The Weil conjectures

by

Colin Hayman

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Pure Mathematics

Waterloo, Ontario, Canada, 2008

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

In discussing the question of rational points on algebraic curves, we are usually concerned with $\mathbb{Q}$. André Weil looked instead at curves over finite fields; assembling the counts into a function, he discovered that it always had some surprising properties. His conjectures, posed in 1949 and since proven, have been the source of much development in algebraic geometry. In this thesis we introduce the zeta function of a variety (named after the Riemann zeta function for reasons which we explain), present the Weil conjectures, and show how they can be used to simplify the process of counting points on a curve. We also present the proof of the conjectures for the special case of elliptic curves.

Acknowledgments

My supervisor, Dr. David McKinnon, has been a tremendous source of guidance and support throughout the writing of this thesis. I am grateful to him and to the many other University of Waterloo faculty, staff, and fellow graduate students who have given me their friendship and understanding. Particular thanks are due to my readers, Dr. John Lawrence and Dr. Yu-Ru Liu; to my officemates, Magda Georgescu and Michelle Ashburner; and to Shonn Martin, the department's Administrative Coordinator for Graduate Studies, whose help in my time here has been indispensable.

I also wish to thank my family. My brothers and grandparents have always been encouraging and supportive. Above all, I thank my parents, Robert and Jennifer Hayman, who gave me their love of learning and have done everything in their power to help me succeed in my graduate studies.

Dedication

To the memory of Lorna Young – a devoted scholar and a loving great-aunt.

Contents

1 Introduction

1.1 The zeta function of a variety

The Weil conjectures, proposed by André Weil in 1949 [1], are a series of conjectures about the number of points on algebraic varieties over finite fields. They centre on the concept of the zeta function of a variety.

Definition. Let K be the finite field with q elements and K_r the degree-r extension of K (i.e. the finite field of order q^r). Given a projective variety V defined over K, we define the *zeta function* of V over K to be the formal power series

$$Z_{V/K}(T) = \exp\left(\sum_{r=1}^{\infty} \frac{N_r}{r} T^r\right),$$

where N_r is the number of points on V over K_r.

Remarks:

1. Note that since $Z_{V/K}(T)$ is a formal power series, we may ignore issues of convergence.

2. Where no ambiguity is possible, we will suppress the subscript V/K and write $Z(T)$.

3. For simplicity, we will usually use affine coordinates and equations for projective varieties, keeping in mind the point at infinity.

This process is reversible. If we have the zeta function, we can recover the N_r by finding the Taylor series of $\log Z(T)$ and equating coefficients. Equivalently, we can use repeated differentiation:

$$N_r = \frac{1}{(r-1)!}\frac{d^r}{dT^r}\log Z(T)\Big|_{T=0}.$$

Because of the exponentiation, we would expect $Z(T)$ to be a transcendental function. Remarkably, as long as V is smooth, the result turns out to have a simpler form. Consider for example the variety V over $\mathbb{P}^1$ defined by the homogeneous equation $Y = X$. No matter which field K and extension K_r we are working in, the only point on this variety is $[1:1]$; thus $N_r = 1$ for all r. But now

$$\begin{aligned} Z_{V/K}(T) &= \exp\left(\sum_{r=1}^{\infty}\frac{T^r}{r}\right) \\ &= \exp(-\log(1-T)) \\ &= \frac{1}{1-T} \end{aligned}$$

For another example, consider the trivial variety V over $\mathbb{P}^n$ defined by no equations, over the fields K_r of order q^r. The number of points in $\mathbb{P}^n$ over K_r is equal to the number of ways to choose $n+1$ elements of K_r not all zero, divided by the number of units in K_r (to eliminate duplicate points).

In other words,

$$\begin{aligned} N_r &= \frac{(q^r)^{n+1} - 1}{q^r - 1} \\ &= (q^r)^n + \cdots + q^r + 1 = \sum_{i=0}^{n} (q^r)^i \end{aligned}$$

Thus we have

$$\begin{aligned} Z_{V/K}(T) &= \exp \sum_{r=1}^{\infty} \left(\sum_{i=0}^{n} q^{ir} \right) \frac{T^r}{r} \\ &= \exp \sum_{r=1}^{\infty} \sum_{i=0}^{n} \frac{q^{ir} T^r}{r} \\ &= \exp \sum_{i=0}^{n} \sum_{r=1}^{\infty} \frac{(q^i T)^r}{r} \\ &= \exp \sum_{i=0}^{n} (-\log(1 - q^i T)) \\ &= \frac{1}{(1-T)(1-qT)\dots(1-q^n T)} \end{aligned}$$

The zeta function in both cases is rational. That this is the case in general is the first of Weil's conjectures, which, without further ado, we now state.

Theorem. (Weil Conjectures) *Let K be a finite field of order $q = p^m$, p prime, and V/K a smooth projective variety of dimension n. Then the zeta function $Z_{V/K}(T)$ has the following properties:*

1. *Rationality:*

$$Z(T) \in \mathbb{Q}(T).$$

2. *Functional Equation: There is an integer ϵ, the Euler characteristic of V, such that*

$$Z\left(\frac{1}{q^n T}\right) = \pm q^{n\epsilon/2} T^{\epsilon} Z(T).$$

3. *Riemann Hypothesis: There is a factorization*

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

with $P_i(T) \in \mathbb{Z}[T]$ for all i. Further, $P_0(T) = 1 - T$, $P_{2n}(T) = 1 - q^n T$, and for each $1 \leq i \leq 2n-1$, we can factor P_i over $\mathbb{C}$ as

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

with $|\alpha_{ij}| = q^{i/2}$.

4. *If V is the reduction mod p of a variety $\tilde{V}$ defined over a subfield of $\mathbb{C}$, then*

$$\deg P_i(T) = b_i(\tilde{V}),$$

the ith topological Betti number of $\tilde{V}$ in the analytic topology.

These are still known today as the Weil conjectures, but they are in fact proven. The special case of curves had been disposed of by Weil himself (in fact, he gave two proofs, in [2] and [3]); this was among the evidence that led him to propose the conjectures. The proof for smooth varieties in general was gradually put together over the following 25 years. Bernard Dwork es-

tablished the rationality condition in 1960 [4]. Alexander Grothendieck led the attempt to attack the conjectures with the theory of étale cohomology, which he created for the purpose; he succeeded in proving all but the Riemann hypothesis [5]. This final gap was closed by Pierre Deligne in 1973 [6], building on Grothendieck's methods.

1.2 Special cases

The Weil conjectures take a simpler form if we assume V is a curve (that is, a variety of dimension $n = 1$). In the Riemann hypothesis for V, we have

$$Z(T) = \frac{P_1(T)}{P_0(T)P_2(T)}$$

with $P_i(T) \in \mathbb{Z}[T]$ for all i; and we also know $P_0(T) = 1-T$, $P_2(T) = 1-qT$, and P_1 factors over $\mathbb{C}$ as

$$P_1(T) = \prod_j (1 - \alpha_j T)$$

with $|\alpha_j| = q^{1/2}$. Writing $P = P_1$, we have

$$Z(T) = \frac{P(T)}{(1-T)(1-qT)}.$$

What else can we say about $P(T)$? If V is the mod p reduction of a curve $\tilde{V}$ over $\mathbb{C}$, then $\deg P$ will be the first topological Betti number of $\tilde{V}$. As it

happens, the Betti numbers of an algebraic curve over $\mathbb{C}$ are

$$b_0 = 1,\ b_1 = 2g,\ b_2 = 1$$

where g is the genus of the curve. [7] Thus P is of degree $2g$ (and b_0 and b_2 correctly correspond to the degrees of $1 - T$ and $1 - qT$).

In the special case where V is an elliptic curve, we can say more. The genus of an elliptic curve is always 1 (since an elliptic curve, viewed in $\mathbb{C}$, is homeomorphic to the surface of a torus); thus $P(T)$ is quadratic. Further, it factors as $(1 - \alpha T)(1 - \beta T)$ for some $\alpha, \beta \in \mathbb{C}$ of modulus $\sqrt{q}$. Since $P(T) \in \mathbb{Z}[T]$, we see that α and β must be complex conjugates (unless one is $\sqrt{q}$ and the other $-\sqrt{q}$, but we will demonstrate that this cannot occur during the proof of the Weil conjectures for elliptic curves). Thus

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

for some $a \in \mathbb{Z}$.

1.3 Connection to the Riemann zeta function

The second and third Weil conjectures are the motivation for the function's name: the famous Riemann zeta function $\zeta(s)$ has analogous properties. Recall that Riemann's ζ is the analytic continuation of the function defined

by

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + ...$$

or, equivalently, by the Euler product

$$\zeta(s) = \prod_{p} \left(\frac{1}{1 - p^{-s}} \right).$$

To see the similarities between this function and $Z_{V/K}(T)$, we will transform the latter as follows:

$$\zeta_{V/K}(s) = Z_{V/K}(q^{-s})$$

This transformed version is the true analog of the Riemann zeta function. (In fact, some sources prefer this to $Z(T)$ as the definition of the zeta function of V.) We will demonstrate why this is so. First, Riemann's ζ obeys a well-known functional equation:

$$\zeta(s) = 2^s \pi^{s+1} \sin \frac{\pi s}{2} \, \Gamma(1-s)\zeta(1-s),$$

which, if we let $\xi(s) = \pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s)$, takes the symmetric form

$$\xi(1-s) = \xi(s).$$

Similarly, if we assume the functional equation for $Z_{V/K}$, we have

$$\begin{aligned}\zeta_{V/K}(n-s) &= Z_{V/K}(\frac{1}{q^n q^{-s}}) \\ &= \pm q^{n\epsilon/2}(q^{-s})^{\epsilon} Z_{V/K}(q^{-s}) \\ &= \pm q^{(n/2-s)\epsilon}\zeta_{V/K}(s);\end{aligned}$$

for the special case of elliptic curves, whose Euler characteristic ϵ is zero (by the basic topological formula $\epsilon = 2 - 2g$), we have

$$\zeta_{V/K}(n-s) = \zeta_{V/K}(s).$$

As for the Riemann hypothesis, the familiar statement for Riemann's ζ is

$$\forall s \notin \mathbb{Z} : \ \zeta(s) = 0 \implies \Re(s) = \frac{1}{2}.$$

(The condition $s \notin \mathbb{Z}$ excludes the trivial zeroes at -2, -4, etc.) Similarly, if $Z_{V/K}$ takes the form in Weil's third conjecture, we have

$$\begin{aligned}\zeta_{V/K}(s) = 0 &\implies Z_{V/K}(q^{-s}) = 0 \\ &\implies \exists i, j : q^s = \alpha_{ij}, \ i \text{ odd}\end{aligned}$$

which, upon taking (complex) logarithms, gives

$$\begin{aligned}\Re(s \log q) &= \Re(\log \alpha_{ij}) \\ (\log q)\Re(s) &= \log |\alpha_{ij}| \\ \Re(s) &= \frac{\log q^{i/2}}{\log q} = \frac{i}{2}.\end{aligned}$$

In the special case of elliptic curves, i can only be 1 here, and we have $\Re(s) = \frac{1}{2}$, exactly as in the standard Riemann hypothesis.

2 Using the Weil conjectures

2.1 Elliptic curves

The Weil conjectures guarantee that the zeta function of a variety can be written as a rational function of a certain form; in particular, it is determined by the values of finitely many constants (the α_{ij} in the Riemann hypothesis). Since the Taylor series of this rational function must match the zeta function, we can find the constants by comparing the initial terms of the Taylor series to the zeta function coefficients. (In general, if there are n constants to find, we will need n of the N_r.) In turn, once we know the constants, we can compute the Taylor series in full. The Weil conjectures thus make it possible to determine all the N_r for a particular variety based on a finite number of them.

As a first example, consider the variety

$$V : y^2 = x^3 - 1$$

over the finite fields K_r of order q^r. If char K is 2 or 3, the variety V will be singular, so we begin with $q = 5$. Since V is an elliptic curve, we have

$$Z(T) = \frac{1 - aT + 5T^2}{(1 - T)(1 - 5T)},\ a \in \mathbb{Z}$$

according to our work in §1.2. Thus we need only determine the value of a to obtain the whole function. Using the Taylor series expansion, we find

$$\log Z(T) = (6 - a)T + (18 - \frac{1}{2}a^2)T^2 + (42 + 5a - \frac{1}{3}a^3)T^3 + ...$$

Recalling that

$$\log Z(T) = \sum_{r=1}^{\infty} \left(\frac{N_r}{r} \right) T^r,$$

we have

$$a = 6 - N_1.$$

Now N_1 is the number of points of V over the field $\mathbb{F}_5$. By straightforward enumeration, we find that the points are

$$[0 : 1 : 0], [0 : 2 : 1], [0 : 3 : 1], [1 : 0 : 1], [2 : 4 : 1], [3 : 1 : 1]$$

for a total of 6. Thus $N_1 = 6$ and $a = 0$, and we can state the exact zeta function:

$$Z_{V/K}(T) = \frac{1 + 5T^2}{(1 - T)(1 - 5T)}.$$

We can now obtain any value of N_r we wish by using the Taylor series coefficients. For example, the coefficient of T^3 in the Taylor series is 42; and enumeration confirms that $N_3 = 126 = 3(42)$.

The same method will work for a general q. Computing the Taylor series of $\log Z(T)$ gives

$$a = 1 + q - N_1,$$

so we only need N_1 to determine the zeta function, and in turn, the number of points on V over any of the fields K_r. (It is particularly interesting to note that any two elliptic curves V_1 and V_2 which have the same number of points in K will have the same number in any extension K_r.) Substituting this expression for a back into the zeta function, we can give the following explicit formula:

Proposition 1. *Let V be a nonsingular elliptic curve defined over the field K of order q. Then the number of points of V over the degree-r extension K_r is given by*

$$N_r = \left[\frac{1}{(r-1)!} \frac{d^r}{dT^r} \log \frac{1 - (1 + q - N)T + qT^2}{(1 - T)(1 - qT)} \right]_{T=0},$$

where N is the number of K-rational points of V.

This is a complicated formula, but it will give us any N_r in terms of N and q. Here are the first few cases, in which some interesting patterns appear:

$$\begin{aligned}
N_2 &= 2N(1+q) - N^2 \\
N_3 &= 3N(1+q+q^2) - 3N^2(1+q) + N^3 \\
N_4 &= 4N(1+q+q^2+q^3) - 2N^2(3+4q+3q^2) + 4N^3(1+q) \\
&\quad + 4N^3(1+q) - N^4 \\
N_5 &= 5N(1+q+q^2+q^3+q^4) - 5N^2(2+3q+3q^2+2q^3) \\
&\quad + 5N^3(2+3q+2q^2) - 5N^4(1+q) + N^5
\end{aligned}$$

2.2 Hyperelliptic curves

Next, consider

$$V' : y^2 = x^6 - 1$$

over the same fields. This is not an elliptic curve, so the form of the zeta function will be more complicated. We must allow for a function of the form

$$Z(T) = \frac{P(T)}{(1-T)(1-5T)}$$

where the degree of P is 4 (twice the genus of V'). However, we know by the Riemann hypothesis for this curve that the roots of P occur in conjugate

pairs and have modulus $\sqrt{5}$. Thus we let

$$P(T) = (1 - aT + 5T^2)(1 - bT + 5T^2),\ a, b \in \mathbb{R}.$$

Computing the Taylor series of this function gives

$$\log Z(T) = (6-a-b)T+(23-\frac{1}{2}(a^2+b^2))T^2+(42+5(a+b)-\frac{1}{3}(a^3+b^3))T^3+...$$

With two constants to find, we need two coefficients in order to determine $P(T)$. The values of N_r this time cannot easily be found by hand, but using a computer program, we can calculate the first few values:

$$N_1 = 6; N_2 = 46; N_3 = 126; N_4 = 526.$$

Once again, we use the rule that the rth coefficient of $\log Z(T)$ is $\frac{N_r}{r}$. This time we get a system of equations:

$$\begin{aligned} 6 - a - b &= 6, \\ 23 - \frac{1}{2}(a^2 + b^2) &= 23. \end{aligned}$$

We can stop here; indeed, we do not even need the first equation, as the second gives us $a = b = 0$ at once. Thus

$$P(T) = (1 + 5T^2)^2$$

and

$$Z(T) = \frac{(1 + 5T^2)^2}{(1 - T)(1 - 5T)}$$

Note that this is the zeta function for $y^2 = x^3 - 1$ with the numerator squared. This is not a coincidence. The details are beyond the scope of this thesis; the key, however, is that V' has a nontrivial automorphism ϕ given by $(x, y) \mapsto (-x, y)$. This, along with the factorization $y^2 = -(x^3 - 1)((-x)^3 - 1)$, makes the curve isomorphic to the Jacobian variety of $y^2 = x^3 - 1$, which in turn brings about the relationship between the two zeta functions.

2.3 Quadratic twists

Consider an elliptic curve in Weierstrass form

$$V : y^2 = f(x) = x^3 + bx + c$$

over the finite fields K_r where $|K| = q = p^m$, $p \neq 2$. We can apply a so-called quadratic twist to this curve by introducing a constant multiplier:

$$\tilde{V} : ay^2 = f(x),\ a \in \mathbb{F}_q,\ a \text{ nonsquare}$$

If a were a square in $\mathbb{F}_q = K$, the results would be of no interest. For suppose $a = k^2$; then the map $(x, y) \to (x, ky)$ is an isomorphism from $\tilde{V}$ to V. Thus we require that a is a nonsquare.

How should we expect the zeta function of $\tilde{V}$ to compare with that of V? To answer this, we must find the connection between the N_r and the $\tilde{N}_r$, where $\tilde{N}_r$ is the number of points on $\tilde{V}$ over K_r.

We begin in $K_1 = K$ and consider the values that x and y can take on. For any x, $f(x)$ is either a square or a nonsquare in K.

- If $f(x)$ is a nonzero square, it has two square roots in K, each a value of y such that (x, y) satisfies $y = f(x)$; thus the two points $[x : y : 1]$ lie on V.

- If $f(x)$ is a nonsquare, then $a^{-1}f(x)$ is a square. (Since $p \neq 2$, the subgroup of squares in the multiplicative group K^* has index 2; it is easy to show that two elements lying outside an index-2 subgroup have a product inside the subgroup.) In this case there will be two values of y satisfying the "twisted" equation $ay^2 = f(x)$ and two points $[x : y : 1]$ on $\tilde{V}$.

- Finally, if $f(x)$ is 0, y must also be 0, so we have one point on each of the curves V and $\tilde{V}$.

Thus each of the q possible values for x gives us two points in total – either two on the same curve or one on each. Taking into account the point at infinity $[0:1:0]$ on each curve, we have the following relationship:

$$N_1 + \tilde{N}_1 = 2(q+1).$$

We can apply the same reasoning in the extension fields K_r, but now we must be careful, since a may become a square. This will happen if and only if K_r is a splitting field for the irreducible quadratic $x^2 - a$. The smallest such splitting field, unique up to isomorphism, is K_2 (recall that one standard way to construct K_r is to adjoin a root of a degree-r irreducible polynomial). So a is a nonsquare in K_r if and only if K_r contains K_2 as a subfield. But a basic result in finite field theory is that

$$\mathbb{F}_{p^m} \text{ is a subfield of } \mathbb{F}_{p^n} \iff m \mid n.$$

Thus a remains a nonsquare in K_r if and only if $2 \nmid r$, i.e. r is odd. Based on our reasoning above for the square and nonsquare cases, we can specify $\tilde{N}_r$ in full:

$$\tilde{N}_r = \begin{cases} 2(q^r+1) - N_r, & r \text{ odd} \\ N_r, & r \text{ even} \end{cases}$$

We can apply this to the zeta function for $\tilde{V}$ (which we will denote $\tilde{Z}$).

$$\begin{aligned}
\log \tilde{Z}(T) &= \sum_r \frac{\tilde{N}_r}{r} T^r \\
&= \sum_{r \text{ odd}} \frac{2(q^r+1) - N_r}{r} T^r + \sum_{r \text{ even}} \frac{N_r}{r} T^r \\
&= 2 \sum_{r \text{ odd}} \frac{q^r+1}{r} T^r + \sum_{r \text{ odd}} \frac{-N_r}{r} T^r + \sum_{r \text{ even}} \frac{N_r}{r} T^r \\
&= \left[2 \sum_{r \text{ odd}} \frac{(qT)^r}{r} + 2 \sum_{r \text{ odd}} \frac{T^r}{r} \right] + \sum_r \frac{N_r}{r} (-T)^r
\end{aligned}$$

which, recognizing the first two sums as Taylor series, becomes

$$\begin{aligned}
&= 2 \left[\frac{1}{2} \log \frac{1+qT}{1-qT} \right] + 2 \left[\frac{1}{2} \log \frac{1+T}{1-T} \right] + \log Z(-T) \\
\therefore \tilde{Z}(T) &= \frac{(1+T)(1+qT)}{(1-T)(1-qT)} Z(-T) \qquad (*)
\end{aligned}$$

This is an interesting relationship. Thus far, however, we have not used the Weil conjectures. Using them gives us not only a better result but also an easier proof. Recall that since V is an elliptic curve, we have

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

where N is the number of K-rational points on V. But $\tilde{V}$ is also elliptic – indeed, the isomorphism $(x, y) \mapsto (ax, ay)$ gives us its equation in Weierstrass form as

$$y^2 = x^3 + (a^{-1}b)x + (a^{-1}c).$$

Thus we can apply the same formula. Recalling that $\tilde{N} = 2(q+1) - N$ (where $\tilde{N} = \tilde{N}_1$), we have

$$1 + q - \tilde{N} = -(1 + q - N),$$

and so

$$\tilde{Z}(T) = \frac{1 + (1 + q - N)T + qT^2}{(1 - T)(1 - qT)},$$

which is the same result we would get by using (*). Thus, given the zeta function of an elliptic curve, one can immediately write down that of its quadratic twist simply by changing the sign of the T coefficient in the numerator.

In particular, for our example of $y^2 = x^3 - 1$ over $K = \mathbb{F}_5$, with the zeta function

$$Z_{V/K}(T) = \frac{1 + 5T^2}{(1 - T)(1 - 5T)},$$

we see that the quadratic twist (e.g. $3y^2 = x^3 - 1$, which is isomorphic to $y^2 = x^3 - 2$) has precisely the same zeta function.

3 Proof of the Weil conjectures for elliptic curves

Weil himself, several years before the 1949 paper posing his conjectures, was the first to prove that they hold for the special case of elliptic curves. We will present this proof. We begin by introducing two concepts critical to the proof: the Tate module and the Weil pairing.

The Tate module

Let V be an elliptic curve over a general field K, and fix an algebraic closure $\overline{K}$ of K. For each integer m, we define the multiplication map $[m]$ on the curve group of V in the natural way (that is, by adding P to itself m times):

$$[m]P = mP.$$

This is clearly an endomorphism. The *m-torsion subgroup* $V[m]$ is the kernel of this map; that is, the set of points of order dividing m.

$$V[m] = \{P \in V : [m]P = O\}$$

This is indeed a subgroup of the curve group of V. Further, note that for any m and k, there is a natural map from $V[km]$ to $V[m]$ given by $P \mapsto [k]P$.

We can say a great deal about the structure of these torsion subgroups:

Theorem 1. *Let V be an elliptic curve over a general field K, and $m \neq 0$ an integer.*

a. The multiplication map $[m]$ on the curve group of V has degree m^2.

b. If $\mathrm{char}(K) = 0$, or if $\mathrm{char}(K) = p$ and $p \nmid m$, then

$$V[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}).$$

c. If $\mathrm{char}(K) = p$, then either

$$V[p^n] \cong \{0\} \qquad \text{for all } n \in \mathbb{Z}^+ \text{ or}$$
$$V[p^n] \cong \mathbb{Z}/p^n\mathbb{Z} \qquad \text{for all } n \in \mathbb{Z}^+.$$

Proof. See [8] §III.6.4. □

However, we have more than this. $V[m]$ is also subject to a natural group action by the Galois group $G_{\overline{K}/K}$. For let $G_{\overline{K}/K}$ act on points of V by acting on each coordinate, and let $\phi \in G_{\overline{K}/K}$ and $P \in V[m]$; then

$$[m]\phi(P) = \phi([m]P) = \phi(O) = O,$$

so $\phi(P) \in V[m]$. Thus each $\phi \in G_{\overline{K}/K}$ acts as an automorphism on $V[m]$,

and we have an injective map (assuming now that m is coprime to $\mathrm{char}(K)$):

$$G_{\overline{K}/K} \to \mathrm{Aut}(V[m]) \cong GL_2(\mathbb{Z}/m\mathbb{Z}).$$

Note that the isomorphism above depends on the basis chosen for $V[m]$; in particular, we have to find one. This is not always convenient. The Tate module is one way to get around this problem: rather than looking for bases for individual m-torsion subgroups, we fit a large class of them together with appropriate maps and find a basis for the entire structure.

Definition. For any elliptic curve V and prime number l, we define the *(l-adic) Tate module* of V to be the inverse limit

$$T_l(V) = \varprojlim V[l^n],$$

where the limit is taken with respect to the natural maps

$$V[l^{n+1}] \xrightarrow{[l]} V[l^n].$$

This construction is analogous to that of the l-adic integers, so it is not surprising that $T_l(V)$ turns out to be a $\mathbb{Z}_l$-module. The action of $\mathbb{Z}_l$ on $T_l(V)$ extrapolates in a natural way from the action of $\mathbb{Z}/l^n\mathbb{Z}$ on $V[l^n]$ for each n, and we have the following:

Proposition 2. *The structure of $T_l(V)$ as a $\mathbb{Z}_l$-module is*

$$T_l(V) \cong \mathbb{Z}_l \times \mathbb{Z}_l \qquad \text{if } l \neq \text{char}(K),$$
$$T_l(V) \cong \{0\} \text{ or } \mathbb{Z}_l \qquad \text{if } l = \text{char}(K).$$

Now the action of $G_{\overline{K}/K}$ on the various groups $V[l^n]$ commutes, as we have seen, with the multiplication maps $[l]$ between them. Thus the action of $G_{\overline{K}/K}$ extends naturally to $T_l(V)$.

Next we consider $\text{End}(V)$, the set of isogenies (morphisms that fix O) on V. If $\phi \in \text{End}(V)$ and $P \in V[l^n]$, we have

$$[l^n]\phi(P) = \phi([l^n]P) = \phi(O) = O,$$

so ϕ induces a map from each $V[l^n]$ to itself. Further, these maps agree with the maps that make up the inverse limit $T_l(V)$. Thus ϕ induces a map on the whole Tate module:

$$\phi_l : T_l(V) \to T_l(V).$$

Further, ϕ_l is $\mathbb{Z}_l$-linear. Thus the map $\phi \mapsto \phi_l$ gives us a ring homomorphism from $\text{End}(V)$ to $\text{End}(T_l(V))$ (where the latter End refers to group homomorphisms, not isogenies). This is injective, and in fact we can say something stronger.

Proposition 3. *If V/K is an elliptic curve and l a prime not equal to*

$\mathrm{char}(K)$, *then the natural map*

$$\mathrm{End}(V) \otimes \mathbb{Z}_l \to \mathrm{End}(T_l(V))$$

is injective.

Proof. See [8] §III.7.4. □

The Weil Pairing

We note first the following fact about divisors on an elliptic curve V:

Proposition 4. *For any family of integers* $\{n_P\}_{P \in V}$*, the divisor*

$$D = \sum n_P P \in Div(V)$$

is principal (that is, the divisor of some rational function) if and only if $D \in \mathrm{Div}^0(V)$ *(i.e.* $\sum n_P = 0$*) and* $\sum [n_P]P = O$ *in the curve group of* V*.*

Proof. See [8] §III.3.5. □

Let V be an elliptic curve over a field K of characteristic p, $\overline{K}$ a fixed algebraic closure of K, and $m \geq 2$ an integer coprime to p if $p \neq 0$. For any $T \in V[m]$, we know by the above proposition that there is a function f in $\overline{K}(V)$, the function field of V over $\overline{K}$, such that

$$\mathrm{div}(f) = mT - mO.$$

Similarly, if $T' \in V$ with $[m]T' = T$, there is a function $g \in \overline{K}(V)$ such that

$$\mathrm{div}(g) = [m] * (T) - [m] * (O) = \sum_{R \in V[m]} (T' + R) - (R).$$

The functions $f \circ [m]$ and g^m have the same divisor, so multiplying f by an element of $\overline{K}^*$ if necessary, we may assume that

$$f \circ [m] = g^m.$$

Now suppose $S \in V[m]$ (S may equal T). Then for any $X \in V$, we have

$$g(X + S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m.$$

Thus we can define the following pairing, which we call the *Weil e_m-pairing*:

$$e_m : V[m] \times V[m] \to \boldsymbol{\mu}_m$$

$$(S, T) \mapsto \frac{g(X + S)}{g(X)},$$

where $\boldsymbol{\mu}_m$ is the multiplicative group of mth roots of unity in $\overline{K}$ (note that this is isomorphic to the mth roots of unity in $\mathbb{C}$ since m is coprime to p) and $X \in E$ is any point such that $g(X + S)$ and $g(X)$ are both defined and nonzero. This pairing has several important properties.

Proposition 5. *The Weil m-pairing is*

a. Bilinear:

$$e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T),$$
$$e_m(S, T_1 + T_2) = e_m(S, T_1)e_m(S, T_2).$$

b. Alternating:

$$e_m(T, T) = 1, \text{ and so } e_m(S, T) = e_m(T, S)^{-1}.$$

c. Nondegenerate:

$$e_m(S, T) = 1 \ \forall S \implies T = O.$$

d. Galois invariant:

$$\phi(e_m(S, T)) = e_m(\phi(S), \phi(T)) \ \forall \phi \in G_{\overline{K}/K}.$$

e. Compatible: If $S \in V[km]$, $T \in V[m]$, then

$$e_{km}(S, T) = e_m([k]S, T).$$

Proof. See [8] §III.8.1. □

Since the Weil m-pairings are based on the m-torsion subgroups of V, it is natural to ask whether we can extend them to the Tate module, which is

an inverse limit of such subgroups. We can indeed do this. First we need a construction analogous to the Tate module for the groups $\boldsymbol{\mu}_m$, so we define the following:

Definition. If K is a field with algebraic closure $\overline{K}$ and l is a prime not equal to $\mathrm{char}(K)$, we define the *(l-adic) Tate module of K* to be the inverse limit

$$T_l(K) = \varprojlim \boldsymbol{\mu}_{l^n},$$

taken with respect to the lth-power maps

$$\boldsymbol{\mu}_{l^{n+1}} \xrightarrow{\pi_l} \boldsymbol{\mu}_{l^n}.$$

given by $\pi_l(x) = x^l$. This is clearly much like the Tate module of an elliptic curve. (In fact, it is isomorphic to their motivating example, $\mathbb{Z}_l$.) Our goal now is to fit together the pairings

$$e_{l^n} : V[l^n] \times V[l^n] \to \boldsymbol{\mu}_{l^n}$$

for all n, to get a pairing of the form

$$e : T_l(V) \times T_l(V) \to T_l(K).$$

We do this in the natural way:

Definition. The *Weil pairing* on $T_l(V)$ is given by

$$e(S,T) = e_{l^n}(S,T)$$

for the smallest $n \geq 0$ such that $S, T \in V[l^n]$.

Clearly such an n must exist and be unique. Now we need only demonstrate that our chosen e is compatible with the maps making up the inverse limits $T_l(V)$ and $T_l(K)$. Recall that these maps are

$$V[l^{n+1}] \xrightarrow{[l]} V[l^n] \text{ and } \boldsymbol{\mu}_{l^{n+1}} \xrightarrow{\pi_l} \boldsymbol{\mu}_{l^n}$$

for all n. To show that e is compatible with these, suppose $V[l^{n+1}]$ is the smallest l^n-torsion subgroup containing the points S and T. Then $V[l^n]$ is the smallest containing $[l]S$ and $[l]T$. Now, using the properties of the Weil l^n-pairings, we have

$$\begin{aligned}(e(S,T))^l &= (e_{l^{n+1}}(S,T))^l \\ &= e_{l^{n+1}}(S,[l]T) \\ &= e_{l^n}([l]S,[l]T) \\ &= e([l]S,[l]T)\end{aligned}$$

and so

$$\pi_l \circ e = e \circ [l],$$

as required. Thus our definition of the Weil pairing is consistent with the inverse limits $T_l(V)$ and $T_l(K)$. Further, since it reduces to some Weil m-pairing for any finite set of points, it inherits all the properties listed in Proposition 5. Thus we conclude the following:

Proposition 6. *For any elliptic curve V/K and prime l not equal to $char(K)$, the Weil pairing*

$$e : T_l(V) \times T_l(V) \to T_l(K)$$

is bilinear, alternating, nondegenerate, and Galois invariant.

Proof of the Weil conjectures

We now have the machinery required to proceed. Let V be an elliptic curve defined over the finite field K of order $q = p^m$. For any prime l, we can construct the Tate module $T_l(V)$, and we have a natural injective map $\mathrm{End}(V) \hookrightarrow \mathrm{End}(T_l(V))$ given by $\phi \mapsto \phi_l$. Further, if $l \neq p$, we know that

$$T_l(V) \cong \mathbb{Z}_l \times \mathbb{Z}_l,$$

where $\mathbb{Z}_l$ is the module of l-adic integers. Thus we can choose a basis $B = \{v_1, v_2\}$ for $T_l(V)$ as a $\mathbb{Z}_l$-module. The map ϕ_l may then be represented with respect to this basis as a 2×2 matrix. We will write $\det(\phi_l)$ and

$\mathrm{tr}(\phi_l)$ for the determinant and trace of this matrix, respectively; note that these are independent of B since any two matrices representing ϕ_l are similar.

We now claim the following:

Proposition 7. *For any ϕ in* $\mathrm{End}(V)$*,*

$$\det(\phi_l) = \deg(\phi)$$

and

$$\mathrm{tr}(\phi_l) = 1 + \deg(\phi) - \deg(1 - \phi).$$

In particular, $\det \phi_l$ *and* $\mathrm{tr}\, \phi_l$ *are in* $\mathbb{Z}$ *and do not depend on* l*.*

Proof. As discussed above, we write

$$[\phi_l]_B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Now we know that the Weil pairing

$$e : T_l(V) \times T_l(V) \to T_l(K)$$

is nondegenerate, bilinear, and alternating. Letting $[m]$ represent the multiplication-

by-m map on V, and making use of the dual isogeny $\hat{\phi}_l$ (see [8]), we have

$$\begin{aligned} e(v_1, v_2)^{\deg \phi} &= e([\deg \phi]v_1, v_2) \\ &= e(\hat{\phi}_l \phi_l v_1, v_2) \\ &= e(\phi_l v_1, \phi_l v_2) \\ &= e(av_1 + cv_2, bv_1 + dv_2) \\ &= e(v_1, v_2)^{ad-bc} \\ &= e(v_1, v_2)^{\det \phi_l}. \end{aligned}$$

But e is nondegenerate, so this implies that $\deg \phi = \det \phi_l$. Applying this to $1 - \phi$ as well, we get

$$\begin{aligned} 1 + \deg \phi - \deg(1 - \phi) &= 1 + \det \phi_l - \det(1 - \phi_l) \\ &= 1 + (ad - bc) - ((1 - a)(1 - d) + bc) \\ &= a + d = \operatorname{tr} \phi_l, \end{aligned}$$

as required. □

With these facts established, let ϕbe the (componentwise) qth-power Frobenius endomorphism on V, which fixes exactly the points of $V(K)$. This allows us to isolate $V(K)$ by comparing ϕ with the identity map:

$$\#V(K) = \deg(1 - \phi)$$

Similarly, for each $r \geq 1$, ϕ^r is the q^rth-power Frobenius endomorphism and fixes exactly the points of $V(K_r)$. Thus

$$\#V(K_r) = \deg(1 - \phi^r)$$

Now consider ϕ_l. By Proposition 7, its characteristic polynomial $\xi(T)$ has integer coefficients. We factor it as

$$\xi(T) = \det(TI - \phi_l) = (T - \alpha)(T - \beta)$$

for some $\alpha, \beta \in \mathbb{C}$. Further, by the same Proposition, we have

$$\det\left(\frac{m}{n}I - \phi_l\right) = \frac{1}{n^2}\det(m - n\phi_l) = \frac{1}{n^2}\deg(m - n\phi) \geq 0$$

for any $\frac{m}{n} \in \mathbb{Q}$. Since a monic quadratic with two distinct real roots must take on negative values, it follows that the roots α and β of $\xi(T)$ are either equal or complex conjugates. (This, at last, is the reason we did not need to consider the possibility of $\sqrt{q}$ and $-\sqrt{q}$ in §1.2.) In either case, $|\alpha| = |\beta|$. But

$$\alpha\beta = \det \phi_l = \deg \phi = q,$$

so

$$|\alpha| = |\beta| = \sqrt{q}. \qquad (*)$$

Now the eigenvalues of ϕ_l^r are exactly the rth powers of the eigenvalues of

ϕ_l, so the characteristic polynomial of ϕ_l^r must be

$$\det(TI - \phi_l^r) = (T - \alpha^r)(T - \beta^r)$$

Combining this with our observation about $V(K_r)$, we get

$$\begin{aligned} \#V(K_r) = N_r &= \deg(1 - \phi^r) \\ &= \det(1 - \phi_l^r) \\ &= 1 - \alpha^r - \beta^r + q^r. \end{aligned}$$

With this information, we can verify the Weil conjectures for V.

Theorem. (Weil conjectures, elliptic case) *If V/K is an elliptic curve where $|K| = q$, there is an $\alpha \in \mathbb{Z}$ such that*

1. $$Z_{V/K}(T) = \frac{1 - aT + qT^2}{(1 - T)(1 - qT)};$$

2. $$Z_{V/K}\left(\frac{1}{qT}\right) = Z_{V/K}(T);$$

3. $$1 - aT + qT^2 = (1 - \alpha T)(1 - \beta T)$$

   where $|\alpha| = |\beta| = \sqrt{q}$.

Proof. 1. We have

$$\begin{aligned}\log Z_{V/K}(T) &= \sum_{r=1}^{\infty} \frac{N_r}{r} T^r \\ &= \sum_{r=1}^{\infty} \frac{1-\alpha^r-\beta^r+q^r}{r} T^r \\ &= \sum_{r=1}^{\infty} \frac{T^r}{r} - \sum_{r=1}^{\infty} \frac{(\alpha T)^r}{r} - \sum_{r=1}^{\infty} \frac{(\beta T)^r}{r} + \sum_{r=1}^{\infty} \frac{(qT)^r}{r} \\ &= -\log(1-T) + \log(1-\alpha T) + \log(1-\beta T) - \log(1-qT),\end{aligned}$$

giving

$$\begin{aligned}Z_{V/K}(T) &= \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)} \\ &= \frac{1-aT+qT^2}{(1-T)(1-qT)}\end{aligned}$$

where $a = \alpha + \beta = \mathrm{tr}(\phi_l) = 1 + q - \deg(1-\phi) \in \mathbb{Z}$, as required.

2. We have

$$\begin{aligned}Z_{V/K}\left(\frac{1}{qT}\right) &= \frac{(1-\frac{\alpha}{qT})(1-\frac{\beta}{qT})}{(1-\frac{1}{qT})(1-\frac{1}{T})} \\ &= \frac{(\alpha-qT)(\beta-qT)}{(1-qT)(q-qT)} \\ &= \left(\frac{\alpha\beta}{q}\right) \frac{(1-\frac{q}{\alpha}T)(1-\frac{q}{\beta}T)}{(1-qT)(1-T)} \\ &= \left(\frac{q}{q}\right) \frac{(1-\beta T)(1-\alpha T)}{(1-qT)(1-T)} = Z_{V/K}(T),\end{aligned}$$

since $\alpha\beta = q$.

3. This follows from (*) and part 1 above.

□

Bibliography

[1] A. Weil. "Numbers of solutions of equations in finite fields." Bull. Amer. Math. Soc. **55**, (1949), 497–508.

[2] A. Weil. "Sur les courbes algébriques et les variétés qui s'en déduisent." Act. Sci. Ind. no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945), Hermann et Cie., Paris, 1948.

[3] A. Weil. "Variétés abéliennes et courbes algébriques." Act. Sci. Ind. no. 1064 = Publ. Inst. Math. Univ. Strasbourg **8** (1946), Hermann et Cie., Paris, 1948.

[4] Dwork, Bernard. "On the rationality of the zeta function of an algebraic variety." Amer. J. Math. **82** (1960), 631–648.

[5] A. Grothendieck. "Formule de Lefschetz et rationalité des fonctions L." Séminaire Bourbaki **279**, Secréteriat Mathématique, Paris, 1965.

[6] P. Deligne. "La conjecture de Weil: I." Inst. Hautes tudes Sci. Publ. Math. **43** (1974), 273–307.

[7] R. Bott and L. W. Tu. "Differential forms in algebraic topology." Graduate Texts in Mathematics **82**, Springer-Verlag, New York-Berlin, 1982.

[8] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 1986.