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

Matthew Dupraz

April 30, 2022

1 Basic Definitions and 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 $\text{char}(\mathbb{F}) \neq 2$, the left hand side can be written as

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

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 $\text{char}(\mathbb{F}) \neq 3$, 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

$$\begin{aligned} y^2 &= (x - \frac{1}{3}\alpha)^3 + \alpha(x - \frac{1}{3}\alpha)^2 + \beta(x - \frac{1}{3}\alpha) + \gamma \\ &= x^3 - \alpha x^2 + \frac{1}{3}\alpha^2 x - \frac{1}{27}\alpha^3 + \alpha x^2 - \frac{2}{3}\alpha^2 x + \frac{1}{9}\alpha^3 + \beta x - \frac{1}{3}\alpha\beta + \gamma \end{aligned}$$

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

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

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

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

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 isomorphic to a torus as a Riemann surface.

First, let's discuss the Riemann surface structure that an elliptic curve has.

Definition 2.1. The *complex topology* on $\mathbb{P}^n$ is the quotient topology induced by the Euclidean topology on $\mathbb{C}^{n+1}$.

Throughout this section we will consider $\mathbb{P}^n$ with the complex topology, and hence an elliptic curve $E(\mathbb{C}) \subset \mathbb{P}^2$ will be equipped with the subspace topology.

Proposition 2.1. *Let $E(\mathbb{C}) \subset \mathbb{P}^2$ be an elliptic curve, then $E(\mathbb{C})$ admits the structure of a Riemann surface.*

Proof. Let $y^2 - x^3 - ax - b = f(x, y) = 0$ be the equation defining $E(\mathbb{C})$. So for all $P = (x_P, y_P) \in E(\mathbb{C})$ with $y_P \neq 0$, $\frac{\partial f}{\partial y}(P) \neq 0$ and hence by the implicit function theorem there exists an open set $V_P \subseteq \mathbb{C}$ containing x_P and an analytic function $g_P : V_P \to \mathbb{C}$, such that $g_P(x_P) = y_P$ and $f(x, g_P(x)) = 0$ for all $x \in V_P$. Furthermore $U_P = \mathcal{G}(g_P) = (\mathrm{id} \times g_P)(V_P) \subset E(\mathbb{C})$, is an open subset of $E(\mathbb{C})$. Hence we define $\phi_P : U_P \to \mathbb{C}, (x, y) \mapsto x$ which is a homeomorphism to its image $\phi_P(U_P) = V_P$ (the inverse to which is given by $x \mapsto (x, g_P(x))$). Hence ϕ_P defines a chart of $E(\mathbb{C})$.

For all $P = (x_P, 0) \in E(\mathbb{C})$ we define the chart $\phi_P : U_P \to \mathbb{C}$ similarly, except we inverse the roles of x and y in the above reasoning. Indeed, $\frac{\partial f}{\partial x}(P) \neq 0$, since $E(\mathbb{C})$ is smooth, hence we get the existence of $V_P \subset \mathbb{C}$ containing y_P and $h_P : V_P \mapsto \mathbb{C}$, such that $h_P(y_P) = x_P$ and $f(h_P(y), y) = 0$ for all $y \in V_P$. We set $U_P := (h_P \times \mathrm{id})(V_P)$ and $\phi_P : U_P \to \mathbb{C}, (x, y) \mapsto y$.

Finally, we have yet to define a chart whose domain covers the point at infinity $O = [0, 1, 0] \in E(\mathbb{C})$. To do this, we can look at $E(\mathbb{C})$ in the chart U_Y instead. We get that in this chart, $E(\mathbb{C})$ is given by the equation.

$$z - x^3 - axz^2 - bz^3 = \tilde{f}(x, z) = 0.$$

We have that $\frac{\partial \tilde{f}}{\partial z}(O) = 1 \neq 0$, hence we can again apply the reasoning from above. We obtain the chart $\phi_O : U_O \to \mathbb{C}, [x, 1, z] \mapsto x$ with inverse $\phi_0^{-1} : \phi_O(U_O) \to \mathbb{C}, x \mapsto [x, 1, \tilde{g}(x)]$.

Now let $P, Q \in E(\mathbb{C}) \setminus \{O\}$, with $y_P \neq 0$ and $y_Q = 0$. We have that

$$\begin{aligned}
\phi_P \circ \phi_Q^{-1}(y) &= \phi_P(h_Q(y), y) = h_Q(y) \\
\phi_Q \circ \phi_P^{-1}(x) &= \phi_Q(x, g_P(x)) = g_P(x) \\
\phi_P \circ \phi_O^{-1}(x) &= \phi_P([x, 1, \tilde{g}(x)]) = \phi_P\left(\frac{x}{\tilde{g}(x)}, \frac{1}{\tilde{g}(x)}\right) = \frac{x}{\tilde{g}(x)} \\
\phi_O \circ \phi_P^{-1}(x) &= \phi_O(x, g_P(x)) = \phi_O\left(\left[\frac{x}{g_P(x)}, 1, \frac{1}{g_P(x)}\right]\right) = \frac{x}{g_P(x)}
\end{aligned}$$

All of these transition maps are holomorphic and by transitivity so are $\phi_O \circ \phi_Q^{-1}$ and $\phi_Q \circ \phi_O^{-1}$. This gives $E(\mathbb{C})$ the structure of a Riemann surface. $\square$

Let's introduce the definition and some basic properties of elliptic functions. For the rest of this section, let $\Lambda \subseteq \mathbb{C}$ be an arbitrary lattice.

Definition 2.2. An *elliptic function* (relative to the lattice Λ) is a meromorphic function f on $\mathbb{C}$, which satisfies

$$f(z+\lambda) = f(z) \qquad \text{for all } \lambda \in \Lambda, z \in \mathbb{C}$$

Notation. The set of elliptic functions relative to the lattice Λ is denoted $\mathbb{C}(\lambda)$.

Remark. $\mathbb{C}(\Lambda)$ is a field with the usual operations of addition and multiplication of complex functions.

Definition 2.3. A *fundamental parallelogram* for Λ is a set of the form

$$D = \{a + r\lambda_1 + s\lambda_2 \mid r, s \in [0,1)\},$$

where $a \in \mathbb{C}$ and λ_1, λ_2 is a basis for Λ.

Proposition 2.2. *An elliptic function with no poles (or no zeros) is constant.*

Notation. For $f \in \mathbb{C}(\Lambda), z \in \mathbb{C}/\Lambda$, we write $f(z), \operatorname{res}_z(f)$ and $\operatorname{ord}_z(f)$ for $f(\bar{z}), \operatorname{res}_{\bar{z}}(f)$ and $\operatorname{ord}_{\bar{z}}(f)$ respectively, for any one representative $\bar{z} \in \mathbb{C}$ of the coset z. This is well defined by the Λ-periodicity of f.

Proposition 2.3. *Let $f \in \mathbb{C}(\Lambda)$.*

(a) $\sum_{z \in \mathbb{C}/\Lambda} \operatorname{res}_z(f) = 0.$

(b) $\sum_{z \in \mathbb{C}/\Lambda} \operatorname{ord}_z(f) = 0.$

Next let us introduce the Weierstrass $\wp$-function, which will serve as a connecting link between elliptic curves and elliptic functions.

Definition 2.4. (a) The Weierstrass elliptic function ($\wp$-function), is defined by the series

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

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

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

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

Proposition 2.4. *(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

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

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

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

and

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

These imply that

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

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

□

Theorem 2.5. *We have that*

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp')$$

Definition 2.5. The *Weierstrass σ-function* (relative to Λ) is the function defined by

$$\sigma(z;\Lambda) = z \prod_{\lambda\in\Lambda\setminus 0} \left(1 - \frac{z}{\lambda}\right) \exp\left(\frac{z}{\lambda} + \frac{1}{2}\left(\frac{z}{\lambda}\right)^2\right)$$

Notation. As before, we write just $\sigma(z)$ for $\sigma(z;\Lambda)$ when Λ is clear from context.

Proposition 2.6. *Let $n_1, \dots, n_r \in \mathbb{Z}$ and $z_1, \dots, z_n \in \mathbb{C}$, such that*

$$\sum n_i = 0 \text{ and } \sum n_i z_i \in \Lambda.$$

Then there exists an elliptic function $f(z) \in \mathbb{C}(\Lambda)$ satisfying

$$\operatorname{div}(f) = \sum n_i(z_i).$$

Proposition 2.7. *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 2.7 becomes

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

Theorem 2.8. *Let g_2, g_3 be the quantities associated to Λ as in the above remark. 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

$$\begin{aligned} \phi : \mathbb{C}/\Lambda &\to E \\ z &\mapsto \begin{cases} [\wp(z), \wp'(z), 1] & \text{if } z \notin \Lambda \\ [0, 1, 0] & \text{if } z \in \Lambda \end{cases} \end{aligned}$$

is a complex analytic isomorphism of complex Lie groups.

Proof. To show E is an elliptic curve, we have to show that it is non-singular. From 1.1 this is the case if and only if the determinant Δ of the polynomial $f(x) = 4x^3 - g_2x - g_3$ is non-zero, in other words if and only if f has no repeated roots. Let $\{\lambda_1, \lambda_2\}$ be a basis of Λ, let $\lambda_3 = \lambda_1 + \lambda_2$. then since $\wp'$ is an odd elliptic function, we have that for $i \in \{1, 2, 3\}$

$$\wp'(\lambda_i/2) = -\wp'(-\lambda_i/2) = -\wp'(\lambda_i/2)$$

and hence $\wp'(\lambda_i/2) = 0$. It follows from 2.7 that $\wp(\lambda_i/2)$ is a root of f. So we need to show that the $\wp(\lambda_i/2)$ are all distinct. The function $\wp(z) - \wp(\lambda_i/2)$ has a double zero at $\lambda_i/2$, since its derivative is $\wp'(z)$ which vanishes at $\lambda_i/2$. Using 2.3 and 2.4, we deduce that these are the only zeroes and hence the $\wp(\lambda_i/2)$ are all distinct. Hence E is indeed an elliptic curve.

The image of ϕ is contained in $E(\mathbb{C})$ by 2.7. Let $[x, y, 1] \in E(\mathbb{C})$, then we have that $\wp(z) - x$ is a non-constant elliptic function, so by 2.2, it has a zero $a \in \mathbb{C}$. Hence $\wp(a) = x$ and hence by 2.7,

$$\wp'(a)^2 = f(\wp(a)) = f(x) = y^2.$$

It follows that $\wp'(a) = \pm y$, hence by replacing a with $-a$ in the case $\wp'(a) = -y$, we get that $\wp'(a) = y$. Hence $\phi(a) = [x, y, 1]$. This shows the surjectivity of ϕ.

Now to show injectivity, suppose $z_1, z_2 \in \mathbb{C}$ are such that $\phi(z_1) = \phi(z_2)$. Suppose $z_1 \not\equiv -z_1 \mod \Lambda$. The function $\wp(z) - \wp(z_1)$ admits the roots $z_1, -z_1, z_2$, but being of order 2, two of these values are congruent mod Λ. Hence $z_2 \equiv \pm z_1 \mod \Lambda$. But since $\wp'(z_1) = \wp'(z_2)$, we get necessarily $z_2 \equiv z_1 \mod \lambda$.

Now, if $z_1 \equiv -z_1 \mod \Lambda$, then

$$\frac{\partial}{\partial z}(\wp(z) - \wp(z_1)) = \wp'(z)$$

and $\wp'(z_1) = \wp'(-z_1) = -\wp'(z_1)$ and hence $\wp'(z_1) = 0$. It follows that z_1 is a double root of $\wp(z) - \wp(z_1)$, which is of order 2. Hence z_2, being also a root of $\wp(z) - \wp(z_1)$, is necessarily congruent to z_1 mod Λ. This shows the injectivity of ϕ.

Now we will show ϕ is an isomorphism of Riemann surfaces. Denote by $\xi : \mathbb{C} \mapsto \mathbb{C}/\Lambda$, the quotient map. Then the charts of $\mathbb{C}/\Lambda$ are given by local sections of ξ. Let $z \in \mathbb{C}$ and $U \ni (x, y)$ an open set such that $\xi|_U$ is injective. Let ψ be a chart of $E(\mathbb{C})$ which we can suppose (up to shrinking U) to be defined on $\phi(\xi(U))$. Depending on the value of $P = \phi(\xi(z))$, ψ will be of one of the three forms as described in the proof of Proposition 2.1. We get that

$$\psi \circ \phi \circ \xi = \begin{cases} \wp & \text{if } P \neq O \text{ and } \wp'(z) \neq 0 \\ \wp' & \text{if } P \neq O \text{ and } \wp'(z) = 0 \\ \frac{\wp}{\wp'} & \text{if } P = O \end{cases}$$

and hence $\psi \circ \phi \circ \xi$ is holomorphic (and seen as a map to its image, it is bijective, and hence biholomorphic). It follows that ϕ is biholomorphic and hence an isomorphism of Riemann surfaces.

Finally, we want to show that ϕ is a group homomorphism. Let $z_1, z_2 \in \mathbb{C}$, then from 2.6, there exists a function $f \in \mathbb{C}(\Lambda)$ with divisor

$$\mathrm{div}(f) = (z_1 + z_2) - (z_1) - (z_2) + (0)$$

Now, by 2.5, we can write $f(z) = F(\wp(z), \wp'(z))$ for some rational function $F(X, Y) \in \mathbb{C}(X, Y)$. We can see F in $\mathbb{C}(E)$ and hence $f = F \circ \phi$. It follows that

$$\mathrm{div}(F) = (\phi(z_1 + z_2)) - (\phi(z_1)) - (\phi(z_2)) + (0)$$

By Proposition **??**, it follows that

$$\phi(z_1 + z_2) = \phi(z_1) + \phi(z_2)$$

$\square$

The following theorem (which we will not prove) gives the converse to 2.8

Theorem 2.9. *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 2.9, we deduce that all curves are homeomorphic to a torus $\mathbb{T}^2$. This allows us to calculate its homology groups.

To calculate the homology groups of a torus, we will use simplicial homology, as in [Hat01, §2.1]. The torus can be given a Δ-complex structure as in Figure 1. The associated chain complex for taking simplicial homology is

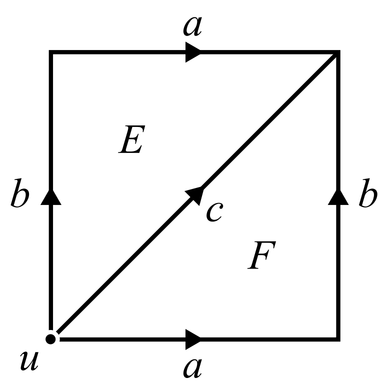

Figure 1: Δ-complex structure of a torus

$$\begin{array}{ccccccccc}
\cdots \longrightarrow 0 \longrightarrow & E\mathbb{Z} \oplus F\mathbb{Z} & \xrightarrow{\partial_2} & a\mathbb{Z} \oplus b\mathbb{Z} \oplus c\mathbb{Z} & \xrightarrow{\partial_1} & u\mathbb{Z} & \longrightarrow 0 \\
 & & & a, b, c & \longmapsto & 0 & \\
 & E, F & \longmapsto & a + b - c & & &
\end{array}$$

Hence we get that

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

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

$$\begin{aligned} b_0(\mathbb{T}^2) &= \mathrm{rk}(\mathbb{Z}) = 1, \\ b_1(\mathbb{T}^2) &= \mathrm{rk}(\mathbb{Z}^2) = 2, \\ b_2(\mathbb{T}^2) &= \mathrm{rk}(\mathbb{Z}) = 1, \end{aligned}$$

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

3 Elliptic Curves over Finite Fields

For this section we fix a prime p and q a power of p.

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 $P_0(T) = 1 - T, P_{2n}(T) = 1 - q^nT$ 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 i^{th} Betti number of the space of complex points of W.

We will now verify Weil's conjecture for elliptic curves. For this we will make use of the homomorphism $\mathrm{End}(E) \to \mathrm{End}(T_l(E)), \psi \mapsto \psi_l$, where l is a prime different from p. If we fix a $\mathbb{Z}_l$-basis of $T_l(E)$, we can write ψ_l as a 2×2 matrix and so we can compute $\det(\psi_l), \mathrm{tr}(\psi_l) \in \mathbb{Z}_l$.

The following proposition tells us that these quantities are not only independent of the choice of basis, but also of the choice of l.

Proposition 3.2. *Let $\psi \in \mathrm{End}(E)$. Then*

$$\det(\psi_l) = \deg(\psi) \text{ and } \mathrm{tr}(\psi_l) = 1 + deg(\psi) - \deg(1-\psi).$$

In particular, $\det(\psi_l), \mathrm{tr}(\psi_l) \in \mathbb{Z}$

Proposition 3.3. *Let $E/\mathbb{F}_q$ be an elliptic curve, and*

$$\phi : E \to E, (x, y) \mapsto (x^q, y^q)$$

the q^{th} Frobenius endomorphism. Let $\alpha, \beta \in \mathbb{C}$ be the roots of the characteristic polynomial of ϕ_l, that is

$$\det(T - \phi_l) = T^2 - \operatorname{tr}(\phi_l)T + \det(\phi_l),$$

then α, β are complex conjugates satisfying $|\alpha| = |\beta| = \sqrt{q}$. Furthermore, for every $n \geq 1$, we have

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n$$

Proof. Fix v_1, v_2 a $\mathbb{Z}_l$-basis for $T_l(E)$, and write the matrix of ψ_l for this basis as

$$\psi_l = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

We have the non-degenerate, bilinear, alternating pairing

$$e : T_l(E) \times T_l(E) \to T_l(\mu)$$

□

Theorem 3.4. *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 $|\alpha| = |\beta| = \sqrt{q}$

Proof. Using the definition of $Z(E/\mathbb{F}_q; T)$, we get

$$\begin{aligned} \log Z(E/\mathbb{F}_q; T) &= \sum_{n=1}^{\infty} (\#E(\mathbb{F}_{q^n})) \frac{T^n}{n} \\ &= \sum_{n=1}^{\infty} (q^n + 1 - \alpha^n - \beta^n) \frac{T^n}{n} \qquad (3.3) \\ &= -\log(1 - qT) - \log(1 - T) + \log(1 - \alpha T) + \log(1 - \beta T) \end{aligned}$$

and hence we get

$$Z(E/\mathbb{F}_q; T) = \frac{(1 - \alpha T)(1 - \beta T)}{(1-T)(1-qT)},$$

which has the desired form. Indeed from (3.3), $|\alpha| = |\beta| = \sqrt{q}$, and

$$\begin{aligned} a = \alpha + \beta = \operatorname{tr}(\phi_l) &= 1 + \deg(\phi) - \deg(1 - \phi) \\ &= 1 + q - \#E(\mathbb{F}_q) \in \mathbb{Z}. \end{aligned}$$

□

Hence the Weil conjectures are verified for elliptic curves. Notice that using the notation from theorem 3.1, $\deg P_0 = 1$, $\deg P_1 = 2$, $\deg P_2 = 1$, hence we would expect the Betti numbers of $E/\mathbb{C}$ to coincide with these values, and indeed, these are exactly the Betti numbers we calculated in Section 2.

References

[Hat01] Allen Hatcher. *Algebraic Topology.* Cambridge University Press, 2001.