Hypersurfaces and the Weil conjectures

Anthony J Scholl

University of Cambridge

13 January 2010

UNIVERSITY OF CAMBRIDGE

Number theory

What do number theorists most like to do?

- (try to) solve Diophantine equations

$$x^n + y^n = z^n, \qquad x,\ y,\ z \geq 1,\ n \geq 3$$

  — no solutions in $\mathbb{Z}$ (Fermat — Wiles)

- For what integers $d \geq 1$ does the equation

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

  have a solution (x, y) in $\mathbb{Q}$?

- ($\iff$ there is a rational right-angled triangle with area d.)
- *Congruent Number Problem* (closely related to the Birch–Swinnerton-Dyer conjecture)

Diophantine equations

Solving Diophantine equations is VERY HARD.

Hilbert's 10th Problem:

- $f(x_1, \ldots, x_n, t) \in \mathbb{Z}[x_1, \ldots, x_n, t]$ polynomial
- Let $S(f) = \{a \in \mathbb{Z} \mid f(x_1, \ldots, x_n, a) = 0 \text{ is soluble in } \mathbb{Z}\}$.

Theorem (Matiyasevich, 1970)

There exists f for which the set $S(f)$ is undecidable

- In other words, given $a \in \mathbb{Z}$ there is no algorithm to determine whether or not $f(\underline{x}, a) = 0$ has a solution in $\mathbb{Z}$.
- Many problems (not necessarily from number theory) can be reduced to Diophantine equations.

Congruences

- A much easier problem: let $f \in \mathbb{Z}[x_1, \ldots, x_n]$ be a polynomial and $m \geq 1$.
- Find solutions to the *congruence*

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{m}$$

- i.e. solve $f = 0$ with $x_i \in \mathbb{Z}/m\mathbb{Z}$.
- For given f and m, just a finite computation
- $f = 0$ soluble in $\mathbb{Z} \implies f \equiv 0 \pmod{m}$ soluble for all m
- But not always $\impliedby$ (even if there are solutions in $\mathbb{R}$)
- Example: for $f = 3x^3 + 4y^3 + 5z^3$, congruence $f \equiv 0 \pmod{m}$ has non-trivial solutions for all m.
- But $f = 0$ has only the trivial solution $(0, 0, 0)$ in $\mathbb{Z}$ (or $\mathbb{Q}$).

Congruences mod p

- *Chinese Remainder Theorem*:
  $f \equiv 0$ soluble mod $m \iff$ soluble mod p^r for every prime power p^r dividing m.
- Often enough to consider just mod p.
- *Hensel's Lemma* $\implies$ mod p solutions usually lift to mod p^r.

e.g. $p \equiv 1 \pmod 4$. Can find $x \in \mathbb{Z}$ with

$$x^2 \equiv -1 \pmod p \qquad \text{(Fermat!)}$$

say $x^2 = -1 + pa$. Then find b with $2bx \equiv a \pmod p$.

$$(x - pb)^2 = -1 + pa - 2pbx + p^2 b^2 \equiv -1 \pmod{p^2}$$

And so on.

Guiding principle — under suitable conditions:

> If $f \equiv 0 \pmod{p}$ has "enough" solutions for every p, and $f = 0$ has solutions in $\mathbb{R}$, then $f = 0$ is likely to have a solution in $\mathbb{Q}$.

- Hardy-Littlewood (circle) method
  Waring's problem: for $k \geq 1$ find the smallest $G = G(k)$ such that all suff. large integers N can be represented

$$N = x_1^k + \cdots + x_G^k, \quad x_i \geq 0$$

- L-functions (Birch–Swinnerton-Dyer conjecture).
- All good reasons to want to study congruences mod p.

Weil, Bull. AMS 1949

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 (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,

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

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

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

Weil 1949

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

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

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

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

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

Varieties

- Equation $y^2 = x^3 - x$ defines a plane curve
- $f(x_1, \ldots, x_n)$ defines a hypersurface V in affine n-space $\mathbb{A}^n$:

  $\{\text{solutions of } f = 0 \text{ in } \mathbb{F}_{p^k}\} = \{\text{points of } V \text{ with coordinates in } \mathbb{F}_{p^k}\}$
- In general for a variety V defined by polynomial equations over $\mathbb{F}_p$, write $V(\mathbb{F}_{p^k}) = \{\text{points of } V \text{ with coordinates in } \mathbb{F}_{p^k}\}$
- Want to understand number of points $N_k = \#V(\mathbb{F}_{p^k})$ as k varies
- e.g. affine space $V = \mathbb{A}^n$ $\qquad N_k = p^{nk}$
- projective space $V = \mathbb{P}^n$ $\qquad N_k = 1 + p^k + \cdots + p^{nk}$.
- projective plane curve $E\colon y^2 = x^3 - x$, p odd

$$N_k = 1 + p^k - \alpha^k - \bar{\alpha}^k = (1 - \alpha^k)(1 - \bar{\alpha}^k)$$

(elliptic curve)

Zeta function

Generating function:

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

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

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

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

Many other examples (Weil and others)

Weil conjectures

Theorem (Weil Conjectures)

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

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

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

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

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

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

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

Weil conjectures: examples

Examples:

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

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

- Diagonal hypersurfaces (Weil 1949):

$$a_1 x_1^d + \cdots + a_m x_m^d = 0$$

- 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

- Rationality: Dwork 1960
- Grothendieck, Artin... 1960s: ℓ-adic cohomology
  - Rationality, functional equation
  - $P_i(T) =$ characteristic polynomial of operator (Frobenius) acting on cohomology space $H^i_\ell(V)$ (depending on auxiliary prime ℓ)
- Deligne 1974:
  - $P_i \in \mathbb{Z}[T]$, independent of ℓ
  - $|\alpha_{ij}| = p^{i/2}$ (Riemann hypothesis for eigenvalues of Frobenius)
- Applications include estimation of exponential sums
- Another proof by Laumon (1987)

Hypersurfaces

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

Betti numbers, some geometry $\implies$

$$Z(V,T) = \frac{1}{(1-T)(1-pT)\cdots(1-p^nT)} \times P_n(T)^{(-1)^n}$$

$$\implies N_k = \sum \pm \operatorname{tr}(F^k) = \underbrace{1 + p^k + \cdots + p^{nk}}_{\#\mathbb{P}^n(\mathbb{F}_{p^k})} + (-1)^n \sum_j \alpha_{n,j}{}^k$$

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

so that

$$\text{(R.H. for } V) \implies \left| N_k - \#\mathbb{P}^n(\mathbb{F}_{p^k}) \right| \le c p^{nk/2}$$

Hypersurfaces

In elementary terms, RH for the hypersurface $V\colon \{f = 0\}$ implies:

- $f(x_0, \ldots, x_{n+1}) \in \mathbb{Z}[x_0 \ldots x_{n+1}]$ a homogeneous polynomial.
- Assume f and $\{\partial f / \partial x_j\}$ have no common zero over the alg. closure of $\mathbb{F}_p$ ("nonsingularity").
- Then for some c, and every $k \geq 1$,

$$\left| N_k - (1 + p^k + \cdots + p^{nk}) \right| \leq c p^{nk/2} \qquad (*)$$

- Conversely, inequality $(*)$ for all $k \geq 1$, some $c \implies$ RH for the zeta function of V.
- Because $(*)$ says $\left| \sum \alpha_{n,j}^k \right| \leq c p^{nk/2}$.
- This easily implies $|\alpha_{n,j}| \leq p^{n/2}$.
- Functional equation $\implies |\alpha_{n,j}| = p^{n/2}$

- So, for hypersurfaces, Riemann hypothesis is equivalent to an entirely elementary Diophantine statement.
- People have looked hard for an elementary proof.
- Only known in dimension 1 (Stepanov, Bombieri, Schmidt)
- For dimension $n > 1$ the only "elementary" result is the Lang–Weil estimate: $\left|N_k - p^{nk}\right| \leq cp^{(2n-1)k/2}$
- If there was, then we get more:

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)

Idea of proof

- Project from a linear subspace:

$$
\begin{array}{ccccc}
 & V & \subset & \mathbb{P}^N & \text{dimension } n \\
 & \Big\downarrow & & \Big\downarrow \text{ projection} & \\
\text{hypersurface (singular)} & V' = \{g = 0\} & \subset & \mathbb{P}^{n+1} &
\end{array}
$$

- Choose some nonsingular hypersurface $\{f = 0\} \subset \mathbb{P}^{n+1}$
- Consider the hypersurface $H_t = \{g + tf = 0\}$ as t varies
- H_t is non-singular outside a finite set S of $t \in \overline{\mathbb{F}}_p = \bigcup \mathbb{F}_{p^k}$.
- What one shows is:

$$\text{R.H. for all } H_t,\ t \notin S \quad \Longrightarrow \quad \text{R.H. for } V$$

- There is no relation between $N_k(V)$ and $N_k(H_t)$, though.

Conclusions

- The proof is complicated but is mostly rather formal
- So if there was an easy proof of RH for hypersurfaces, we would get Deligne's difficult theorem "for free"
- Maybe all this means is. . .
- . . . that counting points on hypersurfaces really is hard.

THE END