INFORMATION & COMPUTER SCIENCES
UNIVERSITY of HAWAI'I at MĀNOA

Ch 4.3: Primes and Greatest Common Divisors

ICS 141: Discrete Mathematics for Computer Science I

KYLE BERNEY
DEPARTMENT OF ICS, UNIVERSITY OF HAWAII AT MANOA

Greatest Common Divisor

- Definition: If a and b are integers, not both zero, than an integer d is called the greatest common divisor of a and b if
  1. $d > 0$
  2. d is a common divisor of both a and b, and
  3. each integer f that is also a common divisor of both a and b is also a divisor of d
- Denoted $\text{GCD}(a, b)$

Greatest Common Divisor

- Definition: If a and b are integers, not both zero, than an integer d is called the greatest common divisor of a and b if
  1. $d > 0$
  2. d is a common divisor of both a and b, and
  3. each integer f that is also a common divisor of both a and b is also a divisor of d
- Denoted $\text{GCD}(a, b)$
- Ex: What is $\text{GCD}(12, 8)$?
  - The positive divisors of 12 are: 1, 2, 3, 4, 6, and 12
  - The positive divisors of 8 are: 1, 2, 4, and 8
  - $\text{GCD}(12, 8) = 4$

Euclidean Algorithm

- Given two positive integers a and b, the $\text{GCD}(a, b)$ can be found by sucessively dividing the larger integer by the smaller integer and replacing the larger integer with the remainder until it becomes 0
- Ex: Find the $\text{GCD}(341, 527)$
  - $527 = 341 \cdot 1 + 186$
  - $341 = 186 \cdot 1 + 155$
  - $186 = 155 \cdot 1 + 31$
  - $155 = 31 \cdot 5 + 0$

$$\text{GCD}(341, 527) = 31$$

Euclidean Algorithm

- Given two positive integers a and b, the $\texttt{GCD}(a, b)$ can be found by sucessively dividing the larger integer by the smaller integer and replacing the larger integer with the remainder until it becomes 0
- Correctness is based on the following lemma
- Lemma 1: Let $a = bq + r$, where a, b, q, and r are integers. Then $\texttt{GCD}(a, b) = \texttt{GCD}(b, r)$

Greatest Common Divisor

- Theorem 1: If a and b are integers, not both zero, then $\texttt{GCD}(a, b)$ exists and is unique

- Proof: (Sketch)
  Use the Euclidean Algorithm to show that $\texttt{GCD}(a, b)$ exists. It follow from the definition of GCD that if both d_1 and d_2 are greatest common divisors of a and b, then $d_1 \mid d_2$ and $d_2 \mid d_1$. By definition, there exists positive integers g and h such that $gd_1 = d_2$ and $hd_2 = d_1$. Hence, $d_2 = ghd_2$ and $1 = gh$, therefore, $g = h = 1$ and $d_1 = d_2$. ■

Linear Combinations

- An integral linear combination of the integers a and b is an expression of the form

$$ax + by$$

Linear Combinations

- An integral linear combination of the integers a and b is an expression of the form

$$ax + by$$

- Theorem 2: (Bezout's Theorem) If $d = \text{GCD}(a, b)$, then there exists integers x and y such that

$$ax + by = d$$

Linear Combinations

- An integral linear combination of the integers a and b is an expression of the form

$$ax + by$$

- Theorem 2: (Bezout's Theorem) If $d = \text{GCD}(a, b)$, then there exists integers x and y such that

$$ax + by = d$$

- Corollary 1: There exists integers x and y satisfying the equation

$$ax + by = c$$

if and only if $d \mid c$, where $d = \text{GCD}(a, b)$

Extended Euclidean Algorithm

- In the Euclidean Algorithm, successive remainders are used
- In the Extended Euclidean Algorithm, successive quotients are additionally used
  - Let $q_1, q_2, \ldots, q_k$ be the sequence of quotients
  - For $i = 1, 2, \ldots, k$, compute s_k and t_k where
    - $s_0 = 1$, $s_1 = 0$, and $s_i = s_{i-2} - q_{i-1} s_{i-1}$
    - $t_0 = 0$, $t_1 = 1$, and $t_i = t_{i-2} - q_{i-1} t_{i-1}$
  - s_k and t_k are the Bezout coefficients, satisfying

$$\text{GCD}(a, b) = as_k + bt_k$$

Extended Euclidean Algorithm

- Ex: Find the Bezout coefficients for 217 and 41
  - $217 = 41 \cdot 5 + 12$
  - $41 = 12 \cdot 3 + 5$
  - $12 = 5 \cdot 2 + 2$
  - $5 = 2 \cdot 2 + 1$
  - $2 = 1 \cdot 2 + 0$

Extended Euclidean Algorithm

- Ex: Find the Bezout coefficients for 217 and 41
  - $217 = 41 \cdot 5 + 12$
  - $41 = 12 \cdot 3 + 5$
  - $12 = 5 \cdot 2 + 2$
  - $5 = 2 \cdot 2 + 1$
  - $2 = 1 \cdot 2 + 0$
  - $q_1 = 5$, $q_2 = 3$, $q_3 = 2$, $q_4 = 2$, and $q_5 = 2$
  - $s_2 = s_0 - q_1 s_1 = 1 - 5(0) = 1$
  - $s_3 = s_1 - q_2 s_2 = 0 - 3(1) = -3$
  - $s_4 = s_2 - q_3 s_3 = 1 - 2(-3) = 7$
  - $s_5 = s_3 - q_4 s_4 = -3 - 2(7) = -17$

Extended Euclidean Algorithm

- Ex: Find the Bezout coefficients for 217 and 41
  - $217 = 41 \cdot 5 + 12$
  - $41 = 12 \cdot 3 + 5$
  - $12 = 5 \cdot 2 + 2$
  - $5 = 2 \cdot 2 + 1$
  - $2 = 1 \cdot 2 + 0$
  - $q_1 = 5$, $q_2 = 3$, $q_3 = 2$, $q_4 = 2$, and $q_5 = 2$
  - $t_2 = t_0 - q_1 t_1 = 0 - 5(1) = -5$
  - $t_3 = t_1 - q_2 t_2 = 1 - 3(-5) = 16$
  - $t_4 = t_2 - q_3 t_3 = -5 - 2(16) = -37$
  - $t_5 = t_3 - q_4 t_4 = 16 - 2(-37) = 90$

Extended Euclidean Algorithm

- Ex: Find the Bezout coefficients for 217 and 41
  - $217 = 41 \cdot 5 + 12$
  - $41 = 12 \cdot 3 + 5$
  - $12 = 5 \cdot 2 + 2$
  - $5 = 2 \cdot 2 + 1$
  - $2 = 1 \cdot 2 + 0$
  - $s_5 = -17$
  - $t_5 = 90$
  - $\text{GCD}(217, 41) = 1 = 217(-17) + 41(90)$

Primes

- Every integer greater than 1 is divisible by at least two integers (1 and itself)
- Definition: An integer p greater than 1 is called prime if its only positive divisors are 1 and p
- If a positive integer greater than 1 is not prime, then it is called composite
- Ex:
  - $2, 3, 5, 7, 11, 13$ are prime
  - $4, 6, 8, 9, 10$ are composite

Relatively Prime

- Definition: We say that integers a and b are relatively prime if $\mathrm{GCD}(a, b) = 1$
- Lemma 2: If a, b, and c are positive integers such that $\mathrm{GCD}(a, b) = 1$ and $a \mid bc$, then $a \mid c$

Relatively Prime

- Definition: We say that integers a and b are relatively prime if $\text{GCD}(a, b) = 1$

- Lemma 2: If a, b, and c are positive integers such that $\text{GCD}(a, b) = 1$ and $a \mid bc$, then $a \mid c$

- Proof: Let a, b, and c be arbitrary positive integers such that $\text{GCD}(a, b) = 1$ and $a \mid bc$. Since $\text{GCD}(a, b) = 1$, it follows from Theorem 2 that there exists integers x and y such that

$$ax + by = 1$$

Multiplying both sides by c,

$$cax + cby = c$$

Relatively Prime

- Definition: We say that integers a and b are relatively prime if $\text{GCD}(a, b) = 1$

- Lemma 2: If a, b, and c are positive integers such that $\text{GCD}(a, b) = 1$ and $a \mid bc$, then $a \mid c$

- Proof: By definition of divisibility, it follows from $a \mid bc$, that there exists an integer k such that $bc = ak$. Hence,

$$cax + aky = c$$

$$a(cx + ky) = c \ .$$

By definition of divisibility, $a \mid c$. ■

Relatively Prime

- Definition: We say that integers a and b are relatively prime if $\mathrm{GCD}(a, b) = 1$

- Corollary 2: If $d = \mathrm{GCD}(a, b)$, then a/d and b/d are relatively prime.

Relatively Prime

- Definition: We say that integers a and b are relatively prime if $\text{GCD}(a, b) = 1$

- Corollary 2: If $d = \text{GCD}(a, b)$, then a/d and b/d are relatively prime.

- Proof: From Theorem 2, there exists integers x and y such that

$$ax + by = d$$

Then

$$\frac{a}{d}x + \frac{b}{d}y = 1$$

It follows from Corollary 1 that $\text{GCD}(a/d, b/d) \mid 1$, and therefore, $\text{GCD}(a/d, b/d) = 1$.

■

Application to Modular Arithmetic

- Proposition 1: Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $\mathrm{GCD}(c, m) = 1$, then $a \equiv b \pmod{m}$

Application to Modular Arithmetic

- Proposition 1: Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $\text{GCD}(c, m) = 1$, then $a \equiv b \pmod{m}$

- Proof: Let m be an arbitrary positive integer and let a, b, and c be arbitrary integers. From Theorem 3 in the lecture notes of Chapter 4.1, $ac \equiv bc \pmod{m}$ implies that $m \mid ac - bc = c(a - b)$. Since $\text{GCD}(c, m) = 1$, it follows from Lemma 2 that $m \mid a - b$. Therefore, from Theorem 3 in the lecture notes of Chapter 4.1, $m \mid a - b$ implies that $a \equiv b \pmod{m}$. ■

Fundamental Theorem of Arithmetic

- Theorem 3: (Fundamental Theorem of Arithmetic) Every positive integer greater than 1 can be written as a product of primes. This is unique, up to the order of factors.

Fundamental Theorem of Arithmetic

- Theorem 3: (Fundamental Theorem of Arithmetic) Every positive integer greater than 1 can be written as a product of primes. This is unique, up to the order of factors.
- Ex:
  - $104 = 2^3 \cdot 13$
  - $105 = 3 \cdot 5 \cdot 7$
  - $308 = 2^2 \cdot 7 \cdot 11$

Fundamental Theorem of Arithmetic

- Theorem 3: (Fundamental Theorem of Arithmetic) Every positive integer greater than 1 can be written as a product of primes. This is unique, up to the order of factors.
- Ex:
  - $104 = 2^3 \cdot 13$
  - $105 = 3 \cdot 5 \cdot 7$
  - $308 = 2^2 \cdot 7 \cdot 11$
- To prove this, we need the following lemma
- Lemma 3: (Euclid's Lemma) Let $a_1 a_2 \ldots a_n \in \mathbb{Z}$ and p be a prime. If $p \mid a_1 a_2 \ldots a_n$, then $p \mid a_i$ for some $i = 1, 2, \ldots, n$

Euclid's Lemma

- Lemma 3: (Euclid's Lemma) Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ and p be a prime. If $p \mid a_1 a_2 \ldots a_n$, then $p \mid a_i$ for some $i = 1, 2, \ldots, n$

Euclid's Lemma

- Lemma 3: (Euclid's Lemma) Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ and p be a prime. If $p \mid a_1 a_2 \ldots a_n$, then $p \mid a_i$ for some $i = 1, 2, \ldots, n$

- Proof: Let n and $a_1, a_2, \ldots, a_n$ be an arbitrary positive integers and p be an arbitrary prime.
  Inductive Hypothesis: Assume inductively that for all integers k, such that $0 < k < n$, $P(k)$ is true. In other words, If $p \mid a_1 a_2 \ldots a_k$, then $p \mid a_i$ for some $i = 1, 2, \ldots, k$
  Base Case: Assume $n = 1$.
  Trivially, $p \mid a_1$ implies that $p \mid a_i$ for $i = 1$.

Euclid's Lemma

- Lemma 3: (Euclid's Lemma) Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ and p be a prime. If $p \mid a_1 a_2 \ldots a_n$, then $p \mid a_i$ for some $i = 1, 2, \ldots, n$

- Proof:
  Inductive Case: Assume $n > 1$.

$$p \mid a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_{n-1}) a_n$$

  If $p \mid a_n$, then we are done. Otherwise, $p \nmid a_n$ and $\mathrm{GCD}(p, a_n) = 1$. It follows from Lemma 2 that $p \mid a_1 a_2 \ldots a_{n-1}$. And from our inductive hypothesis, since $0 < n - 1 < n$, we know that $p \mid a_i$ for some $i = 1, 2, \ldots, n - 1$.

■

Fundamental Theorem of Arithmetic

- Theorem 3: (Fundamental Theorem of Arithmetic) Every positive integer greater than 1 can be written as a product of primes. This is unique, up to the order of factors.

Fundamental Theorem of Arithmetic

- Theorem 3: (Fundamental Theorem of Arithmetic) Every positive integer greater than 1 can be written as a product of primes. This is unique, up to the order of factors.

- Proof: Let n be an arbitrary positive integer greater than 1. We will first show that n can be written as a product of primes.
  Inductive Hypothesis: Assume inductively that for all integers k, such that $1 < k < n$, $P(k)$ is true. In other words, k can be written as a product of primes.
  Base Case: Assume $n = 2$.
  Trivially, 2 is prime and can be written as itself.

Fundamental Theorem of Arithmetic

- Theorem 3: (Fundamental Theorem of Arithmetic) Every positive integer greater than 1 can be written as a product of primes. This is unique, up to the order of factors.

- Proof:
  Inductive Case: Assume $n > 2$.
  If n is prime, then trivially n can written as itself.
  Otherwise, n is composite and $n = ab$ for some integers a and b such that $1 < a < n$ and $1 < b < n$.

Fundamental Theorem of Arithmetic

- Theorem 3: (Fundamental Theorem of Arithmetic) Every positive integer greater than 1 can be written as a product of primes. This is unique, up to the order of factors.

- Proof:
  Inductive Case: Assume $n > 1$.
  From our inductive hypothesis, since $1 < a < n$ and $1 < b < n$, a and b can both be written as a product of primes. Let $a = p_1 p_2 \dots p_r$ and $b = q_1 q_2 \dots q_s$ for some positive integers r and s and primes $p_1, p_2, \dots, p_r$ and $q_1, q_2, \dots, q_s$. Then

$$n = ab = (p_1 p_2 \dots p_r)(q_1 q_2 \dots q_s)$$

  is a product of primes.

Fundamental Theorem of Arithmetic

- Theorem 3: (Fundamental Theorem of Arithmetic) Every positive integer greater than 1 can be written as a product of primes. This is unique, up to the order of factors.

- Proof: Next, we will show that the factorization is unique. Assume for the sake of contradiction that there exists a positive integer that does not have a unique factorization of primes. From the Well-Ordering Principle, there exists a least element n that satisfies this assumption. For some positive integers r and s, let $p_1 p_2 \ldots p_r$ and $q_1 q_2 \ldots q_s$ be some primes, such that

$$n = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$$

Fundamental Theorem of Arithmetic

- Theorem 3: (Fundamental Theorem of Arithmetic) Every positive integer greater than 1 can be written as a product of primes. This is unique, up to the order of factors.

- Proof:
  By definition of divisibility, $p_1 \mid q_1 q_2 \ldots q_s$. It follows from Lemma 3 that $p_1 \mid q_i$ for some $i = 1, 2, \ldots, s$. Without loss of generality, assume that $p_1 \mid q_1$. Since p_1 and q_1 are both prime, it must be that $p_1 = q_1$. Hence, we can cancel them out

  $$p_2 \ldots p_r = q_2 \ldots q_s$$

  We now have two distinct prime factorizations of some integer strictly smaller than n, a contradiction since we assumed that n was the least integer that does not have a unique factorization of primes. ■

Trial Division

- Theorem 4: If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$

Trial Division

- Theorem 4: If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$

- Proof: Let n be an arbitrary composite integer.
  By defintion of a composite integer, n has some factor a such that $1 < a < n$. By definition of a factor,

$$n = ab$$

  where b is a positive integer greater than 1. We will first show that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Trial Division

- Theorem 4: If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$

- Proof:
  Assume for the sake of contradiction that $a > \sqrt{n}$ and $b > \sqrt{n}$. Then,
  $$ab > \sqrt{n} \cdot \sqrt{n} = n$$
  A contradiction, since $n = ab$. Thus, $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Trial Division

- Theorem 4: If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$

- Proof:
  Without loss of generality, assume that $a \leq \sqrt{n}$. If a is prime, then we are done. Otherwise, using Theroem 3, a can be written as a product of primes, and consequently, n has a prime divisor less than or equal to $\sqrt{n}$. ■

Trial Division

- Theorem 4: If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$

- It follows from Theorem 4 that an integer n is prime if it is not divisible by any prime less than or equal to $\sqrt{n}$
- Leads to a brute-force algorithm, known as trial division
  - Divide n by all primes not exceeding $\sqrt{n}$
  - n is prime if it is not divisible by any of these primes (and composite otherwise)

Trial Division

- Ex: Is 101 prime?
  - $\sqrt{101} \approx 10.05$
  - Primes less than or equal to $\sqrt{101}$ are: 2, 3, 5, and 7
  - $2 \nmid 101$ since $101/2 = 50.5$
  - $3 \nmid 101$ since $101/3 \approx 33.3$
  - $5 \nmid 101$ since $101/5 = 20.2$
  - $7 \nmid 101$ since $101/7 \approx 14.4$
  - Therefore, 101 is prime

Finding the Prime Factorization

- From Theorem 4, n has a prime factor less than or equal to $\sqrt{n}$.

1. Staring from the smallest prime 2, find whether n has a prime factor $\leq \sqrt{n}$.
2. If a prime factor p is found, then continue factoring n/p
3. Otherwise, n is prime and its factorization is itself

Finding the Prime Factorization

1. Staring from the smallest prime 2, find whether n has a prime factor $\leq \sqrt{n}$.
2. If a prime factor p is found, then continue factoring n/p
3. Otherwise, n is prime and its factorization is itself

- Ex: Find prime factorization of 7007
  - $7 \mid 7007$ and $7007/7 = 1001$
  - $7 \mid 1001$ and $1001/7 = 143$
  - $11 \mid 143$ and $143/11 = 13$
  - 13 is prime
  - Therefore, $7007 = 7 \cdot 7 \cdot 11 \cdot 13$

Applications of Factoring and Primes

- Factoring and primality testing is important to cryptography
  - RSA encryption is based on the fact that multiplying is much easier than factoring
- Currently, there is no polynomial-time algorithm for factoring integers

Applications of Factoring and Primes

- The greatest common divisor and least common multiple can be found using prime factorizations

- 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
- Denoted $\text{LCM}(a, b)$

Applications of Factoring and Primes

- The greatest common divisor and least common multiple can be found using prime factorizations

- Let $a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$
  - Each exponent is a non-negative integer
  - All primes occuring in the prime factorization of either a or b are included in both factorizations (with a 0 exponent, if necessary)

$$\text{GCD}(a, b) = p_1^{\text{MIN}(a_1, b_1)} p_2^{\text{MIN}(a_2, b_2)} \ldots p_n^{\text{MIN}(a_n, b_n)}$$

$$\text{LCM}(a, b) = p_1^{\text{MAX}(a_1, b_1)} p_2^{\text{MAX}(a_2, b_2)} \ldots p_n^{\text{MAX}(a_n, b_n)}$$

Euclid's Theorem

- Theorem 5: (Euclid's Theorem) There are infinitely many primes

Euclid's Theorem

- Theorem 5: (Euclid's Theorem) There are infinitely many primes

- Proof: Consider any arbitrary finite list of prime numbers $p_1, p_2, \ldots, p_n$. We will show that there exists at least one additional prime number not included in this list. Let $P = p_1 p_2 \ldots p_n$ and let $q = P + 1$.
  If q is prime, then we have found an additonal prime not in the list.

Euclid's Theorem

- Theorem 5: (Euclid's Theorem) There are infinitely many primes

- Proof:
  Otherwise, q is composite and there exists some prime factor p such that $p \mid q$. If p is on our list of primes, then $p \mid P$. It follows from Theorem 1 (statement 1.) in the lecture notes of Chapter 4.1, that if $p \mid q$ and $p \mid P$ then $p \mid q - P = 1$. Since no prime numbers divides 1, p cannot be on our list of primes. Therefore, at least one more prime number exists that is not in the list. ■

Prime Number Theorem

- Let $\pi(x)$ be the number of prime numbers less than x
- Theorem 6: (Prime Number Theorem) The ratio of $\pi(x)$ and $x/\ln x$ approaches 1 as x grows without bounds.

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$$

- It follows that a "good" approximation of $\pi(x)$ is

$$\pi(x) \approx \frac{x}{\ln x}$$

- "Good" approximation means that the relative error of the approximation approaches 0 as x increases without bound