Counting Different Kinds of Prime Numbers

Cooper O'Kuhn

November 5, 2020

Preliminaries

Prime Number: a natural number p with no factors besides trivially 1 and p itself.

Preliminaries

Prime Number: a natural number p with no factors besides trivially 1 and p itself.

Examples:

2 and 3 are prime. 4 is not prime because $4 = 2 \times 2$. 5 is prime. 6 is not prime because $6 = 2 \times 3$. etc.

Preliminaries

Prime Number: a natural number p with no factors besides trivially 1 and p itself.

Examples:

2 and 3 are prime. 4 is not prime because $4 = 2 \times 2$. 5 is prime. 6 is not prime because $6 = 2 \times 3$. etc.

Theorem (Fundamental Theorem of Arithmetic)

Every natural number can be written as the product of primes numbers uniquely (up to permutation of the factors)

Preliminaries

Prime Number: a natural number p with no factors besides trivially 1 and p itself.

Examples:

2 and 3 are prime. 4 is not prime because $4 = 2 \times 2$. 5 is prime. 6 is not prime because $6 = 2 \times 3$. etc.

Theorem (Fundamental Theorem of Arithmetic)

Every natural number can be written as the product of primes numbers uniquely (up to permutation of the factors)

Examples:

$30 = 2 \times 3 \times 5; 74 = 37 \times 2; 100 = 2 \times 2 \times 5 \times 5$ or $2^2 \times 5^2$

Counting Primes Themselves

Theorem (Infinitely Many Primes, Euclid)

There are infinitely many prime numbers.

Counting Primes Themselves

Theorem (Infinitely Many Primes, Euclid)

There are infinitely many prime numbers.

For a real number x, define

$$\pi(x) := \#\{\text{prime } p : p \leq x\}.$$

Counting Primes Themselves

Theorem (Infinitely Many Primes, Euclid)

There are infinitely many prime numbers.

For a real number x, define

$$\pi(x) := \#\{\text{prime } p : p \leq x\}.$$

E.g.

$$\pi(10) = \#\{2, 3, 5, 7\} = 4, \;\; 40\ \%.$$

$$\pi(100) = \#\{2, 3, 5, 7, ..., 83, 89, 97\} = 25, \;\; 25\ \%$$

$$\pi(1000) = \#\{2, 3, 5, 7, ..., 983, 997\} = 168, \;\; 16.8\ \%.$$

The Prime Number Theorem

Theorem (Hadamard, de la Vallee Poussin, 1896)

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

The Prime Number Theorem

Theorem (Hadamard, de la Vallee Poussin, 1896)

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

i.e.

$$\lim_{x \to \infty} \frac{\pi(x)}{\left(\frac{x}{\ln x}\right)} = 1.$$

The Prime Number Theorem

Theorem (Hadamard, de la Vallee Poussin, 1896)

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

i.e.

$$\lim_{x \to \infty} \frac{\pi(x)}{\left(\frac{x}{\ln x}\right)} = 1.$$

More specifically,

$$\pi(x) \sim Li(x)$$

where

$$Li(x) = \int_2^x \frac{1}{\ln t} dt \sim \frac{x}{\ln x}.$$

Prime Number Theorem, Examples

x	$\pi(x)$	$x/\ln(x)$	% Error
100	25	22	12%
1,000	168	144	14%
10,000	1229	1085	11%

x	$\pi(x)$	$Li(x)$	% Error
100	25	29	16%
1,000	168	176	4.8%
10,000	1229	1245	1.5%

Primes in Arithmetic Progressions

Question

How do primes behave in arithmetic progressions? e.g. Primes p of the form $p = 4k + 1$ i.e. $1 \bmod 4$ like 5,17,37, etc.

Primes in Arithmetic Progressions

Question

How do primes behave in arithmetic progressions? e.g. Primes p of the form $p = 4k + 1$ i.e. $1 \bmod 4$ like 5,17,37, etc.

Modulus and remainder must be coprime i.e. not share any common factors. ex: 9k + 3 versus 9k + 4.

Primes in Arithmetic Progressions

Question

How do primes behave in arithmetic progressions? e.g. Primes p of the form $p = 4k + 1$ i.e. $1 \bmod 4$ like 5,17,37, etc.

Modulus and remainder must be coprime i.e. not share any common factors. ex: 9k + 3 versus 9k + 4.

Theorem (Dirichlet)

If a and q are coprime, then there are infinitely many primes which are $a \bmod q$.

Prime Number Theorem in Arithmetic Progressions

Question

Do primes favor certain arithmetic progressions over others? For instance, are there more primes which have last digit 1 than there are primes with last digit 3?

Prime Number Theorem in Arithmetic Progressions

Question

Do primes favor certain arithmetic progressions over others? For instance, are there more primes which have last digit 1 than there are primes with last digit 3?

Let $\phi(q)$ be the number of natural numbers coprime and less than or equal to q. Ex: $\phi(9) = \#\{1, 2, 4, 5, 7, 8\} = 6$.

Prime Number Theorem in Arithmetic Progressions

Question

Do primes favor certain arithmetic progressions over others? For instance, are there more primes which have last digit 1 than there are primes with last digit 3?

Let $\phi(q)$ be the number of natural numbers coprime and less than or equal to q. Ex: $\phi(9) = \#\{1, 2, 4, 5, 7, 8\} = 6$.

Let $\pi(x; a, q) := \#\{p \equiv a \bmod q : p \leq x\}$

Prime Number Theorem in Arithmetic Progressions

Question

Do primes favor certain arithmetic progressions over others? For instance, are there more primes which have last digit 1 than there are primes with last digit 3?

Let $\phi(q)$ be the number of natural numbers coprime and less than or equal to q. Ex: $\phi(9) = \#\{1,2,4,5,7,8\} = 6$.

Let $\pi(x; a, q) := \#\{p \equiv a \bmod q : p \leq x\}$
Example: last digit of the primes less than x.

x	$\pi(x;1,10)$	$\pi(x;3,10)$	$\pi(x;7,10)$	$\pi(x;9,10)$	$\frac{\pi(x)}{4}$
100	5	7	6	5	6
1000	40	42	46	38	42
10000	306	310	308	303	307

Example of PNT in Arithmetic Progressions

Theorem (PNT for Arithmetic Progressions)

For fixed q, we have, as x goes to infinity,

$$\pi(x; a, q) \sim \frac{\pi(x)}{\phi(q)}.$$

Uniformity in q

Question

How large can we make q so that the PNT in arithmetic progression still holds? Can q grow with x?

Motivations: sieve theory, pushing theorems to their limits, Generalized Riemann Hypothesis (GRH).

Uniformity in q

Question

How large can we make q so that the PNT in arithmetic progression still holds? Can q grow with x?

Motivations: sieve theory, pushing theorems to their limits, Generalized Riemann Hypothesis (GRH).

Theorem

If GRH holds, then for any small fixed $\varepsilon > 0$ and all $q < x^{\frac{1}{2}-\varepsilon}$, we have

$$\pi(x; a, q) \sim \frac{\pi(x)}{\phi(q)}$$

as x goes to infinity.

Siegel-Walfisz Theorem

Theorem (Siegel-Walfisz)

Let $A > 0$ be a large real number. For any $q < (\ln x)^A$, we have

$$\pi(x; a, q) \sim \frac{\pi(x)}{\phi(q)}.$$

as x goes to infinity.

Strongest unconditional result which achieves uniformity in q.

Siegel-Walfisz Theorem

Theorem (Siegel-Walfisz)

Let $A > 0$ be a large real number. For any $q < (\ln x)^A$, we have

$$\pi(x; a, q) \sim \frac{\pi(x)}{\phi(q)}.$$

as x goes to infinity.

Strongest unconditional result which achieves uniformity in q.

However, note that for large x, $(ln(x))^A \ll x^{\frac{1}{2}}$.

Bombieri-Vinogradov Theorem

Question

Do we need to look at individual q? What about if we introduce some averaging in q? Can we obtain better results? Would this kind of result even be useful?

Bombieri-Vinogradov Theorem

Question

Do we need to look at individual q? What about if we introduce some averaging in q? Can we obtain better results? Would this kind of result even be useful?

Let $Error(x; a, q) := \left|\pi(x; a, q) - \frac{\pi(x)}{\phi(q)}\right|$. (Recall: $\pi(x; a, q) \sim \frac{\pi(x)}{\phi(q)}$).

Bombieri-Vinogradov Theorem

Question

Do we need to look at individual q? What about if we introduce some averaging in q? Can we obtain better results? Would this kind of result even be useful?

Let $Error(x; a, q) := \left|\pi(x; a, q) - \frac{\pi(x)}{\phi(q)}\right|$. (Recall: $\pi(x; a, q) \sim \frac{\pi(x)}{\phi(q)}$).

Let

$$E(x; q) = \max_{\substack{1 \leq a < q \\ a,q \text{ coprime}}} E(x; a, q)$$

Bombieri-Vinogradov Theorem

Question

Do we need to look at individual q? What about if we introduce some averaging in q? Can we obtain better results? Would this kind of result even be useful?

Let $Error(x; a, q) := \left|\pi(x; a, q) - \frac{\pi(x)}{\phi(q)}\right|$. (Recall: $\pi(x; a, q) \sim \frac{\pi(x)}{\phi(q)}$).

Let

$$E(x; q) = \max_{\substack{1 \leq a < q \\ a,q \text{ coprime}}} E(x; a, q)$$

Let $Q \geq 3$ be somewhat large compared with x. Consider

$$\frac{1}{Q} \sum_{q=1}^{Q} Error(x, q).$$

Bombieri-Vinogradov Theorem

The gist: $\frac{1}{Q}\sum_{q=1}^{Q} Error(x,q)$ is "small" enough to be dealt with in nearly all cases if Q is "somewhat" less than the square root of x.

Bombieri-Vinogradov Theorem

The gist: $\frac{1}{Q}\sum_{q=1}^{Q} Error(x,q)$ is "small" enough to be dealt with in nearly all cases if Q is "somewhat" less than the square root of x.
More specifically,

Theorem (Bombieri-Vinogradov)

For a small, fixed $\varepsilon > 0$ and any fixed $A > 0$, if $Q < x^{\frac{1}{2}-\varepsilon}$, there exists a constant $c(A)$ such that

$$\sum_{q \leq Q} E(x,q) < c(A)\frac{x}{(\ln(x))^A}.$$

The constant $c(A)$ is ineffective.

Primes in Polynomials

Question

We've looked at primes in degree 1 polynomials $qn + a$. What about higher degree polynomials like $n^2 + 1$ or multivariable polynomials like $a^2 + b^2$?

Primes in Polynomials

Question

We've looked at primes in degree 1 polynomials $qn + a$. What about higher degree polynomials like $n^2 + 1$ or multivariable polynomials like $a^2 + b^2$?

Conjecture (Landau)

There are infinitely many primes p of the form $n^2 + 1$.

Examples: $5 = 2^2 + 1,\ 17 = 4^2 + 1,\ 101 = 10^2 + 1$

Primes in Polynomials

Theorem (Fermat)

Every prime $p \equiv 1 \bmod 4$ can be written as the sum of two squares of integers i.e. $p = a^2 + b^2$. Furthermore, this representation is unique.

Examples: $101 = 1^2 + 10^2$ $113 = 7^2 + 8^2$

Question

If $p = a^2 + b^2$ *and* $a < b$*, how small can* a *be? For example* $101 = 1^2 + 10^2$*, versus* $113 = 7^2 + 8^2$.

Question

If $p = a^2 + b^2$ *and* $a < b$*, how small can* a *be? For example* $101 = 1^2 + 10^2$*, versus* $113 = 7^2 + 8^2$.

Let

$$\pi_\delta(x) = \#\{p \le x : p = a^2 + b^2 : a \le p^{\frac{1}{2}-\delta}\}$$

Question

If $p = a^2 + b^2$ and $a < b$, how small can a be? For example $101 = 1^2 + 10^2$, versus $113 = 7^2 + 8^2$.

Let

$$\pi_\delta(x) = \#\{p \leq x : p = a^2 + b^2 : a \leq p^{\frac{1}{2}-\delta}\}$$

Theorem (Kubilius)

There exists a $\delta_0 > 0$ such that for all $0 < \delta < \delta_0$, we have

$$\pi_\delta(x) \sim \frac{cx^{1-\delta}}{\ln x}$$

for some constant c.

The current world record for δ_0 is $\frac{12}{37}$.

What we did

What we did: combined these theorems (and generalized). A taste:

What we did

What we did: combined these theorems (and generalized). A taste: Let

$$\pi_\delta(x; r, q) = |\{p \le x : p = a^2 + b^2 : a < p^{\frac{1}{2} - \delta} : p \equiv r \bmod q\}|$$

What we did

What we did: combined these theorems (and generalized). A taste: Let

$$\pi_\delta(x; r, q) = |\{p \leq x : p = a^2 + b^2 : a < p^{\frac{1}{2}-\delta} : p \equiv r \bmod q\}|$$

Theorem (Khale, O, Panidapu, Sun, Zhang)

(Worded version) The prime counting function $\pi_\delta(x; r, q)$ obeys a Bombieri-Vinogradov type theorem as do variants generalized to polynomials in more variables which obey a particular set of algebraic conditions.

Proof Methods

Uses information about $\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \ldots$ for $s > 1$

Proof Methods

Uses information about $\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \ldots$ for $s > 1$

Euler Proved:

$$\zeta(s) = \left(\prod_{p \text{ prime}} \left(1 - \frac{1}{p^s} \right) \right)^{-1}$$

Can view $\zeta(s)$ as a function of complex variable s extended to the entire complex plane (Riemann).

Proof Methods

Zeroes of $\zeta(s) \implies$ Poles of $\frac{1}{\zeta(s)} \implies$ Important!

$$\xi(s) = \frac{1}{2}\pi^{-\frac{s}{2}} s(s-1)\Gamma\left(\frac{s}{2}\right)\zeta(s),$$

$$\xi(s) = \xi(1-s)$$

Proof Methods

Zeroes of $\zeta(s) \implies$ Poles of $\frac{1}{\zeta(s)} \implies$ Important!

$$\xi(s) = \frac{1}{2}\pi^{-\frac{s}{2}} s(s-1)\Gamma\left(\frac{s}{2}\right)\zeta(s),$$

$$\xi(s) = \xi(1-s)$$

Riemann Hypothesis

Theorem (Analytic fact)

All zeroes of ζ are either at the negative even integers or in the strip $0 \leq Re(s) \leq 1$

Theorem (Hadamard, de la Vallee Poussin, 1896)

$\zeta(s) \neq 0$ *if* $Re(s) = 1$. *Furthermore, PNT follows.*

Riemann Hypothesis

Theorem (Analytic fact)

All zeroes of ζ *are either at the negative even integers or in the strip* $0 \leq Re(s) \leq 1$

Theorem (Hadamard, de la Vallee Poussin, 1896)

$\zeta(s) \neq 0$ *if* $Re(s) = 1$. *Furthermore, PNT follows.*

Conjecture (Riemann)

For $0 < Re(s) < 1$, $\zeta(s) = 0$ *if and only if* $Re(s) = \frac{1}{2}$.
Furthermore,

$$|\pi(x) - Li(x)| \leq x^{\frac{1}{2}+\varepsilon}.$$

Counting Other Types of Prime Numbers

Example: primes in arithmetic progressions.

Let

$$\chi(n) := \begin{cases} +1 & n \equiv 1 \bmod 4 \\ -1 & n \equiv 3 \bmod 4 \\ 0 & n \equiv 0, 2 \bmod 4 \end{cases}$$

As a sequence, $\chi : 1, 0, -1, 0, 1, 0, -1, 0, 1, 0, -1, 0, \ldots$

Counting Other Types of Prime Numbers

Example: primes in arithmetic progressions.
Let

$$\chi(n) := \begin{cases} +1 & n \equiv 1 \bmod 4 \\ -1 & n \equiv 3 \bmod 4 \\ 0 & n \equiv 0, 2 \bmod 4 \end{cases}$$

As a sequence, $\chi : 1, 0, -1, 0, 1, 0, -1, 0, 1, 0, -1, 0, \ldots$
Properties

1. $\chi(nm) = \chi(n)\chi(m)$
2. χ is periodic with period 4.
3. If n is odd,

$$\frac{1 + \chi(n)}{2} := \begin{cases} 1 & n \equiv 1 \bmod 4 \\ 0 & n \equiv 3 \bmod 4 \end{cases}$$

Fourier Expansion

More generally, there exist functions $\chi_1, \ldots, \chi_{\phi(q)}$ (called Dirichlet characters modulo q) with period q such that $|\chi_j| = 1$ and the function

$$f_{a,q}(n) := \begin{cases} 1 & n \equiv a \bmod q \\ 0 & \text{otherwise} \end{cases}$$

can be written as

$$f_{a,q}(n) = \frac{1}{\phi(q)} \sum_{j=1}^{\phi(q)} \overline{\chi_j(a)} \chi_j(n)$$

Fourier Expansion

More generally, there exist functions $\chi_1, \ldots, \chi_{\phi(q)}$ (called Dirichlet characters modulo q) with period q such that $|\chi_j| = 1$ and the function

$$f_{a,q}(n) := \begin{cases} 1 & n \equiv a \bmod q \\ 0 & \text{otherwise} \end{cases}$$

can be written as

$$f_{a,q}(n) = \frac{1}{\phi(q)} \sum_{j=1}^{\phi(q)} \overline{\chi_j(a)} \chi_j(n)$$

It suffices to study

$$L(s, \chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

to count primes in arithmetic progressions.

L-functions

These L-functions admit analytic continuation similarly to the ζ-function.

Theorem

No L-functions have any zeroes s with $Re(s) = 1$. Furthermore, PNT for arithmetic progressions for fixed q follows.

L-functions

These L-functions admit analytic continuation similarly to the ζ-function.

Theorem

No L-functions have any zeroes s with $Re(s) = 1$. *Furthermore, PNT for arithmetic progressions for fixed q follows.*

Conjecture (GRH)

$L(s, \chi) = 0$ *in the strip* $0 \leq Re(s) \leq 1$ *if and only if* $Re(s) = \frac{1}{2}$.