Lecture #12: Primes, GCDs, and Representations
Primes & Greatest Common Divisors

- Prime representations
- Important theorems about primality
- Greatest Common Divisors
- Least Common Multiples
- Euclid’s algorithm
Once and for all, what are prime numbers?

**Definition:** A prime number is a positive integer \( p \) greater than 1 that is divisible by only 1 and itself. If a number is not prime, it is called a composite number.

**Mathematically:** \( p \) is prime \( \iff p > 1 \land \forall \, x \in \mathbb{Z}^+ \left[ (x \neq 1 \land x \neq p) \rightarrow x \nmid p \right] \)

**Examples:** Are the following numbers prime or composite?

- 23
- 42
- 17
- 3
- 9
Any positive integer can be represented as a unique product of prime numbers!

**Theorem (The Fundamental Theorem of Arithmetic):** Every positive integer greater than 1 can be written uniquely as a prime or the product of two or more primes where the prime factors are written in order of non-decreasing size.

**Examples:**
- $100 = 2 \times 2 \times 5 \times 5 = 2^2 \times 5^2$
- $641 = 641$
- $999 = 3 \times 3 \times 3 \times 37 = 3^3 \times 37$
- $1024 = 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 = 2^{10}$

**Note:** Proving the fundamental theorem of arithmetic requires some mathematical tools that we have not yet learned.
Theorem: If $n$ is a composite integer, then $n$ has a prime divisor less than or equal to $\sqrt{n}$.

Proof:

- If $n$ is composite, then it has a positive integer factor $a$ with $1 < a < n$ by definition. This means that $n = ab$, where $b$ is an integer greater than 1.
- Assume $a > \sqrt{n}$ and $b > \sqrt{n}$. Then $ab > \sqrt{n}\sqrt{n} = n$, which is a contradiction. So either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.
- Thus, $n$ has a divisor less than or equal to $\sqrt{n}$.
- By the fundamental theorem of arithmetic, this divisor is either prime, or is a product of primes. In either case, $n$ has a prime divisor less than or equal to $\sqrt{n}$.

\[\square\]
Applying contraposition leads to a naive primality test

**Corollary:** If \( n \) is a positive integer that does not have a prime divisor less than or equal to \( \sqrt{n} \), then \( n \) is prime.

**Example:** Is 101 prime?
- The primes less than or equal to \( \sqrt{101} \) are 2, 3, 5, and 7
- Since 101 is not divisible by 2, 3, 5, or 7, it must be prime

**Example:** Is 1147 prime?
- The primes less than or equal to \( \sqrt{1147} \) are 2, 3, 5, 7, 11, 13, 17, 23, 29, and 31
- \( 1147 = 31 \times 37 \), so 1147 must be composite
This approach can be generalized

The Sieve of Eratosthenes is a brute-force algorithm for finding all prime numbers less than some value $n$

**Step 1:** List the numbers less than $n$

<p>| | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>3</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>7</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td>13</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>17</td>
<td>X</td>
<td>19</td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td>23</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>29</td>
<td>X</td>
<td>31</td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>37</td>
<td>X</td>
<td>X</td>
<td>41</td>
</tr>
<tr>
<td>X</td>
<td>43</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>47</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td>53</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>59</td>
<td>X</td>
<td>61</td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>67</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

**Step 2:** If the next available number is less than $\sqrt{n}$, cross out all of its multiples

**Step 3:** Repeat until the next available number is $> \sqrt{n}$

**Step 4:** All remaining numbers are prime
**Theorem:** There are infinitely many prime numbers.

**Proof:** By contradiction

- Assume that there are only a finite number of primes $p_1, \ldots, p_n$.
- Let $Q = p_1 \times p_2 \times \ldots \times p_n + 1$.
- By the fundamental theorem of arithmetic, $Q$ can be written as the product of two or more primes.
- Note that no $p_j$ divides $Q$, for if $p_j \mid Q$, then $p_j$ also divides $Q - p_1 \times p_2 \times \ldots \times p_n = 1$.
- Therefore, there must be some prime number not in our list. This prime number is either $Q$ (if $Q$ is prime) or a prime factor of $Q$ (if $Q$ is composite).
- This is a contradiction since we assumed that all primes were listed. Therefore, there are infinitely many primes.  

*This is a non-constructive existence proof!*
In-class exercises

Problem 1: What is the prime factorization of 984?

Problem 2: Is 157 prime? Is 97 prime?

Problem 3: Is the set of all prime numbers countable or uncountable? If it is countable, show a 1-to-1 correspondence between the prime numbers and the natural numbers.
Greatest common divisors

**Definition:** Let $a$ and $b$ be integers, not both zero. The largest integer $d$ such that $d \mid a$ and $d \mid b$ is called the **greatest common divisor** of $a$ and $b$, denoted by $\text{gcd}(a, b)$.

**Note:** We can (naively) find GCDs by comparing the common divisors of two numbers.

**Example:** What is the GCD of 24 and 36?

- Factors of 24: $1, 2, 3, 4, 6, 8, 12, 24$
- Factors of 36: $1, 2, 3, 4, 6, 9, 12, 18, 36$
- $\therefore \text{gcd}(24, 36) = 12$
Sometimes, the GCD of two numbers is 1

Example: What is gcd(17, 22)?

- Factors of 17: 1, 17
- Factors of 22: 1, 2, 11, 22
- ∴ gcd(17, 22) = 1

Definition: If gcd(a, b) = 1, we say that a and b are relatively prime, or coprime. We say that a₁, a₂, …, aₙ are pairwise relatively prime if gcd(aᵢ, aⱼ) = 1 ∀i, j.

Example: Are 10, 17, and 21 pairwise coprime?

- Factors of 10: 1, 2, 5, 10
- Factors of 17: 1, 17
- Factors of 21: 1, 3, 7, 21
We can leverage the fundamental theorem of arithmetic to develop a better algorithm.

Let: \( a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \) and \( b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n} \)

Then:

\[
\text{gcd}(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}
\]

**Example:** Compute \( \text{gcd}(120, 500) \)

- \( 120 = 2^3 \times 3 \times 5 \)
- \( 500 = 2^2 \times 5^3 \)
- So \( \text{gcd}(120, 500) = 2^2 \times 3^0 \times 5 = 20 \)
Better still is Euclid’s algorithm

**Observation:** If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$

Proved in section 4.3 of the book

So, let $r_0 = a$ and $r_1 = b$. Then:

- $r_0 = r_1q_1 + r_2 \quad 0 \leq r_2 < r_1$
- $r_1 = r_2q_2 + r_3 \quad 0 \leq r_3 < r_2$
- ...
- $r_{n-2} = r_{n-1}q_{n-1} + r_n \quad 0 \leq r_n < r_{n-1}$
- $r_{n-1} = r_nq_n$

$\gcd(a, b) = r_n$
Examples of Euclid’s algorithm

*Example:* Compute gcd(414, 662)
- $662 = 414 \times 1 + 248$
- $414 = 248 \times 1 + 166$
- $248 = 166 \times 1 + 82$
- $166 = 82 \times 2 + 2$  \[\text{gcd}(414, 662) = 2\]
- $82 = 2 \times 41$

*Example:* Compute gcd(9888, 6060)
- $9888 = 6060 \times 1 + 3828$
- $6060 = 3828 \times 1 + 2232$
- $3828 = 2232 \times 1 + 1596$
- $2232 = 1596 \times 1 + 636$
- $1596 = 636 \times 2 + 324$
- $636 = 324 \times 1 + 312$
- $324 = 312 \times 1 + 12$  \[\text{gcd}(9888, 6060) = 12\]
- $312 = 12 \times 26$
**Definition:** The least common multiple of the integers $a$ and $b$, where neither is 0, is the smallest positive integer that is divisible by both $a$ and $b$. The least common multiple of $a$ and $b$ is denoted lcm($a, b$).

**Example:** What is lcm(3,12)?
- Multiples of 3: 3, 6, 9, 12, 15, ...
- Multiples of 12: 12, 24, 36, ...
- So lcm(3,12) = 12

**Note:** lcm($a, b$) is guaranteed to exist, since a common multiple exists (i.e., $ab$).
We can leverage the fundamental theorem of arithmetic to develop a better algorithm.

Let: \( a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \) and \( b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n} \)

Then:

\[
lcm(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}
\]

\[
\text{Greatest multiple of } p_1 \text{ in either } a \text{ or } b
\]

\[
\text{Greatest multiple of } p_2 \text{ in either } a \text{ or } b
\]

**Example:** Compute lcm(120, 500)

- \( 120 = 2^3 \times 3 \times 5 \)
- \( 500 = 2^2 \times 5^3 \)
- So lcm(120, 500) = \( 2^3 \times 3 \times 5^3 = 3000 \) << 120 \times 500 = 60,000
LCMs are closely tied to GCDs

Note: $ab = \text{lcm}(a, b) \times \text{gcd}(a, b)$

**Example:** $a = 120 = 2^3 \times 3 \times 5$, $b = 500 = 2^2 \times 5^3$

- $120 = 2^3 \times 3 \times 5$
- $500 = 2^2 \times 5^3$
- $\text{lcm}(120, 500) = 2^3 \times 3 \times 5^3 = 3000$
- $\text{gcd}(120, 500) = 2^2 \times 3^0 \times 5 = 20$
- $\text{lcm}(120, 500) \times \text{gcd}(120, 500)$
In-class exercises

Problem 4: Use Euclid’s algorithm to compute $\gcd(92928, 123552)$.

Problem 5: Compute $\gcd(24, 36)$ and $\operatorname{lcm}(24, 36)$. Verify that $\gcd(24, 36) \times \operatorname{lcm}(24, 36) = 24 \times 36$.

(Submit both on Top Hat after a few minutes to work)
Final Thoughts

- Prime numbers play an important role in number theory.
- There are an infinite number of prime numbers.
- Any number can be represented as a product of prime numbers; this has implications when computing GCDs and LCMs.
- Next time: Proof by Induction.