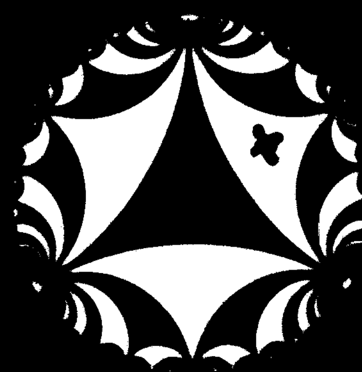

75

①

Two questions of Ramanujan (1916–1997)

(1). Which integers $n > 0$ are represented by $x_1^2 + x_2^2 + 10x_3^2$?

$$n = x_1^2 + x_2^2 + 10x_3^2$$

He notes that

$4^{\lambda}(16\mu + 6)$ is not represented

Nor are

3, 7, 21, 31, 33, 43, 67, 79, 87, 133,
217, 219, 223, 253, 307, 391,

also not 679, 2719

All other numbers less than $2 . 10^{10}$ are represented (Galway)

②

$$\Delta(q) = q\left[(1-q)(1-q^2)(1-q^3)\cdots\right]^{24}$$

$$= q - 24q^2 + 252q^3 - 1472q^4 \cdots$$

$$:= \sum_{n=1}^{\infty} \tau(n) q^n$$

n	$\tau(n)$	n	$\tau(n)$
1	+1	16	+987136
2	−24	17	−6905934
3	+252	18	+2727432
4	−1472	19	+10661420
5	+4830	20	−7109760
6	−6048	21	−4219488
7	−16744	22	−12830688
8	+84480	23	+18643272
9	−113643	24	+21288960
10	−115920	25	−25499225
11	+534612	26	+13865712
12	−370944	27	−73279080
13	−577738	28	+24647168
14	+401856	29	+128406630
15	+1217160	30	−29211840

He observes

(i) $$\tau(mn) = \tau(m)\,\tau(n)$$

if m and n have no common factors.

(ii) $$|\tau(p)| \leq 2p^{11/2}$$ if p is a prime number.

OR the reciprocals α, β of the roots of the quadratic equation $1 - \tau(p)T + p^{11}T^2$ satisfy $$|\alpha| = |\beta| = p^{11/2}.$$

• **Lagrange (1770)** Every positive integer is a sum of four squares.

Three squares:
look at remainders when dividing by 8

"mod 8"

x	0	1	2	3	4	5	6	7
x^2	0	1	4	1	0	1	4	1

so $x^2+y^2+z^2$ is never 7 mod 8.

Similarly no number $4^a(8b+7)$ is a sum of three squares.

— local congruencial obstruction.

GAUSS (1801) – local to global principal

If $n \neq 4^a(8b+7)$ Then
$n = x^2+y^2+z^2$!

C.L. Siegel (1933-51)

Gave a complete generalization and a formula for quadratic forms F, $F(x_1, \dots x_n)$.

Mass Formula:

The total number of representations of m by $F = F_1$ together with $F_2, \dots, F_h$ (the F_j's are in the same genus) in terms of (local) counting congruence

$$N_F(q) = \#\{(x_1, x_2, \dots x_n) \bmod q : F(x_1, \dots, x_n) \equiv m \pmod q\}$$

- $x_1^2 + x_2^2 + x_3^2$ and $x_1^2 + x_2^2 + x_3^2 + x_4^2$ have only one form in their genus.

- F_1: $x_1^2 + x_2^2 + 10x_3^2$

  F_2: $2x_1^2 + 2x_2^2 + 3x_3^2 - 2x_1x_2$

So falls short of answering Ramanujan.

- Ono (95-97) - Soundararajan (99-01):

Assume the "Grand Riemann Hypothesis" then 2719 is in fact the largest exception to representability for F_1.

- Iwaniec (99-00) - Duke-Schulze Pillot (99-00):

The list of exceptions for F_1 is finite.

(Not effective due to the use of another of Siegel's Theorems).

Generating functions:

Euler
Ramanujan

a_n, $n \geq 1$, want to understand these numbers.

$$\sum_{n=1}^{\infty} a_n q^n := F(q).$$

Look for properties of F, eg transformations in q which relate values of F, ie symmetries of F.

eg: $$\Delta(q) = q \prod_{n=1}^{\infty} (1-q^n)^{24} \qquad |q|<1$$

set $q = e^{2\pi i z}$ $\qquad z = x+iy,\ y>0$
$\in \mathbb{H}$

(Jacobi): $$\Delta\left(\frac{az+b}{cz+d}\right) = (cz+d)^{12} \Delta(z)$$

for a, b, c, d integers $ad-bc=1$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{modular group}$$

$\Delta(z)$ is a "modular form"

(MANY PROOFS KNOWN)

7

A. Weil (1958 – 98)

1948 CONJECTURES (FOLLOWING E. ARTIN'S 1923 THESIS)

V: $f(x_0, x_1, x_2, \ldots, x_n) = 0$ (*)

homogeneous polynomial integer coeff.

(or even a system of such equations)

- count solutions in congruences

if $\gcd(m, n) = 1$ then counting mod mn, reduces to mod m, and mod n, independently.

mod p^r for $r \geq 1$, p prime.

Note mod p, $\{0, 1, \ldots, p-1\}$ forms a <u>field</u>, $\mathbb{F}_p$.

<u>Fact</u>: For each $r \geq 1$ there is a unique field with p^r elements $\mathbb{F}_{p^r}$.

$N_{f,p}(r) = \#$ of solutions (projective) to (*) with coordinates in $\mathbb{F}_{p^r}$.

How do these vary with r?

[Galois symmetry group]

generating function ("ZETA FUNCTION")

$$\exp\left(\sum_{r=1}^{\infty} \frac{N_{f,p}(r)}{r} T^r\right) =: Z_p(f,T)$$

WEIL CONJECTURES:

(i) $Z(f,T)$ is a rational function of T (with explicit degree depending on the topology of V)

This means $$N(r) = \sum_{j=1}^{n} \beta_j^r - \sum_{k=1}^{m} \alpha_k^r$$

for complex numbers β_j, α_k.

(ii) functional equation symmetry

$Z(f,T)$ is related to $Z(f, 1/Tp^{n-1})$

(iii) The reciprocals of the zeros of $Z(f,T)$ lie on the circles $|T| = p^{(n-1)/2}$.

– analogue of the Riemann Hypothesis.

(i) proved by Dwork (83-84)

(ii)+(i) by Grothendieck — new cohomology

(iii) proved by P. Deligne (84-)

— monodromy symmetry

Remarkably (iii) + theory of modular forms [Eichler (64-65), Shimura (82-84), Sato (60-61), Ihara (65-66), Deligne]

$\Longrightarrow$ Ramanujan's Conjecture about $\tau(n)$:

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

[(ii) had been solved early on by Mordell.

$\perp$

11

What is the Riemann Hypothesis?

. about p varying!

Riemann's Zeta Function (generating of type)

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = 1^{-s} + 2^{-s} + 3^{-s} + \cdots$$

$$= (1+2^{-s}+(2^2)^{-s}+\cdots)(1+3^{-s}+(3^2)^{-s}+\cdots)(1+5^{-s}+\cdots)\cdots$$

Euler $\left\{ \begin{aligned} &= \prod_p (1+p^{-s}+p^{-2s}+p^{-3s}+\cdots) \\ &= \prod_p \frac{1}{1-p^{-s}} \end{aligned} \right.$

information about $\zeta(s)$ carries that for the distribution of primes.

Riemann showed (1859)

(i) how to make sense of $\zeta(s)$ for all complex s

(ii) functional equation $\zeta(s)$ is related to $\zeta(1-s)$

(iii) Riemann Hypothesis: All the zeros of $\zeta(s)$ in $\mathrm{Re}(s) > 0$ are on $\mathrm{Re}(s) = \frac{1}{2}$.

A. Selberg (49—)

proved that a positive proportion of the (infinitely many) zeros are on the line $Re(s)=\frac{1}{2}$. The tools he developed for this purpose are the basis for many recent advances.

E. Bombieri (77–)

proved approximations to generalizations of the Riemann Hypothesis for Dirichlet's zeta Functions. These show that the hypothesis is true on average in a very strong sense. His work can be used as a substitute for the hypothesis in many applications.

Mixing these together (Hasse, Weil)

V: $f(x_0, x_1, \ldots x_n) = 0$

defined with integer coeff.

For each prime p (large ones at least).
we have

$Z_p(f, T)$ counts solutions over $\mathbb{F}_{p^r}$

How do these vary with p?

Define the Zeta function:

$$Z_f(s) = \prod_p Z_p(f, p^{-s})$$

It contains all the local diophantine data V has to offer.

(i) Does it extend as a function of s?

(ii) Does it satisfy functional equations

(iii) Where are the zeros and poles located?

The only general result is for V an elliptic curve (next most complex after quadratic forms)

(affine)

E: $y^2 = x^3 + ax + b$

a, b integers.

$Z_E(s)$ its Hasse-Weil Zeta Function

- Wiles (95–)

(i) and (ii) are true for $L_E(s)$, it extends as a function of s and satisfies a functional equation.

This is equivalent to his proof of the "Shimura-Taniyama-Weil" conjecture that E corresponds to a modular form.

$\Longrightarrow$ Fermat's Last Theorem

Frey, Serre (00), Ribet (83-84)

We know where to look for the answer to the problem of analyzing the general $Z_v(s)$.

Generalizations of $\mathbb{H}$ the upper half plane and its transformations

$$z \longrightarrow \frac{az+b}{cz+d}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad ad-bc = 1$$

- $\mathbb{H}$ is replaced by a symmetric space S
- the group of motions by a general (semisimple) group G
- the modular form symmetry by invariance by a discrete group Γ.

(16)

Central theme of study at IAS

- Siegel, Weil in connection with quadratic forms
- Selberg spectral theory of $\Gamma\backslash G/S$ + trace formula
- Harish Chandra (63-83)
  harmonic analysis on S and representations of G
- A. Borel (57-03) The theory of algebraic groups G and arithmetic subgroups Γ
- Deligne, Shimura, arithmetic moduli.
- R. Langlands (72-)
  representation theory and a unified vision.

H. Weyl (34-51)