The Riemann Hypothesis

Winnie Li

Pennsylvania State University, U.S.A.
National Center for Theoretical Sciences, Taiwan

Primes

Primes in $\mathbb{Z}$ are $2, 3, 5, 7, 11, ...$

Theorem There are infinitely many prime numbers.

Proof 1 (Euclid). Suppose there were only finitely many, call them $p_1, p_2, ..., p_n$. Consider

$$N = p_1 p_2 \cdots p_n + 1.$$

Either it is a prime, or it is divisible by a prime. Either way, we have found a new prime, a contradiction.

Proof 2. The series $\sum_p \frac{1}{p}$ diverges.

The distribution of primes

Let $\pi(x) =$ the number of primes $p \leq x$.

Gauss in a letter of 1849 stated:

$$\pi(x) \sim Li(x) : \quad = \int_2^x \frac{1}{\log t} dt$$
$$= \frac{x}{\log x} + \frac{1!x}{(\log x)^2} + \frac{2!x}{(\log x)^3} + \cdots .$$

This means that the primes have density $\frac{1}{\log x}$ for x large, or equivalently,

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1.$$

Prime Number Theorem $\pi(x) \sim \frac{x}{\log x}$ for x large.

First proved by Hadamard and de la Vallée Poussin independently in 1896 using complex analysis, Selberg and Erdös gave an "elementary" proof in 1949, shortest proof was given by D. Newman in 1980.

A very rough sketch given by T. Tao:

Listen to the "music" of the primes. We start with a "sound wave" that is "noisy" at the prime numbers and silent at other numbers; this is the von Mangoldt function. Then we analyze its notes or frequencies by subjecting it to a process akin to Fourier transform; this is the Mellin transform. Then we prove, and this is the hard part, that certain "notes" cannot occur in this music. This exclusion of certain notes leads to the statement of the prime number theorem.

The Riemann Zeta Function

In calculus we learned that the series

$$\sum_{n=1}^{\infty} \frac{1}{n^{\sigma}}$$

converges (absolutely) if $\sigma > 1$ and diverges if $\sigma \leq 1$. This is seen from the integral test:

$$\sum_{n=1}^{\infty} \frac{1}{n^{\sigma}} > \int_{1}^{\infty} \frac{1}{x^{\sigma}} dx > \sum_{n=2}^{\infty} \frac{1}{n^{\sigma}}.$$

Using integration by parts, one can show that

$$\sum_{n=1}^{\infty} \frac{1}{n^{\sigma}} - \int_{1}^{\infty} \frac{1}{x^{\sigma}} dx = 1 + \int_{1}^{\infty} (x - [x])(\frac{1}{x^{\sigma}})' dx.$$

So for $\sigma > 1$ we get

$$\sum_{n=1}^{\infty} \frac{1}{n^\sigma} - \frac{1}{\sigma - 1} = 1 - \sigma \int_1^\infty (x - [x]) x^{-\sigma-1} dx. \qquad (1)$$

Since $1 > x - [x] \geq 0$, the last integral converges for $\sigma > 0$.

The Riemann zeta function is defined in the complex variable s:

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s},$$

which converges absolutely for $\Re s > 1$ to a holomorphic function, and (1) shows that (after replacing σ by s) it can be continued analytically to $\Re s > 0$, holomorphic everywhere except for a simple pole at $s = 1$.

Properties of $\zeta(s)$

In his memoir published in 1860, Riemann proved:

(a) The function $\zeta(s)$ can be analytically continued to the whole s-plane, holomorphic everywhere except for a simple pole with residue 1 at $s = 1$;

(b) $\zeta(s)$ satisfies the functional equation

$$\Lambda(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s) = \Lambda(1-s).$$

Consequences:

$$\zeta(s) = \sum_{n \geq 1} n^{-s} = \prod_{p \text{ prime}} (1 + p^{-s} + p^{-2s} + \cdots)$$

$$= \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}} \qquad \text{for } \Re s > 1.$$

- $\zeta(s) \neq 0$ on $\Re s > 1$.
- $\Gamma(s) \neq 0 \Rightarrow \zeta(s) \neq 0$ on $\Re s > 1$ and $\Re s < 0$.
- $\Gamma(s)$ has simple poles at $s = 0, -1, -2, ... \Rightarrow \zeta(s) = 0$ at $s = -2, -4, ...$, called *trivial zeros* of $\zeta(s)$.
- $\zeta(s) \neq 0$ on the line $\Re s = 1$, and hence on $\Re s = 0$. So the remaining *nontrivial zeros* of $\zeta(s)$ lie in the critical strip $0 < \Re s < 1$.

Conjectures of Riemann

(a') $\zeta(s)$ has infinitely many nontrivial zeros in the critical strip, they are symmetrical w.r.t. the real axis and the vertical line $\Re s = 1/2$. In fact, the number of zeros $N(T)$ of $\zeta(s)$ in the critical strip with $0 < \Im s \leq T$ satisfies

$$N(T) = \frac{T}{2\pi} \log \frac{T}{2\pi} - \frac{T}{2\pi} + O(\log T).$$

(b') **Riemann Hypothesis**: All nontrivial zeros of $\zeta(s)$ lie on the line $\Re(s) = 1/2$.

(c') Explicit formula for $\pi(x)$, relating the distribution of primes in terms of the nontrivial zeros of $\zeta(s)$. RH would imply

$$\pi(x) = Li(x) + O(\sqrt{x} \log x).$$

Evidence for the RH

- Computation of $N(T)$ can be done by using Cauchy's integral

$$N(T) - 1 = \frac{1}{2\pi i} \int_{\partial R} -\frac{\zeta(s)'}{\zeta(s)} ds.$$

- $\zeta(s)$ and $\zeta(s)'$ can be computed to high precision using the MacLaurin summation formula or the Riemann-Siegel formula.
- Compute the integral, divided by $2\pi i$ and round the real part to the nearest integer to get $N(T)$.
- $\Lambda(\frac{1}{2} + it)$ is real for real t. Strategically pick values of $t \in [0, T]$ and testing for the sign. There will be odd number of zeros between two consecutive sign changes. If the number of sign changes agree with $N(T)$, then we have shown that all zeros up to height T are simple and lie on the line $\Re s = 1/2$.

- Have verified for first 10^{23} zeros.
- Data also supports independent conjecture by Dyson-Montgomery on spacing of zeros.
- The work of Selberg and Levinson shows that more than 40% of nontrivial zeros are simple and satisfy RH.
- It is also known that hypothetical exceptions of nontrivial zeros are rare when we move away from the line $\Re s = 1/2$.

Generalizations of RH

$\zeta(s)$ is the prototype of many zeta and L-functions in number theory. They all have Euler product, analytic continuation, and satisfy functional equations. The nontrivial zeros are conjectured to lie on the line of symmetry, called generalized RH.

Some examples of ζ and L-functions:

1. Dedekind zeta function attached to a number field K:

$$\zeta_K(s) = \sum_{\text{integral ideal } \mathfrak{A} \neq 0} N(\mathfrak{A})^{-s} = \prod_{\text{prime ideal } \mathfrak{P}} \frac{1}{1 - N(\mathfrak{P})^{-s}};$$

2. Given a Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to S^1$, its associated L-function is

$$L(\chi, s) = \sum_{n \geq 1} \chi(n) n^{-s} = \prod_p \frac{1}{1 - \chi(p)p^{-s}};$$

3. L-function attached to an elliptic curve E defined over $\mathbb{Q}$ of conductor N:

$$L(E,s) = \prod_{p \nmid N} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \prod_{p|N} \frac{1}{1 - a_p p^{-s}};$$

4. L-function attached to a holomorphic cuspidal (new)form f of weight k and level N and character χ, which is a Hecke eigenfunction with eigenvalue a_p at each p:

$$L(f,s) = \prod_{p \nmid N} \frac{1}{1 - a_p p^{-s} + \chi(p) p^{k-1-2s}} \prod_{p|N} \frac{1}{1 - a_p p^{-s}};$$

5. Same as #4 except that f is a real analytic Maass wave form which is an eigenfunction of the Laplace operator;

6. L-function attached to an automorphic representation π of GL_n or a group of Lie type over a number field. Attach $\Lambda(\pi, s)$.

For cases 3 and 4, it is also known that "local RH" holds, namely, at $p \nmid N$, the factors of

$$1 - a_p p^{-s} + \chi(p) p^{k-1-2s} = (1 - \alpha_p p^{-s})(1 - \beta_p p^{-s})$$

satisfy

$$|\alpha_p| = |\beta_p| = p^{(k-1)/2}.$$

When this holds in general for case 6, we say that the representation is tempered.

None of the RH over number fields are known. Not all have arithmetic or geometric nature, eg. cases 5 and 6.

Does this suggest that a "proof" of RH should be independent of arithmetic and geometry?

Why is RH/GRH important?

- It describes the law of distribution of primes in $\mathbb{Z}$.
- Hardy and Littlewood showed: under GRH, every large odd integer is a sum of 3 primes.

  Later I. Vinogradov proved this unconditionally.
- Under GRH, Miller gave an algorithm to determine whether n is a prime in $O((\log n)^4)$ steps.

  In 2004 Agrawal-Kayal-Saxena obtained an algorithm in $O((\log n)^{15/2})$ steps unconditionally.
- (Serre) Given two non-isogeneous elliptic curves E and E' over $\mathbb{Q}$ with conductors N_E, $N_{E'}$, resp., there is a prime p which is $O((\log(N_E N_{E'}))^2)$ for which E and E' have good reduction at p and their number of points mod p are different. (with GRH)

- (Artins primitive root conjecture): If an integer b is neither ± 1 nor a perfect square, then b is a primitive root for infinitely many primes p, that is, b mod p generates the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^{\times}$. Originally proved by Hooley under GRH.

  Heath-Brown showed unconditionally: there are at most three b's for which Artin conjecture does not hold.

- Ramanujan points out that congruence tests prevent $x^2 + y^2 + 10z^2$ representing any positive integer of the form $4^{\lambda}(16\mu + 6)$. He asks which numbers not of this form are not represented and lists 16 such. There are in fact exactly 18 such exceptions: $3, 7, 21, 31, 33, 43, 67, 79, 87, 133, 217, 219, 223, 253, 307, 391, 679, 2719$, proved by Ono-Soundararajan under GRH.

  Duke and Schulze-Pillot: this holds unconditionally for general ternary quadratic forms, with a finite list of exceptional values.

Improvements are based on approximations to GRH: zero-free regions and zero density theorems.

Zeta functions for curves over finite fields

X : smooth irred. proj. curve of genus g defined over $\mathbb{F}_q$.
$N_n = \#X(\mathbb{F}_{q^n})$ for each $n \geq 1$
The zeta function of X was introduced by F. K. Schmidt in 1931:

$$Z(X;u) = \exp\left(\sum_{n\geq 1} \frac{N_n}{n} u^n\right) = \frac{P(u)}{(1-u)(1-qu)}$$
$$= \prod_{v \text{ closed points of } X} \frac{1}{1-u^{\deg v}},$$

where $P(u) = (1-\alpha_1 u)\cdots(1-\alpha_{2g}u) \in \mathbb{Z}[u]$.

Riemann Hypothesis: $|\alpha_i| = q^{1/2}$ for $i = 1, ..., 2g$, proved by Hasse (1933) for $g = 1$ and Weil (1948) in general.

Set $u = q^{-s}$, then RH says all zeros of $Z(X; q^{-s})$ lie on $\Re s = \frac{1}{2}$.

Zeta functions for varieties defined over finite fields

V: smooth irred. proj. variety of dim. d defined over $\mathbb{F}_q$

The zeta function of V is

$$Z(V,u) = \exp(\sum_{n\geq 1} \frac{N_n}{n} u^n) = \prod_{v \text{ closed pts}} (1-u^{\deg v})^{-1}$$
$$= \frac{P_1(u)P_3(u)\cdots P_{2d-1}(u)}{P_0(u)P_2(u)\cdots P_{2d}(u)}.$$

Here $N_n = \#V(\mathbb{F}_{q^n})$ and each $P_i(u)$ is a polynomial in $\mathbb{Z}[u]$ with constant term 1.

RH: the roots of $P_i(u)(\neq 1)$ have absolute value $q^{-i/2}$.

Conjectured by Weil, proved by Deligne for general d, using machinery developed by Grothendieck.

Possible approaches to prove RH

RH for varieties over finite fields have important applications in number theory. For instance, they were used to proved the "local RH" for elliptic curves and holomorphic cusp forms alluded earlier. Further, the field of rational functions on a curve defined over a finite field has many properties parallel to number fields. The validity of RH for varieties should be regarded as an "evidence" for the RH over number fields. Goal: to find "analogous" approaches.

The RH for varieties was proved by interpreting the zeros/poles as eigenvalues of the Frobenius automorphism on certain cohomological spaces. For $\zeta(s)$ a similar idea was proposed by Hilbert and Polya that the nontrivial zeros of $\zeta(s)$ could be the eigenvalues of a self-adjoint linear operator on some Hilbert space.

Counter argument: There is no "self-adjointness" in the proof for varieties. Instead, the second step in the proof of RH for varieties is to "deform the given variety in a family". The family has a symmetry group (the monodromy group) which is used together with its high tensor power representations and a positivity argument to prove the Weil Conjectures for each member of the family at once. Should try to find a family to "deform".

The spectral nature of zeros goes well with known statistical fluctuations of zeros. The high zeros of $\Lambda(s)$ and $\Lambda(\pi, s)$ all behave the same way, agreeing with the fluctuations of eigenvalues of large random unitary matrices in the Gaussian Unitary Ensemble (GUE). For low-lying zeros, the fluctuations of zeros can be classified into three types, GUE, the Gaussian Orthogonal Ensemble (GOE), and Gaussian Symplectic Ensemble (GSE). For varieties,

this is well studied by Katz and Sarnak. So to deform ζ, should search among those $\Lambda(\pi, s)$ with the same behavior for low-lying zeros as $\xi(s)$. This philosophy fits well with the known data.

This gives a strong evidence that the zeros of L-functions should have a spectral interpretation. This is given via Langlands' theory of Eisenstein series. Can construct Eisenstein series whose poles are the zeros of a given L-function (hence the zeros can in this way be thought of as resonances for a spectral problem). Combining this with a positivity argument using the inner product formula for Eisenstein series (Maass Selberg Formula) yields effective zero free regions in $\Re(s) \leq 1$ for all L-functions whose analytic continuation and functional equations are known. This method should be considered as the most powerful one towards GRH.

Zeta functions of graphs

The Ihara zeta function of a finite graph X is defined as

$$Z(X,u) = \prod_{[C]} \frac{1}{1-u^{l(C)}} = \exp\left(\sum_{n\geq 1} \frac{N_n}{n} u^n\right),$$

where $[C]$ runs through all equiv. classes of primitive geodesic cycles C in X, $l(C)$ is the length of C, and N_n is the number of geodesic cycles in X of length n.

Properties of Ihara zeta functions

- Ihara (1968): Let X be a finite $(q+1)$-regular graph. Then its zeta function $Z(X,u)$ is a rational function of the form

$$Z(X,u) = \frac{(1-u^2)^{\chi(X)}}{\det(I - Au + qu^2 I)},$$

  where $\chi(X) = \#V - \#E = -\frac{q-1}{2}\#V$ is the Euler characteristic of X and A is the (vertex) adjacency matrix of X.

- X is Ramanujan if and only if $Z(X,u)$ satisfies RH, i.e. the nontrivial poles of $Z(X,u)$ have absolute value $q^{-1/2}$.

  Ramanujan graphs are spectrally optimal.