CS 3333: Mathematical Foundations

Primes, GCD, and LCM

Primes, GCD, and LCM

- **Prime Numbers**: Let p be a positive integer greater than 1. p is a prime number if the only positive factors of p are 1 and p.

Primes, GCD, and LCM

- **Prime Numbers**: Let p be a positive integer greater than 1. p is a prime number if the only positive factors of p are 1 and p.
- If p has a positive factor other than 1 and p, then p is a composite number.

Primes, GCD, and LCM

- **Prime Numbers**: Let p be a positive integer greater than 1. p is a prime number if the only positive factors of p are 1 and p.
- If p has a positive factor other than 1 and p, then p is a composite number.
- Examples:
  - $p = 5$

Primes, GCD, and LCM

- **Prime Numbers**: Let p be a positive integer greater than 1. p is a prime number if the only positive factors of p are 1 and p.
- If p has a positive factor other than 1 and p, then p is a composite number.
- Examples:
  - $p = 5$; factors: 1, 5

Primes, GCD, and LCM

- **Prime Numbers**: Let p be a positive integer greater than 1. p is a prime number if the only positive factors of p are 1 and p.
- If p has a positive factor other than 1 and p, then p is a composite number.
- Examples:
  - $p = 5$; factors: 1, 5; it is prime

Primes, GCD, and LCM

- **Prime Numbers**: Let p be a positive integer greater than 1. p is a prime number if the only positive factors of p are 1 and p.
- If p has a positive factor other than 1 and p, then p is a composite number.
- Examples:
  - $p = 5$; factors: 1, 5; it is prime
  - $p = 6$

Primes, GCD, and LCM

- **Prime Numbers**: Let p be a positive integer greater than 1. p is a prime number if the only positive factors of p are 1 and p.
- If p has a positive factor other than 1 and p, then p is a composite number.
- Examples:
  - $p = 5$; factors: 1, 5; it is prime
  - $p = 6$; factors: 1, 2, 3, 6

Primes, GCD, and LCM

- **Prime Numbers**: Let p be a positive integer greater than 1. p is a prime number if the only positive factors of p are 1 and p.
- If p has a positive factor other than 1 and p, then p is a composite number.
- Examples:
  - $p = 5$; factors: 1, 5; it is prime
  - $p = 6$; factors: 1, 2, 3, 6; it is composite

Primes, GCD, and LCM

- **Prime Numbers**: Let p be a positive integer greater than 1. p is a prime number if the only positive factors of p are 1 and p.
- If p has a positive factor other than 1 and p, then p is a composite number.
- Examples:
  - $p = 5$; factors: 1, 5; it is prime
  - $p = 6$; factors: 1, 2, 3, 6; it is composite
- 1 is neither a prime nor a composite number.

Primes, GCD, and LCM

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

Primes, GCD, and LCM

- **Theorem 1 - Fundamental Theorem of Arithmetic**: Every positive integer greater than 1 can be written uniquely as a prime or as a product of two or more primes written in the order of nondecreasing size.
- In other words: every natural number greater than 1 can be written as a product involving only prime factors.

Primes, GCD, and LCM

- **Theorem 1 - Fundamental Theorem of Arithmetic**: Every positive integer greater than 1 can be written uniquely as a prime or as a product of two or more primes written in the order of nondecreasing size.
- In other words: every natural number greater than 1 can be written as a product involving only prime factors.
- Examples (prime factorizations):
  - 100

Primes, GCD, and LCM

- **Theorem 1 - Fundamental Theorem of Arithmetic**: Every positive integer greater than 1 can be written uniquely as a prime or as a product of two or more primes written in the order of nondecreasing size.
- In other words: every natural number greater than 1 can be written as a product involving only prime factors.
- Examples (prime factorizations):
  - $100 = 4 \cdot 25$

Primes, GCD, and LCM

- **Theorem 1 - Fundamental Theorem of Arithmetic**: Every positive integer greater than 1 can be written uniquely as a prime or as a product of two or more primes written in the order of nondecreasing size.
- In other words: every natural number greater than 1 can be written as a product involving only prime factors.
- Examples (prime factorizations):
  - $100 = 4 \cdot 25 = 2 \cdot 2 \cdot 5 \cdot 5$

Primes, GCD, and LCM

- **Theorem 1 - Fundamental Theorem of Arithmetic**: Every positive integer greater than 1 can be written uniquely as a prime or as a product of two or more primes written in the order of nondecreasing size.
- In other words: every natural number greater than 1 can be written as a product involving only prime factors.
- Examples (prime factorizations):
  - $100 = 4 \cdot 25 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$

Primes, GCD, and LCM

- **Theorem 1 - Fundamental Theorem of Arithmetic**: Every positive integer greater than 1 can be written uniquely as a prime or as a product of two or more primes written in the order of nondecreasing size.
- In other words: every natural number greater than 1 can be written as a product involving only prime factors.
- Examples (prime factorizations):
  - $100 = 4 \cdot 25 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
  - 1024

Primes, GCD, and LCM

- **Theorem 1 - Fundamental Theorem of Arithmetic**: Every positive integer greater than 1 can be written uniquely as a prime or as a product of two or more primes written in the order of nondecreasing size.
- In other words: every natural number greater than 1 can be written as a product involving only prime factors.
- Examples (prime factorizations):
  - $100 = 4 \cdot 25 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
  - $1024 = 2^{10}$

Primes, GCD, and LCM

- **Theorem 2**: If n is a composite integer, then n has a prime factor less than or equal to $\sqrt{n}$.

Primes, GCD, and LCM

- **Theorem 2**: If n is a composite integer, then n has a prime factor less than or equal to $\sqrt{n}$.
- Examples: Find the prime factorizations of (a) 101 and (b) 7007.

Primes, GCD, and LCM

- **Theorem 3**: There are infinitely many primes.

Primes, GCD, and LCM

- **Theorem 3**: There are infinitely many primes.
- **Theorem 4**: The number of primes not exceeding x approaches $\frac{x}{\ln x}$ as $x \to \infty$.

Primes, GCD, and LCM

- **Definition**: If a prime number x has the form $x = 2^p - 1$ for some prime number p, then x is a Mersenne prime.

Primes, GCD, and LCM

- **Definition**: If a prime number x has the form $x = 2^p - 1$ for some prime number p, then x is a Mersenne prime.
- Note that $x = 2^p - 1$ for a prime number p does not necessarily imply that x is a prime number.

Primes, GCD, and LCM

- **Definition**: If a prime number x has the form $x = 2^p - 1$ for some prime number p, then x is a Mersenne prime.
- Note that $x = 2^p - 1$ for a prime number p does not necessarily imply that x is a prime number.
- Examples:
  - $2^3 - 1 = 7$

Primes, GCD, and LCM

- **Definition**: If a prime number x has the form $x = 2^p - 1$ for some prime number p, then x is a Mersenne prime.
- Note that $x = 2^p - 1$ for a prime number p does not necessarily imply that x is a prime number.
- Examples:
  - $2^3 - 1 = 7 \implies$ 7 is a Mersenne prime.

Primes, GCD, and LCM

- **Definition**: If a prime number x has the form $x = 2^p - 1$ for some prime number p, then x is a Mersenne prime.
- Note that $x = 2^p - 1$ for a prime number p does not necessarily imply that x is a prime number.
- Examples:
  - $2^3 - 1 = 7 \implies$ 7 is a Mersenne prime.
  - $2^5 - 1 = 31$

Primes, GCD, and LCM

- **Definition**: If a prime number x has the form $x = 2^p - 1$ for some prime number p, then x is a Mersenne prime.
- Note that $x = 2^p - 1$ for a prime number p does not necessarily imply that x is a prime number.
- Examples:
  - $2^3 - 1 = 7 \implies$ 7 is a Mersenne prime.
  - $2^5 - 1 = 31 \implies$ 31 is a Mersenne prime.

Primes, GCD, and LCM

- **Definition**: If a prime number x has the form $x = 2^p - 1$ for some prime number p, then x is a Mersenne prime.
- Note that $x = 2^p - 1$ for a prime number p does not necessarily imply that x is a prime number.
- Examples:
  - $2^3 - 1 = 7 \implies$ 7 is a Mersenne prime.
  - $2^5 - 1 = 31 \implies$ 31 is a Mersenne prime.
  - $2^{11} - 1 = 2047 = 23 \cdot 89$ (a composite number).

Primes, GCD, and LCM

- **Greatest Common Divisor (GCD)**: Let a and b be non-zero integers. The largest positive integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b and is denoted $\gcd(a, b)$.

Primes, GCD, and LCM

- **Greatest Common Divisor (GCD)**: Let a and b be non-zero integers. The largest positive integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b and is denoted $\gcd(a, b)$.
- If $\gcd(a, b) = 1$, then a and b are relatively prime.

Primes, GCD, and LCM

- **Greatest Common Divisor (GCD)**: Let a and b be non-zero integers. The largest positive integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b and is denoted $\gcd(a, b)$.
- If $\gcd(a, b) = 1$, then a and b are relatively prime.
- Example 1: Find gcd(24,36).

Primes, GCD, and LCM

- **Greatest Common Divisor (GCD)**: Let a and b be non-zero integers. The largest positive integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b and is denoted $\gcd(a, b)$.
- If $\gcd(a, b) = 1$, then a and b are relatively prime.
- Example 1: Find gcd(24,36).
  - Factors of 24: 1, 2, 3, 4, 6, 8, 12, 24

Primes, GCD, and LCM

- **Greatest Common Divisor (GCD)**: Let a and b be non-zero integers. The largest positive integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b and is denoted $\gcd(a, b)$.
- If $\gcd(a, b) = 1$, then a and b are relatively prime.
- Example 1: Find gcd(24,36).
  - Factors of 24: 1, 2, 3, 4, 6, 8, 12, 24
  - Factors of 36: 1, 2, 3, 4, 6, 9, 12, 18, 36

Primes, GCD, and LCM

- **Greatest Common Divisor (GCD)**: Let a and b be non-zero integers. The largest positive integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b and is denoted $\gcd(a, b)$.
- If $\gcd(a, b) = 1$, then a and b are relatively prime.
- Example 1: Find gcd(24,36).
  - Factors of 24: 1, 2, 3, 4, 6, 8, 12, 24
  - Factors of 36: 1, 2, 3, 4, 6, 9, 12, 18, 36
  - $\gcd(24{,}36) = 12$

Primes, GCD, and LCM

- **Greatest Common Divisor (GCD)**: Let a and b be non-zero integers. The largest positive integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b and is denoted $\gcd(a, b)$.
- If $\gcd(a, b) = 1$, then a and b are relatively prime.
- Example 1: Find gcd(24,36).
  - Factors of 24: 1, 2, 3, 4, 6, 8, 12, 24
  - Factors of 36: 1, 2, 3, 4, 6, 9, 12, 18, 36
  - $\gcd(24,36) = 12$
- Example 2: Find gcd(15,22).

Primes, GCD, and LCM

- **Greatest Common Divisor (GCD)**: Let a and b be non-zero integers. The largest positive integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b and is denoted $\gcd(a, b)$.
- If $\gcd(a, b) = 1$, then a and b are relatively prime.
- Example 1: Find gcd(24,36).
  - Factors of 24: 1, 2, 3, 4, 6, 8, 12, 24
  - Factors of 36: 1, 2, 3, 4, 6, 9, 12, 18, 36
  - $\gcd(24{,}36) = 12$
- Example 2: Find gcd(15,22).
  - Factors of 15: 1, 3, 5, 15

Primes, GCD, and LCM

- **Greatest Common Divisor (GCD)**: Let a and b be non-zero integers. The largest positive integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b and is denoted $\gcd(a, b)$.
- If $\gcd(a, b) = 1$, then a and b are relatively prime.
- Example 1: Find gcd(24,36).
  - Factors of 24: 1, 2, 3, 4, 6, 8, 12, 24
  - Factors of 36: 1, 2, 3, 4, 6, 9, 12, 18, 36
  - $\gcd(24{,}36) = 12$
- Example 2: Find gcd(15,22).
  - Factors of 15: 1, 3, 5, 15
  - Factors of 22: 1, 2, 11, 22

Primes, GCD, and LCM

- **Greatest Common Divisor (GCD)**: Let a and b be non-zero integers. The largest positive integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b and is denoted $\gcd(a, b)$.
- If $\gcd(a, b) = 1$, then a and b are relatively prime.
- Example 1: Find gcd(24,36).
  - Factors of 24: 1, 2, 3, 4, 6, 8, 12, 24
  - Factors of 36: 1, 2, 3, 4, 6, 9, 12, 18, 36
  - $\gcd(24{,}36) = 12$
- Example 2: Find gcd(15,22).
  - Factors of 15: 1, 3, 5, 15
  - Factors of 22: 1, 2, 11, 22
  - $\gcd(15{,}22) = 1$ (therefore 15 and 22 are relatively prime).

Primes, GCD, and LCM

- Integers $a_1, a_2, \ldots a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ for every $1 \leq i, j \leq n$, $i \neq j$.

Primes, GCD, and LCM

- Integers $a_1, a_2, \ldots a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ for every $1 \leq i, j \leq n$, $i \neq j$.
- Example: Problem 17 b: Are 14, 15, and 21 pairwise relatively prime?

Primes, GCD, and LCM

- Integers $a_1, a_2, \ldots a_n$ are pairwise relatively prime if $\gcd(a_i, a_j)$ $= 1$ for every $1 \leq i, j \leq n$, $i \neq j$.
- Example: Problem 17 b: Are 14, 15, and 21 pairwise relatively prime?
  - $\gcd(14{,}15) = 1$

Primes, GCD, and LCM

- Integers $a_1, a_2, \ldots a_n$ are pairwise relatively prime if $\gcd(a_i, a_j)$ $= 1$ for every $1 \leq i, j \leq n$, $i \neq j$.
- Example: Problem 17 b: Are 14, 15, and 21 pairwise relatively prime?
  - gcd(14,15) = 1
  - gcd(14,21) = 7

Primes, GCD, and LCM

- Integers $a_1, a_2, \ldots a_n$ are pairwise relatively prime if gcd(a_i, a_j) $= 1$ for every $1 \leq i, j \leq n$, $i \neq j$.
- Example: Problem 17 b: Are 14, 15, and 21 pairwise relatively prime?
  - gcd(14,15) $= 1$
  - gcd(14,21) $= 7$
  - gcd(15,21) $= 3$

Primes, GCD, and LCM

- Integers $a_1, a_2, \ldots a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ for every $1 \leq i, j \leq n$, $i \neq j$.
- Example: Problem 17 b: Are 14, 15, and 21 pairwise relatively prime?
  - gcd(14,15) $= 1$
  - gcd(14,21) $= 7$
  - gcd(15,21) $= 3$
  - 14, 15, and 21 are not pairwise relatively prime.

Primes, GCD, and LCM

- **Least Common Multiple (LCM)**: The least common multiple of two integers a and b is the smallest positive integer that is divisible by both a and b. It is denoted by $\text{lcm}(a, b)$.

Primes, GCD, and LCM

- **Least Common Multiple (LCM)**: The least common multiple of two integers a and b is the smallest positive integer that is divisible by both a and b. It is denoted by $\mathrm{lcm}(a, b)$.
- Example: 6 and 8

Primes, GCD, and LCM

- **Least Common Multiple (LCM)**: The least common multiple of two integers a and b is the smallest positive integer that is divisible by both a and b. It is denoted by $\text{lcm}(a, b)$.
- Example: 6 and 8
  - Multiples of 6: 6, 12, 18, 24, 30, 36, . . .

Primes, GCD, and LCM

- **Least Common Multiple (LCM)**: The least common multiple of two integers a and b is the smallest positive integer that is divisible by both a and b. It is denoted by $\mathrm{lcm}(a, b)$.
- Example: 6 and 8
  - Multiples of 6: 6, 12, 18, 24, 30, 36, ...
  - Multiples of 8: 8, 16, 24, 32, 40, 48, ...

Primes, GCD, and LCM

- **Least Common Multiple (LCM)**: The least common multiple of two integers a and b is the smallest positive integer that is divisible by both a and b. It is denoted by $\mathrm{lcm}(a, b)$.
- Example: 6 and 8
  - Multiples of 6: 6, 12, 18, 24, 30, 36, ...
  - Multiples of 8: 8, 16, 24, 32, 40, 48, ...
  - $\mathrm{lcm}(6,8) = 24$

Primes, GCD, and LCM

- If $a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$, then we can compute $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ in the following way:

Primes, GCD, and LCM

- If $a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$, then we can compute $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ in the following way:
  - $\gcd(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$

Primes, GCD, and LCM

- If $a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$, then we can compute $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ in the following way:
  - $\gcd(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$
  - $\operatorname{lcm}(a, b) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$

Primes, GCD, and LCM

- If $a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$, then we can compute $\gcd(a, b)$ and $\text{lcm}(a, b)$ in the following way:
  - $\gcd(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$
  - $\text{lcm}(a, b) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$
- Example: $24 = 2^3 \cdot 3^1$ and $36 = 2^2 \cdot 3^2$

Primes, GCD, and LCM

- If $a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$, then we can compute $\gcd(a, b)$ and $\text{lcm}(a, b)$ in the following way:
  - $\gcd(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$
  - $\text{lcm}(a, b) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$
- Example: $24 = 2^3 \cdot 3^1$ and $36 = 2^2 \cdot 3^2$
  - $\gcd(24{,}36) = 2^{\min(3,2)} \cdot 3^{\min(1,2)} = 2^2 \cdot 3^1 = 12.$

Primes, GCD, and LCM

- If $a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$, then we can compute $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ in the following way:
  - $\gcd(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$
  - $\operatorname{lcm}(a, b) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$
- Example: $24 = 2^3 \cdot 3^1$ and $36 = 2^2 \cdot 3^2$
  - $\gcd(24{,}36) = 2^{\min(3,2)} \cdot 3^{\min(1,2)} = 2^2 \cdot 3^1 = 12.$
  - $\operatorname{lcm}(24{,}36) = 2^{\max(3,2)} \cdot 3^{\max(1,2)} = 2^3 \cdot 3^2 = 72.$

Primes, GCD, and LCM

- **Theorem 5**: Let a and b be positive integers. Then $ab = \gcd(a, b) \cdot \mathrm{lcm}(a, b)$.

Primes, GCD, and LCM

- There is a more efficient way to compute the greatest common divisor of two positive integers. It is known as **the Euclidean Algorithm**.

Primes, GCD, and LCM

- There is a more efficient way to compute the greatest common divisor of two positive integers. It is known as **the Euclidean Algorithm**.
- **Lemma 1**: Let $a = q \cdot b + r$, where a, b, q, r are integers and $0 \leq r < |b|$. Then $\gcd(a, b) = \gcd(b, r)$.

Primes, GCD, and LCM

- There is a more efficient way to compute the greatest common divisor of two positive integers. It is known as **the Euclidean Algorithm**.
- **Lemma 1**: Let $a = q \cdot b + r$, where a, b, q, r are integers and $0 \leq r < |b|$. Then $\gcd(a, b) = \gcd(b, r)$.
- In other words, $\gcd(a, b) = \gcd(b, a \mod b)$.

Primes, GCD, and LCM

- Euclidean Algorithm - takes positive integers a and b as input:
- $x := a$
  $y := b$
  while $y \neq 0$ **do**
  $r := x \mod y$
  $x := y$
  $y := r$
  end while
  Return x

Primes, GCD, and LCM

- **Theorem 6**: Let a, b be positive integers. Then there exist two integers s and t such that $\gcd(a, b) = s \cdot a + t \cdot b$.

Primes, GCD, and LCM

- **Lemma 3**: If p is prime and $p \mid a_1 \cdot a_2 \cdots a_n$, where each a_i is a positive integer, then $p \mid a_i$ for some i.

Primes, GCD, and LCM

- Practice problems:
  - Find all primes ≤ 30.

Primes, GCD, and LCM

- Practice problems:
  - Find all primes ≤ 30.
  - Section 4.3 Problem 15: Find all positive integers less than 30 that are relatively prime to 30.