ICTS LECTURES

THE RAMANUJAN CONJECTURE AND SOME DIOPHANTINE EQUATIONS

PETER SARNAK

THE RAMANUJAN CONJECTURE

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

$$= q\prod_{m=1}^{\infty}(1-q^m)^{24} := q + \tau(2)q^2 + \cdots$$

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

$\tau(1)=1$, $\tau(2)=-24$, $\tau(3)=252$, $\tau(4)=-1472$
$\tau(5)=4830$, $\tau(6)=-6048$, $\cdots$

In his 1916 paper Ramanujan conjectures that

(i) $\tau(mn)=\tau(m)\tau(n)$ if $\gcd(m,n)=1$

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

TABLE V.

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

18. Let us consider more particularly the case in which $r+s=10$. The order of $E_{r,s}(n)$ is then the same as that of $\tau(n)$. The determination of this order is a problem interesting in itself. We have proved that $E_{r,s}(n)$, and therefore $\tau(n)$, is of the form $O(n^7)$ and not of the form $o(n^5)$. There is reason for supposing that $\tau(n)$ is of the form $O(n^{\frac{11}{2}+\epsilon})$ and not of the form $o(n^{\frac{11}{2}})$. For it appears that

It would follow that, if n and n' are prime to each other, we must have

$$\tau(nn') = \tau(n)\,\tau(n'). \quad \text{.......................(103)}$$

Let us suppose that (102) is true, and also that (as appears to be highly probable)

$$\{2\tau(p)\}^2 \leqslant p^{11}, \quad \text{..........................(104)}$$

so that θ_p is real. Then it follows from (102) that

$$n^{-\frac{11}{2}}\,|\,\tau(n)\,| \leqslant (1+a_1)(1+a_2)\dots(1+a_r),$$

that is to say

$$|\,\tau(n)\,| \leqslant n^{\frac{11}{2}}\,d(n), \quad \text{..........................(105)}$$

where $d(n)$ denotes the number of divisors of n.

FROM HARDY'S 12 LECTURES ON RAMANUJAN

X

RAMANUJAN'S FUNCTION $\tau(n)$

10.1. I proved in Lecture IX that

$$(10.1.1)\quad r_{24}(n) = \frac{16}{691}\sigma_{11}^{*}(n) + \frac{128}{691}\{(-1)^{n-1}259\tau(n) - 512\tau(\tfrac{1}{2}n)\},$$

where $\sigma_{11}^{*}(n)$ is a simple "divisor function" of n, and $\tau(n)$ is defined by

$$(10.1.2)\qquad g(x) = x\{(1-x)(1-x^2)\ldots\}^{24} = \sum_{1}^{\infty}\tau(n)x^n.$$

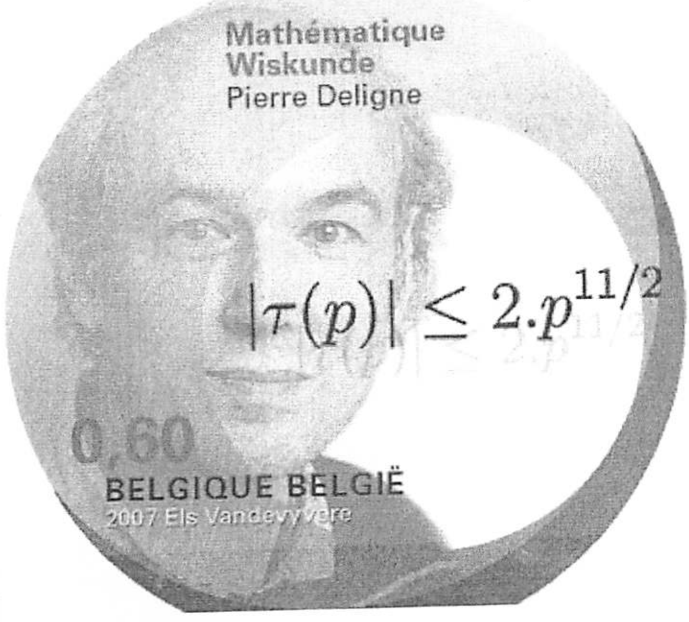
I shall devote this lecture to a more intensive study of some of the properties of $\tau(n)$, which are very remarkable and still very imperfectly understood. We may seem to be straying into one of the backwaters of mathematics, but the genesis of $\tau(n)$ as a coefficient in so fundamental a function compels us to treat it with respect.

FROM A.WEIL'S 1974 RITT LECTURES

to the inequality $|\tau(p)| \leqq 2p^{11/2}$). The first statement was proved by Mordell not very long after Ramanujan; the conjecture is still very much of an open problem, although some progress has been made. There is not one among the number-theorists I know who wouldn't be very happy and proud if he could prove it. But Hardy's remarkable comment is: "We seem to have drifted into one of the back-waters of mathematics." To him it was just another inequality; he found it curious that anyone could get deeply interested in it. In fact, he becomes apologetic and explains that, in spite of the apparent lack of interest of this problem it might still have some features which made it not unworthy of Ramanujan's attention.

(i) WAS PROVEN BY MORDELL
→ HECKE AND THE MODERN THEORY OF MODULAR FORMS

(ii) WAS PROVEN BY DELIGNE USING ARITHMETIC GEOMETRY WEIL CONJECTURES, ...



ICM 2010

$|\tau(n)| \le n^{11/2} d(n)$

HYDERABAD • INDIA

- About
- IMU GA

WHY IS IT SO IMPORTANT AND WHY WAS RAMANUJAN SO INTERESTED?

$$q = e^{2\pi i z}, \quad z \in \mathbb{H}$$

upper half plane

$$\Delta(z) = \sum_{n=1}^{\infty} \tau(n) e^{2\pi i n z}$$

(the discriminant function) is a holomorphic modular (cusp) form of weight 12 for $SL_2(\mathbb{Z})$

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

"periodicity"

for $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$

= 2x2 matrices with $a, b, c, d \in \mathbb{Z}$, $ad - bc = 1$.

That is $\tau(n)$'s are the Fourier coefficients of a modular form.

· Modular forms are gold mine of modern number theory (starting with Ramanujan) and their coefficients carry precious information.

· The Ramanujan Conjecture extends as Ramanujan was surely aware, to all such modular forms.

· Today modular forms are studied not only for 2×2 matrices but $n \times n$ matrices – "Langlands program" and the Ramanujan Conjectures have been extended to this setting and are one of the central unsolved problems.

· There are hosts of far-reaching applications even of the partial results that are known in general.

For Ramanujan the Conjecture was natural in connection with his innovative study of quadratic forms following Gauss, Legendre and Lagrange.

<u>Lagrange:</u> every positive number is a sum of four squares

$$f(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

then if $n > 0$, $f(x) = n$ has whole number solutions, x_1, x_2, x_3, x_4.

RAMANUJAN asks about other f's

$$f(x_1, x_2, x_3, x_4) = a x_1^2 + b x_2^2 + c x_3^2 + d x_4^2.$$

ON THE EXPRESSION OF A NUMBER IN THE FORM $ax^2 + by^2 + cz^2 + du^2$

(*Proceedings of the Cambridge Philosophical Society*, XIX, 1917, 11—21)

1. It is well known that all positive integers can be expressed as the sum of four squares. This naturally suggests the question: *For what positive integral values of a, b, c, d can all positive integers be expressed in the form*

$$ax^2 + by^2 + cz^2 + du^2 ? \qquad (1\cdot1)$$

I prove in this paper that there are only 55 sets of values of a, b, c, d for which this is true.

The more general problem of finding all sets of values of a, b, c, d, for which all integers *with a finite number of exceptions* can be expressed in the form (1·1), is much more difficult and interesting. I have considered only very special cases of this problem, with two variables instead of four; namely, the cases in which (1·1) has one of the special forms

THERE IS AN INTERESTING VARIATION OF RAMANUJAN'S LIST OF 55 UNIVERSAL (I.E REPRESENTING ALL POSITIVE NUMBERS) DIAGONAL FORMS DUE TO CONWAY AND SCHNEEBERGER. THE STRONGEST FORM IS THE "290 THEOREM OF BHARGAVA AND HANKE" (2005)

NAMELY THAT IF AN ~~AN~~ INTEGRAL QUADRATIC FORM REPRESENTS ALL POSITIVE NUMBERS UP TO 290, THEN IT IS UNIVERSAL.

The connection to the R.C. is that if f is a form in 4-variables

$\tau_f(n) = \#$ of solutions to $f(x) = n$, then

$$\tau_f(n) = E_f(n) + C_f(n)$$

where $E_f(n)$ is explicit and of magnitude $\simeq n$. (if not zero)

$C_f(n)$ is of magnitude $\sqrt{n}$ if R.C. for weight $k=2$ holds.

So for n large R.C. determines if $\tau_f(n) > 0$!

- Ramanujan's analysis led him to forms f in three variables which are much more problematic.

SUMS OF THREE SQUARES:

WHICH NUMBERS ARE SUMS OF 3 SQUARES

$$f(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2 = n$$

NOTE: THERE IS A 'LOCAL' OBSTRUCTION

IF $n \equiv 7 \pmod{8}$

THEN n IS NOT REPRESENTED

IN FACT $n = 4^a(8b+7)$
then NOT.

THEOREM (GAUSS-LEGENDRE 1800) LOCAL TO GLOBAL

IF $n \neq 4^a(8b+7)$, $n > 0$

THEN n is A SUM OF

THREE SQUARES!

RAMANUJAN WAS LED TO OTHER
f's IN 3-VARIABLES.

11

FROM HIS 1917 paper on quaternary forms

Again, the even numbers which are not of the form $x^2+y^2+10z^2$ are the numbers

$$4^{\lambda}(16\mu+6),$$

while the odd numbers that are not of that form, viz.

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

do not seem to obey any simple law.

Actually today we know, thanks to Duke, Iwaniec, Schulze-Pillot (1990), that among the odd no's there are only finitely many exceptions (ineffective!)

(1997):
ASSUMING THE GENERALIZED RIEMANN HYPOTHESIS ONO AND SOUNDARARAJAN HAVE SHOWN THAT THIS FINITE LIST CONSISTS OF THE ABOVE TOGETHER WITH 679 AND 2719

HILBERT'S ELEVENTH PROBLEM

11. Quadratische Formen mit beliebigen algebraischen Zahlencoeffizienten.

Unsere jetzige Kenntnis der Theorie der quadratischen Zahlkörper {Hilbert, Ueber den Dirichletschen biquadratischen Zahlenkörper, Mathematische Annalen, Bd. 45; Ueber die Theorie der relativquadratischen Zahlkörper, Bericht der Deutschen Mathematiker-Vereinigung 1897 und Mathematische Annalen. Bd. 51 ; Ueber die Theorie der relativ-Abelschen Körper, Nachrichten d. K. Ges. d. Wiss. zu Göttingen 1898; Grundlagen der Geometrie, Festschrift zur Enthüllung des Gauss-Weber-Denkmals in Göttingen, Leipzig 1899, Kapitel VIII § 83} setzt uns in den Stand, die Theorie der quadratischen Formen mit beliebig vielen Variabeln und beliebigen algebraischen Zahlencoefficienten erfolgreich in Angriff zu nehmen. Damit wird insbesondere zu der interessanten Aufgabe, eine quadratische Gleichung beliebig vieler Variabeln mit algebraischen Zahlencoeffizienten in solchen ganzen oder gebrochenen Zahlen zu lösen, die in dem durch die Coefficienten bestimmten algebraischen Rationalitätsbereiche gelegen sind.

OUR PRESENT KNOWLEDGE OF THE THEORY OF QUADRATIC NUMBER FIELDS PUTS US IN A POSITION TO ATTACK SUCCESSSFULLY THE THEORY OF QUADRATIC FORMS WITH ANY NUMBER OF VARIABLES AND WITH ALGEBRAIC NUMERICAL COEFFIENTS. THIS LEADS IN PARTICULAR TO THE INTERESTING PROBLEM: TO SOLVE A GIVEN QUADRATIC EQUATION WITH ALGEBRAIC NUMERICAL COEFFICIENTS BY INTEGRAL OR FRACTIONAL NUMBERS BELONGING TO THE ALGEBRAIC REALM OF RATIONALITY DETERMINED BY THE COEFFICIENTS [1].

• THE SOLUTION OF HILBERT'S 11-TH PROBLEM FOR RATIONAL NUMBERS IN A NUMBER FIELD- IE A LOCAL TO GLOBAL PRINCIPLE IS DUE TO HASSE (1923).

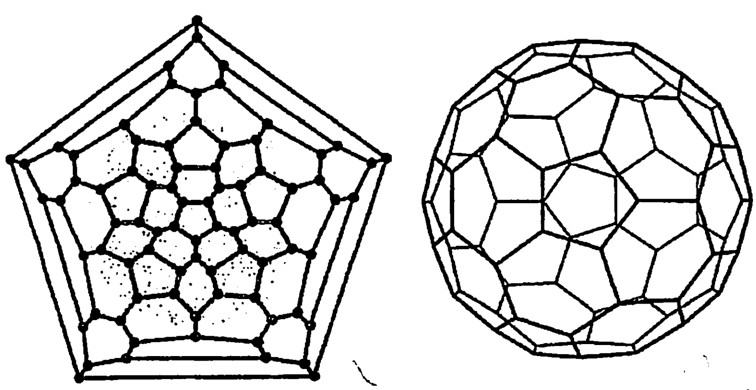
• THE SOLUTION TO THE PROBLEM OVER THE INTEGERS IN A NUMBER FIELD (I.E. A LOCAL TO GLOBAL PRINCIPLE WITH FINITELY MANY EXCEPTIONS) IS MUCH MORE DIFFICULT; SIEGEL, KNESER, CASSELS, ...
THE MOST DIFFICULT CASE OF 3-VARIABLES WAS FINALLY RESOLVED (INEFFECTIVELY) IN 2000 (COGDELL-PIATETSKI SHAPIRO-S).

• ONE OF THE KEY INGREDIENTS IS PROGRESS TOWARDS THE R.C. FOR THE EXOTIC 'MAASS WAVE FORMS'.

THESE APPLICATIONS OF R.C. ARE ALONG LINES THAT ONE MIGHT SAY, RAMANUJAN WOULD HAVE EXPECTED. THERE ARE MANY APPLICATIONS, ESPECIALLY OF GENERALIZATION THAT GO IN VERY DIFFERENT DIRECTIONS, EG. TO COMBINATORICS AND COMPUTER SCIENCE:

RAMANUJAN GRAPHS (1986): (LUBOTZKY-PHILLIPS-SARNAK, MARGULIS)

THESE ARE OPTIMALLY CONNECTED SPARSE GRAPHS — OPTIMAL "EXPANDERS" IN NETWORK THEORY AND COMPUTER SCIENCE, CODING THEORY, ...



$n=80$
deg$=3$

Largest known planar cubic Ramanujan graphs

FINALLY WE CONSIDER A DIOPHANTINE GEOMETRY PROBLEM OF A SIMILAR FLAVOR TO THE PREVIOUS BUT FOR WHICH AUTOMORPHIC FORMS METHODS DON'T APPLY. HOWEVER NEW TECHNIQUES BASED ON A "WEAK R.C", IE EXPANSION FOR RELATED ARITHMETIC GRAPHS IS CRITICAL.

INTEGRAL APOLLONIAN PACKINGS

Scale the picture by a factor of 252 and let
$a(c)$ = curvature of the circle $c = 1/\mathrm{radius}(c)$.

The curvatures are displayed. Note the outer one by convention has a negative sign.
By a theorem of Apollonius, place unique circles in the lines.

17

The Diophantine miracle is the curvatures are integers!

Repeat ad infnitum to get an integral Apollonian packing:

- There are infinitely many such P's.

Basic questions (Diophantine)
Which integers appear as curvatures?
Are there infinitely many prime curvatures, twin primes i.e. pairs of tangent circles with prime curvature?

- The structure (integral) F. Soddy (1936)
- Diophantine set up and questions

R. GRAHAM, J. LAGARIAS, C. MELLOWS, L. WILKS AND C. YAN (2000)

- MANY OF THE DIOPHANTINE PROBLEMS ARE NOW SOLVED THANKS TO RECENT ADVANCES IN SIEVE THEORY (AFFINE SIEVE), ERGODIC THEORY OF INFINITE VOLUME HYPERBOLIC MANIFOLDS AND THEIR SPECTRAL THEORY, GEOMETRY AND ADDITIVE COMBINATORICS

2006–2012, ...

LIST: S, GAMBURG, BOURGAIN, E. FUCHS, H. OH, KONTOROVICH, VARJU, SANDEN

ONE REMAINING BASIC QUESTION IS A LOCAL TO GLOBAL ONE

E. FUCHS (THESIS 2010): GIVES LOCAL OBSTRUCTIONS; ALL CURVATURES $a(C)$ for $C \in \mathcal{P}_0$ SATISFY

(*) $a(C) \equiv 0, 4, 12, 13, 16, 21 \pmod{24}$.

AND THESE ARE THE ONLY CONGRUENCE OBSTUCTIONS.

LOCAL TO GLOBAL CONJECTURE

EXCEPT FOR FINITELY MANY n's (AND THE LIST IS LARGE), EVERY n SATISFYING (*) IS A CURVATURE OF SOME $C \in \mathcal{P}_0$.

THE CONNECTION TO HILBERT'S 11-TH PROBLEM IS THAT THE n's CORRESPOND TO COORDINATES OF A "THIN" SUBGROUP OF AN ARITHMETIC GROUP ACTING ON A CONE. IF THIS GROUP WEREN'T THIN THEN THE ABOVE PROBLEM ~~WOULD~~ BECOMES AN INTEGRAL DIOPHANTINE EQUATION IN 3-VARIABLES!

ONE RECENT RESULT IS

THEOREM (BOURGAIN-KONTOROVICH 2012): THE SET OF n's FAILING TO SATISFY THE LOCAL TO GLOBAL PRINCIPLE ABOVE HAS ZERO DENSITY.

A CRITICAL INGREDIENT IN THE ANALYSIS IS A WEAK RAMANUJAN TYPE CONJECTURE THAT CAN BE ESTABLISHED FOR THIS THIN GROUP (BOURGAIN-GAMBURD-S).

(VARJU IN GENERAL).

SOME REFERENCES

S. RAMANUJAN "ON CERTAIN ARITHMETICAL FUNCTIONS" T.C.P.S. XXII, 1916, 159–184.

S. RAMANUJAN "ON THE EPRESSION OF A NUMBER IN THE FORM $ax^2+by^2+cz^2+du^2$" PROC. CAM. PHIL. SOC (TCPS) XIX, 1917, 11–21.

G.H. HARDY "RAMANUJAN: TWELVE LECTURES ON SUBJECTS SUGGESTED BY HIS LIFE AND WORKS" CHELSEA PUBL. (1999 EDITION).

A. WEIL "TWO LECTURES ON NUMBER THEORY; PAST AND PRESENT" COLLECTED WORKS 279–302, Vol III. (1974).

P. DELIGNE "LA CONJECTURE DE WEIL I" PUBL. IHES. 43 (1974) 273–307.

C.F. GAUSS SECTIONS 291–293 OF "DISQUESTIONES ARITHMETICAE" 1800.

D. HILBERT "MATHEMATICAL PROBLEMS" SEE B.A.M.S. (1902) 437-479.

H. HASSE 1923 THESIS; "UBER DE DARSTELLBARKEIT VON ZAHLEN DURCH QUADRATICHE FORMEN IN KORPER DER RATIONAL ZAHLEN".

W. DUKE and R. SCHUTZE-PILLOT "REPRESENTATION OF INTEGERS BY POSITIVE TERNARY QUADRATIC FORMS AND EQUIDISTRIBUTION OF LATTICE POINTS IN ELLIPSOIDS" INV. MATH. 99 (1990) 49-57.

K. ONO AND K. SOUNDARARAJAN "RAMANUJAN'S TERNARY QUADRATIC FORM" INV. MATH 130 (1997) 415-454.

J. COGDELL "ON SUMS OF THREE SQUARES" J. THEOR. NOM. BORDEAUX 15 (2003), 33-44.

A. LUBOTZKY, R. PHILLIPS, P. SARNAK "RAMANUJAN GRAPHS" COMBNITATORICA 8 (1988) 261-277.

G. MARGULIS "EXPLICIT GROUP THEORETIC CONSTRUCTIONS OF COMBINATORIAL SCHEMES AND THEIR APPLICATIONS FOR CONSTRUCTIONS OF EXPANDERS AND CONCETRATORS" JNL. PROBL. INFOR. TRANSMITION (1988).

R. GRAHAM, J. LAGARIAS, C. MALLOWS, A. WILKS, C. YAN "APOLLONIAN CIRCLE PACKINGS: NUMBER THEORY" JNL OF NO THEORY 100 (2003) 1-45.

P. SARNAK "INTEGRAL APOLLOMAN PACKINGS" AM. MATH MONTHLY 118 (2011) 291-306.