By the Riemann inequality the latter spaces keep on growing in dimension and eventually, for $n \gg 0$ the space $l(D+no)$ has dimension n. We can also vary D by adding divisors D' of the following form. For some point p of X we can consider the divisor which has $a_p = -1$ and $a_o = 1$, $a_q = 0$ for all points X other than o and p. By doing this many times we have an infinite parameter variation of the data.

The space $E(D)$ can be identified with a subspace of $k((T))$. This lies in the class of subspaces V with the property that for all m sufficiently large there are exactly m linearly independent Laurent series in V of the form

$$f(T) = a_{-m} T^{-m} + a_{-m+1} T^{-m+1} + \cdots.$$

The collections of all such spaces forms the *infinite Grassmannian*. Replacing D by $D+D'$ gives another such subspace. As D' approaches the trivial divisor this gives an infinitesimal action. This infinitesimal action is the iso-spectral flow. We note here that in the case of rank 1 the integral manifold of this flow is the Jacobian of the curve X.

The infinite Grassmannian and the associated group action is a purely combinatorial construction, involving the symmetric functions and associated polynomials. Since all *pointed* Riemann surfaces occur on the infinite Grassmannian we can now attempt to study the collections of all curves in a purely combinatorial fashion.

5. Further reading and references

A much more complete historical sketch of the theory of Riemann surfaces (and algebraic geometry in general) may be found in the book: Shafarevich, I. R., *Basic Algebraic Geometry*, Springer–Verlag, Berlin, 1977. This book also contains more details about sections 3.2 and 4.1.

For the formalism of Lax operators (section 2.1) and their use in solving the iso-spectral problem (section 2.2) we have followed the exposition of: Motohico Mulase, *J. Diff. Geom.*, 1984, **19**, 403–430. Much of the formalism comes from the original papers of Burchnall and Chaundy.

The definition of Riemann surfaces arising out of one variable function theory (section 3.1) can be studied from chapter 8 of the book: Lars Ahlfors, *Complex Analysis*, McGraw-Hill Kogakusha, International student edition, 2nd edition, 1966.

The geometry of projective curves is a well-developed subject and the book (Arabarello, E., Cornalba, M., Griffiths, P. A. and Harris, J., *Grundlehr. Math. Wiss.*, 1985, 267) covers all the unproved assertions of section 4.1 and much more. Section 4.2 is adapted from a Hilbert space approach of Segal and Wilson: Wilson, G., in *Geometry Today*, Proceedings of Giornata di Geometria, Rome 1984, Birkhäuser, Boston, 1985.

The Weil conjectures

V. Srinivas

School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Bombay 400 005, India

1. Diophantine equations

In number theory, one of the problems of basic interest is to find all integer solutions of an equation

$$f(X_1, \ldots, X_n) = 0,$$

where f is a polynomial with integer coefficients; such problems are known as *Diophantine problems*. It is also of interest to study systems of such equations, and to consider algebraic integer solutions (for example, solutions with $X_i = \Sigma_j a_{ij} \zeta^j$, where ζ is a primitive nth root of unity, and the a_{ij} are integers).

As a first step, one may instead look for integers X_i such that $f(X_1, \ldots, X_n)$ is *divisible by a given prime number p*. Since 0 is divisible by p, this is certainly an 'easier' problem to solve, in the sense that if it has no solution, neither does the original Diophantine problem.

Equivalently, one considers $\mathbf{F}_p$, the *integers modulo p*; one description of these is as follows—$\mathbf{F}_p = \{0, 1, \cdots, p-1\}$, where we define the sum of two such numbers to be the remainder obtained on dividing their sum (as integers) by p. Their product is similarly defined as the remainder obtained on dividing the integer product by p. These modified operations produce a *field*, i.e. an algebraic system in which one can perform the usual operations of addition, multiplication and division by non-zero elements, and these operations have the standard properties. This is an example of a finite field. There is a mapping $\mathbf{Z} \to \mathbf{F}_p$ (called 'reduction modulo p') which associates to each integer the

remainder on dividing it by p. Similarly, a polynomial f (or system of polynomials) yields a polynomial $\bar{f}$ (or system) with coefficients in $\mathbf{F}_p$. Now our problem of finding values of f which are divisible by p is equivalent to solving the equation $\bar{f}(x_1, \ldots, x_n)=0$ for x_i in $\mathbf{F}_p$.

For example, consider the Diophantine equations $3x^2-y^2+2=0$, and $7x^3-y^3+2=0$. We see by simple computations that the first equation has no solution over $\mathbf{F}_3$, the integers modulo 3, while the second equation has no solution in $\mathbf{F}_7$. Hence neither equation has integer solutions. A more complicated example is the following. Consider the equation $x^2+y^2-a=0$, where a is a given integer; in simple language, we are asking if a is a sum of two squares. Let p be an odd prime; the corresponding equation over $\mathbf{F}_p$ is $x^2+y^2-\bar{a}=0$, where $\bar{a}\in\mathbf{F}_p$ is the image of $a\in\mathbf{Z}$. Write the equation as $x^2-\bar{a}=-y^2$. Let $A\subset\mathbf{F}_p$ denote the set of possible values of $x^2-\bar{a}$, and $B\subset\mathbf{F}_p$ the set of possible values of $-y^2$; then one sees easily that A, B each have exactly $(p+1)/2$ elements. Since $\mathbf{F}_p$ has p elements, the two sets A, B must have a non-trivial intersection. Hence the equation $x^2+y^2-\bar{a}=0$ always has a solution in $\mathbf{F}_p$. The situation for the original Diophantine equation is much more complicated. The odd prime numbers are all of the form $4q+1$ or $4q+3$ for suitable q; for example, 5, 13, 17 are of the form $4q+1$, while 3, 7, 11 are of the form $4q+3$. One can show the equation $x^2+y^2=a$ has an integer solution precisely when either $a=0$, or $a>0$, and any prime factor p of a, where $p=4q+3$, divides a to an *even* power. The key step here is Fermat's *two square theorem*, that any prime $p=4q+1$ is a sum of two squares.

In a similar fashion, the first approximations to solving problems over rings of algebraic integers are analogous problems over finite fields.

An excellent introduction to theory of polynomial equations over finite fields, assuming a minimal background, is given by Ireland and Rosen[1].

2. Finite fields

We first recall a few facts about finite fields, which may help the uninitiated reader. First, any finite field k contains one of the fields $\mathbf{F}_p$, for some prime p. Then for every $x\in k$, we have

$$px=x+x+\cdots+x \text{ (with } p \text{ terms)}=0.$$

We express this by saying that k has *characteristic* p (in contrast, a field containing the field $\mathbf{Q}$ of rational numbers is said to be of characteristic 0). Then k is a finite dimensional vector space over $\mathbf{F}_p$. If k has dimension n as an $\mathbf{F}_p$-vector space, and $v_1, \ldots, v_n$ is a basis, then any element of k is uniquely expressible as $\Sigma_i a_i v_i$ with $a_i\in\mathbf{F}_p$. There are p choices for each a_i, so k must have $q=p^n$ elements. The non-zero elements of k thus form a multiplicative group of p^n-1 elements. An elementary theorem in group theory now implies that any non-zero x in k satisfies $x^{p^n-1}=1$. Hence the elements of k are precisely the roots of the polynomial $x^{p^n}-x$. This forces any two finite fields with p^n elements to be *isomorphic*, i.e. there is essentially only *one* field $\mathbf{F}_{p^n}$ with p^n elements. Further, if $q=p^n$, the finite field $\mathbf{F}_q$ is contained in each of the fields $\mathbf{F}_{q^m}$, $m\geq 1$, and no others.

Another important property of finite fields k of characteristic p is the *Frobenius mapping* $F: k\to k$, $F(x)=x^p$. This clearly satisfies $F(xy)=F(x)F(y)$; miraculously, it also satisfies $F(x+y)=F(x)+F(y)$ (this follows from the fact that the binomial coefficients $\binom{p}{r}$, with $0<r<p$, are all divisible by p). One can also consider the powers of F. If k contains $\mathbf{F}_{p^n}$, then the subfield $\mathbf{F}_{p^n}$ is precisely the set of elements of k fixed by the n-fold composition $F^n=F\circ F\circ\cdots\circ F$. This is just a restatement of the fact that the elements of $\mathbf{F}_{p^n}$ are precisely the roots of $x^{p^n}-x=0$.

Let $\mathbf{F}_q$ be the finite field with q elements, and consider a system of polynomial equations.

$$\left.\begin{aligned} f_1(X_1,\ldots,X_d)&=0\\ &\vdots\\ f_k(X_1,\ldots,X_d)&=0 \end{aligned}\right\} \quad \cdots \qquad (*)$$

where the f_i have coefficients in $\mathbf{F}_q$.

Problem: How many solutions does the system (*) have with $X_1\in\mathbf{F}_q$?

Even for equations in 1 variable, there is no simple answer (for example, consider the equation $X^n=a$). However, it turns out that a more reasonable problem is the following:

Problem': Let

a_n = the number of solutions of the system (*) with $X_i\in\mathbf{F}_{q^n}$.

Find 'good properties' of the *sequence* $a_1, a_2, \ldots, a_n, \cdots$

The 'good properties' of the sequence a_n are given by the *Weil conjectures*. These are stated in terms of the zeta function, which we now discuss.

3. Zeta functions

We define the *zeta function* of the system (*) to be the formal power series

$$Z(t)=\exp\left(\sum_{n=1}^{\infty} a_n \frac{t^n}{n}\right).$$

This 'encodes' the whole collection of numbers $\{a_1, a_2, \ldots, a_n, \ldots\}$.

One may ask

(i) isn't it more natural to consider instead the 'usual' generating function

$$f(t) = \sum_{n=1}^{\infty} a_n t^n$$

(which is essentially the logarithmic derivative of $Z(t)$)? (ii) why should $Z(t)$ be called a 'zeta function'?

To understand why the zeta function defined above is the 'correct' one, we recall first the definition of the famous *Riemann zeta function*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \text{ where } \mathscr{R}S > 1.$$

By a theorem of Euler, this can be rewritten as

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

Euler's formula is essentially equivalent to the unique factorization of positive integers into products of prime numbers. Riemann showed that this function can be analytically continued to **C** with 1 singularity, a pole at $s=1$, and satisfies a functional equation (where $\Gamma(s)$ is the gamma function)

$$\zeta(1-s) = \frac{\pi^{\frac{1}{2}-s}\,\Gamma\left(\frac{s}{2}\right)}{\Gamma\left(\frac{1-s}{2}\right)}\zeta(s).$$

The famous *Riemann hypothesis*, which is still unproved, is the assertion that all zeroes of this function in the half plane $\mathscr{R}s>0$ lie on the line $\mathscr{R}s=1/2$.

From the standpoint of algebra, prime numbers are just the generators of maximal ideals in the ring of integers. A *ring* is, roughly speaking, a system in which we can perform operations analogous to addition. subtraction and multiplication, but division may not be possible; an *ideal* is a subset I which is closed under addition, and under multiplication by any element of the ring—for example, the integers **Z** form a ring, and the multiples of a fixed integer n form an ideal, denoted by (n); these are the only possible ideals in **Z**. An ideal (n) contains (m) precisely if n divides m; hence maximal ideals (ideals $I \neq \mathbf{Z}$ not contained in any larger such ideals) correspond to prime numbers.

Another example of a ring is $k[X_1,\ldots,X_n]$, the k-algebra of polynomials in $X_1,\ldots,X_n$ with coefficients in k. Any ideal I in $k[X_1,\ldots,X_n]$ is finitely generated, i.e. there exist polynomials $f_1,\ldots,f_r$ such that I consists of all polynomials expressible in the form $a_1f_1+\cdots a_rf_r$, where $a_1,\ldots,a_r$ are arbitrary polynomials; this is called the ideal generated by $f_1,\ldots,f_r$, and denoted $(f_1,\ldots,f_n)$. This finite generation theorem is the *Hilbert basis theorem.*

Analogous to the integers modulo n, one can form the quotient ring of the polynomial ring modulo an ideal I—here two polynomials are considered equivalent if their difference lies in I, and the defining properties of an ideal ensure that addition and multiplication are well defined on equivalence classes. The polynomials vanishing at a point form a maximal ideal, as one easily sees; conversely, if the coefficient field k is *algebraically closed*, then any maximal ideal is the ideal of polynomials vanishing at a point (this assertion is a special case of the famous *Hilbert Nullstellensatz*). By analogy, if k is arbitrary, we may try to regard maximal ideals as 'points' in some sense. If k is finite, then the maximal ideals are precisely those ideals whose quotient ring is a finite field.

Now consider the ring

$$R = \frac{\mathbf{F}_q[X_1,\ldots,X_d]}{(f_1(X_1,\ldots,X_d),\ldots,f_d(X_1,\ldots,X_d))}$$

naturally associated with the system of equations (*). Then one can prove that the zeta function satisfies the product formula

$$Z(t) = \prod_{\mathscr{M} \subset R,\ \mathscr{M} \text{ maximal ideal}} \frac{1}{(1-t^{[R/\mathscr{M}:\mathbf{F}_q]})},$$

where $[R/\mathscr{M}:\mathbf{F}_q]=n$ if card $R/\mathscr{M}=q^n$. Hence if we substitute $t=q^{-s}$, where s is a complex variable, then

$$Z(q^{-s}) = \prod_{\mathscr{M} \subset R,\ \mathscr{M} \text{ maximal ideal}} \frac{1}{(1-(\text{card } R/\mathscr{M})^{-s})}.$$

This is analogous to Euler's product formula for the Riemann zeta function,

$$\zeta(s) = \prod_{\mathscr{M} \subset \mathbf{Z},\ \mathscr{M} \text{ maximal ideal}} \frac{1}{(1-(\text{card } \mathbf{Z}/\mathscr{M})^{-s})}.$$

4. Computing the zeta function: some examples

Example 1: Consider the 'empty' system of equations in d variables; then

$$a_n = \text{card } \mathbf{F}_{q^n}^{\oplus d} = q^{nd},$$

$$R = \mathbf{F}_q[X_1,\ldots,X_d],$$

and so

$$Z(t) = \exp\left(\sum_{n=1}^{\infty} \frac{q^{nd}t^n}{n}\right) = \exp\left(\sum_{n=1}^{\infty} \frac{(q^dt)^n}{n}\right)$$

$$= \frac{1}{1-q^dt}.$$

Now a system of equations (*) defines an *affine algebraic variety* over the field $\mathbf{F}_q$ (see Mohan Kumar's accompanying article, page 218). The $\mathbf{F}_q$-algebra we associated to (*) is then the ring of polynomial functions (or *regular functions*) on this variety.

More generally, one can define an 'abstract' algebraic variety over a field k as something obtained by 'patching' together open subsets which are affine algebraic varieties over k (examples are given by *projective varieties*, discussed in my accompanying article, page 222). In particular, for $k=\mathbf{F}_q$, it makes sense to speak of the zeta function $Z_X(t)$ of a variety X defined over $\mathbf{F}_q$,

$$Z_X(t)=\exp\left(\sum_{n=1}^{\infty} a_n(X)\frac{t^n}{n}\right),$$

where

$a_n(X)$ = number of '$\mathbf{F}_q$-valued points' of X.

Then example 1 above corresponds to the case $X=\mathbf{A}^d_{\mathbf{F}_q}$, the *affine space* over $\mathbf{F}_q$. Clearly, if

$$X=\coprod_{i=1}^{r} X_i$$

is a disjoint union of subvarieties defined over $\mathbf{F}_q$, then

$$a_n(X)=\sum_{i=1}^{r} a_n(X_i),$$

$$Z_X(t)=\prod_{i=1}^{r} Z_{X_i}(t).$$

Example 2. Let $\mathbf{P}^d_{\mathbf{F}_q}$ be the projective d-space over $\mathbf{F}_q$. Then

$$\mathbf{P}^d_{\mathbf{F}_q}=\mathbf{A}^d_{\mathbf{F}_q}\coprod\mathbf{A}^{d-1}_{\mathbf{F}_q}\coprod\cdots\coprod\mathbf{A}^1_{\mathbf{F}_q}\coprod\mathbf{A}^0_{\mathbf{F}_q},$$

(where $\mathbf{A}^0_{\mathbf{F}_q}$ is a over $\mathbf{F}_q$); hence

$$Z_{\mathbf{P}^d_{\mathbf{F}_q}}(t)=\prod_{i=0}^{d}\frac{1}{1-q^it}.$$

Example 3. Let $X=\mathbf{G}_{\mathbf{F}_q}(k,d)$, the Grassmannian of k-dimensional sub-spaces of a d-dimensional space $\mathbf{A}^d_{\mathbf{F}_q}$ (see my article on Projective algebraic varieties, this issue). Then X has a natural structure as a variety over $\mathbf{F}_q$, and one has a decomposition of X as a disjoint union of affine spaces of various dimensions, the so-called *Schubert cells.*

Let

b_{2i} = (number of Schubert cells $\cong \mathbf{A}^i$).

One knows that $N=k(d-k)$ is the dimension of $\mathbf{G}(k,d)$, and so

$$Z_X(t)=\prod_{i=0}^{N}\frac{1}{(1-q^it)^{b_{2i}}}$$

Over the complex number field $\mathbf{C}$, the analogous Schubert cells give a cell decomposition* of the complex Grassmannian $\mathbf{G}_{\mathbf{C}}(k,d)$ with cells $\mathbf{A}^i_{\mathbf{C}}\cong\mathbf{C}^i\cong\mathbf{R}^{2i}$ only in even dimensions; hence b_{2i} equals the $2i$ th *Betti number* of the complex Grassmannian, from standard theorems in topology.

Since $\mathbf{G}_{\mathbf{C}}(k,d)$ is a compact complex manifold of dimension n, hence a compact, oriented topological manifold of dimension $2n$, the *Poincaré duality theorem* gives that $b_{2i}=b_{2(N-i)}$. Hence:

$$Z_X\left(\frac{1}{q^Nt}\right)=\prod_{i=0}^{N}\frac{1}{\left(1-\frac{1}{q^{N-i}t}\right)^{b_{2i}}}=\prod_{i=0}^{N}\frac{(-q^{N-i}t)^{b_{2i}}}{(1-q^{N-i}t)^{b_{2i}}}$$

$$=(-t)^{\Sigma_i b_{2i}}q^{\Sigma_i(N-i)b_{2i}}\prod_{i=0}^{N}\frac{1}{(1-q^{N-i}t)^{b_{2i}}}.$$

But

(a) $b_{2i}=b_{2(N-i)}$, so that the last product is just $Z_X(t)$

(b) $\Sigma_i(N-i)b_{2i}=1/2(\Sigma_i(N-i)b_{2i}+\Sigma_i i\,b_{2i})=N/2(\Sigma_i b_{2i})$

For any space X with a cell decomposition with finitely many cells, the *topological Euler characteristic is* $\Sigma_i(-1)^i n_i$ where n_i is the number of cells of dimension i; this number is a topological invariant of the space X. This generalizes the familiar *Euler formula* $V-E+F=2$ for any triangulation of the 2-sphere, where V, E, F are the numbers of vertices (=0-cells), edges (=1-cells) and faces (=2-cells).

Hence, if $\chi=\Sigma_i b_{2i}$ is the topological Euler characteristic of the complex Grassmannian, then we have

$$Z_X\left(\frac{1}{q^Nt}\right)=(-q^{N/2}t)^{\chi}Z_X(t).$$

If we write

$$\zeta_X(s)=Z_X(q^{-s})$$

we may rewrite the above as

$$\zeta_X(N-s)=(-q^{N/2-s})^{\chi}\zeta_X(s)$$

i.e. $\zeta_X(s)$ satisfies a *functional equation*, analogous to that satisfied by the Riemann zeta function.

Example 3. Let X be a non-singular projective curve

*A sort of generalized triangulation.

of genus g over $\mathbf{F}_q$. One can show its zeta function has the form

$$Z_X(t) = \frac{P_X(t)}{(1-t)(1-qt)}$$

where $P_X(t)$ has the following properties.

(i) $P_X(t) = t^{2g}q^g + c_1 t^{2g-1} + \cdots + c_{2g-1}t + 1$ for some $c_i \in \mathbf{Z}$

(ii) If α is a root of $P_X(t)=0$, then $1/q\alpha$ is also a root; hence

$$P_X(t) = \prod_{i=1}^{g} (1-(\beta_i + \beta_i^{-1})q^{1/2}t + qt^2)$$

(the roots are the numbers $\beta_i^{\pm 1} q^{-1/2}$; this is equivalent to a functional equation between $Z_X(t)$ and $Z_X(1/qt)$, or equivalently, between $\zeta_X(s)$ and $\zeta_X(1-s)$).

(iii) for any root α of $P_X(t)=0$,

$$|\alpha| = |1/q\alpha| = q^{-1/2}.$$

Thus, the zeroes of $\zeta_X(s)$ lie on the line Re $s=1/2$; equivalently, the quadratic factors $1-(\beta_i+\beta_i^{-1})q^{1/2}t+qt^2$ have *real* coefficients. Note the analogy with the Riemann hypothesis.

5. The Weil conjectures

The Weil conjectures are a generalization of the above properties to arbitrary varieties. We first state the conjectures.

5.1 *The conjectures*

1. (*Rationality*) Let X be an algebraic variety over the finite field $\mathbf{F}_q$. Then the zeta function $Z_X(t)$ is a rational function,

$$Z_X(t) = \frac{P(t)}{Q(t)},$$

with $P(t), Q(t) \in 1 + t\mathbf{Z}[t]$ (i.e. P, Q have constant term 1 and integer coefficients).

2. Suppose X is a non-singular, complete (i.e. 'compact') variety of dimension N over $\mathbf{F}_q$ (for example, X is a non-singular projective variety). Then

(a) (*Functional equation*) $Z_X(t)$ satisfies a functional equation

$$Z_X\left(\frac{1}{q^N t}\right) = (\pm q^{N/2})^{\chi} Z_X(t)$$

for some integer χ (which we may call the 'Euler characteristic' of X);

(b) there is a factorization

$$Z_X(t) = \prod_{i=0}^{2N} P_i(t)^{(-1)^{i+1}} = \frac{P_1(t)P_3(t)\cdots P_{2N-1}(t)}{P_0(t)P_2(t)\cdots P_{2N}(t)}$$

where

(i) $P_i(t) \in 1 + t\mathbf{Z}[t]$
(ii) $P_0(t) = 1-t$, $P_{2N}(t) = 1 - q^N t$

(iii) $P_i\left(\frac{1}{q^N t}\right) = \left(\frac{-1}{tq^{N-i/2}}\right)^{b_i} P_{2N-i}(t)$ where $b_i = \deg P_i = \deg P_{2N-i}$; in particular, b_i is even if i is odd (we may call b_i the 'ith Betti number' of X; this formula implies the functional equation, with $\chi = \Sigma(-1)^i b_i$)

(iv) if α is a root of $P_i(t)=0$, then

$$|\alpha| = q^{-i/2}$$

(this statement is known as *Weil's Riemann hypothesis*); equivalently, $P_i(t)$ has a factorization

$$P_i(t) = \prod_{j=1}^{b_i} (1-\alpha_{ij}t)$$

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

From Weil's Riemann hypothesis, it follows that the factors $P_i(t)$ are pairwise relatively prime over $\mathbf{Z}$, so such a factorization of $Z_X(t)$, if it exists, is unique;

(c) (*Comparison*) If X is obtained by 'reduction modulo p' from a non-singular, complete variety Y in characteristic zero, and $Y_{\mathbf{C}}$ is the corresponding complex variety, then in the factorization of $Z_X(t)$,

$$\deg P_i(t) = b_i(Y_{\mathbf{C}}),$$

where $b_i(Y_{\mathbf{C}})$ denotes the ith Betti number of the complex manifold $Y_{\mathbf{C}}$.

5.2 *Some history*

The Weil conjectures are stated in the paper of Weil[2]; he had earlier proved them for curves and abelian varieties, extending earlier results of Artin, Hasse and others. The paper[2] contains a proof for hypersurfaces of the form $\Sigma a_i X_i^r = 0$ (for a self-contained account of Weil's proof in this case, see the book[1]). Weil's computation generalizes one made by Hardy and Littlewood for the hypersurface defined by $X_1^k + X_2^k + \cdots + X_s^k = 0$ in the course of their solution of the famous Waring problem, using the Hardy Ramanujan *circle method* (the *Waring Problem* is to show that for any positive integer k, every positive integer can be written as a sum of $s(k$-th) powers, for some (sufficiently large) fixed s; for example, every positive integer is a sum of 4 squares, of 9 cubes, of 19 fourth powers, etc.)

The rationality of the zeta function was first proved by Dwork (1960). The rationality and functional equation follow in a 'formal' way from the existence of a 'Weil cohomology theory' (we discuss this below), as was remarked by Weil himself; such a theory is Grothendieck's *étale cohomology*, developed by him along with M. Artin. Another Weil cohomology theory is Grothendieck's *crystalline cohomology*.

Independently, the rationality and functional equation were proved by Lubkin in 1968 for varieties obtained by 'reduction modulo p'.

The Riemann hypothesis was first proved by Deligne in 1973; he gave a second proof, published in 1980, and a third proof using Deligne's 'l-adic Fourier transform' was given by Laumon in 1984 (ref. 3).

A more or less self-contained proof of the Weil conjectures, including Deligne's first proof of the Riemann hypothesis, may be found in the book of Freitag and Kiehl[4]. An expository account of Deligne's first proof, assuming some background, may be found in Katz's article[5]. Dieudonné has given another expository account, giving some history, and assuming less background of the reader (ref. 6); this is reprinted in the book by Freitag and Kiehl[4].

5.3 *An application: the Ramanujan conjecture*

Let

$$f(z)=z\prod_{n=1}^{\infty}(1-z^n)^{24}$$

$$=\sum_{n=1}^{\infty}\tau(n)z^n.$$

The function $\Delta(t)=f(e^{2\pi it})$ is the so-called *elliptic modular function*; the numbers $\tau(n)$ are thus interpreted as its Fourier coefficients. Ramanujan[7] conjectured* in a paper in 1912 that

$$|\tau(p)|\leq 2p^{11/2}$$

for any prime number p. Deligne[8] showed that Ramanujan's conjecture follows from Weil's Riemann hypothesis. In fact, $\Delta(t)$ is an example of a *modular form* for $SL_2(\mathbf{Z})$; there is a generalization of Ramanujan's conjecture to certain other modular forms that was stated by Petersson, which also follows from Weil's Riemann hypothesis.

*In fact what Ramanujan conjectured was that the quadratic polynomial $1+2\tau(p)x+p^{11}x^2$ has roots $p^{-11/2}(\cos\theta\pm i\sin\theta)$, for a *real* angle θ, this polynomial is related to the Euler factor at p of the associated Dirichlet series.

6. Weil cohomology theories

We have already observed that the Weil conjectures seem to have a topological flavour. One can make this more precise, and give them a 'topological' interpretation.

We begin with the property stated earlier that an element a of the algebraic closure $\bar{\mathbf{F}}_q$ of $\mathbf{F}_q$ lies in the subfield $\mathbf{F}_{q^n}$ precisely if it satisfies

$$a^{q^n}=a.$$

Next, if

$$R=\mathbf{F}_q[X_1,\cdots,X_d]/(f_1,\cdots,f_k)\ ,$$

where the f_i have coefficients in $\mathbf{F}_q$, then there is an $\mathbf{F}_q$-algebra mapping

$$F:R\to R,$$

$$a\to a^q,$$

the *Frobenius homomorphism*. To see that F is well defined, note that it is well defined on the polynomial ring $\mathbf{F}_q[X_1,\cdots,X_d]$, and satisfies $F(f_i)=f_i^q$, so maps the ideal $(f_1,\cdots,f_k)$ generated by the f_i into itself. The above definition can be extended to varieties defined over $\mathbf{F}_q$—given such a variety X, there is an algebraic map of varieties $F:X\to X$, the *Frobenius mapping*. It is easy to see that F preserves the set of $\mathbf{F}_{q^n}$-valued points of X; further, a point over the algebraic closure of $\mathbf{F}_q$ has coordinates in $\mathbf{F}_{q^n}$ precisely if it is a *fixed point* of $F^n=F\circ F\circ\cdots\circ F$, the n-fold composite.

Suppose now that Y is a non-singular projective variety over $\mathbf{C}$ of dimension N, and that $f:Y\to Y$ is a map of varieties such that f^n has isolated fixed points for each n. Then we may apply the *Lefschetz fixed point formula* in algebraic topology to compute the number of fixed points of f^n, in terms of the action of the mapping f on the *cohomology groups* of Y.

Let $H^i(Y,C)$ denote the ith cohomology group of Y, which is a finite dimensional vector space over $\mathbf{C}$. Any mapping $f:Y\to Y$ of varieties induces a linear transformation f^* on each of the cohomologies $H^i(Y,\mathbf{C})$, which we may regard as a matrix. From standard properties of cohomology (basically, that it is a 'functor') the matrix representing the action of f^n is the nth power of that representing f.

The Lefschetz formula states that the number of fixed points of f^n is an alternating sum of *traces* of linear transformations (i.e. matrices),

$$\sum_{i=0}^{2N}(-1)^i\,\mathrm{Tr}\,(f^n\,|\,H^i(Y,\mathbf{C})).$$

In particular, this alternating sum, which is *a priori* a complex number, is actually a positive integer. If

$$a_n=\text{number of fixed points of } f^n,$$

then

$$\sum_{n=1}^{\infty} a_n \frac{t^n}{n} = \sum_{n=1}^{\infty} \frac{t^n}{n} \left(\sum_{i=0}^{2N} (-1)^i \operatorname{Tr}(f^n \mid H^i(Y, \mathbf{C})) \right)$$

$$= \sum_{i=0}^{2N} (-1)^i \left(\sum_{n=1}^{\infty} \frac{\operatorname{Tr}(f^n \mid H^i(Y, \mathbf{C}))}{n} t^n \right)$$

Now if V is a vector space of dimension d over $\mathbf{C}$, $A: V \to V$ a linear transformation with eigenvalues $\alpha_1, \ldots, \alpha_d$, then

$$\sum_{n=1}^{\infty} \frac{\operatorname{Tr}(A^n \mid V)}{n} t^n = \sum_{n=1}^{\infty} \frac{\alpha_1^n + \cdots + \alpha_d^n}{n} t^n$$

$$= \log \prod_{j=1}^{d} \frac{1}{1 - \alpha_j t}$$

$$= \log P(A, V; t)^{-1},$$

where

$$P(A, V; t) = \det(I - tA \mid V)$$

is (essentially) the characteristic polynomial of A acting on V (I is the identity transformation).

Hence, the 'zeta function' of the self-map $f: Y \to Y$ satisfies

$$Z(t) = \prod_{i=0}^{2N} (\det(I - ft \mid H^i(Y, \mathbf{C}))^{(-1)^{i+1}}.$$

This is clearly a rational function with complex coefficients; since its Taylor series has rational coefficients, the rational function itself is a ratio of polynomials with rational coefficients.

A *Weil cohomology theory* is a rule which associates to each non-singular projective variety X of dimension N over a finite field $\mathbf{F}_q$ a finite collection of finite dimensional vector spaces $H^i(X)$ over a field K of characteristic zero, such that if $f: X \to X$ is any self-map of X with only a finite number of fixed points (in particular, f is the Frobenius mapping F, or a power of F), then the number of fixed points is given by the Lefschetz fixed point formula. If this is the case, the rationality of the zeta function follows easily (except that the rational function has coefficients in the field K of characteristic zero which forms the 'coefficients' for the cohomology; but this implies the assertion with $\mathbf{Q}$ coefficients, as before).

Suppose further that the cohomology groups satisfy a version of Poincaré duality. This will mean that $H^i(X)$ and $H^{2 \dim X - i}(X)$ have the same dimensions over K, and the matrices associated to the action of F on $H^i(X)$ and $H^{2N-i}(X)$ are (up to appropriate scalars) the transpose inverse of each other. The functional equation then reduces to the fact that if a linear transformation has eigenvalues $\alpha_1, \ldots, \alpha_r$, then its transpose inverse has eigenvalues $\alpha_1^{-1}, \ldots, \alpha_r^{-1}$.

In Grothendieck's étale cohomology, $K = \mathbf{Q}_l$, the field of *l-adic numbers*, where l is a prime number different from p, the characteristic of $\mathbf{F}_q$. All of the above properties hold for étale cohomology, so that the rationality conjecture and the functional equation are valid.

7. Weil's Riemann hypothesis

The Riemann hypothesis does not seem to be 'purely topological'. Serre had proved a 'Riemann hypothesis' for the 'zeta function' of a self-map $f: Y \to Y$ of a variety Y over $\mathbf{C}$, using properties of the cohomology groups, like the *Hodge decomposition* (and other facts from what is called *Hodge theory*). Some of these properties of cohomology were stated, and 'proved', by Lefschetz; however, his proofs of some of them (notably what is called the *Hard Lefschetz theorem*) are considered insufficiently rigorous by modern standards.

Grothendieck observed that one can rephrase Serre's argument cleverly so as to omit any explicit reference to Hodge theory, and instead use properties of certain 'natural' operations and structures on cohomology (including the Hard Lefschetz theorem). The properties of these 'natural' operations, however, at present can only be partly proved; for example, the Hard Lefschetz theorem can only be proved at present using Hodge theory, or, ironically, deduced as a *consequence* of Weil's Riemann hypothesis.

The analogous properties for Grothendieck's étale cohomology are essentially Grothendieck's *standard conjectures*, formulated by him in his article in the Bombay Colloquium on Algebraic Geometry in 1968. These are as yet unproven; Grothendieck ends his article with the statement:

> Alongside the problem of resolution of singularities, the proof of the standard conjectures seems to me to be the most urgent task in algebraic geometry.

Deligne's two proofs of the Riemann hypothesis use the techniques of *vanishing cycles* and *monodromy*, introduced by Lefschetz in his 'proofs' mentioned above. In the first proof, Deligne also uses the 'Rankin trick' and a lemma of Kazhdan and Margulis. The second proof (see ref. 9) instead uses a variant (due to Deligne) of the 'method of Hadamard and de la Vallee Poussin', originally used in the proof of the famous *prime number theorem*; in particular, Deligne gives a 'conceptual' proof, using the unitary representation theory of compact topological groups (like Galois groups!), that various zeta functions have no zeroes on

a certain line, which corresponds to (and includes) the classical statement (proved by Hadamard and de la Vallee Poussin) that the Riemann zeta function has no zeroes on Re $s = 1$.

1 Ireland, K. and Rosen, M., A classical introduction to modern number theory, Grad. Texts in Math. No. 84, Springer, 1982.
2. Weil, A., *Bull Am Math Soc.*, 1949, **55**.
3. Illusie, L., *Deligne's l-adic Fourier Transform*, Proc. Symp. Pure Math. 46 AMS, 1987.
4 Freitag, E. and Kiehl, R., Étale Cohomology and the Weil Conjectures, Ergebnisse Math 3, Folge, Springer-Verlag, 1987, vol 13.
5. Katz, N., An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields, Proc. Symp Pure Math 28, AMS, 1976.
6. Dieudonné, J., *Math. Intell.*, 1975, **10**.
7 Ramanujan, S., *Proc. Cambridge Philos. Soc.*, 1916, **22**, 159
8. Deligne, P., Seminaire Bourbaki 355, Springer Lect., Notes No. 179, 1971.
9. Deligne, P., *Publ Math. IHES*. 1980. **52**, 137–152.
10. Deligne, P., *Publ. Math. IHES*, 1974, **43**, 273–307.
11. Kleiman, S., in *Advanced Studies in Pure Mathematics* (eds. Giraud, J *et al*), North Holland, 1968, vol. 3.

Some thoughts on Srinivasa Ramanujan

Srinivasa Ramanujan was a mystic, a true mystic in the full significance of the term. He was intensely religious, almost superstitious in some daily observances — he will not take food unless cooked by people he approved; he was a very strict vegetarian. While in England he practically cooked his own meal. Some persons said that this was largely responsible for fatal failure in his health. I am not quite so sure.

That he was highly intuitive and got at the truth of things as in a flash cannot be denied. He saw truth and knew it though he found it difficult to explain it to others in terms of logical sequence. When I was in Trivandrum, I used to go to Madras often on University and other business. Mr Ramanujan was then a Clerk in the Madras Port Trust Office. Somehow he took a fancy to me and used to visit me whenever I was at Madras; perhaps he found a sympathetic listener to what he intended to say. He used to show his notes to me, but I was rarely able to make head or tail of at least some of the things he had written. One day he was explaining a relation to me; and he suddenly turned round and said, "Sir, an equation has no meaning for me unless it expresses a thought of God". I was simply stunned. I had meditated over this remark times out of number since. To me, that single remark was the essence of Truth about God, Man and the Universe. In that statement I saw the real Ramanujan, the philosopher–mystic–mathematician.

* * *

Childlike simplicity was his dominant feature. He gave me the impression of a God-centred man, to whom every event down here was only an outer expression of an idea in the Cosmic Mind. A true philosopher tries to get at the Mind of God through such expressions in the manifested world. To him every phenomenon here is a window through which to gaze at the typical thought in the Mind of God, where everything exists beyond time and space. Down here we are aware of things only in relationship in space and time. To Ramanujan God is the fountain-source of all ideas; all our sciences and philosophies are intended only to link up this phenomenal world with the noumenal world in the Cosmic Mind.

To him all the religious observances had not only a spiritual aspect, but a disciplinary aspect as well. These trained one in self-control without which there can be no development of the higher, spiritual side of human nature. Hence he clung to these observances so rigidly; they meant so much more to him than mere forms.

[Extracts from a note written by Ramanuja Srinivasan (1887–1975), Professor of Mathematics, Maharajah's College, Trivandrum (1910–1942). This was written in the early twenties (almost immediately after Srinivasa Ramanujan died)].

Mathematics conference

His Excellency the Governor of Madras opened today the first conference of the Indian Mathematical Society at the Presidency College which was attended by a large number of leading mathematicians from various parts of the Presidency, besides several from Bombay.

In the course of his speech in declaring the Conference open, His Excellency said: The methods of mathematics play an increasing and important part in the discussion and elucidation of numerous problems in sociology, economics and other studies in the expanding complex of our environment, and it is a matter of great moment that among those who have to deal with these studies should be a body of men who are accustomed to the rigorous principles of mathematical proof, and who find intellectual relaxation and refreshment in keeping themselves informed of modern developments in what is, I suppose, the oldest science in the world. Moreover, it is at any rate a science which has always made a strong appeal to the Indian intellect, and has received from it important contributions. It is, for example, I suppose probable that to India we owe the decimal notation and the invention of Algebra, and India can point to a least one epoch in which it produced a number of brilliant mathe-

(See page 276)