemann-Roch

$$h^0(\mathcal{O}(D + O)) = 1$$

Choose a nonzero function $f \in H^0(\mathcal{O}(D + O)$. $\operatorname{div} f$ is necessary of the form p for some $p \in X$. So that $f \in H^0(\mathcal{O}(D + O - p))$ This implies that divisor class of D and $p - O$ are equal. Therefore α is surjective.

Suppose that $\alpha(p) = \alpha(q)$ and that $p \neq q$. Then $p - q$ is principle. This implies that there is a function f with simple pole at p and no other poles. Viewing f as map $f : E \to \mathbb{P}^1$, we can see that this implies that f is degree 1. So we are forced to conclude that $E \cong \mathbb{P}^1$ but this is impossible since the genera are different. So α is injective. □

Corollary 1.4.6. *E has the structure of abelian group in a natural way.*

Without the word "natural", the result would be quite useless. We can interpret this to mean, that the group operations are connected to the structure of E as an algebraic variety, in the sense that they are morphisms. We refer to [Si] or other standard texts for an explanation or why this holds.

Let us return to case when $k = \mathbb{C}$ and reinterpret the theory of theta functions in terms of divisors. Given V_N as before, $f \in V_N - \{0\}$ is *not* a function on $E = \mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$. However, we can attach an effective divisor D_f to it by taking the divisor of zeros of f in a fundamental parallelogram as in lemma 1.3.3. This lemma shows that $\deg D_f = N^2$. If $g \in V_N$ is another nonzero function, g/f is invariant and therefore a meromorphic function on E. We can see that $D_g = D_f + \operatorname{div}(g/f)$, so that D_g is linearly equivalent to D_f. This tells us that $g/f \in H^0(E, \mathcal{O}(D_f))$. So the map $g \mapsto g/f$ gives an injective homomorphism, which we can view as an inclusion

$$V_N \subseteq H^0(E, \mathcal{O}(D_f))$$

Since both sides have dimension N^2, we must have equality. In particular, theorem 1.3.5 follows from theorem 1.4.4. Finally, we note that there is even an analogue of the Heisenberg group due to Mumford. We won't get into that here, but instead refer to his paper *On the equations defining Abelian varieties I, Inventiones 1966* for details.