Primes, The Prime Number Theorem, And Applications

Evan P. Dummit

Northeastern University

Northeastern Math Club

September 12th, 2025

Outline of Talk

We will start with some basic facts about prime numbers and prime factorizations, and give an application or two.

Next, we will discuss the Prime Number Theorem, some history, and some of the different mathematical ideas involved in its statement and proof.

Finally, we will talk briefly about how the notion of a prime number can be generalized.

Primes!

Let's warm up with the definition of a prime number. Any takers?

Primes!

Let's warm up with the definition of a prime number. Any takers?

Definition

A prime number is a positive integer p such that there is no integer d with $1 < d < p$ that divides p.
A number n greater than 1 that is not prime is composite: it can be factored as $n = ab$ where $1 < a, b < n$.

Here are the 25 primes less than 100:

_____

Primes!

Let's warm up with the definition of a prime number. Any takers?

Definition

A prime number is a positive integer p such that there is no integer d with $1 < d < p$ that divides p.
A number n greater than 1 that is not prime is composite: it can be factored as $n = ab$ where $1 < a, b < n$.

Here are the 25 primes less than 100: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

We can see, for instance, that 57 is not prime[1], because $57 = 3 \cdot 19$.

[1] There is a famous apocryphal story told about Alexander Grothendieck, a quite eminent mathematician who developed a great deal of abstract algebraic geometry, in which when asked to give a specific example of a prime to which a result applied, he responded with "57".

Primes and Factorization, I

The primes are the "building blocks" of the integers under multiplication: every positive integer can be written as a product of primes, and primes are as "broken down" as possible.

Theorem (Prime Factorizations)

Every positive integer n has a prime factorization, meaning that it can be written as a product of zero or more primes.

Primes and Factorization, I

The primes are the "building blocks" of the integers under multiplication: every positive integer can be written as a product of primes, and primes are as "broken down" as possible.

Theorem (Prime Factorizations)

Every positive integer n has a prime factorization, meaning that it can be written as a product of zero or more primes.

- Proof: Induction on n. For the base case $n = 1$, take the empty product.
- For the inductive step, suppose all positive integers less than n have a prime factorization. If n is prime, then it is already factored, so assume $n = ab$ is composite with $1 < a, b < n$.
- Then both a and b are less than n and thus have prime factorizations: multiplying them gives a factorization of n.

Primes and Factorization, II

Here are some examples of prime factorizations:

- $14 =$

Primes and Factorization, II

Here are some examples of prime factorizations:

- $14 = 2 \cdot 7$.
- $16 =$

Primes and Factorization, II

Here are some examples of prime factorizations:

- $14 = 2 \cdot 7$.
- $16 = 2 \cdot 2 \cdot 2 \cdot 2$.
- $19 =$

Primes and Factorization, II

Here are some examples of prime factorizations:

- $14 = 2 \cdot 7$.
- $16 = 2 \cdot 2 \cdot 2 \cdot 2$.
- $19 = 19$.
- $27 =$

Primes and Factorization, II

Here are some examples of prime factorizations:

- $14 = 2 \cdot 7$.
- $16 = 2 \cdot 2 \cdot 2 \cdot 2$.
- $19 = 19$.
- $27 = 3 \cdot 3 \cdot 3$.
- $2025 =$

Primes and Factorization, II

Here are some examples of prime factorizations:

- $14 = 2 \cdot 7$.
- $16 = 2 \cdot 2 \cdot 2 \cdot 2$.
- $19 = 19$.
- $27 = 3 \cdot 3 \cdot 3$.
- $2025 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5$.
- $719558101 =$

Primes and Factorization, II

Here are some examples of prime factorizations:

- $14 = 2 \cdot 7$.
- $16 = 2 \cdot 2 \cdot 2 \cdot 2$.
- $19 = 19$.
- $27 = 3 \cdot 3 \cdot 3$.
- $2025 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5$.
- $719558101 = 19 \cdot 149 \cdot 433 \cdot 587$.

Question: Are prime factorizations unique?

Primes and Factorization, II

Here are some examples of prime factorizations:

- $14 = 2 \cdot 7$.
- $16 = 2 \cdot 2 \cdot 2 \cdot 2$.
- $19 = 19$.
- $27 = 3 \cdot 3 \cdot 3$.
- $2025 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5$.
- $719558101 = 19 \cdot 149 \cdot 433 \cdot 587$.

Question: Are prime factorizations unique?
Answer: No, for example, $14 = 2 \cdot 7 = 7 \cdot 2$ has two different factorizations.

Primes and Factorization, III

Okay, fine, writing the terms in a different order is a silly thing to do. Pleasantly, if we declare rearrangements of the same factors to be equivalent, then in fact every positive integer has only one possible prime factorization:

Primes and Factorization, III

Okay, fine, writing the terms in a different order is a silly thing to do. Pleasantly, if we declare rearrangements of the same factors to be equivalent, then in fact every positive integer has only one possible prime factorization:

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer has a prime factorization, and the factorization is unique up to rearranging the terms: if $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$ *where the* p_i *and* q_i *are primes, then* $k = l$ *and the* q_i *can be rearranged so that* $p_i = q_i$ *for each* i*.*

To prove this result we need another fact about prime numbers.

Primes and Factorization, IV: Saline Drip

To prove this result we need a fact about prime numbers.

Lemma (Euclid's Lemma / Prime Divisibility Property)

If p is a prime number and p divides a product ab, then p must divide at least one of the terms a and b.

This result requires a bit more work (and some results about common divisors) to establish and, in fact, is used by the professionals as the definition of a prime in other contexts.

Primes and Factorization, IV: Saline Drip

To prove this result we need a fact about prime numbers.

Lemma (Euclid's Lemma / Prime Divisibility Property)

If p is a prime number and p divides a product ab, then p must divide at least one of the terms a and b.

This result requires a bit more work (and some results about common divisors) to establish and, in fact, is used by the professionals as the definition of a prime in other contexts. We will take it[2] for granted here[3].

[2] But if you want to know how to prove Euclid's Lemma, you can do as any student should and just look it up on wikipedia: `https://en.wikipedia.org/wiki/Euclid%27s_lemma`

[3] The wikipedia article says that Bezout's lemma was unknown in Euclid's time, and that is not really an accurate summary of the history because of how the Greeks viewed numbers in geometric terms, as explained by Granville in 'It is not 'Bezout's identity'", `https://arxiv.org/abs/2406.15642`

Primes and Factorization, V

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer has a prime factorization, and the factorization is unique up to rearranging the terms.

- Proof: Induction on k. If $k = 0$ then $n = 1$ and the only possible factorization of 1 is the empty product.
- For the inductive step, suppose integers less than n have a unique prime factorization and $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$.
- Then p_k divides the product $q_1 q_2 \cdots q_l$ so by Euclid's Lemma, it divides some q_i, which by rearranging we can assume is q_l.
- Then because q_l is prime and $p_k > 1$ we must have $p_k = q_l$, and then $n/p_k = p_1 p_2 \cdots p_{k-1} = q_1 q_2 \cdots q_{l-1}$.
- Since this number is less than n, by induction its prime factorization is unique, and thus so is n's.

A Factorization Application

There are lots of applications of uniqueness of prime factorizations, but here is a pretty famous one.

Theorem (Irrationality of $\sqrt{2}$)

The number $\sqrt{2}$ is irrational, which is to say, there do not exist integers m and n such that $\sqrt{2} = m/n$.

A Factorization Application

There are lots of applications of uniqueness of prime factorizations, but here is a pretty famous one.

Theorem (Irrationality of $\sqrt{2}$)

The number $\sqrt{2}$ is irrational, which is to say, there do not exist integers m and n such that $\sqrt{2} = m/n$.

- Suppose by way of contradiction that $\sqrt{2}$ were rational, so that $\sqrt{2} = m/n$, so that $2n^2 = m^2$.

A Factorization Application

There are lots of applications of uniqueness of prime factorizations, but here is a pretty famous one.

Theorem (Irrationality of $\sqrt{2}$)

The number $\sqrt{2}$ is irrational, which is to say, there do not exist integers m and n such that $\sqrt{2} = m/n$.

- Suppose by way of contradiction that $\sqrt{2}$ were rational, so that $\sqrt{2} = m/n$, so that $2n^2 = m^2$. If m and n have prime factorizations $m = 2^{m_2}3^{m_3}\cdots$ and $n = 2^{n_2}3^{n_3}\cdots$, then $2n^2 = m^2$ gives $2^{2m_2+1}3^{m_3}\cdots = 2^{2n_2}3^{2n_3}\cdots$.
- By the uniqueness of prime factorizations, all of the corresponding exponents must be equal. In particular, $2m_2 + 1 = 2n_2$, but this is impossible since the left-hand side is odd and the right-hand side is even.
- This is a contradiction, so $\sqrt{2}$ cannot be rational.

How Many Primes?, I

There are lots of questions to ask about primes. Here's one:

Question

How many prime numbers are there?

Certainly there are at least 25, because I listed 25 primes earlier on: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Are there more?

How Many Primes?, I

There are lots of questions to ask about primes. Here's one:

Question

How many prime numbers are there?

Certainly there are at least 25, because I listed 25 primes earlier on: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Are there more? Sure, we could keep going: 101, 103, 107, 109

How Many Primes?, I

There are lots of questions to ask about primes. Here's one:

Question

How many prime numbers are there?

Certainly there are at least 25, because I listed 25 primes earlier on: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Are there more? Sure, we could keep going: 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181

How Many Primes?, I

There are lots of questions to ask about primes. Here's one:

Question

How many prime numbers are there?

Certainly there are at least 25, because I listed 25 primes earlier on: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Are there more? Sure, we could keep going: 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257

How Many Primes?, I

There are lots of questions to ask about primes. Here's one:

Question

How many prime numbers are there?

Certainly there are at least 25, because I listed 25 primes earlier on: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Are there more? Sure, we could keep going: 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419

How Many Primes?, I

There are lots of questions to ask about primes. Here's one:

Question

How many prime numbers are there?

Certainly there are at least 25, because I listed 25 primes earlier on: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Are there more? Sure, we could keep going: 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587

Do you think we are ever going to run out of primes?

How Many Primes?, II: Aye-Aye, Captain

Not enough? Okay, here's some more: 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997, 1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049, 1051, 1061, 1063, 1069, 1087, 1091, 1093, 1097, 1103, 1109, 1117, 1123, 1129, 1151, 1153, 1163, 1171, 1181, 1187, 1193, 1201, 1213, 1217, 1223, 1229, 1231, 1237, 1249, 1259, 1277, 1279, 1283, 1289, 1291, 1297, 1301, 1303, 1307, 1319, 1321, 1327, 1361, 1367, 1373, 1381, 1399, 1409, 1423, 1427, 1429, 1433, 1439, 1447, 1451, 1453, 1459, 1471, 1481, 1483, 1487, 1489, 1493, 1499, 1511, 1523, 1531, 1543, 1549, 1553, 1559, 1567, 1571, 1579, 1583, 1597, 1601, 1607, 1609, 1613, 1619, 1621, 1627, 1637, 1657, 1663, 1667, 1669, 1693, 1697, 1699, 1709, 1721, 1723, 1733, 1741, 1747, 1753, 1759, 1777, 1783, 1787, 1789, 1801, 1811, 1823, 1831, 1847, 1861, 1867, 1871, 1873, 1877, 1879, 1889, 1901, 1907, 1913, 1931, 1933, 1949, 1951, 1973, 1979, 1987, 1993, 1997, 1999, 2003, 2011, 2017, 2027....

How Many Primes?, III

In fact there are infinitely many primes, as shown by Euclid:

Theorem (Euclid's Theorem)

There are infinitely many prime numbers. Precisely, given a finite list $p_1, \ldots, p_k$ of primes, we can find a new prime not on the list.

How Many Primes?, III

In fact there are infinitely many primes, as shown by Euclid:

Theorem (Euclid's Theorem)

There are infinitely many prime numbers. Precisely, given a finite list $p_1, \ldots, p_k$ of primes, we can find a new prime not on the list.

- Proof: Suppose we have a list of primes $p_1, p_2, \ldots, p_k$, and consider $n = p_1 p_2 \cdots p_k + 1$.
- Since $n > 1$, let q be any prime divisor of n (possibly n itself).
- Suppose that q was one of the p_i: then p_i divides both $n = p_1 p_2 \cdots p_k + 1$ and also (clearly) the product $p_1 p_2 \cdots p_k$.
- But then p_i also divides the difference $n - p_1 p_2 \cdots p_k = 1$, which is impossible.
- Therefore, q is a new prime not on the list, as desired.

How Many Primes?, IV

Euclid's proof is very elegant, and it provides a basic answer to the question: there are infinitely many primes. But we can refine this question.

How Many Primes?, IV

Euclid's proof is very elegant, and it provides a basic answer to the question: there are infinitely many primes. But we can refine this question.

- Let's reformulate it and instead ask: how common are primes?
- It might not be entirely clear how to make this question precise, so let's try an experiment.

Fun, Argue-With-Your-Neighbor Activity

Rank the following four kinds of positive integers from least common to most common:

1. *Even numbers*
2. *Powers of 2*
3. *Perfect squares*
4. *Integers bigger than 10000*

How Many Primes?, V

This seems like a good general idea: count how many numbers are in each group and see which one is the biggest. Great!

How Many Primes?, V

This seems like a good general idea: count how many numbers are in each group and see which one is the biggest. Great! Data:

Group	Even	Power of 2	Square	>10000
≤ 10	5	4	3	0
≤ 30	15	5	5	0
≤ 100	50	7	10	0
≤ 300	150	9	17	0
≤ 1000	500	10	31	0
≤ 3000	1500	12	54	0
≤ 10000	5000	14	100	0
≤ 30000	15000	15	173	40000
≤ 100000	50000	17	316	90000

How Many Primes?, V

This seems like a good general idea: count how many numbers are in each group and see which one is the biggest. Great! Data:

Group	Even	Power of 2	Square	>10000
≤ 10	5	4	3	0
≤ 30	15	5	5	0
≤ 100	50	7	10	0
≤ 300	150	9	17	0
≤ 1000	500	10	31	0
≤ 3000	1500	12	54	0
≤ 10000	5000	14	100	0
≤ 30000	15000	15	173	40000
≤ 100000	50000	17	316	90000

The >10000 group is last for a while but then jumps into the lead. Even numbers are second, followed by squares, then powers of 2.

How Many Primes?, VI: Better Than Emacs

The point is that we are really interested in "asymptotic" behavior: how many of our numbers are in the range $[1, X]$ as X grows very large. For the numbers we just examined, we can describe the growth rates like this:

- The number of even numbers in the range $[1, X]$ is about $X/2$.

How Many Primes?, VI: Better Than Emacs

The point is that we are really interested in "asymptotic" behavior: how many of our numbers are in the range $[1, X]$ as X grows very large. For the numbers we just examined, we can describe the growth rates like this:

- The number of even numbers in the range $[1, X]$ is about $X/2$.
- The number of powers of 2 in the range $[1, X]$ is about $\log_2 X$.

How Many Primes?, VI: Better Than Emacs

The point is that we are really interested in "asymptotic" behavior: how many of our numbers are in the range $[1, X]$ as X grows very large. For the numbers we just examined, we can describe the growth rates like this:

- The number of even numbers in the range $[1, X]$ is about $X/2$.
- The number of powers of 2 in the range $[1, X]$ is about $\log_2 X$.
- The number of squares in the range $[1, X]$ is about $\sqrt{X}$.

How Many Primes?, VI: Better Than Emacs

The point is that we are really interested in "asymptotic" behavior: how many of our numbers are in the range $[1, X]$ as X grows very large. For the numbers we just examined, we can describe the growth rates like this:

- The number of even numbers in the range $[1, X]$ is about $X/2$.
- The number of powers of 2 in the range $[1, X]$ is about $\log_2 X$.
- The number of squares in the range $[1, X]$ is about $\sqrt{X}$.
- The number of >10000 numbers in the range $[1, X]$ is about X. (Yes, yes, it's actually $X - 10000$, but for big X, that's basically just X.)

So how about for primes? What does the number of primes in the range $[1, X]$ look like?

How Many Primes?, VII

Here, I'll add primes to the data table for you:

Group	Even	Power of 2	Square	> 10000	Primes
≤ 10	5	4	3	0	4
≤ 30	15	5	5	0	10
≤ 100	50	7	10	0	25
≤ 300	150	9	17	0	62
≤ 1000	500	10	31	0	168
≤ 3000	1500	12	54	0	430
≤ 10000	5000	14	100	0	1229
≤ 30000	15000	15	173	40000	3245
≤ 100000	50000	17	316	90000	9592

So what do you think? How fast does the number of primes grow?

How Many Primes?, VIII

It seems like the number of primes is growing fairly fast: a lot faster than squares. But it's not linear, like even numbers, since the proportion of numbers that are prime does seem to be going down:

X	10^1	10^2	10^3	10^4	10^5	10^6
Primes $\leq X$	4	25	168	1229	9592	78498
Proportion	0.400	0.250	0.168	0.123	0.096	0.078
1/ Proportion	2.500	4.000	5.952	8.136	10.425	12.739
Powers of 3 $\leq X$	2	4	6	8	10	12

How Many Primes?, VIII

It seems like the number of primes is growing fairly fast: a lot faster than squares. But it's not linear, like even numbers, since the proportion of numbers that are prime does seem to be going down:

X	10^1	10^2	10^3	10^4	10^5	10^6
Primes $\leq X$	4	25	168	1229	9592	78498
Proportion	0.400	0.250	0.168	0.123	0.096	0.078
1/ Proportion	2.500	4.000	5.952	8.136	10.425	12.739
Powers of 3 $\leq X$	2	4	6	8	10	12

It seems like the growth rate is something like $X/$ [something that grows slowly]. Roughly how fast does the denominator quantity (the 1 / Proportion row) grow?

(Ignore that row about powers of 3, I don't know why it's there.)

How Many Primes?, IX: X Marks The Spot

Actually... hmmm... it looks like the reciprocal of the proportion is growing at a similar rate as the number of powers of 3 less than or equal to X, which is essentially $\log_3 X$.

[4] Just as in every other mathematical situation ever!

How Many Primes?, IX: X Marks The Spot

Actually... hmmm... it looks like the reciprocal of the proportion is growing at a similar rate as the number of powers of 3 less than or equal to X, which is essentially $\log_3 X$.

- So if we unwind all of that, the number of primes less than or equal to X should be roughly equal to $\frac{X}{\log X}$ for some choice of logarithm.
- Which logarithm base should we take? Well, we can convert between any choices, but it turns out that the correct answer is the natural logarithm[4].

That is, in fact, the content of the Prime Number Theorem.

[4] Just as in every other mathematical situation ever!

The Prime Number Theorem, I

Now for the official statement:

Theorem (The Prime Number Theorem)

For a positive real number X, let $\Pi(X)$ be the number of primes in the interval $[1, X]$. We then have the asymptotic $\Pi(X) \sim \frac{X}{\ln X}$, in the sense that the ratio of these two quantities approaches 1 as $X \to \infty$. Explicitly, the limit $\lim_{X\to\infty} \frac{\Pi(x)}{X/\ln X}$ exists and equals 1.

The Prime Number Theorem, I

Now for the official statement:

Theorem (The Prime Number Theorem)

For a positive real number X, let $\Pi(X)$ be the number of primes in the interval $[1, X]$. We then have the asymptotic $\Pi(X) \sim \frac{X}{\ln X}$, in the sense that the ratio of these two quantities approaches 1 as $X \to \infty$. Explicitly, the limit $\lim_{X\to\infty} \frac{\Pi(x)}{X/\ln X}$ exists and equals 1.

The presence of the natural logarithm explains why using powers of 3 got fairly close, because the logarithm base $e = 2.718281828\ldots$ is pretty close to 3.

The Prime Number Theorem, II

As it happens, there is another formulation of the Prime Number Theorem that is actually much better:

Theorem (The Prime Number Theorem, Alternative)

For a positive real number X, let $\Pi(X)$ be the number of primes in the interval $[1, X]$, and let $\mathrm{Li}(X)$ denote the logarithmic integral given by $\mathrm{Li}(X) = \displaystyle\int_2^X \frac{1}{\ln t}\, dt$. Then $\Pi(X) \sim \mathrm{Li}(X)$ as $X \to \infty$.

The Prime Number Theorem, II

As it happens, there is another formulation of the Prime Number Theorem that is actually much better:

Theorem (The Prime Number Theorem, Alternative)

For a positive real number X, let $\Pi(X)$ be the number of primes in the interval $[1, X]$, and let $\mathrm{Li}(X)$ denote the logarithmic integral given by $\mathrm{Li}(X) = \int_2^X \frac{1}{\ln t}\, dt$. Then $\Pi(X) \sim \mathrm{Li}(X)$ as $X \to \infty$.

In fact, this version of the theorem is equivalent to the version with $X/\ln(X)$, in that either version of the theorem implies the other. To see why, we need to do a little calculus[5].

[5] Really, shouldn't it be we *get* to do a little calculus?

The Prime Number Theorem, III

Let's see why $\mathrm{Li}(X) = \displaystyle\int_2^X \frac{1}{\ln t}\,dt$ is roughly $\dfrac{X}{\ln X}$.

- Integrating by parts yields $\displaystyle\int_2^X \frac{1}{\ln t}\,dt = \frac{X}{\ln X} - \frac{2}{\ln 2} - \int_2^X \frac{1}{(\ln t)^2}\,dt$. Then,

$$\begin{aligned}\int_2^X \frac{1}{(\ln t)^2}\,dt &= \int_2^{\sqrt{X}} \frac{1}{(\ln t)^2}\,dt + \int_{\sqrt{X}}^X \frac{1}{(\ln t)^2}\,dt \\ &\leq \sqrt{X}\cdot\frac{1}{(\ln 2)^2} + X\cdot\frac{4}{(\ln X)^2}.\end{aligned}$$

- So this means the second integral is much smaller (by a factor of $4/\ln X$) than $X/\ln X$, so asymptotically, $\mathrm{Li}(x) \sim X/\ln X$.

The Prime Number Theorem, IV

So why do I say that the logarithmic integral is a better approximation? Well, just take a look:

X	$\Pi(X)$	$X/\ln X$	$\mathrm{Li}(X)$	$\Pi(X) - \frac{X}{\ln X}$	$\Pi(X) - \mathrm{Li}(X)$
10	4	4	5	0	-1
10^2	25	22	29	3	-4
10^3	168	145	177	23	-9
10^4	1229	1086	1245	143	-16
10^5	9592	8686	9268	906	-37
10^6	78498	72382	78627	6116	-129
10^7	664579	620421	664917	44158	-338
10^8	5761455	5426811	5762208	332774	-753

The logarithmic integral's errors are much, much smaller!

The Prime Number Theorem, V

The Prime Number Theorem has a long history. Early history:

- It was known since antiquity (Euclid, 2000 years ago) that there are infinitely many primes.
- The first published statement of something like PNT was due to Legendre in 1798: he said $\Pi(X) = X/(a \ln X + b)$ for some constants a and b, and refined a decade later to $\Pi(X) = X/(\ln X + A(X))$ for a function $A(X) \approx 1.08366\ldots$.

[6] He used tables of primes compiled by others; he didn't do it all himself!

The Prime Number Theorem, V

The Prime Number Theorem has a long history. Early history:

- It was known since antiquity (Euclid, 2000 years ago) that there are infinitely many primes.
- The first published statement of something like PNT was due to Legendre in 1798: he said $\Pi(X) = X/(a \ln X + b)$ for some constants a and b, and refined a decade later to $\Pi(X) = X/(\ln X + A(X))$ for a function $A(X) \approx 1.08366\ldots$.
- Gauss, however, had done his own studies on primes already, in 1792, and came up with the heuristic that the number of primes in $[a, b]$ should be approximately $\int_a^b \frac{1}{\ln t}\, dt$.
- He checked by hand[6], for instance, that there were 6762 primes between 2,600,000 and 2,700,000, while $\int_{2600000}^{2700000} \frac{1}{\ln t}\, dt = 6761.33$. Pretty good!

[6] He used tables of primes compiled by others; he didn't do it all himself!

The Prime Number Theorem, VI

Another important step along the way came from Euler in the mid-1700s, with a new proof that there are infinitely many primes. Here is the motivation for his argument:

- Observe that $(1+\frac{1}{2}+\frac{1}{4})(1+\frac{1}{3}) =$
  $1+\frac{1}{2}+\frac{1}{4}+\frac{1}{3}+\frac{1}{6}+\frac{1}{12} = 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{6}+\frac{1}{12}.$
- The product contains the terms $1/n$ for all n that are a product of one of $\{1,2,4\}$ with one of $\{1,3\}$.

The Prime Number Theorem, VI

Another important step along the way came from Euler in the mid-1700s, with a new proof that there are infinitely many primes. Here is the motivation for his argument:

- Observe that $(1+\frac{1}{2}+\frac{1}{4})(1+\frac{1}{3}) = 1+\frac{1}{2}+\frac{1}{4}+\frac{1}{3}+\frac{1}{6}+\frac{1}{12} = 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{6}+\frac{1}{12}$.
- The product contains the terms $1/n$ for all n that are a product of one of $\{1,2,4\}$ with one of $\{1,3\}$.
- Euler's observation is that if we extend this product to include all possible terms: namely, $1+\frac{1}{p}+\frac{1}{p^2}+\cdots+\frac{1}{p^k}+\cdots$ for a prime p, then the resulting distributed product over all primes p will be the sum over all terms $1/n$ for all positive integers n.

The Prime Number Theorem, VII

Here's Euler's proof:

- Suppose $p_1, \ldots, p_k$ are all the primes.
- By unique factorization, if we distribute out the product $\left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \cdots\right)\left(1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \cdots\right) \cdots \left(1 + \frac{1}{p_k} + \frac{1}{p_k^2} + \cdots\right)$ then we will get a sum of terms of the form $1/n$ where n ranges over all positive integers whose prime factors are among $p_1, p_2, \ldots, p_k$.

The Prime Number Theorem, VII

Here's Euler's proof:

- Suppose $p_1, \ldots, p_k$ are all the primes.
- By unique factorization, if we distribute out the product $\left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \cdots\right)\left(1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \cdots\right) \cdots \left(1 + \frac{1}{p_k} + \frac{1}{p_k^2} + \cdots\right)$ then we will get a sum of terms of the form $1/n$ where n ranges over all positive integers whose prime factors are among $p_1, p_2, \ldots, p_k$.
- This is every positive integer, so the sum is just the harmonic series $1 + \frac{1}{2} + \frac{1}{3} + \cdots$, which diverges to infinity.
- But, each of the terms in the product is a geometric series, and using the formula $1 + r + r^2 + \cdots = 1/(1-r)$, we see the product is just $\frac{1}{1-1/p_1} \cdot \frac{1}{1-1/p_2} \cdots \frac{1}{1-1/p_k}$, which is finite.
- That's impossible, as we just said the product was infinite!

The Prime Number Theorem, VIII

Euler's proof contains a very important lesson, namely, that we can prove things about arithmetic (that there are infinitely many prime numbers) using analysis (that the harmonic series diverges).

This idea is at the heart of many major results in 19th-century number theory, including the proof of the Prime Number Theorem.

The Prime Number Theorem, VIII

Euler's proof contains a very important lesson, namely, that we can prove things about arithmetic (that there are infinitely many prime numbers) using analysis (that the harmonic series diverges).

This idea is at the heart of many major results in 19th-century number theory, including the proof of the Prime Number Theorem. Here's one such result, proven in 1837 by Dirichlet:

Theorem (Primes in Arithmetic Progressions)

Suppose a is relatively prime to m. Then there are infinitely many primes in the arithmetic sequence $\{a, a+m, a+2m, a+3m, \dots\}$. Equivalently, there are infinitely many primes congruent to a modulo m.

For example, taking $a = 1$ and $m = 10$ implies that there are infinitely many primes with units digit 1.

The Zeta Function, I: For One Like Roman Numerals

Dirichlet's brilliant idea was to study a special function now named after Riemann: the zeta function.

Definition

The Riemann zeta function is the infinite series $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.

The Zeta Function, I: For One Like Roman Numerals

Dirichlet's brilliant idea was to study a special function now named after Riemann: the zeta function.

Definition

The Riemann zeta function is the infinite series $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.

You may be wondering: what exactly is s?

- This series for the zeta function was actually considered by Euler much earlier, and he (and others like Dirichlet) took s to be a real number. Using the integral test, one can see that the series above only converges when $s > 1$.
- As shown by Euler, using the idea from his proof earlier, the zeta function can also be written as an infinite product over primes: $\zeta(s) = \prod_{p \text{ prime}} \frac{1}{(1 - p^{-s})}$ when $s > 1$.

The Zeta Function, II

The insight of Riemann was to consider the series $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ for complex values of s, not just real values.

- Riemann in his (only!) paper on the zeta function, in 1857, showed that complex-analytic properties of the zeta function are deeply connected with properties of the prime numbers.
- To give a vague idea: as Euler showed, the fact that the series for $\zeta(s)$ diverges at $s = 1$ (equivalently, that $\zeta(s)$ has a pole at $s = 1$) implies that there are infinitely many primes.

The Zeta Function, II

The insight of Riemann was to consider the series $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ for complex values of s, not just real values.

- Riemann in his (only!) paper on the zeta function, in 1857, showed that complex-analytic properties of the zeta function are deeply connected with properties of the prime numbers.
- To give a vague idea: as Euler showed, the fact that the series for $\zeta(s)$ diverges at $s = 1$ (equivalently, that $\zeta(s)$ has a pole at $s = 1$) implies that there are infinitely many primes.
- By comparing the sum and product expansions of $\zeta(s)$, one can write more explicit formulas relating prime-counting functions and the zeta function.
- In particular, Riemann was able to connect the asymptotic growth of the prime-counting function $\Pi(X)$ to the existence and distribution of the zeroes of $\zeta(s)$.

The Zeta Function, III: Ay-yi-yi Title Joke

In this paper, Riemann posed his famous hypothesis, that all of the nontrivial zeroes of the zeta function lie on the line $\mathrm{Re}(s) = 1/2$.

- This conjecture is still unresolved to this day, and it is (almost certainly) the biggest open problem in mathematics.

The Zeta Function, III: Ay-yi-yi Title Joke

In this paper, Riemann posed his famous hypothesis, that all of the nontrivial zeroes of the zeta function lie on the line $\mathrm{Re}(s) = 1/2$.

- This conjecture is still unresolved to this day, and it is (almost certainly) the biggest open problem in mathematics.

The Prime Number Theorem was finally proven in 1896, independently, by Hadamard and de la Vallee Poussin.

- Both of their proofs relied on establishing that there are no zeroes of the zeta function on the line $\mathrm{Re}(s) = 1$: this piece of information turns out to be strong enough to establish the estimate in the Prime Number Theorem.
- Sadly, explaining how this works in detail would require an entire semester's worth of complex analysis (Math 4555) and also analytic number theory (usually in Math 4527)... but I'd be happy to tell you once you've learned those things!

The Zeta Function, IV

Ultimately, the Prime Number Theorem can be formulated in terms of an asymptotic estimate for the prime-counting function $\Pi(X)$.

- The version proven by Hadamard and de la Vallee Poussin is equivalent to saying that $\Pi(X) = \mathrm{Li}(X) + o\left(\frac{X}{(\ln X)^2}\right)$.

The Zeta Function, IV

Ultimately, the Prime Number Theorem can be formulated in terms of an asymptotic estimate for the prime-counting function $\Pi(X)$.

- The version proven by Hadamard and de la Vallee Poussin is equivalent to saying that $\Pi(X) = \mathrm{Li}(X) + o\left(\dfrac{X}{(\ln X)^2}\right)$.
- Here, the o-notation means that $\Pi(X)$ equals $\mathrm{Li}(X)$ plus an error term that is bounded by a fixed constant times $\dfrac{X}{(\ln X)^2}$.
- Since $\mathrm{Li}(X)$ equals $\dfrac{X}{\ln X}$ plus an error term of that same exact size (as we saw before) this also says $\Pi(X) = \dfrac{X}{\ln X} + o\left(\dfrac{X}{(\ln X)^2}\right)$.

The Zeta Function, V: For Vendetta

Here's a fun question: what's the best possible bound we can give for the error term in the Prime Number Theorem?

- It turns out that it depends on which approximation we use! If we use the logarithmic integral approximation (which we saw was numerically much better) then we have the following conjecture:

Conjecture (Conjectured Prime-Counting Estimate)

We have the asymptotic $\Pi(X) = \mathrm{Li}(X) + o\left(\sqrt{X}\ln X\right)$, *with the error term on the order of* $\sqrt{X}\ln X$.

This conjecture is unresolved, and for a pretty good reason: it's actually *equivalent* to the Riemann hypothesis!

What Is A Prime, Really?

Okay, so, that's the Prime Number Theorem in a nutshell. There are lots of other conjectures and theorems about primes out there (the Mersenne prime conjecture, the Green-Tao theorem, the Goldbach conjecture, the twin prime conjecture, conjectures about Fermat primes, the bounded prime gap theorem, etc.).

But what I want to wrap the talk up with is this question: how can we generalize the idea of a prime? The fundamental idea, really, is the notion of unique factorization.

(pause for audience to think about things they have "factored" before)

Primes and Polynomials, I

In fact, as you may have heard, polynomials also have unique factorization! For polynomials, the analogue of a prime number is an irreducible polynomial: a polynomial that doesn't have any nontrivial factorization.

Primes and Polynomials, I

In fact, as you may have heard, polynomials also have unique factorization! For polynomials, the analogue of a prime number is an irreducible polynomial: a polynomial that doesn't have any nontrivial factorization.

- Example: For polynomials with real coefficients, $x - 3$ and $x^2 + 1$ are irreducible, but $x^2 - x - 2$ is not, since $x^2 - x - 2 = (x - 2)(x + 1)$.

Primes and Polynomials, I

In fact, as you may have heard, polynomials also have unique factorization! For polynomials, the analogue of a prime number is an irreducible polynomial: a polynomial that doesn't have any nontrivial factorization.

- Example: For polynomials with real coefficients, $x - 3$ and $x^2 + 1$ are irreducible, but $x^2 - x - 2$ is not, since $x^2 - x - 2 = (x - 2)(x + 1)$.
- Example: For polynomials with rational coefficients, $x^2 - 2$ and $x^3 - 5$ are irreducible, but $x^4 + 4$ is not, since $x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2)$.

Primes and Polynomials, II: Attack of the Clones

Is there a Prime Number Theorem for polynomials? Well... sort of!

- One issue is that we need to specify where the coefficients come from: after all, $x^2 - 2$ is irreducible if we only allow rational number coefficients, but it factors as $(x - \sqrt{2})(x + \sqrt{2})$ if we allow real numbers.
- If we fix the field of coefficients F, then we could ask: how many irreducible polynomials are there of a given degree d?

Primes and Polynomials, II: Attack of the Clones

Is there a Prime Number Theorem for polynomials? Well... sort of!

- One issue is that we need to specify where the coefficients come from: after all, $x^2 - 2$ is irreducible if we only allow rational number coefficients, but it factors as $(x - \sqrt{2})(x + \sqrt{2})$ if we allow real numbers.
- If we fix the field of coefficients F, then we could ask: how many irreducible polynomials are there of a given degree d?
- For lots of fields the answer is a sad "infinitely many". For example, with rational coefficients all of the polynomials $x - \alpha$ are irreducible for any rational number α.
- We will only get a finite number if the field F itself is finite: for example, if F is the field $\mathbb{Z}/p\mathbb{Z}$ of integers modulo p where p is a prime.

Primes and Polynomials, III

We can, however, count irreducible polynomials over finite fields:

Theorem (Counting Irreducible Polynomials)

Let F be a finite field of cardinality q. Then the number of monic irreducible polynomials of degree n with coefficients in F is $\frac{1}{n}q^n + o(q^{n/2})$.

Primes and Polynomials, III

We can, however, count irreducible polynomials over finite fields:

Theorem (Counting Irreducible Polynomials)

Let F be a finite field of cardinality q. Then the number of monic irreducible polynomials of degree n with coefficients in F is $\frac{1}{n}q^n + o(q^{n/2})$.

There is actually an exact formula involving the "Mobius μ-function" (for the initiated, the formula is $\frac{1}{n}\sum_{d|n}\mu(d)q^{n/d}$).

- Example: The number of irreducible monic quadratic polynomials is $(q^2 - q)/2$, while the number of irreducible monic polynomials of degree 4 is $(q^4 - q^2)/2$.

Primes and Polynomials, IV: A New Hope

Let's rephrase this polynomial-counting result. A monic polynomial of degree n has a total of n possible coefficients, so there are $X = q^n$ such polynomials.

- So, in terms of that number X, the theorem says that the number of irreducible polynomials is equal to $\frac{1}{n}q^n + o(q^{n/2}) = \frac{X}{\log_q X} + o(\sqrt{X})$.
- And that looks exactly like the "best possible" error bound conjectured by the Riemann hypothesis! (Well, except for the different logarithm base.)
- Why does it work out like that? Because, in fact, we can actually prove the Riemann hypothesis in the polynomial case. (This is the "Riemann hypothesis for function fields"[7].)

[7] To learn more, take Math 7360: Number Theory in Function Fields!

Wrap-Up

There is a vast amount more to say about primes, of course – there are even more general rings of numbers (for instance, the famous Gaussian integers $a + bi$ where a and b are integers) where we can formulate the notion of a prime, and we can prove analogues of many of these results in those general settings.

- If you're interested in seeing more, what you want to do is learn some number theory!
- We offer two undergraduate courses in number theory: Math 3527 (Number Theory 1) and Math 4527 (Number Theory 2). Keep an eye out for them!

Thanks!

Thanks to Toby Busick-Warner and the other math club organizers for providing me the opportunity to speak here today!

Please also allow me to advertise the Putnam Club, which meets Wednesdays from 6pm-7:30pm in 509 Lake. We get together to (try to) solve some problems from old Putnam exams, and also eat pizza. If you like competition math and/or problem-solving, come check us out!

I hope you enjoyed my talk, and I'd like to thank you for attending! Enjoy your weekend!