Concerning André Weil's 1949 paper

Alexander Russell Perlis

Submitted 20 May 1997 to the faculty of the Department of Mathematics of The University of Arizona in partial fulfillment of the written preliminary examination.

Here follows an expository introduction to the conjectures stated by André Weil in 1949. The intended audience comprises non-specialists, and the goal is to stimulate further interest in this topic.

Consider $y^2 = x^3 - 1$ modulo some fixed prime p, say $p = 7$, count the solutions over the finite field $\mathbf{F}_p$, and furthermore do the same over each finite-degree extension of $\mathbf{F}_p$. Counting the point at infinity, there turn out to be 4 solutions over $\mathbf{F}_7$, 48 solutions over $\mathbf{F}_{7^2}$, 364 solutions over $\mathbf{F}_{7^3}$, 2496 solutions over $\mathbf{F}_{7^4}$, ...

Now switch to the complex numbers: the solutions to $y^2 = x^3 - 1$ compose an elliptic curve; attached to the underlying topological space is certain data, namely Betti numbers, and since we are talking about a torus in the present example, those numbers are 1, 2, and 1.

Question: *What is the connection between the counting data obtained over finite fields and the topological data obtained over the complex numbers?*

Answer: *If you organize the counting data into a certain power series and exponentiate, then the resulting "zeta function" turns out to be a rational function, whose factors are in one-to-one correspondence, in a certain way, with the Betti numbers; precisely, the degrees of factors in the numerator correspond to the even Betti numbers, and the degrees of factors in the denominator correspond to the odd Betti numbers.*

In the present example, the zeta function is

$$Z(U) = \text{EXP}\left(\frac{4U}{1} + \frac{48U^2}{2} + \frac{364U^3}{3} + \frac{2496U^4}{4} + \cdots\right),$$

which turns out to be the rational function

$$Z(U) = \frac{(1 - 4U + 7U^2)}{(1 - U)(1 - 7U)}.$$

In his 1949 paper, *Numbers of solutions of equations in finite fields*, André Weil does two things: he demonstrates a technique for counting solutions to equations over finite fields, and he states certain conjectures, among them the connection between counting data and topological data given above. The period 1949–73 saw the proof of each of these so-called "Weil conjectures", with many important mathematical developments along the way; in particular, Pierre Deligne's proof of the last remaining conjecture used "étale cohomology" (and its specialization, the "ℓ-adic cohomology"), which was developed by Michael Artin and Alexander Grothendieck (among others) with the settling of the Weil conjectures in mind.

There are two parts to Weil's paper: the demonstration of a technique for counting solutions to certain equations over finite fields, and the stating of the Weil conjectures (which concern more than the particular equations handled in the first part). Except that the former lends evidence to the latter, the two parts are independent: some readers may wish to learn how to count solutions to equations over finite fields without being interested in the Weil conjectures, while other readers may wish to understand the conjectures without knowing Weil's counting technique, and the point is that each option is a viable one. (Of course, why not do both?)

Weil's counting technique concerns equations of the form

$$a_0 x_0^{n_0} + a_1 x_1^{n_1} + \cdots + a_r x_r^{n_r} = b, \qquad (*)$$

which might be called "diagonal" to draw attention to the fact that the variables appear once each and separated from one another. One easily (but tediously) counts solutions to $(*)$ over the finite field $\mathbf{F}_p$ by checking all possibilities. Weil provides a more elegant technique; in fact, he does more. To lend evidence to his conjectures, Weil ultimately wishes to compute the zeta function; this requires knowing the number of solutions to $(*)$ simultaneously over each finite-degree extension of $\mathbf{F}_p$, and furthermore requires that the formulas involved be manageable when it comes time to showing that the zeta function is indeed rational. Weil's counting technique provides the necessary formulas.

Here follows a brief sketch of his technique. He starts with an arbitrary finite field $\mathbf{F}_q$, and expresses the number of solutions to $(*)$ over that field in terms of certain character sums. These sums are simplified slightly, and then expressed in terms of Jacobi sums. The Jacobi sums, in turn, are expressed in terms of Gauss sums. At this point, one has a nice formula for counting solutions to $(*)$ over $\mathbf{F}_q$; in particular, by precomputing all possible Gauss sums (there are only $q - 1$ of them), one may quickly count solutions to lots of different equations of the form $(*)$. Since q was arbitrary, one now knows the number of solutions to $(*)$ over each finite-degree extension of a fixed finite field; but, the formulas are not yet related in a useful way. Remember, at this point everything is expressed in terms of Gauss sums, and here a theorem of Hasse–Davenport does the trick: it establishes the necessary relationship between the Gauss sums obtained over a particular finite field and the Gauss sums obtained over each extension of that field. (An elegant proof of Hasse–Davenport is included in Weil's paper.)

For complete details of Weil's technique, see my separate† account (attached).

Now for the zeta function. Fix a finite field $\mathbf{F}_q$ and an equation of the form $(*)$. Let N_ν denote the number of solutions to $(*)$ over the degree ν extension $\mathbf{F}_{q^\nu}$. Let

$$Z(U) = \text{EXP}\left(\sum_{\nu=1}^{\infty} \frac{N_\nu U^\nu}{\nu}\right).$$

To define this so-called "zeta function", we have organized the counting data into a power series, made a minor adjustment, and exponentiated. Weil claims that this zeta function is rational in general, but immediately moves on to counting *projective* solutions to diagonal homogeneous equations

$$a_0 x_0^n + a_1 x_1^n + \cdots + a_r x_r^n = 0, \qquad (**)$$

and shows that the zeta function in this case is indeed rational, in fact of the form

$$Z(U) = \frac{P(U)}{(1-U)(1-qU)(1-q^2U)\cdots(1-q^{r-1}U)},$$

where the polynomial P has a certain degree, say d. Weil next observes that the Betti numbers of the variety defined by $(**)$ over the complex numbers are 1 in each even dimension, d in one of the odd dimensions, and 0 otherwise, and this precisely matches the degrees of the numerator and denominator factors of $Z(U)$. (The particular data given in this paragraph is correct only when the number of variables in $(**)$ is odd. Otherwise the factor $P(U)$ moves to the denominator, and the Betti numbers adjust accordingly.)

Now for the highlight. Start with V an arbitrary (affine or projective) nonsingular variety of dimension m defined over $\mathbf{F}_q$, and let N_ν denote, as before, the number of points on V that are rational over (live in) $\mathbf{F}_{q^\nu}$, and define the zeta functions $Z(U)$ as before. The Weil conjectures are:

- $Z(U)$ is a rational function with factorization
$$Z(U) = \frac{P_1(U)P_3(U)\cdots P_{2m-1}(U)}{P_0(U)P_2(U)\cdots P_{2m}(U)},$$
where $P_0(U) = 1-U$, $P_{2m}(U) = 1-q^m U$, and where each polynomial P_h has integer coefficients, constant term 1, and roots of absolute value $q^{-h/2}$.
- The Euler–Poincaré characteristic χ of V, defined as usual as the self intersection number of the diagonal of $V \times V$, may be calculated as
$$\chi = \sum_{h=0}^{2m} (-1)^h \, \text{DEG}(P_h).$$
- $Z(U)$ has the functional equation:
$$Z(q^{-m}U^{-1}) = \pm q^{\chi \frac{m}{2}} U^\chi Z(U).$$
- If V arose, via reduction modulo a prime, from a nonsingular variety $\overline{V}$ defined over a number field, then the degrees of the polynomials P_h match the topological Betti numbers of $\overline{V}$ (viewed as a variety over the complex numbers).

The portion of the conjecture above concerning the absolute value of the roots is equivalent to the statement that the function $\zeta(s) = Z(q^{-s})$ has poles and zeros precisely when $\text{RE}(s) = \frac{1}{2}h$, where $0 \le h \le 2m$, and is referred to as the "Riemann hypothesis". (In the case that V is a curve, this Riemann hypothesis says that the zeros of ζ occur precisely when $\text{RE}(s) = \frac{1}{2}$.) The functional equation for $Z(U)$ given above is equivalent to

$$\zeta(m-s) = \pm q^{\chi(\frac{m}{2}-s)} \zeta(s),$$

which takes on a familiar appearance when we restrict to genus 1 curves: $\zeta(1-s) = \pm\zeta(s)$.

Finally, some history. Emil Artin (1924) introduced the zeta function, and verified the Riemann hypothesis for a few genus 1 curves. Friedrich Schmidt (1931) showed that the zeta function for curves is rational and has a functional equation. Helmut Hasse (1933) established the Riemann hypothesis for all genus 1 curves. Relying on results from the Italian school (whose rigor was questionable), Weil (1940) sketched a proof of the Riemann hypothesis for arbitrary genus curves. Weil (1946) introduced the necessary rigor with his book *Foundations of Algebraic Geometry*, and then (1948) gave a complete account of his earlier sketch. Until 1949, all results concerned curves; then Weil stated the famous conjectures for arbitrary varieties. Bernard Dwork (1960) used p-adic functional analysis to establish the rationality of the zeta function for arbitrary varieties. Serguei Stepanov (1969) simplified Weil's proof of the Riemann hypothesis for curves, and Enrico Bombieri (1972) further simplified the proof. It was known throughout this time that a cohomology theory with appropriate properties would prove the Weil conjectures. Various theories were attempted by Jean-Pierre Serre, Weil, and others. The ℓ-adic cohomology turned out to be the right one, with the last crucial piece, necessary for the Riemann hypothesis, having been put in place by Deligne (1973).

† I thought carefully about whether to include more details in the present expository account (such as giving the definition of Gauss sums and Jacobi sums), and reached the conclusion that doing so would spill the beans sufficiently so that any successful clean-up job would require a complete account of Weil's technique. Because this would draw too much attention from the important Weil conjectures, I decided to separate that account.