Divisibility

\[ a, b \text{ integers } a \mid b \iff \text{some integer } c \text{ satisfies } ac = b \]

Basic block: prime numbers \( p \neq 1 \)
\[ \text{divisible by } 1, p \text{ alone} \]

Fundamental Theorem of Arithmetic (later)

Any positive \( n = p_1 \cdot p_2 \cdots p_r \)
\( p_i \) prime, uniquely determined by \( n \)
(May be repeats) (change signs, or order)

\[ 12 = 2 \cdot 2 \cdot 3 \]
\[ 35 = 5 \cdot 7 = -7 \cdot (-5) \]

Old problem: find all primes!

\[ 2, 3, 5, 7, 11, 13, \ldots \]

No formula for the primes!
Famous problem "find" all primes

Riemann hypothesis: predicts formula

Thm (Euclid) There are $\infty$ many primes

pf: Consider the first $n$ primes

$P_1 = 2, P_2 = 3, \ldots, P_n$

Consider $(P_1 P_2 P_3 \cdots P_n) + 1 = N$

if $N$ is prime, then done, because $N > P_1 P_2 \cdots P_n$

$\Rightarrow$ means there are $n+1$ primes (at least)

if $N$ is not a prime, then it is divisible by some prime

why? (any number is div by some prime)

say by a prime $q$
But \( q \neq p_1, p_2, \ldots, p_n \) because
\( N \) has remainder 1 when I divide
by \( p_1, \ldots, p_n \)
So we have another prime \( q \) not on

\[
2 \cdot 3 \cdot 5 + 1 = 31, \text{ prime}
\]
\[
2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211 \text{ is \( \geq \) prime}
\]
but if not then any \( q | 211 \)
\[
2 \cdot 3 \cdot 5 \cdot 7 = 210 \text{ have rem } = 1
\]
when I divide into 211
Fact any integer $n = \text{product of primes}$

$\text{pf: }$ if $n$ is prime nothing to prove

if not then $n = a \cdot b$, $a, b < n$

by induction $a = \text{product of primes}$

$b = \text{product of primes}$

$n = a \cdot b = \text{product of primes}$

Fund thm $\implies$ only one way to do this

How to generate a list of primes??

Method: Sieve of Eratosthenes

key idea: if $n = a \cdot b$, $a, b < n$ (positive)

then at least one of $a, b < \sqrt{n}$
To find primes ≤ 100

Proceed as follows

If \( n \leq 100 \), \( n = ab \) \( \Rightarrow \) one of \( a, b \) \( \leq \sqrt{100} = 10 \)

So one of \( a, b \) is div by a prime ≤ 10

\( \Rightarrow \) have to have a factor of 2, 3, 5, 7

Make a list of numbers ≤ 100

Check out mults of 2, 3, 5, 7

Whatever is left is prime ≤ 100

Repeat: find all primes ≤ \((100)^2\)

Question: how to find big primes??

Possible, not hard

Also possible to test big numbers for primeness without trial division
How many primes are there?
Pick a number at random: what is the chance it is prime?
\[ \text{Ans (won't prove) about } \frac{x}{\ln x} \text{ numbers } \leq x \text{ are prime} \]

Prob of a random \# \leq x to be prime is \[ \frac{1}{\ln x} \]

(Prime number thm)
Section 3.3 Greatest common divisors

start with $a, b > 0$

Def $\text{gcd} (a, b) = (a, b)$

Greatest common divisor

= biggest integer dividing both

eg $(12, 18) = 6$

$(13, 17) = 1$

$\text{gcd} (24, 30) = 6$

Fact (important) it is possible to find $\text{gcd} (a, b)$ without factoring $a$ or $b$

Goal of 3.3, 3.4 develop a method (Euclidean algorithm) to find $\text{gcd} (a, b)$ which is efficient for large $a, b$ and does not require factoring
Thm (goal) let \(a, b\) denote positive integers. Then \(d = (a, b) = \gcd\) is the smallest positive number of the form \(d = ma + nb\) with \(m, n\) integers.

Not obvious at all that the value of \(d\) coming out of \(\text{thm}\) is the \(\gcd\).

Important special case:

- Suppose \(a, b\) have no common factor \(\iff\) \(\gcd = 1\) (relatively prime).
- Then \(\text{thm} \implies 1 = \gcd = ma + nb\) for some \(m, n\).