Math 299 **Lecture 10: Sections 4.1 and 4.2**
Divisibility of Integers and Congruence of Integers

Definition: Let a, b be non-zero integers. We say b is **divisible** by a (or a divides b, or b is a multiple of a) 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 $a \mid c$.

Exercises

1. If $a, b \in \mathbb{Z}$ and $a \geq 2$, then $a \nmid b$ or $a \nmid b+1$.

2. Let $x \in \mathbb{Z}$. If 3 doesn't divide $x^2 - 1$, then $3|x$.

3. Let $n \in \mathbb{Z}$. Then $3|(2n^2 + 1)$ if and only if $3 \nmid n$.

Remainder of division. Modulo operation.

1. Definition : x is divisible by y if $\exists k \in \mathbb{Z}$ such that $x = k \cdot y$.

   If x is not divisible by 3, what are our options? For $k \in \mathbb{Z}$

   (1) $x = 3k + 1$.
   (2) $x = 3k + 2$.

   Can we generalize this? What are the possibilities for x if x is not divisible by r?

Congruence modulo n

Definition : For integers x, y and $n \geq 2$, we say that x is **congruent** to y **modulo** n, written $x \equiv y\,(mod\,n)$ if $n \mid (x - y)$.

Example

- $1142 \equiv x \ (mod\ 5)$. Find x for $x \in \{x \in \mathbb{Z} | 10 \leq x \leq 15\}$.

Each integer x can be expressed in exactly one of the following forms:

$$x = 2k \quad \text{or} \quad x = 2k + 1, \quad \text{for some } k \in \mathbb{Z}.$$

Thus,

$$x \equiv 0(mod\,2) \quad \text{or} \quad x \equiv 1(mod\,2)$$

and only one of the above is possible.

How can we generalize this if the divisor is 5?

How about if the divisor is 8?

Theorem 1 . Given integers a, b, c, d and m, if $a \equiv b(mod\, m)$ and $c \equiv d(mod\, m)$, then

(1) $a + c \equiv b + d(mod\, m)$.

(2) $a \cdot c \equiv b \cdot d(mod\, m)$.

Theorem 2. If n is a square number (perfect square), then $n \equiv 0(mod\, 4)$ or $n \equiv 1(mod\, 4)$.

Exercises

1. For $n \in \mathbb{Z}$, prove that $9n^2 + 3n - 2$ is even.

2. Prove $n^2 - 2$ is not divisible by 3 if n is an integer.

3. If n is an integer not divisible by 3, then $n^2 = 1$ (mod 3).

4. Prove that if n is any integer which is not divisible by 5, then n^2 leaves a remainder of 1 or 4 when it is divided by 5.

5. What cases should we consider if we would like to prove that if n is a positive integer then $n^7 - n$ is divisible by 7?