Chap. 4.3 - Greatest Common Divisor

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

Examples:
\[
gcd(12, 30) = 6 \\
gcd(12, -30) = 6 \\
gcd(16, 9) = 1 \\
gcd(16, 36) = 4 \\
gcd(7, 63) = 7 \\
gcd(7, 0) = 7
\]

**Greatest Common Divisor**

**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:** Are 10, 17 and 21 pairwise relatively prime?

**Example:** Are 10, 19, and 24 pairwise relatively prime?
What numbers can be created using 12 and 30 as building blocks?

- That means $12s + 30t$
- Can you create any positive integer using this formula?

Can you create 6 using $12s + 30t$?

$6 = 12s + 30t$

Can you create any positive integer using this formula?

Can you create 4?

$-4 = 12x + 30y$

$= 6(2x + 5y)$

NO, must be a multiple of 6

Can you create 6 using $12s + 30t$?

$6 = 12s + 30t$

$= 12(3) + 30(-1) = 36 - 30 = 6$, yes!

Can you create any multiple of 6 using 12 and 30?

Yes

$12(3m) + 30(-m) = 6m$

Can you create any number using 16 and 9 as building blocks?

$16s + 9t$

To create any number $m$:

$16(4) + 9(-7) = 64 - 63 = 1$

Yes, can create any number with 16 and 9

To create any number $m$:

$16(4m) + 9(-7m) = m$

Bézout showed back in 18th century

gcds as Linear Combinations

Étienne Bézout (1730-1783)

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

(proof in exercises of Section 5.2)

Idea:

Definition: If $a$ and $b$ are positive integers, then integers $s$ and $t$ such that $\gcd(a,b) = sa + tb$ are called Bézout coefficients of $a$ and $b$. The equation $\gcd(a,b) = sa + tb$ is called Bézout’s identity.
Euclidean Algorithm

• The Euclidian algorithm is an efficient method for computing the greatest common divisor of two integers. It is based on the idea that \( \gcd(a, b) \) is equal to \( \gcd(a, c) \) when \( a > b \) and \( c \) is the remainder when \( a \) is divided by \( b \).

**Example:** Find \( \gcd(91, 287) \):
- \( 287 = 91 \cdot 3 + 14 \) \quad (\text{Divide } 287 \text{ by } 91)
- \( 91 = 14 \cdot 6 + 7 \) \quad (\text{Divide } 91 \text{ by } 14)
- \( 14 = 7 \cdot 2 + 0 \) \quad (\text{Divide } 14 \text{ by } 7)

Stopping condition

\[ \gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = 7 \]

Euclid

(325 B.C.E. – 265 B.C.E.)

Correctness of Euclidean Algorithm

**Lemma 1:** Let \( a = bq + r \), where \( a, b, q, \) and \( r \) are integers. Then \( \gcd(a, b) = \gcd(b, r) \).

**Proof:**
- Suppose that \( d \) divides both \( a \) and \( b \).
- Suppose that \( d \) divides both \( b \) and \( r \).
- Therefore, \( \gcd(a, b) = \gcd(b, r) \).

Euclidean Algorithm

• The Euclidean algorithm expressed in pseudocode is:

```plaintext
procedure gcd(a, b: positive integers)
    x := a
    y := b
    while y \( \neq 0 \)
        \( r := x \mod y \)
        x := y
        y := r
    return x \{ \gcd(a, b) \text{ is } x \}
```

Correctness of Euclidean Algorithm

• Suppose that \( a \) and \( b \) are positive integers with \( a \geq b \). Let \( r_0 = a \) and \( r_1 = b \). Successive applications of the division algorithm yields:

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

• Eventually, a remainder of zero occurs in the sequence of terms: \( a = r_0 > r_1 > r_2 > \cdots \geq 0 \). The sequence can’t contain more than \( a \) terms.
Finding gcds as Linear Combinations

**Example:** Express \(\text{gcd}(252, 198) = 18\) as a linear combination of 252 and 198.

**Solution:** First use the Euclidean algorithm to show \(\text{gcd}(252, 198) = 18\)

- Now working backwards, from iii and i above
- Substituting the 2\(^{nd}\) equation into the 1\(^{st}\) yields:
- Substituting \(54 = 252 - 1 \cdot 198\) (from )) yields:

  - This method illustrated above is a two pass method. It first uses the Euclidian algorithm to find the gcd and then works backwards to express the gcd as a linear combination of the original two integers.

Euclid’s algorithm

- It is smart!
- It is fast!
  - If \(a > b\), then finds gcd\((a,b)\) in \(5 \log_{10} b\) steps

What are the worse numbers to try?

- How about \(\text{gcd}(99, 98)\)?
- How about \(\text{gcd}(99, 50)\)?
- How about \(\text{gcd}(89, 55)\)?

Recognize Fibonacci numbers?

Primes

**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:** 7 is prime only factors are 1 and 7, 9 is composite because it is divisible by 3. What about 1?
The Fundamental Theorem of Arithmetic

**Theorem:** 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:**
- \(105 = \)
- \(641 = \)
- \(221 = \)
- \(1024 = \)

---

**The Sieve of Erastosthenes**

Erastothenes (276-194 B.C.)

- The *Sieve of Erastosthenes* 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:

---

The Sieve of Erastosthenes

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

To see this, note that if \(n = ab\), then \(a \leq \sqrt{n}\) or \(b \leq \sqrt{n}\).

**Trial division**, a very inefficient method of determining if a number \(n\) is prime, is to try every integer \(i \leq \sqrt{n}\) and see if \(n\) is divisible by \(i\).

In previous example, why did we use only 2, 3, 5 and 7?
Infinitude of Primes

Euclid
(325 B.C.E. – 265 B.C.E.)

Theorem: There are infinitely many primes. (Euclid)

Proof: Assume finitely many primes: \( p_1, p_2, \ldots, p_n \)
- Let \( q = p_1 p_2 \cdots p_n + 1 \)
- Either \( q \) is prime or by the fundamental theorem of arithmetic it is a product of primes.
  - But none of the primes \( p_j \) divides \( q \) since if \( p_j | q \), then \( p_j \) divides \( q - p_1 p_2 \cdots p_n = 1 \).
  - Hence, there is a prime not on the list \( p_1, p_2, \ldots, p_n \). It is either \( q \), or if \( q \) is composite, it is a prime factor of \( q \).
This contradicts the assumption that \( p_1, p_2, \ldots, p_n \) are all the primes.
- Consequently, there are infinitely many primes.

Mersenne Primes

Marin Mersenne
(1588-1648)

Definition: Prime numbers of the form \( 2^p - 1 \), where \( p \) is prime, are called Mersenne primes.
- \( 2^2 - 1 = 3, 2^3 - 1 = 7, 2^5 - 1 = 31, \) and \( 2^7 - 1 = 127 \) are Mersenne primes.
- \( 2^{11} - 1 = 2047 \) is not a Mersenne prime since \( 2047 = 23 \cdot 89 \).
- There is an efficient test for determining if \( 2^p - 1 \) is prime.
- The largest known prime numbers are Mersenne primes.
- As of mid 2011, 47 Mersenne primes were known, the largest is \( 2^{43,112,609} - 1 \), which has nearly 13 million decimal digits.
- The Great Internet Mersenne Prime Search (GIMPS) is a distributed computing project to search for new Mersenne Primes.

http://www.mersenne.org/

Distribution of Primes

- Mathematicians have been interested in the distribution of prime numbers among the positive integers. In the nineteenth century, the prime number theorem was proved which gives an asymptotic estimate for the number of primes not exceeding \( x \).

Prime Number Theorem: The ratio of the number of primes not exceeding \( x \) and \( x/\ln x \) approaches 1 as \( x \) grows without bound. (\( \ln x \) is the natural logarithm of \( x \))
  - The theorem tells us that the number of primes not exceeding \( x \), can be approximated by \( x/\ln x \).
  - The odds that a randomly selected positive integer less than \( n \) is prime are approximately \( (n/\ln n)/n = 1/\ln n \).

Generating Primes

- Finding large primes with hundreds of digits is important in cryptography.
- There is no simple function \( f(n) \) such that \( f(n) \) is prime for all positive integers \( n \).
- Consider
  - \( f(n) = n^2 - n + 41 \) is prime for all integers \( 1, 2, \ldots, 40 \).
  - But \( f(41) = 41^2 \) is not prime.
- Fortunately, we can generate large integers which are almost certainly primes. See Chapter 7.
Conjectures about Primes
Many conjectures about them are unresolved, including:

- **Goldbach’s Conjecture.** Every even integer \( n, n > 2 \), is the sum of two primes. It has been verified by computer for all positive even integers up to \( 1.6 \cdot 10^{18} \). The conjecture is believed to be true by most mathematicians.

- There are infinitely many primes of the form \( n^2 + 1 \), where \( n \) is a positive integer. But it has been shown that there are infinitely many primes of the form \( n^2 + 1 \), where \( n \) is a positive integer or the product of at most two primes.

- **The Twin Prime Conjecture:** The twin prime conjecture is that there are infinitely many pairs of twin primes. Twin primes are pairs of primes that differ by 2. Examples are 3 and 5, 5 and 7, 11 and 13, etc. The current world’s record for twin primes (as of mid 2011) consists of numbers 65,516,468,355·23 \( \pm 1 \), which have 100,355 decimal digits.
LCM and GCD relation

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

**Example:** \( \gcd(20, 15) \cdot \text{lcm}(20, 15) \)

**Proof:**

Consequences of Bézout’s Theorem

**Lemma 2:** If \( a, b, \) and \( c \) are positive integers such that \( \gcd(a, b) = 1 \) and \( a \mid bc \), then \( a \mid c \).

**Proof:** Assume \( \gcd(a, b) = 1 \) and \( a \mid bc \).
- Since \( \gcd(a, b) = 1 \), by Bézout’s Theorem there are integers \( s \) and \( t \) such that \( sa + tb = 1 \).

**Lemma 3:** If \( p \) is prime and \( p \mid a_1 a_2 \cdots a_n \), then \( p \mid a_i \) for some \( i \).

*Proof uses mathematical induction; see Exercise 64 of Section 5.1*

- Lemma 3 is crucial in the proof of the uniqueness of prime factorizations.

Uniqueness of Prime Factorization

- We will prove that a prime factorization of a positive integer where the primes are in nondecreasing order is unique. (This is part of the fundamental theorem of arithmetic. The other part, which asserts that every positive integer has a prime factorization into primes, will be proved in Section 5.2.)

**Proof:** (by contradiction) Suppose that the positive integer \( n \) can be written as a product of primes in two distinct ways:
\[ n = p_1 p_2 \cdots p_s \text{ and } n = q_1 q_2 \cdots q_r \]
- Remove all common primes from the factorizations to get
\[ p_i p_2 \cdots p_s = q_j q_2 \cdots q_r \]
- By Lemma 3, it follows that \( p_i \mid q_j \), for some \( k \), contradicting the assumption that \( p_i \) and \( q_j \) are distinct primes.

- Hence, there can be at most one factorization of \( n \) into primes in nondecreasing order.

Dividing Congruences by an Integer

- Dividing both sides of a valid congruence by an integer does not always produce a valid congruence (see Section 4.1).

- But dividing by an integer relatively prime to the modulus does produce a valid congruence:

**Theorem 7:** Let \( m \) be a positive integer and let \( a, b, \) and \( c \) be integers. If \( ac \equiv bc \mod m \) and \( \gcd(c, m) = 1 \), then \( a \equiv b \mod m \).

**Proof:**