# Elliptic Curves and the Weil Conjectures

Andrew Potter

April 24, 2008

## 1 Elliptic Curves and the Group Law

First of all, we would like to recall the definition of an elliptic curve, and the group law on it.

**Definition 1.1.** An *elliptic curve* over a field $k$ of characteristic not 2 or 3 is the set of solutions to an equation of the form

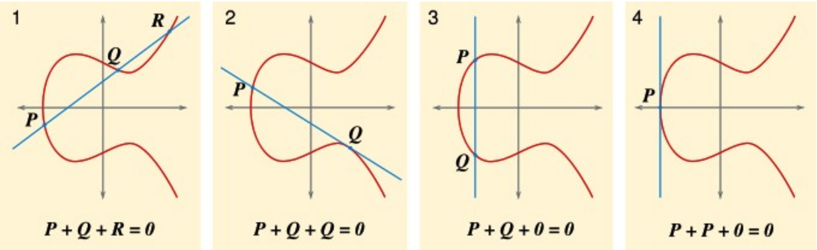
$$y^2 = x^3 + ax + b, \text{ where } a, b \in k \text{ and } -16(4a^3 + 27b^2) \neq 0.$$

The latter equation ensures non-singularity. This equation obviously defines an affine variety, but we should think of it as implicitly defining the corresponding projective variety obtained by homogenising the affine curve. That is, we really mean the projective curve given by the substitution $x = X/Z$, $y = Y/Z$:

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

What extra points at infinity do we gain by considering the projective curve? These can be found by setting $Z = 0$, which means $X = 0$, and so the only point at infinity is $[0, 1, 0]$, which we think of as sitting "at infinity on the $y$-axis".

In order to define a group law on an elliptic curve, we use Bézout's Theorem, which says that two projective curves of degrees $m$ and $n$ respectively intersect in exactly $mn$ points. Say we want to "add" the points $P$ and $Q$ on an elliptic curve $E$ (over $\mathbb{R}$, for argument's sake). We draw the straight line between $P$ and $Q$ and note that by Bézout, this line (of degree 1) will intersect the elliptic curve (of degree 3) in exactly one point other than $P$ and $Q$. Call this point $R$. We then reflect $R$ in the $x$-axis, and call it $-R$. Then we define $P + Q = -R$. Picture 1 below illustrates this definition.



For $Q+Q$, we take the line to be the tangent line at the point $Q$, illustrated by picture 2.

If, as in picture 3, we have $P = -Q$, we see that the line joining the two points does not appear to intersect the curve again, contradicting Bézout's Theorem.

This is because each vertical line intersects the point at infinity $\mathcal{O} = [0, 1, 0]$ we calculated earlier. This point $\mathcal{O}$ will act as the identity element of the group, so that, as one would expect, the inverse of $P$ is $-P$.

Finally, picture 4 illustrates the remaining case where we want to calculate $P + P$ in the case that $P = -P$.

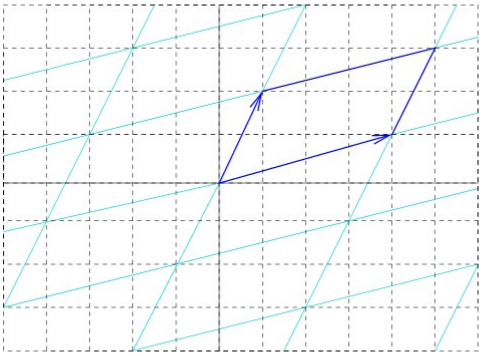
It is easy to check that these definitions of the group operation, identity element, and inverses make sense. Showing that the group operation is associative, however, is by no means trivial!

## 2 Elliptic Curves over $\mathbb{C}$

We now consider elliptic curves over $\mathbb{C}$. The main point to take away from this case is that an elliptic curve over $\mathbb{C}$ "is" a torus.

**Definition 2.1.** Let $v_1, v_2 \in \mathbb{C}$ be complex numbers in the plane which, as vectors in $\mathbb{R}^2$ are linearly independent. A *lattice* $\Lambda$ in $\mathbb{C}$ is a free abelian group of the form $v_1\mathbb{Z} + v_2\mathbb{Z}$.

Using our lattice $\Lambda$, we now consider the space $\mathbb{C}/\Lambda$, which we can think of as the *fundamental parallelogram* with edges $0$, $v_1$, $v_1+v_2$, $v_2$ with opposite sides of the parallelogram identified. This is a group, and we perform addition in $\mathbb{C}/\Lambda$ by adding vectors normally in $\mathbb{C}$, and then reducing back into the fundamental parallelogram. See the picture below.



The point is that $\mathbb{C}/\Lambda$ "is" a torus through the identification of opposite sides of the fundamental parallelogram. To see this, take a rectangular sheet of paper and identify opposite edges by folding the paper over to form a cylinder, and then identify the other two edges by twisting the cylinder around into a torus.

In order to see the connection with elliptic curves, we introduce, for each lattice $\Lambda$, a function $\wp(z)$ on $\mathbb{C}/\Lambda$ which satisfies a differential equation of the form

$$\wp'(z)^2 = 4\wp(z)^3 + a\wp(z) + b, \text{ for some } a, b \in \mathbb{C}.$$

This equation looks very familiar, and in fact, one can show that for each lattice $\Lambda$, there exists an isomorphism $\phi : \mathbb{C}/\Lambda \longrightarrow E$, where $E$ is the elliptic curve given by the equation $y^2 = 4x^3 + ax + b$, given by

$$\phi(z) = (\wp(z), \wp'(z)) = (x, y).$$

So the moral of the story is that there is a one-to-one correspondence between lattices $\Lambda \in \mathbb{C}$ and elliptic curves over $\mathbb{C}$, so that elliptic curves "are" tori.

## 3 Elliptic Curves over Finite Fields

We now consider an elliptic curve over a finite field $\mathbb{F}_q$ of $q = p^r$ elements, where $p$ is a prime and $r \in \mathbb{N}$. Because we have only a finite number of elements in our field $\mathbb{F}_q$, the group of points on an elliptic curve $E(\mathbb{F}_q)$ is also finite. We would like to know exactly how many points are on our elliptic curve.

**Theorem 3.1. Hasse's Theorem**
Let $E$ be an elliptic curve over a finite field $\mathbb{F}_q$. Then there exists an integer $a$ such that

$$|E(\mathbb{F}_q)| = q + 1 - a, \text{ where } |a| \leq 2\sqrt{q}.$$

This theorem gives us a bound on the number of points on $E$, i.e. $|E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$. In particular, $E(\mathbb{F}_q) \neq 0$. We can think of this theorem as telling us that the number of points on $E$ differs from the number of points on the projective line (i.e. $q+1$) by an "error term" $a$ which is bounded by $2\sqrt{q}$.

## 4 The Weil Conjectures

Let $X$ be a nonsingular, $d$-dimensional projective variety over the finite field $\mathbb{F}_q$ of $q$ elements. Let $N_k$ be the number of points on $X$ over the field of $q^k$ elements. The *zeta function* of $X$ is defined as

$$\zeta(X, s) = \exp\left(\sum_{k=1}^{\infty} \frac{N_k}{k}(q^{-s})^k\right).$$

Often we will want to make the substitution $t = q^{-s}$. When we wish to consider the zeta function of $X$ as a function of $t$, the definition becomes

$$Z(X, t) = \exp\left(\sum_{k=1}^{\infty} \frac{N_k}{k} t^k\right).$$

With this set-up, we can now state the Weil Conjectures:

- *Rationality*: $Z(X, t)$ is a rational function of $t$.

  More specifically, $Z(X, t)$ has the following form:

  $$Z(X, t) = \frac{P_1(t)P_3(t)\dots P_{2d-1}(t)}{P_0(t)P_2(t)\dots P_{2d}(t)},$$

  where each $P_i$ is a polynomial with integer coefficients, $P_0(t) = 1 - t$, $P_{2d}(t) = 1 - q^d t$, and for $1 \leq i \leq 2d - 1$,

  $$P_i(t) = \prod_{j=1}^{\beta_i}(1 - \alpha_{i,j}t),$$

  where the $\alpha_{i,j}$ are algebraic integers, and $\beta_i \in \mathbb{N}$ for all $i$ and $j$.

- *Riemann Hypothesis*: $|\alpha_{i,j}| = q^{i/2}$ for all $i$ and $j$.
- *Functional Equation*: Let $\chi$ be the Euler-Poincaré characteristic of $X$. Then
$$Z(X, \frac{1}{q^d t}) = \pm q^{d\chi/2} t^{\chi} Z(X,t).$$
- *Betti Numbers*: Recall that $\beta_i$ is the degree of $P_i(t)$ as above. Then
$$\chi = \sum_{i=0}^{2d} (-1)^i \beta_i.$$
Furthermore, if $X$ is the reduction mod $p$ of a nonsingular projective variety $Y$ over $\mathbb{C}$, then $\beta_i$ is the $i$th *Betti number* of $Y$.

As an example, let $X = E$ be an elliptic curve over $\mathbb{F}_q$. The dimension of $E$ is $d = 1$. Chapter V of Silverman's *The Arithmetic of Elliptic Curves* shows that the zeta function $Z(E,t)$ is given by
$$Z(E,t) = \frac{1 - at + qt^2}{(1-t)(1-qt)},$$
where $a$ is the trace of Frobenius endomorphism, i.e. the integer which satisfies $|E| = q + 1 - a$, and $|a| \leq 2\sqrt{q}$.

Clearly, then, $Z(E,t)$ is a rational function of $t$. Also it is of the required form:
$$Z(E,t) = \frac{P_1(t)}{P_0(t)P_2(t)},$$
where $P_0(t) = 1 - t$ and $P_2(t) = 1 - qt$. $P_1(t)$ clearly factorises as required:
$$P_1(t) = (1 - \alpha_1 t)(1 - \alpha_2 t), \qquad \text{where } \alpha_1, \alpha_2 \in \mathbb{C}.$$

The Riemann Hypothesis comes from a direct equivalence with Hasse's Theorem. One can see this from the observation that $a = -(\alpha_1 + \alpha_2) \leq 2\sqrt{q}$ (by Hasse's Theorem), and also $\alpha_1\alpha_2 = q$, so $|\alpha_1| = |\alpha_2| = \sqrt{q}$.

For an elliptic cuve (which we should think of as just being a torus), the Euler-Poincaré characteristic is just $\chi = 0$. We can get this from the equation $\chi = 2 - 2g$, where $g$ is the genus (for a torus, this is 1). The (first) Betti number is 2. This arises from the rank of the homology group $H_1(E)$, but we should think of this as the "maximum number of cuts we can make on the torus without cutting it in two".