10.09

2.4
Sequences and Summations (continued)

10th formula: $\sum_{k=0}^{n} a + kd = \frac{[a+(a+nd)](n+1)}{2}$
S = ((first term + last term) * number of terms) / 2
for progressions like S = 1 + 3 + 5 + 7

4.1
Divisibility and Modular Arithmetic

Definition
Let a and b be integers and $a \neq 0$. We say a divides b if there is an integer c s.t. $b = ac$, or equivalently, if $\frac{b}{a}$ is an integer.
If a divides b, we say a is a factor or divisor of b, and b is a multiple of a. IF a divides b, we write $a|b$.
If a does not divide b, we write a X b.

Example
$3|9$ since $9 = 3 * 3$
$\frac{9}{3} = 3$ is an integer
3 X 7 since $\frac{7}{3}$ is not an integer

Any integer divides 0. $a \neq 0$
$0 = a * 0$ for any a
$\frac{0}{a} = 0$

Theorem
Let a, b, c be integers, $a \neq 0$.
1. If $a|b$ and $a|c$, then $a|(b + c)$
2. If $a|b$, then $a|bc$ for all integers c
3. If $a|b$ and $b|c$, then $a|c$

Theorem
Suppose a, b, c are integers, $a \neq 0$, Also, $a|b$ and $a|c$. Then, $a|(mb + nc)$, where m and n are integers.

Theorem: Division Algorithm
Suppose a and d are integers, $d > 0$. Then there are unique integers q and r s.t. $a = dq + r$, where $0 \leq r \leq d$
$a = d * q + r$
a is the dividend
d is the divisor
q is the quotient
r is the remainder

Example
Divide 13 by 3
$13 = 3 * 4 + 1$

Definition

q = a div d
r = a mod d

Example
$13 = 3 * 4 + 1$
So 13 div 3 = 4, and 13 mod 3 = 1

Definition Suppose a, b, m are integers, $m > 0$. a is congruent to b modulo m if $m|(a-b)$. We write $a \equiv b$ (mod m) if a is congruent to b modulo. $a \equiv b$(mod m) is called a congruence, and m is its modulus.
If a is not congruent to b modulo m, we write $a/\equiv b$ (modulo) m.
$a \equiv b$ (mod m) $\Leftrightarrow m|(a-b)$

Theorem
Suppose a, b, m are integers $m > 0$. $a \equiv b$ (mod m) if and only if a mod m = b mod m

Theorem
Suppose a, b, m are integers, $m > 0$. a and b are congruent modulo m if and only if there is some integer k s.t. $a = b + km$
$b \equiv a$ (mod m) $\Leftrightarrow a \equiv b$ (mod m)

Proof
$a \equiv b$ (mod m) $\Rightarrow m|(a-b) \Rightarrow a - b = km \Rightarrow a = b + km.$

Theorem
Suppose a, b, c, d, m are integers, $m > 0$.
If $a \equiv b$ (mod m) and $c \equiv d$ (mod m), then $a + c \equiv b + d$ (mod m) and $a * c \equiv b * d$ (mod m)

Theorem
Suppose a, b, m are integers $m > 0$. Then (a + b) mod m = ((a mod m) + (b mod m)) mod m
$(a * b)$ mod m = ((a mod m) ∗ (b mod m)) mod m

$Z_m = \{0, 1, 2, 3, ..., m-1\}$
$Z_5 = \{0, 1, 2, 3, 4\}$
Define operations on Z_m as $a +_m b = (a + b)$ mod m
$a *_m b = (A * b)$ mod m

Example
$Z_5 = \{0, 1, 2, 3, 4\}$
$3 +_5 4 = (3 + 4)$ mod 5 = 7 mod 5 = 2
$3 +_5 4 = 2$
$3 *_5 2 = (3 * 2)$ mod 5 = 6 mod 5 = 1
$3 *_5 2 = 1$

$(a +_m b) +_m C = a +_m (b +_m C)$
$a +_m b = b +_m a$
$a *_m b = b *_m a$
$a +_m 0 = a$
$a *_m 1$ = a
a and (m - a) are additive inverses of each other

$a *_m (b +_m c)$
$= a *_m b + a *_m c$
$(a +_m b) *_m c$
$= a *_m c +_m b *_m c$

4.2
Integer Representations and Algorithms

Let b be an integer and $b > 1$. Any positive integer n can be written uniquely as $n = a_k b^k + a_{k-1} b^{k-1} + ... + a_1 b + a_0$
base b expansion of n

Example
$(123)_{10} = 1 * 10^2 + 2 * 10 + 3$
$(112)_3 = 1 * 3^2 + 1 * 3^1 + 2$
$(1001)_2 = 1 * 2^3 + 0 * 2^2 + 0 * 2^1 + 1$

base 2: binary
base 8: octal
base 10: decimal
base 16: hexadecimal

Example
Convert $(111)_{10}$ into base 5
Divide 111 by 5
111 = 5 * 22 + 1
22 = 5 * 4 + 2
4 = 5 * 0 + 4
the remainder column gives the digits from bottom (largest) to top
$(111)_{10} = (421)_5$

to convert a positive integer base 10 to any base b, use b as the divisor

convert from any base to an base: use base 10 as the middleman

converting powers of two
$2 \to 8$
$8 \to 2$
(read it in the textbook)

4.3
Primes/Greatest Common Divisors

Definition: suppose p is an integer and p ¿ 1. p is called a prime number if its only positive factors are 1 and p. A positive integer greater than 1 that is not a prime is called a composite number.
n is composite means $\exists a$ s.t. $a|n$ and $1 < a < n$
first couple of primes: 2,3,5,7,11,13,17,23,...

The Fundamental Theorem of Arithmetic

Every integer greater than 1 can be written uniquely as a prime or a product of two or more primes, where the primes are in a non-decreasing order (prime factorization)

Example
$36 = 2 * 2 * 3 * 3 = 2^2 + 3^2$
$16 = 2 * 2 * 2 * 2 = 2^4$
$7 = 7$

Definition
Suppose a and b are integers, not both 0. The largest integer d s.t. $d|a$ and $d|b$ is the greatest common divisor of a and b. We write d = gcd (a,b).

Definition
Integers a and b are relatively prime if their gcd is 1

Definition
$a_1, a_2, ..., a_n$ are pairwise relatively prime if gcd $(a_i, a_j) = 1$ for $1 \leq i < j \leq n$
For $i \neq j$ gcd $(a_i, a_j) = 1$
gcd (5, 1) = gcd (10,5)

Theorem
$a = p_1^{a_1} p_2^{a_2} ... p_n^{a_n}$
$b = p_1^{b_1} p_2^{b_2} ... p_n^{b_n}$
gcd $(a, b) = P_1^{min(a_1,b_1)} * P_2^{min(a_2,b_2)} * * * P_n^{min(a_n,b_n)}$

$a = 2^3 * 3^2 * 5^1$
$b = 2^2 * 3^3 * 5^1$
gcd $(360, 540) = 2^{min(3,2)} * 3^{min(2,3)} * 5min(1,1) = 2^2 * 3^2 * 5^1 = 4 * 9 * 5 = 180$
if only one number has the prime then just ignore it, because it autommatically would not be a factor of the other number

Definition
Suppose a and b are integers. The least common multiple is the smallest positive integer divisible by both a and b. We denote is as lcm (a, b).

Example
lcm (12, 18)
12, 42, 36, 48, ...
18, 36, 54, 72, ...
36 is the lcm

Theorem
$a = p_1^{a_1} p_2^{a_2} ... p_n^{a_n}$
$b = p_1^{b_1} p_2^{b_2} ... p_n^{b_n}$
lcm $(a, b) = P_1^{max(a_1,b_1)} * P_2^{max(a_2,b_2)} * * * P_n^{max(a_n,b_n)}$

Example
$a = 2^2 * 3^2$
$b = 2^2 * 3^3$

$lcm(72, 108) = 2^{max(3,2)} * 3^{max(2,3)} = 2^3 * 3^3 = 8 * 27 = 216$

Fact
$max(x, y) + min(x, y) = x + y$
$max(1, 2) + min(1, 2) = 2 + 1$
$max(1, 1) + min(1, 1) = 1 + 1$

Theorem
$(gcd(a, b))(lcm(a, b)) = ab$
$a = p_1^{a_1} p_2^{a_2} ... p_n^{a_n}$
$b = p_1^{b_1} p_2^{b_2} ... p_n^{b_n}$
$(gcd(a, b))(lcm(a, b)) = ... = P_1^{min(a_1,b_1)+max(a_1,b_1)} + ... + P_n^{min(a_n,b_n)+max(a_n,b_n)} = ... = ab$

Euclidean Algorithm
Lemma
Suppose $a = b * q + r$
Then $gcd(a, b) = gcd(b, r)$

Example
Find $gcd(120, 62)$
$120 = 62 * 1 + 58$
$62 = 58 * 1 + 4$
$58 = 4 * 14 + 2$
$4 = 2 * 2 + 0$
Last divisor is $gcd(120, 62)$
$gcd(120, 62) = 2$

Bezout's Theorem
Suppose a and b are positive integers, and $d = gcd(a, b)$. Then there exists integers s and t s.t $d = sa + tb$.
s and t are called the Bezout coefficients of a and b.
$gcd(120, 62) = 2$
2 = 58 - 4 * 14
4 = 62 - 58 * 1
2 = 58 - (62 - 58 * 1) * 15
2 = 15 * 58 - 14 * 62
58 = 120 - 62 * 1