Inventiones math. 23, 73–77 (1974)

Some Consequences of the Riemann Hypothesis for Varieties over Finite Fields

Nicholas M. Katz (Princeton) and William Messing (Cambridge, Mass.)

Abstract. We deduce from Deligne's form of the Riemann hypothesis and the hard Lefschetz theorem in ℓ-adic cohomology the corresponding facts for any "reasonable" cohomology theory, in particular for crystalline cohomology, and give some applications to algebraic cycles.

I.

Let X be a projective smooth absolutely irreducible variety of dimension n over $\mathbb{F}_q$. Fix a prime number $\ell \neq p = \operatorname{char}(\mathbb{F}_q)$, and denote by $H^i(X)$ the étale cohomology groups $H^i(\bar{X}, \mathbb{Q}_\ell)$, and by F the Frobenius relative to $\mathbb{F}_q$. For any polynomial $g(T) = \Pi(1-\alpha_i T)$, and any integer $r \geqq 1$, we denote by $g(T)^{(r)}$ the polynomial $\Pi(1-(\alpha_i)^r T)$.

Deligne has proven that:

D1. For every integer $i \geqq 0$, the polynomial

$$P^i(X/\mathbb{F}_q, T) = \det(1 - TF \mid H^i(X))$$

lies in $\mathbb{Z}[T]$, and its reciprocal zeroes all have complex absolute value $q^{i/2}$.

D2. For every integer $d \geqq 2$, and every Lefschetz pencil $\{X_t\}_{t \in \mathbb{P}^1}$ of hypersurface sections of degree d of X, the polynomial $P^{n-1}(X/\mathbb{F}_q, T)$ may be reconstructed as the least common multiple of all complex polynomials $f(T)$ such that whenever $t \in \mathbb{F}_{q^r}$ is a parameter value such that X_t is smooth, the polynomial $f(T)^{(r)}$ divides $P^{n-1}(X_t/\mathbb{F}_{q^r}, T)$.

D3. Let $L \in H^2(X)$ denote the class of a hyperplane. Then for $i \leqq n$, $L^i\colon H^{n-i}(X) \to H^{n+i}(X)$ is an isomorphism.

We should point out that although D3 is a *consequence* of D2 in any "reasonable" theory (as we shall see), Deligne *deduced* D2 from D3 via his monodromy techniques.

II.

Now let $\mathscr{H}$ be any cohomology theory defined for projective smooth absolutely irreducible varieties over finite extensions of $\mathbb{F}_p$ with values in finite-dimensional graded anticommutative algebras over a coefficient field K of characteristic zero, which satisfies

Poincaré Duality. Let $X/\mathbb{F}_q$ be as above, $n = \dim X$. Then $\mathscr{H}^{2n}(X)$ is one-dimensional, $\mathscr{H}^i(X) \otimes \mathscr{H}^{2n-i} \to \mathscr{H}^{2n}(X)$ is a perfect pairing, and

Frobenius F relative to $\mathbb{F}_q$ acts as multiplication by q^n [this implies that F is an *automorphism* of each $\mathscr{H}^i(X)$].

Weak Lefschetz. Given X, there is an integer $d_0 = d_0(X)$ such that if $f\colon Y \hookrightarrow X$ is any smooth hypersurface section of X of degree $d \geqq d_0$, then $f^*\colon \mathscr{H}^i(X) \to \mathscr{H}^i(Y)$ is an *isomorphism* for $i \leqq n-2$, and is injective for $i = n-1$.

Zeta-Function Formula. For X as above, let

$$\mathscr{P}^i(X/\mathbb{F}_q, T) = \det(1 - TF \mid \mathscr{H}^i(X)).$$

Then the zeta function $Z(X/\mathbb{F}_q, T)$ is given by the formula

$$Z(X/\mathbb{F}_q, T) = \prod_{i=0}^{2n} (\mathscr{P}^i(X/\mathbb{F}_q, T))^{(-1)^{i+1}}.$$

We should remark that ℓ-adic cohomology, $\ell \neq p$, and crystalline cohomology are such theories!

Theorem 1. *For any theory $\mathscr{H}$ as above, for every $X/\mathbb{F}_q$ as above, we have*

$$\mathscr{P}^i(X/\mathbb{F}_q, T) = P^i(X/\mathbb{F}_q, T) \qquad \textit{for every } i.$$

Proof. It suffices to prove the equality after an arbitrary extension of scalars from $\mathbb{F}_q$ to $\mathbb{F}_{q^d}$, i.e. to prove that $\mathscr{P}^{i(d)} = P^{i(d)}$ for some $d \geqq 1$. For then the reciprocal zeroes of each $\mathscr{P}^i$ will be algebraic integers all of whose conjugates have complex absolute value $q^{i/2}$, and the cohomological expression of the zeta function in the theory $\mathscr{H}$ shows that for i odd (resp. for i even), the reciprocal roots of $\mathscr{P}^i$ are precisely those reciprocal zeroes (resp. poles) of the zeta function of $X/\mathbb{F}_q$ all of whose conjugates have complex absolute value $q^{i/2}$. As the reciprocal roots of P^i admit the same description, we have $\mathscr{P}^i = P^i$.

The proof proceeds by induction on $n = \dim X$. At the expense of an extension of scalars, we may choose a Lefschetz pencil $\{X_t\}$ of hypersurface sections of high $(\geqq d_0(X))$ degree defined over $\mathbb{F}_q$, such that at least one of the sections X_{t_0}, $t_0 \in \mathbb{F}_q$, is smooth. Using the weak Lefschetz theorem in *both* theories (for $X_{t_0} \hookrightarrow X$), and induction, we have the equality $\mathscr{P}^i = P^i$ for $i \leqq n-2$, from which it follows for $i \geqq n+2$ by Poincaré duality. Again by the weak Lefschetz theorem, for every parameter value $t \in \mathbb{F}_{q^r}$ such that X_t is smooth, we have

$$\begin{array}{ccc} \mathscr{P}^{n-1}(X/\mathbb{F}_q, T)^{(r)} & \text{divides} & \mathscr{P}^{n-1}(X_t/\mathbb{F}_{q^r}, T) \\ & & \Big\| \ \text{by induction} \\ & & P^{n-1}(X_t/\mathbb{F}_{q^r}, T). \end{array}$$

Hence by D2, it follows that $\mathcal{P}^{n-1}(X/\mathbb{F}_q, T)$ divides $P^{n-1}(X/\mathbb{F}_q, T)$. By Poincaré Duality, this implies that $\mathcal{P}^{n+1}(X/\mathbb{F}_q, T)$ *divides* $P^{n+1}(X/\mathbb{F}_q, T)$.

If we equate the cohomological expressions of the zeta function of $X/\mathbb{F}_q$:

$$\Pi\left(P^i(X/\mathbb{F}_q, T)\right)^{(-1)^{i+1}} = \Pi\left(\mathcal{P}^i(X/\mathbb{F}_q, T)\right)^{(-1)^{i+1}}$$

then we may cancel the terms with $i \leqq n-2$ and $i \geqq n+2$, cross-multiply and get

$$R^{n-1} \cdot R^{n+1} = R^n \quad \text{where} \quad R^i = \frac{P^i}{\mathcal{P}^i}.$$

This shows that $\mathcal{P}^n$ *divides* P^n. By the Riemann hypothesis D1, the absolute values of the reciprocal zeroes of these three polynomials R^{n-1}, R^{n+1}, R^n are respectively $q^{\frac{n-1}{2}}$, $q^{\frac{n+1}{2}}$, $q^{\frac{n}{2}}$. Thus the equality $R^{n-1} \cdot R^{n+1} = R^n$ is impossible unless $R^{n-1} = R^{n+1} = R^n = 1$, whence $\mathcal{P}^i = P^i$ for every i. QED

Corollary 1. 1) $\dim_K \mathcal{H}^i(X) = \dim_{\mathbb{Q}_\ell} H^i(X)$.

2) *Deligne's theorems* D1, D2, D3 *hold with* H^i *and* P^i *replaced by* $\mathcal{H}^i$ *and* $\mathcal{P}^i$.

Proof. The first statement follows from the theorem by equating the *degrees* of P^i and $\mathcal{P}^i$. As D1 and D2 are statements about the P^i, they are also true for the $\mathcal{P}^i$. To conclude, we must explain how D3 follows from D2 in *any* theory $\mathcal{H}$. Let $f\colon Y \to X$ be the inclusion of a smooth hypersurface section of high degree, defined over $\mathbb{F}_{q^r}$. We must show that for $1 \leqq i \leqq n$, the bilinear form $(a, b) \mapsto a\, b\, L^i$ on $\mathcal{H}^{n-i}(X)$ is non-degenerate. For $2 \leqq i \leqq n$ this follows from D3 on Y by weak Lefschetz and the projection formula $a\, b\, L^i = f_*\left(f^*(a)\, f^*(b)\, L^{i-1}\right)$, valid because $L = f_*(1)$. Let $I = \text{image}\left(f^*\colon \mathcal{H}^{n-1}(X) \to \mathcal{H}^{n-1}(Y)\right)$, and let $I^\perp \subset \mathcal{H}^{n-1}(Y)$ be its orthogonal. It remains to show that $I \cap I^\perp = 0$, i.e. that cup-product is non-degenerate on I. Consider the exact sequence

$$0 \to I \cap I^\perp \to I \oplus I^\perp \to \mathcal{H}^{n-1}(Y) \to \mathcal{H}^{n-1}(Y)/I + I^\perp \to 0.$$

Denoting by $Z(\ )$ the characteristic polynomial of Frobenius relative to $\mathbb{F}_{q^r}$, we obtain the polynomial identity

$$Z\left(\mathcal{H}^{n-1}(Y)\right) \cdot Z(I \cap I^\perp) = Z(I) \cdot Z(I^\perp) \cdot Z\left(\mathcal{H}^{n-1}(Y)/I + I^\perp\right),$$

or more conveniently.

$$(*) \quad \mathcal{P}^{n-1}(Y/\mathbb{F}_{q^r}, T) \overset{\text{dfn}}{=} Z\left(\mathcal{H}^{n-1}(Y)\right) = Z(I) \cdot Z(I^\perp/I \cap I^\perp) \cdot Z\left(\mathcal{H}^{n-1}(Y)/I + I^\perp\right).$$

Notice that $\mathcal{H}^{n-1}(Y)/I + I^\perp$ is *dual* to $I \cap I^\perp$, and $I \cap I^\perp$ is isomorphic by f^* with $\text{Ker}\left(L\colon \mathcal{H}^{n-1}(X) \to \mathcal{H}^{n+1}(X)\right)$. Thus if we write

$$\det(1 - TF \mid \text{Ker}\, L) = \Pi(1 - \alpha_i T),$$

and *define* $g(T)=\Pi\left(1-(q^{n-1}/\alpha_i)\,T\right)$, then (recalling that we are over $\mathbb{F}_{q^r}$) we obtain the formula

$$Z\left(\mathscr{H}^{n-1}(Y)/I+I^{\perp}\right)=g(T)^{(r)}.$$

Again because we are over $\mathbb{F}_{q^r}$, we have

$$Z(I)=\mathscr{P}^{n-1}(X/\mathbb{F}_q,T)^{(r)}.$$

Using these last two formulas to substitute into $(*)$, we see that $\mathscr{P}^{n-1}(Y/\mathbb{F}_{q^r},T)$ is divisible by $g(T)^{(r)}\cdot\mathscr{P}^{n-1}(X/\mathbb{F}_q,T)^{(r)}$. Replacing if necessary q by q^d, and letting Y vary in a Lefschetz pencil defined over $\mathbb{F}_{q^d}$, this contradicts D2 unless $g(T)^{(d)}=1$, i.e., unless

$$\operatorname{Ker}\left(L\colon \mathscr{H}^{n-1}(X)\to\mathscr{H}^{n+1}(X)\right)$$

is *zero*. QED

Corollary (Ogus). *If $f\colon Y\hookrightarrow X$ is the inclusion of a smooth hypersurface section of any degree, then $f^*\colon \mathscr{H}^i(X)\to\mathscr{H}^i(Y)$ is an isomorphism if $i\leqq n-2$, and injective for $i=n-1$.*

Proof. By the weak Lefschetz theorem in ℓ-adic cohomology and Corollary I, 1), we know that for $i\leqq n-2$, $\dim\mathscr{H}^i(X)=\dim\mathscr{H}^i(Y)$, so it suffices to show that for $i\leqq n-1$, $f^*\colon\mathscr{H}^i(X)\to\mathscr{H}^i(Y)$ is injective. This follows from the commutative diagram

$$\begin{array}{ccccc}
\mathscr{H}^i(X) & \xrightarrow{f^*} & \mathscr{H}^i(Y) & \xrightarrow{f^*} & \mathscr{H}^{i+2}(X)\\
 & \searrow^{L^{n-i}} & & & \downarrow{\scriptstyle L^{n-1-i}}\\
 & & & & \mathscr{H}^{2n-i}(X)
\end{array}$$

in which the oblique arrow is an isomorphism by D3.

III. Application to Cycles

Theorem 2. 1) *Assume further that $\mathscr{H}$ is either a "Weil cohomology" in the sense of* [3], *or is crystalline cohomology tensored with the fraction field of the Witt vectors of the algebraic closure of $\mathbb{F}_q$ (in the crystalline theory, the "class of an algebraic cycle" is presently defined only for smooth subvarieties). Let X be a projective smooth absolutely irreducible variety over $\mathbb{F}_q$ of dimension n. Then the Künneth components of the diagonal Δ on $X\times X$ are rationally algebraic cycles independent of the theory $\mathscr{H}$; in fact they are $\mathbb{Q}$-linear combination of the graphs of Frobenius and its iterates.*

2) *If $\mathscr{H}$ is a Weil cohomology, then for any integrally algebraic cycle Z on $X\times X$ of codimension n, the induced endomorphism of each $\mathscr{H}^i(X)$ has a characteristic polynomial which lies in $\mathbb{Z}[T]$ and is independent*

of the theory $\mathscr{H}$. For any integrally algebraic cycle Z on $X \times X$, the characteristic polynomial of the induced total endomorphism of $\oplus_i \mathscr{H}^i(X)$ lies in $\mathbb{Z}[T]$ and is independent of the theory $\mathscr{H}$.

Proof. 1) By D1 and Theorem 1, it follows that the polynomials $G^i(T) = \det(T1 - F|\mathscr{H}^i(X))$ are pairwise relatively prime in $\mathbb{Q}[T]$. Hence for each i we can find a polynomial $\Pi^i(T) \in \mathbb{Q}[T]$ which is divisible by $G^j(T)$ for $j \neq i$, and which is congruent to 1 modulo $G^i(T)$. Letting F denote the graph of Frobenius, it follows from the Cayley-Hamilton theorem that the rationally algebraic cycle $\Pi^i(F)$ defines the endomorphism "projection onto $\mathscr{H}^i(X)$" of $\oplus_j \mathscr{H}^j(X)$. The second assertion 2) follows from 1) for any Weil cohomology, cf. [3, Prop. 2.6]. QED

References

1. Deligne, P.: Lectures at the International Geometry Colloquium. July 4–11, 1973 Cambridge, England
2. Berthelot, P.: Le théorème de Lefschetz «Faible» en Cohomologie Cristalline. To appear
3. Kleiman, S.: Algebraic Cycles and the Weil Conjectures, in Dix Exposés sur la Cohomologie des Schemas, pp. 359–386. Amsterdam: North-Holland 1969

Nicholas Katz
Princeton University
Department of Mathematics
Princeton, N.J. 08540/USA

William Messing
MIT
Department of Mathematics
Cambridge, Mass./USA

(Received August 8, 1973)