Universality and the Riemann Hypothesis

Paul Gauthier*, Extinguished professor
Université de Montréal

Informal Analysis Seminar focusing on Universality

Kent State University, April 11-13, 2014

Wer die Zetafunktion kennt, kennt die Welt!

Riemann Hypothesis = RH

Number one unsolved problem in mathematics is the Riemann Hypothesis.
Bagchi gave an equivalent formulation in terms of the spectacular universality theorem of Voronin.

Euler zeta function

$$\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x}, \quad x > 1.$$

Riemann zeta function is meromorphic extension of ζ to all of $\mathbb{C}$. It has (so-called trivial) zeros at $-2, -4, \cdots, -2n, \cdots$.
Other zeros are called non-trivial zeros.

Riemann Hypothesis. All non-trivial zeros of $\zeta(z)$ lie on the critical axis $\Re z = 1/2$.

Easy. All non-trivial zeros lie in the fundamental strip $0 \leq \Re z \leq 1$.

Prime number theorem(conjectured by Legendre)
Let $\pi(x)$ = number of primes $\leq x$. Then,

$$\pi(x) \sim \frac{x}{\ln x}$$

Strong prime number theorem(conjectured by Gauss)

$$\pi(x) \sim \text{Li}(x), \quad \text{where} \quad \text{Li}(x) = \int_2^x \frac{dt}{\ln t}$$

Prime Number Theorem **implies**
non-trivial zeros lie in the fundamental strip $0 < \Re z < 1$.

RH is **equivalent** to the following error estimates

$$\pi(x) = \text{Li}(x) + \mathcal{O}(\sqrt{x} \ln x)$$

$$\pi(x) = \text{Li}(x) + \mathcal{O}(\sqrt{x} x^{\varepsilon}), \quad \text{for every} \quad \varepsilon > 0$$

Partial confirmation of the RH

PNT is equivalent to the assertion that non-trivial zeros lie in $0 < \Re z < 1$.

Bohr and Landau proved in 1914 that the proportion of the zeros lying within ε distance from the critical line equals 1, for every $\varepsilon > 0$. That is 100% of the zeros lie in the strip $1/2 - \varepsilon < \Re z < 1/2 + \varepsilon$.

What about the proportion ON the critical axis? Conrey proved that at least $2/5$ are on the critical axis.

RH verified for the first 10^{10} zeros.

Other zeta-functions

There are many zeta-functions, which resemble the Riemann zeta-function and there are analogs of the RH concerning the zeros of these zeta-functions. The main zeta-functions with regard to the RH are zeta-functions over **number fields** and zeta-functions over **function fields.**

An (algebraic) **number field** F is a finite (hence algebraic) field extension of the field $\mathbb{Q}$ of rational numbers. Thus, $\mathbb{Q} \subset F \subset \mathbb{C}$. Strangely, the field of algebraic numbers is not an algebraic number field.

Examples. $\mathbb{Q}$ is a number field and also the Gaussian field $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$

An (algebraic) **function field** F is a finite (hence algebraic) field extension of the field $\mathbb{Q}(z)$ of rational functions.

Examples. The function field of an algebraic curve is an example and every algebraic function field is isomorphic to such a field. An algebraic curve is the zero set of a polynomial $p(z, w) = 0$.

Varieties

A **manifold** is locally euclidian. For example, a curve is a 1-dimensional manifold and a surface is a 2-dimensional manifold.

A **variety** V is like a manifold, except there might be a few singular points
Example: $V = \{(x, y) \in \mathbb{R}^2 : xy = 0\}$ looks like $\mathbb{R}$ except at the singular point $(0, 0)$.

We may define meromorphic functions on a (complex) manifold or variety.

A **Function field of a variety** is the field of meromorphic functions on a variety.

Given a number field or a function field F we can associate a zeta-function ζ_F. For example, $\zeta_{\mathbb{Q}}$ is the Riemann zeta-function.

Status of Riemann Hypothesis

There is no number field for which the RH has been either confirmed or disproved. Recall that the original RH is for the (Riemann) zeta-function of the number field $\mathbb{Q}$.

The only zeta-functions for which the the RH has been confirmed are zeta-functions over finite fields.

A variety V is over some field K. That is, V looks locally like K^n, except at a few singular points. For example, a variety over $\mathbb{R}$ is a real variety and a variety over $\mathbb{C}$ is a complex variety.

By a zeta-function over a finite field, we mean the zeta-function of the function field F_V of a variety V over a finite field K.

Weil proved the RH for zeta-functions of elliptic curves over finite fields in 1940. Deligne extended this to varieties over finite fields (1974,1980). One of the crowning achievements of 20th century mathematics. Many consider this the main evidence that the original RH is true.

Prime Gaps

Order the prime numbers $p_1 < p_2 < \cdots < p_n < \cdots$

The distance $p_{n+1} - p_n$ between two consecutive primes is a prime gap.

Theorem $\limsup(p_{n+1} - p_n) = +\infty$. That is, there are arbitrarily large prime gaps.

Proof. If $k < p_{n+1}$, then $q|k \to q \leq p_n$. Thus $\prod_{q \leq p_n} q + k$ is a composite number. The sequence of composite numbers

$$\prod_{q \leq p_n} q + 2, \prod_{q \leq p_n} q + 3, \cdots, \prod_{q \leq p_n} q + (p_{n+1} - 1)$$

is of length $p_{n+1} - 1$ so there are arbitrarily large prime gaps. qed.

How small can gaps be?

Of course $p_{n+1} - p_n \geq 2$. If $p_{n+1} - p_n = 2$, they are called twin primes (as close as possible).

Twin Prime Conjecture. There are infinitely many twin primes. That is, $\liminf(p_{n+1} - p_n) = 2$.

ZHANG Yitang, New Hampshire, May 2013

$\liminf(p_{n+1} - p_n) < +\infty$ more precisely $< 70{,}000{,}000$

Zhang uses solution of RH for curves (Weil) and varieties (Deligne).

Maynard, CRM, Université de Montréal, Nov 2013

$$\liminf(p_{n+1} - p_n) \leq 600$$

Similar result independently by Terrence TAO (private communication to Maynard).

RH and Computer Security

Computer security is based on the simple fact that it is easy for me to construct a large number for which I know the prime factors, but it would take you a very long time to find those prime factors. That is how we build “secure" codes. I put secure in parentheses because no method is presently known for finding prime factors rapidly. But perhaps someone will find such a rapid method. Then ALL codes will be compromised: private, industrial, financial, military, governmental, whatever.

If RH is true, then one can indeed prove that certain algorithms for factoring primes converge faster than others. But this does not help us to **find** new algorithms. Thus, since the RH is thought to be true, one can merely assume the RH and choose those algorithms which RH favors. To recapitulate, just knowing that RH is true would have no practical application in improving speed of code breaking. However, it is likely that the *proof* (of which we have no idea) of the RH would yield important information. Indeed, the proof of the RH over finite fields has furnished important information for cryptography.

Existence of a universal function

Birkhoff (1929). There exists an entire function f whose translates approximate *all* entire functions. That is, for each entire function g, there is a sequence $\{a_n\}$ such that

$$f(z + a_n) \longrightarrow g(z), \qquad \text{for all } z \in \mathbb{C}.$$

Such a function f is called a *universal* function.

Most entire functions are universal.

No example of an *entire* universal function is known.

The Riemann zeta-function $\zeta(s)$ is the **only known** function universal in this sense.

Wer die Zetafunktion kennt, kennt die Welt!

Remark. $\zeta(s)$ is *not* entire, but it is as close to being entire as possible. It has only one pole and that pole is simple.

The other Birkhoff and MacLane

GEORGE D. Birkhoff (1929). There exists an entire function f whose **translates** approximate all entire functions. That is, for each entire function g, there is a sequence $\{a_n\}$ of complex numbers such that

$$f(z + a_n) \longrightarrow g(z), \qquad \text{for all } z \in \mathbb{C}.$$

GERALD Maclane (1952). There exists an entire function f whose **derivatives** approximate *all* entire functions. That is, for each entire function g, there is a sequence $\{n_k\}$ of natural numbers such that

$$f^{(n_k)}(z) \longrightarrow g(z), \qquad \text{for all } z \in \mathbb{C}.$$

George Birkhoff and Gerald MacLane are respectively the **father** and **brother** of Garrett Birkhoff and Saunders MacLane, authors of the famous book on algebra.

Zero-free hypothesis

Voronin. For every **zero-free** function f holomorphic in the strip $1/2 < \Re z < 1$, there is a sequence of reals numbers such that $\zeta(z+it_j) \to f(z)$ uniformly on compact subsets of the strip.

Remark 1. *If the zero-free hypothesis can be removed from Voronin's Universality Theorem, the Riemann Hypothesis fails*

This can be shown using Rouché's Theorem. Note that it has not been shown that the zero-free hypothesis cannot be removed, so this is a possible way of disproving the Riemann Hypothesis. In this connection, note that the zero-free hypothesis is missing from the following.

Theorem 1. *For every f holomorphic in the strip $1/2 < \Re z < 1$, there is an increasing sequence of compact sets $K_1 \subset K_2 \subset \cdots$, whose union is the strip and a sequence of real numbers t_j such that*

$$\max_{z \in K_j} |\zeta(z + it_j) - f(z)| < \frac{1}{j}.$$

Voronin's spectacular universality theorem states that, for each zero-free function g holomorphic in the strip $S = (1/2 < \Re z < 1)$, for each compact $K \subset S$, for each $\epsilon > 0$, there is a real number t, such that

$$\sup_{z \in K} |\zeta(z + it) - g(z)| < \epsilon.$$

In fact, there exist **many** such t. To make this statement precise, we need to introduce cylic, hypercylic and frequently hypercyclic vectors.

For an operator $T : X \to X$ and $x \in X$, the *orbit* of x is $O(x) = \{Tx, T^2x, \cdots, T^kx, \cdots\}$, where

$$T^kx = T(T(T(\cdots Tx))) \quad k \text{ times},$$

$< O(x) >$ is the subspace generated by $O(x)$.

x is a *cyclic* vector for T if $< O(x) >$ is dense in X.

x is a *hypercyclic* vector for T if the orbit itself $O(x)$ is dense in X.

$\mathcal{H}(\mathbb{C})$ the space of entire functions. For $a \in \mathbb{C}$, C_a is the translation operator on $\mathcal{H}(\mathbb{C})$ defined by $(C_a f)(z) = f(z+a)$.

Birkhoff. For each $a \neq 0$, there is a hypercyclic entire function f for the translation operator C_a on $\mathcal{H}(\mathbb{C})$. The translates of f approximate *all* entire functions. That is, for each $g \in \mathcal{H}(\mathbb{C})$, there is a sequence $\{n_k\}$ in $\mathbb{N}$, such that

$$f(z + n_k a) \to g(z).$$

Such an entire function is called *universal*.

Hypercyclicity is generic. Most entire functions are universal.

No example is known.

The Riemann zeta-function is universal (for vertical translation in strip $S = (1/2 < \Re z < 1)$.

The Riemann zeta-function is not entire.

But almost - only one simple pole with residue 1.

For $A \subset (0, +\infty)$, lower and upper density of A:

$$\underline{d}(A) = \liminf_{T \to +\infty} \frac{meas(A \cap (0, T])}{T}$$

$$\overline{d}(A) = \limsup_{T \to +\infty} \frac{meas(A \cap (0, T])}{T}$$

For $A \subset \mathbb{N}$, lower and upper density of A wrt $\mathbb{N}$:

$$\underline{d}(A) = \liminf_{N \to +\infty} \frac{\#(A \cap \{1, 2 \cdots, N\})}{N}$$

$$\overline{d}(A) = \limsup_{N \to +\infty} \frac{\#(A \cap \{1, 2 \cdots, N\})}{N}$$

Let $T : X \to X$ and $Y \subset X$. A vector $x \in X$ is

frequently hypercyclic in Y

for the operator T if, for each $y \in Y$ and each neighbourhood U of y in X,

$$\underline{d}\{k \in \mathbb{N} : T^k x \in U\} > 0.$$

Bayart-Grivaux have defined x to be

frequently hypercyclic

for T if we may take $Y = X$.

Frequent hypercyclicity not generic, but

the set of hypercyclic vectors for an operator $T : X \to X$, if not empty, is dense.

$S = \{z : 1/2 < \Re z < 1\}$, $\mathcal{F}(S)$ a family of functions on S, $\mathcal{F}_o(S)$ the family of zero-free functions in $\mathcal{F}(S)$.

Voronin Universality Theorem(Reich, Gonek, Bagchi). ζ is frequently hypercyclic for vertical translation C_i in the family $\mathcal{H}_o(S)$. In fact,

for each compact $K \subset S$, with $\mathbb{C} \setminus K$ connected, for each $f \in A_o(K) = C_o(K) \cap \mathcal{H}(K^o)$, for each $\epsilon > 0$,

$$\overline{d}\{k \in \mathbb{N} : \max_K |\zeta(z + ik) - f(z)| < \epsilon\} > 0;$$

for each $\Delta > 0$,

$$\overline{d}\{k \in \mathbb{N} : \max_K |\zeta(z + ik\Delta) - f(z)| < \epsilon\} > 0;$$

$$\overline{d}\{t \in \mathbb{R}^+ : \max_K |\zeta(z + it) - f(z)| < \epsilon\} > 0.$$

$S = \{z : 1/2 < \Re z < 1\}$. If $f \in \mathcal{H}(S)$ is frequently hypercyclic for C_i, then f is *strongly recurrent* in S for vertical translation. For each compact $K \subset S$, for each $\epsilon > 0$,

$$\overline{d}\{k \in \mathbb{N} : \max_K |f(z + ik) - f(z)|\} > 0.$$

Theorem 2 (Bagchi)**.** *TFAE*

1) The Riemann Hypothesis holds.

2) The Riemann zeta-function ζ is strongly recurrent for vertical translation.

Theorem 3. *For each* $\Delta > 0$, *there exists a sequence of functions*

$$\varphi_n(z) \to \zeta(z), \qquad z \in \mathbb{C}$$

Each φ_n *strongly recurrent in* $1/2 < \Re z < 1$ *for vertical translation along the arithmetic progression*

$$i\Delta, i2\Delta, \cdots, ik\Delta, \cdots.$$

φ_n *meromorphic, simple pole, residue* 1, *at* $z = 1$

$$\varphi_n(x) \in \mathbb{R}, \qquad \forall x \in \mathbb{R}$$

A remarkable equivalence

Conjecture 1. [Andersson] If $\mathbb{C} \setminus K$ is connected, then, for every $f \in A(K)$ zero-free on K^o, and $\epsilon > 0$, there is a polynomial zero-free on K, such that

$$\max_{z \in K} |p(z) - f(z)| < \epsilon.$$

Conjecture 2. [Andersson] If $\mathbb{C} \setminus K$ is connected, and K lies in the strip $1/2 < \Re z < 1$, then, for every $f \in A(K)$ zero-free on K^o, and $\epsilon > 0$, then

$$\underline{d}\left(\{t > 0 : \max_{z \in K} |\zeta(z + it) - f(z)| < \epsilon\}\right) > 0.$$

The first conjecture is an extremely natural problem on polynomial approximation. The second conjecture, gives a significant improvement on Voronin's spectacular universality theorem. The following theorem is remarkable.

Andersson. These two conjectures are equivalent.

THANKYOU!