Elliptic Curves over $\mathbb{C}$ and over Finite Fields

Matthew Dupraz

April 5, 2022

1 Basic Facts

1.1 Weierstrass Equation

Our main interest are *elliptic curves*, which are curves in $\mathbb{P}^2$ of genus 1. These are characterized by the homogeneous equation

$$Y^2Z + aXYZ + bYZ^2 = X^3 + cX^2Z + dXZ^2 + eZ^3 \tag{1}$$

for some $a, b, c, d, e \in \mathbb{F}$. Setting $U_Z = \{[X, Y, Z] \in \mathbb{P}^2 \mid Z \neq 0\}$, we can study the solutions of (1) on U_Z using the change of coordinates $x = X/Z$ and $y = Y/Z$. We obtain the following equation

$$y^2 + axy + by = x^3 + cx^2 + dx + e \tag{2}$$

We can further simplify this equation with linear changes of variables. First notice that if $\mathrm{char}(\mathbb{F}) \neq 2$, the left hand side can be written as

$$y(y + ax + b) = (y + \frac{1}{2}(ax + b) - \frac{1}{2}(ax + b))(y + \frac{1}{2}(ax + b) + \frac{1}{2}(ax + b))$$

$$= (y + \frac{1}{2}(ax + b))^2 - \frac{1}{4}(ax + b)^2$$

Hence by replacing y with $y + \frac{1}{2}(ax + b)$ and collecting the terms in each monomial, we get an equation of the form

$$y^2 = x^3 + \alpha x^2 + \beta x + \gamma \tag{3}$$

If $\mathrm{char}(\mathbb{F}) \neq 3$, we can also get rid of the term in x^2 with a linear change of variables. replacing x with $x - \frac{1}{3}\alpha$ yields

$$y^2 = (x - \frac{1}{3}\alpha)^3 + \alpha(x - \frac{1}{3}\alpha)^2 + \beta(x - \frac{1}{3}\alpha) + \gamma$$

$$= x^3 - \alpha x^2 + \frac{1}{3}\alpha^2 x - \frac{1}{27}\alpha^3 + \alpha x^2 - \frac{2}{3}\alpha^2 x + \frac{1}{9}\alpha^3 + \beta x - \frac{1}{3}\alpha\beta + \gamma$$

Collecting the terms in each monomial, we get an equation of the form

$$y^2 = x^3 + Ax + B \tag{4}$$

with $A, B \in \mathbb{F}$. Plugging back the substitutions $x = X/Z$ and $y = Y/Z$, we obtain the homogeneous equation

$$Y^2 Z = X^3 + AXZ^2 + BZ^3 \tag{5}$$

1.2 Singularities

We suppose $\mathbb{F}$ is algebraically closed.

We have that an elliptic curve $V \subset \mathbb{P}_2(\mathbb{F})$ is the projective variety

$$V = V(X^3 + AXZ^2 + BZ^3 - Y^2 Z) = V(F) \tag{6}$$

We are interested in the case where the curve is smooth. By the regular preimage theorem, V is smooth if all its points are non-singular, i.e. if for all $P = [x, y, z] \in V$,

$$\nabla F(P) = \begin{bmatrix} 3x^2 + Az^2 \\ -2yz \\ 2Axz + 3Bz^2 - y^2 \end{bmatrix} \neq 0$$

If $P = [0, 1, 0]$, then

$$\nabla F(P) = \begin{bmatrix} 0 \\ 0 \\ -1 \end{bmatrix} \neq 0$$

hence the point at infinity is never singular. It follows that when looking for singularities, we can consider just the case where $z \neq 0$, since else we have necessarily $x = 0$ and so $P = [0, 1, 0]$. So if there are any singularities of V, they are on $V \cap U_Z$. So V is non-singular precisely when $V \cap U_Z$ is non-singular. Using the isomorphism $V \cap U_Z \to W, [X, Y, Z] \mapsto (\frac{X}{Z}, \frac{Y}{Z})$ it suffices to study singularities on $W = V(x^3 + Ax + B - y^2) = V(f)$

Let $\Delta = 4A^3 + 27B^2$ be the discriminant of the polynomial $g(x) = x^3 + Ax + B$, we have the following criteria for the existence of singularities of V.

Proposition 1.1. *W (and equivalently V) is non-singular if and only if $\Delta \neq 0$.*

Proof. Suppose there is a point $P = (x_0, y_0) \in W$ that is singular, then we have

$$\begin{bmatrix} 3x_0^2 + A \\ -2y_0 \end{bmatrix} = 0$$

Hence we have that $g'(x_0) = 3x_0^2 + A = 0$ and $y_0 = 0$. In particular, since $P \in W$, also $g(x_0) = 0$, and hence since $g(x_0) = g'(x_0) = 0$, x_0 is a double root of g and so the discriminant $\Delta = 4A^3 + 27B^2$ of g is zero.

Suppose instead that $\Delta = 0$, then g admits a double root $x_0 \in \mathbb{F}$ (since we supposed $\mathbb{F}$ algebraically closed) which is unique since g is a cubic polynomial. Then $P = (x_0, 0) \in V$. Furthermore,

$$\nabla f(P) = \begin{bmatrix} 3x^2 + A \\ 0 \end{bmatrix}$$

We have that $3x^2 + A = g'(x) = 0$, hence $\nabla f(P) = 0$ and so W is singular at P. $\square$

2 Elliptic Curves over $\mathbb{C}$

The goal of this section is to show an elliptic curve is homeomorphic to a torus.

Definition 2.1. Let $\Lambda \subseteq \mathbb{C}$ be a lattice

(a) The Weierstrass elliptic function ($\wp$-function), is defined by the series

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

(b) The Eisenstein series (of Λ) of weight k, where $k \geq 2$ is an integer is the series

$$G_k(\Lambda) = \sum_{\lambda \in \Lambda \backslash \{0\}} \lambda^{-k}$$

Notation. If Λ is known from context, we write simply $\wp(z)$ and G_k for $\wp(z; \Lambda), G_k(\Lambda)$ respectively.

Proposition 2.1. *Let Λ be a lattice.*

(a) The Eisenstein series $G_k(\Lambda)$ is absolutely convergent for all $k \geq 3$.

(b) The series defining the Weierstrass $\wp$-function converges absolutely and uniformly on every compact subset of $\mathbb{C} \setminus \Lambda$. It defines a meromorphic function on $\mathbb{C}$ with double poles of residue 0 at each lattice point.

(c) The Weierstrass $\wp$-function is an even elliptic function.

Proof. (a) Let λ_1, λ_2 be basis vectors of Λ. Let

$$A_N := \{ n\lambda_1 + m\lambda_2 \in \Lambda \mid n, m \in \mathbb{Z}, \max(|n|, |m|) = N \}.$$

Let also

$$m = \min\{ |a\lambda_1 + b\lambda_2| \mid a, b \in \mathbb{R}, \max(|a|, |b|) = 1 \},$$

then m is well defined and strictly positive, as it's the minimum of a compact subset of $\mathbb{R}$, which does not contain zero. We have that

$$\#A_N = (2N + 1)^2 - (2N - 1)^2 = 8N.$$

Furthermore, $\min\{ |\lambda|, \lambda \in A_N \} \geq Nm$, so we get

$$\sum_{\lambda \in \Lambda \backslash 0} \frac{1}{|\lambda|^k} \leq \sum_{N=1}^{\infty} \frac{\#A_N}{\min\{ |\lambda|, \lambda \in A_N \}^k} = \sum_{N=1}^{\infty} \frac{8}{m^k N^{k-1}} < \infty.$$

(b) If $|\lambda| > 2|z|$, then we have that

$$|2\lambda - z| \le 2|\lambda| + |z| \le \frac{5}{2}|\lambda|$$

and

$$|z - \lambda| = |\lambda| \left| \frac{z}{\lambda} - 1 \right| \ge \frac{1}{2}|\lambda|.$$

These imply that

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

Hence using (a) we see that for $z \in \mathbb{C} \setminus \Lambda$, the series for $\wp(z)$ converges absolutely and uniformly on any compact subset of $\mathbb{C} \setminus \Lambda$. It follows that the series defines a holomorphic function on $\mathbb{C} \setminus \Lambda$, furthermore, it is clear from the series expansion that $\wp$ has a double pole with residue 0 at each point of Λ.

(c) TO BE ADDED

$\square$

Proposition 2.2. *Let Λ be a lattice. For all $z \in \mathbb{C} \setminus \Lambda$, we have that*

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

Remark. We write

$$g_2 = g_2(\Lambda) = 60G_4 \text{ and } g_3 = g_3(\Lambda) = 60G_3.$$

Then the equation in 2.2 becomes

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

Theorem 2.3. *Let $\Lambda \subseteq \mathbb{C}$ be a lattice and g_2, g_3 its associated quantities. Let $E/\mathbb{C}$ be the curve given by the equation*

$$E : y^2 = 4x^3 - g_2 x - g_3$$

then E is an elliptic curve and the map

$$\phi : \mathbb{C}/\Lambda \to E$$

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

is a complex analytic isomorphism of complex Lie groups.

The following theorem gives the converse to 2.3

4

Theorem 2.4. *Let $E/\mathbb{C}$ be a non-singular curve given by the equation*

$$E : y^2 = 4x^3 - ax - b.$$

Then there exists a lattice $\Lambda \subseteq \mathbb{C}$ unique up to homothety, such that $a = g_2(\Lambda)$ and $b = g_3(\Lambda)$

Since any elliptic curve is isomorphic to a curve given by an equation as in 2.4, we deduce that all curves are homeomorphic to a torus $\mathbb{T}^2$. This allows us to calculate its homology groups.

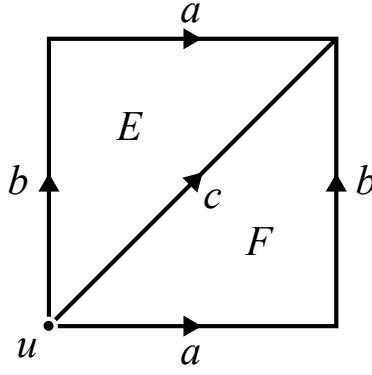The torus can be given the following Δ-complex structure as in Figure 1.

Figure 1: Δ-complex structure of a torus

The associated chain complex for taking simplicial homology is

$$\cdots \longrightarrow 0 \longrightarrow E\mathbb{Z} \oplus F\mathbb{Z} \xrightarrow{\partial_2} a\mathbb{Z} \oplus b\mathbb{Z} \oplus c\mathbb{Z} \xrightarrow{\partial_1} u\mathbb{Z} \longrightarrow 0$$

$$a, b, c \longmapsto 0$$

$$E, F \longmapsto a + b - c$$

Hence we get that

$$H_0(\mathbb{T}^2) \cong \mathbb{Z},$$
$$H_1(\mathbb{T}^2) = \ker \partial_1 / \operatorname{im} \partial_2 = a\mathbb{Z} \oplus b\mathbb{Z} \oplus c\mathbb{Z}/(a + b - c)\mathbb{Z} \cong \mathbb{Z}^2,$$
$$H_2(\mathbb{T}^2) = \ker \partial_2 = (E - F)\mathbb{Z} \cong \mathbb{Z},$$

and $H_n(\mathbb{T}^2) = 0$ for $n \geq 3$. We deduce that the associated Betti numbers are

$$b_0(\mathbb{T}^2) = \operatorname{rk}(\mathbb{Z}) = 1,$$
$$b_1(\mathbb{T}^2) = \operatorname{rk}(\mathbb{Z}^2) = 2,$$
$$b_2(\mathbb{T}^2) = \operatorname{rk}(\mathbb{Z}) = 1,$$

and $b_n(\mathbb{T}^2) = 0$ for $n \geq 3$.

3 Elliptic Curves over Finite Fields

Definition 3.1. The zeta function of $V/\mathbb{F}_q$ is defined as the power series

$$Z(V/\mathbb{F}_q; T) = \exp\left(\sum_{n=1}^{\infty} (\#V(\mathbb{F}_{q^n})) \frac{T^n}{n}\right)$$

Notation. When $V/\mathbb{F}_q$ is known from context, we write simply $Z(T)$ instead of $Z(V/\mathbb{F}_q; T)$

Theorem 3.1 (Weil Conjectures)**.** *Let $V/\mathbb{F}_q$ be a smooth projective variety of dimension N.*

(a) *Rationality: $Z(T) \in \mathbb{Q}(T)$. More precisely, there is a factorization*

$$Z(T) = \frac{P_1(T) \cdots P_{2n-1}(T)}{P_0(T) P_2(T) \cdots P_{2n}(T)},$$

where $P_0(T) = 1 - T, P_{2n}(T) = 1 - q^n T$ and for each $1 \leq i \leq 2n - 1$, $P_i(T)$ factors (over $\mathbb{C}$) as

$$P_i(T) = \prod_j (1 - \alpha_{ij} T)$$

(b) *Functional Equation: The zeta function satisfies*

$$Z\left(\frac{1}{q^N T}\right) = \pm q^{N\frac{\epsilon}{2}} T^\epsilon Z(T),$$

for some integer ϵ (called the Euler characteristic of V)

(c) *Riemann Hypothesis: $|\alpha_{ij}| = q^{i/2}$ for all $1 \leq i \leq 2n - 1$ and all j.*

(d) *Betti Numbers: If $V/\mathbb{F}_q$ is a reduction mod p of a non-singular projective variety W/K, where K is a number field embedded in the field of complex numbers, then the degree of P_i is the ith Betti number of the space of complex points of W.*

Theorem 3.2. *Let $E/\mathbb{F}_q$ be an elliptic curve. Then there exists an $a \in \mathbb{Z}$ such that*

$$Z(T) = \frac{1 - aT + qT^2}{(1 - T)(1 - qT)}.$$

Furthermore,

$$Z\left(\frac{1}{qT}\right) = Z(T)$$

and

$$1 - aT + qT^2 = (1 - \alpha T)(1 - \beta T)$$

with $|\alpha| = |\beta| = \sqrt{q}$

Hence the Weil conjectures are verified for elliptic curves. Notice that $\deg P_0 = 1$, $\deg P_1 = 2$, $\deg P_2 = 1$, which coincides with the Betti numbers we calculated in Section 2.