Primes and GCDs

Lecture/Week 9

Copyright ©2023. All Rights Reserved.

Dr. Bonaventure Chidube Molokwu
bonaventure.molokwu[at]concordia.ca

Gina Cody School of Engineering and Computer Science
Concordia University
Montreal
Quebec - Canada

Introduction

Lecture/Week Outline & Learning Outcomes

1. **Lesson/Week Outline:**
   1.1 Prime Numbers and their Properties.
   1.2 Conjectures and Open Problems about Primes.
   1.3 Greatest Common Divisors and Least Common Multiples.
   1.4 The Euclidian Algorithm.

2. **Learning Outcomes:**
   2.1 State the properties of Prime Number as well as examples of Prime Numbers.
   2.2 Implement the operations of Greatest Common Divisors and Least Common Multiples.

Primes and GCDs

1 Primes
- Introduction
- Erastosthenes
- Infinitude
- Mersenne Prime
- Generating Primes
- Conjecture ⟶ Prime
- Class Activity

GCD & LCM
- gcd
- Relative Prime
- gcd() via Prime Factorization
- lcm
- lcm() via Prime Factorization
- Euclidean Algorithm
- Bézout's Theorem
- Dividing Congruences
- Class Activity

Q & A

- **Prime:** A positive integer, p, that is greater than 1 and its only positive factors are 1 and p.
  Examples: $2, 3, 5, 7, \ldots$

- **Composite:** A positive integer, p, that is greater than 1, and is NOT *Prime*. Examples: $4, 6, 8, 9, \ldots$

- **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*. Examples: $(4 = 2 \times 2)$; $(6 = 2 \times 3)$; $(8 = 2 \times 2 \times 2)$; $(9 = 3 \times 3)$; etc.

Primes and GCDs

Primes
2 Introduction
Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture → Prime
Class Activity

GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity

Q & A

- **Sieve of Erastosthenes:** This technique can be used to find all Primes not exceeding a specified positive integer, $n \in \mathbb{Z}^+$. This involves computing $p_i \in P : \forall\, p_i \ \leq \lceil \sqrt{n} \rceil$.

  For example: To find all Primes from $1, \ldots, 100$. Hence, we compute: $\forall\, p_i \ \leq \lceil \sqrt{100} \rceil; \quad \forall\, p_i \ \leq 10; \quad P = \{2, 3, 5, 7\}$

  1. Delete all integers divisible by 2 (*except 2 itself*).
  2. Delete all integers divisible by 3 (*except 3 itself*).
  3. Delete all integers divisible by 5 (*except 5 itself*).
  4. Delete all integers divisible by 7 (*except 7 itself*).
  5. Therefore, the remaining integers are not divisible by any of the previous integers, *other than 1*; and these represent the Primes.

Primes and GCDs

Primes
Introduction
3 Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture ⟶ Prime
Class Activity

GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity

Q & A

- **Example:** Using the *Sieve of Erastosthenes*, the Primes between 1 and 100 are: $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97\}$

- **Infinitude of Primes:** There are infinitely many primes.

  Proof: We can give a proof by *Contradiction*.

  Assume that there exist a countable number, n, of primes such that: $p_1, p_2, p_3, \ldots, p_n$

Primes and GCDs
Primes
Introduction
Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture → Prime
Class Activity
GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity
Q & A

- **Infinitude of Primes:**

  Let $q = (p_1 \times p_2 \times p_3 \times \ldots \times p_n) + 1$

  $\therefore$ via Fundamental Theorem of Arithmetic, q is either a new *Prime* OR it is the product two/more *Primes*.

  IF: no $p_i \in (p_1, p_2, p_3, \ldots, p_n)$ *divides* q. In other words, $p_i \nmid q$.

  THEN: a new *Prime* OR a product of two/more new *Primes*, q, is computed and $q \notin (p_1, p_2, p_3, \ldots, p_n)$.

  Conclusively, this contradicts our initial assumption that there exist a countable number, n, of primes.

Primes and GCDs

Primes
Introduction
Erastosthenes
5 Infinitude
Mersenne Prime
Generating Primes
Conjecture ⟶ Prime
Class Activity

GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity

Q & A

- **Example 1:** Let us compute a new Prime with regard to the first three (3) prime numbers.

  First three (3) primes: $\{2, 3, 5\}$

  $q = (2 \times 3 \times 5) + 1 = 30 + 1 = 31$

- **Example 2:** Let us compute a new Prime with regard to the first five (5) prime numbers.

  First five (5) primes: $\{2, 3, 5, 7, 11\}$

  $q = (2 \times 3 \times 5 \times 7 \times 11) + 1 = 2310 + 1 = 2311$

Primes and GCDs
Primes
Introduction
Erastosthenes
6 Infinitude
Mersenne Prime
Generating Primes
Conjecture → Prime
Class Activity
GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity
Q & A

- **Mersenne Prime:** This is a Prime Number that can be uniquely represented in the form: $2^p - 1$, where p is Prime Number.
- **Examples of Mersenne Primes:**

  $p = 2; \quad 2^2 - 1 = 4 - 1 = 3$ is a Mersenne Prime

  $p = 3; \quad 2^3 - 1 = 8 - 1 = 7$ is a Mersenne Prime

  $p = 5; \quad 2^5 - 1 = 32 - 1 = 31$ is a Mersenne Prime

  $p = 7; \quad 2^7 - 1 = 128 - 1 = 127$ a Mersenne Prime
- **Examples of Non-Mersenne Primes:**

  $p = 11; \quad 2^{11} - 1 = 2048 - 1 = 2047 = 23 \times 89$

Primes and GCDs

Primes
Introduction
Erastosthenes
Infinitude
7 Mersenne Prime
Generating Primes
Conjecture ⟶ Prime
Class Activity

GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity

Q & A

- The generation or computation of newer Primes is of both *theoretical* and *practical* interests.
- Large Primes can be useful in designing encryption algorithms and ciphertexts.
- Currently, there exist no generic formula or function, $f(n)$, that always produces Primes with respect to positive integers.

Primes and GCDs

Primes
Introduction
Erastosthenes
Infinitude
Mersenne Prime
8 Generating Primes
Conjecture ⟶ Prime
Class Activity

GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity

Q & A

Primes
Conjectures about Primes

- **Goldbach's Conjecture:** Every even integer (n), such that $n > 2$, is the sum of exactly two Prime Numbers. This has been verified by computer for all positive even integers up to 1.6×10^{18}.

- **The Twin Prime Conjecture:** Twin Primes are pairs of Prime Numbers that differ by 2. E.g. 3 & 5; 5 & 7; 11 & 13; etc. Thus, there are infinitely many pairs of Twin Primes.

  P.S. The world's record for Twin Primes (as of early 2018) consists of the numbers $2,996,863,034,895 \times 2^{1,290,000} \pm 1$.

Primes and GCDs

Primes
Introduction
Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture → Prime
Class Activity

GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity

Q & A

Navigate to: `www.kahoot.it`

Game PIN: available in-class

Primes and GCDs
Primes
Introduction
Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture ⟶ Prime
10 Class Activity
GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity
Q & A

Greatest Common Divisor/Factor
gcd()

- **Greatest Common Divisor:** Let a and b be integers, and are not both zero. Hence, the largest integer, d, such that $d \mid a$ and $d \mid b$, is called the greatest common divisor (gcd) of a and b.
- The greatest common divisor of a and $b \equiv gcd(a, b)$.
- **Example:** What is the greatest common divisor (gcd) of 16 and 24?
  Factors/Divisors of 16: $\{1, 2, 4, \mathbf{8}, 16\}$
  Factors/Divisors of 24: $\{1, 2, 3, 4, 6, \mathbf{8}, 12, 24\}$
  Therefore, the gcd(16, 24) is **8**.

Primes and GCDs

Primes
Introduction
Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture ⟶ Prime
Class Activity

GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity

Q & A

Greatest Common Divisor/Factor

gcd() and relatively Prime

- Two integers a and b are **relatively Prime** if their greatest common divisor is **1**.

- **Example:** Evaluate 7 and 10 with respect to their greatest common divisor (gcd).

  <u>Solution:</u>

  Factors/Divisors of 7: $\{\mathbf{1}, 7\}$

  Factors/Divisors of 10: $\{\mathbf{1}, 2, 5, 10\}$

  Therefore, the gcd(7, 10) is **1**.

  Hence, 7 and 10 are *relatively Prime*.

Primes and GCDs

Primes
Introduction
Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture $\longrightarrow$ Prime
Class Activity

GCD & LCM
gcd
12 Relative Prime
gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity

Q & A

Greatest Common Divisor/Factor

gcd() and pairwise relatively Prime

- 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 10, 17 and 21 are *pairwise relatively prime*.

  Factors/Divisors of 10: $\{1, 2, 5, 10\}$

  Factors/Divisors of 17: $\{1, 17\}$

  Factors/Divisors of 21: $\{1, 3, 7, 21\}$

  Therefore, the gcd(10, 17) = **1**; the gcd(10, 21) = **1**; and the gcd(17, 21) = **1**.

  So, 10, 17, and 21 are *pairwise relatively Prime*.

Primes and GCDs

Primes
- Introduction
- Erastosthenes
- Infinitude
- Mersenne Prime
- Generating Primes
- Conjecture ⟶ Prime
- Class Activity

GCD & LCM
- gcd
- Relative Prime
- gcd() via Prime Factorization
- lcm
- lcm() via Prime Factorization
- Euclidean Algorithm
- Bézout's Theorem
- Dividing Congruences
- Class Activity

Q & A

- Given two integers a and b, via the **Fundamental Theorem of Arithmetic**; we can represent a and b as *Primes* or *products of Primes*.
- $a = p_1^{e_1} \times p_2^{e_2} \times \ldots \times p_n^{e_n}$ *Prime Factorization of a*
  $b = p_1^{f_1} \times p_2^{f_2} \times \ldots \times p_n^{f_n}$ *Prime Factorization of b*
  e_i, f_i and p_i are exponents (non-negative) and primes, respectively.
- Thus, we collate all Primes present in the *Prime Factorization* of either a or b.
  gcd(a,b) = $p_1^{min(e_1,f_1)} \times p_2^{min(e_2,f_2)} \times \ldots \times p_n^{min(e_n,f_n)}$

Primes and GCDs

Primes
Introduction
Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture → Prime
Class Activity

GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity

Q & A

Greatest Common Divisor/Factor

Greatest Common Divisor via Prime Factorizations

- **Example:** Using *Prime Factorization* method, find the greatest common divisor (gcd) of 16 and 24?

  Solution:

  Prime Factorization of 16: $2 \times 8 = 2^4$

  Prime Factorization of 24: $8 \times 3 = 2^3 \times 3$

  gcd(16, 24) = $2^{min(4,3)} \times 3^{min(0,1)}$

  gcd(16, 24) = $2^3 \times 3^0$

  gcd(16, 24) = 8×1

  Therefore, the gcd(16, 24) = **8**.

Primes and GCDs
Primes
Introduction
Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture⟶Prime
Class Activity
GCD & LCM
gcd
Relative Prime
15 gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity
Q & A

Greatest Common Divisor/Factor

Greatest Common Divisor via Prime Factorizations

- **Example:** Using *Prime Factorization* method, find the greatest common divisor (gcd) of 120 and 500?

<u>Solution:</u>

Prime Factorization of 120: $8 \times 15 = 2^3 \times 3 \times 5$

Prime Factorization of 500: $4 \times 125 = 2^2 \times 5^3$

$\gcd(120, 500) = 2^{min(3,2)} \times 3^{min(1,0)} \times 5^{min(1,3)}$

$\gcd(120, 500) = 2^2 \times 3^0 \times 5^1$

$\gcd(120, 500) = 4 \times 1 \times 5$

Therefore, the $\gcd(120, 500) =$ **20**.

Primes and GCDs

Primes
- Introduction
- Erastosthenes
- Infinitude
- Mersenne Prime
- Generating Primes
- Conjecture → Prime
- Class Activity

GCD & LCM
- gcd
- Relative Prime
- gcd() via Prime Factorization
- lcm
- lcm() via Prime Factorization
- Euclidean Algorithm
- Bézout's Theorem
- Dividing Congruences
- Class Activity

Q & A

- **Example:** A classroom comprises: 48 females & 40 males. In an exam, the instructor wishes to have students sit in rows such that each row has the same number of students, and each row is composed of same-gender students. Efficiently, how many students/row and rows can be achieved?

  Solution:

  Prime Factorization of 48: $2 \times 2 \times 2 \times 2 \times 3 = 2^4 \times 3$

  Prime Factorization of 40: $2 \times 2 \times 2 \times 5 = 2^3 \times 5$

  gcd(48, 40) = $2^{min(4,3)} \times 3^{min(1,0)} \times 5^{min(0,1)}$

  gcd(48, 40) = $2^3 \times 3^0 \times 5^0$

  gcd(48, 40) = $8 \times 1 \times 1$

  Therefore, the gcd(48, 40) = No. of Students/Row = **8**.

  Furthermore, No. of achieveable rows = $\frac{48+40}{8} = \frac{88}{8} = \mathbf{11}$.

Primes and GCDs

Primes
Introduction
Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture → Prime
Class Activity

GCD & LCM
gcd
Relative Prime
17 gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity

Q & A

Least Common Multiple
lcm()

- **Least Common Multiple:** Let a and b be integers. Hence, the smallest positive integer, c, such that $a \mid c$ and $b \mid c$, is called the least common multiple (lcm) of a and b.
- The least common multiple of a and $b \equiv lcm(a, b)$.
- **Example:** What is the least common multiple (lcm) of 3 and 5?
  Multiples of 3: $\{3, 6, 9, 12, \mathbf{15}, 18, \ldots\}$
  Multiples of 5: $\{5, 10, \mathbf{15}, 20, 25, \ldots\}$
  Therefore, the lcm(3, 5) is **15**.

Primes and GCDs

Primes
Introduction
Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture ⟶ Prime
Class Activity

GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
18 lcm
lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity

Q & A

Least Common Multiple

Least Common Multiple via Prime Factorizations

- Given two integers a and b, via the **Fundamental Theorem of Arithmetic**; we can represent a and b as *Primes* or *products of Primes*.
- $a = p_1^{e_1} \times p_2^{e_2} \times \ldots \times p_n^{e_n}$ *Prime Factorization of a*
  $b = p_1^{f_1} \times p_2^{f_2} \times \ldots \times p_n^{f_n}$ *Prime Factorization of b*
  e_i, f_i and p_i are exponents (non-negative) and primes, respectively.
- Thus, we collate all Primes present in the *Prime Factorization* of either a or b.
  lcm(a,b) = $p_1^{max(e_1,f_1)} \times p_2^{max(e_2,f_2)} \times \ldots \times p_n^{max(e_n,f_n)}$

Primes and GCDs
Primes
Introduction
Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture ⟶ Prime
Class Activity
GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
19 lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity
Q & A

Least Common Multiple

Least Common Multiple via Prime Factorizations

- **Example:** Using *Prime Factorization* method, find the least common multiple (lcm) of 3 and 5?

  Solution:

  Prime Factorization of 3: 3

  Prime Factorization of 5: 5

  $\text{lcm}(3, 5) = 3^{max(1,0)} \times 5^{max(0,1)}$

  $\text{lcm}(3, 5) = 3^1 \times 5^1$

  $\text{lcm}(3, 5) = 3 \times 5$

  Therefore, the lcm(3, 5) = **15**.

Primes and GCDs

Primes
Introduction
Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture ⟶ Prime
Class Activity

GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
20 lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity

Q & A

Least Common Multiple
Least Common Multiple via Prime Factorizations

- **Example:** Using *Prime Factorization* method, find the least common multiple (lcm) of 20 and 42?

  Solution:

  Prime Factorization of 20: $4 \times 5 = 2^2 \times 5$

  Prime Factorization of 42: $2 \times 3 \times 7$

  $\text{lcm}(20, 42) = 2^{max(2,1)} \times 3^{max(0,1)} \times 5^{max(1,0)} \times 7^{max(0,1)}$

  $\text{lcm}(20, 42) = 2^2 \times 3^1 \times 5^1 \times 7^1$

  $\text{lcm}(20, 42) = 4 \times 3 \times 5 \times 7$

  Therefore, the $\text{lcm}(20, 42) = \mathbf{420}$.

Primes and GCDs

Primes
Introduction
Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture → Prime
Class Activity

GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity

Q & A

Least Common Multiple

Least Common Multiple via Prime Factorizations

- **Example:** An xmas' tree lighting possesses the following properties: Red Light $\Rightarrow$ illuminates every 2 seconds.
  Blue Light $\Rightarrow$ illuminates every 3 seconds.
  Yellow Light $\Rightarrow$ illuminates every 4 seconds.
  Thus, when will all three (3) lights illuminate at same time?

  Solution:

  Prime Factorization of 2: 2

  Prime Factorization of 3: 3

  Prime Factorization of 4: 2^2

  lcm(2, 3, 4) = $2^{max(1,0,2)} \times 3^{max(0,1,0)}$

  lcm(2, 3, 4) = $2^2 \times 3^1$

  lcm(2, 3, 4) = 4×3

  Therefore, lcm(2, 3, 4) = Sync 3-light illumination = **12**secs.

Primes and GCDs

Primes
Introduction
Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture → Prime
Class Activity

GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity

Q & A

- The Euclidean algorithm is an efficient method for computing the greatest common divisor (gcd) of two integers, a and b.

Algorithm 1 Euclidean Algorithm for gcd(a, b)

Input: $a \in \mathbb{Z}^+, b \in \mathbb{Z}^+$

Output: $gcd(a, b) \in \mathbb{Z}^+$

while $b \neq 0$ ***and*** $a > b$ **do**

$\quad r = a \textbf{ mod } b$

$\quad a = b$

$\quad b = r$

return $gcd(a, b) = a$

Primes and GCDs

Primes
Introduction
Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture ⟶ Prime
Class Activity

GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
23 Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity

Q & A

Euclidean Algorithm

Euclidean Algorithm for gcd()

- **Example:** Using the *Euclidean Algorithm*, find the greatest common divisor (gcd) of 91 and 287?

  Solution:

  $r_1 = 287 \textbf{ mod } 91 = 14$

  $r_2 = 91 \textbf{ mod } 14 = 7$

  $r_3 = 14 \textbf{ mod } 7 = 0$

  $r_4 = 7 \textbf{ mod } 0 = STOP$

  $\therefore\ \gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = \mathbf{7}$.

Primes and GCDs

Primes
Introduction
Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture ⟶ Prime
Class Activity

GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
24 Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity

Q & A

- **Example:** Using the *Euclidean Algorithm*, find the greatest common divisor (gcd) of 360 and 210?

  Solution:

  $r_1 = 360 \textbf{ mod } 210 = 150$

  $r_2 = 210 \textbf{ mod } 150 = 60$

  $r_3 = 150 \textbf{ mod } 60 = 30$

  $r_4 = 60 \textbf{ mod } 30 = 0$

  $r_5 = 30 \textbf{ mod } 0 = STOP$

  $\therefore$ gcd(360, 210) = gcd(210, 150) = gcd(150, 60) = gcd(60, 30) = **30**.

Primes and GCDs
Primes
Introduction
Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture → Prime
Class Activity
GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
25 Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity
Q & A

Euclidean Algorithm Proof for gcd()

Correctness of the Euclidean Algorithm for gcd()

- Given two integers, a and b, where $a > b$. Prove that gcd(a, b) = gcd(b, r).
  $q \in \mathbb{Z} = a \,\textbf{div}\, b = \lfloor \frac{a}{b} \rfloor$
  $r \in \mathbb{N} = a \,\textbf{mod}\, b = a - (b \cdot q)$
- $r = a - (b \cdot q)$ .... (1)
  $a = (b \cdot q) + r$ .... (2)
- Suppose $d \in \mathbb{Z}$ divides a and b in (1). Thus, d must divide $a - (b \cdot q) = r$ in (1).
- Suppose $d \in \mathbb{Z}$ divides b and r in (2). Thus, d must divide $(b \cdot q) + r = a$ in (2).
- Conclusively, gcd(a, b) = gcd(b, r)

Primes and GCDs
Primes
Introduction
Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture → Prime
Class Activity
GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
26 Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity
Q & A

gcds as Linear Combinations
Bézout's Theorem

- **Bézout's Theorem:** Given two positive integers, a and b; then there exist integers s and t, known as *Bézout Coefficients*, such that $gcd(a, b) = s \cdot a + t \cdot b$

- **Example 1:** Express the gcd(252, 198) = 18 as a linear combination of 252 and 198.

Solution:

- **Step 1 ($a = (b \cdot q) + r$):** Apply Euclidean Algorithm to compute and express the gcd(252, 198) = 18.

$252 = (198 \cdot 1) + 54 \ldots\ldots\ldots\ldots\ldots\ldots (1)$

$198 = (54 \cdot 3) + 36 \ldots\ldots\ldots\ldots\ldots\ldots (2)$

gcds as Linear Combinations
Bézout's Theorem

- **Step 1 ($a = (b \cdot q) + r$):** *Contd.*

  $54 = (36 \cdot 1) + 18 \ldots\ldots\ldots\ldots\ldots\ldots (3)$

  $36 = (18 \cdot 2) + 0 \ldots\ldots\ldots\ldots\ldots\ldots (4)$ *STOP*

  $\therefore$ gcd(252, 198) = gcd(198, 54) = . . . = **18.**

- **Step 2 ($r = a - (b \cdot q)$):** Proceed reversely, and show that 18 = gcd(252, 198).

  From (3): $18 = 54 - (36 \cdot 1) \ldots\ldots\ldots\ldots (5)$

  From (2): $36 = 198 - (54 \cdot 3) \ldots\ldots\ldots\ldots (6)$

  Substitute $198 - (54 \cdot 3)$ for 36 in . . . (5)

  $$18 = 54 - (1 \cdot (198 - (54 \cdot 3)))$$

Primes and GCDs

Primes
Introduction
Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture ⟶ Prime
Class Activity

GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity

Q & A

- **Step 2 ($r = a - (b \cdot q)$):** Proceed reversely, ...

$$18 = 54 - (1 \cdot 198 - 1 \cdot (3 \cdot 54))$$

$$18 = 1 \cdot 54 - 1 \cdot 198 + 3 \cdot 54$$

$$18 = 4 \cdot 54 - 1 \cdot 198 \ldots\ldots\ldots\ldots (7)$$

From (1): $54 = 252 - (1 \cdot 198) \ldots\ldots\ldots\ldots (8)$

Substitute $252 - (1 \cdot 198)$ for 54 in ... (7)

$$18 = 4 \cdot (252 - (1 \cdot 198)) - 1 \cdot 198$$

$$18 = 4 \cdot 252 - 4 \cdot 198 - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$$

- **Conclusion:** gcd(252, 198) = 18 = $4 \cdot 252 - 5 \cdot 198$

  Bézout Coefficients = $(s, t) = (4, -5)$

Primes and GCDs

Primes
- Introduction
- Erastosthenes
- Infinitude
- Mersenne Prime
- Generating Primes
- Conjecture $\longrightarrow$ Prime
- Class Activity

GCD & LCM
- gcd
- Relative Prime
- gcd() via Prime Factorization
- lcm
- lcm() via Prime Factorization
- Euclidean Algorithm
- 29 Bézout's Theorem
- Dividing Congruences
- Class Activity

Q & A

- **Example 2:** Express the gcd(450, 120) as a linear combination of 120 and 450.

Solution:

- **Step 1 ($a = (b \cdot q) + r$):** Apply Euclidean Algorithm to compute and express the gcd(450, 120).

$450 = (120 \cdot 3) + 90 \ldots\ldots\ldots\ldots\ldots\ldots (1)$

$120 = (90 \cdot 1) + 30 \ldots\ldots\ldots\ldots\ldots\ldots (2)$

$90 = (30 \cdot 3) + 0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$ *STOP*

Therefore, the gcd(450, 120) = gcd(120, 90) = gcd(90, 30) = **30**.

Primes and GCDs

Primes
Introduction
Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture ⟶ Prime
Class Activity

GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity

Q & A

gcds as Linear Combinations
Bézout's Theorem

- **Step 2 ($r = a - (b \cdot q)$):** Proceed reversely, and show that $30 = \gcd(450, 120)$.

  From (2): $30 = 120 - (90 \cdot 1) \ldots\ldots\ldots\ldots\ldots (4)$

  From (1): $90 = 450 - (120 \cdot 3) \ldots\ldots\ldots\ldots\ldots (5)$

  Substitute $450 - (120 \cdot 3)$ for 90 in . . . (4)

$$30 = 120 - (1 \cdot (450 - (120 \cdot 3)))$$

$$30 = 1 \cdot 120 - 1 \cdot 450 + 3 \cdot 120$$

$$30 = 4 \cdot 120 - 1 \cdot 450$$

- **Conclusion:** $\gcd(450, 120) = 30 = 4 \cdot 120 - 1 \cdot 450$

  Bézout Coefficients = $(s, t) = (4, -1)$

Primes and GCDs

Primes
Introduction
Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture → Prime
Class Activity

GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity

Q & A

Dividing Congruences by an Integer

Dividing Congruence Relations by a Relative Prime

- Dividing a valid congruence by an integer, $c \in \mathbb{Z}$, does not always preserves its validity.
- However, dividing a valid congruence by an integer, $c \in \mathbb{Z}$, which is **relatively Prime** to its modulus relation always preserves the validity.

Proof: $gcd(c, m) = 1$

IF a and b are integers, and $m \in \mathbb{Z}^+$ is a positive integer; THEN $a \equiv b \pmod{m}$ is valid if $m \mid a - b$.

Multiplying both sides of $a \equiv b \pmod{m}$ by $c \in \mathbb{Z}$, still preserves the validity: $c \cdot a \equiv c \cdot b \pmod{m}$

$\frac{c \cdot a}{c} \equiv \frac{c \cdot b}{c} \pmod{m} \quad \rightarrow \quad a \equiv b \pmod{m}$

Primes and GCDs

Primes
- Introduction
- Erastosthenes
- Infinitude
- Mersenne Prime
- Generating Primes
- Conjecture → Prime
- Class Activity

GCD & LCM
- gcd
- Relative Prime
- gcd() via Prime Factorization
- lcm
- lcm() via Prime Factorization
- Euclidean Algorithm
- Bézout's Theorem
- Dividing Congruences
- Class Activity

Q & A

Navigate to: `www.kahoot.it`

Game PIN: available in-class

Primes and GCDs

Primes
- Introduction
- Erastosthenes
- Infinitude
- Mersenne Prime
- Generating Primes
- Conjecture → Prime
- Class Activity

GCD & LCM
- gcd
- Relative Prime
- gcd() via Prime Factorization
- lcm
- lcm() via Prime Factorization
- Euclidean Algorithm
- Bézout's Theorem
- Dividing Congruences
- Class Activity

Q & A

1. **Compute the following, viz: gcd(10, 12) and lcm(10, 12), respectively.**
   A. 2 and 60
   B. 60 and 2
   C. 1 and 120
   D. None of the above

2. $a \cdot b = \color{blue}{gcd(a, b)} \cdot \color{red}{lcm(a, b)}$
   A. True
   B. False
   C. Partially True
   D. None of the above

Primes and GCDs

Primes
Introduction
Erastosthenes
Infinitude
Mersenne Prime
Generating Primes
Conjecture $\longrightarrow$ Prime
Class Activity

GCD & LCM
gcd
Relative Prime
gcd() via Prime Factorization
lcm
lcm() via Prime Factorization
Euclidean Algorithm
Bézout's Theorem
Dividing Congruences
Class Activity

Q & A

Questions?
&
Answers!