11.1: Divisibility Properties of Integers

Prime Numbers and Composites

Definition: If p is an integer greater than 1, then p is a **prime number** if the only divisors of p are 1 and p.

Definition: A positive integer greater than 1 that is not a prime number is called **composite**.

In other words, a composite number is a positive integer that has at least one positive divisor other than one or itself.

So, if $n > 0$ is an integer and $\exists a, b \in \mathbb{Z}$, $1 < a, b < n$ such that $n = a \times b$, then n is a composite number.

Sieve of Eratosthenes and Interesting Facts about Primes

- There are no efficient algorithms known that will determine whether a given integer is prime or find its prime factors.
- The above is used in many of the current cryptosystems.
- There is no known procedure that will generate prime numbers.
- **Twin primes conjecture**: There are infinitely many prime pairs, that is, consecutive odd prime numbers, such as 5 and 7, or 41 and 43. No one so far has been able to prove or disprove it.
- **Goldbach's conjecture**: Every even integer greater than 2 can be expressed as the sum of two primes. No one so far has been able to prove or disprove it.

Sieve of Eratosthenes:

11.2 The Division Algorithm

Definition: Let a, b be non-zero integers. We say

$$b \text{ is } \textbf{divisible} \text{ by } a \text{ (or } a \text{ divides } b\text{)}$$

if there is an integer x such that $a \cdot x = b$.
And if this is the case we write $a \mid b$, otherwise we write $a \nmid b$.

Theorem 1. For all integers a, b, and c,

1. If $a \mid b$ and $a \mid c$, then $a \mid (xb + yc) \quad \forall x, y \in \mathbb{Z}$.
2. If $a \mid b$, then $a \mid (bc)$.
3. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Theorem 2. Let $a, b \in \mathbb{Z} - \{0\}$.

1. If $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$.
2. If $a \mid b$, then $|a| \leq |b|$.

Theorem (The Division Algorithm). Let a and b be integers with $a, b > 0$. There exist unique integers q and r such that $b = aq + r$ and $0 \leq r < a$.

Definition: $b = aq + r$ and $0 \leq r < a$

b is called the **dividend**.

a is called the **divisor**.

q is called the **quotient**.

r is called the **remainder**.

Theorem (The Division Algorithm, General Form). Let a and b be integers with a, b with $a \neq 0$. There exist unique integers q and r such that $b = aq + r$ and $0 \leq r < |a|$.

Example. Find the quotient and remainder if

1. $b = 27$, $a = 4$
2. $b = -27$, $a = -4$
3. $b = 27$, $a = -4$

Proof of the Division Algorithm.

The set of integers modulo n Let a relation R defined on $\mathbb{Z}$ by aRb if $a \equiv b \pmod{n}$. With the aid of the *Division Algorithm*, the equivalence class of an integer r in the set of $\mathbb{Z}_n$ is

$$[r] = \{ nq+r : q \in \mathbb{Z}\} = \{\cdots, -2n+r, -n+r, r, n+r, 2n+r, \cdots\}.$$

That is, $[r]$ consists of all those integers having a remainder of r when divided by n.

Remark:

A. $\mathbb{Z}_n = \{[0], [1], \cdots, [n-1]\}$.

B. Every equivalence class $[i]$ in $\mathbb{Z}_n$ is nonempty.

C. The equivalence classes $[0], [1], \cdots, [n-1]$ are pairwise disjoint, that is, $[i] \cap [j] = \emptyset$ for $i \neq j$.

D. $\mathbb{Z} = [0] \cup [1] \cup \cdots \cup [n-1]$.

E. Therefore, Z_n is a *partition* of $\mathbb{Z}$.

11.3 Greatest Common Divisor

Definition: Given two integers b and c at least one of which is not 0, we say a is the **greatest common divisor** of b and c if a is the greatest among all common divisors of b and c. The greatest common divisor of b and c is denoted by $\gcd(b, c)$ or simply (b, c).

Why do we require that "at least one of b and c be nonzero"?
Could we make sense of $\gcd(0, 0)$?

Find

1. $\gcd(24, 36)$
2. $\gcd(22, 35)$

Theorem 3. For any integers a and b, the followng properties hold:

1. $\gcd(a, b) = \gcd(b, a)$,
2. $\gcd(a, b) \geq 1$,
3. $\gcd(a, b) = \gcd(|a|, |b|)$,
4. $\gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1$,
5. $\gcd(a, b) = \gcd(a + nb, b)$, $\forall n \in \mathbb{Z}$.
   - Use the following lemma to prove 5.

     Lemma. If $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ for all integers m and n.

Definition. An integer n is called a **linear combination** of $x, y \in \mathbb{Z}$ if $\exists k, m \in \mathbb{Z}$ such that $mx + ky = n$.

- Is 1 a linear combination of 5 and 8?
- Is 7 a linear combination of 2 and 6?

Theorem 4. Let a and b be integers that are not both 0. Then $\gcd(a, b)$ is the least positive integer that is a linear combination of a and b.

Theorem 5. Let a and b be integers that are not both 0. Then $d = \gcd(a, b)$ if and only if d that positive integer which satisfies the following two conditions:

- d is a common divisor of a and b;
- if c is any common divisor of a and b, then $c \mid d$.