Lecture 1: Prime numbers

Natural Numbers

We use $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ to denote the set of natural numbers. These numbers naturally arise from counting objects in everyday life. Most of the numbers we encounter in daily life are not larger than 10^{100}.
In fact, according to estimates from Google, the total number of atoms in the observable universe is approximately 10^{80}. Thus, it is physically impossible to count objects beyond this number.

Despite these physical limitations, mathematicians seek to extend the idea of counting to arbitrarily large numbers, such as 10^{1000}, $10^{1000000}$, and beyond.

Prime Numbers

A **prime number** p is a positive integer greater than 1 that cannot be expressed as a nontrivial product $p = a \cdot b$, where both $a \neq 1$ and $b \neq 1$. In other words, a prime number has no divisors other than 1 and itself. For more information about prime numbers, check out this [link to a prime numbers article].

Lemma (Homework): To prove a number n is prime, it suffices if it is divisible by a number up to $\sqrt{n}$
.

On the other hand, a **composite number** is a positive integer greater than 1 that can be expressed as a nontrivial product, i.e., it has divisors other than 1 and itself.

Infinitely many prime numbers

Theorem (Euclid): There are infinitely many prime numbers.

Proof: Assume, for the sake of contradiction, that there are only finitely many prime numbers. Let these primes be

$$p_1, p_2, p_3, \dots, p_n.$$

Now, consider a new number N, which is the product of all these primes plus one:

$$N = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_n + 1.$$

Since N is larger than any of the primes $p_1, p_2, \dots, p_n$, it is not divisible by any of these primes. That is, for each prime p_i, we have:

$$N \div p_i \neq 0.$$

Now, two possibilities arise:

1. N **is prime**: If N is prime, then it is a prime number that is not in our original list of primes, contradicting the assumption that we had already listed all primes.
2. N **is composite**: If N is composite, then it must have a prime divisor. However, since N is not divisible by any of the primes in our list, N must have a prime divisor that is not in our list, again leading to a contradiction.

In both cases, we reach a contradiction. Therefore, our assumption that there are only finitely many prime numbers must be false.

Thus, there must be infinitely many prime numbers. QED.

Constructing the Prime Sequence Explicitly: The Sieve of Eratosthenes

The **Sieve of Eratosthenes** (Khan Academy example) is a classical algorithm used to generate all prime numbers up to a given limit. The idea behind is quite straighforward. Basically we remove all possible composite numbers and the rest is the set of prime numbers. The method works by systematically eliminating the multiples of each prime number starting from 2. The procedure can be described as follows:

1. **Step 1**: Write down all integers from 2 up to a given number n (e.g., 100). These numbers are the candidates for being prime.
2. **Step 2**: Start with the smallest number in the list, which is 2. Mark all of its multiples (except 2 itself) as non-prime (i.e., composite). The multiples of 2 are:

$$4, 6, 8, 10, 12, 14, 16, 18, \ldots$$

3. **Step 3**: Move to the next unmarked number, which is 3. Mark all of its multiples (except 3 itself) as non-prime. The multiples of 3 are:

$$6, 9, 12, 15, 18, 21, \ldots$$

4. **Step 4**: Move to the next unmarked number, 5. Mark all of its multiples (except 5 itself) as non-prime. The multiples of 5 are:

$$10, 15, 20, 25, 30, \ldots$$

5. **Step 5**: Repeat this process for the next unmarked numbers, namely 7, 11, and so on, marking their multiples as non-prime.

6. **Step 6**: Once you have processed numbers up to $\sqrt{n}$, the remaining unmarked numbers in the list are all prime.

Class activity: Find all prime numbers up to 100.

Remarks

Euclid's proof is by contradiction so cannot produce the prime numbers explictly. At the same time, Sieve of Eratosthenes cannot prove Euclid's theorem on infinitely many prime.

Homework 1: Is $N = p_1 p_2 ... p_n + 1$ always a prime?
Hint: Try to use ChatGPT to come up a python code to verify that and ask ChatGPT to explain.

Homework 2: Ask ChatGPT for a Python code to realize the sieve method.

Twin Prime Conjecture

The **Twin Prime Conjecture** (wiki link) is a famous unsolved hypothesis in number theory, proposed by the mathematician **Bernhard Riemann** in the 19th century. It asserts that there are infinitely many pairs of **twin primes** — prime numbers that differ by exactly 2. In other words, the conjecture suggests that there are infinitely many prime numbers p such that both p and $p+2$ are prime. Some of the first examples of twin primes are the pairs:

$$(3,5),(5,7),(11,13),(17,19),(29,31),(41,43),\ldots$$

Goldbach's Conjecture

The **Goldbach's Conjecture** (wiki link) is one of the oldest unsolved problems in number theory, first proposed by the German mathematician **Christian Goldbach** in 1742. The conjecture asserts that every even integer greater than 2 can be expressed as the sum of two prime numbers. In mathematical terms, it states that for every even integer $n \geq 4$, there exist prime numbers p_1 and p_2 such that:

$$n = p_1 + p_2$$

For example:

- $4 = 2 + 2$
- $6 = 3 + 3$
- $8 = 3 + 5$
- $10 = 3 + 7$
- $12 = 5 + 7$

Despite extensive computational evidence supporting the conjecture, no general proof has yet been found. The conjecture has been verified for very large numbers, with modern computers checking even numbers up to 4×10^{18}. Although the conjecture is widely believed to be true, it remains unproven, and a formal proof is still one of the major open questions in number theory. The conjecture is closely related to the distribution of prime numbers and is often considered one of the most important unsolved problems in mathematics.

Homework 3: Randomly pick 3 even numbers less than 100 and verify Goldbach's conjecture.

Reading assignment: p129-p140

Selected homework problems:

You are encouraged to solve all problems given the snow day...

p134, 4.500
p135, 4.010, 4.110, 4.410, 4.510
p136, 4.020, 4.320, 4.620, 4.820
p140, 4.040, 4.140, 4.440, 4.640