Math 55 Lecture 6 §4.1, 4.2 (4.3)

§4.1 Intro to number theory: integers & division

Def: If a and b are integers with $a \neq 0$, we say that a **divides** b if

Ex:

Theorem 1: Let a, b, c be integers. Then
(i) If $a|b$ and $b|c$ then $a|c$
(ii) If $a|b$ and $a|c$ then $a|mb+nc$ whenever m and n are integers.

Pf:

Division Algorithm: Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, s.t.

Def: Above, d is the , a is the , q is the , r is the

Notation:

Ex:

Ex: Evaluate these quantities:

(a)

(b)

(c)

(d)

Modular arithmetic:

Def: If $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, and $m \in \mathbb{Z}^+$ then a is congruent to b modulo m if

Notation:

Ex:

Thm 2: Let $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$. Then $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$.

Pf:

Thm 3: Let $m \in \mathbb{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a+c \equiv b+d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Pf:

Ex:

Ex:

Ex: Show that if n is an integer, then $n^2 \equiv 0$ or $1 \pmod 4$.

Pf:

Ex: Show that if m is pos. integer of the form $4k+3$ for some non-neg integer k, then m is not the sum of the squares of two integers.

Pf:

§4.2 Representations of integers

In everyday life we use decimal notation, eg:

Theorem: Let $b \in \mathbb{Z}^+$, $b > 1$. If $n \in \mathbb{Z}^+$, it can be expressed uniquely in form

This representation is called
Notation.

Ex:

Def: The base 2 representation of n is its
The base 10 " " "
The base 16 " " "

For base 16, use 16 different "digits":

Ex: What is hexadecimal expansion of

Given an integer n, how do we write its base b expansion?

Algorithm:

Ex: What is base 7 expansion of

§4.3 Primes.

Def: A positive integer p greater than 1 is **prime** if

Fundamental Theorem of Arithmetic (proved later)
Every positive integer greater than 1 can be written uniquely as a

Ex:

Theorem: If n is composite, then n has a prime divisor

Proof:

Ex: