Randomness in Number Theory

Peter Sarnak
Mahler Lectures 2011
<table>
<thead>
<tr>
<th>Number Theory</th>
<th>Probability Theory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whole numbers</td>
<td>Random objects</td>
</tr>
<tr>
<td>Prime numbers</td>
<td>Points in space</td>
</tr>
<tr>
<td>Arithmetic operations</td>
<td>Geometries</td>
</tr>
<tr>
<td>Diophantine equations</td>
<td>Matrices</td>
</tr>
<tr>
<td>:</td>
<td>Polynomials</td>
</tr>
<tr>
<td>:</td>
<td>Walks</td>
</tr>
<tr>
<td>:</td>
<td>Groups</td>
</tr>
<tr>
<td>Automorphic forms</td>
<td>Percolation theory</td>
</tr>
</tbody>
</table>
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.
⇒ Understanding and proving the law allows for a complete understanding of a phenomenon.
⇐ 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 derandomization of probabilistic algorithms “expanders”.

Peter Sarnak Mahler Lectures 2011
Randomness in Number Theory
Illustrate the Dichotomy with Examples

(0) Is $\pi = 3.14159265358979323 \ldots$ a normal number?
$\pi$ is far from rational;
Mahler (1953): $\left| \pi - \frac{p}{q} \right| > q^{-42}$.

(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 …)
“The ignorance conjecture”
(2) A classical diophantine equation

Sums of three squares: for \( n > 0 \), solve

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

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

\[ \mathcal{E}(n) := \text{set of solutions.} \]

E.g. for \( n = 5 \), the \( P \)'s are

\[ (\pm 2, \pm 1, 0), (\pm 1, \pm 2, 0), (\pm 2, 0, \pm 1), \]
\[ (\pm 1, 0, \pm 2), (0, \pm 2, \pm 1), (0, \pm 1, \pm 2) \]

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

Gauss/Legendre (1800): \( N(n) > 0 \) iff \( n \neq 4^a(8b + 7) \).
(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 \( S^2 \).
Figure 1. 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.
One can prove some of these random features.

- It is only in dimension 3 that the $\tilde{E}(n)$’s are random. For dimensions 4 and higher, the distances between points in $\tilde{E}(n)$ have ‘explicit’ high multiplicities. For 2 dimensions there aren’t enough points on a circle — not random.

(3) **Examples from Arithmetic:**

$P$ 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 \( \overline{x} := x^{-1} \pmod{p} \) 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 \( x \mapsto \overline{x} \) behaves like a random involution of \( \{1, 2, \ldots, p - 1\} \).

One of the many measures of the randomness is the sum

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

If random, this sum of \( p - 1 \) complex numbers of modulus 1 should cancel to about size \( \sqrt{p} \).
Fact: \(|S(1, p)| \leq 2\sqrt{p}\). (A. Weil 1948)
Follows from the “Riemann hypothesis for curves over finite fields”. The fact that arithmetic operations such as \(x \mapsto \overline{x} \pmod{p}\) are random are at the source of many pseudo-random constructions: e.g.

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

Largest known planar cubic Ramanujan graphs

\(n = 80\)
\(\text{deg} = 3\)
Arithmetic construction:
\( q \equiv 1 \pmod{20} \) prime

\[
1 \leq i \leq q - 1 \quad ; \quad i^2 \equiv -1 \pmod{q}
\]

\[
1 \leq \beta \leq q - 1 \quad ; \quad \beta^2 \equiv 5 \pmod{q}
\]

\( S \) the six \( 2 \times 2 \) matrices with entries in \( \mathbb{F}_q \) and of determinant 1.

\[
S = \left\{ \frac{1}{\beta} \begin{bmatrix} 1 \pm 2i & \phantom{-}0 \\ 0 & 1 \mp 2i \end{bmatrix}, \quad \frac{1}{\beta} \begin{bmatrix} 1 & \pm 2 \\ \mp 2 & 1 \end{bmatrix}, \quad \frac{1}{\beta} \begin{bmatrix} 1 & \pm 2i \\ \pm 2i & 1 \end{bmatrix} \right\}
\]

Let \( V_q \) be the graph whose vertices are the matrices \( A \in \text{SL}_2(\mathbb{F}_q) \), \( |V_q| \sim q^3 \), 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 $|\text{SL}_2(\mathbb{F}_q)|$ vertices, optimal expander. Here arithmetic mimics or even betters random.

(4) **The Möbius Function**

\[
n \geq 1, \quad n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}
\]

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

<table>
<thead>
<tr>
<th>$n$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mu(n)$</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>0</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
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, . . . .

Very simplest question thinking 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?
\[ \frac{1}{N} \sum_{n \leq N} \mu(n), \quad N \leq 100\,000 \]

Is

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

This 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 \( \rho \) of \( \zeta(s) \) have real part 1/2. Write \( \rho = 1/2 + i\gamma \) for the zeros.

\[ \gamma_1 = 14.21 \ldots \quad \text{(Riemann)} \]

and the first \( 10^{10} \) zeros are known to satisfy RH.
$0 < \gamma_1 \leq \gamma_2 \leq \gamma_3 \ldots$

Are the $\gamma_j$’s random?
Scale first so as to form meaningful local statistics

$$\hat{\gamma}_j := \frac{\gamma_j \log \gamma_j}{2\pi}$$

$\hat{\gamma}_j, j = 1, 2, \ldots$ don’t behave like random numbers but rather like eigenvalues of a random (large) hermitian matrix! GUE

Nearest neighbor spacings among 70 million zeroes beyond the $10^{20}$-th zero of zeta, versus $\mu_1(GUE)$
(6) **Modular Forms**

Modular (or automorphic) forms are a goldmine and are at the center of modern number theory. I would like to see an article “The Unreasonable Effectiveness of Modular Forms”

Who 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 mine precious information.
Below is the nodal set \( \{ \phi = 0 \} \) of a highly excited modular form for \( \text{SL}_2(\mathbb{Z}) \).

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

\( \phi(z) \) is \( \text{SL}_2(\mathbb{Z}) \) periodic. Is the zero behaving randomly? How many components does it have?

Hejhal–Rackner nodal lines for \( \lambda = 1/4 + R^2, \ R = 125.313840 \)
Hejhal–Rackner nodal lines for $\lambda = 1/4 + R^2$, $R = 125.313840$
The physicists Bogomolny and Schmit (2002) suggest that for random waves

\[ N(\phi_n) = \# \text{ of components } \sim cn \]

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

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

(7) **Randomness and Algebra?**
How many ovals does a random real plane projective curve of degree \( t \) have?

Harnack: \( \# \text{ of ovals} \leq \frac{(t-1)(t-2)}{2} + 1 \)

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


