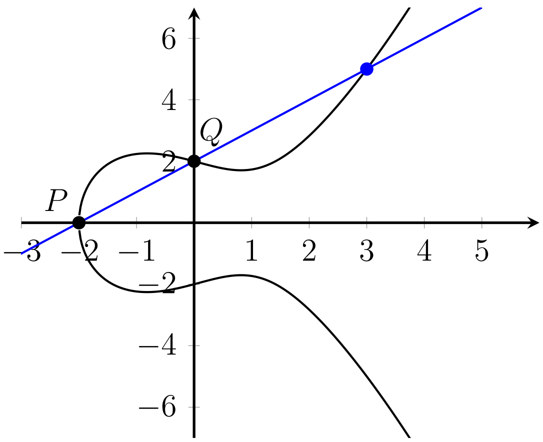
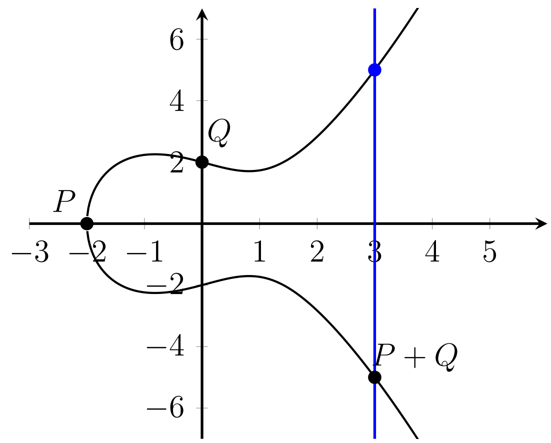
§Motivation

Consider the curve $y^2 = x^2 - 2x + 4$ together with O, a point at infinity. We can define addition of points on the curve as follows:



To add points P and Q, take the line through them and find the third point of intersection on the curve. (If $P = Q$, we take the tangent line.)



Then take the line through this new point and O. The third point of intersection of this line with the curve is $P + Q$.

Exercise: The points on the curve with this addition form a group with identity O.

This curve is an example of a Weierstrass curve, which have the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

plus a point at infinity. In this case we had coefficients $a_i \in \mathbb{Z}$.

Questions: Can we define Weierstrass curves for other coefficients? Where do these curves live? Do they have a group structure?

§What is an Elliptic Curve? (Part I)

For a curve C over a field K we have:

- The field of functions on C, over K or over $\overline{K}$ (denoted $K(C)$ and $\overline{K}(C)$ respectively).
- $Div(C)$, the free abelian group generated by the points of C with a subgroup of principal divisors (elements of the form $\sum_{P\in C} ord_P(f)P$ for some $f \in \overline{K}(C)^\times$).
- A partial ordering on $Div(C)$ as follows: $D \geq 0$ if all coefficients in $D = \sum_{P\in C} n_P P$ are nonnegative. $D_1 \geq D_2$ if $D_1 - D_2 \geq 0$.
- $Pic(C)$, the quotient of $Div(C)$ by the subgroup of principal divisors.
- Ω_C, the space of differential forms on C.
- A map $div : \Omega_C \to Div(C)$. Any class in the image of div in $Pic(C)$ is called a canonical divisor.

For any $D = \sum_{P\in C} n_P P \in Div(C)$, we define:

- $degD = \sum_{P\in C} n_P$
- A finite dimensional vector space $\mathcal{L}(D) = \{f \in \overline{K}(C)^\times | div(f) \leq -D\} \cup \{0\}$
- An integer $\ell(D)$ equal to the dimension of $\mathcal{L}(D)$ over $\overline{K}(C)$.

Theorem 1. *(Riemann-Roch) Let C be a smooth curve and let K_C be a canonical divisor. Then there exists some integer $g \geq 0$, called the genus of C, such that for every divisor $D \in Div(C)$,*

$$\ell(D) - \ell(K_C - D) = deg(D) - g + 1$$

Definition. *(Version 1)*
*An **elliptic curve** over a field K is a smooth, projective curve $E \subset \mathbb{P}^2_K$ of genus one with a base point.*

§Elliptic Curves Over $\mathbb{C}$

Let $\Lambda \subset \mathbb{C}$ be a lattice. Recall that the complex torus $\mathbb{C}/\Lambda$ has a complex Lie group structure. We will see that if we want to understand elliptic curves over $\mathbb{C}$, we can study complex tori.

Definition. *An **elliptic function** relative to Λ is a meromorphic function on $\mathbb{C}$ compatible with quotienting by the lattice. (I.E. For all $z \in \mathbb{C}$, $\omega \in \Lambda$, $f(z+\omega) = f(z)$.)*
The field of all elliptic functions with respect to Λ is denoted by $\mathbb{C}(\Lambda)$.

Definition. *The **Weierstrass $\wp$-function** relative to Λ is given by*

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\omega\in\Lambda\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

Fact. All elliptic functions are rational combinations of $\wp$ and $\wp'$.

Definition. *The **Eisenstein series of weight** $2k$ is given by*

$$G_{2k}(\Lambda) = \sum_{\omega\in\Lambda\setminus\{0\}} \omega^{-2k}$$

Proposition 1. *Let g_2 denote $60G_4(\Lambda)$ and g_3 denote $140G_6(\Lambda)$. Then $y^2 = 4x^3 - g_2x - g_3$ is an elliptic curve that is isomorphic as a complex Lie group to $\mathbb{C}/\Lambda$.*

Proposition 2. *Let E be an elliptic curve over $\mathbb{C}$. Then there exists a lattice $\Lambda \subset \mathbb{C}$ unique up to homothety such that $\mathbb{C}/\Lambda \cong E$ (as complex Lie groups).*

(Note: Λ_1 is homothetic to Λ_2 if there exists $\alpha \in \mathbb{C}^\times$ such that $\Lambda_1 = \alpha\Lambda_2$)

The isomorphism from $\mathbb{C}/\Lambda$ to the associated elliptic curve E is given by $z \mapsto [\wp(z), \wp'(z), 1]$.

§What is an Elliptic Curve? (Part II)

Definition. *(Version 2)*
An ***elliptic curve*** *over a (commutative) ring R, is a smooth projective curve (1-dim. variety), $E \subset \mathbb{P}^2_R$ of genus one with base point.*

Or, if you like, a group scheme over $Spec(R)$ that is a relative 1-dim., smooth, proper curve over R.

Note: For any algebraic variety, the genus is $g = -\big(\chi(\mathcal{O}) - 1\big)$, where $\mathcal{O}$ is the structure sheaf and χ is the Euler characteristic.

Definition. *Let R be a commutative ring. A* ***generalized Weierstrass equation*** *C over R has the form*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

with $a_i \in R$, $C \subset \mathbb{P}^2_R$.

We will generally want to write this in affine coordinates, letting $x = X/Z$, $y = Y/Z$:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

but we also must include the single point on the curve where $Z = 0$, $O = [0, 1, 0]$.

Here are a whole bunch of things associated to our Weierstrass equation that may be useful later:

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2 \\
b_4 &= 2a_4 + a_1a_3 \\
b_6 &= a_3^2 + 4a_6 \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 24b^4 \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\
j &= c_4^3/\Delta
\end{aligned}$$

The discriminant is $\Delta \in \mathbb{Z}[a_1, \ldots, a_6]$, and we say that C is smooth if Δ is invertible in R.

We could check that $2^6 3^3 \Delta = c_4^3 - c_6^2$, so if 2 and 3 are invertible in R, $\Delta = \dfrac{c_4^3 - c_6^2}{2^6 3^3}$.
A group law on E, a non-singular Weierstrass curve with distinguished point O, is determined by requiring the sum of any three colinear points to be O.

Proposition 3. *Any elliptic curve over R is isomorphic (incl. $O \mapsto [0, 1, 0]$) to a curve given by a Weierstrass equation with coefficients in R. Conversely, every smooth curve given by a Weierstrass equation with coefficients in R is an elliptic curve over R with base point $O = [0, 1, 0]$.*

Proof sketch for the case where R is a field:
Riemann–Roch (eventually) implies that if $degD > 2g-2$, then $\ell(D) = degD - g + 1$.

Given an elliptic curve E over K, $g = 1$ and $deg(nO) = n > 2(1) - 2$ for any positive integer n. So, $\ell(nO) = deg(nO) - 1 + 1 = n$.
Choose $x, y \in K(E)$ such that $\{1, x\}$ is a basis for $\mathcal{L}\big(2(O)\big)$ and $\{1, x, y\}$ is a basis for $\mathcal{L}\big(3(O)\big)$. Then $1, x, y, xy, x^2, y^2, x^3$ are seven elements of $\mathcal{L}\big(6(O)\big)$, which has dimension 6. Thus, there exists some relation $0 = A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3$. A change of coordinates gives us a Weierstrass curve. It remains to show that E is isomorphic to the curve described by this equation.

Given a smooth Weierstrass curve C, we can construct a differential $\omega \in \Omega_C$ such that $div(\omega) = 0$. Then, by Riemann–Roch, $2g - 2 = deg\big(div(\omega)\big) = 0$. So E has genus one and we take $O = [0, 1, 0]$.

§Isomorphisms

Since our definition of elliptic curve includes a base point, we want isomorphisms of elliptic curves to fix the point $O = [0, 1, 0]$.
All of these isomorphisms take the form $x \mapsto u^2x + r$, $y \mapsto u^3y + su^2x + t$ for some $r, s, t \in R, u \in R^\times$.
What happens to all the things associated to this curve under the isomorphism?

$$
\begin{aligned}
a_1 &\mapsto u^{-1}(a_1 + 2s)\\
a_2 &\mapsto u^{-2}(a_2 - sa_1 + 3r - s^2)\\
a_3 &\mapsto u^{-3}(a_3 + ra_1 + 2t)\\
a_4 &\mapsto u^{-4}(a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st)\\
a_6 &\mapsto u^{-6}(a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1)\\
b_2 &\mapsto u^{-2}(b_2 + 12r)\\
b_4 &\mapsto u^{-4}(b_4 + rb_2 + 6r^2)\\
b_6 &\mapsto u^{-6}(b_6 + 2rb_4 + r^2b_2 + 4r^3)\\
b_8 &\mapsto u^{-8}(b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4)\\
c_4 &\mapsto u^{-4}c_4\\
c_6 &\mapsto u^{-6}c_6\\
\Delta &\mapsto u^{-12}\Delta\\
j &\mapsto j
\end{aligned}
$$

Things to note: If Δ is invertible in R, so is the new discriminant. The term j is invariant under isomorphism.
Given any Weierstrass curve with coefficients in $\mathbb{Z}[a_1, \ldots, a_6]$, an isomorphism can be written down to the universal Weierstrass curve over $A = \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ given by $C_{a_1,\ldots,a_6} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

§Defining a Formal Group Law

Given a Weierstrass curve $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, we can expand about O to get a formal group law.

- We use the substitution $z = -\dfrac{x}{y}$, $w = -\dfrac{1}{y}$ and arrive at

  $$w = z^3 + (a_1z + a_2z^2)w + (a_3 + a_4z)w^2$$

  We then repeatedly substitute this expression for w on the right hand side to get a formal power series in z equal to w.

  – More precisely, let $f_1(z, w) = z^3 + (a_1z + a_2z^2)w + (a_3 + a_4z)w^2$ and let $f_{m+1}(z, w) = f_m(z, f(z, w))$.
  We take $w(z) = \lim\limits_{m\to\infty} f_m(z, 0)$.

- Let $x(z) = \dfrac{z}{w(z)}$ and $y(z) = -\dfrac{1}{w(z)}$. Then $\big(x(z), y(z)\big)$ is a formal solution to the Weierstrass equation.

- Given $\big(z_1, w(z_1)\big)$ and $\big(z_2, w(z_2)\big)$ we can then find z_3 such that $(z_1, w(z_1)) + (z_2, w(z_2)) = -(z_3, w(z_3))$.

  – We have $x(z) = \dfrac{z}{w(z)} = \dfrac{1}{z^2} - \dfrac{a_1}{z} - a_3z - (a_4 + a_1a_3)z^2 - \dots$ and
  $y(z) = -\dfrac{1}{w(z)} = -\dfrac{1}{z^3} + \dfrac{a_1}{z^2} + \dfrac{a_2}{z} + a_3 + (a_4 + a_1a_3)z - \dots$. The line connecting $(z_1, w(z_1))$ and $(z_2, w(z_2))$ is $w = \lambda z + \nu$ where $\lambda = \dfrac{w_2 - w_1}{z_2 - z_1} = \sum\limits_{n=3}^{\infty} A_{n-3}\dfrac{z_2^n - z_1^n}{z_2 - z_1}$ and $\nu = w_1 - \lambda z_1$.
  Setting this equal to our Weierstrass equation for w yields a cubic in z. The roots of this cubic are z_1, z_2, and $z_3 = -z_1 - z_2 - \dfrac{a_1\lambda + a_3\lambda^2 + a_2\nu + 2a_4\lambda\nu + 3a_6\lambda^2\nu}{1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3} \in \mathbb{Z}[a_1, \dots, a_6][\![z_1, z_2]\!]$.
  The group law requires that $\big(z_1, w(z_1)\big) + \big(z_2, w(z_2)\big) + \big(z_3, w(z_3)\big) = O$.

- So, in order to determine the formal group law $F(z_1, z_2)$ associated to E, we will require that $F(z_1, z_2) = i(z_3)$ where $i(z_3)$ is the z-coordinate of $-(z_3, w(z_3))$.

  – We have $z = -\dfrac{x}{y}$ and the inverse of (x, y) is $(x, -y - a_1x - a_3)$.
  So,

  $$\begin{aligned} F(z_1, z_2) = i(z_3) &= \frac{x(z_3)}{y(z_3) + a_1x(z_3) + a_3} \\ &= z_1 + z_2 - a_1z_1z_2 - a_2(z_1^2z_2 + z_1z_2^2) + (-2a_3z_1^2z_2 + (a_1a_2 - 3a_3)z_1^2z_2^2 - 2a_3z_1z_2^3) + \dots \end{aligned}$$

§What is an Elliptic Curve? (Part III)

Definition. *A* ***(generalized) elliptic curve*** *over a scheme S is a morphism of schemes $E \to S$ where each fibre is an elliptic curve. In each fibre we then have a distinguished point O and together these form the identity section $e : S \to E$. We can formally complete the curve at this identity section to get the formal group law. (Zariski locally, this looks like the formal group law we have already given.)*

Recommended Resources

The content relating to elliptic curves over fields comes primarily from Joseph Silverman's books *The Arithmetic of Elliptic Curves* and *Advanced Topics in the Arithmetic of Elliptic Curves*.
Resources for the rest of the content include Ravi Vakil's *The Rising Sea*, Charles Rezk's course notes on tmf, and Robin Hartshorne's *Algebraic Geometry*.