Section 3 - Divisibility

• **Definition:** If $n$ and $d$ are integers and $d \neq 0$, then $n$ is divisible by $d$ provided $n = d \cdot k$ for some integer $k$.

• Alternatively, we say:
  
  - $n$ is a multiple of $d$
  - $d$ is a factor of $n$
  - $d$ is a divisor of $n$
  - $d$ divides $n$ (denoted with $d \mid n$).
Properties of Divisibility

• **Divisors of 0:** If $k$ is a non-zero integer, then $k$ divides 0 since $0 = k \cdot 0$.

• **Positive Divisors of a Positive Number:**
  If $a$ and $b$ are positive integers and $a \mid b$, is $a \leq b$?
  Yes. Since $a \mid b$, $\exists k \in \mathbb{Z}$, such that $b = a \cdot k$.
  Moreover, $0 < k$, since $a$ and $b$ are, so $1 \leq k$.
  Thus: $a = a \cdot 1 \leq a \cdot k = b$.
  Therefore $a \leq b$.

• **Divisors of 1:** The only divisors of 1 are 1 and $-1$. 
Divisibility of Algebraic Terms

• Let $a$ and $b$ be integers.

• Does $3 \mid (3a + 3b)$?
  Yes, since $(3a + 3b) = 3(a + b)$ and $(a + b) \in \mathbb{Z}$.

• Does $5 \mid 10ab$?
  Yes again, since $10ab = 5(2ab)$ and $(2ab) \in \mathbb{Z}$.

• If $m \in \mathbb{Z}$ and $m \mid (a + b)$, does $m \mid a$ and $m \mid b$?
  No. $2 \mid 8$ but $2 \nmid 5$ and $2 \nmid 3$. 
Divisibility and Non-divisibility

• There is another way to test for divisibility: If \( d \mid n \), there is integer \( k \) with \( n = dk \), then \( k = (n/d) \). So, if \( (n/d) \) is an integer, then \( d \mid n \).

• This leads to an easy way to test for non-divisibility: If \( (n/d) \) is not an integer, then \( d \) cannot divide \( n \).

• Examples:

\[
3 \mid 12 \text{ since } 12/3 = 4 \in \mathbb{Z}.
\]
\[
5 \nmid 12 \text{ since } 12/5 = 2.4 \notin \mathbb{Z}.
\]
Proving Properties of Divisibility

- **Theorem:** *Transitivity of Divisibility*
  For all $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $b \mid c$, then $a \mid c$.

- **Proof:** Let $a$, $b$, and $c$ be integers, and assume $a \mid b$ and $b \mid c$. Thus there exist $m, n \in \mathbb{Z}$ with $b = ma$ and $c = nb$.

  Now, $c = nb = n(ma) = (nm)a$. Since $m, n \in \mathbb{Z}$, we have $nm \in \mathbb{Z}$, therefore $a \mid c$. QED

- **Example:** $3 \mid 9$ and $9 \mid 909$, therefore $3 \mid 909$. 
Divisibility by a Prime

• **Theorem:** Every positive integer greater than 1 is divisible by a prime number.

• **Proof:** Let \( n \in \mathbb{Z} \) with \( n > 1 \). Then either \( n \) is prime or composite. If \( n \) is prime, it is divisible by itself, and we are done.

   Now, assume \( n \) is composite. Thus there are integers (greater than 1) \( a \) and \( b \), such that \( n = ab \). If \( a \) is prime, we are done. If not, factor \( a \), .... Will we eventually get to a prime factor?
Standard Factored Form

• **Definition:** Given any integer \( n > 1 \), the *standard factored form* of \( n \) is an expression of the form:
  \[ n = (p_1)^{e_1} \cdot (p_2)^{e_2} \cdot (p_3)^{e_3} \cdots (p_k)^{e_k}, \]
  where \( k \) is a positive integer; \( p_1, p_2, \ldots, p_k \) are prime numbers with \( p_1 < p_2 < \ldots < p_k \); and \( e_1, e_2, \ldots, e_k \) are positive integers.

• **Example:** \[ 3300 = 33 \cdot 100 = 3 \cdot 11 \cdot 10^2 = 2^2 \cdot 3 \cdot 5^2 \cdot 11. \]
Unique Factorization Theorem

- **Theorem:** Given any integer $n > 1$, there exist positive integer $k$; prime numbers $p_1, p_2, ..., p_k$; and positive integers $e_1, e_2, ..., e_k$, with

$$n = (p_1)^{e_1} \cdot (p_2)^{e_2} \cdot (p_3)^{e_3} \cdots (p_k)^{e_k},$$

and any other expression of $n$ as a product of prime numbers is identical to this except, perhaps, for the order in which the factors appear.

- This is also referred to as the *Fundamental Theorem of Arithmetic*. 
Fundamental Theorem of Arithmetic

• Theorem: Every positive integer greater than 1 has a unique factorization as the product of primes.

• Proof: (outline)

  1. Apply the previous theorem to each composite factor encountered.

  2. Sort the final listing to get the prime factors in increasing (decreasing?) numeric order.

  3. Rewrite using exponents.