Primes and Open Problems in Number Theory
Part I

A. S. Mosunov

University of Waterloo
Math Circles

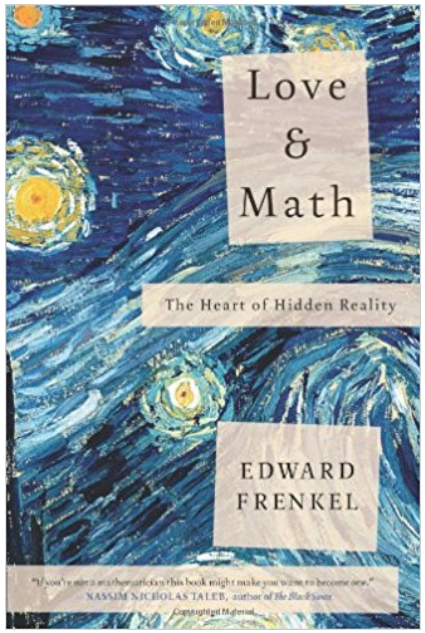
February 7th, 2018

Goals

- Explore the area of mathematics called **Number Theory**.
- Specifically, we will look at **prime numbers** and questions about primes that mathematicians are trying to solve.
- **Goal 1.** Understand the state of the art.
- **Goal 2.** Understand the open problems.
- **Goal 3.** Get inspired!

Love and Math

- Edward Frenkel wrote a book *Love and math: the heart of hidden reality*, which I highly recommend to all of you!



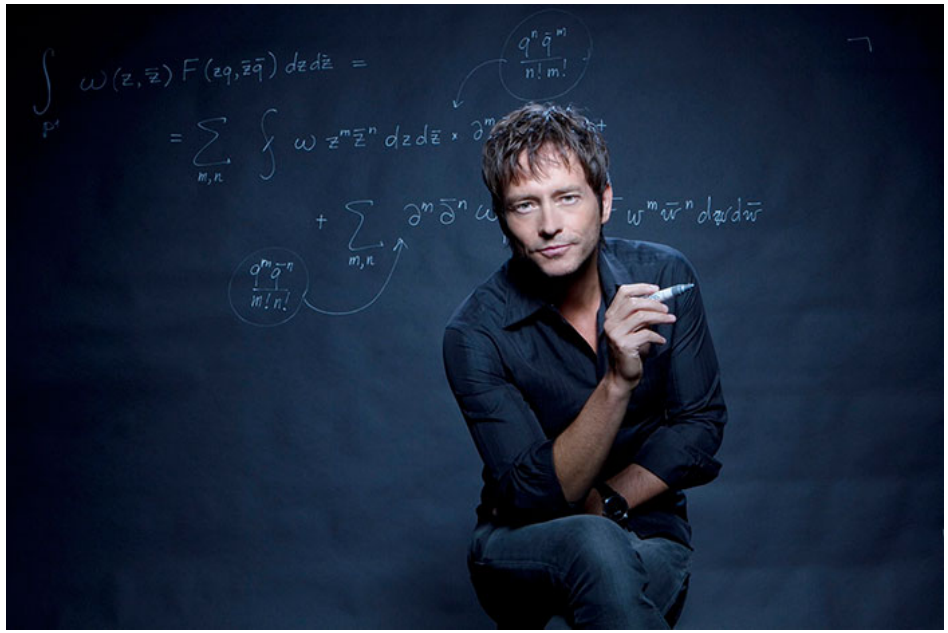


Figure: Edward Frenkel and his book.

Pictures from `https://images-na.ssl-images-amazon.com/images/I/612d9ocw9VL._SX329_BO1,204,203,200_.jpg` and `http://projects.thestar.com/math-the-canadian-who-reinvented-mathematics/img/edward-frenkel.jpg`.

BACKGROUND

Number Theory

- Number theory is undoubtedly the oldest mathematical discipline known to the world.
- It is the area of mathematics that studies properties of numbers, such as $2, 0, -1, 22/7$, or π.

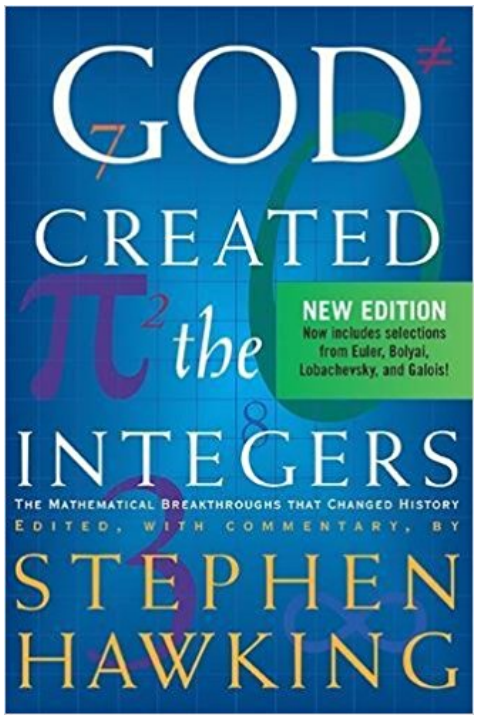


Figure: Stephen Hawking's book.

Picture from `https://images-na.ssl-images-amazon.com/images/I/513w%2BH6XuEL._SX328_BO1,204,203,200_.jpg`.

Why Study Number Theory?

- It is beautiful.
- It is mysterious.
- Because we want to ~~become famous and make lots of money~~ make an impact!
- It is applicable! A large part of modern cryptography resides on difficult number theoretical problems.

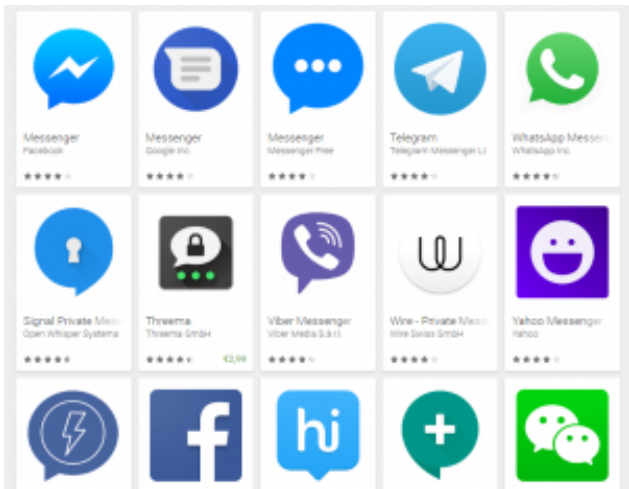


Figure: Messengers which (hopefully) deploy cryptographic protocols.

Picture from `https://blog.online-convert.com/wp-content/uploads/2017/02/OC_Apps_GooglePlay-300x232.png`.

Primes

- A number $p \geq 2$ is called **prime** if it is divisible only by 1 and p. Otherwise it is called **composite**.
- **Exercise.** Find first 15 primes.
- **Answer.** First 15 prime numbers are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, \ldots$$

- The largest prime number known to date is

$$2^{77232917} - 1$$

and it was discovered in December 2017. This number has 23249425 digits.

Primes in Nature

- Cicadas live underground, and their reproductive cycle is N years, where N is either 13 or 17. How do cicadas know about prime numbers?
- The hypothesis is that, if N is a big prime, then it is least likely to be a multiple of the length of a predator's population cycle which could kill them off.
- See Manjul Bhargava's Fields Medal Symposium 2016 talk: `https://youtu.be/LP253wHIo08?t=24m51s`.

Figure: Periodical cicada.

Picture from `https://en.wikipedia.org/wiki/Periodical_cicadas#/media/File:Magicicada_tredecassini_NC_XIX_male_dorsal_trim.jpg`.

Properties of Primes

- Let a and b be integers. We say that a **divides** b when $b = ak$ for some integer k. We write $a \mid b$ in this case, and $a \nmid b$ otherwise.
- For each integer $n \geq 2$ there exists a prime p such that $p \mid n$.
- **The Fundamental Theorem of Arithmetic.** Any integer greater than 1 can be written uniquely (up to reordering) as the product of primes.
- This is why in his talk Bhargava calls primes "the atoms of the universe" of integers.
- **Euclid's Theorem.** (circa 300BC) There are infinitely many prime numbers.

Primes at Work

- **Example.** We can factor the number 660 as follows:

$$660 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 11 = 2^2 \cdot 3 \cdot 5 \cdot 11.$$

- **Exercise.** Factor the numbers 9350, 2020, and 2018.
- **Proof of Euclid's Theorem.** The proof is by contradiction, so we suppose that there are finitely many primes. Let us call them $p_1 = 2, p_2 = 3, \ldots, p_k$. We consider the number

$$n = p_1 p_2 \cdots p_k + 1.$$

- The number n is composite, which means that there is some prime p_i such that $p_i \mid n$. But then p_i divides both n and $p_1 p_2 \cdots p_k$, so it must be the case that $p_i \mid 1$. Since $p_i > 1$, we arrive to a contradiction.

Exercise: Euler's Proof of Euclid's Theorem

1. In this exercise, we will prove Euclid's Theorem using the proof of Leonhard Euler.
2. Consider the **harmonic series**

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\ldots.$$

3. Prove that, for any positive integer n,

$$\frac{1}{2n-1}+\frac{1}{2n}>\frac{1}{n}.$$

4. Suppose that there is a real number H such that $H=1+1/2+1/3+1/4+\ldots$. Derive a contradiction by proving that $H>1/2+H$ using the inequality above. Conclude that $1+1/2+1/3+1/4+\ldots$ approaches infinity.

Exercise: Euler's Proof of Euclid's Theorem

5. Use the Fundamental Theorem of Arithmetic to prove that every fraction $1/n$ appears in the infinite product

$$\left(1+\frac{1}{2}+\frac{1}{2^2}+\ldots\right)\times\left(1+\frac{1}{3}+\frac{1}{3^2}+\ldots\right)\times\left(1+\frac{1}{5}+\frac{1}{5^2}+\ldots\right)\times\ldots$$

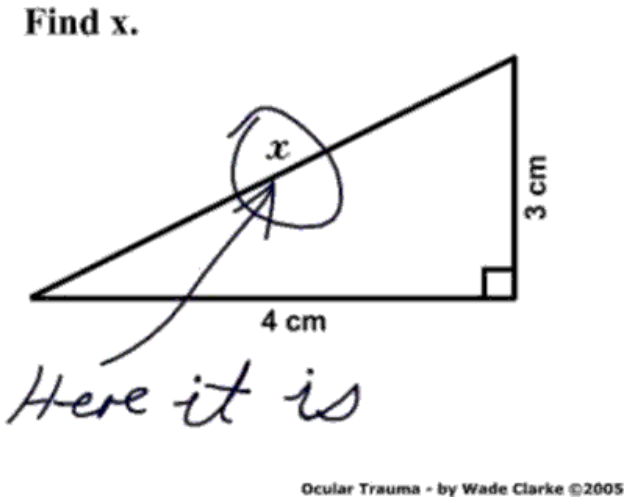
   exactly once. Conclude that this product is equal to the harmonic series.

6. Note that the sequence $1, p^{-1}, p^{-2}, \ldots$ is a geometric progression. Explain why foe each prime p the sum $1+p^{-1}+p^{-2}+\ldots$ is finite.

7. If the number of primes would be finite, what would happen to the above product? Derive a contradiction to the fact that $1+1/2+1/3+1/4+\ldots$ approaches infinity.

BREAK

Now we are finally ready to begin our journey!



Picture from `http://www.mathwarehouse.com/jokes/images/find-x-funny-math-image-joke.png`.

What We Do Not Know

- In 1912, at the International Congress of Mathematics, Edmund Landau listed the following four basic problems about primes that still remain unresolved.
- **Goldbach's Conjecture, 1742.** Can every even integer greater than 2 be written as a sum of two primes?
- **Twin Prime Conjecture, 1849.** Are there infinitely many prime numbers p and q such that $|p-q|=2$?
- **Legendre's Conjecture, $\sim$1800.** Does there always exist a prime between two consecutive perfect squares?
- **(Weak) Bunyakovsky's Conjecture, 1857.** Are there infinitely many primes of the form n^2+1?

What We Do Know

- **Helfgott's Theorem, 2013.** Every odd number exceeding 5 can be expressed as a sum of three primes.
- **(Improved) Zhang's Theorem, 2013.** There are infinitely many distinct primes p and q such that $|p-q| \leq 246$.
- **Chebyshev's Theorem, 1852.** For $n > 1$ there always exists a prime between n and $2n$.
- **Ingham's Theorem, 1937.** For all sufficiently large n there always exists a prime between n^3 and $(n+1)^3$.
- **Prime Number Theorem, 1896.** Up to $x > 1$, there are "approximately" $x/\ln x$ prime numbers.
- **Green-Tao Theorem, 2004.** Given a positive integer d, there always exist distinct prime numbers $p_1, p_2, \ldots, p_d$ which form an arithmetic progression.

Prime Number Theorem

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

Prime Number Theorem

- **Question.** For a positive real number x, how many primes are there up to x?
- Let $\pi(x)$ denote the total number of primes $p \leq x$.
- **Exercise.** Compute $\pi(10)$, $\pi(50)$ and $\pi(100)$.
- In 1790's, Legendre and Gauss independently conjectured that $\pi(x)$ is "approximately" equal to $x/\ln x$.

Figure: (The only portrait of) Legendre and Gauss.

Pictures from `https://upload.wikimedia.org/wikipedia/commons/0/03/Legendre.jpg` and `https://upload.wikimedia.org/wikipedia/commons/thumb/e/ec/Carl_Friedrich_Gauss_1840_by_Jensen.jpg/1200px-Carl_Friedrich_Gauss_1840_by_Jensen.jpg`.

How does $\pi(x)$ behave?

x	$\pi(x)$	$x/\ln x$	$\mathrm{Li}(x)$
10	4	4	5
10^2	25	22	29
10^3	168	145	176
10^4	1229	1086	1245
10^5	9592	8686	9628
10^6	78498	72382	78626
10^7	664579	620421	664917
10^8	5761455	5428681	5762208
10^9	50847534	48254942	50849234
10^{10}	455052511	434294482	455055614
10^{11}	4118054813	3948131654	4118066400
10^{12}	37607912018	36191206825	37607950280
10^{13}	346065536839	334072678387	346065645809
10^{14}	3204941750802	3102103442166	3204942065691
10^{15}	29844570422669	28952965460217	29844571475287
10^{16}	279238341033925	271434051189532	279238344248556
10^{17}	2623557157654233	2554673422960305	2623557165610821
10^{18}	24739954287740860	24127471216847324	24739954309690414
10^{19}	234057667276344607	228576043106974646	234057667376222381
10^{20}	2220819602560918840	2171472409516259138	2220819602783663483
10^{21}	21127269486018731928	20680689614440563221	21127269486616126181

Table: Values of $\pi(x)$, $x/\ln x$ and $\mathrm{Li}(x) = \int_2^x (1/\ln u)du$.

The Mysterious Function Li(x)

- In fact, the **logarithmic integral**

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\ln u}\, du$$

approximates $\pi(x)$ even better than $x/\ln x$!

- Think about an integral as the area under the graph.

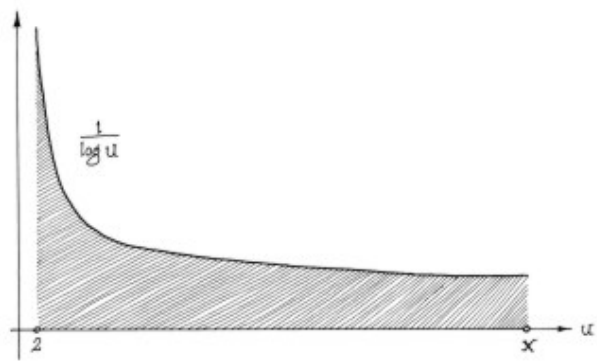


Figure: The area under the graph of $1/\ln u$ for $2 \leq u \leq x$ is equal to $\mathrm{Li}(x)$.

Picture from
http://empslocal.ex.ac.uk/people/staff/mrwatkin/zeta/invlog.jpg.

Prime Number Theorem

- Here is the Prime Number Theorem:

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

- It was proved independently by Jacques Hadamard and Charles Jean de la Vallée-Poussin in 1896.
- All this is saying is that, when x is very very very large, the value $\pi(x)/(x/\ln x)$ is very very very close to 1.


Figure: Hadamard and de la Vallée-Poussin.

Pictures from `https://www.biografiasyvidas.com/biografia/h/fotos/hadamard.jpg` and `https://upload.wikimedia.org/wikipedia/commons/e/e5/De_La_Valle_Poussin.jpg`.

Prime Number Theorem

- **Exercise.** Compute $\pi(x)/(x/\ln x)$ for $x = 10^2, 10^4, 10^8$. Note that $\pi(10^4) = 1229$ and $\pi(10^8) = 5761455$.
- Here are the graphs of $\pi(x)/(x/\ln x)$ and $\pi(x)/\mathrm{Li}(x)$.

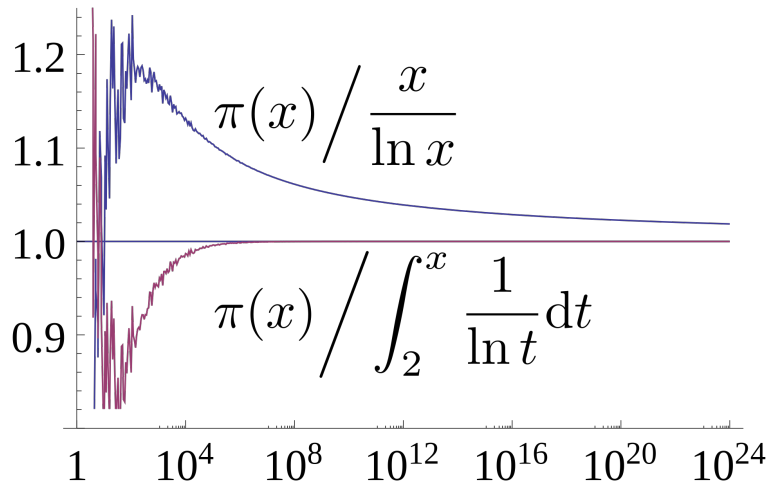


Figure: Ratios of functions in PNT.

Picture from `https://upload.wikimedia.org/wikipedia/commons/thumb/8/87/Prime_number_theorem_ratio_convergence.svg/2000px-Prime_number_theorem_ratio_convergence.svg.png`.

Formula for the n-th Prime

- **Question.** Is there a formula for the n-th prime?
- **Answer.** No, but given n we can estimate the value of p_n relatively well.
- Let p_n be the n-th prime, and note that $\pi(p_n) = n$. Wouldn't it be great if $\pi(x)$ had an inverse? Then we could just compute $p_n = \pi^{-1}(n)$.
- It turns out this heuristic explanation gives the right intuition: since $\pi(n) \sim g(n)$, where $g(n) = n/\ln n$, we have $p_n \sim g^{-1}(n)$.
- In fact, $g^{-1}(n) \sim n \ln n$, which means that $p_n \sim n \ln n$.
- Under the assumption of the **Riemann Hypothesis**, in 2012 de Reyna and Toulisse proved that

$$\left| p_n - \mathrm{Li}^{-1}(n) \right| \leq \frac{1}{\pi} \sqrt{n} (\log n)^{5/2}$$

for all $n \geq 11$.

How PNT Was Proved?

- In 1859, Riemann proved PNT under the assumption of the **Riemann Hypothesis** (RH).
- Both Hadamard and de la Vallée-Poussin found a way to bypass proving RH.
- In 1900, Hilbert introduced the list of 23 unsolved mathematical problems. RH was #8. A large portion of XX century mathematics revolved around these problems.
- RH is among several Hilbert's problems that remains unsolved to this day. It is one of seven Millenium Prize Problems announced by the Clay Mathematics Institute in 2000. The prize is one million dollars.

- **ONE**
- **MILLION**
- **DOLLARS**

Picture from
http://s3.amazonaws.com/newbucketoprsuit/wp-content/uploads/2016/06/07074617/how-to-make-a-million-dollars-walter-white.jpg

What is RH?

- We define the **Riemann zeta function** as

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \dots.$$

- The Riemann hypothesis concerts the solutions to the equation $\zeta(s) = 0$.
- Here s is a **complex number**. That is, a number of the form $s = x + iy$, where x and y are real numbers, and i is a number such that $i^2 = -1$.
- Hadamard and de la Vallée-Poussin managed to identify a certain region where $\zeta(s) \neq 0$, and derive PNT from there.

More on PNT

- The modern version of PNT can be significantly improved if RH is true.
- In fact, many other theorems rely on RH, and often theorems are proved conditionally or unconditionally, depending on whether the assumption of RH was involved in the proof.
- There is an "elementary" proof of PNT due to Atle Selberg, over which he had a dispute with Paul Erdős. See `http://www.math.columbia.edu/~goldfeld/ErdosSelbergDispute.pdf`.

Exercise: Erdős' Proof of Euclid's Theorem

1. In 1938, Paul Erdős presented the proof of Euclid's Theorem, which resulted in a non-trivial lower bound on the prime counting function $\pi(n)$.
2. A positive integer n is a **perfect square** if it is of the form $n = m^2$. Give five examples of perfect squares.
3. A positive integer n is **squarefree** if no perfect square, except for 1, divides n. Give five examples of squarefree numbers.
4. Prove that every positive integer n can be factored uniquely as $n = s^2 t$, where s, t are positive integers and t is squarefree.
5. Prove that there are at most $\sqrt{n}$ perfect squares not exceeding n.
6. Prove that there are at most $2^{\pi(n)}$ squarefree numbers not exceeding n.
7. Prove that $2^{\pi(n)}\sqrt{n} \geq n$. Why does this inequality proves Euclid's Theorem?

The End

- THANK YOU FOR COMING!
- P.S. Check out the documentary *N is a Number* about Paul Erdős. Here is the link: `https://www.youtube.com/watch?v=uPsFjRvNQG4`.

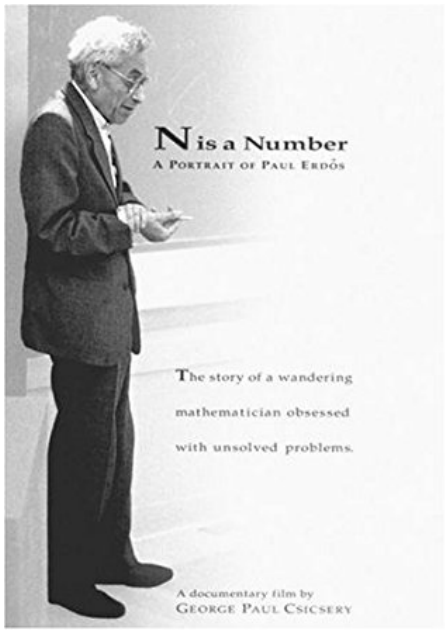


Figure: Poster for the documentary about Erdős.

Picture from `https://images-na.ssl-images-amazon.com/images/I/41ldhzNSOuL._SY445_.jpg`.