The Weil Conjectures

V Srinivas and Kapil H Paranjape

We attempt an elementary exposition of the Weil conjectures. There are numerous references to articles that have appeared earlier in *Resonance* which the reader might find useful to follow up.

V Srinivas is currently with School of Mathematics, TIFR, Mumbai.

Kapil H Paranjape after spending about a decade at the School of Mathematics, TIFR, Mumbai, and about a year at ISI, Bangalore is currently with the Institute of Mathematical Sciences, Chennai.

Diophantine Equations Modulo p

One of the fundamental problems of number theory is to find integer solutions to a system V of polynomial equations in a number of variables:

$$\begin{aligned} f_1(X_1,\ldots,X_n) &= 0 \\ f_2(X_1,\ldots,X_n) &= 0 \\ &\vdots \\ f_r(X_1,\ldots,X_n) &= 0 \end{aligned}$$

Such problems go under the name *Diophantine problems.* (A famous example is the Fermat problem [7] where one wishes to find solutions of $X_1^n + X_2^n - X_3^n = 0$ in integers for various choices of a positive integer n.) One can also ask for solutions in other rings (i.e. 'number systems') such as solutions involving square roots, cube roots, other algebraic numbers [6], real numbers, complex numbers and so on. A very important theorem called Hilbert's *Nullstellensatz* asserts that if the above system has any solutions at all (i.e. is *consistent*) then it has solutions in complex numbers. However, it is clear that finding integer solutions or indeed even proving their existence is much harder; there is actually a theorem of Matiyasevič that the existence of such solutions cannot be decided by an automated process (= algorithm = computer; see[4])!

As a first step towards finding solutions in integers, Gauss introduced the method of *working modulo a prime number* p. That is, we find substitutions $X_i \mapsto a_i$ for the variables

$X_1, \ldots, X_n$ so that the values of $f_1, \ldots, f_r$ become divisible by p; note that 0 *is* divisible by p. Now there is no need to distinguish those substitutions (a_i) and (b_i) which differ by multiples of p (i. e. $a_i - b_i = c_i p$) since this will not affect the divisibility of the values of f_j. Thus, we consider solutions in $\mathbb{F}_p$, the *field* of integers modulo p (see *Box* 1).

Now we have only finitely many values to substitute and check for the existence of solutions in $\mathbb{F}_p$. Consider the equation $3X^2 - Y^2 + 2 = 0$. By substitution of *all* possible values for X and Y from $\mathbb{F}_3$ we see that this equation has no solutions in $\mathbb{F}_3$; hence it has no solutions among integers either! On the other hand, the reader should be aware that there may be solutions modulo p without corresponding integer solutions. As an example we consider the equation $X^5 + Y^5 - Z^5 = 0$ which acquires a solution $(1, 1, -1)$ in the field $\mathbb{F}_3$ but has no solutions in integers of the form (a, b, c) with a, b, c all non-zero.

Zeta Function of V

One way of looking at an integer solution to a system V of polynomial equations is to think of it as a real or complex solution which *just happens* to be an integer solution! Similarly, in order to solve equations in a field such as $\mathbb{F}_p$ it is useful examine all solutions in a *larger* field and then (somehow) pick those which are actually in $\mathbb{F}_p$.

Box 1. Finite fields

The field $\mathbb{F}_p$ can be thought of as follows. We consider the collection of integers $\{0, \ldots, (p-1)\}$. We perform addition and multiplication in this collection by following the usual addition and multiplication operations by taking the remainder of division by p. One interesting result is that subtraction and division by non-zero elements becomes possible. Thus $\mathbb{F}_p$ is an example of a finite field.

Finite fields were first studied extensively by Galois. He showed that all finite fields are characterised by their size q which is a power p^a of a prime number p. The (unique) field with q elements is then denoted by $\mathbb{F}_q$. If $\mathbb{F}_q$ is contained in $\mathbb{F}_{q'}$ then q' is a power q^b of q; moreover, one can show that $x \mapsto x^q$ preserves the addition(!) and multiplication operations in $\mathbb{F}_q$. Now a generalisation of Fermat's little theorem is the statement that $x^q = x$ for an element of $\mathbb{F}_q'$ *precisely* when x is actually in $\mathbb{F}_q$.

A version of Hilbert's Nullstellensatz assures us that if the above system V has a solution in a field containing $\mathbb{F}_p$ then it has a solution in a *finite field* $\mathbb{F}_q$ containing $\mathbb{F}_p$. The *Frobenius* mapping $F : \mathbb{F}_q \to \mathbb{F}_q$ (see *Box* 1) takes solutions $(a_1, \ldots, a_n)$ of V into other solutions; moreover a solution is fixed (i. e. $F(a_i) = a_i$) *precisely* when it is a solution in $\mathbb{F}_p$. Thus we are led to the study of the sequence of numbers $a_k = \#(V(\mathbb{F}_q))$; the number of solutions of V in the field $\mathbb{F}_q$ where $q = p^k$.

The next step is a bewildering one for those (such as the authors) not sufficiently well indoctrinated in the philosophy of *generating functions*. It suffices to say that through the study of a generating function it is easier to study the *entire* sequence $\{a_n\}$ than it is to study the individual elements of it.

Motivated by these ideas and analogies with the Riemann Zeta function, Hasse and Weil introduced the function

$$\zeta_V(s) = \exp\left(\sum_{k=1}^{\infty}(a_k p^{-ks})/k\right)$$

called the Hasse–Weil Zeta function; here exp denotes the usual exponential function $\exp(x) = e^x = \sum_{i=0}^{\infty} x^i/i!$. Since the number p is a prime that will be fixed for the rest of the discussion it is less cumbersome to discuss

$$Z_V(t) = \exp\left(\sum_{k=1}^{\infty}(a_k t^k)/k\right),$$

so that $\zeta_V(s) = Z_V(p^{-s})$.

Each system V represents an *affine algebraic variety*. When the equations are homogeneous, a constant multiple of a solution is again a solution; zero is also a common solution for these equations. Thus we can examine the associated *projective algebraic variety* W by examining the sequence of integers $b_k = (a_k - 1)/(p^k - 1)$ and the associated function

$$Z_W(t) = \exp\left(\sum_{k=1}^{\infty}(b_k t^k)/k\right)$$

When we speak of the zeta function of an affine or projective variety, this is what we mean.

Topology of Algebraic Varieties

As mentioned above the system of equations V has 'enough' solutions over the complex numbers. We now digress to examine the geometry of this solution set $V(\mathbb{C})$ and present the geometrical part of Weil's motivation.

$V(\mathbb{C})$ is called the *complex analytic variety* and each individual solution, a point of the variety. An algebraic condition (the Jacobian criterion) allows us to predict the existence (or lack thereof) of singularities ('kinks') in this complex variety. When there are no singularities we say the variety is *smooth*. Since the Jacobian criterion is algebraic, one can even check it for solutions over finite fields (where there is apparently no 'geometry' which leads us to this notion). Thus V is said to be smooth over $\mathbb{F}_p$ if the Jacobian criterion is satisfied at every solution in $\mathbb{F}_q$ for some q.

We now restrict ourselves to the case of homogeneous equations and to the associated projective variety W by ignoring the zero solution and identifying solutions that are multiples of each other.

Returning to the geometrical case, one shows that the smoothness of the variety W makes $W(\mathbb{C})$ a *manifold* (see [2]) of dimension $2d_W$; where d_W is an algebraically defined number called the dimension of W. Again, we note that we have a notion of dimension even when we are examining the solutions over $\mathbb{F}_q$!

Poincaré, Alexandroff, E Noether and others have defined the *homology groups* $H_i(W(\mathbb{C}), \mathbb{Q})$ and an *intersection product*

$$H_i(W(\mathbb{C}), \mathbb{Q}) \times H_{2d_W - i}(W(\mathbb{C}), \mathbb{Q}) \rightarrow \mathbb{Q},$$

so that there is a vector space basis $\{e_{i,k}\}$ of $H_i(W(\mathbb{C}), \mathbb{Q})$ with $e_{i,k} \cdot e_{2d_W - i,k} = 1$, where the $(\cdot)$ denotes the intersection product. The dimension of $H_i(W(\mathbb{C}), \mathbb{Q})$, which is the size of the basis, is called the i-th Betti number of $W(\mathbb{C})$.

Let F be a self-map of W (i. e. F is a way of producing new solutions from old ones). Lefschetz proved the following beautiful formula for the number $L(F)$ of fixed points of F *counted properly*; $L(F)$ is called the Lefschetz number.

$$L(F) = \sum_{i=1}^{2d_W} (-1)^i \left(\sum_k F(e_{i,k}) \cdot e_{2d_W - i,k} \right).$$

When F is the identity we obtain $L(F) = \chi(W(\mathbb{C}))$ the Euler characteristic of $W(\mathbb{C})$ (see [3] and [1]).

Weil looked at this circle of ideas and said '*if only*'. If only these geometrical ideas can be extended to the study of the solutions over a finite field, then we can use Lefschetz formula to count the number of solutions over $\mathbb{F}_p$ since these are *precisely* the fixed points of the Frobenius map. Of course, this map is only for solutions in a finite field and has no analogue for $W(\mathbb{C})$ but while making conjectures such 'minor' difficulties should be ignored!

The Weil Conjectures

We first state the conjectures.

1. Rationality

The Hasse–Weil Zeta function is a rational function,

$$Z_W(t) = \frac{P(t)}{Q(t)}.$$

where $P(t)$ and $Q(t)$ are polynomials with integer coefficients and constant term 1.

2. Functional Equation

When W is a *smooth* projective variety,

$$Z_W\left(\frac{1}{q^{d_W} t}\right) = (-q^{d_W/2})^{\chi} Z_W(t),$$

where χ is the Euler characteristic of W as above.

3. Factorisation

When W is a *smooth* projective variety this conjecture refines the above two.

$$Z_W(t) = \frac{P_1(t)\ldots P_{2d_W-1}(t)}{P_0(t)\ldots P_{2d_W}(t)},$$

where $P_i(t)$ are polynomials with integer coefficients and constant term 1, $P_0(t) = 1 - t$ and

$$P_i\left(\frac{1}{q^{d_W}t}\right) = \left(\frac{-1}{tq^{d_W-1/2}}\right)^{b_i} P_{2d_W-i}(t).$$

Here b_i is the degree of P_i and is to be equal to the i-th Betti number of W as above.

4. Weil's Riemann Hypothesis

If α is a complex number so that $P_i(\alpha) = 0$, then $|\alpha| = q^{-i/2}$. Note that it follows from this that the $P_i(t)$ have no common factors (since they have no roots in common) and so the factorisation is unique!

Historical Remarks

The Weil conjectures are stated in a paper in 1949. He had earlier proved these conjectures for the case of curves ($d_V = 1$) and Abelian varieties by extending earlier results of Artin, Hasse and others. This paper contains a proof for the case of a single homogeneous equation of the form $\sum_i a_i X_i^r$. Weil's computation for this case generalises one made by Hardy and Littlewood for the case $a_i = 1$ in their paper on the Waring problem.

The rationality of the zeta function was first proved by Dwork in 1960. All the conjectures except Weil's Riemann hypothesis follow in a 'formal' way from the existence of a suitable theory of homology groups so that the Lefschetz formula can be applied. One such theory was Grothendieck's *étale* theory developed by him in collaboration with M Artin and others. Another such theory is Grothendieck's *crystalline* cohomology. From this Grothendieck was able to

prove all the conjectures (except Weil's Riemann hypothesis) in a more general setting than the one described in the article. Under the above restricted context an independent proof was given by Lubkin in 1968.

Weil's Riemann hypothesis was first proved by Deligne in 1973 by developing another topological idea of Lefschetz (called the weak Lefschetz theorem) in the context of the étale theory of Grothendieck. Deligne gave a second proof in 1980 which is perhaps more number theoretic. In the process of this proof the second part of Lefschetz topological work (the hard Lefschetz theorem) was shown in the étale context.

The Weil conjectures form the keystone to the further study of the topological and number-theoretical properties of varieties *in tandem*. In 1969 Grothendieck proposed a vast program going under the title *Motives*. He set out some *standard conjectures* which would prove Weil's Riemann hypothesis and much much more. Though Grothendieck's student Deligne proved the Weil conjectures, the standard conjectures are as yet unresolved and the grand program of Grothendieck is yet to be completed. Truly, has Grothendieck seen further by standing on the shoulders of the giant Weil?

Acknowledgements

This article is based on an earlier article by V Srinivas [5] that appeared in a special issue of *Current Science* which was devoted to algebraic geometry. The original article has been tuned by Kapil Paranjape in order that it may *resonate* with our readers – any wrong notes and off-beats can thus be blamed on the latter. Kapil Paranjape also fondly remembers the first lecture on the Weil conjectures given to him by V Srinivas in the IIT Kanpur aerodrome while a storm raged outside for about four hours and the IIT Jazz band had a practice session!

Suggested Reading

[1] **Subhashis Nag, On the Shapes of Algebraic Loci, *Resonance*, Vol. 2, No. 7, July 1996.**

[2] **Kapil H Paranjape, Geometry, *Resonance*, Vol. 1, No. 6, June 1996.**

[3] **Vishwambhar Pati, The Punctured Plane, *Resonance*, Vol. 1, No. 4, April 1996.**

[4] **R K Shyamsundar, Universality and Incomputability, *Resonance*, Vol. 2, No. 10, October 1997.**

[5] **V Srinivas, The Weil Conjectures, *Current Science*, Vol. 63, No. 5, 10 September 1992.**

[6] **Rajat Tandon, The Class Number Problem, *Resonance*, Vol. 3, Nos. 6 and 7, June–July 1998.**

[7] **C S Yogananda, Fermat's Last Theorem, *Resonance*, Vol. 1, No. 1, January 1996.**

Address for Correspondence
V Srinivas
School of Mathematics
Tata Institute of Fundamental Research, Homi Bhabha Road
Mumbai 400 005, India.
Email:srinivas@math.tifr.res.in

Kapil H Paranjape
The Institute of Mathematical Sciences, CIT Campus
Taramani P.O.
Chennai 600 113, India.
Email: kapil@imsc.ernet.in