Definition: A positive integer \( p \) greater than 1 is called prime if the only positive factors of \( p \) are 1 and \( p \). A positive integer that is greater than 1 and is not prime is called composite.

Example: The integer 11 is prime because its only positive factors are 1 and 11, but 12 is composite because it is divisible by 3, 4, and 6.

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

Examples:

a. \( 50 = 2 \cdot 5^2 \)
b. \( 121 = 11^2 \)
c. \( 256 = 2^8 \)

Theorem: If \( n \) is a composite integer, then \( n \) has a prime divisor less than or equal to \( \sqrt{n} \).

Proof:
Example: Show that 97 is prime.

Example: Find the prime factorization of each of these integers
   a.  143
   b.  81

Theorem: There are infinitely many primes.

Proof:
Questions:

1. The proof of the previous theorem by
   A. Contrapositive
   B. Contradiction
   C. Direct

2. Is the proof constructive OR nonconstructive?

3. Have we shown that Q is prime?

The Sieve of Eratosthenes can be used to find all primes not exceeding a specified positive integer. For example, begin with the list of integers between 1 and 100.

a. Delete all the integers, other than 2, divisible by 2.
b. Delete all the integers, other than 3, divisible by 3.
c. Next, delete all the integers, other than 5, divisible by 5.
d. Next, delete all the integers, other than 7, divisible by 7.
e. Since all the remaining integers are not divisible by any of the previous integers, other than 1, the primes are:
   \{2,3,5,7,11,15,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97\}
Mersenne primes (French monk Marin Mersenne): \(2^p - 1\)

\[
\begin{align*}
2^2 - 1 &= 3 \\
2^3 - 1 &= 7 \\
2^5 - 1 &= 31 \text{ etc.} \\
2^{11} - 1 &= 2047 = 23 \cdot 89 \\
2^{42,643,801} - 1
\end{align*}
\]

Conjectures and open problems about primes.

Example: \(f(n) = n^2 - n + 41\)

\[
\begin{align*}
f(1) &= 41, \\
f(2) &= 43, \\
f(3) &= 47, \\
f(4) &= 53
\end{align*}
\]

Is \(f(n)\) prime for all positive integers \(n\)?

For every polynomial with integer coefficients, there is a positive integer \(y\) such that \(f(y)\) is composite.

Goldbach’s Conjecture: Every even integer \(n, n > 2\), is the sum of two primes.

\[
\begin{align*}
4 &= 2 + 2 \\
6 &= 3 + 3 \\
8 &= 3 + 5 \\
10 &= 3 + 7 \\
12 &= 5 + 7
\end{align*}
\]

The conjecture has been checked for all positive even integers up to \(1.6 \cdot 10^{18}\), BUT there is NO proof.

The Twin Prime Conjecture: There are infinitely many twin primes.

Twin primes are a pair of primes that differ by 2:

\[
\begin{align*}
3 &\text{ & } 5, & 11 &\text{ & } 13, \\
5 &\text{ & } 7, & 17 &\text{ & } 19, \\
& & 4967 &\text{ & } 4969
\end{align*}
\]
Greatest Common Divisors and Least Common Multiples

**Definition:** Let \( a \) and \( b \) be integers, not both zero. The largest integer \( d \) such that \( d | a \) and \( d | b \) is called the *greatest common divisor* of \( a \) and \( b \).

**Notation:** \( \gcd(a, b) \)

One way to find the greatest common divisor is to find all positive common divisors of both integers and then take the largest divisor.

**Example:** What is the greatest common divisor of 12 and 24?

**Example:** What is the greatest common divisor of 11 and 25?

**Definition:** The integers \( a \) and \( b \) are *relatively prime* if their greatest common divisor is 1.

**Definition:** The integers \( a_1, a_2, \ldots, a_n \) are pairwise relatively prime if \( \gcd(a_i, a_j) = 1 \), whenever \( 1 \leq i < j \leq n \).

**Example:** Determine whether the integers in each of these sets are pairwise relatively prime.

a. 21, 34, and 55 

b. 14, 17, 85
Another way to find the greatest common divisor of two integers is to use their prime factorization.

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

Then \( \gcd(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdot \ldots \cdot p_n^{\min(a_n, b_n)} \)

**Example:** Find the greatest common divisor of 30030 and 2244.

Prime factorization can also be used to find the least common multiple of two numbers.

**Definition:** The least common multiple of the positive integers \( a \) and \( b \) is the smallest positive integer that is divisible by both \( a \) and \( b \).

**Notation:** \( \text{lcm}(a, b) \)

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

Then \( \text{lcm}(a, b) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdot \ldots \cdot p_n^{\max(a_n, b_n)} \)

**Example:** Find the least common multiple of \( 2^2 \cdot 3^3 \cdot 5^5 \) and \( 2^5 \cdot 3^3 \cdot 5^2 \)
Theorem: Let \( a \) and \( b \) be positive integers. Then \( ab = \gcd(a, b) \cdot \text{lcm}(a, b) \)

Finding the \( \gcd \) of two positive integers using their prime factorizations is not efficient because there is no efficient algorithm for finding the prime factorization of a positive integer.

Euclidean Algorithm

Example: Find the greatest common divisor of 91 and 287.

Lemma: Let \( a = bq + r \), where \( a, b, q, \) and \( r \) are integers. Then \( \gcd(a, b) = \gcd(b, r) \).

The algorithm can be written as a sequence of equations. Let \( r_0 = a \) and \( r_1 = b \).

\[
\begin{align*}
    r_0 &= r_1q_1 + r_2 \quad 0 \leq r_2 \leq r_1 \\
    r_1 &= r_2q_2 + r_3 \quad 0 \leq r_3 \leq r_2 \\
    &\quad \vdots \\
    r_{n-2} &= r_{n-1}q_{n-1} + r_n \quad 0 \leq r_n \leq r_{n-1} \\
    r_{n-1} &= r_nq_n
\end{align*}
\]

- If \( a \) is smaller than \( b \), the first step of the algorithm swaps the numbers.
- The remainders decrease with every step but can never be negative. A remainder \( r_n \) must eventually equal zero. Then the algorithm stops.

\[ \gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) \]
Example: Find the greatest common divisor of 123 and 277.

**gcd as a Linear Combinations**

**Bezout’s Theorem:** If \(a\) and \(b\) are positive integers, then there exists integers \(s\) and \(t\) such that \(\gcd(a, b) = sa + tb\).

Example: Express \(\gcd(252, 198) = 18\) as a linear combination of 252 and 198.
Example: Express $gcd(35, 78)$ as a linear combination of 35 and 78.