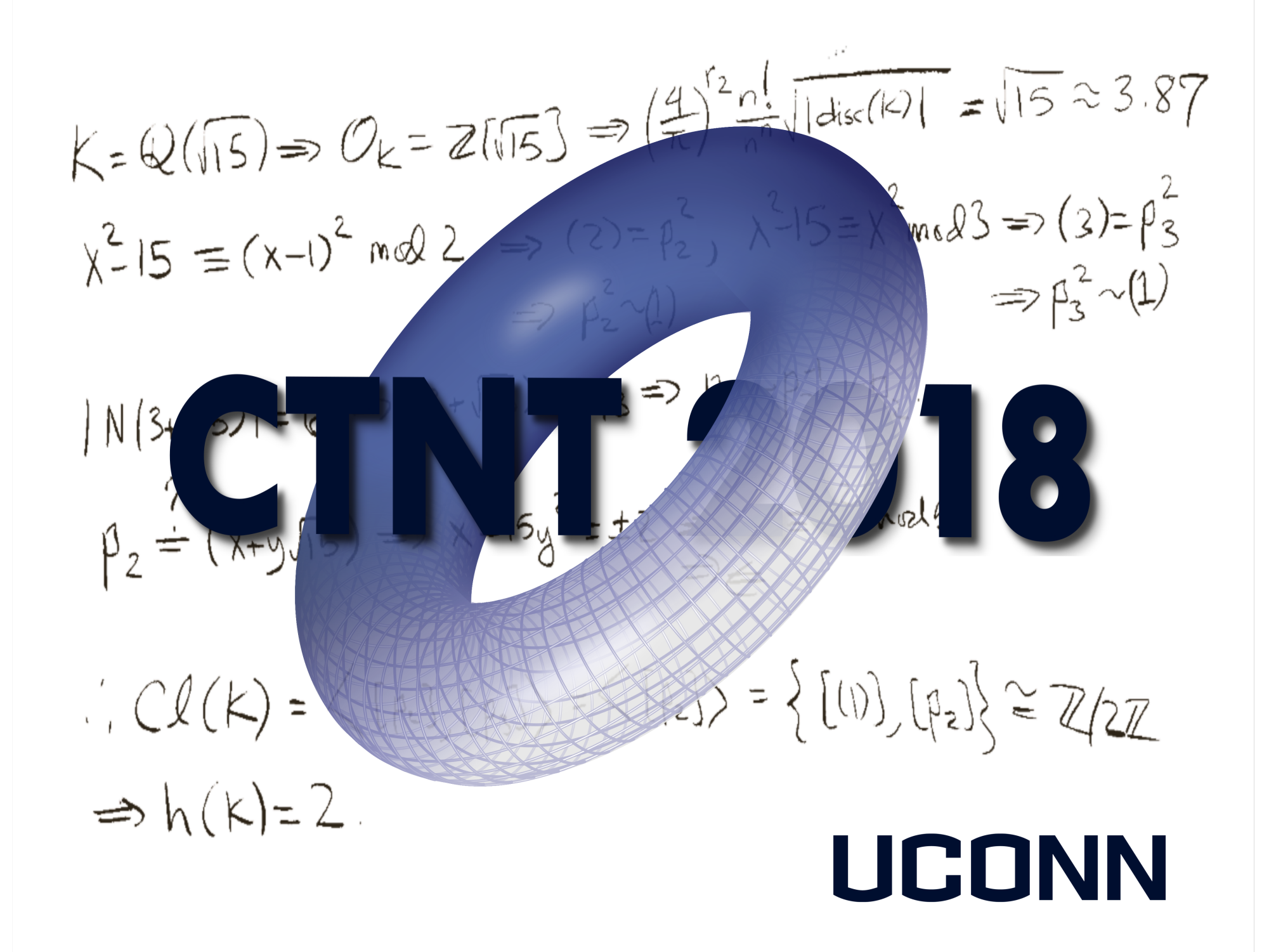

CTNT 2018
UCONN

Arithmetic Statistics
Lecture 1

Álvaro Lozano-Robledo

Department of Mathematics
University of Connecticut

May 28th

CTNT 2018
Connecticut Summer School
in Number Theory

Question

What is “Arithmetic Statistics”?

Our **goal**: count or enumerate number theoretic objects of a certain type, up to a bound.

Number-theoretic objects:

- Prime numbers, twin primes, Wieferich primes, etc,
- Binary quadratic forms, binary cubic forms, etc.
- Number fields, class groups of number fields,
- Zeta functions, L-functions,
- Elliptic curves, torsion subgroups of elliptic curves, ranks, Tate-Shafarevich groups,

among others.

Question

What is “Arithmetic Statistics”?

What **questions** are we trying to answer?

We fix a number-theoretic object and we ask:

- Do they exist?
- Are there finitely many or infinitely many such objects?
- Can we parametrize these objects in families?
- Is there a notion of “size” or “height”?
- How many objects are there up to a given height? Asymptotically?
- How many objects are there relative to another number-theoretic object?

Question

What is “Arithmetic Statistics”?

Examples:

- Prime numbers p, ordered by $|p|$, their absolute value.
- Prime numbers $p \equiv 1 \bmod 4$,

Question

What is “Arithmetic Statistics”?

Examples:

- Prime numbers p, ordered by $|p|$, their absolute value.
- Prime numbers $p \equiv 1 \bmod 4$, compared to the family of primes $p \equiv 3 \bmod 4$, ordered by $|p|$.
- Twin primes p, $q = p + 2$, ordered by $|p|$.
- Primes of the form $p = n^2 + 1$.
- Wieferich primes: p such that $2^{p-1} - 1$ is divisible by p^2.

Question

What is “Arithmetic Statistics”?

Examples:

- Binary quadratic forms $f(x, y) = ax^2 + bxy + cy^2$, ordered by their discriminant $|\operatorname{disc}(f)| = |b^2 - 4ac|$.
- Binary quadratic forms $f(x, y)$ ordered by $\max(|a|, |b|, |c|)$.
- Binary quadratic forms $f(x, y)$ of fixed discriminant.
- Higher-order binary forms (e.g., cubic).

Question

What is “Arithmetic Statistics”?

Examples:

- Number fields K, ordered by the absolute value of their discriminant $|\mathrm{Disc}(K)|$.
- Number fields up to $|\mathrm{Disc}(K)| \leq D$, filtered by a fixed invariant (e.g., fixed degree, or fixed Galois group $\mathrm{Gal}(K/\mathbb{Q}) = G$).
- Class groups $\mathrm{Cl}(K)$ of number fields up to a bound on the discriminant (e.g., class groups of imaginary quadratic fields).

Question

What is “Arithmetic Statistics”?

Examples:

- Elliptic curves $E/\mathbb{Q} : y^2 = x^3 + ax + b$, ordered by the absolute value of their discriminant $|16(4a^3 + 27b^2)|$.
- Elliptic curves $E/\mathbb{Q}$ ordered by their conductor.
- Torsion subgroups of elliptic curves up to a bound of their discriminant.
- Ranks of elliptic curves up to a bound of their discriminant (e.g., average rank up to a given bound).
- Tate-Shafarevich groups of elliptic curves up to a bound of their discriminant.

Prime Numbers

Prime Numbers

2, 3, 5, 7, 11, 13, 17, 19,...

Leonhard Euler
1707 – 1783

Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the mind will never penetrate.

The prime number theorem was formulated by Gauss, Legendre, and Dirichlet (1790's to 1820's) and proved by Hadamard, and de la Vallée-Poussin, in 1896.

Theorem (The Prime Number Theorem)

Let $\pi(X)$ be the cardinality of the set of prime numbers $2 \leq p \leq X$. Then:

$$\pi(X) \sim \frac{X}{\log X}, \qquad \textit{i.e.,} \qquad \lim_{X \to \infty} \frac{\pi(X)}{\frac{X}{\log X}} = 1.$$

A-M. Legendre
1752 – 1833

J. C. F. Gauss
1777 – 1855

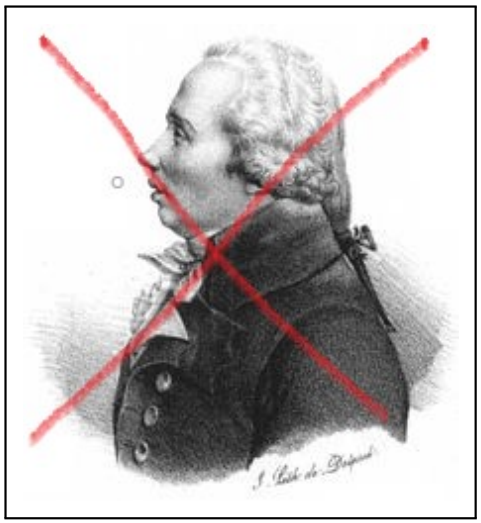
J. P. G. L. Dirichlet
1805 – 1859

The prime number theorem was formulated by Gauss, Legendre, and Dirichlet (1790's to 1820's) and proved by Hadamard, and de la Vallée-Poussin, in 1896.

Theorem (The Prime Number Theorem)

Let $\pi(X)$ be the cardinality of the set of prime numbers $2 \leq p \leq X$. Then:

$$\pi(X) \sim \frac{X}{\log X}, \qquad \textit{i.e.,} \qquad \lim_{X \to \infty} \frac{\pi(X)}{\frac{X}{\log X}} = 1.$$



A-M. Legendre
1752 – 1833

J. C. F. Gauss
1777 – 1855

J. P. G. L. Dirichlet
1805 – 1859

The prime number theorem was formulated by Gauss, Legendre, and Dirichlet (1790's to 1820's) and proved by Hadamard, and de la Vallée-Poussin, in 1896.

Theorem (The Prime Number Theorem)

Let $\pi(X)$ be the cardinality of the set of prime numbers $2 \leq p \leq X$. Then:

$$\pi(X) \sim \frac{X}{\log X}, \qquad \textit{i.e.,} \qquad \lim_{X \to \infty} \frac{\pi(X)}{\frac{X}{\log X}} = 1.$$

A-M. Legendre
1752 – 1833

J. C. F. Gauss
1777 – 1855

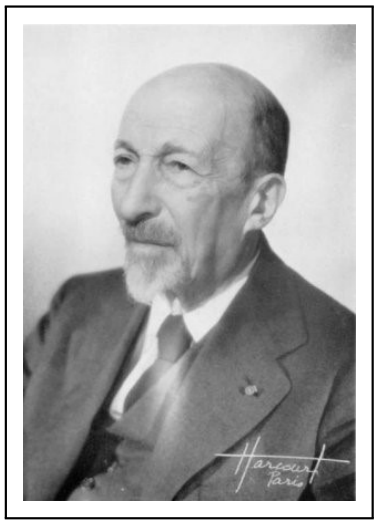
J. P. G. L. Dirichlet
1805 – 1859

The prime number theorem was formulated by Gauss, Legendre, and Dirichlet (1790's to 1820's) and proved by Hadamard, and de la Vallée-Poussin, in 1896.

Theorem (The Prime Number Theorem)

Let $\pi(X)$ be the cardinality of the set of prime numbers $2 \leq p \leq X$. Then:

$$\pi(X) \sim \frac{X}{\log X}, \qquad \textit{i.e.,} \qquad \lim_{X \to \infty} \frac{\pi(X)}{\frac{X}{\log X}} = 1.$$



Jacques Hadamard
1865 – 1963

C. J. de la Vallée Poussin
1866 – 1962

The prime number theorem was formulated by Gauss, Legendre, and Dirichlet (1790's to 1820's) and proved by Hadamard, and de la Vallée-Poussin, in 1896.

Theorem (The Prime Number Theorem)

Let $\pi(X)$ be the cardinality of the set of prime numbers $2 \leq p \leq X$. Then:

$$\pi(X) \sim \frac{X}{\log X}, \qquad \textit{i.e.,} \qquad \lim_{X \to \infty} \frac{\pi(X)}{\frac{X}{\log X}} = 1.$$

x	$\pi(x)$	$\frac{x}{ln(x)}$	$\frac{x}{ln(x)-1}$	$\int_2^x \frac{1}{ln(t)} dt$
10^2	25	22	28	29
10^3	168	145	169	177
10^4	1229	1086	1218	1245
10^5	9592	8686	9512	9629
10^6	78498	72382	78030	78627
10^7	664579	620421	661459	664917
10^8	5761455	5428681	5740304	5762208
10^9	50847534	48254942	50701542	50849234
10^{10}	455052511	434294482	454011971	455055614

Let us *conjecture* the prime number theorem, using a probabilistic/statistical approach.

Let us *conjecture* the prime number theorem, using a probabilistic/statistical approach.

ASSUMPTION: There is a "mathematical law" that describes the distribution of primes, in the following sense:

(a) For large n, we have $\pi(n) \approx \int_2^n W(x)dx$ (so that $W(x)$ can be interpreted as a probability density function of prime numbers).

(b) For $X \gg \Delta X$, we have $\pi(X + \Delta X) - \pi(X) \approx W(X) \cdot \Delta X$.

Let us *conjecture* the prime number theorem, using a probabilistic/statistical approach.

ASSUMPTION: There is a "mathematical law" that describes the distribution of primes, in the following sense:

(a) For large n, we have $\pi(n) \approx \int_2^n W(x)dx$ (so that $W(x)$ can be interpreted as a probability density function of prime numbers).

(b) For $X \gg \Delta X$, we have $\pi(X + \Delta X) - \pi(X) \approx W(X) \cdot \Delta X$.

Proposition (exercise!)

We have $\log(n!) \sim n \cdot \log n$*, or, in other words,* $\lim_{n\to\infty} \dfrac{\log(n!)}{n \cdot \log n} = 1$.

Now, let us give a second formula for $\log(n!)$ in terms of prime numbers.

Definition

For an integer a, we let $\nu_p(a)$ be the largest non-negative integer such that $p^{\nu_p(a)}$ divides a. In other words, $a = p^{\nu_p(a)} \cdot m$, with $\gcd(m, p) = 1$.

Since $\nu_p(ab) = \nu_p(a) + \nu_p(b)$, it follows that

$$\nu_p(n!) = \nu_p(1) + \nu_p(2) + \nu_p(3) + \cdots + \nu_p(n).$$

Definition

For an integer a, we let $\nu_p(a)$ be the largest non-negative integer such that $p^{\nu_p(a)}$ divides a. In other words, $a = p^{\nu_p(a)} \cdot m$, with $\gcd(m, p) = 1$.

Since $\nu_p(ab) = \nu_p(a) + \nu_p(b)$, it follows that

$$\nu_p(n!) = \nu_p(1) + \nu_p(2) + \nu_p(3) + \cdots + \nu_p(n).$$

For each $n, k \geq 1$, and prime p, define numbers:

$$N_k = N_{p,k}(n) = \#\{m \in \mathbb{N} : 1 \leq m \leq n, \text{ and } p^k \mid n\},$$

and

$$M_k = M_{p,k}(n) = \#\{m \in \mathbb{N} : 1 \leq m \leq n, \text{ and } \nu_p(m) = k\}.$$

Definition

For an integer a, we let $\nu_p(a)$ be the largest non-negative integer such that $p^{\nu_p(a)}$ divides a. In other words, $a = p^{\nu_p(a)} \cdot m$, with $\gcd(m, p) = 1$.

Since $\nu_p(ab) = \nu_p(a) + \nu_p(b)$, it follows that

$$\nu_p(n!) = \nu_p(1) + \nu_p(2) + \nu_p(3) + \cdots + \nu_p(n).$$

For each $n, k \geq 1$, and prime p, define numbers:

$$N_k = N_{p,k}(n) = \#\{m \in \mathbb{N} : 1 \leq m \leq n, \text{ and } p^k \mid n\},$$

and

$$M_k = M_{p,k}(n) = \#\{m \in \mathbb{N} : 1 \leq m \leq n, \text{ and } \nu_p(m) = k\}.$$

Then, $N_k \approx n/p^k$, and $M_k = N_k - N_{k+1} \approx n/p^k - n/p^{k+1}$. Hence:

$$\nu_p(n!) = 1 \cdot M_1 + 2 \cdot M_2 + 3 \cdot M_3 + \cdots .$$

$$
\begin{aligned}
\nu_p(n!) &= 1 \cdot M_1 + 2 \cdot M_2 + 3 \cdot M_3 + \cdots \\
&= 1 \cdot (N_1 - N_2) + 2 \cdot (N_2 - N_3) + 3 \cdot (N_3 - N_4) + \cdots \\
&= N_1 + N_2 + N_3 + \cdots \\
&\approx \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \cdots \\
&\approx \frac{n}{p} \cdot \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \\
&= \frac{n}{p} \cdot \frac{p}{p-1} = \frac{n}{p-1}.
\end{aligned}
$$

$$\begin{aligned}
\nu_p(n!) &= 1 \cdot M_1 + 2 \cdot M_2 + 3 \cdot M_3 + \cdots \\
&= 1 \cdot (N_1 - N_2) + 2 \cdot (N_2 - N_3) + 3 \cdot (N_3 - N_4) + \cdots \\
&= N_1 + N_2 + N_3 + \cdots \\
&\approx \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \cdots \\
&\approx \frac{n}{p} \cdot \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \\
&= \frac{n}{p} \cdot \frac{p}{p-1} = \frac{n}{p-1}.
\end{aligned}$$

Thus, for large n, we have

$$\begin{aligned}
\log(n!) &= \log\left(\prod_{2 \le p \le n} p^{\nu_p(n!)}\right) = \sum_{2 \le p \le n} \log\left(p^{\nu_p(n!)}\right) \\
&\approx \sum_{2 \le p \le n} \log\left(p^{n/(p-1)}\right) = \sum_{2 \le p \le n} \frac{n}{p-1} \cdot \log p.
\end{aligned}$$

Thus, we have deduced two asymptotic relations for $\log(n!)$, namely

$$n \cdot \log n \sim \log(n!) \sim \sum_{2 \leq p \leq n} \frac{n}{p-1} \cdot \log p.$$

Thus, we have deduced two asymptotic relations for $\log(n!)$, namely

$$n \cdot \log n \sim \log(n!) \sim \sum_{2 \leq p \leq n} \frac{n}{p-1} \cdot \log p.$$

Setting $n = X$, we obtain $\log X \sim \sum_{2 \leq p \leq X} \frac{\log p}{p-1}$.

Thus, we have deduced two asymptotic relations for $\log(n!)$, namely

$$n \cdot \log n \sim \log(n!) \sim \sum_{2 \leq p \leq n} \frac{n}{p-1} \cdot \log p.$$

Setting $n = X$, we obtain $\log X \sim \sum_{2 \leq p \leq X} \frac{\log p}{p-1}$.

We shall reinterpret the sum as a Riemann sum. Let

$$[2, X] = [2 = X_1, X_2] \cup [X_2, X_3] \cup \cdots \cup [X_r, X_{r+1} = X]$$

with $r \gg 0$ so that $\pi(X_{k+1}) - \pi(X_k) \approx W(X_k)\Delta X_k$ for each $0 \leq k \leq r$, and if $p \in [X_k, X_{k+1}]$, then $p \approx X_k$.

Thus, we have deduced two asymptotic relations for $\log(n!)$, namely

$$n \cdot \log n \sim \log(n!) \sim \sum_{2 \leq p \leq n} \frac{n}{p-1} \cdot \log p.$$

Setting $n = X$, we obtain $\log X \sim \sum_{2 \leq p \leq X} \frac{\log p}{p-1}$.

We shall reinterpret the sum as a Riemann sum. Let

$$[2, X] = [2 = X_1, X_2] \cup [X_2, X_3] \cup \cdots \cup [X_r, X_{r+1} = X]$$

with $r \gg 0$ so that $\pi(X_{k+1}) - \pi(X_k) \approx W(X_k)\Delta X_k$ for each $0 \leq k \leq r$, and if $p \in [X_k, X_{k+1}]$, then $p \approx X_k$. Then,

$$\log X \sim \sum_{2 \leq p \leq X} \frac{\log p}{p-1} = \sum_{j=1}^{r+1} W(X_j) \cdot \frac{\log(X_j)}{X_j - 1} \Delta X_j \sim \int_2^X W(t) \cdot \frac{\log t}{t-1} dt.$$

Note that if $\log X = \int_2^X W(t) \cdot \frac{\log t}{t-1} dt$, then taking derivatives we obtain

$$\frac{1}{X} = W(X) \frac{\log X}{X-1}$$

Note that if $\log X = \int_2^X W(t) \cdot \frac{\log t}{t-1} dt$, then taking derivatives we obtain

$$\frac{1}{X} = W(X) \frac{\log X}{X-1}$$

and therefore

$$W(X) = \frac{X-1}{X \log X} \approx \frac{1}{\log X}$$

for large X.

Note that if $\log X = \int_2^X W(t) \cdot \frac{\log t}{t-1} dt$, then taking derivatives we obtain

$$\frac{1}{X} = W(X) \frac{\log X}{X-1}$$

and therefore

$$W(X) = \frac{X-1}{X \log X} \approx \frac{1}{\log X}$$

for large X. It follows that

$$\pi(X) \sim \int_2^X W(t) dt \sim \int_2^X \frac{1}{\log t} dt.$$

Theorem (The Prime Number Theorem (Dirichlet))

Let $\pi(X)$ be the cardinality of the set of prime numbers $p \leq X$. Then:

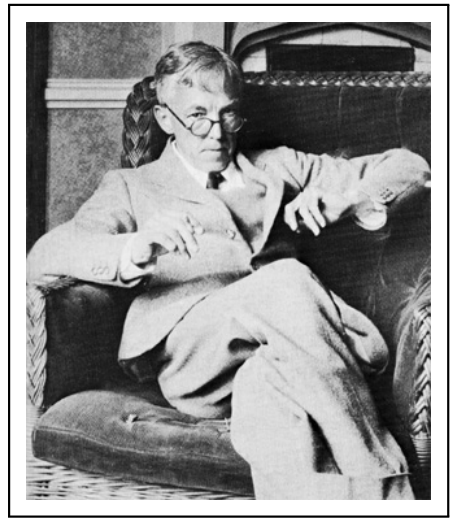
$$\pi(X) \sim \mathrm{Li}(X),$$

where $\mathrm{Li}(X) = \int_2^X \frac{1}{\log t} dt$.

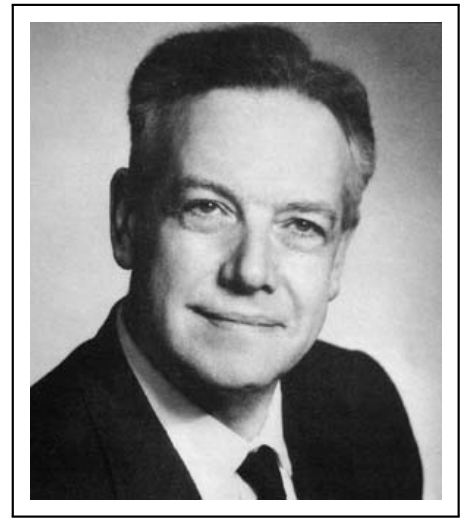
Warning! We have not proved the prime number theorem. We have proved that IF there is a probability density function $W(X)$ that describes the distribution of the prime numbers, then the distribution is $W(X) = 1/\log X$.

However, Dirichlet's theorem is true, and this motivates the heuristic that the probability that a number n is prime, should be approximately $1/\log n$. This heuristic has been used to motivate a number of conjectures.

Pierre de Fermat
1607 – 1665



G. H. Hardy
1877 – 1947



E. M. Wright
1906 – 2005

Conjecture

There are only finitely many Fermat primes.

Recall that a number of the form $F_n = 2^{2^n} + 1$, for $n \geq 0$, is called a Fermat number. If F_n is prime, then we call it a Fermat prime.

Conjecture

There are only finitely many Fermat primes.

Recall that a number of the form $F_n = 2^{2^n} + 1$, for $n \geq 0$, is called a Fermat number. If F_n is prime, then we call it a Fermat prime.

"**Proof.**" If the numbers F_n behave as random numbers, then each F_n is prime with probability $1/\log(F_n)$.

Conjecture

There are only finitely many Fermat primes.

Recall that a number of the form $F_n = 2^{2^n} + 1$, for $n \geq 0$, is called a Fermat number. If F_n is prime, then we call it a Fermat prime.

"**Proof.**" If the numbers F_n behave as random numbers, then each F_n is prime with probability $1/\log(F_n)$. Thus, the expected number of prime numbers among $F_0, F_1, F_2, \ldots$, is given by

$$\sum_{n=0}^{\infty} \frac{1}{\log(F_n)} = \sum_{n=0}^{\infty} \frac{1}{\log(2^{2^n}+1)} \leq \sum_{n=0}^{\infty} \frac{1}{\log(2^{2^n})}$$

$$= \sum_{n=0}^{\infty} \frac{1}{2^n \log(2)} = \frac{1}{\log 2} \sum_{n=0}^{\infty} \frac{1}{2^n} = \frac{2}{\log 2} = 2.8853\ldots$$

Conjecture

There are only finitely many Fermat primes.

Recall that a number of the form $F_n = 2^{2^n} + 1$, for $n \geq 0$, is called a Fermat number. If F_n is prime, then we call it a Fermat prime.

"**Proof.**" If the numbers F_n behave as random numbers, then each F_n is prime with probability $1/\log(F_n)$. Thus, the expected number of prime numbers among $F_0, F_1, F_2, \ldots$, is given by

$$\sum_{n=0}^{\infty} \frac{1}{\log(F_n)} = \sum_{n=0}^{\infty} \frac{1}{\log(2^{2^n}+1)} \leq \sum_{n=0}^{\infty} \frac{1}{\log(2^{2^n})}$$

$$= \sum_{n=0}^{\infty} \frac{1}{2^n \log(2)} = \frac{1}{\log 2} \sum_{n=0}^{\infty} \frac{1}{2^n} = \frac{2}{\log 2} = 2.8853\ldots$$

There are only 5 known Fermat primes: 3, 5, 17, 257, and 65537.

Conjecture (Twin Prime Conjecture)

There are infinitely many prime numbers p such that $q = p + 2$ is a also prime.

Such as (3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73), (101, 103), (107, 109), (137, 139),...

Range 1-x	Ten Power (x)	Number of Twin Primes $_2\pi(x)$
1-10	10^1	2
1-100	10^2	8
1-1,000	10^3	35
1-10,000	10^4	205
1-100,000	10^5	1,224
1-1,000,000	10^6	8,169
1-10,000,000	10^7	58,980
1-100,000,000	10^8	440,312
1-1,000,000,000	10^9	3,424,506
1-10,000,000,000	10^{10}	27,412,679
1-100,000,000,000	10^{11}	224,376,048
1-1,000,000,000,000	10^{12}	1,870,585,220
1-10,000,000,000,000	10^{13}	15,834,664,872
1-100,000,000,000,000	10^{14}	135,780,321,665
1-1,000,000,000,000,000	10^{15}	1,177,209,242,304
1-10,000,000,000,000,000	10^{16}	10,304,195,697,298

Conjecture (Twin Prime Conjecture)

There are infinitely many prime numbers p such that $q = p + 2$ is a also prime.

"**Proof.**" If n and $n + 2$ behave as independent random numbers, then n and $n + 2$ are simultaneously prime with probability

$$\frac{1}{\log n} \cdot \frac{1}{\log(n+2)}.$$

Conjecture (Twin Prime Conjecture)

There are infinitely many prime numbers p such that $q = p + 2$ is a also prime.

"**Proof.**" If n and $n + 2$ behave as independent random numbers, then n and $n + 2$ are simultaneously prime with probability $\frac{1}{\log n} \cdot \frac{1}{\log(n+2)}$. Thus, the expected number of twin primes up to $n \leq X$ is approximately

$$\sum_{n=2}^{X} \frac{1}{\log n} \cdot \frac{1}{\log(n+2)} \approx \sum_{n=2}^{X} \frac{1}{(\log n)^2} \approx \int_2^X \frac{1}{(\log t)^2} dt.$$

Conjecture (Twin Prime Conjecture)

There are infinitely many prime numbers p such that $q = p + 2$ is a also prime.

"**Proof.**" If n and $n + 2$ behave as independent random numbers, then n and $n + 2$ are simultaneously prime with probability $\frac{1}{\log n} \cdot \frac{1}{\log(n+2)}$. Thus, the expected number of twin primes up to $n \leq X$ is approximately

$$\sum_{n=2}^{X} \frac{1}{\log n} \cdot \frac{1}{\log(n+2)} \approx \sum_{n=2}^{X} \frac{1}{(\log n)^2} \approx \int_2^X \frac{1}{(\log t)^2} dt.$$

However, the independence cannot possibly be true (e.g., if n is even, $n + 2$ is even), so one expects that a proportion of numbers needs to be ruled out for congruence restrictions, so that the number of twin primes is approximately

$$C \cdot \int_2^X \frac{1}{(\log t)^2} dt \quad \text{for some constant } C.$$

Conjecture (Prime Constellation Conjecture; Hardy, Littlewood)

Let $C = 2 \cdot \prod_{p \geq 3} \left(1 - \frac{1}{(p-1)^2}\right) \approx 1.32032363\ldots$ *and let* $\pi_2(X)$ *be the number of primes* $p \leq X$ *such that* $q = p + 2$ *is also prime. Then,*

$$\pi_2(X) \sim C \cdot \int_2^X \frac{1}{(\log t)^2} dt.$$

G. H. Hardy
1877 – 1947

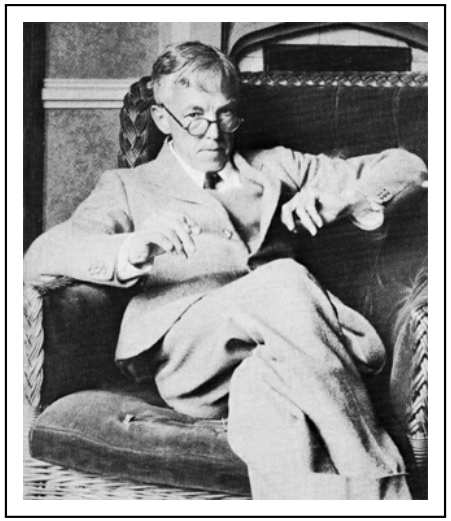
John Littlewood
1885 – 1977

Conjecture (Prime Constellation Conjecture; Hardy, Littlewood)

Let $a_1 = 0, a_2, \ldots, a_k$ be integers such that there is no prime p with the property that the set $\{a_i \bmod p\}$ covers all the values modulo p. Then, there are infinitely many prime constellations p, $p + a_2$,..., $p + a_k$, and the number of such primes $p \leq X$ is asymptotic to

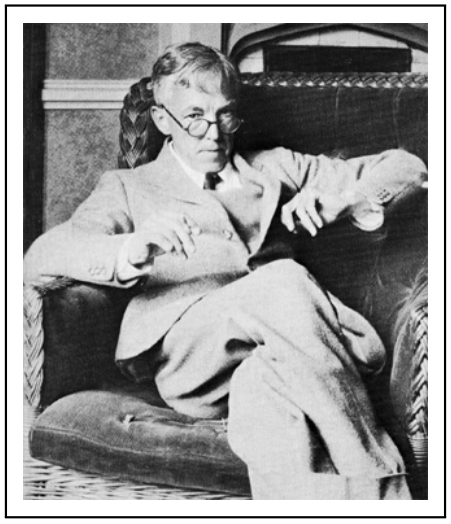
$$\pi_{a_1,\ldots,a_k}(X) \sim C_{a_1,\ldots,a_k} \cdot \int_2^X \frac{1}{(\log t)^k} dt,$$

for some explicit constant $C_{a_1,\ldots,a_k} > 0$.



G. H. Hardy

John Littlewood



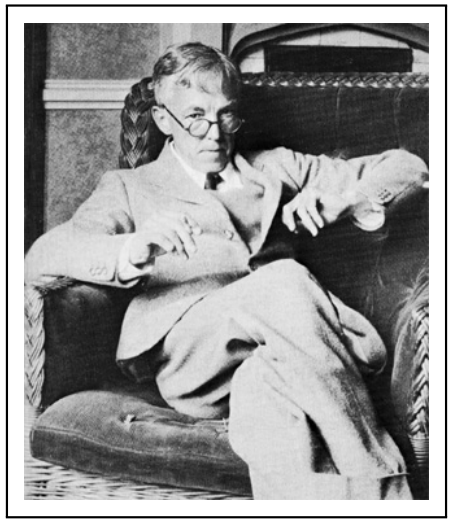
G. H. Hardy
1877 – 1947

John Littlewood
1885 – 1977

Conjecture ("2nd Conjecture"; Hardy, Littlewood)

Let $k \geq 1$ be fixed. Then all $n > 0$ sufficiently large, we have

$$\pi(k) \geq \pi(n+k) - \pi(n).$$



G. H. Hardy
1877 – 1947

John Littlewood
1885 – 1977

Conjecture ("2nd Conjecture"; Hardy, Littlewood)

Let $k \geq 1$ be fixed. Then all $n > 0$ sufficiently large, we have

$$\pi(k) \geq \pi(n+k) - \pi(n).$$

"**Proof.**" Clearly,

$$\sum_{j=2}^{k} \frac{1}{\log j} \gg \sum_{h=n+1}^{n+k} \frac{1}{\log h} \quad \text{for large enough } n.$$

WARNING! Heuristics can be misleading!

In 1973, Douglas Hensley and Ian Richards showed that the prime constellation and 2nd conjectures of Hardy and Littlewood are incompatible.

WARNING! Heuristics can be misleading!

In 1973, Douglas Hensley and Ian Richards showed that the prime constellation and 2nd conjectures of Hardy and Littlewood are incompatible.

- There is an admissible k-tuple (or prime constellation) of 447 integers $a_1 = 0, \ldots, a_{447} \leq 3159$.

WARNING! Heuristics can be misleading!

In 1973, Douglas Hensley and Ian Richards showed that the prime constellation and 2nd conjectures of Hardy and Littlewood are incompatible.

- There is an admissible k-tuple (or prime constellation) of 447 integers $a_1 = 0, \ldots, a_{447} \leq 3159$.
- By H-W's prime constellation conjecture, there must be infinitely many primes p such that $p, p + a_2, \ldots, p + a_{447}$ are primes in the interval $[p, p + 3159]$.

WARNING! Heuristics can be misleading!

In 1973, Douglas Hensley and Ian Richards showed that the prime constellation and 2nd conjectures of Hardy and Littlewood are incompatible.

- There is an admissible k-tuple (or prime constellation) of 447 integers $a_1 = 0, \ldots, a_{447} \leq 3159$.
- By H-W's prime constellation conjecture, there must be infinitely many primes p such that $p, p + a_2, \ldots, p + a_{447}$ are primes in the interval $[p, p + 3159]$.
- Thus, for each of those primes $\pi(p + 3159) - \pi(p - 1) \geq 447$.

WARNING! Heuristics can be misleading!

In 1973, Douglas Hensley and Ian Richards showed that the prime constellation and 2nd conjectures of Hardy and Littlewood are incompatible.

- There is an admissible k-tuple (or prime constellation) of 447 integers $a_1 = 0, \ldots, a_{447} \leq 3159$.
- By H-W's prime constellation conjecture, there must be infinitely many primes p such that $p, p + a_2, \ldots, p + a_{447}$ are primes in the interval $[p, p + 3159]$.
- Thus, for each of those primes $\pi(p + 3159) - \pi(p - 1) \geq 447$.
- However, $\pi(3160) = 446$.
- So $\pi(3160) < \pi(X + 3160) - \pi(X)$ would happen for infinitely many values of X, violating the 2nd conjecture.

WARNING! Heuristics can be misleading!

In 1973, Douglas Hensley and Ian Richards showed that the prime constellation and 2nd conjectures of Hardy and Littlewood are incompatible.

- There is an admissible k-tuple (or prime constellation) of 447 integers $a_1 = 0, \ldots, a_{447} \leq 3159$.
- By H-W's prime constellation conjecture, there must be infinitely many primes p such that $p, p + a_2, \ldots, p + a_{447}$ are primes in the interval $[p, p + 3159]$.
- Thus, for each of those primes $\pi(p + 3159) - \pi(p - 1) \geq 447$.
- However, $\pi(3160) = 446$.
- So $\pi(3160) < \pi(X + 3160) - \pi(X)$ would happen for infinitely many values of X, violating the 2nd conjecture.

Exercise: Find an admissible k-tuple $a_1 = 0, \ldots, a_{447} \leq 3159$.

Let p be an odd prime. By Fermat's little theorem we have $2^{p-1} \equiv 1 \bmod p$. Thus, $2^{p-1} \equiv 1 + pk \bmod p^2$.

Let p be an odd prime. By Fermat's little theorem we have $2^{p-1} \equiv 1 \bmod p$. Thus, $2^{p-1} \equiv 1 + pk \bmod p^2$.

Definition

An odd prime p is called a Wieferich prime (in base 2) if

$$2^{p-1} \equiv 1 \bmod p^2.$$

The first Wieferich prime is $p = 1093$ (Meissner, 1913). The second, $p = 3511$, was found by Beeger in 1922. If there is another one, the next Wieferich prime is $> 4.9 \cdot 10^{17}$.

Let p be an odd prime. By Fermat's little theorem we have $2^{p-1} \equiv 1 \bmod p$. Thus, $2^{p-1} \equiv 1 + pk \bmod p^2$.

Definition

An odd prime p is called a Wieferich prime (in base 2) if

$$2^{p-1} \equiv 1 \bmod p^2.$$

The first Wieferich prime is $p = 1093$ (Meissner, 1913). The second, $p = 3511$, was found by Beeger in 1922. If there is another one, the next Wieferich prime is $> 4.9 \cdot 10^{17}$.

Conjecture

The number of Wieferich primes up to X is approximately $\log(\log X)$.

Note: $\log(\log(10^3)) \approx 1.93$, $\log(\log(10^6)) \approx 2.62$, $\log(\log(10^{17})) \approx 3.60$.

Exercise: give a reasonable heuristic that justifies this conjecture.

Marie-Sophie Germain
$1776 - 1831$

Definition

A prime p is called a Sophie Germain prime if $q = 2p + 1$ is also prime.

For example: $(2, 5)$, $(3, 7)$, $(5, 11)$, $(11, 23)$, etc.

Marie-Sophie Germain
$1776 - 1831$

Definition

A prime p is called a Sophie Germain prime if $q = 2p + 1$ is also prime.

For example: $(2, 5)$, $(3, 7)$, $(5, 11)$, $(11, 23)$, etc.

Conjecture

There are infinitely many Sophie Germain primes.

Exercise: give a reasonable asymptotic for the number of Sophie Germain primes $p \leq X$.

THANK YOU

alvaro.lozano-robledo@uconn.edu

http://alozano.clas.uconn.edu

"*If by chance I have omitted anything*
more or less proper or necessary,
I beg forgiveness,
since there is no one who is without fault
and circumspect in all matters."

Leonardo Pisano (Fibonacci), *Liber Abaci*.