Hypersurfaces and the Weil conjectures

Anthony J Scholl

University of Cambridge

14 October 2009

UNIVERSITY OF CAMBRIDGE

What are the Weil conjectures?

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

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

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 mod p, this being the ostensible purpose of the whole highly ingenious and intricate investigation. As an incidental consequence ("*coronidis loco*," p. 89),

Weil, the historian

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 ....

Weil, the (merciless) historian

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).

Weil 1949

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

$$\#\{(x, y) \in \mathbb{F}_p^2 \mid y^2 = x^3 - x\} = p - 2u$$

$$p = u^2 + v^2, \quad u \equiv 1 + v \bmod 4, \; v \equiv 0 \bmod 2$$

Weil 1949

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

$$\#\{(x, y) \in \mathbb{F}_p^2 \mid y^2 = x^3 - x\} = p - 2u$$

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

Weil 1949

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

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

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

Weil 1949

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

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

$$p = u^2 + v^2, \quad u \equiv 1 + v \bmod 4, \; v \equiv 0 \bmod 2$$
$$= \pi\bar{\pi}, \qquad \pi = u + iv \equiv 1 \bmod 2(1+i)\mathbb{Z}[i]$$

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

Weil 1949

Varying $q = p^r$: (Hasse, Davenport–Hasse...)

$$\#\{(x,y) \mid x,y \in \mathbb{F}_{p^r},\ y^2 = x^3 - x\}$$

Weil 1949

Varying $q = p^r$: (Hasse, Davenport–Hasse. . .)

$$\#\big\{(x,y) \;\big|\; x,y \in \mathbb{F}_{p^r},\; y^2 = x^3 - x\big\}$$

$$= \begin{cases} p^r - \pi^r - \bar{\pi}^r & \text{if } p \equiv 1 \bmod 4 \\ p^r & \text{if } p \equiv 3 \bmod 4,\ r \text{ odd} \\ p^r - 2(-p)^{r/2} & \text{if } p \equiv 3 \bmod 4,\ r \text{ even} \end{cases}$$

Weil 1949

Varying $q = p^r$: (Hasse, Davenport–Hasse. . .)

$$\#\{(x,y) \mid x,y \in \mathbb{F}_{p^r},\ y^2 = x^3 - x\}$$

$$= \begin{cases} p^r - \pi^r - \bar{\pi}^r & \text{if } p \equiv 1 \bmod 4 \\ p^r & \text{if } p \equiv 3 \bmod 4,\ r \text{ odd} \\ p^r - 2(-p)^{r/2} & \text{if } p \equiv 3 \bmod 4,\ r \text{ even} \end{cases}$$

$$= p^r - \alpha^r - \bar{\alpha}^r$$

where $\alpha = \begin{cases} \pi & (p \equiv 1 \bmod 4) \\ \sqrt{-p} & (p \equiv 3 \bmod 4) \end{cases}$

Weil 1949

Varying $q = p^r$: (Hasse, Davenport–Hasse...)

$$\#\{(x,y) \mid x,y \in \mathbb{F}_{p^r},\ y^2 = x^3 - x\}$$

$$= \begin{cases} p^r - \pi^r - \bar{\pi}^r & \text{if } p \equiv 1 \bmod 4 \\ p^r & \text{if } p \equiv 3 \bmod 4,\ r \text{ odd} \\ p^r - 2(-p)^{r/2} & \text{if } p \equiv 3 \bmod 4,\ r \text{ even} \end{cases}$$

$$= p^r - \alpha^r - \bar{\alpha}^r$$

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

Zeta function

- $q = p^e$, $\mathbb{F}_q$, $\mathbb{F}_{q^r}$

Zeta function

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

Zeta function

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

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:

- $N_r(\mathbb{A}^n) = q^{nr}$

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:

- $N_r(\mathbb{A}^n) = q^{nr}$
- $N_r(\mathbb{P}^n) = 1 + q^r + q^{2r} + \cdots + q^{nr}$

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 $E\colon y^2 = x^3 - x$, $q = p$ odd
  $N_r = 1 + p^r - \alpha^r - \bar{\alpha}^r = (1 - \alpha^r)(1 - \bar{\alpha}^r)$

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 $E\colon y^2 = x^3 - x$, $q = p$ odd
  $N_r = 1 + p^r - \alpha^r - \bar{\alpha}^r = (1 - \alpha^r)(1 - \bar{\alpha}^r)$
- $V = \{a_0 x_0^d + \cdots + a_{n+1} x_{n+1}^d = 0\} \subset \mathbb{P}^{n+1}$, $a_i \in \mathbb{F}_q^*$
  Explicit formula for N_r in terms of Jacobi sums

Zeta function

Generating function:

$$\sum_{r=1}^{\infty} N_r(V) T^r$$

Zeta function

Generating function:

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

Zeta function

Generating function:

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

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

Zeta function

Generating function:

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

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

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

Zeta function

Generating function:

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

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

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

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

Weil conjectures

Theorem (Weil Conjectures)

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

Weil conjectures

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*

Weil conjectures

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*

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

Weil conjectures

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*

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

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

Weil conjectures

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

Weil conjectures

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

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

Weil conjectures

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*

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

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

(2) $P_i(T) = \prod_{j=1}^{b_i}(1 - \alpha_{ij}T) \in \mathbb{Z}[T]$ $\quad (\alpha_{2n-i,j} = q^n/\alpha_{i,j})$

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

Weil conjectures

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) $P_i(T) = \prod_{j=1}^{b_i} (1 - \alpha_{ij} T) \in \mathbb{Z}[T]$ $\quad (\alpha_{2n-i,j} = q^n/\alpha_{i,j})$

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

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

Weil conjectures: examples

Examples:

- $V = \mathbb{P}^n$

Weil conjectures: examples

Examples:

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

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

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)

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'

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

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

Weil conjectures

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

ℓ-adic cohomology

- k field, algebraic closure $\bar{k}$, $\ell \neq char(k)$

ℓ-adic cohomology

- k field, algebraic closure $\bar{k}$, $\ell \neq char(k)$
- Variety $V/k \longrightarrow H^i_\ell(V)$, $0 \leq i \leq 2\dim(V)$ finite-dimensional vector spaces $/\mathbb{Q}_\ell$.

ℓ-adic cohomology

- k field, algebraic closure $\bar{k}$, $\ell \neq char(k)$
- Variety $V/k \longrightarrow H^i_\ell(V)$, $0 \leq i \leq 2\dim(V)$
  finite-dimensional vector spaces $/\mathbb{Q}_\ell$.
- Functorial: $f\colon V \to W \implies f^*\colon H^i_\ell(W) \to H^i_\ell(V)$

ℓ-adic cohomology

- k field, algebraic closure $\bar{k}$, $\ell \neq char(k)$
- Variety $V/k \longrightarrow H^i_\ell(V)$, $0 \leq i \leq 2\dim(V)$
  finite-dimensional vector spaces $/\mathbb{Q}_\ell$.
- Functorial: $f\colon V \to W \implies f^*\colon H^i_\ell(W) \to H^i_\ell(V)$
- $\mathrm{Gal}(\bar{k}/k)$ acts on $H^i_\ell(V)$.

ℓ-adic cohomology

- k field, algebraic closure $\bar{k}$, $\ell \neq char(k)$
- Variety $V/k \longrightarrow H^i_\ell(V)$, $0 \leq i \leq 2\dim(V)$
  finite-dimensional vector spaces $/\mathbb{Q}_\ell$.
- Functorial: $f\colon V \to W \implies f^*\colon H^i_\ell(W) \to H^i_\ell(V)$
- $\mathrm{Gal}(\bar{k}/k)$ acts on $H^i_\ell(V)$.
- $k = \mathbb{F}_q \implies$ Frobenius endomorphism $F_q\colon V \to V$, $x \mapsto x^q$

ℓ-adic cohomology

- k field, algebraic closure $\bar{k}$, $\ell \neq char(k)$
- Variety $V/k \longrightarrow H^i_\ell(V)$, $0 \leq i \leq 2\dim(V)$ finite-dimensional vector spaces $/\mathbb{Q}_\ell$.
- Functorial: $f\colon V \to W \implies f^*\colon H^i_\ell(W) \to H^i_\ell(V)$
- $\mathrm{Gal}(\bar{k}/k)$ acts on $H^i_\ell(V)$.
- $k = \mathbb{F}_q \implies$ Frobenius endomorphism $F_q\colon V \to V$, $x \mapsto x^q$
- $\implies F = F_q^*\colon H^i_\ell(V) \to H^i_\ell(V)$

ℓ-adic cohomology

- k field, algebraic closure $\bar{k}$, $\ell \neq char(k)$
- Variety $V/k \longrightarrow H^i_\ell(V)$, $0 \leq i \leq 2\dim(V)$
  finite-dimensional vector spaces $/\mathbb{Q}_\ell$.
- Functorial: $f\colon V \to W \implies f^*\colon H^i_\ell(W) \to H^i_\ell(V)$
- $\mathrm{Gal}(\bar{k}/k)$ acts on $H^i_\ell(V)$.
- $k = \mathbb{F}_q \implies$ Frobenius endomorphism $F_q\colon V \to V$, $x \mapsto x^q$
- $\implies F = F_q^*\colon H^i_\ell(V) \to H^i_\ell(V)$

- $\{\text{Fixed points of } F_q^r\colon V \to V\} \quad = \quad V(\mathbb{F}_{q^r})$

ℓ-adic cohomology

- k field, algebraic closure $\bar{k}$, $\ell \neq char(k)$
- Variety $V/k \longrightarrow H^i_\ell(V)$, $0 \leq i \leq 2\dim(V)$
  finite-dimensional vector spaces $/\mathbb{Q}_\ell$.
- Functorial: $f\colon V \to W \implies f^*\colon H^i_\ell(W) \to H^i_\ell(V)$
- $\mathrm{Gal}(\bar{k}/k)$ acts on $H^i_\ell(V)$.
- $k = \mathbb{F}_q \implies$ Frobenius endomorphism $F_q\colon V \to V$, $x \mapsto x^q$
- $\implies F = F_q^*\colon H^i_\ell(V) \to H^i_\ell(V)$

$$\phi_q \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$$

- $\{\text{Fixed points of } F_q^r\colon V \to V\} \quad = \quad V(\mathbb{F}_{q^r})$

ℓ-adic cohomology

- k field, algebraic closure $\bar{k}$, $\ell \neq char(k)$
- Variety $V/k \longrightarrow H^i_\ell(V)$, $0 \leq i \leq 2\dim(V)$
  finite-dimensional vector spaces $/\mathbb{Q}_\ell$.
- Functorial: $f\colon V \to W \implies f^*\colon H^i_\ell(W) \to H^i_\ell(V)$
- $\mathrm{Gal}(\bar{k}/k)$ acts on $H^i_\ell(V)$.
- $k = \mathbb{F}_q \implies$ Frobenius endomorphism $F_q\colon V \to V$, $x \mapsto x^q$
- $\implies F = F_q^*\colon H^i_\ell(V) \to H^i_\ell(V)$

  $$F = \phi_q^{-1} \qquad \phi_q \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$$
- $\{\text{Fixed points of } F_q^r\colon V \to V\} \quad = \quad V(\mathbb{F}_{q^r})$

ℓ-adic cohomology, II

- Lefschetz fixed point formula: (V projective)

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

ℓ-adic cohomology, II

- Lefschetz fixed point formula: (V projective)

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

- $\implies$ (rationality) with $P_i = \det\bigl(1 - TF | H^i_\ell(V)\bigr) \in \mathbb{Q}_\ell[T]$

ℓ-adic cohomology, II

- Lefschetz fixed point formula: (V projective)

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

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

Riemann hypothesis

- Deligne 1974:

Riemann hypothesis

- Deligne 1974:
- $P_i \in \mathbb{Z}[T]$, independent of ℓ

Riemann hypothesis

- Deligne 1974:
- $P_i \in \mathbb{Z}[T]$, independent of ℓ
- $|\alpha_{ij}| = q^{i/2}$ (Riemann hypothesis)

Riemann hypothesis

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

Riemann hypothesis

- 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

$V = \{f(x_0, \ldots, x_{n+1}) = 0\} \subset \mathbb{P}^{n+1}$ nonsingular hypersurface:

Hypersurfaces I

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

$$H^i_\ell(V) = \begin{cases} 0 & i \text{ odd} \neq n \\ \mathbb{Q}_\ell & i \text{ even} \neq n \end{cases}$$

Hypersurfaces I

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

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

Hypersurfaces I

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

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

$$\implies N_r = \sum \pm \mathrm{tr}(F^r) = 1 + q^r + \cdots + q^{nr} + (-1)^n \sum_j \alpha_{n,j}{}^r$$

Hypersurfaces I

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

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

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

Hypersurfaces I

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

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

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

$|{-}| = q^{n/2}$ by RH

Hypersurfaces I

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

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

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

$|-| = q^{n/2}$ by RH

so that

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

Hypersurfaces I

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

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

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

$|-| = q^{n/2}$ by RH

so that

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

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.

Hypersurfaces I

- So, for hypersurfaces, Riemann hypothesis is equivalent to an entirely elementary Diophantine statement.
- Is there an elementary proof?

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)

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: $|N_r - q^{nr}| \leq cq^{(2n-1)r/2}$

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:

Hypersurfaces II

Theorem

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

Hypersurfaces II

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).

Hypersurfaces II

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.

Reduction steps

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

- Free to replace $\mathbb{F}_q$ by a finite extension

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

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.

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 $X \dashrightarrow V_0 = \{f = 0\} \subset \mathbb{P}^{n+1}$, $f \in \mathbb{F}_q[x_0, \ldots, x_{n+1}]$

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 $X \dashrightarrow V_0 = \{f = 0\} \subset \mathbb{P}^{n+1}$, $f \in \mathbb{F}_q[x_0, \ldots, x_{n+1}]$
- 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 $X \dashrightarrow V_0 = \{f = 0\} \subset \mathbb{P}^{n+1}$

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

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

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

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

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

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

- By hypothesis, RH holds for each V_t, $t \neq 0$

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

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

  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 $V \to T$, i.e. $\pi\colon W \to V$ which is

I: passing to a semistable family

- Suppose there exists a *semistable model* for the family $V \to T$, i.e. $\pi\colon W \to V$ which is
  - birational

I: passing to a semistable family

- Suppose there exists a *semistable model* for the family $V \to T$, i.e. $\pi\colon W \to V$ which is
  - birational
  - an isomorphism away from $V_0 \subset V$; and

I: passing to a semistable family

- Suppose there exists a *semistable model* for the family $V \to T$, i.e. $\pi\colon W \to V$ which is
  - birational
  - an isomorphism away from $V_0 \subset V$; and
  - fibre W_0 is a (reduced) normal crossings divisor (with smooth components)

I: passing to a semistable family

- Suppose there exists a *semistable model* for the family $V \to T$, i.e. $\pi\colon W \to V$ 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

I: passing to a semistable family

- Suppose there exists a *semistable model* for the family $V \to T$, i.e. $\pi\colon W \to V$ 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

I: passing to a semistable family

- Suppose there exists a *semistable model* for the family $V \to T$, i.e. $\pi\colon W \to V$ 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)

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

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
- $H^n_\ell(W_K)$ acted on by $G = \mathrm{Gal}(\bar{K}/K) \supset I = \mathrm{Gal}(\bar{K}/\bar{\mathbb{F}}_q((t)))$, inertia subgroup

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
- $H^n_\ell(W_K)$ acted on by $G = \mathrm{Gal}(\bar{K}/K) \supset I = \mathrm{Gal}(\bar{K}/\bar{\mathbb{F}}_q((t)))$, inertia subgroup
- I-invariants $H^n_\ell(W_K)^I$ acted on by $G/I = \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$.

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
- $H^n_\ell(W_K)$ acted on by $G = \mathrm{Gal}(\bar{K}/K) \supset I = \mathrm{Gal}(\bar{K}/\bar{\mathbb{F}}_q((t)))$, inertia subgroup
- I-invariants $H^n_\ell(W_K)^I$ acted on by $G/I = \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) \ni F = \phi_q^{-1}$.

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
- $H^n_\ell(W_K)$ acted on by $G = \mathrm{Gal}(\bar{K}/K) \supset I = \mathrm{Gal}(\bar{K}/\bar{\mathbb{F}}_q((t)))$, inertia subgroup
- I-invariants $H^n_\ell(W_K)^I$ acted on by $G/I = \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) \ni F = \phi_q^{-1}$.
- **local monodromy**: RH for all the W_t $(t \neq 0) \implies$ eigenvalues α of F on $H^n_\ell(W_K)^I$ have $|\alpha| \leq q^{n/2}$.

III: Rapoport–Zink spectral sequence

- W_0 = union of nonsingular components Y_k, intersecting transversally

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 $H^*_\ell(Y_{k_0} \cap \cdots \cap Y_{k_s})$, $s \geq 0$

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

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 $H^*_\ell(Y_k)$

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

Complications

- Resolution of singularities not known in char. p
- Without it, cannot construct birational $W \to V$

Complications

- Resolution of singularities not known in char. p
- Without it, cannot construct birational $W \to V$
- Fortunately De Jong's theory of alterations works here

Complications

- Resolution of singularities not known in char. p
- Without it, cannot construct birational $W \to V$
- Fortunately De Jong's theory of alterations works here
- Obtain $W \to V$ and finite group Γ acting on W such that $W/\Gamma \to V$ is birational, up to a morphism which is purely inseparable (and after replacing T by a finite covering)

Complications

- Resolution of singularities not known in char. p
- Without it, cannot construct birational $W \to V$
- Fortunately De Jong's theory of alterations works here
- Obtain $W \to V$ and finite group Γ acting on W such that $W/\Gamma \to V$ 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.

Complications

- Resolution of singularities not known in char. p
- Without it, cannot construct birational $W \to V$
- Fortunately De Jong's theory of alterations works here
- Obtain $W \to V$ and finite group Γ acting on W such that $W/\Gamma \to V$ 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

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"

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. . .

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