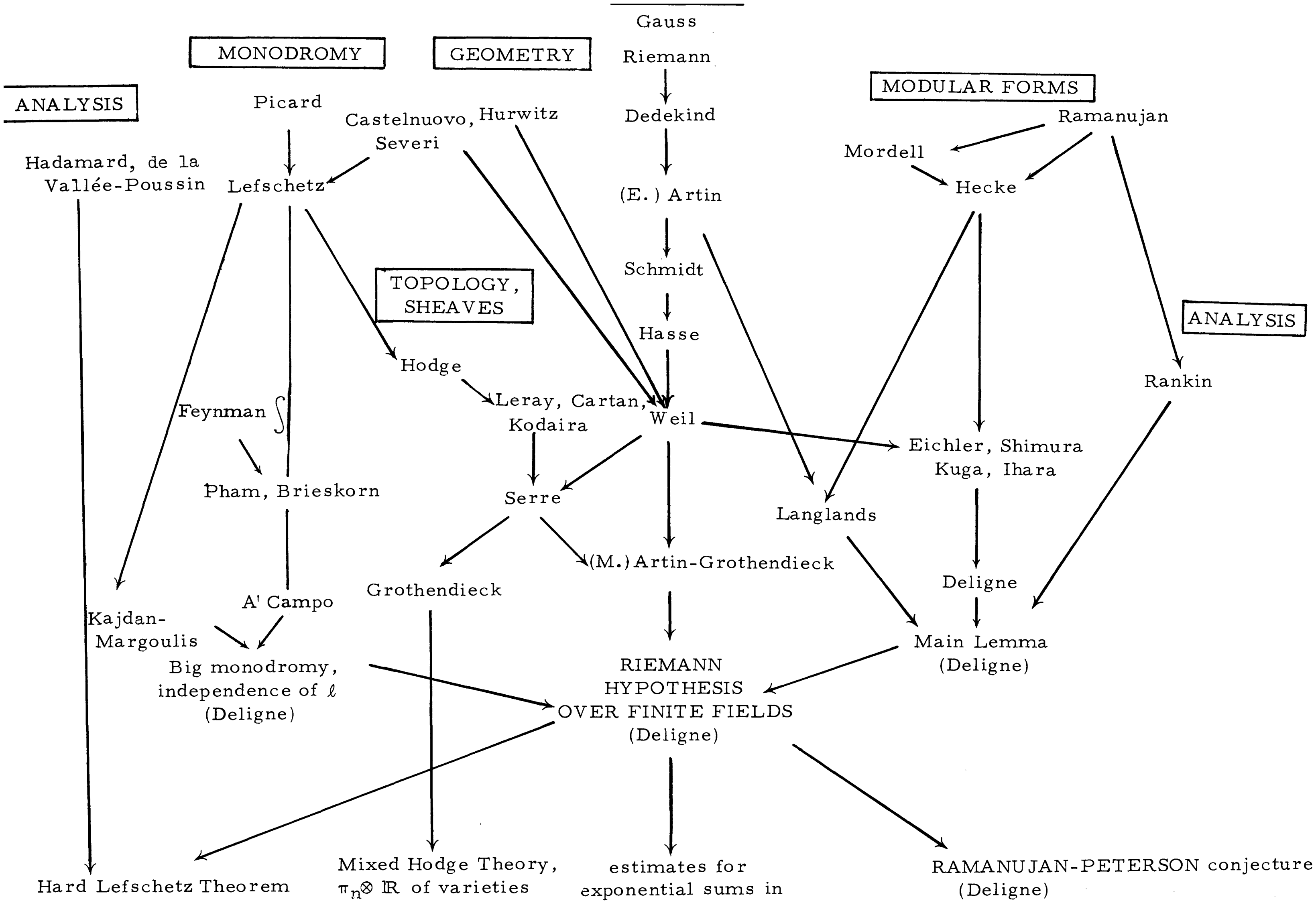
Proceedings of Symposia in Pure Mathematics
Volume 28, 1976

AN OVERVIEW OF DELIGNE's PROOF OF THE RIEMANN HYPOTHESIS FOR VARIETIES OVER FINITE FIELDS

Nicholas M. Katz

Table of Contents


ANALYSIS
MONODROMY
GEOMETRY
Gauss
Riemann
Dedekind
(E.) Artin
Schmidt
Hasse
MODULAR FORMS
Ramanujan
Mordell
Hecke
Picard
Castelnuovo, Severi
Hurwitz
Hadamard, de la Vallée-Poussin
Lefschetz
TOPOLOGY, SHEAVES
Hodge
Leray, Cartan, Kodaira
Weil
ANALYSIS
Rankin
Feynman ∫
Pham, Brieskorn
Serre
Eichler, Shimura Kuga, Ihara
Langlands
Grothendieck
(M.) Artin-Grothendieck
Deligne
A' Campo
Kajdan-Margoulis
Big monodromy, independence of ℓ (Deligne)
Main Lemma (Deligne)
RIEMANN HYPOTHESIS OVER FINITE FIELDS (Deligne)
Hard Lefschetz Theorem
Mixed Hodge Theory, π_n⊗ ℝ of varieties
estimates for exponential sums in
RAMANUJAN-PETERSON conjecture (Deligne)

Introduction to congruences

The fundamental problem in number theory is surely that of solving equations in integers. Since this problem is still largely inaccessible, we shall content ourselves with the problem of solving polynomial congruences modulo p. The idea of looking at congruences comes up naturally in trying to prove that a given equation has no solutions in integers. For example, the equation

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

can have no solutions in integers, because the corresponding congruence modulo three has no solutions in integers modulo three (the left side is 0 or 1 mod 3, the right side is -1 mod 3).

Now when we look at a congruence modulo p,

$$f(x_1, \ldots, x_n) \equiv 0 \quad \text{mod } p$$

it is most natural to look for solutions not only in the prime field $\mathbb{F}_p$ but also in all of its finite extension fields $\mathbb{F}_{p^n}$. If we identify solutions which are conjugate over $\mathbb{F}_p$, we arrive at the notion of a "prime divisor" $\mathfrak{p}$ (a maximal ideal of $\mathbb{F}_p[x_1, \ldots, x_n]/(f)$). The norm of such a prime divisor, noted $N\mathfrak{p}$, is the cardinality of its residue field. Thus $N\mathfrak{p} = p^{\deg \mathfrak{p}}$, where $\deg\mathfrak{p}$ is the number of conjugate solutions which $\mathfrak{p}$ "is."

The Zeta Function

Mindful of the analogy with the Riemann zeta function, we introduce with E. Artin [2] the infinite product

$$\prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-s})^{-1} \qquad \text{convergent for } \mathrm{Re}(s) >> 0$$

If we make the change of variable $T = p^{-s}$, we obtain

$$\prod_{\wp} (1 - T^{\deg \wp})^{-1}$$

whose logarithm is easily computed to be

$$\sum_{n \geq 1} \frac{T^n}{n} N_n,$$

where

$$N_n = \text{the number of solutions with coordinates in } \mathbb{F}_{p^n}.$$

So for any algebraic variety X over a finite field $\mathbb{F}_q$ (q some power of p), we introduce its zeta function

$$Z(X/\mathbb{F}_q, T) \overset{\text{dfn}}{=\!=} \exp\left(\sum \frac{T^n}{n} N_n\right);\ N_n = \#\, X(\mathbb{F}_{q^n})$$

$$= \prod_{\wp} (1 - T^{\deg \wp})^{-1}$$

$$= \prod_{\wp} (1 - N\wp^{-s})^{-1} \qquad T = q^{-s}$$

as a formal series in T with $\mathbb{Z}$-coefficients. It contains all of the diophantine information that X has to offer.

Let's compute an easy example. Let $X = \mathbb{A}^r$, the r-dimensional affine space over $\mathbb{F}_q$, whose points with values in $\mathbb{F}_{q^n}$ are simply the r-tuples of elements of $\mathbb{F}_{q^n}$. There are q^{rn} such r-tuples, whence

$$N_n = q^{rn}$$

$$Z(\mathbb{A}^r/\mathbb{F}_q, T) = \exp\left(\sum \frac{T^n}{n} q^{rn}\right) = \frac{1}{1 - q^r T}$$

In fact, E. Artin (1924) had introduced the zeta function only for the function fields of curves over finite fields, as an analogue of the Dedekind zeta function of an arbitrary algebraic number field, in its s-form

$$\zeta(s) = \prod_{y} (1 - Ny^{-s})^{-1} = \sum_{\mathfrak{A}} N\mathfrak{A}^{-s}$$

the last sum extended over all "integral divisors" of the function field. It was only seven years later (1931) that F. K. Schmidt [40] showed that the

Riemann-Roch theorem on the curve itself could be used to establish that for a curve $X/\mathbb{F}_q$ of genus g, its zeta function is a rational function of $T = q^{-s}$ which has the precise form

$$\zeta(s) = \frac{P(q^{-s})}{(1-q^{-s})(1-q^{1-s})} = \frac{P(T)}{(1-T)(1-qT)}$$

where $P(T) = \prod_{i=1}^{2g}(1 - \alpha_i T)$ is a polynomial of degree $2g$ with $\mathbb{Z}$-coefficients, whose roots are permuted by $\alpha \longmapsto q/\alpha$. In terms of the complex variable s, this is a functional equation under $s \longmapsto 1 - s$. The "Riemann Hypothesis", first formulated by E. Artin [2], asserts that the zeroes of this zeta function $\zeta(s)$ all lie on the line $\mathrm{Re}(s) = 1/2$, or equivalently that

$$|\alpha_i| = \sqrt{q}$$

If we take the logarithms of both sides of the equality

$$\exp\left(\sum \frac{N_n}{n} T^n\right) = \frac{\prod_{i=1}^{2g}(1 - \alpha_i T)}{(1-T)(1-qT)}$$

we obtain

$$N_n = 1 + q^n - \sum_{i=1}^{2g} \alpha_i^n$$

the expression of the distribution of primes in terms of the zeroes of the zeta function. The Riemann Hypothesis becomes equivalent to the diophantine statement

$$|N_n - 1 - q^n| \leq 2g \sqrt{q}^{\,n},$$

an equivalence first pointed out by Hasse [23].

The first special case of the Riemann Hypothesis had been done by Gauss, for the lemniscatic elliptic curve $y^2 = x^4 - 1$ over any $\mathbb{F}_p$. E. Artin ([2]) verified some more special cases, and in 1933 Hasse was able to prove it for arbitrary elliptic (genus g=1) curves.

Hasse (1933 and 1934) gave two quite different proofs. The first [22] was based on the theory of complex multiplication, and consisted in lifting the elliptic curve with its Frobenius endomorphism to characteristic zero. His second proof ([24],[25]) was explicitly geometric, based on a direct study of the endomorphism ring of the elliptic curve. Hasse and Deuring pointed out ([14 bis],[26]) the relevance of the theory of correspondences to doing the case of curves of higher genus.

Weil (1940 and 1941) then sketched two different proofs of the Riemann Hypothesis for a curve of arbitrary genus g over a finite field. The first ([51]) attacked the problem by using the points of finite order prime to p on the Jacobian of the curve as a sort of first homology group of the curve. Following Hurwitz, he interpreted a correspondence of the curve with itself as giving rise to an endomorphism of the Jacobian, which allowed him to attach an ℓ-adic $2g \times 2g$ matrix to the correspondence, and to interpret its trace in terms of the number of fixed points of the correspondence. He then deduced the Riemann Hypothesis from the positivity of the "Rosatti involution" (cf., [38],[61]). The second proof [52], which dispensed with Hurwitz's "transcendental" theory (i.e., with ℓ-adic matrices and the Jacobian), was based entirely upon Severi's theory of correspondences of the curve with itself. The zeta function was easily expressed in terms of intersection-numbers of correspondences. In terms of these intersection numbers, Weil defined a "trace function" on the ring of all (suitable equivalence classes of) correspondences. The Riemann Hypothesis then followed from a positivity property of this trace (Castelnuovo's inequality, cf., [61],[37]). In the case of a curve of genus <u>one</u>, this proof reduces essentially to Hasse's geometric proof.

Although the correspondence formalism and the positivity statements upon which Weil based his proofs were "well known" in Italian algebraic geometry, and their complex analogues rigorously proven by transcendental methods (cf., [61], pp. 552-5), the lack of adequate foundations for abstract (in the sense of [61]) algebraic geometry led Weil to write his Foundations of Algebraic Geometry [53]. This done, he gave complete accounts of his two proofs, the second in Sur les courbes algébriques et les variétes qui s'en déduisent [54] and the first, generalized to arbitrary abelian varieties, in Variétés abéliennes et courbes algébriques [55].

The Weil conjectures

Then in 1949, Weil conjectured what should be true for higher dimensional varieties [57]. Let X be an n-dimensional projective non-singular variety over $\mathbb{F}_q$. Then

(1) $Z(X/\mathbb{F}_q, T)$ is a rational function of T

(2) Moreover, $Z(X\mathbb{F}_q, T) = \dfrac{P_1(T)\, P_3(T) \ldots P_{2n-1}(T)}{P_0(T)\, P_2(T) \ldots P_{2n}(T)}$

where $P_i(T) = \prod_{j=1}^{b_i} (1 - \alpha_{ij}T), \qquad |\alpha_{ij}| = \sqrt{q}^{\,i}$,

the last equality being the "Riemann Hypothesis" in this setting.

(3) Under $\alpha \longmapsto q^n/\alpha$, the $\alpha_{i,j}$ are carried bijectively to the $\alpha_{2n-i,j}$. In terms of the complex variable s, this is a functional equation for $s \longmapsto n - s$.

(4) In case X is the "reduction modulo p" of a non-singular projective variety $\mathbb{X}$ in characteristic zero, then b_i is the i'th topological Betti number of $\mathbb{X}$ as complex manifold.

The moral is that the topology of the complex points of $\mathbb{X}$, expressed through the classical cohomology groups $H^i(\mathbb{X}, \mathbb{C})$, determines the form of the zeta function of X, i.e., determines the diophantine shape of X. There is a heuristic argument for this, as follows (cf., [61]). Among all elements of the algebraic closure of $\mathbb{F}_p$, the elements of $\mathbb{F}_q$ are singled out as the fixed points of the Frobenius morphism $x \longrightarrow x^q$. More generally, if

$\underline{x} = (,\ldots,x_i,\ldots)$ is a solution of some equations which are defined over $\mathbb{F}_q$, the $F(\underline{x}) \overset{\text{dfn}}{=\!=} (,\ldots,x_i^q,\ldots)$ will also be a solution of the same equations, and the point $\underline{x}$ will have its coordinates in $\mathbb{F}_q$ precisely if $F(\underline{x}) = \underline{x}$. Thus F is an endomorphism of our variety X over $\mathbb{F}_q$, and

$$N_n = \#\ \mathrm{Fix}\ (F^n)\ ;$$

$$Z(X/\mathbb{F}_q, T) = \exp\ (\Sigma\ \frac{T^n}{n}\ \#\ \mathrm{Fix}\ (F^n))$$

Suppose we consider instead a compact complex manifold $\mathbb{X}$, and an endomorphism $\mathbb{F}$ of $\mathbb{X}$ with reasonable fixed points. Then the Lefschetz fixed point formula would give us

$$\#\ \mathrm{Fix}\ (\mathbb{F}^n) = \Sigma\,(-1)^i\ \mathrm{trace}\ (\mathbb{F}^n | H^i(\mathbb{X}, \mathbb{C})),$$

which is formally equivalent to the identity

$$\exp\left(\sum_{n\geq 1} \frac{T^n}{n} \#\,\mathrm{Fix}\ (\mathbb{F}^n)\right) = \prod_{i=0}^{2n} \det\left(1 - T\mathbb{F} | H^i(\mathbb{X}, \mathbb{C})\right)^{(-1)^{i+1}}$$

The search for a "cohomology theory for varieties over finite fields" which could justify this heuristic argument has been responsible, directly and indirectly, for much of the tremendous progress made in algebraic geometry these past twenty-five years. Weil's proofs of the Riemann Hypothesis for curves over finite fields had already necessitated his Foundations. Around the same time, Zariski had also begun emphasizing the need for an abstract algebraic geometry; his disenchantment with the lack of rigor in the Italian school had come after writing his famous monograph Algebraic Surfaces [63], which gave the "state of the art" as of 1934 (cf., [64). The possibility of transposing to abstract algebraic varieties with their "Zariski topology" the far-reaching topological and sheaf-theoretic methods which had been developed by Picard, Lefschetz, Hodge, Kodaira, Leray, Cartan, ... in dealing with complex varities was implicit in Weil's 1949 Chicago lecture notes "Fibre Spaces in Algebraic Geometry" [58]. The transposition was carried out by Serre in his famous article "Faisceaux Algébriques Cohéhents" [41]. From the point of view of the Weil conjectures, however, this theory was still inadequate, for when applied to varieties in characteristic p it gave cohomology groups which were vector spaces in characteristic p, so could only give "mod p" traces formulas, i.e., could only give "mod p" congruences for numbers of rational points.

ℓ-adic cohomology

After some false starts (e.g. Serre's Witt vector cohomology [42],[43]) and Dwork's "unscheduled" (because apparently non-cohomological) proof [16] of the rationality conjecture (1) for any variety over $\mathbb{F}_q$, M. Artin and A. Grothendieck developed a "good" cohomology theory [3], based on the notion of étale covering space, and generalizing Weil's ℓ-adic matrices. In fact, they developed a whole slew of theories, one for each prime number $\ell \neq p$, whose coefficient field was the field $\mathbb{Q}_\ell$ of ℓ-adic numbers. Each theory gave a factorization of zeta

$$Z(T) = \prod_{i=0}^{2n} P_{i,\ell}(T)^{(-1)^{i+1}}$$

into an alternating product of $\mathbb{Q}_\ell$-adic polynomials, satisfying conjecture (3). In the case when X could be lifted to $\mathbb{X}$ in characteristic zero, they proved that $P_{i,\ell}$ was a polynomial of degree $b_i(\mathbb{X})$. They did not prove that the $P_{i,\ell}$ in fact had $\mathbb{Q}$-coefficients, nor à fortiori that the $P_{i,\ell}$ were independent of ℓ. This meant that in the factorization of an individual $P_{i,\ell}$

$$P_{i,\ell}(T) = \prod_{j=1}^{b_i} (1 - \alpha_{i,j,\ell} T)$$

the roots $\alpha_{i,j,\ell}$ were only algebraic over $\mathbb{Q}_\ell$, but possibly not algebraic over $\mathbb{Q}$, and so they might not even have archimedean absolute values. (Of course, by a theorem of Fatou, the actual reciprocal zeroes and poles of the rational function Z(T) are algebraic integers, the problem is that there might be cancellation between the various $P_{i,\ell}$ in the ℓ-adic factorization of zeta.)

So the question became how to introduce archimedean considerations into the ℓ-adic theory. Even before the ℓ-adic theory had been developed, Serre (1960), following a suggestion of Weil ([61], p. 556), had formulated and proved a Kahlerian analogue of the Weil conjectures, by making essential use of the Hodge Index theorem. In part inspired by this, in part inspired by his own earlier (1958) realization that the Castelnuovo inequality used by Weil was a consequence of the Hodge Index theorem on a surface ([20], [37]), Grothendieck in the early sixties formulated some very difficult positivity and existence conjectures about algebraic cycles, the so-called "standard conjectures" (cf., [15], [31]) whose truth would imply both the independence of ℓ and the Riemann Hypothesis.

Much to everyone's surprise at the time of Deligne's proof, Deligne managed to avoid these conjectures altogether, except to deduce one of them, the "hard" Lefschetz theorem giving the existence of the "primitive decomposition" of cohomology of a projective non-singular variety, a result previously known only over $\mathbb{C}$, and there by Hodge's theory of harmonic integrals. The rest of the "standard conjectures" remain open. In fact, the generally accepted dogma that the Riemann Hypothesis could not be proven before these conjectures had been proven (cf., [15], I, p. 224 for example) probably had the effect of delaying for a few years the proof of the Riemann Hypothesis.

It is quite striking to note that in Deligne's deduction of the hard Lefschetz theorem from the Riemann Hypothesis for varieties over finite fields, he makes essential use of a famous piece of classical analysis, the Hadamard-de Vallé Poussin method of proving that the usual Riemann zeta function has no zeroes on the line $\mathrm{Re}(s) = 1$. He was led to the method in studying Yoshida's proof [62] of the function field analogue of the Sato-Tate conjecture about the distribution of the angles of the eigenvalues of Frobenius in families of elliptic curves. Yoshida needed to show that a certain L-function had no zero on the line Re(s) = 1, and did so using some powerful estimates of Selberg. Deligne realized that Selberg's results gave much more than was needed for the equidistribution question, and checked that the original classical argument of Hadamard-de Vallée Poussin could be used instead. He went on to notice that the method could be used to slightly improve the Lang-Weil inequality for the absolute values of the eigenvalues of Frobenius on H^2 of a projective smooth surface from $|\alpha| \leq q^{3/2}$ to $|\alpha| < q^{3/2}$. (The Riemann Hypothesis in this case is $|\alpha| = q$.)

The new ingredients

So what was it that finally allowed the Riemann Hypothesis for varieties over finite fields to be proven? There were two principal ingredients.

(1) Monodromy of Lefschetz pencils. In the great work of Lefschetz [35] on the topology of algebraic varieties, he introduced the technique of systematically "fibering" a projective variety by its hyperplane sections, and then expressing the cohomology of that variety in terms of the cohomology of those fibres. The general Lefschetz theory was successfully transposed into ℓ-adic cohomology, but it didn't really bear diophantine fruit until Kajdan-Margoulis [30] proved that the "monodromy group" of a Lefschetz pencil of odd fibre dimension was as "large as possible." Deligne realized that if the same result were true in even fibre dimension as well, then it would be possible to inductively prove the independence of ℓ and the rationality of the $P_{i,\ell}$ of X, by recovering them as generalized "greatest common divisors" of the $P_{i,\ell}$ of the hyperplane sections. But the Kajdan-Margoulis proof was Lie-algebra theoretic in nature, via the logarithms of the various Picard-Lefschetz transformations in the monodromy group. The restriction to odd fibre dimension

was necessary because in that case the Picard-Lefschetz transformations were unipotent, so had interesting logarithms, while in even fibre-dimension they were of finite order. Soon after, A'Campo [1] found a counterexample to a conjecture of Brieskorn that the local monodromy of isolated singularities should always be of finite order. Turning sorrow to joy, Deligne realized that A'Campo's example could be used to construct (non-Lefschetz) pencils which would have unipotent local monodromy. These he used to make the Kajdan-Margoulis proof work in even fibre-dimension as well, and so to establish the "independence of ℓ" and rationality of the $P_{i,\ell}$ (cf., [50]).

With this result, the importance of monodromy considerations for diophantine questions was firmly established.

(2) Modular forms, Rankin's method, and the cohomological theory of L-series.

In the years after the Weil conjectures, experts in the theory of modular forms began to suspect a strong relation between the Weil conjectures and the Ramanujan conjecture on the order of magnitude of $\tau(n)$. Recall that the $\tau(n)$ are the q-expansion coefficients of the unique cusp form Δ of weight twelve on $SL_2(\mathbb{Z})$:

$$\Delta(q) = q\left(\prod_{n\geq 1}(1-q^n)\right)^{24} = \Sigma\tau(n)\cdot q^n$$

As an arithmetic function, $\tau(n)$ occurs essentially as the error term in the formula for the number of representations of n as a sum of 24 squares. The Ramanujan conjecture is that

$$|\tau(n)| \leq n^{11/2}\cdot d(n),\ d(n) = \#\text{ divisors of } n.$$

According to the Hecke theory (which had been "prediscovered" by Mordell for Δ) the Dirichlet series corresponding to Δ admits an Euler product:

$$\sum_{n\geq 1}\tau(n)\cdot n^{-s} = \prod_p\left(\frac{1}{1-\tau(p)\cdot p^{-s}+p^{11-2s}}\right)$$

The truth of the Ramanujan conjecture for all $\tau(n)$ is then a formal consequence of its truth for all $\tau(p)$ with p prime:

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

This last inequality may be interpreted as follows. Consider the polynomial $1 - \tau(p)T + p^{11}T^2$ and factor it:

$$1 - \tau(p)T + p^{11}T^2 = (1 - \alpha(p)T)(1 - \beta(p)\ T).$$

Then the Ramanujan conjecture for $\tau(p)$ is equivalent to the equality

$$|\alpha(p)| = |\beta(p)| = p^{11/2}$$

If there were a projective smooth variety X over $\mathbb{F}_p$ such that the polynomial $1 - \tau(p)\cdot T + p^{11}T^2$ divided $P_{11}(X/\mathbb{F}_p, T)$, then the Riemann Hypothesis for X would imply the Ramanujan conjecture for $\tau(p)$ The search for this X was carried out by Eichles, Shimura, Kuga, and Ihara (cf., [29],[32]). They constructed an X which "should have worked," but because their X was not compact and had no obvious smooth compactification, its polynomial P_{11} did not necessarily have all its roots of the correct absolute value. Deligne then showed how to compactify their X and how to see that the Hecke polynomial $1 - \tau(p)\,T + p^{11}T^2$ divided a certain factor of P_{11}, the roots of which factor would have the "correct" absolute values if the Weil conjectures were true. Thus the truth of the Ramanujan conjecture became a consequence of the universal truth of the Riemann Hypothesis for varieties over finite fields.

In 1939, Rankin [39] had obtained the then-best estimate for $\tau(n)$ (namely $\tau(n) = O(n^{29/5})$) by studying the poles of the Dirichlet series

$$\sum(\tau(n))^2 \cdot n^{-s}$$

Langlands [34] pointed out that the idea of Rankin's proof could easily be used to prove the Ramanujan conjecture, provided one knew enough about the location of the poles of an infinite collection of Dirichlet series formed from Δ by forming even tensor powers: for each even integer 2n one needed to know the poles of the function represented by the Euler product

$$\prod_{p} \prod_{i=0}^{2n} \left(\frac{1}{1 - \alpha(p)^{i} \beta(p)^{2n-i} p^{-s}} \right)^{\binom{2n}{i}}$$

Deligne studied Rankin's original paper in an effort to understand the remarks of Langlands. He realized that for L-series over curves over finite fields (instead of over Spec. ($\mathbb{Z}$)), Grothendieck's cohomological theory [19] of such L-series together with the Kajdan-Margoulis monodromy result gave an a priori hold on the poles: Rankin's methods could therefore be combined with Lefschetz pencil-monodromy techniques to yield the Riemann Hypothesis for varieties over finite fields, and with it the Ramanujan-Peterson conjecture as a corollary.

Deligne's proof in a special case

Formulation of the problem

I would now like to explain the idea of Deligne's proof by treating the special case of odd-dimensional non-singular hypersurfaces (so including the case of non-singular plane curves!). This special case, which was in fact the first case that Deligne treated, illustrates the main ideas without overwhelming the cohomological novice. In the general case, the ideas explained here occur as the "Main Lemma."

Let's consider a non-singular hypersurface $X_0 \subset \mathbb{P}^{2n}$ of degree d, over the field $\mathbb{F}_q$. Its zeta function is of the form

$$Z(X_0/\mathbb{F}_q, T) = \frac{P(X_0/\mathbb{F}_q, T)}{\prod_{i=0}^{2n-1} (1 - q^i T)}$$

where $P(X_0/\mathbb{F}_q, T)$ is a polynomial with integral coefficients and constant term one, whose degree $b = \deg P$ is the middle Betti number of any smooth degree d complex hypersurface of dimension 2n-1. Explicitly,

$$b = \frac{((d-1)^{2n} - 1)(d-1)}{d}$$

Over $\mathbb{C}$, we may factor it

$$P(X_0/\mathbb{F}_q, T) = \prod_{i=1}^{b} (1 - \alpha_i T)$$

According to the functional equation, $\alpha \longrightarrow q^{2n-1}/\alpha$ permutes the α_i. The Riemann Hypothesis for X_0 is the assertion that the complex absolute values of the α_i are all given by

$$|\alpha_i| = \sqrt{q}^{\,2n-1} \qquad i=1,\ldots,b$$

In view of the fact that $\alpha \longmapsto q^{2n-1}/\alpha$ permutes the α_i, these equalities are equivalent to the inequalities

$$|\alpha_i| \leq \sqrt{q}^{\,2n-1} \qquad i=1,\ldots,b.$$

If we equate the cohomological and diophantine expressions for the zeta function, we get

$$Z(X_0/\mathbb{F}_q, T) = \exp\Big(\sum_{r\geq 1} \frac{T^r}{r} N_r\Big) = \frac{\prod_{i=1}^{b} (1-\alpha_i T)}{\prod_{i=0}^{2n-1} (1-q^i T)}$$

Equating coefficients of the logarithms, we get

$$N_r - \sum_{i=0}^{2n-1} q^{ri} = -\sum_{i=1}^{b} \alpha_i^r ,$$

so that the Riemann Hypothesis for X_0 is equivalent to the diophantine estimates

$$\Big|N_r - \sum_{i=0}^{2n-1} q^{ri}\Big| \leq b\sqrt{q^r}^{\,2n-1} \quad , \; r=1,2,\ldots$$

However, the most fruitful equivalent formulation of the Riemann Hypothesis for X_0 turns out to be the following form * of the inequality $|\alpha_i| \leq \sqrt{q}^{\,2n-1}$:

* The power series $\dfrac{1}{P(X_0/\mathbb{F}_q, T)} \in \mathbb{Q}[[T]]$ converges (in the archimedean sense) for $|T| < 1/\sqrt{q}^{\,2n-1}$.

A geometric construction

The first step in proving the Riemann Hypothesis for X_0 is to consider not only X_0 itself, but an entire one parameter family (in fact, a Lefschetz pencil) X_t of hypersurfaces in the same ambient projective space. The idea of simultaneously proving the Riemann Hypothesis for all varieties in a suitable family containing the one of initial interest was suggested to Deligne by Bombieri's relating to him that Swinnerton-Dyer had obtained weak estimates in the case of elliptic curves by considering certain L-series attached to "the" universal family of elliptic curves, and relating them to modular forms (!).

Suppose that X_0 is defined by the vanishing of a homogeneous form F of degree d. Choose any other form G of the same degree also defined over $\mathbb{F}_q$, and consider the one parameter family of forms $F + tG$. Denote by X_t the corresponding hypersurface.

It is not difficult to see that, possibly after replacing $\mathbb{F}_q$ by a finite extension, we can choose G in such a way that

a) the hypersurface of equation G is smooth, and intersects X_0 transversely.

b) for all but finitely many values of t in the algebraic closure of $\mathbb{F}_q$, the hypersurface X_t is smooth, while for the remaining values it has one and only one singular point, which is an "ordinary double point."

Let us denote by $\mathbb{A}^1$ the affine t-line over $\mathbb{F}_q$, and by $S \subset \mathbb{A}^1$ the finite set of exceptional parameter values. We will simultaneously prove the Weil conjectures for all the X_t, $t \in \mathbb{A}^1 - S$, by making use of the ℓ-adic "glue" which holds them together. This glue is a certain ℓ-adic representation of a certain arithmetic fundamental group.

The role of monodromy

The classical setting. Suppose first that the ground field is $\mathbb{C}$ rather than $\mathbb{F}_q$. Then the various X_t, $t \in \mathbb{A}^1 - S$, fit together to form a fibration over

$\mathbb{A}^1 - S$ which is locally (on $\mathbb{A}^1 - S$) trivial in the C^∞ sense. The middle-dimensional cohomology groups $H^{2n-1}(X_t, \mathbb{Q})$ therefore form a <u>local coefficient system</u> on $\mathbb{A}^1 - S$, or, what is the same once we pick a base-point $t_0 \in \mathbb{A}^1 - S$, they give a <u>representation</u> of $\pi_1(\mathbb{A}^1 - S)$ on $H^{2n-1}(X_{t_0}, \mathbb{Q})$. This representation <u>respects</u> the alternating intersection-form $\langle , \rangle$ on $H^{2n-1}(X_{t_0}, \mathbb{Q})$, so gives a homomorphism of $\pi_1(\mathbb{A}^1 - S)$ to the symplectic group $Sp = \mathrm{Aut}(H^{2n-1}(X_{t_0}, \mathbb{Q}), \langle , \rangle)$. The Kajdan-Margoulis theorem asserts that the image of π_1 in Sp is <u>Zariski-dense</u>: any polynomial function on **Sp** which vanishes on the image of π_1 is identically zero.

<u>The ℓ-adic setting</u>. Over the ground field $\mathbb{F}_q$, if we fix a prime number ℓ prime to q, Grothendieck's theory of ℓ-adic cohomology provides us with a similar but even richer structure.

Recall that the arithmetic fundamental group π_1^{arith} of $\mathbb{A}^1 - S$ is a compact totally disconnected group, defined as the quotient of the galois group of the algebraic closure $\overline{\mathbb{F}_q(t)}$ over $\mathbb{F}_q(t)$ by the closed subgroup generated by the inertial subgroups attached to all places of $\overline{\mathbb{F}_q(t)}$ lying over points of $\mathbb{A}^1 - S$. The subgroup $\pi_1^{\mathrm{geom}} \subset \pi_1^{\mathrm{arith}}$ is the corresponding quotient of the galois group of $\overline{\mathbb{F}_q(t)}$ over $\overline{\mathbb{F}}_q(t)$. It is this "geometric fundamental group" which is the analogue of the fundamental group in the classical case. It sits in π_1^{arith} as a closed normal subgroup, with quotient group $\mathrm{gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \simeq \hat{\mathbb{Z}}$, the canonical generator being the Frobenius automorphism $a \longrightarrow a^q$ of $\overline{\mathbb{F}}_q$.

$$0 \longrightarrow \pi_1^{\mathrm{geom}} \longrightarrow \pi_1^{\mathrm{arith}} \xrightarrow{\text{"degree"}} \hat{\mathbb{Z}} \longrightarrow 0$$

Just as in algebraic number theory, there is associated to each closed point $x \in \mathbb{A}^1 - S$ and to each place $\overline{x}$ of $\overline{\mathbb{F}_q(t)}$ lying over it, a well-defined Frobenius element $\mathcal{F}_{\overline{x}} \in \pi_1^{\mathrm{arith}}$ whose degree in $\hat{\mathbb{Z}}$ is the integer $\deg(x) \overset{\mathrm{dfn}}{=\!=} \mathrm{degree}\,(\mathbb{F}_q(x)/\mathbb{F}_q)$. If we change $\overline{x}$ but keep x fixed, the element

$\mathcal{F}_{\bar{x}}$ changes by conjugation. Unfortunately, we will need to consider not the $\mathcal{F}_{\bar{x}}$ but their inverses, which we christen $F_{\bar{x}} \overset{\text{dfn}}{=\!=} (\mathcal{F}_{\bar{x}})^{-1}$. We denote by F_x the conjugacy class in π_1^{arith} of all $F_{\bar{x}}$ for points $\bar{x}$ lying over a fixed x; the degree of F_x in $\hat{\mathbb{Z}}$ is the integer $-\deg(x)$.

The ℓ-adic theory provides us with the following data:

1) a b-dimensional $\mathbb{Q}_\ell$-space V with a continuous representation of π_1^{arith} in $\text{Aut}(V)$, such that for every closed point $x \in A^1 - S$, we recover the numerator of the zeta function of $X_x/\mathbb{F}_q(x)$ by the formula

$$\det(1 - TF_x \mid V) = P(X_x/\mathbb{F}_q(x), T) \in \mathbb{Q}[T]$$

2) an alternating auto-duality intersection form $\langle , \rangle$ on V with values in $\mathbb{Q}_\ell(1-2n)$ which is respected by $\pi_1^{\text{arithmetic}}$. This means that $\langle , \rangle$ is a $\mathbb{Q}_\ell$-valued autoduality such that for $g \in \pi_1^{\text{arith}}$, $v, w \in V$, we have

$$\langle gv, gw \rangle = q^{(1-2n)\deg(g)} \langle v, w \rangle.$$

Thus

$$\begin{cases} \langle \gamma v, \gamma w \rangle = \langle v, w \rangle \text{ for } \gamma \in \pi_1^{\text{geom}} \\ \langle F_{\bar{x}} v, F_{\bar{x}} w \rangle = q^{(2n-1)\deg x} \langle v, w \rangle \text{ for each } F_{\bar{x}} \end{cases}$$

The ℓ-adic version of the Kajdan-Margoulis theorem is that the image of π_1^{geom} in $\text{Aut}(V)$ is Zariski dense (in fact, ℓ-adically open) in the symplectic group $\text{Sp}(V, \langle , \rangle)$.

The proof: a heuristic

We have set out to prove the Riemann Hypothesis for all of the $X_x/\mathbb{F}_q(x)$, $x \in \mathbb{A}^1 - S$. As we have already noted, this is equivalent to proving that for each closed point $x \in \mathbb{A}^1 - S$, the series

$$\frac{1}{P(X_x/\mathbb{F}_q(x), T)} \in \mathbb{Q}[[T]]$$

is convergent archimedeanly for $|T| < 1/\sqrt{q^{\deg x}}^{\,2n-1}$, or equivalently, (if we replace T by $T^{\deg x}$) that the series

$$\frac{1}{\det(1 - T^{\deg x} F_x|V)} = \frac{1}{P(X_x/\mathbb{F}_q(x), T^{\deg x})} \in \mathbb{Q}[[T]]$$

is convergent archimedeanly for $|T| < 1/\sqrt{q}^{\,2n-1}$.

To clarify the basic idea, let us begin by explaining how we could directly deduce this last estimate if two apparently false suppositions were simultaneously true (cf., the Remark at the end of the proof). The first supposition is that each of the series $1/\det(1 - T^{\deg x} F_x|V) \in \mathbb{Q}[[T]]$ has <u>positive</u> coefficients. The second is that the infinite product

$$L(V, T) \overset{\text{dfn}}{=\!=} \prod_x \frac{1}{\det(1 - T^{\deg x} F_x|V)} \in \mathbb{Q}[[T]]$$

is archimedeanly convergent for $|T| < 1/\sqrt{q}^{\,2n-1}$ when viewed as a power series. Granting these suppositions, we would simply remark that as each of the factors $1/\det(1 - T^{\deg x} F_x|V)$ is a series with constant term <u>one</u>, the supposition that its coefficients are <u>positive</u> means that the power series for $L(V,T)$ also has positive coefficients which are term-by-term greater than or equal to the coefficients of any of the factors. Therefore, the supposed archimedean convergence of $L(V,T)$ for $|T| < 1/\sqrt{q}^{\,2n-1}$ would imply that each of the factors $1/\det(1 - T^{\deg x} F_x|V)$ is itself archimedeanly convergent for $|T| < 1/\sqrt{q}^{\,2n-1}$.

<u>The actual proof: "squaring"</u>

We must now explain how to get around the fact that our suppositions are not simultaneously true. The non-positivity of the coefficients of the individual factor $1/\det(1 - T^{\deg x} F_x|V)$ is eliminated by <u>replacing</u> V by any of its <u>even</u>

tensor powers $V^{\otimes 2k}$. (Replacing V by $V^{\otimes 2}$ is analogous to Rankin's replacing $\sum \tau(n)\cdot n^{-s}$ by $\sum (\tau(n)^2 \cdot n^{-s}$.) To see that $1/\det(1-T^{\deg x}F_x|V^{\otimes 2k})$ has positive coefficients, we argue as follows. For any integer $m \geq 1$, we have the formula

$$1/\det(1-T^{\deg x}F_x|V^{\otimes m}) = \exp\left(\sum_{n\geq 1} \frac{T^n}{n} \operatorname{trace}(F_x^n|V^{\otimes m})\right)$$

$$= \exp\left(\sum_{n\geq 1} \frac{T^n}{n} (\operatorname{trace}(F_x^n|V))^m\right)$$

For $m = 1$, this formula, together with the fact that the series $1/\det(1-T^{\deg x}F_x|V)$ has rational coefficients shows that all of the numbers $\operatorname{trace}(F_x^n|V)$ are rational. This rationality, together with the above formula for $m = 2k$, shows that $1/\det(1-T^{\deg x}F_x|V^{\otimes 2k})$ is the exponential of a series with positive coefficients, and therefore has positive coefficients itself.

Review of L-series

Thus in order to apply the argument, we need information on the radius of convergence of the power series

$$L(V^{\otimes 2k}, T) \overset{\text{dfn}}{=\!=} \prod_x \frac{1}{\det(1-T^{\deg x}F_x|V^{\otimes 2k})}.$$

Happily, this information is provided by Grothendieck's cohomological expression for the L-function $L(M,T)$ associated to any continuous finite-dimensional $\mathbb{Q}_\ell$-adic representation of π_1^{arith}. Grothendieck gives a formula for $L(M,T)$ which shows it to be a rational function of T and which, more important for us, gives an à priori hold on its poles, as follows.

Let $M_{\pi_1^{\text{geom}}}$ denote the largest quotient space of M on which π_1^{geom} acts trivially:

$$M_{\pi_1^{\text{geom}}} = M \Big/ \sum_{\gamma \in \pi_1^{\text{geom}}} (1-\gamma)M$$

This factor space is a representation of $\pi_1^{arith}/\pi_1^{geom} \simeq \hat{\mathbb{Z}}$, so the unique element $F \in \hat{\mathbb{Z}}$ of degree -1 (the <u>inverse</u> of the automorphism $a \longrightarrow a^q$ of $\overline{\mathbb{F}_q}$) acts on it. Grothendieck's formula for L-series asserts that the product

$$\det(1-qTF|M_{\pi_1 geom})\cdot L(M,T)$$

is a <u>polynomial</u>.

<u>The end of the proof</u>

We now apply this to $M = V^{\otimes 2k}$. The key point is to compute $(V^{\otimes 2k})_{\pi_1 geom}$ and the action of F upon it, for then we will know the poles of $L(V^{\otimes 2k}, T)$. Because the image of π_1^{geom} in $Sp = \mathrm{Aut}\,(V, \langle,\rangle)$ is Zariski-dense (by the Kajdan-Margoulis theorem), their covariants are the same:

$$(V^{\otimes 2k})_{\pi_1 geom} \simeq (V^{\otimes 2k})_{Sp}$$

The tensor covariants of the symplectic group, or rather their dual, are well known from classical invariant theory. By the definition of covariants, linear forms on $(V^{\otimes 2k})_{Sp}$ are the same thing as Sp-invariant 2k-linear forms on V, and these are all sums of "complete contractions": for each partition of the set $\{1, \quad ., 2k\}$ into two ordered sets $\{a_1, \ldots, a_k, b_1, \ldots, b_k\}$, the corresponding complete contraction is the 2k-linear form on V

$$(v_1, \ldots, v_{2k}) \longrightarrow \prod_{i=1}^{k} \langle v_{a_i}, v_{b_i} \rangle$$

If we remember the action of π_1^{arith}, then the intersection form $\langle,\rangle$ on V takes values in $\mathbb{Q}_\ell(1-2n)$, and we see that the product $\prod_{i=1}^{k} \langle v_{a_i}, v_{b_i} \rangle$ lies in $\mathbb{Q}_\ell(k(1-2n))$. So if we pick a maximal linearly independent set of complete contractions, we get an isomorphism

$$(V^{\otimes 2k})_{Sp} \simeq \oplus\ \mathbb{Q}_\ell(k(1-2n));$$

a space on which F acts as multiplication by $q^{k\cdot(2n-1)}$.

Referring back to Grothendieck's theorem, the denominator of $L(V^{\otimes 2k},T)$ is at worst given by

$$\det(1-qTF|\oplus\mathbb{Q}_\ell(k(1-2n))) = \text{a power of } (1-q^{1+k(2n-1)}T).$$

Therefore the series $L(V^{\otimes 2k},T)$ converges archimedeanly for $|T| < 1/q^{1+k(2n-1)}$.

The positivity argument then shows that each factor $\dfrac{1}{\det(1-T^{\deg x}F_x|V^{\otimes 2k})}$ converges archimedeanly for $|T| < 1/q^{1+k(2n-1)}$.

Now suppose that $\alpha(x)$ is an eigenvalue of F_x on V. We must prove that $|\alpha(x)| \leq 1/\sqrt{q^{\deg x}}^{\,2n-1}$. But $\alpha(x)^{2k}$ will be an eigenvalue of F_x on $V^{\otimes 2k}$, and therefore $1/\det(1-T^{\deg x}F_x|V^{\otimes 2k})$ will have a pole at $T = 1/\alpha(x)^{2k/\deg x}$. But as this series converges for $|T| < 1/q^{1+k(2n-1)}$, we must have the inequality

$$|1/\alpha(x)^{2k/\deg x}| \geq 1/q^{1+k(2n-1)}$$

or equivalently

$$|\alpha(x)|^{2k/\deg x} \leq q^{1+k(2n-1)}$$

or equivalently

$$|\alpha(x)| \leq \sqrt{q^{\deg x}}^{\,(2n-1+1/k)}.$$

Letting k tend to $+\infty$, we obtain

$$|\alpha(x)| \leq \sqrt{q^{\deg x}}^{\,2n-1}. \qquad \text{Q.E.D.}$$

Remark The cohomological expression for $L(V^{\otimes 2k+1},T)$ together with the fact that the symplectic group has no covariants in any odd tensor power of its standard representation shows that in fact each of the L series $L(V^{\otimes 2k+1},T)$ is a polynomial, so has infinite radius of convergence. But it is only for the even tensor powers $V^{\otimes 2k}$ that we can be sure that each local factor $1/\det(1-T^{\deg x}F_x|V^{\otimes 2k})$ has positive coefficients.

Applications

The most striking arithmetic consequence is the generalized Ramanujan-Peterson conjecture on the order of magnitude of the coefficients of cusp forms of weight two or more on congruence subgroups of $SL_2(\mathbb{Z})$. (Deligne and Serre have also proven the conjecture for forms of weight one (unpublished), but the proof is logically independent of the Riemann Hypothesis.)

Another arithmetic application is the estimation of exponential sums in several variables. Though technically difficult, the idea goes back to Weil [56], who showed how the Riemann Hypothesis for curves over finite fields gave the "good" estimate for exponential sums in one variable.

As for geometric applications, we have already mentioned the hard Lefschetz theorem. There is also a whole chain of ideas built around the "yoga of weights," Grothendieck's catch-phrase for deducing results on the cohomology of arbitrary varieties by assuming the Riemann Hypothesis for projective non-singular varieties over finite fields (cf., [7]). The whole of Deligne's "mixed Hodge theory" for complex varieties ([8], [9]), developed before his proof of the Riemann Hypothesis, is intended to prove results about the cohomology of these varieties which follow from the Riemann Hypothesis and from the systematic application of Hironaka's resolution of singularities. The recent work of Deligne, Griffiths, Morgan and Sullivan on the rational homotopy type of complex varieties is also considerably clarified by the use of the Riemann Hypothesis.

Some open questions

1. Independence of ℓ

Let X be an arbitrary variety over an algebraically closed field k. For each prime number ℓ distinct from the characteristic of k, the ℓ-adic cohomology groups $H^i(X, \mathbb{Q}_\ell)$ and the ℓ-adic groups "with compact support"

$H^i_{comp}(X, \mathbb{Q}_\ell)$ are known ([10]) to be finite-dimensional $\mathbb{Q}_\ell$-vector spaces. Let us denote by $b^{comp}_{i,\ell}(X)$ their dimensions. It is unknown whether these numbers are independent of ℓ, except in some special cases, as follows.

When the field k is of characteristic zero, the "comparison theorem" [2] asserts that if we "choose" an embedding of k into the complex number field $\mathbb{C}$, and denote by $X(\mathbb{C})$ the corresponding analytic space over $\mathbb{C}$ with its usual topology, then we have isomorphisms

$$H^i(X, \mathbb{Q}_\ell) \simeq H^i_{sing}(X(\mathbb{C}), \mathbb{Q}) \otimes \mathbb{Q}_\ell$$

$$H^i_{comp}(X, \mathbb{Q}_\ell) \simeq H^i_{comp,\ sing}(X(\mathbb{C}), \mathbb{Q}) \otimes \mathbb{Q}_\ell$$

where H^i_{sing} (resp. $H^i_{comp,\ sing}$) denotes classical singular cohomology (resp. with compact support) of usual topological spaces.

When the field k is of characteristic p, an easy specialization argument reduces us to considering only the case when k is the algebraic closure of a finite field $\mathbb{F}_q$, and X/k comes by extension of scalars from a variety $X_0/\mathbb{F}_q$.

In case X/k is proper and smooth, then $b_{i,\ell}(X) = b^{comp}_{i,\ell}(X)$, just because X is already "compact," and we can use the Riemann Hypothesis for $X_0/\mathbb{F}_q$ (extended by Deligne to the proper (not necessarily projective) and smooth case in [6]) to interpret $b_{i,\ell}(X)$ as the number of complex zeroes (if i is odd) or poles (if i is even) of the zeta function $Z(X_0/\mathbb{F}_q, T)$ which lie on the circle $|T| = q^{-i/2}$. Because the zeta function itself is independent of ℓ, this shows that the integer $b_{i,\ell}(X)$ is independent of ℓ, and that the (a priori ℓ-adic) polynomial $\det(1-TF|H^i(X, \mathbb{Q}_\ell))$ has $\mathbb{Q}$-coefficients which are independent of ℓ.

However, when X/k fails to be proper and smooth, this argument breaks down. For arbitrary X/k, Deligne has proven (cf., [6]) that for each $\ell \neq p$, the polynomial $\det(1-TF|H^i_{comp}(X,\mathbb{Q}_\ell))$, whose degree is $b^{comp}_{i,\ell}(X)$, has algebraic numbers as coefficients, and that each of its reciprocal zeroes (the eigenvalues of F on $H^i_{comp}(X,\mathbb{Q}_\ell)$) is an algebraic number α for which there exists an integer $j \leq i$ (j depending upon α) such that α and all of its conjugates over $\mathbb{Q}$ have $|\alpha| = q^{j/2}$. But it is unknown if $\det(1-TF|H^i_{comp}(X,\mathbb{Q}_\ell))$ has $\mathbb{Q}$-coefficients, and a fortiori if it is independent of ℓ. It is the <u>mixing</u> of eigenvalues between the various H^i_{comp} that prevents us from expressing the polynomials $\det(1-TF|H^i_{comp}(X,\mathbb{Q}_\ell))$ in terms of $Z(X_0/\mathbb{F}_q, T)$, as we could do in the proper and smooth case. [A sufficiently strong form of Hironaka's resolution of singularities [27] (at present established only in characteristic zero) would allow the recovery of these characteristic polynomials intrinsically in terms of the zeta functions of the various proper and smooth varieties which would enter into a compactification and resolution of X. But perhaps one can get by without resolution.]

2. <u>An elementary proof</u> (cf., [4])

Now that we <u>know</u> the Riemann Hypothesis for varieties over finite fields, can we give an elementary proof by directly counting rational points? For curves, this has been done recently by Bombieri-Stepanov. An added difficulty in the higher dimensional case is that for the "typical" variety of dimension $d > 1$, the Riemann Hypothesis does not seem to be equivalent to any diophantine statement: the highest cohomology group H^{2d} gives the dominant contribution to the number of rational points, and <u>all</u> the rest of the cohomology is an error term:

$$N_n = q^{dn} + O(q^{n(d-\frac{1}{2})}).$$

<u>This</u> estimate, however, was established in 1953 by Lang-Weil [33] as a consequence of the Riemann Hypothesis for <u>curves</u>. There are, of course, many

special classes of varieties (e.g. curves, complete intersections, simply connected surfaces) for which the Riemann Hypothesis is equivalent to a diophantine estimate, and a direct proof valid for these would certainly be of great interest.

3. The Hasse-Weil zeta function (cf., [59], [61])

With the proof of all the Weil conjectures, we may regard the question of number of solutions of equations in finite fields as being fairly well understood. What is not at all understood is the question of solutions of equations in rational numbers. It is expected that the Hasse-Weil zeta function will play an important role in this question. To fix ideas, suppose that X is a projective smooth scheme over $\mathbb{Z}[1/N]$ (i.e., X is a projective non-singular variety over $\mathbb{Q}$ which has "good reduction" at all primes p which are prime to some "conductor" N). Then for each prime p which is prime to N, the "reduction mod p" of X, noted $X(p)$, is a projective smooth variety over $\mathbb{F}_p$. For each integer $0 \leq i \leq \dim(X/\mathbb{Z}[1/N])$, we consider the i'th polynomial $P_i(X(p)/\mathbb{F}_p, T)$ occurring in the zeta function of $X(p)/\mathbb{F}_p$. The i'th Hasse-Weil L-function is defined to be the Dirichlet series with Euler product (over primes not dividing N)

$$L(i; X, s) = \prod_p \frac{1}{P_i(X(p)/\mathbb{F}_p, p^{-s})} .$$

It is convergent for $\mathrm{Re}(s) > 1 + i/2$ by the Riemann Hypothesis for the $X(p)$'s. The Hasse-Weil zeta function is by definition the alternating product of these L-functions.

It is generally conjectured that each of the L functions $L(i, X, s)$ admits a meromorphic extension to the entire s-plane, satisfies a functional equation under $s \longrightarrow i+1-s$, and has all of its zeroes in the half-plane $\mathrm{Re}(s) \leq \frac{i+1}{2}$, with all the zeroes which are not introduced by Γ-factors in the functional equation lying on the line $\mathrm{Re}(s) = \frac{i+1}{2}$. The last conjecture is the "generalized Riemann Hypothesis."

From the point of view of arithmetic algebraic geometry, a variety X over $\mathbb{Z}[1/N]$ is the analogue of a family of varieties parameterized by a curve over a finite field. For such families, the analogues of the Hasse-Weil L-functions are the L-functions associated to the various ℓ-adic representations of π_1^{arith} which the ℓ-adic cohomology provides; the meromorphy (in fact, rationality as a function of p^{-s}) of these latter L functions, and their functional equations, are provided by Grothendieck's theory of such L-functions. The location of their zeroes is a generalized form of the Riemann Hypothesis for varieties over finite fields (which has also been proven by Deligne, but is still unpublished).

What has been proven about the Hasse-Weil L-functions? The meromorphic continuation and functional equation have been established only for very special X (e.g., elliptic curves with complex multiplication [13], [14], diagonal hypersurfaces [60], curves uniformized by modular functions [48], and X of dimension zero). There is not a single known case of the Riemann Hypothesis. In the simplest case, when the variety X over $\mathbb{Z}$ is "a point" (i.e., $X = \mathrm{Spec}(\mathbb{Z})$), the Hasse-Weil zeta function $\zeta(X,s)$ becomes the Riemann zeta function!

Bibliography

1. N. A'Campo. Sur la monodromie des singularités isolées d'hypersurfaces complexes. Inv. Math. 20, Fasc. 2 (1973), 147-170.

2. E. Artin. Quadratische Körper in Gebiete der höheren Kongruenzen I and II, Math. Zeit. 19 (1924), 153-246.

3. M. Artin, A. Grothendieck and J.-L. Verdier. SGA 4 Théorie des topos et cohomologie étale des schémas. Lecture Notes in Mathematics 269, 270, 305. Berlin-Heidelberg-New York. Springer-Verlag 1972.

4. E. Bombieri. Counting points on curves over finite fields (d'après A. Stepanov) Séminaire N. Bourbaki 1972/73, June, 1973, Exposé 430. To appear in Springer Lecture Notes in Mathematics.

5. P. Deligne. La conjecture de Weil I. Publ Math. IHES 43 (1974), 273-307.

6. __________. La conjecture de Weil II, to appear; this material was presented by Deligne in his 1973/74 Seminar at IHES.

7. __________. Théorie de Hodge I. Proceedings of the 1970 International Congress of Mathematicians, Nice. Gauthier-Villars, Paris, 1971.

8. __________. Théorie de Hodge II. Pub. Math. IHES 41 (1972).

9. __________. Théorie de Hodge III, to appear in Pub. Math. IHES.

10. __________. Inputs of étale cohomology. Lectures at the 1974 AMS Summer Institute on Algebraic Geometry, Arcata, California.

11. __________. Formes modulaires et représentations ℓ-adiques. Séminaire Bourbaki 1968/69, Exposé 355. Lecture Notes in Mathematics 179, Springer-Verlag, Berlin-Heidelberg-New York, 1971.

12. P. Deligne and N. Katz. SGA 7, part II. Groupes de monodromie en géométrie algébrique. Lecture Notes in Mathematics 340, Springer-Verlag, Berlin-Heidelberg-New York, 1973.

13. M. Deuring. Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins, Drei Mitteilungen. Nach. Akad. Wiss. Göttingen, 1953, pp. 85-94, 1955 pp. 13-43 and 1956, pp. 37-76.

14. __________. On the zeta function of an elliptic function field with complex multiplication. Proceedings of the International Symposium on Algebraic Number Theory, Tokyo-Nikko, 1956, pp. 47-50.

14 bis. __________. Arithmetische Theorie der Korrespondenzen algebraischen Funktionenkörpes I. J. reine angew. Math. 177 (1937), 161-191.

15. J. Dieudonne. Cours de Géometrie Algébrique I, II. Presses Universitaires de France, Paris, 1974.

16. B. Dwork. On the rationality of the zeta function of an algebraic variety. Amer. J. Math. 82 (1960), 631-648.

17. M. Eichler. Eine Verallgemeinerung der Abelschen Integrale. Math. Zeit 67 (1957), 267-298.

18. A. Grothendieck. SGA 7 part I. Groupes de monodromie en geometrie algébrique. Lecture Notes in Mathematics 288. Berlin-Heidelberg-New York, Springer-Verlag, 1973.

19. __________. Formule de Lefschetz et rationalité des fonctions L.

Séminaire Bourbaki 1964/65, Exposé 279. W. A. Benjamin, New York, 1966.

20. __________. Sur une note de Mattuck-Tate. J. Reine. Angew. Math. 200 Heft 3/4 (1958), 208-215.

21. G. H. Hardy. Ramanujan. Twelve lectures on subjects suggested by his life and work. Chelsea, New York: originally published by Cambridge University Press, 1940.

22. H. Hasse. Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidschen Kongruenz-zetafunktionen in gewissen elliptischen Fällen. Ges. d. Wiss. Nachrichten. Math-Phys. Klasse, 1933, Heft 3, 253-262.

23. __________. Uber die Kongruenz-zetafunktionen, Sitz-ber. d. Preuss. Akad. d. Wiss, 1934, 250.

24. __________. Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionen körpern. Abh. Math. Sem. Univ. Hamburg, 10 (1934), 325-348.

25. __________. Zur Theorie der abstrakten elliptischen Funktionenkörper, I, II and III. J. Reine Angew. Math 175 (1936).

26. __________. Über die Riemannsche Vermutung in Funktionenkörpern, Comptes Rendus du congrès international des mathématiciens, Oslo (1930), pp. 189-206.

27. H. Hironaka. Resolution of singularities of an algebraic variety over a field of characteristic zero, I, II. Annals of Math. 79 (1964), 109-326.

28. W. Hodge. The theory and applications of harmonic integrals, Cambridge University Press, Cambridge, 1941.

29. Y. Ihara. Hecke polynomials as congruence zeta functions in elliptic modular case. Annals of Math. Ser.2 85 (1967), 267-295.

30. Kajdan and Margoulis. Personal communication to P. Deligne, October, 1971.

31. S. Kleiman. Algebraic cycles and the Weil conjectures, in Dix exposés sur la cohomologie des schémas, North Holland, Amsterdam and Paris, 1968.

32. M. Kuga and G. Shimura. On the zeta function of a fibre variety whose fibres are abelian varieties. Annals of Math. Ser.2 82 (1965), 478-539.

33. S. Lang and A. Weil. Number of points of varieties in finite fields. Amer. J. Math., 76 (1954), 819-827.

34. R. Langlands. Problems in the theory of automorphic forms in Lectures in modern analysis and applications III. Lecture notes in Mathematics,

170, pp. 18-61, Springer-Verlag, Berlin-Heidelberg-New York, 1970.

35. S. Lefschetz. L'analysis situs et la géométrie algébrique. Gauthier-Villars, Paris, 1924.

36. D. Lehner. Note on the distribution of Ramanujan's tau function. Math. of Comp., vol. 24, no. 111, July 1970, 741-743.

37. A. Mattuck and J. Tate. On the inequality of Castelnuovo-Severi. Abh. Math. Sem., Hamburg, 22 (1958), 295.

38. D. Mumford. Abelian Varieties. Oxford University Press, Bombay, 1970.

39. R. A. Rankin. Contributions to the theory of Ramanujan's function $\tau(n)$ and similar arithmetical functions II. Proc. Comb. Phil. Soc. 35 (1939).

40. F. K. Schmidt. Analytische Zahlenthéorie in Körpern der Characteristik p. Math. Zeit. 33 (1931), 1-32.

41. J.-P. Serre. Faisceaux algébriques cohérents, Annals of Math. 61, no. 2, March 1955, 197-278.

42. ________. Sur la topologie des variétés algébriques en caractéristique p. Contrés de topologie, Mexico, 1956.

43. ________. Quelques propriétédes variétés abéliennes en caractéristique p. Amer. J. Math. LXXX, no. 3 (1958), 715-739.

44. ________. Analogues Kahlériens de certaines conjectures de Weil, Annals of Math. 71, ser. 2 (1960).

45. ________. Rationalité des fonctions ζ des variétés algébriques (d'aprés Bernard Dwork). Séminare Bourbaki 1959/60, Exposé 198. W. A. Benjamin, New York, 1966.

46. ________. Zeta and L functions in Arithmetic Algebraic Geometry, Harper and Row, New York, 1965.

47. ________. Valeurs propres des endomorphismes de Frobenius (d'après P. Deligne). Séminaire Bourbaki 973/74, February 1974, Exposé 446. To appear in Springer Lecture Notes in Mathematics.

48. G. Shimura. Correspondances modulaires et les fonctions ζ de courbes algébriques. M. Math. Soc. Japan 10 (1958), 1-28.

48bis. ________. Sur les intégrales attachés aux former automorphes. J. Math. Soc. Japan 11 (1959), 291-311.

49. G. Shimura and Y. Taniyama. Complex multiplication of abelian varieties and its applications to number theory. Pub. Math. Soc. Japan, no. 6, 1961.

50. J.-L. Verdier. Indépendance par rapport à ℓ des polynomes caractéristiques des endomorphismes de Frobenius de la cohomologie ℓ-adique

(d'après P. Deligne). Séminaire Bombaki 1972/73. Exposé 423. To appear in Springer Lecture Notes in Mathematics.

51. A. Weil. Sur les fonctions algébriques à corps de constantes fine. C. R. Acad. Sci. Paris 210 (1940), 592-594.

52. __________. On the Riemann Hypothesis in function-fields. Proc. Nat. Acad. Sci. U.S.A. 27 (1941), 345-347.

53. __________. Foundations of algebraic geometry, Amer. Math. Soc. Colloq. Pub., Vol. XXIX, New York, 1946.

54. __________. Sur les courbes algébriques et les variétés qui s'en déduisent, Hermann, Paris, 1948.

55. __________. Variétés abeliennes et courbes algébriques, Hermann, Paris, 1948.

56. __________. On some exponential sums. Proc. Nat. Acad. Sci. U.S.A., 34 (1948), 204-207.

57. __________. Number of solutions of equations in finite fields, Bull. A.M.S. 55 (1949), pp. 497-508.

58. __________. Fibre Spaces in algebraic geometry. (Notes by A. Wallace) University of Chicago, 1952.

59. __________. Number theory and algebraic geometry. Proceedings of the 1950 International Congress of Mathematicians, Cambridge, vol. 2, pp. 90-100, A.M.S., Providence, 1952.

50. __________. Jacobi sums as Grossencharaktere, Trans. A.M.S. 73 (1952), 487-495.

61. __________. Abstract versus classical algebraic geometry. Proceedings of the 1954 International Congress of Mathematicians, Vol. III, 550-558, North-Holland, Amsterdam, 1956.

62. H. Yoshida. On an analogue of the Sato conjecture. Inv. Math. 19, 4 (1973), 261-277.

63. O. Zariski. Algebraic Surfaces - Band III, Heft 5, Ergébnisse der Math. und Grenz., 1935 - second supplemented edition, Band 61, Ergébnisse, Springer-Verlag, Berlin-Heidelberg-New York, 1971.

64. __________. Collected Works, vol. II, M.I.T. Press, Cambridge, 1973, especially the preface.