

The Weil Conjectures

Clemens Koppensteiner

December 4, 2009

Given an algebraic variety over a finite field, one can consider the number of points of this variety over field extensions of the base field. The Weil conjectures (now actually a theorem) are a close description of the generating function of these numbers. Working towards their proof was a major motivation for Grothendieck's "modern" version of algebraic geometry. We will first discuss how to count the number of points on elliptic curves over finite fields (something that is of high importance in modern cryptography), proving the Weil conjectures for elliptic curves on the way. Then will give an idea how the proof in the general case proceeds, without going into any details.

An important note on this text: This document is basically a written form of a talk that I gave in the Part III Seminars in Cambridge in December 2009. While I am rather confident that the mathematics in the first part of this document, I really do not know anything about étale cohomology. The purpose of this talk was just to give an introduction to this important theorem. Therefore the statements in the last part of this text might not be entirely correct. If you find any errors, please let me know (e.g. at me@caramdir.at).

With that disclaimer out of the way, let's proceed to the mathematics. Basically, the Weil conjectures are about the number of points on an algebraic variety. Before we talk about them in general, we will begin by discussing how to count the number of points on an elliptic curve. But first, apart from mathematical curiosity, why would you even want to do this? Let's have a look at early public key cryptography. As you probably know, public key cryptosystems are typically built around a mathematical operation that is easy to do one way, but whose inverse is hard – where "hard" means that it is computationally infeasible. In the early eighties there were basically two types of public key cryptosystems around. One was RSA, which uses the observation that multiplying two integers is easy, but factoring an integer is not. The other systems were Diffie-Hellman type systems which are built around the discrete logarithm problem.

So, what is the discrete logarithm problem? Suppose you are given a finite group G . Then, given an element g of G and an exponent e it is easy to compute g^e . However given elements g and g^e , calculating e is often hard. Classically Diffie-Hellman type systems

use this observation in the multiplicative groups of finite prime fields. However, in the early eighties some algorithms were developed that made calculating discrete logarithms in these groups a little bit less infeasible. Thus there was some concern about the security of these systems and cryptographers were searching for new groups in which to apply Diffie-Hellman type systems. One idea that was floating around was to use the group of points on an elliptic curve over a finite field.

Maybe here is good point to introduce elliptic curves. If you already know what they are, just skip this paragraph. Basically an elliptic curve is just the set of solutions of an equation of the form $y^2 = x^3 + ax^2 + bx + c$ where a , b and c are fixed coefficients in some field. One should really look at this in a projective setting, so the point at infinity in the y -direction is also on the curve. It is usually denoted \mathcal{O} . Given two points, say P_1 and P_2 , we can draw the line through these points (if $P_1 = P_2$, use the tangent), intersect it with curve in a third point and reflect the new point on the x -axis. We define this last point (which by symmetry lies on the curve) to be the sum of P_1 and P_2 . One easily checks that this gives a group structure on the points with the point at infinity acting as the identity. Note that this works over any field (see for example [Sil92] for details). The cool thing about elliptic curves is that this group structure is natural in the following sense: Let ψ be a morphism of elliptic curves that preserves the identity. Then ψ is actually a group homomorphism. This should be all you need to know about elliptic curves for what we want to do – apart from some theorems which I will tell you later.

Back to cryptography: As mentioned, the idea was to use the group of points of an elliptic curve over a finite field for cryptographic purposes. This idea was quite successful and still provides some of the most secure public key cryptosystems. However to actually implement these systems, one additional ingredient is necessary: One needs to know the size of the group. In other words, one needs to know the number of points on the elliptic curve.

How can one count the points without actually having to go through all possible points in the plane? First, note that in geometry one usually tries to avoid working over an algebraically non-closed field. So we will consider the elliptic curve over the algebraic closure $\bar{\mathbb{F}}_q$. Then the \mathbb{F}_q -rational points on the elliptic curve, denoted $E(\mathbb{F}_q)$, are just the set of all points (x, y) on the curve over $\bar{\mathbb{F}}_q$ with both coordinates in the small field. Another way to characterize these points is to use the Frobenius morphism ϕ_q , which is an automorphism of the curve sending every point (x, y) to (x^q, y^q) . From elementary facts about finite fields we know that the \mathbb{F}_q -rational points are exactly the fixed points of the Frobenius morphism. The Frobenius is a nice morphism sending the identity to the identity, so it is a group homomorphism and the fixed points are exactly the kernel of $1 - \phi_q$. We want to know the number of these points. There is a theorem that the number of points in the kernel is equal to the degree of the map for sufficiently nice morphisms of elliptic curves. So we arrive at

$$\#E(\mathbb{F}_q) = \deg(1 - \phi_q).$$

At this point we are somewhat stuck, so we might as well make some wishes that would help use to move one. The first thing is that we'd really like to work over a field of

characteristic zero, because they are just easier. Also we aren't that good in algebraic geometry, but we all know about linear algebra. These wishes might seem unreasonable but the elliptic curve fairy grants both of them! But on the downside, we have to introduce some further notation.

Let ℓ be a prime number different from the characteristic of \mathbb{F}_q . Let $E[\ell^n]$ be the ℓ^n -torsion of E , i.e. the kernel of the multiplication-by- ℓ^n map. Then there are natural maps $E[\ell^{n+1}]$ to $E[\ell^n]$ that are just multiplication by ℓ . This gives an inverse system and the inverse limit of this system is called the Tate module of E , denoted $T_\ell E$. It is a non-trivial theorem of elliptic curves, that $E[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^2$, so the magic of elliptic curves makes it such that the Tate module is actually just a free module of rank two over the ℓ -adic integers, i.e. $T_\ell E \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$. So we are in characteristic zero now and we are pretty close to linear algebra. Tensoring with the ℓ -adic numbers \mathbb{Q}_ℓ would completely give linear algebra, but this is not actually necessary. We are interested in morphisms, so consider an endomorphism ψ . We can restrict it to the torsion subgroups and then the inverse limit gives us a map on the Tate module which we also denote by ψ . This map has to be \mathbb{Z}_ℓ -linear. In other words, to every endomorphism of the elliptic curve we can associate a 2×2 matrix with ℓ -adic integer coefficients. Moreover the magic of elliptic curves provides us with the fact that the degree of ψ equal to the determinant of this matrix.

Returning to our calculation above, we see that the number of rational points is equal to the determinant of $1 - \phi_q$, which, by linear algebra, is equal to $1 - \text{tr } \phi_q + \det \phi_q$. But the last determinant is equal to the degree of the Frobenius which is just q . Hence,

$$\#E(\mathbb{F}_q) = 1 - \text{tr } \phi_q + q.$$

So all we need to do is figure out the trace and there are several algorithms which do just that (in polynomial time in $\log q$).

However instead of describing these algorithms we will try to find out how the number of points behaves under field extensions, say $\mathbb{F}_{q^n}/\mathbb{F}_q$. Since the number of points in an integer and 1 and q are integers, the trace of the Frobenius has to be an integer. Thus the characteristic polynomial $t^2 - (\text{tr } \phi_q)t + q$ of the Frobenius has integer coefficients and we can factor it over the complex numbers, say into $(T - \alpha)(T - \beta)$. To see what happens when we extend the base field we need to figure out the trace of the Frobenius of the bigger field. But this is just the original Frobenius applied n times and linear algebra tells out that this trace is $\alpha^n + \beta^n$. Moreover we can calculate that the absolute values of α and β are both \sqrt{q} .

Plugging this into what we calculated above we have that number of points over the extended field is $1 - \alpha^n - \beta^n + q^n$. Since this is a sequence of integers we could, just for fun, have a look at the corresponding generating function

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

By the geometric series the right side is a rational function in t . However with some trickery, we can make it even nicer. Adding an exponential function and an "over n ",

we get

$$\exp\left(\sum_n \#E(\mathbb{F}_{q^n}) \frac{t^n}{n}\right) = \exp\left(\sum_n (1 - \alpha^n - \beta^n + q^n) \frac{t^n}{n}\right) = \frac{(1 - \alpha t)(1 - \beta t)}{(1 - t)(1 - qt)}.$$

And what we did right now was proving the Weil conjectures for elliptic curves.

So, you have already read three pages and we even proved the Weil conjectures for elliptic curves, but I still haven't told you what the Weil conjectures actually are. Unfortunately, to state them in their full generality we need some further notation.

Let X be a smooth projective variety over some finite field, say $k = \mathbb{F}_q$. If you do not like schemes, you can think of this in a classical way as the set of solutions of system of polynomial equations and ignore the next few sentences. We would like to consider X as a variety over some field extension of k , say $k_n = \mathbb{F}_{q^n}$. For this set X_{k_n} to be the fibred product $X \times_{\text{Spec } k} \text{Spec } k_n$. The Weil conjectures are about k_n -valued (or rational) points of X , denoted $X(k_n)$, which are per definition all closed points p of X_{k_n} with residue field $k(p)$ equal to k_n . Then we put the number of rational points into a generating function like we did in the elliptic curve case. This is the *Zeta-function*

$$Z(X; t) = \exp\left(\sum_n \#X(k_n) \frac{t^n}{n}\right).$$

Why didn't we just take a normal generation function? One reason is that the thing with the exponential map turned out to be quite nice in the elliptic curve case. Another reason is an analogy to L -functions from number theory. One can express the Zeta-function as a product

$$Z(X; t) = \prod_{\substack{p \in X \\ p \text{ closed}}} \frac{1}{1 - t^{[k(p):k]}}.$$

This looks quite like an Euler product like for say the Riemann zeta function.

Now we can finally state the Weil conjectures!

Weil Conjectures. *Let X be a smooth projective variety over \mathbb{F}_q . Put $k_n = \mathbb{F}_{q^n}$ and $d = \dim X$. Then:*

1. *The Zeta function is rational, i.e. $Z(X; t) \in \mathbb{Q}(t)$.*
2. *There is a functional equation*

$$Z\left(X; \frac{1}{q^d t}\right) = \pm q^{d \frac{E}{2}} t^E Z(X; t)$$

for some integer E .

3. *We can write*

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

where all $P_i(t) \in \mathbb{Z}[t]$. We always have $P_0(t) = 1 - t$ and $P_{2d}(t) = 1 - q^d t$ and we can factor the rest as $P_i(t) = \prod_j (1 - \alpha_{ij} t)$ with $|\alpha_{ij}| = q^{i/2}$ and this is the important part – the absolute value of α_{ij} equal to $q^{i/2}$. This is called the analogue to the Riemann hypothesis.

4. If we set $B_i = \deg P_i(t)$, then the integer E from the functional equation is $\sum (-1)^i B_i$. This isn't surprising, but what is surprising is that when X arises in a sufficiently nice way from a complex variety, then the B_i are the usual Betti numbers from algebraic topology.

Weil himself proved these statements for curves and Abelian varieties but got stuck after this. So I guess he started to dream about the elliptic curves fairy and wrote a wish list. Like we did for elliptic curves he wanted to have linear algebra and characteristic zero. But he was a bit more specific than we were and wished for something that is now known as a *Weil cohomology theory* (or more correctly a *weak Weil cohomology theory*). That is L -vector spaces $H^i(X)$ where the characteristic of L is zero that give a contravariant functor from varieties to vector spaces such that the following properties are true:

- All the spaces should be finite dimensional with $H^0(X)$ and $H^1(X)$ one-dimensional. Further they should vanish for all negative i and all $i > 2d$.
- He wished for a nice cohomology theory and nice cohomology theories have a Poincaré duality: There is a non-degenerate natural pairing

$$H^i(X) \times H^{2d-i}(X) \rightarrow H^{2d}(X) \cong L.$$

- Further he liked the idea with the trace, so he wished for something that is called a Lefschetz fixed-point formula: Let ψ be a regular morphism from X to itself. Then the number of fixed points of ψ counted with multiplicity, that is the intersection number of the graph of ψ with the diagonal in $X \times X$ is equal to $\sum_i (-1)^i \text{tr}(\psi|H^i(X))$.

Assuming we have such a Weil cohomology theory the first assertion of the conjectures can be proved by just using the Lefschetz fixed-point formula on the Frobenius, inserting this into the Zeta function, reordering the sums and using some linear algebra. The second statement basically follows from Poincaré duality.

The elliptic curve fairy didn't gift Weil with such a cohomology theory, but Grothendieck did (with help from M. Artin, Verdier and others). He invented ℓ -adic étale cohomology, which unfortunately is too complicated to describe here. This proved the first two statements. However the Riemann hypothesis analogue proved to be more difficult and it took another ten years and careful study of ℓ -adic étale cohomology by Deligne to prove it and the statement about the Betti numbers.

This text was really just a view on the Weil conjectures as seen from a really high viewpoint (like the ISS), so I will leave you with a few pointers to the literature on the subject. First, all the statements about elliptic curves I referred to (and much

more) can be found in [Sil92] (by the way, I consider this as one of the most well-written mathematical books). More about basic algebraic geometry, in particular rational points and the Frobenius morphism can be found in [Liu02], especially section 3.2. A nice overview of the Weil conjectures and the history of their proof is [Maz74]. The whole (or at least at lot of) theory of étale cohomology can be found in [FK88]. Not as complete, but easier to read are the lecture notes [Mil08].

References

- [FK88] Eberhard Freitag and Reinhardt Kiehl. *Etale Cohomology and the Weil Conjecture*. Springer, Berlin Heidelberg, 1988.
- [Liu02] Qing Liu. *Algebraic Geometry and Arithmetic Curves*. Oxford University Press, New York, 2002.
- [Maz74] Berry Mazur. Eigenvalues of Frobenius. In Robin Hartshorne, editor, *Algebraic geometry, Arcata 1974: proceedings*. American Mathematical Society, 1974.
- [Mil08] James S. Milne. Lectures on Etale Cohomology, 2008. Available from World Wide Web: www.jmilne.org/math/.
- [Sil92] Joseph H Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, New York, 1992.