Prime numbers and their distribution

Theorem: Suppose \( n \) is composite. Then \( n \) has a prime factor which is less than or equal to \( \sqrt{n} \).

Proof: Since \( n \) is composite, there are integers \( a, b > 1 \) such that

\[ n = a \cdot b \]

So one of \( a, b \) should be \( \leq \sqrt{n} \).

(Because if \( a > \sqrt{n} \Rightarrow a \cdot b > \sqrt{n} \cdot \sqrt{n} = n \) a contradiction)

Assume \( a \leq \sqrt{n} \)

Take any prime \( p \) dividing \( a \). This prime divides \( n \) and \( p \leq a \). This \( p \) does the job.
How to use this theorem to find the number of primes less than a given number $x$?

- Write down all the numbers from 1 to $x$.
- Look at primes less than $\sqrt{x}$.
  
  $2, 3, 5, 7, \ldots, \text{largest prime less than } \sqrt{x} = p_n$

- Cross out all numbers divisible by 2.
  
  $\ldots$ divisible by 3.

  
  divisible by $p_n$
Sieve of Eratosthenes

\[ x = 25 \]

\[ \sqrt{x} = 5 \]

2, 3, 5 are the primes \( \leq 5 \).
(1896) Hadamard, de la Vallee Poussin

(Prime Number Theorem)

\[ \pi(x) \sim \frac{x}{\log x} \]

What this precisely means is:

\[ \lim_{x \to \infty} \frac{\pi(x)}{\left( \frac{x}{\log x} \right)} = 1 \]

(Dirichlet's) Theorem on primes in arithmetic progressions.

Theorem: Let \( a, b \) be positive integers which are co-prime \( (\gcd(a,b) = 1) \). Then the arithmetic progression \( \{ an + b \mid n = 0, 1, 2, 3, \ldots \} \) contains an infinite number of primes.
What do we want to study about the primes?

The prime counting function \( \Pi(x) \) is defined by the following:

\[
\Pi(x) = \# \text{ of primes } \leq x
\]

\( \Pi(5) = 3 \)

\( \Pi(10) = 4 \)

'Roughly','

How does \( \Pi(x) \) look like?

(Gauss) He conjectured that

\[
\Pi(x) \sim \int_{2}^{x} \frac{1}{\log t} \, dt
\]

as \( x \to \infty \)
The Greatest Common Divisor of two integers.

Bezout's Theorem. Let $a$ and $b$ be integers.

Then there exist integers $m$ and $n$ such that

$$\gcd(a, b) = ma + nb$$

Examples

$a = 2, b = 3$

$\gcd(a, b) = 1$

$m = -1, n = 1$ works.

$m = 2, n = -1$ works too.
$a = 2, b = 1$

$3, 5, 7, 9, 11, \ldots$

$5, 9, 13, 17, 21, \ldots$

$3, 7, 11, 15, 19, \ldots$
Lemma: Let $a, b$ be non-zero integers. Then $\gcd(a, b)$ is the least positive integer which can be written as a linear combination $ma + nb$ for some integers $m, n$.

Proof: Let

$$S = \{ \text{All linear combinations } ma + nb \text{ such that } ma + nb > 0 \}.$$

$S$ is non-empty.

(S has $a = 1 - a + 0 - b > 0$)

By the well-ordering principle, $S$ has a least element $d$.

To show that $\gcd(a, b) = d$.

Strategy: $\gcd(a, b) \mid d$

and $d \mid \gcd(a, b)$
(i) \( \gcd(a, b) \mid d \).

Remember \( d \in \mathbb{S} \), so \( d = ma + nb \) for some \( m, n \in \mathbb{Z} \).

Suppose \( e = \gcd(a, b) \)

\[
e \mid a \quad \Rightarrow \quad e \mid ma + nb = d
\]

\[
e \mid d.
\]

(ii) \( d \mid \gcd(a, b) = e \). To prove this assertion, it is enough to prove that \( d \mid a \) and \( d \mid b \).

Enough to show that \( d \mid a \). \( \checkmark \) (by symmetry)

Division algorithm: \( a = qd + r \) for quotient \( q \) and the remainder \( 0 \leq r < d \).

To show that the remainders \( r = 0 \).
\[ r = a - qd \]

Remember again that \( d \in S \), so \( d = ma + nb \) for some \( m,n \in \mathbb{Z} \)

\[ r = a - q(ma + nb) \]

\[ = (1 - mq)a + (-qn)b \]

This is in \( S \), so \( r \in S \).

but \( 0 \leq r < d \)

\( d \) is the least element of \( S \), so \( r \) cannot be positive.

\[ q_2 = 0. \]