RANDOMNESS IN NUMBER THEORY

PETER SARNAK

SIMONS INSTITUTE BERKELEY

APRIL 15 2019

FROM PAUL COHEN'S PAPER (PHIL TRANS ROYAL SOC 2005,
"SKOLEM AND PESSIMISM ABOUT PROOF IN MATHEMATICS"

..... WITH LUCK, WE REACH A CONTRADICTION AND THEREBY PROVE SOMETHING. BUT SUPPOSE ONE ASKS AN UNNATURAL STATEMENT ABOUT PRIMES, SUCH AS THE TWIN PRIME QUESTION. PERHAPS ON THE BASIS OF STATISTICAL CONSIDERATIONS, WE EXPECT THE PRIMES TO SATISFY THIS LAW. BUT THE PRIMES SEEM RATHER RANDOM, AND IN ORDER TO PROVE THAT THE STATISTICAL HYPOTHESIS IS TRUE WE HAVE TO FIND SOME LOGICAL LAW THAT IMPLIES IT. IS IT NOT VERY LIKELY THAT, SIMPLY AS A RANDOM SET OF NUMBERS, THE PRIMES DO SATISFY THE HYPOTHESIS ....

THEREFORE, MY CONCLUSION IS THE FOLLOWING. I BELIEVE THAT THE VAST MAJORITY OF STATEMENTS ABOUT INTEGERS ARE TOTALLY AND PERMANENTLY BEYOND PROOF IN ANY REASONABLE SYSTEM. HERE I AM USING PROOF IN THE SENSE THAT MATHEMATICIANS USE THAT WORD. CAN STATISTICAL EVIDENCE BE REGARDED AS PROOF? I WOULD LIKE TO HAVE AN OPEN MIND AND SAY WHY NOT? IF THE FIRST TEN BILLION ZEROS OF THE ZETA FUNCTION LIE ON THE LINE WHOSE REAL PART IS 1/2, WHAT CONCLUSION SHALL WE DRAW? I FEEL INCOMPETENT EVEN TO SPECULATE ON HOW FUTURE GENERATIONS WILL REGARD NUMERICAL EVIDENCE OF THIS KIND. IN THIS PESSIMISTIC SPIRIT, I MAY CONCLUDE BY ASKING IF WE ARE WITNESSING THE END OF THE ERA OF PURE PROOF, BEGUN SO GLORIOUSLY BY THE GREEKS. I HOPE THAT MATHEMATICS LIVES FOR A VERY LONG TIME, AND THAT WE DO~~ES~~ NOT REACH THAT DEAD END FOR MANY GENERATIONS TO COME.

NUMBER THEORY	PROBABILITY THEORY
WHOLE NUMBERS	RANDOM OBJECTS
PRIME NUMBERS	GEOMETRIES
ARITHMETIC	MATRICES
	POLYNOMIALS
DIOPHANTINE EQUATIONS	⋮
⋮	WALKS
	GROUPS
	⋮
	PERCOLATION
AUTOMORPHIC FORMS	UNIVERSAL LAWS

DICHOTOMY: IN A TYPICAL NUMBER THEORETIC PROBLEM, EITHER THERE IS A RIGID ALGEBRAIC STRUCTURE (EG A FORMULA) OR THE ANSWER IS DIFFICULT TO DETERMINE AND IN THAT CASE IT IS RANDOM W.R.T SOME PROBABILISTIC LAW

- THE LAW CAN BE QUITE UNEXPECTED AND TELLIN
- ESTABLISHING THE LAW CAN BE VERY DIFFICULT AND IS OFTEN THE CENTRAL ISSUE.

THE RANDOMNESS PRINCIPLE HAS IMPLICATIONS IN BOTH DIRECTIONS.

$\Longrightarrow$ UNDERSTANDING AND PROVING THE LAW ALLOWS FOR A COMPLETE UNDERSTANDING OF A PHENOMENON.

$\Longleftarrow$ THE FACT THAT AN EXPLICIT ARITHMETICAL OR DIOPHANTINE PROBLEM BEHAVES RANDOMLY CAN BE OF GREAT PRACTICAL VALUE

EG: TO PRODUCE PSEUDO-RANDOM NUMBERS.

WE ILLUSTRATE THE DICHOTOMY WITH EXAMPLES

(A) $\pi = 3.14159265358979323846\ldots$

IS IT NORMAL? IT IS KNOWN THAT THAT π IS NOT TOO STRUCTURED, IT DOES NOT HAVE A PERIODIC DECIMAL, BUT WHILE IT IS SURELY NORMAL THIS SEEM HOPELESS TO PROVE

(B) ARITHMETIC AND QUADRATIC DIOPHANTINE EQUATIONS

PRIMES:

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~
~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~ 29
, ...,

ARE THEY RANDOM OR STRUCTURED?

$\pi(x) :=$ THE NUMBER OF PRIMES LESS THAN x.

PRIME NUMBER THEOREM (1896)

AS x GOES TO INFINITY, $\dfrac{\pi(x)\log x}{x} \rightarrow 1.$

GAUSS SUMS:

p AN ODD PRIME

$$g(p) = \sum_{x=0}^{p-1} e^{2\pi i x^2/p}$$

SINCE $e^{2\pi i m} = 1$ FOR $m \in \mathbb{Z}$, THE SUM TAKES PLACE FOR x IN ARITHMETIC MODULO p, THAT IS ONLY DEPENDS ON THE REMAINDER WHEN x IS DIVIDED BY p

$$\mathbb{F}_p := \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$$

WITH THE USUAL RULES OF ARITHMETIC IS A "FIELD"

$$g(p)^2 = \begin{cases} p & \text{IF } p \equiv 1(4) \\ -p & \text{IF } p \equiv 3(4) \end{cases}.$$

WHICH SQUARE ROOT IS IT?

GAUSS:

$$g(p) = \begin{cases} \sqrt{p} & p \equiv 1(4) \\ i\sqrt{p} & p \equiv 3(4) \end{cases}$$

From correspondence of Gauss to Le Blanc (= Sophie Germain) and Wilhelm Olbers.

This theorem is already hinted at in the *Disquisitiones Arithmeticae,* p. 636 or more precisely, only a special case of it, namely the one where n is a prime number, to which the others could be reduced. What is written there between *Quaecunque igitur radix etc.* and *valde sunt memoribilia,* is rigorously proved there, but what follows, i.e., the determination of the sign, is exactly what has tortured me all the time. This shortcoming spoiled everything else that I found; and hardly a week passed during the last four years where I have not made this or that vain attempt to untie that knot—especially vigorously during recent times. But all this brooding and searching was in vain, sadly I had to put the pen down again. Finally, a few days ago, it has been achieved—but not by my cumbersome search, rather through God's good grace, I am tempted to say. As the lightning strikes the riddle was solved; I myself would be unable to point to a guiding thread between what I knew before, what I had used in my last attempts, and what made it work. Curiously enough the solution now appears to me to be easier than many other things that have not detained me as many days as this one years, and surely no one whom I will once explain the material will get an idea of the tight spot into which this problem had locked me for so long. Now I cannot resist to occupy myself with writing up and elaborating on this material. However, my astronomical work should not be completely neglected all the same.

STRUCTURED ANSWERS:

CLOSELY RELATED IS HIS FAMOUS QUADRATIC RECIPROCITY:

p, q PRIMES $\equiv 1(4)$, THEN p HAS A SQUARE ROOT mod q IFF q HAS A SQURE ROOT mod p

THIS KIND OF STRUCTURED RECIPROCITY IS THE ORIGIN OF MODERN RECIPROCITIES, CLASS FIED THEORY AND LANGLANDS RECIPROCITY IN AUTOMORPHIC FORMS.

STICKING TO ARITHMETIC OF $\mathbb{F}_p$, AS x ADVANCES LINEARLY THROUGH $1, 2, \ldots, p-1$ HOW DO THE NUMBERS

$$x^{-1} \pmod{p}$$

ARRANGE THEMSELVE

EXCEPT FOR THE FIRST FEW ($1^{-1} = 1$) THERE APPEAR TO BE NO RULE FOR x^{-1}, $x \to x^{-1}$ LOOKS LIKE A RANDOM INVOLUTION.

ONE MEASURE IS:
$$S(a,p) = \sum_{x=1}^{p-1} e^{2\pi i a x/p} \cdot e^{2\pi i x^{-1}/p}$$

FACT: $|S(a,p)| \leq 2\sqrt{p}$.

THIS FOLLOWS FROM THE PROVEN "RIEMANN HYPOTHESIS" FOR CURVES OVER FINITE FIELDS!

THE FACT THAT THE OPERATION $x \to x^{-1} \pmod{p}$ IS IN THIS WAY PSEUDO-RANDOM IS AT THE SOURCE OF VARIOUS CONSTRUCTIONS.

RAMANUJAN GRAPHS:

THESE ARE EXPLICIT AND OPTIMALLY HIGHLY CONNECTED SPARSE GRAPHS ("EXPANDERS")

CONSTRUCTION: $p \equiv 1\ (20)$ PRIME

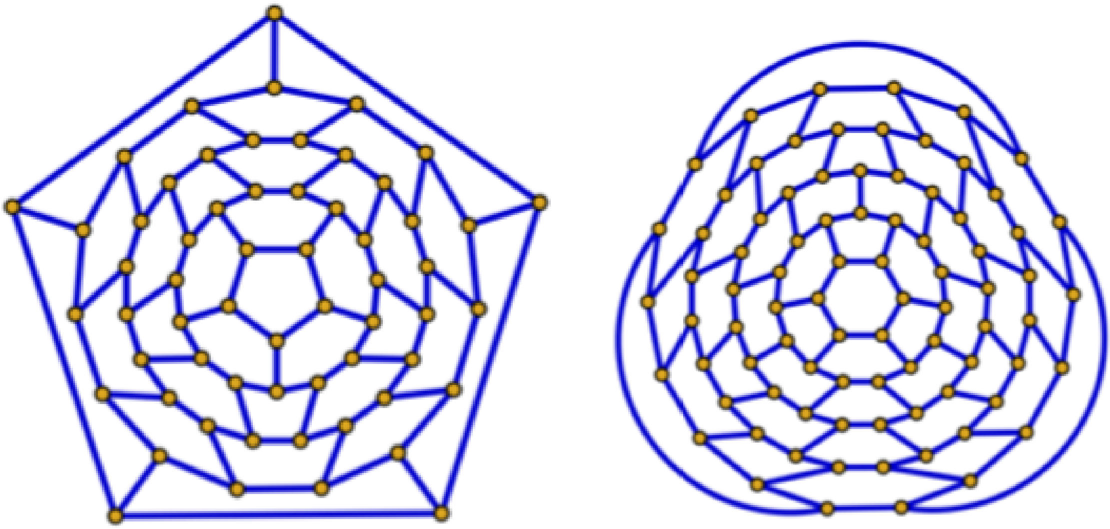
LET $1 \leq i \leq p-1$ SATISFY $i^2 \equiv -1\ (p)$ (RECIPROCIT

$1 \leq \beta \leq p-1$ SATISFY $\beta^2 = 5\ (p)$ (")

$$S = \left\{ \frac{1}{\beta}\begin{bmatrix} 1 \pm 2i & 0 \\ 0 & 1 \mp 2i \end{bmatrix}, \frac{1}{\beta}\begin{bmatrix} 1 & \pm 2 \\ \mp 2 & 1 \end{bmatrix}, \frac{1}{\beta}\begin{bmatrix} 1 & \pm 2i \\ \pm 2i & 1 \end{bmatrix} \right\}$$

A SET OF SIX MATRICES IN "$SL_2(\mathbb{F}_p)$", THE GROUP OF 2×2 MATRICES WITH DETERMINANT 1.

THE SIX REGULAR GRAPH V_p WHOSE VERTICES ARE THE MATRICES g IN $SL_2(\mathbb{F}_p)$ (THERE ARE ABOUT p^3 OF THEM) AND WHOSE EDGES RUN BETWEEN g AND sg WITH $s \in S$, IS A RAMANUJAN GRAPH.



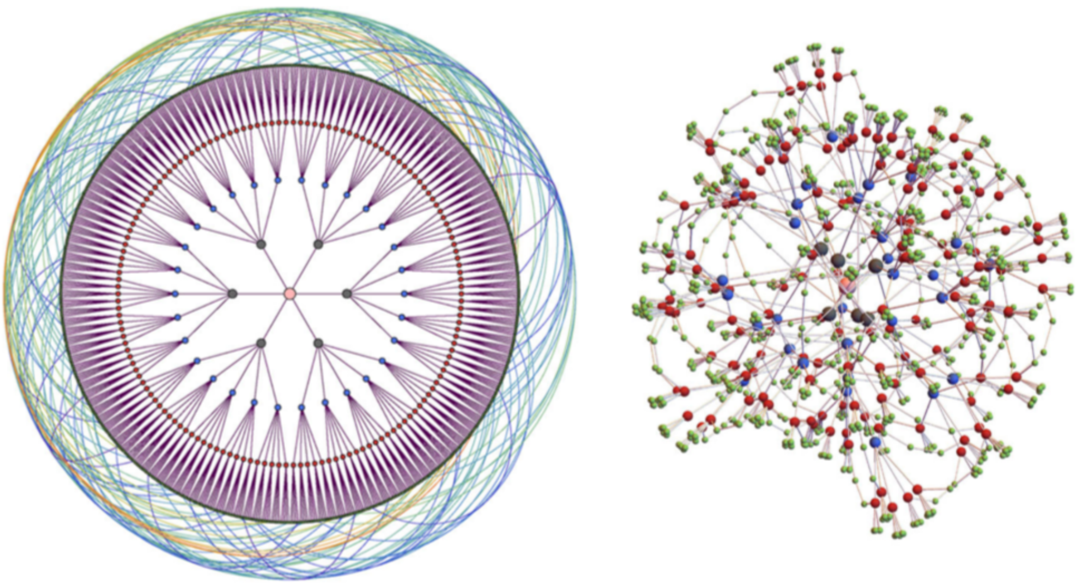


Figure 1: A ball of radius 4 in the Lubotzky–Phillips–Sarnak 6-regular Ramanujan graph on $n = 12{,}180$ vertices via $\mathrm{PSL}(2, \mathbb{F}_{29})$

(a) THEY HAVE OPTIMAL SPECTRAL EXPANSION PROPERTIES, ESSENTIALY OPTIMALLY SMALL DIAMETER

(b) ONE CAN NAVIGATE THE GRAPH EFFICIENTLY (POLYNOMIAL IN PATH LENGTH). IF g AND h ARE IN V_p AND $g^{-1}h$ IS DIAGONAL THEN ONE CAN FIND THE SHORTEST PATH FROM g TO h. IN GENERAL THIS ALLOWS US TO FIND A PATH WHICH IS THREE TIMES LONGER THAN OPTIMAL

(c) THE PROBLEM OF FINDING THE SHORTEST PATH FROM g TO h IN THESE GRAPHS IS NP-COMPLETE!

(•) THE FUNCTION FIELD RIEMANN HYPOTHESIS AND AUTOMORPHIC FORMS ARE CRUCIAL INGREDIENTS IN THE ANALYSIS.

(••) THE EXISTENCE OF (BIPARTITE) RAMANUJAN GRAPHS OF ANY DEGREE WAS ACHIEVED MORE RECENTLY USING IDEAS FROM STATISTICAL PHYSICS (LEE-YANG TYPE THEOREMS) AND INTERLACING POLYNOMIALS, THIS THEME IS ONE OF THE CENTRAL ONES IN THE POLYNOMIALS PROGRAM THIS SEMESTER

SIMILAR IDEAS CONNECTED WITH THE DIOPHANTINE ANALYSIS OF

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$$

(VIA GENERAL QUATERNION

LEADS TO THE CONSTRUCTION OF OPTIMAL UNIVERSAL GATES FOR QUANTUM COMPUTING "GOLDEN GATES".

	CLASSICAL	QUANTUM
1 BIT	$\{0,1\}$	$\psi \in \mathbb{C}^2$, $\lvert\psi\rvert^2 = 1$
n BITS	$\{0,1\}^n$	$(\mathbb{C}^2)^{\otimes n}$
1 BIT GATE	$\sim$	$\boxed{A}$ $A \in U(2)$ $A^* A = I$.
2 BIT GATE	$\wedge$	CNOT $\boxed{X}$ $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
UNIVERSAL	$\sim$, $\wedge$	CLIFFORD + T + CNOT

TEXT BOOK QUANTUM GATES:

1-QUBIT

HADAMARD	$\boxed{H}$	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
PHASE	$\boxed{S}$	$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\frac{\pi}{8}$ OR T	$\boxed{T}$	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

H AND S GENERATE A FINITE SUBGROUP OF $U(2)$ OF ORDER 24; THE CLIFFORD GROUP. ADDING T TO THESE YIELDS A UNIVERSAL SINGLE QUBIT GATE SET, WHICH IS OPTIMAL FOR APPROXIMATION AND NAVIGATION (IDENTICAL TO $SL_2(\mathbb{F}_p)$ FEATURES).

(C) Parity

One of the most elusive number theoretic functions, both theoretically and computationally, is $\lambda(n)$ the parity of the number of prime factors of n.

$$\lambda_3(n) = \text{parity of the number of prime factors } p \text{ dividing } n,\ p \equiv 3 \qquad (4)$$

$$\lambda_1(n) = \text{parity of the number of prime factors } p \text{ dividing } n,\ p \equiv 1 \qquad (4)$$

For n odd

n	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39
$\lambda_3(n)$	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1
$\lambda_1(n)$	1	1	−1	1	1	1	−1	−1	−1	1	1	1	1	1	−1	1	1	−1	−1	−1
$\lambda(n)$	1	−1	−1	−1	1	−1	−1	1	−1	−1	1	−1	1	−1	−1	−1	1	1	−1	1

- $\lambda_3(n)$ is clearly structured.
- $\lambda_1(n)$ and $\lambda(n)$ appear to be random.

It is expected that λ has no self correlations (no patterns have been observed), and as a consequence that λ is uncorrelated or "disjoint" from any sequence observed in a zero entropy dynamical system:

$$\frac{1}{N}\sum_{n\leqslant N}\lambda(n)f(n) \to 0 \quad \text{as } N \to \infty \text{ for such } f. \qquad (**)$$

MANY HARD EARNED THEOREMS ABOUT PRIME NUMBERS ESTABLISH SOME RANDOMNESS IN $\lambda(n)$ THROUGH INSTANCES OF (**) AS A CRUCIAL STEP.

FOR EXAMPLE (xx) FOR $f(n) \equiv 1$ IS EQUIVALENT TO THE PRIME NUMBER THEOREM

· THE QUANTITATIVE VERSION OF THE LAST IN TERMS OF THE (RANDOM) SQUARE ROOT CANCELLATION IS:

$$\left| \sum_{n \leq N} \lambda(n) \right| \leq C_\varepsilon N^{\frac{1}{2}+\varepsilon}, \quad \text{FOR } \varepsilon > 0$$

IS EQUIVALENT TO THE (REAL) RIEMANN HYPOTHESIS.

THE ISSUE HERE IS NOT THE OBVIOUS RANDOM WALK MODEL BUT TO PROVE SOMETHING TOWARDS THIS RANDOMNESS.

SO WHAT IS THIS RIEMANN HYPOTHESIS?

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p} \left(1 - p^{-s}\right)^{-1} \quad \text{FOR } \operatorname{Re}(s) > 1$$

RIEMANN SHOWS: $\Lambda(s) := \pi^{-s/2} \Gamma\left(\frac{s}{2}\right) \zeta(s)$.

EXTENDS TO AN ANALYTIC FUNCTION OF s IN THE COMPEX PLANE WITH SIMPLE POLES AT $s=0$ AND $s=1$ AND SATISFIES THE SYMMETRY

$$\Lambda(1-s) = \Lambda(s)$$

RIEMANN HYPOTHESIZES: THAT ALL THE ZEROS $\rho = \beta + i\gamma$ OF $\Lambda(s)$ ARE ON THE SYMMETRY LINE $\beta = \frac{1}{2}$

$$\leq -\gamma_j \leq \ldots -\gamma_2 < -\gamma_1 < 0 < \gamma_1 < \gamma_2 \ldots \leq \gamma_j \ldots$$

$\gamma_1 \simeq 14.21 \ldots$

THESE ZEROS DON'T OBEY ANY OBVIOUS FORMULA AND THE RANDOMNESS LAWS THAT GOVERN THEIR BEHAVIOR LIE DEEPER AND ARE SUGGESTIVE.

THE SCALED LOCAL SPACING STATISTICS OF THE γ_j'S FOLLOW PERFECTLY THE LAWS OF "GUE" THE GAUSSIAN UNITARY ENSEMBLE OF RANDOM MATRIX THEORY.

THIS SUGGESTS STRONGLY THAT THE ZEROS ARE EIGENVALUES OR ENERGY LEVELS.

THE ABOVE PHENOMENON TURNS OUT TO BE UNIVERSAL FOR THE ZEROS OF ALL ZETA FUNCTIONS OF AUTOMORPHIC FORMS. MOREOVER VERSIONS HAVE BEEN PROVEN FOR THE FUNCTION FIELD ANALOGUE WHICH HAS BEEN A VERY ACTIVE AND FRUITFUL AREA FOR THE LAST DECADE.

- THERE ARE 10 FAMILIES OF RANDOM MATRIX ENSEMBLES CORRESPONDING TO CARTAN'S 10 FAMILIES OF SYMMETRIC SPACES. APPARENTLY ONLY FOUR OF THESE (TYPE III) ARISE AS ZEROS OF ZETA'S (MONODROMY).

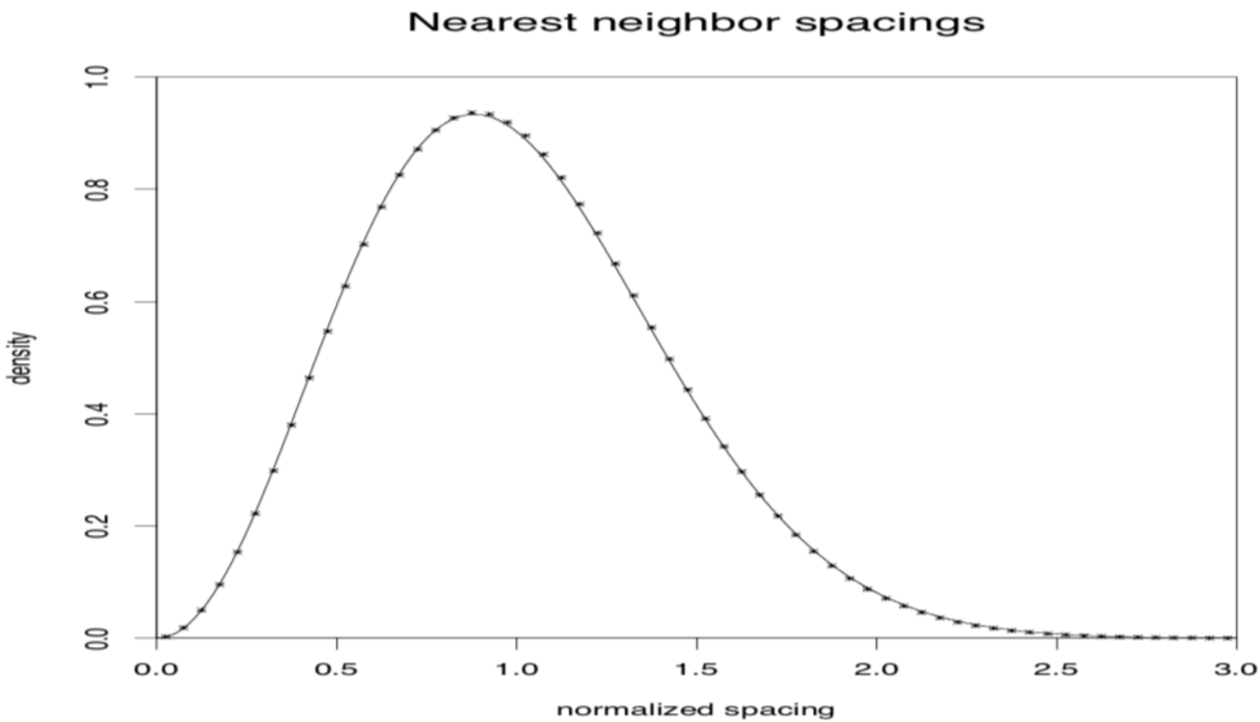


FIGURE 1. Probability density of the normalized spacings δ_n. Solid line: Gue prediction. Scatterplot: empirical data based on a billion zeros near zero # $1.3 \cdot 10^{16}$.

(D) MODULAR FORMS

MODULAR (OR AUTOMORPHIC) FORMS ARE A GOLD MINE WHICH IS AT THE CENTER OF MODERN NUMBER THEORY (FOR EXAMPLE THEY FEATURE CRUCIALLY IN THE PROOF OF FERMAT'S LAST THEOREM). A PAPER TITLED "THE UNREASONABLE EFFECTIVENESS OF MODULAR FORMS IN NUMBER THEORY" IS OVERDUE.

MY ARGUMENT WOULD BE THAT THEY VIOLATE OUR BASIC RANDOMNESS PRINCIPLE:

- THEY HAVE BOTH RIGID AND RANDOM FEATURES

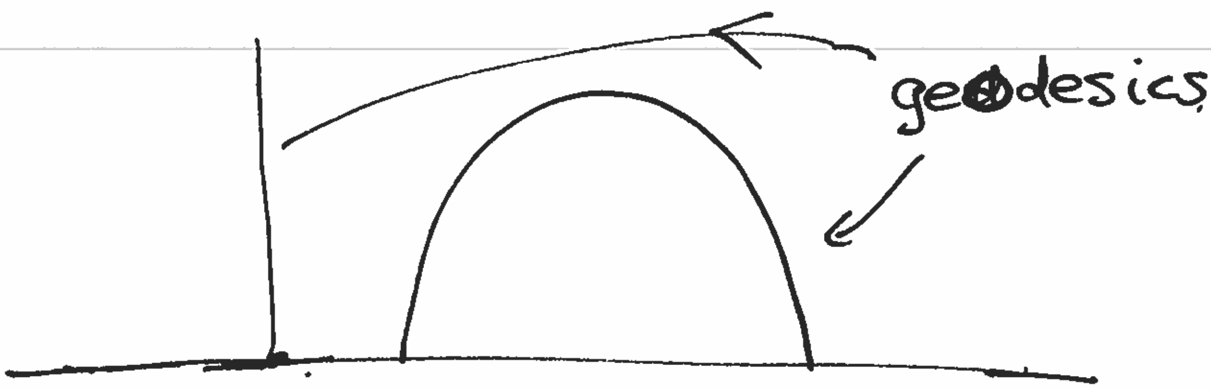
- THEY CANNOT BE WRITTEN DOWN EXPLICITLY (IN GENERAL) YET ONE CAN CALCULATE (PRIMARILY WITH THE TRACE FORMULA) WITH THEM ALMOST TO THE BITTER END AND EXTRACT PRECIOUS INFORMATION.

MODULAR FORMS ARE VIBRATIONAL MODES OF RIGID MEMBRANES / GEOMETRIES. MORE PRECISELY THEY ARE SIMULTANEOUS EIGENFUNCTIONS OF OPERATORS (INCLUDING DIFFERENTIAL) ON ARITHMETIC LOCALLY SYMMETRIC SPACES

THE MOST BASIC SETTING BEING

$\mathbb{H} = \{ z : \ \mathrm{Im}(z) > 0 \}$ THE NONEUCLIDEAN PLANE WITH LINE ELEMENT

$$ds = \frac{|dz|}{y}$$



$\Gamma = SL_2(\mathbb{Z})$ 2×2 INTEGRAL MATRICES WITH DETERMINANT 1.

ACTS ISOMETRICALLY ON $\mathbb{H}$ BY

$$z \overset{\gamma}{\longmapsto} \frac{az+b}{cz+d}, \ \gamma \in \Gamma$$

IDENTIFYING THE ORBITS OF POINTS EQUIVALENT UNDER Γ GIVES THE QUOTIENT $\mathbb{H}/\Gamma = X$ THE MODULAR SURFACE.

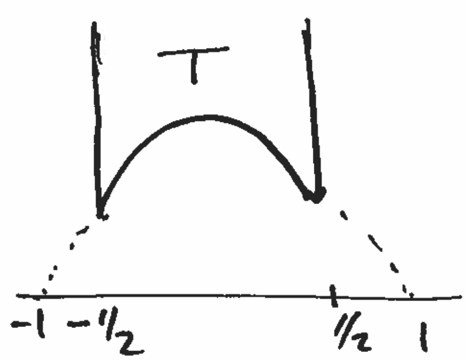
THE MODULAR FORMS ARE SOLUTIONS TO

$$\Delta\phi + \lambda\phi = 0 \,, \quad \phi(\gamma z) = \phi(z)$$

$$\Delta = y^2\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}\right)$$

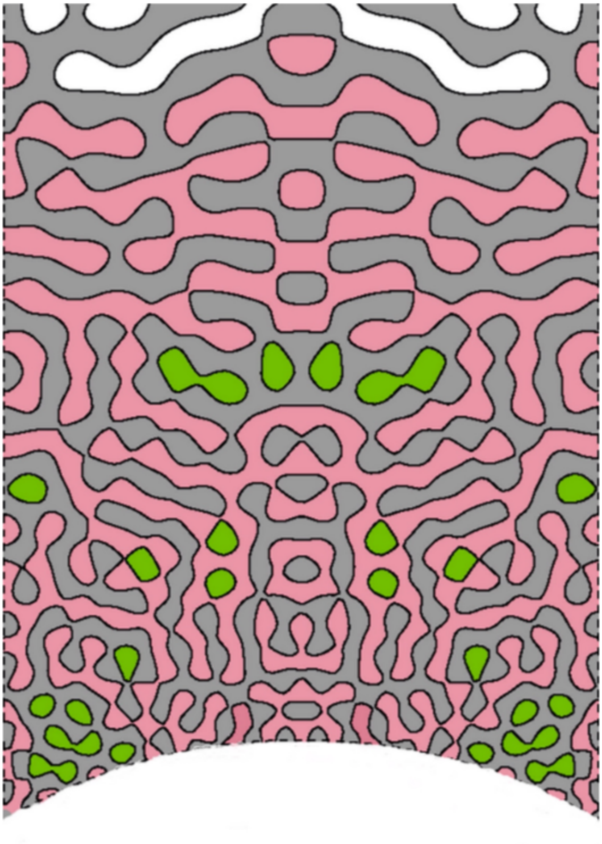
ϕ IS AN EIGEN-MODE OF A VIBRATING (HYPERBOLIC) TRIANGLE.

PHYSICALLY ONE CAN THINK OF THESE AS THE EIGENFUNCTIONS OF THE QUANTIZATION OF A HAMILTONIAN, WHICH IS THE CLASSICAL BILLIARD MOTION IN THE TRIANGLE T



THIS CLASSICAL MOTION IS CHAOTIC AND SO THE MODULAR FORMS ARE "EXPLICIT" MODES OF A CHAOTIC SYSTEM.

Nodal portrait



THERE ARE MANY RANDOM FEATURES THAT SUCH A ϕ_n (THE n-th MODE) EXHIBITS. WE DISCUSS THE NUMBER $N(\phi_n)$ OF NODAL DOMAINS.

FOR A RANDOM MONOCHROMATIC WAVE THE NUMBER SATISFIES

$$N(\phi_n) \sim c_2 n \qquad C_2 = 0.016\ldots$$

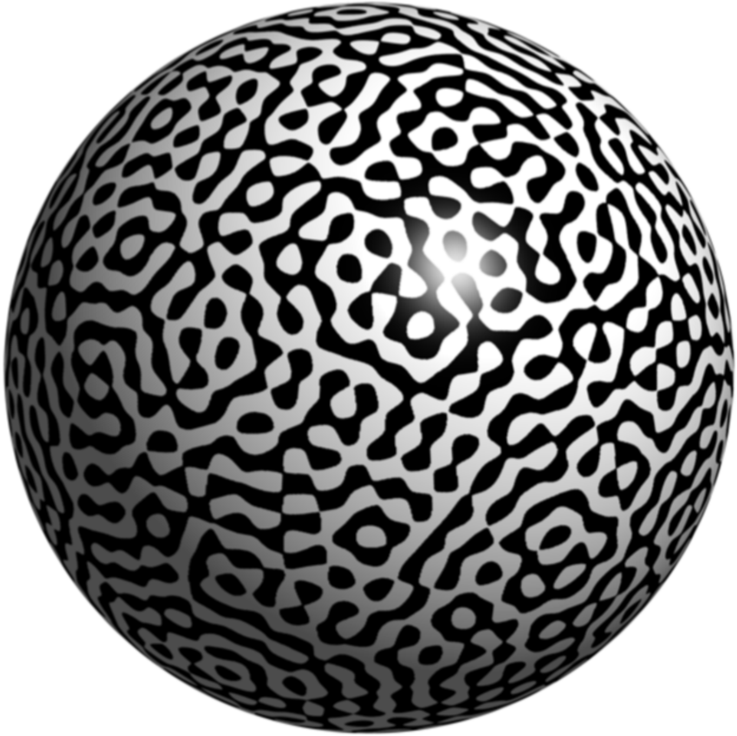
IN DIMENSION 2.

AND THE PERCETAGES OF CONNECTIVITIES OF THE NODAL DOMAINS IS

CONNECTIVITY	1	2	3	4	5	6	7	8
%	.906	.055	.010	.006	.003	.002	.001	.000[illegible]

THIS RANDOM MODEL AGREES HANDSOMELY WITH OUR 'EXPLICIT' ARITHMETIC MODULAR FORMS.

Nodal portrait: Random spherical harmonic ($\alpha = 1$)



random spherical harmonic of degree $= 80$. (A. Barnett)

PROVING SUCH LAWS IN A SPECIFIC SYSTEM, MEANS PROVING SOME RANDOMNESS AND IS OF COURSE VERY DIFFICULT. THERE HAS BEEN SOME PROGRESS RECENTLY

- USING ADVANCED NUMBER THEORETIC AND ERGODIC THEORY TOOLS $\Longrightarrow$

$$N(\phi_n) \to \infty \quad \text{AS} \quad n \to \infty \quad \text{FOR } X.$$

CONCLUSION:

• ESTABLISHING FULL RANDOMNESS LAWS THAT
APPLY TO NONSTRUCTURED NUMBER THEORETIC
PROBLEMS IS USUALLY VERY DIFFICULT. THE
PARTIAL RANDOMNESS THAT CAN BE ESTABLISH
INDIRECTLY VIA COMBINATORIAL AND STRUCTURED
FEATURES, IS OFTEN DECISIVE IN APPLICATIONS.

• PAUL & COHEN IS NO DOUBT CORRECT ABOUT
OUR NOT BEING ABLE TO SETTLE MOST OF
THE PROBLEMS THAT ONE MIGHT POSE IN NUMBER
THEORY. HOWEVER I DON'T SHARE HIS
PESSIMISM, SINCE WE MATHEMATICIANS
SEEM VERY GOOD AT SIFTING OUT THE
FUNDAMENTAL PROBLEMS THAT DRIVE THE
SUBJECT AND THESE ARE ONES THAT CAN BE
RESOLVED. SO HIS EXAMPLES OF TWIN PRIMES (UN-
NATURAL OR UNMOTIVATED "NON MOTIVIC" AS SERRE QUIPED)
AND THE RIEMANN HYPOTHESIS ARE ONES THAT I
(AND COHEN ON MOST DAYS) BELIEVE WILL BE SOLVED.
OUR SUBJECT IS VERY FAR FROM DRYING
UP, IN FACT WE ARE PRIVELAGED TO LIVE IN
A GOLDEN ERA OF MATHEMATICS WHEN SOME OF THESE
FUNDAMENTAL PROBLEMS WERE SOLVED

Some references

[1] Heath-Brown; D.R., Patterson, S.J., *The distribution of Kummer sums at prime arguments,* Journal für die reine und angewandte Mathematik 310 (1979)

[2] Lubotzky, A.; Phillips, R.; Sarnak, P., *Ramanujan graphs,* Combinatorica 8 (1988), no. 3, 261–277.

[3] Ross, Neil J.; Selinger, Peter, *Optimal ancilla-free Clifford+T approximation of z-rotations,* Quantum Inf. Comput. 16 (2016), no. 11–12, 901–953

[4] Katz, Nicholas M.; Sarnak, Peter, *Zeroes of zeta functions and symmetry,* Bull. Amer. Math. Soc. (N.S.) 36 (1999), no. 1, 1–26

[5] Odlyzko, A. M., *On the distribution of spacings between zeros of the zeta function,* Math. Comp. 48 (1987), no. 177, 273–308. (Reviewer: S. L. Segal) 11M26 (11-04 11Y35)

[6] 434 DOC. 45. QUANTUM THEOREM [p. 82] Doc. 45. *On the Quantum Theorem of Sommerfeld and Epstein* by A. Einstein (Presented at the session of May 11)

[7] Nazarov, Fedor; Sodin, Mikhail, *On the number of nodal domains of random spherical harmonics,* Amer. J. Math. 131 (2009), no. 5, 1337–1357

[8] Sardari, Naser T, *Complexity of strong approximation on the sphere,* `arXiv:1703.02709`

[9] Jang, Seung uk; Jung, Junehyuk, *Quantum unique ergodicity and the number of nodal domains of eigenfunctions,* J. Amer. Math. Soc. 31 (2018), no. 2, 303–318

A. MARCUS / D. SPIELMAN / N. SRIVASTAVA

"INTERLACING FAMILIES I: RAMANUJAN GRAPHS OF ALL DEGREES" ANN. MATH 182 (2015) 307-325

P. COHEN

"SKOLEM AND PESSIMISM ABOUT PROOF IN MATHEMATICS"

PHIL. TRANS. R. SOC. A (2005) 2407-2418.