Math 299 **Lecture 25: Divisibility of Integers and Infinity of Primes**

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

b is **divisible** by a (or a divides b)

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 $a \nmid b$.

Exercise 1.

1. Prove that if $ab \mid ac$, then $b \mid c$, where a, b, $c \in \mathbb{Z}$, and $a \neq 0$.

2. Using the notion of *divisibility*, give a formal definition of an *even* and an *odd* integer.

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

1. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
2. If $a \mid b$, then $a \mid (bc)$.
3. If $a \mid b$ and $b \mid c$, then $a \mid c$.

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

Definition: $a = qd + r$ and $0 \leq r < d$

a is called the **dividend**.

d is called the **divisor**.

q is called the **quotient**.

r is called the **remainder**.

Ex. Find the quotient and remainder if

(1) $a = 27$, $d = 4$

(2) $a = -27$, $d = 4$

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 the prime factorization of an integer.
- 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:

Infinity of Primes

Theorem: There are infinitely many prime numbers.

Proof:

The Fundamental Theorem of Arithmetic Fundamental Theorem of Arithmetic: Every positive integer greater than one can be written uniquely as a product of primes, where the prime factors are written in nondecreasing order.

Proof:

Theorem. If n is a composite integer, then n has a factor less than or equal to $\sqrt{n}$.

In fact, we can similarly prove that

Corollary. If n is a composite integer, then n has at least one prime factor less than or equal to $\sqrt{n}$.

EX. Show that 113 is a prime.