An Elementary Proof of Hasse's Theorem on Elliptic Curves over Finite Fields

George Walker

February 16, 2009

The Weil conjectures describe the number of rational points on a nonsingular variety over a finite field.

We concern ourselves with the first "interesting" case of the Weil conjectures, the case of an *elliptic curve*, that is a smooth irreducible projective curve of genus 1 together with a distinguished point, called the *origin*.

Note that the presence of a distinguished point may not seem so stringent a restriction if you're used to thinking about varieties over algebraically closed fields, but a genus 1 curve over, say, $\mathbb{Q}$ can fail to have any rational points. However we shall see that a genus 1 curve over a *finite* field always has rational points, and so the Theorem always applies to them.

Theorem 1 (Hasse)**.** *Let E be an elliptic curve over $\mathbb{F}_q$. Then there exist complex numbers α and β with $|\alpha| = |\beta| = \sqrt{q}$ such that for each $k \in \mathbb{N}$, $\#E(\mathbb{F}_{q^k}) = 1 + q^k - \alpha^k - \beta^k$.*

Corollary 2 (Hasse)**.** *For E an elliptic curve over $\mathbb{F}_q$, $|\#E(\mathbb{F}_q) - 1 - q| \leq 2\sqrt{q}$.*

A fundamental property of elliptic curves is the addition law, which turns the points of an elliptic curve into an abelian group. For an elliptic curve E given as a nonsingular cubic in $\mathbb{P}^2$ with origin O, this can be described geometrically as follows. Given points A and B on E, let C be the third intersection of the line AB with E. Then $A+B$ is the third intersection of the line OC with E. Although this definition is most useful for explicit computations, it requires some effort to verify that the addition law is associative.

We also need the notion of an *isogeny* between elliptic curves E_1 with E_2, with origins O_1 and O_2, respectively. It is simply a regular map from E_1 to E_2 mapping O_1 to O_2. One can show that such a map is automatically a group homomorphism, and if it is not the zero map then it is finite and surjective. The *degree* of the isogeny is its degree as a finite map, that is, the degree of the field extension of function fields induced by the isogeny. (By convention, the degree of the zero isogeny is 0.) The isogeny is said to be *separable* or *purely inseparable* if this field extension is separable or purely inseparable, respectively. For our purposes we can think of the degree of a separable isogeny as the cardinality of the kernel.

Examples of isogenies include the multiplication by n isogeny $[n] : E \to E$ for $n \in \mathbb{Z}$, which is separable of degree n^2, and for an elliptic curve defined over a finite field of order

q, the Frobenius isogeny $F : E \to E$, which applies the map $x \to x^q$ to the coordinates of points, F is purely inseparable of degree q.

The following constuction, of the *dual isogeny* , will be of great use to us. If you are interested in the proofs, take a looks at [J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer (GTM 106), 1986].

Proposition 3. *To every isogeny $\phi : E_1 \to E_2$ can be associated a unique isogeny $\hat{\phi} : E_2 \to E_1$ such that $\hat{\phi} \circ \phi = [\deg \phi]_{E_1}$ and $\phi \circ \hat{\phi} = [\deg \phi]_{E_2}$. The following also hold:*

1. $\widehat{[n]} = [n]$;
2. *for $\phi_1, \phi_2 : E_1 \to E_2$, $\widehat{\phi_1 + \phi_2} = \hat{\phi}_1 + \hat{\phi}_2$;*
3. *for $\phi_1 : E_1 \to E_2$ and $\phi_2 : E_2 \to E_3$, $\widehat{\phi_2 \circ \phi_1} = \hat{\phi}_1 \circ \hat{\phi}_2$;*
4. $\deg \hat{\phi} = \deg \phi$;
5. $\widehat{\hat{\phi}} = \phi$.

This proposition gives us a way of computing the degree of an isogeny by manipulating the isogeny and its dual. This is the key to the proof of the Weil conjectures.

We shall prove Theorem 1 and we shall also see that every genus 1 curve over a finite field is elliptic.