Randomness in Number Theory*

Peter Sarnak

Number Theory	Probability Theory
Whole numbers	Random objects
Prime numbers	Points in space
Arithmetic operations	Geometries
Diophantine equations	Matrices
⋮	Polynomials
⋮	Walks
⋮	Groups
⋮	⋮
Automorphic forms	Percolation theory

Number theoretic dichotomy: Either there is a rigid structure (e.g. a simple closed formula) in a given problem, or the answer is difficult to determine and in that case it is random according to some probabilistic law.

- The probabilistic law can be quite unexpected and telling.
- Establishing the law can be very difficult and is often the central issue.

The randomness principle has implications in both directions.

$\Rightarrow$ Understanding and proving the law allows for a complete understanding of a phenomenon.

$\Leftarrow$ The fact that a very explicit arithmetical problem behaves randomly is of great practical value.

Examples:

- To produce pseudo-random numbers,
- Construction of optimally efficient error correcting codes and communication networks,
- Efficient derandomisation of probabilistic algorithms "expanders".

Illustrate the Dichotomy with examples.

0. Is $\pi = 3.14159265358979323\ldots$ a Normal Number?

π is far from rational;

*Slides from the Mahler Lectures 2011

Mahler (1953):

$$\left|\pi - \frac{p}{q}\right| > q^{-42}, \quad p,q \geqslant 2\,.$$

1. In Diophantine Equations

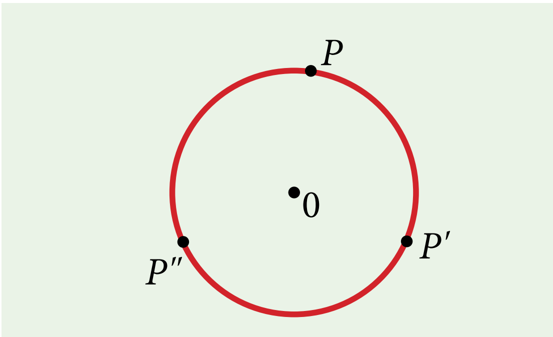
A bold conjecture: Bombieri–Lang takes the dichotomy much further. If V is a system of polynomial equations with rational number coefficients ("a smooth projective variety defined over $\mathbb{Q}$"), then all but finitely many rational solutions arise from ways that we know how to make them (parametric, special subvarieties, group laws …)

2. A Classical Diophantine Equations

Sums of three squares: for $n > 0$, solve

$$x^2 + y^2 + z^2 = n\,; \quad x,y,z \in \mathbb{Z}\,.$$

If $P = (x,y,z)$, $d^2(P,0) = n$.

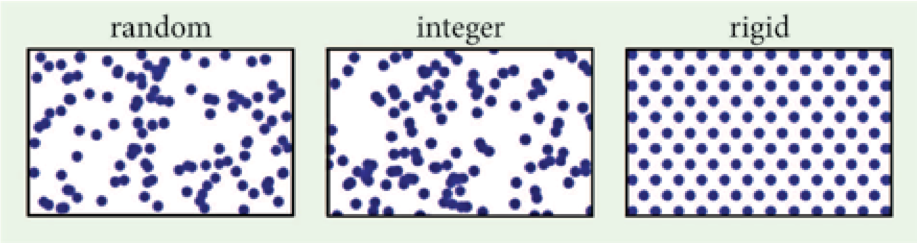


Points P, P' and P'' at distance $\sqrt{n}$ from the origin D.

$\mathcal{E}(n)$:= sets of solutions.
Examples: for $n = 5$, the P's are

$$(\pm 2, \pm 1, 0),\ (\pm 1, \pm 2, 0),\ (\pm 2, 0, \pm 1),$$
$$(\pm 1, 0, \pm 2),\ (0, \pm 2, \pm 1),\ (0, \pm 1, \pm 2),$$

$N(n) := \#\mathcal{E}(n)$, the cardinality of $\mathcal{E}(n)$, that is the number of solutions, so $N(5) = 24$.
$N(n)$ is not a random function of n but it is difficult to understand.



Projections of lattice points coming from the prime $n = 1299709$ (center), versus random points (left) and rigid points (right). The plot displays an area containing about 120 points.

If random, this sum of $p-1$ complex numbers of modulus 1 should cancel to about size $\sqrt{p}$.

Fact:

$$|S(1,p)| \le 2\sqrt{p}. \quad [15]$$

Gauss/Legendre (1800): $N(n) > 0$ iff $n \ne 4^a(8b+7)$. (This is a beautiful example of a local to global principle.)

$N(n) \approx \sqrt{n}$ (if not zero).
Project these points onto the unit sphere

$$P = (x,y,z) \mapsto \frac{1}{\sqrt{n}}(x,y,z) \in S^2 .$$

We have no obvious formula for locating the P's and hence according to the dichotomy they should behave randomly. It is found that they behave like N randomly placed points on S^2.

- One can prove some of these random features.
- It is only in dimension 3 that the $\hat{\mathcal{E}}(n)$'s are random. For dimensions 4 and higher, the distances between points in $\hat{\mathcal{E}}(n)$ have "explicit" high multiplicities. For 2 dimensions there aren't enough points on a circle — not random.

3. Examples from Arithmetic

p is a (large) prime number. Do arithmetic in the integers keeping only the remainders when divided by p. This makes $\{0,1,\ldots,p-1\} := \mathbb{F}_p$ into a finite field.

Now consider $x = 1,2,3,\ldots,p-1$ advancing linearly. How do $\bar{x} := x^{-1} \pmod{p}$ arrange themselves? Except for the first few, there is no obvious rule, so perhaps randomly?

Experiments show that this is so. For example, statistically, one finds that $x \mapsto \bar{x}$ behaves like a random involution of $\{1,2,\ldots,p-1\}$.

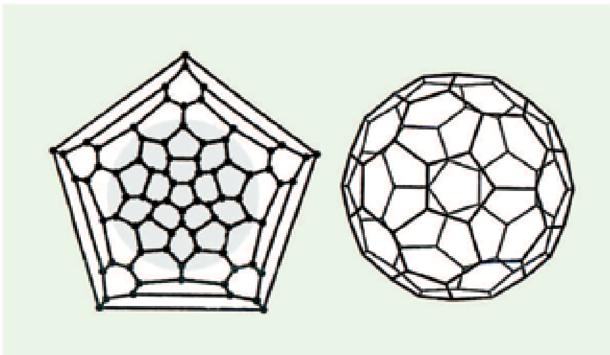
One of the many measures of the randomness is the sum

$$S(1,p) = \sum_{x=1}^{p-1} e^{2\pi i(x+\bar{x})/p}.$$

Follows from the "Riemann hypothesis for curves over finite fields". The fact that arithmetic operations such as $x \mapsto \bar{x} \pmod{p}$ are random is at the source of many pseudo-random constructions.

Examples:

Ramanujan Graphs: These are explicit and optimally highly connected sparse graphs (optimal expanders).



$n = 80, \ \deg = 3$

Largest known planar cubic Ramanujan graphs

Arithmetic construction:
$q \equiv 1 \pmod{20}$ prime

$$1 \le i \le q-1\,; \quad i^2 \equiv -1 \pmod{q}$$
$$1 \le \beta \le q-1\,; \quad \beta^2 \equiv 5 \pmod{q}$$

S the six 2×2 matrices with entries in $\mathbb{F}_q$ and of determinant 1.

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

Let V_q be the graph whose vertices are the matrices $A \in SL_2(\mathbb{F}_q)$, $|V_q| \sim q^3$, and edges run between g and sg with $s \in S$ and $g \in V_q$.

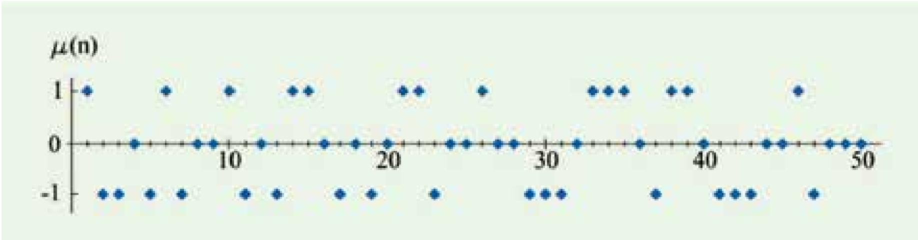
V_q is optimally highly connected, 6 regular graph on $|SL_2(\mathbb{F}_q)|$ vertices, an optimal expander. Here artihmetic mimics or even betters random.

4. The Möbius Function

$$n \geq 1, \quad n = p_1^{e_1} p_2^{e_2} \cdots P_k^{e_k}$$

$$\mu(n) = \begin{cases} 0 & \text{if } e_j \geq 2 \text{ for some } j, \\ (-1)^k & \text{otherwise.} \end{cases}$$

n	1	2	3	4	5	6	7	8	9	10
$\mu(n)$	1	−1	−1	0	−1	1	−1	0	0	1



Graph of values of $\mu(n)$.

Is $\mu(n)$ random? What laws does it follow. There is some structure, e.g. from the squares

$$\mu(4k) = 0 \quad \text{etc.}$$

One can capture the precise structure/randomness of $\mu(n)$ via dynamical systems, entropy, ...

The simplest question is to think of a random walk on $\mathbb{Z}$ moving to the right by 1 if $\mu(n) = 1$, to the left if $\mu(n) = -1$, and sticking if $\mu(n) = 0$. After N steps?

$$A(N) = \frac{1}{N} \sum_{n \leq N} \mu(n), \quad N \leq 100\,000; \text{ see graph below}$$

$$\left| \sum_{n \leq N} \mu(n) \right| \ll_\varepsilon N^{1/2+\varepsilon}, \quad \varepsilon > 0?$$

This is equivalent to the Riemann hypothesis! So in this case establishing randomness is one of the central unsolved problems in mathematics.

One can show that for any A fixed and N large,

$$\left| \sum_{n \leq N} \mu(n) \right| \leq \frac{N}{(\log N)^A}.$$

5. The Riemann Zeta Function

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}, \quad s > 1$$

it is a complex analytic function of s (all s).

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}.$$

Riemann Hypothesis: All the nontrivial zeros ρ of $\zeta(s)$ have real part 1/2. Write $\rho = 1/2 + i\gamma$ for the zeros.

$\gamma_1 = 14.21\ldots$ Riemann

and the first 10^{10} zeros are known to satisfy RH.

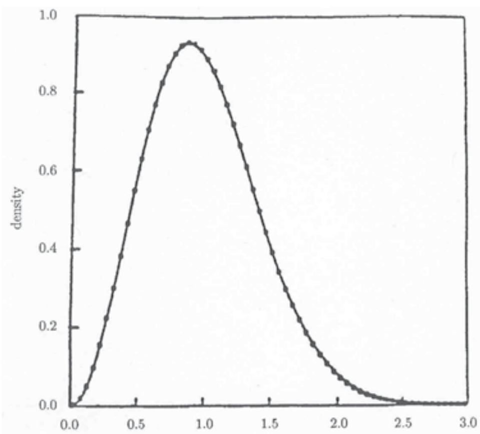
$$0 < \gamma_1 \leq \gamma_2 \leq \gamma_3 \ldots$$

Are the γ_j's random?

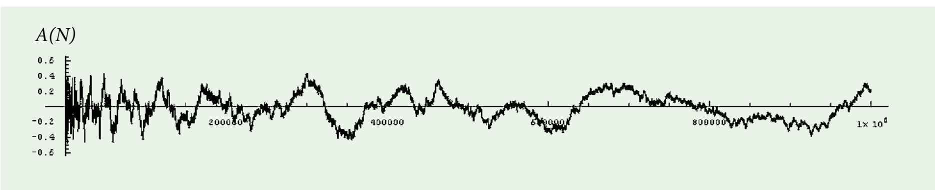
Scale first so as to form meaningful local statistics

$$\hat{\gamma}_j := \frac{\gamma_j \log \gamma_j}{2\pi}, \text{ these have unit mean spacing}.$$

$\hat{\gamma}_j$, $j = 1, 2, \ldots$ do not behave like random numbers but rather like eigenvalues of a random (large) hermitian matrix! <u>GUE</u> (Gaussian Unitary Ensemble).



Nearest neighbour spacings among 70 million zeroes beyond the 10^{20}-th zero of zeta, versus μ_1 (GUE), see [12].

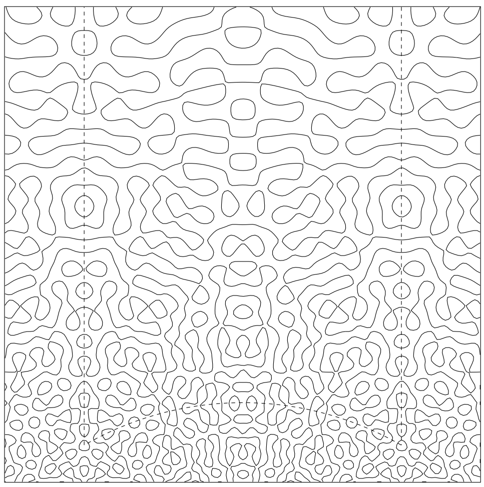


Graph of the average of $\mu(n)$ up to N.

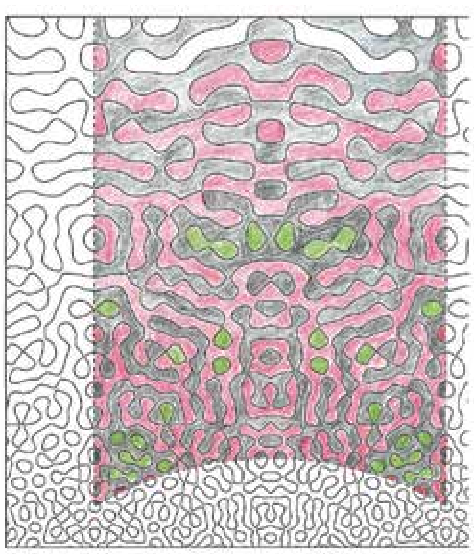
6. Modular Forms

Modular (or automorphic) forms are a goldmine and are at the centre of modern number theory. I would like to see an article "The Unreasonable Effectiveness of Modular Forms in Number Theory". Why are they so? I think it is because they violate our basic principle.

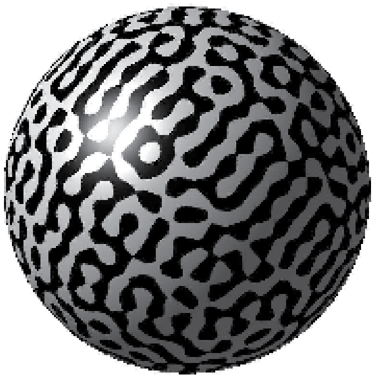
- They have many rigid and many random features.
- They cannot be written down explicitly (in general).
- But one can calculate things associated with them to the bitter end, sometimes enough to extract precious information.



Hejhal–Rackner nodal lines for $\lambda = 1/4 + R^2$, $R = 125.313840$



Hejhal–Rackner nodal domains for $\lambda = 1/4 + R^2$, $R = 125.313840$



Nodal domains for a random spherical harmonic of degree 40 [A Barnett].

On the left is the nodal set $\{\phi = 0\}$ of a highly excited modular form for $SL_2(\mathbb{Z})$.

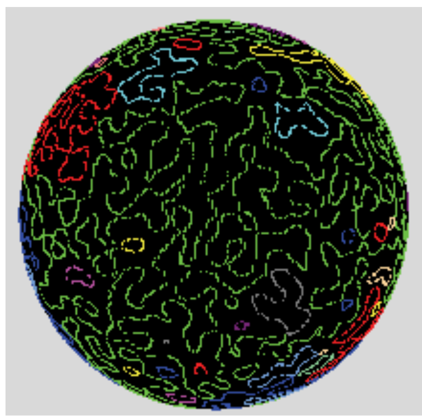
$$\Delta\phi + \lambda\phi = 0, \quad \lambda = \frac{1}{4} + R^2 .$$

$\phi(z)$ is $SL_2(\mathbb{Z})$ periodic. Is the zero set behaving randomly? How many components does it have? The physicists Bogomolny and Schmit (2002) suggest that for random waves

$$N(\phi_n) = \text{The number of components} \sim cn$$

$c = \frac{3\sqrt{3}-5}{\pi}$, comes from an exactly solvable critical percolation model!

- The modular forms apparently obey this rule. Some of this but much less can be proven.
- These nodel lines behave like random curves of degree $\sqrt{n}$.



A random real plane curve of degree 50 [M. Nastasescu].

7. Randomness and Algebra?

How many ovals does a random real plane projective curve of degree t have?

Harnack: The number of ovals $\leq \frac{(t-1)(t-2)}{2} + 1$

Answer: the random curve is about 4% Harnack, # of ovals $\sim c't^2$, $c' = 0.0182\ldots$ (Nazarov–Sodin, Nastasescu).

References

[1] E. Bogomolny and C. Schmit, *Phys. Rev. Letter* **80** (2002) 114102.
[2] E. Bombieri, The Riemann Hypothesis, claymath.org.
[3] J. Bourgain, Z. Rudnick and P. Sarnak, Local statistics of lattice points on the sphere, anXiv:1204.0134 (2012).
[4] C. F. Gauss, *Disquitiones Arithmeticae*, Sections 291–293.
[5] D. Hejhal and B. Rackner, *Exp. Math.* **1** (1992) 275–305.
[6] S. Hoory, N. Linial and A. Wigderson, Expander graphs and their applications, *BAMS* **43** (2006) 439–561.
[7] T. Kotnik and J. van de Lune, On the order of the Mertens function, *Exp. Math.* **13** (2004) 473–481.
[8] R. Lubotzky, R. Phillips and P. Sarnak, Ramanujan graphs, *Combinatorica* **8** (1988) 261–277.
[9] K. Mahler, *Indag. Math.* **15** (1953) 30–42.
[10] M. Nastasescu, The number of ovals of a real plane curve, Senior thesis, Princeton (2011).
[11] F. Nazarov and M. Sodin, *Am. J. Math.* **131** (2009) 1337–1357.
[12] A. Odlyzko, The 10^{20}-th zero of the Riemann zeta function and its million nearest neighbours, *A.T.T.* (1989).
[13] P. Sarnak, Three lectures on the Mobius function, randomness and dynamics, publications.ias.edu/sarnak/paper/512.
[14] P. Sarnak, Letter to B. Gross and J. Harris on ovals of random plane curves, publications.ias.edu/ sarnak/paper/510 (2011).
[15] A. Weil, *Proc. Nat. Acad. Sci. USA* (1948) 204–207.

Peter Sarnak
Institute of Advanced Study, USA
sarnak@math.ias.edu

Peter Sarnak obtained his PhD from Stanford University. He has been Eugune Higgins Professor of Mathematics at Princeton University since 2002. He is also on the permanent faculty at the School of Mathematics of the Institute for Advanced Study. Sarnak has made major contributions to number theory and to questions in analysis motivated by number theory. His interest in mathematics is wide-ranging, and his research focuses on the theory of zeta functions and automorphic forms with applications to number theory, combinatorics, and mathematical physics. His rewards include George Pólya Prize 1998, Ostrowski Prize 2001, Levi L Conant Prize 2003 and Frank Nelson Cole Prize 2005.