

Hypersurfaces and the Weil conjectures

Anthony J Scholl

University of Cambridge

20 May 2009, Antalya Cebir Günleri



UNIVERSITY OF
CAMBRIDGE

were
What ~~are~~ the Weil conjectures?

NUMBERS OF SOLUTIONS OF EQUATIONS IN FINITE FIELDS

ANDRÉ WEIL

The equations to be considered here are those of the type

$$(1) \quad a_0x_0^{n_0} + a_1x_1^{n_1} + \cdots + a_rx_r^{n_r} = b.$$

Such equations have an interesting history. In art. 358 of the *Disquisitiones* [1 a],¹ Gauss determines the Gaussian sums (the so-called cyclotomic “periods”) of order 3, for a prime of the form $p=3n+1$, and at the same time obtains the numbers of solutions for all congruences $ax^3-by^3\equiv 1\pmod p$. He draws attention himself to the elegance of his method, as well as to its wide scope; it is only much later, however, viz. in his first memoir on biquadratic residues [1b], that he gave in print another application of the same method; there he treats the next higher case, finds the number of solutions of any congruence $ax^4-by^4\equiv 1\pmod p$, for a prime of the form $p=4n+1$, and derives from this the biquadratic character of $2\pmod p$, this being the ostensible purpose of the whole highly ingenious and intricate investigation. As an incidental consequence (“*coronidis loco*,” p. 89),

vestigation. As an incidental consequence (“*coronidis loco*,” p. 89), he also gives in substance the number of solutions of any congruence $y^2 \equiv ax^4 - b \pmod{p}$; this result includes as a special case the theorem stated as a conjecture (“*observatio per inductionem facta gravissima*”) in the last entry of his *Tagebuch* [1c];² and

² It is surprising that this should have been overlooked by Dedekind and other authors who have discussed that conjecture (cf. M. Deuring, *Abh. Math. Sem. Hamburgischen Univ.* vol. 14 (1941) pp. 197–198).

- Gauss (*Disquisitiones Arithmeticae*)
 $ax^3 - by^3 \equiv 0 \pmod{p}, \quad p \equiv 1 \pmod{3}$
 $ax^4 - by^4 \equiv 0 \pmod{p}, \quad p \equiv 1 \pmod{4}$
- Dedekind
- Jacobi, Lebesgue
- Hardy–Littlewood (Waring's problem)
- Davenport–Hasse (varying degree of field)

Gauss: if $p \equiv 1 \pmod{4}$ is prime,

$$\begin{aligned} \#\{(x, y) \in \mathbb{F}_p^2 \mid y^2 = x^3 - x\} &= p - 2u \\ &= p - \pi - \bar{\pi} \end{aligned}$$

$$\begin{aligned} p &= u^2 + v^2, & u &\equiv 1 + v \pmod{4}, & v &\equiv 0 \pmod{2} \\ &= \pi\bar{\pi}, & \pi &= u + iv \equiv 1 \pmod{2(1+i)\mathbb{Z}[i]} \end{aligned}$$

If $p \equiv 3 \pmod{4}$, then $\#\{\dots\} = p$

Gauss, Davenport–Hasse:

$$\begin{aligned} & \#\{(x, y) \mid x, y \in \mathbb{F}_{p^r}, y^2 = x^3 - x\} \\ &= \begin{cases} p^r - \pi^r - \bar{\pi}^r & \text{if } p \equiv 1 \pmod{4} \\ p^r & \text{if } p \equiv 3 \pmod{4}, r \text{ odd} \\ p^r - 2(-p)^{r/2} & \text{if } p \equiv 3 \pmod{4}, r \text{ even} \end{cases} \\ &= p^r - \alpha^r - \bar{\alpha}^r \end{aligned}$$

where $\alpha = \begin{cases} \pi & (p \equiv 1 \pmod{4}) \\ \sqrt{-p} & (p \equiv 3 \pmod{4}) \end{cases}$, $|\alpha| = p^{1/2}$

Zeta function

- $q = p^e, \mathbb{F}_q, \mathbb{F}_{q^r}$
- $V =$ variety defined over \mathbb{F}_q
- $N_r = N_r(V) = \#V(\mathbb{F}_{q^r})$

Examples:

- $N_r(\mathbb{A}^n) = q^{nr}$
- $N_r(\mathbb{P}^n) = 1 + q^r + q^{2r} + \cdots + q^{nr}$
- $V =$ projective plane curve $E: y^2 = x^3 - x, q = p$ odd
 $N_r = 1 + p^r - \alpha^r - \bar{\alpha}^r = (1 - \alpha^r)(1 - \bar{\alpha}^r)$
- $V = \{a_0x_0^d + \cdots + a_{n+1}x_{n+1}^d = 0\} \subset \mathbb{P}^{n+1}, a_i \in \mathbb{F}_q^*$
Explicit formula for N_r in terms of Jacobi sums

Zeta function

Generating function:

$$\sum_{r=1}^{\infty} N_r(V) T^r = T \frac{d}{dT} \log Z(V, T)$$

$$V = \mathbb{A}^n \quad Z(V, T) = \frac{1}{1 - q^n T}$$

$$\mathbb{P}^n \quad \frac{1}{(1 - T)(1 - qT) \cdots (1 - q^n T)}$$

$$E \quad \frac{P_1(T)}{(1 - T)(1 - qT)}, \quad P_1(T) = (1 - \alpha T)(1 - \bar{\alpha} T)$$

Theorem (Weil Conjectures)

$V \subset \mathbb{P}^N/\mathbb{F}_q$ nonsingular, dimension n , absolutely irreducible.

(1) $Z(V, T) \in \mathbb{Q}(T)$ — *rationality*

$$Z(V, T) = \frac{P_1 \dots P_{2n-1}}{P_0 P_2 \dots P_{2n}}$$

$$P_0 = 1 - T, P_{2n} = 1 - q^n T$$

(2) $P_i(T) = \prod_{j=1}^{b_i} (1 - \alpha_{ij} T) \in \mathbb{Z}[T]$

$= (\text{monomial}) \times P_{2n-i}(1/q^n T)$ — *functional equation*

(3) $|\alpha_{ij}| = q^{i/2}$ — “*Riemann Hypothesis*” (RH)

Weil conjectures: examples

Examples:

- $V = \mathbb{P}^n$
- V any nonsingular curve (Hasse, Weil):

$$Z(V, T) = \frac{P_1(T)}{(1-T)(1-qT)}, \quad \deg P_1 = 2 \times (\text{genus of } V)$$

- Diagonal hypersurfaces (Weil 1949)
- In general, if V is obtained by reduction mod p of a variety V' in characteristic 0, $b_i = \deg P_i$ should be Betti numbers of V'
- Hypothesis V nonsingular is essential: e.g. singular curve $V = \{y^2 = x^3 + x^2\} \subset \mathbb{P}^2$ (over \mathbb{F}_p , $p \neq 2$) has

$$Z(V, T) = \frac{P_1(T)}{(1-T)(1-pT)}, \quad P_1(T) = \begin{cases} 1-T & p \equiv 1 \pmod{4} \\ 1+T & p \equiv 3 \pmod{4} \end{cases}$$

- Rationality: Dwork 1960
- Grothendieck, Artin... 1960s: ℓ -adic cohomology
- Deligne 1974: Riemann hypothesis (Lefschetz pencils)

- k field, algebraic closure \bar{k} , $\ell \neq \text{char}(k)$
- Variety $V/k \rightarrow H_\ell^i(V)$, $0 \leq i \leq 2 \dim(V)$
finite-dimensional vector spaces $/\mathbb{Q}_\ell$.
- Functorial in V
- $\text{Gal}(\bar{k}/k)$ acts on $H_\ell^i(V)$.
- $k = \mathbb{F}_q \implies$ Frobenius endomorphism $F_q: V \rightarrow V$, $x \mapsto x^q$
- $\implies F = F_q^*: H_\ell^i(V) \rightarrow H_\ell^i(V)$
 \parallel
 $\phi_q^{-1} \quad \phi_q \in \text{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$
- $\{\text{Fixed points of } F_q^r: V \rightarrow V\} = V(\mathbb{F}_{q^r})$

- Lefschetz fixed point formula: (V projective)

$$\#V(\mathbb{F}_{q^r}) = \#\{\text{fixed points of } F_{q^r}\} = \sum (-1)^i \text{tr}(F^r | H_\ell^i(V))$$

- \implies (rationality) with $P_i = \det(1 - TF | H_\ell^i(V)) \in \mathbb{Q}_\ell[T]$
- Poincaré duality (V nonsingular) \implies (functional equation)

- Deligne 1974:
- $P_i \in \mathbb{Z}[T]$, independent of ℓ
- $|\alpha_{ij}| = q^{i/2}$ (Riemann hypothesis)
- Monodromy of Lefschetz pencils
- Laumon: proof using Fourier transform (Brylinski)

Hypersurfaces I

$V = \{f(x_0, \dots, x_{n+1}) = 0\} \subset \mathbb{P}^{n+1}$ nonsingular hypersurface:
outside degree n , cohomology is very simple:

$$H_{\ell}^i(V) = \begin{cases} 0 & i \text{ odd } \neq n \\ \mathbb{Q}_{\ell}(F = q^{i/2}) & i \text{ even } \neq n \end{cases}$$

$$\implies N_r = \sum \pm \text{tr}(F^r) = \underbrace{1 + q^r + \dots + q^{nr}}_{\#\mathbb{P}^n(\mathbb{F}_{q^r})} + (-1)^n \sum_j \alpha_{n,j}^r$$

\nearrow
 $|\alpha_{n,j}| = q^{n/2}$ by RH

so that

$$(\text{R.H. for } V) \implies |N_r - \#\mathbb{P}^n(\mathbb{F}_{q^r})| \leq cq^{nr/2} \quad (*)$$

Conversely, inequality (*) for all $r \geq 1 \implies$ RH for V

Hypersurfaces I

- So, for hypersurfaces, Riemann hypothesis is equivalent to an entirely elementary Diophantine statement.
- Is there an elementary proof?
- Only known in dimension 1 (Stepanov, Bombieri, Schmidt)
- For dimension $n > 1$ the only “elementary” result is the Lang–Weil estimate: $|N_r - q^{nr}| \leq cq^{(2n-1)r/2}$
- If there was, then we get more:

Theorem

Riemann hypothesis for hypersurfaces “implies” Riemann hypothesis for all varieties (nonsingular, projective).

- “Implies” means that there is a proof that doesn't use monodromy of Lefschetz pencils (Deligne) or ℓ -adic Fourier transform (Laumon).
- Proof necessarily uses ℓ -adic cohomology (as RH for a general variety is *not* equivalent to an inequality on numbers of points)

Reduction steps

X/\mathbb{F}_q smooth projective — want to prove RH for X .

- Free to replace \mathbb{F}_q by a finite extension
- Induction on dimension
- Can replace X by any birationally equivalent (projective nonsingular) variety.
- There exists birational map $X \dashrightarrow V_0 = \{f = 0\} \subset \mathbb{P}^{n+1}$,
 $f \in \mathbb{F}_q[x_0, \dots, x_{n+1}]$
- But V_0 is almost always a *singular* hypersurface, to which RH doesn't apply.

I: deformation to smooth hypersurfaces

- X/\mathbb{F}_q smooth and projective;
- birational map $X \dashrightarrow V_0 = \{f = 0\} \subset \mathbb{P}^{n+1}$
- Deform V_0 to a pencil

$$V \longrightarrow T \subset \mathbb{A}^1, \quad V_t = \{f + tg = 0\}$$


whose fibre V_t is nonsingular for all $0 \neq t \in T$.

- By hypothesis, RH holds for each V_t , $t \neq 0$
- Want to somehow transfer this to X via V_0

I: passing to a semistable family

- Suppose there exists a *semistable model* for the family $V \rightarrow T$, i.e. $\pi: W \rightarrow V$ which is
 - birational
 - an isomorphism away from $V_0 \subset V$; and
 - fibre W_0 is a (reduced) normal crossings divisor (with smooth components)
- In char. 0, resolution of singularities would give this, after replacing T by finite covering
- If W exists, then X is birational to a component of W_0
- Enough to prove RH for this component.

II: local monodromy

- Let $K = \mathbb{F}_q((t))$ (formal Laurent series)
- Then $W_K = \{f + tg = 0\} \subset \mathbb{P}^{n+1}$ is a nonsingular hypersurface over K
- $H_\ell^n(W_K)$ acted on by $G = \text{Gal}(\bar{K}/K) \supset I = \text{Gal}(\bar{K}/\bar{\mathbb{F}}_q((t)))$, inertia subgroup
- I -invariants $H_\ell^n(W_K)^I$ acted on by $G/I = \text{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) \ni F = \phi_q^{-1}$. 
- **local monodromy**: RH for all the W_t ($t \neq 0$) \implies eigenvalues α of F on $H_\ell^n(W_K)^I$ have $|\alpha| \leq q^{n/2}$.

III: Rapoport–Zink spectral sequence

- $W_0 =$ union of nonsingular components Y_k , intersecting transversally
- \exists spectral sequence computing $H_\ell^*(W_K)$ in terms of $H_\ell^*(Y_{k_0} \cap \cdots \cap Y_{k_s})$, $s \geq 0$
- Induction on dimension implies that for $s \neq 0$, these cohomology groups satisfy RH
- Local monodromy estimate + analysis of spectral sequence \implies RH also holds for $s = 0$ i.e. for each $H_\ell^*(Y_k)$
- This is what we wanted to show

Complications

- Resolution of singularities not known in char. p
- Without it, cannot construct birational $W \rightarrow V$
- Fortunately De Jong's theory of alterations works here
- Obtain $W \rightarrow V$ and finite group Γ acting on W such that $W/\Gamma \rightarrow V$ is birational, up to a morphism which is purely inseparable (and after replacing T by a finite covering)
- $H_\ell^*(W_t)^\Gamma$ will then be essentially $H_\ell^*(V_t)$, hence satisfies RH.
- Same argument with local monodromy and Rapoport–Zink spectral sequence goes through.

Conclusions

- The proof is complicated but is mostly rather formal
- So if there is an easy proof of RH for hypersurfaces, we get RH for all varieties “for free”
- Maybe all this means is. . .
- . . . that counting points on hypersurfaces really is difficult.

THE END