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:

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

Lecture 2: Prime Factorization and More on Factors

Fundamental theorem of arithmetics

Every positive integer n has a unique prime factorization.

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$$

Proof First we prove the existence. If n is a prime, then $n = n$. If n is a composite number, then $n = n_1 n_2$. We can continue the process on n_1 and n_2 until we get a prime fractorization.

Second, we prove the uniqueness. If there are two factorizations,

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} = q_1^{m_1} q_2^{m_2} \cdots q_l^{m_l}$$

Since p_1 is a factor of the right hand side, p_1 must equal to some q_i. Now dividing both sides on p_1 to get a smaller product. So it reduces to prove uniqueness for smaller n. Now we may repeat such argument to prove the uniquenss. QED.

Example

- $420 = 10 \cdot 42 = (2 \cdot 5) \cdot (2 \cdot 3 \cdot 7) = 2^2 \cdot 3 \cdot 5 \cdot 7$
- $729 = 9^3$
- $181 =?$ not trivial, so it may be a prime. suffices to divide prime numbers up to 13.

Perfect squares

Perfect squares are of the form n^2. Its prime factorization has all even powers.

Example

- $2^{10} \cdot 3^6 \cdot 7^{30} = (2^5)^2 (3^3)^2 (7^{15})^2$

It is useful to memorize them checking a number is prime of not. Below is the list of squares of numbers from 1 to 30, split into three columns:

1 to 10 Squares	11 to 20 Squares	21 to 30 Squares
$1^2 = 1$	$11^2 = 121$	$21^2 = 441$
$2^2 = 4$	$12^2 = 144$	$22^2 = 484$

1 to 10 Squares	11 to 20 Squares	21 to 30 Squares
$3^2 = 9$	$13^2 = 169$	$23^2 = 529$
$4^2 = 16$	$14^2 = 196$	$24^2 = 576$
$5^2 = 25$	$15^2 = 225$	$25^2 = 625$
$6^2 = 36$	$16^2 = 256$	$26^2 = 676$
$7^2 = 49$	$17^2 = 289$	$27^2 = 729$
$8^2 = 64$	$18^2 = 324$	$28^2 = 784$
$9^2 = 81$	$19^2 = 361$	$29^2 = 841$
$10^2 = 100$	$20^2 = 400$	$30^2 = 900$

Factor counting formula

If $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, then the number of factors are

$$(n_1 + 1)(n_2 + 1) \cdots (n_k + 1).$$

Example

- $n = p^a$ has $a + 1$ factors: $1 = p^0, p = p^1, p^2, ..., p^a$
- $n = p_1^a p_2^b$ has $(a + 1)(b + 1)$ factors.

Product of factors

Factors usually come in pairs, $n = a \cdot (n/a)$. For example,

- $42 = 1 * 42 = 2 * 21 = 3 * 14 = 7 * 6$
- $169 = 1 * 169 = 13^2$.

So the product of all factors of n is $n^{\frac{\#\text{factors}}{2}}$. The number of factors is even if and only if n is a perfect square.

Sum of factors

The factors of $20 = 2^2 \cdot 7$ are

- $1 = 2^0, 2 = 2^1, 4 = 2^2$
- $7 = 2^0 \cdot 7, 14 = 2^1 \cdot 7, 28 = 2^2 \cdot 7$

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

Lecture 3: Greatest Common Divisors and Least Common Multiples

Greatest Common Divisor

Given two positive integers a and b, the **greatest common divisor (factor)** is the largest factor that divides both a and b. We use $\gcd(a, b)$ to denote the greatest common divisor (GCD).

Example

- If a divides b, then $\gcd(a, b) = a$.
  - $\gcd(3, 6) = 3$
  - $\gcd(12, 2) = 2$
- If p is a prime, then $\gcd(p, a) = 1$ or p.
  - $\gcd(5, 16) = 1$
  - $\gcd(5, 100) = 5$
- $\gcd(a, b)$ is always less than a and b.
  - $\gcd(15, 24) = 3$
  - $\gcd(91, 52) = 13$

GCD from the prime factorization

Example

- Since $91 = 7 * 13$ and $52 = 2^2 * 13$, then GCD can be read directly from the common prime factors, in this case, it is 13.
- In general, once you know the prime factorization, just pick the common prime factors and the smaller exponent.
  - $$\gcd(2^2 * 3^3 * 5, 2^3 * 3^2 * 7) = 2^2 * 3^2 = 36$$
  - $$\gcd(2^{100} * 3^{40} * 13^2, 3^7 * 5^5 * 13) = 3^7 * 13$$
- If you already observe a common factor c, then

$$\gcd(a, b) = c \cdot \gcd(\frac{a}{b}, \frac{b}{c})$$

  - $\gcd(112, 80) = 4 * \gcd(28, 20) = 16$
  - $\gcd(126, 162) = 6 * \gcd(21, 27) = 18$

Warning: This is a really inefficient algorithm. In general, prime factorization is costly even for computers when the number is very large.

Homework Ask ChatGPT for a prime factorization algorithm and ask it to time the algorithm. Try a relatively large number about 10 digits for example.

Euclidean algorithm (300 BC)

The most efficient algorithm (Wiki link) to calculate $\gcd(a, b)$:

- Step 1: Assume a is the smaller number. Calculate b divided by a with the remaider r:

$$b = k \cdot a + r$$

- Step 2: If $r = 0$, then $\gcd(a, b) = a$. If $r \neq 0$, then $\gcd(a, b) = \gcd(a, r)$. Now repeat Step 1 on $\gcd(a, r)$.

Example

- $\gcd(80, 112) = \gcd(80, 32) = \gcd(16, 32) = 16$
- $\gcd(105, 252) = \gcd(105, 42) = \gcd(21, 42) = 21$
- $\gcd(162, 126) = \gcd(36, 126) = \gcd(36, 18) = 18$
- $\gcd(80, 112 + 80 * 123456789) = \gcd(80, 112) = 16$
- $\gcd(1800000001, 30) = 1$
- $\gcd(a, a + 1) = 1$

We can define $\gcd(a, b, c)$.
Example Find a, b, c such that $\gcd(a, b, c) = 1$ but GCD of any two are not 1.
Solution: $\gcd(2 * 3, 3 * 5, 5 * 2) = 1$

Least common multiple

Given two positive integers a and b, the **least common multiple** is the smallest number that both a and b divides. We use $\text{lcm}(a, b)$ to denote LCM. We always have

$$\text{lcm}(a, b) \leq ab$$

Example

- $\text{lcm}(4, 6) = 12$
- $\text{lcm}(12, 16) = 48$
- If $\gcd(a, b) = 1$, in other words, no common factors, then $\text{lcm}(a, b) = ab$.
  - $\text{lcm}(4, 13) = 52$

Their sum equals $(1+2+4)(1+7)=56$. This generalizes to all cases. If $n=p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$, then the sum of factors are

$$(1+p_1+p_1^2+\cdots+p_1^{n_1})\cdots(1+p_k+p_k^2+\cdots+p_k^{n_k})$$

If the sum of factors equals the number itself, we call it a **perfect number**. The first two are 6 and 28.

Homework Use ChatGPT to understand the relation between perfect numbers and Mersenne primes.

Class activity

Any prime number is either 2 or an odd prime number.
Theorem Any odd prime number of the form $4k+1$ is a sum of two squares.

- very difficult, need college math

Theorem Any odd prime number of the form $4k+3$ is not a sum of two squares.

- relatively easy, proved in later lectures

Prime table up to 300:

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	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				

    - $\text{lcm}(a, a+1) = a(a+1)$
- If c divides both a and b, then

$$\text{lcm}(a, b) = c \cdot \text{lcm}(a/c, b/c)$$

LCM formula

LCM via prime factorization is quite easy.Take all prime factors and the higher exponents.

Example

- $\text{lcm}(2^2, 2 * 3) = 2^2 * 3 = 12$
- $\text{lcm}(2^2 * 3^3 * 5, 2 * 3 * 7) = 2^2 * 3^3 * 5 * 7$

We can use the following formula to calculate LCM in general.

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

Number Proof
If $a = 2^3 \cdot 3^5 \cdot 7 \cdot 17$ and $b = 2^2 \cdot 3^7 \cdot 7^2 \cdot 19$, then

$$\text{gcd}(a, b) = 2^2 \cdot 3^5 \cdot 7$$

$$\text{lcm}(a, b) = 2^3 \cdot 3^7 \cdot 7^2 \cdot 17 \cdot 19$$

You can verify this directly.

Proof We can pull out GCD as below.

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

Note that $\frac{a}{\text{gcd}(a,b)}, \frac{b}{\text{gcd}(a,b)}$ have no common GCD. Thus

$$\text{lcm}(\frac{a}{\text{gcd}(a, b)}, \frac{b}{\text{gcd}(a, b)}) = \frac{a}{\text{gcd}(a, b)} \cdot \frac{b}{\text{gcd}(a, b)}$$

Plug this into the first equation. We are done.

Lecture 4: Decimal vs Binary, and more

A math joke

We have "Thanksgiving = Christmas" because $\text{Dec } 25 = \text{Oct } 31$.

Decimal or Base-Ten system

Base-Ten system (decimal numeral system) is mostly used because we have ten fingers. All numbers are expressed by $0, 1, \cdots, 9$. The base-ten expression has the following expression.

Example

$$\begin{aligned} 12345 &= 10000 + 2000 + 300 + 40 + 5 \\ &= 1 * 10^4 + 2 * 10^3 + 3 * 10^3 + 4 * 10^1 + 5 * 10^0 \\ &= 12345_{10} \\ &= \text{Dec } (12345) \end{aligned}$$

Base-Two (Binary) system

That is the computer numbering system because computer has know 2 digits 0 and 1... You can only use 0 and 1 to label a number $0, 1, 10, 11, 100, 101, 110, 111, 1000....$

- $10_2 = 1 * 2^1 + 0 * 2^0 = 2_{10}$
- $111_2 = 1 * 2^2 + 1 * 2^1 + 1 * 2^0 = 7_{10}$
- $10111 = 1 * 2^4 + 111 = 23_{10}$

Base-Three (Ternery) system

You can only use $0, 1, 2$ to label a number $0, 1, 2, 10, 11, 12, 20, 21, 22, 100, 101, 102, 110, ...$

- $122_3 = 1 * 3^2 + 2 * 3^1 + 2 = 17$
- $122_3 = 200_3 - 1_3 = 18 - 1 = 17$

Base-Eight (Octal) system

You can only use $0, ..., 7$ to label a number $0, 1, 2, 3, 4, 5, 6, 7, 10, ...$

- $\text{Oct } 31 = 31_8 = 3 * 8^1 + 1 = 25_{10} = \text{Dec } 31$ (the joke)

Base-Sixteen (Hexadecimal) system

You can only use $0, ..., 9, A, B, C, D, E, F$ to label a number $0, 1, 2, 3, 4, 5, 6, 7, 10, A, B, C, D, E, F, 10, 11, ...$

- $BB = 11 * 16 + 11 = 187_{10}$

Base-n system

With the proper labels, you can design any base-n system. $n < 10$ is easy because we can borrow the ten digits. For n is large, you need to design your own "digit" such as $A, B, C, ...$

Convert a decimal to other base

Use long division.

- Convert 25_{10} to octal
  - $25 = 3 * 8 + 1$
  - So $25_{10} = 31_8$. The joke again.
- Convert 78_{10} to binary
  - **repetitively divides 2 until you cannot. Collect the last divisor and other remaiders in the reserve way**.
    - 78=2*39+0
    - 39=2*19+1
    - 19=2*9+1
    - 9=2*4+1
    - 4=2*2+0
    - 2=2*1+0
  - $78_{10} = 1001110_2 = 2^6 + 2^3 + 2^2 + 2^1 = 64 + 8 + 4 + 2 = 78$
- Convert 78_{10} to base 3.
  - $78 = 3 * 26 + 0$
  - $26 = 3 * 8 + 2$
  - $8 = 3 * 2 + 2$
  - So $78_{10} = 2220_3$

Addition and substraction

Use long addition and substraction!!

- $111_2 + 11_2 = 1010_2$
- the above is the same as $7 + 3 = 10$.
- $10010_2 - 1101_2 = 101_2$

- the above is the same as $18 - 13 = 5$.

Long addition/substraction really works for any base! But need to be careful on add/minus one.

- for octals, $7_8 + 4_8 = 13_8$
- for binary, only need to remember $1_2 + 1_2 = 10_2$ and $10_2 - 1_2 = 1_2$

Multiplication and division

Use long multiplication and long division!!

$9 * 9$ multiplication table for binary

- $0 * 0 = 0$
- $0 * 1 = 1 * 0 = 0$
- $1 * 1 = 1$

Computer likes this because it is really easy!! No need to memorize $9 * 9$ multiplication table. We can do that too but it is too late.... We get so used to decimal system.

Homework Create a base-5 $5 * 5$ multiplication table.

Example

work below out use long multiplication/division

- $111_2 * 11_2 = 7 * 3 = 21$
- $1001110_2 / 110_2 = 78/6 = 13 = 1101_2$

Bonus

- We know $1/3 = 0.33333.....$ What is the division in base three?

$$1_3/10_3 = 0.1_3 = 0.33333....$$

  This extends to all fractions or rational numbers.
- We know $1/2 = 0.5$. What is the division in base two?

$$1/2 = 1_2/10_2 = 0.1$$

- But in base 3

$$1/2 = 0.11111....._3 = \frac{1}{3} + \frac{1}{3^2} + \frac{1}{3^3} + ...$$

- In fact, for any base n,

$$\frac{1}{n-1} = 0.11111.....{}_n = \frac{1}{n} + \frac{1}{n^2} + \frac{1}{n^3} + ...$$

- We know in base $3_{10} = 10_3$. But 10_3 is not a prime!! Because 2 can not divide 10_3. Thus a prime number is a prime number for any base.

Lecture 5:

Unit Digit

What is the last digit of

- $456 * 789 \to 2$
- $307 * 188 \to 6$
- the last digit of a perfect square can only be $0, 1, 4, 9, 6, 5$.
- 3^{2025}
  - $3^1 = 3, 3^2 = 9, 3^3 = 27, 3^4 = 81$, always repeats as $3, 9, 7, 1, 3, ...$
  - $2025 = 4 * k + 1$, so the last digit is 3.
- 2^k: $2 \to 4 \to 8 \to 6 \to 2 \to ....$
- 4^k: $4 \to 6 \to 4 \to 6 \to ...$
- $5^k, 6^k$: always 5 or 6
- 7^k: $7 \to 9 \to 3 \to 1 \to 7 \to ...$
- 8^k: $8 \to 4 \to 2 \to 6 \to 8 \to ...$
- 9^k: $9 \to 1 \to 9 \to ...$
- the power unit digit repeats itself by a period of $1, 2, 4$.

Lemma a^4 and a have the same unit digit for any number a.

Remainder

The unit digit of a number is the remainder of that number divided by 10. The remainder divided by n is actually the unit digit in base n.

Example

What is the remainder of 2^{2025} divided by 3?

- Find a pattern
  - $2^1 = 2$
  - $2^2 \to_3 1$
  - $2^3 \to_3 1 * 2 \to_3 2$
- order 2!!

Example

What is the remainder of 4^{2025} divided by 5?

- Find a pattern
  - $4^1 = 4$
  - $4^2 \to_5 1$
  - $4^3 \to_5 1 * 4 \to_3 4$
- order 2!!
- Try 2^k divided by 5, $2 \to 4 \to 3 \to 1$,order 4.
- Try 3^k, $3 \to 4 \to 2 \to 1$, order 4.

Example

What is the remainder of 3^{2025} divided by 7?

- Find a pattern
  - $3^1 = 3$
  - $3^2 = 9 \to_7 2$
  - $3^3 = 27 \to_7 6$, note that $2 * 3 = 6$ as well
  - $3^4 \to_7 6 * 3 \to_7 4$
  - $3^5 \to_7 4 * 3 \to_7 5$
  - $3^6 \to_7 5 * 3 \to_7 1$
- order 6!!
- 2^k divided by 7, $2 \to 4 \to 1$, order 3
- 4^k divided by 7, $4 \to 2 \to 1$, order 3
- 5^k divided by 7, $5 \to 4 \to 6 \to 2 \to 3 \to 1$, order 6
- 6^k divided by 7, $6 \to 1 \to 6$, order 2

Fermart's Little Theorem When p is a prime, the repeating order divides $p - 1$.

This is not true for composite number. 3^k divided by 4, $3 \to 1$, order 2, not divides $4 - 1 = 3$.

Homework Ask ChatGPT to write a python code to verify Fermat's little theorem for primes up to 100. For each p, what is the number with repeating order exactly $p - 1$? Any pattern?

Fractions

divided by $9, 99, 999, ...$

Example

- $\frac{4}{9} = 0.\overline{4}$
- $\frac{41}{99} = 0.\overline{41}$
- $\frac{181}{999} = 0.\overline{181}$

- $\frac{31}{111} = \frac{279}{999} = 0.\overline{279}$

Terminating

A fraction is terminating in decimal expansion if the denominator contains prime factors only 2 and 5. Remember the formula $10^k = 2^k 5^k$.

Example

- $\frac{1}{25} = \frac{4}{100} = 0.04$
- $\frac{1}{8} = \frac{125}{1000} = 0.125$
- $\frac{3}{625} = \frac{3*2^4}{10000} = 0.0048$

Decimals to Fractions

Introduce x.

Example

- $x = 0.1\overline{3}$
  - $10x = 1.\overline{3} = \frac{4}{3}$
  - $x = \frac{4}{30}$
- $x = 0.\overline{37}$
  - $100x = 37 + x$
  - $x = \frac{37}{99}$
- $x = 0.\overline{142857}$
  - $1000000x = 142857 + x$
  - $x = \frac{142857}{999999} = \frac{1}{7}$

A magic number

A decimal that contains all natural numbers, thus every number anywhere, social security number, credit card number, your home address number, etc. Remember that number lies between 0.12 and 0.13, which encodes all numbers...

$$a = 0.12345678910111213...$$