MATH406 NOTES

CHAPTER 1: THE INTEGERS

1.1 Types of Number, Well-Ordering, Floors and Ceilings

1. Types of numbers and notation
2. Well-ordered sets
   - Def: A set of numbers is **well-ordered** if every **non-empty** subset has **a least element**
   - Axiom: Z^+ is well-ordered
3. Floors and Ceilings
   - for $x \in R$ and $n \in Z$, $\lfloor x \rfloor = n$ iff $n \leq x < n+1$
   - for $x \in R$ and $n \in Z$, $\lceil x \rceil = n$ iff $n-1 < x \leq n$

4. Countable and Uncountable Sets
   - Def: A set S is **countably infinite** if it can be placed in 1-1 correspondence with Z^+
   - Def: A set S is **countable** if it is either **finite** or **countably infinite**

1.2 Sums and Products

1. Notation
   (A) The sum: $\sum_{j=m}^{n} a_j = a_m + a_{m+1} + \cdots + a_n$
   (B) The product: $\prod_{j=m}^{n} a_j = a_m . a_{m+1} \dots a_n$
2. Some sums:
   (A) $\sum_{j=1}^{n} 1 = n$
   (B) $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$
   (C) $\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}$
   (D) $\sum_{j=0}^{n} r^j = \frac{r^{n+1}-1}{r-1}$
3. Some techniques:
   (A) Telescoping: Often partial fractions can help
   (B) Trimming: Change starting index from m to 1
   (C) Reindexing: Substitution

1.3 Induction

1. Weak Induction: Base case: We show $P(n_\circ)$ is true (plug it in and show!)
   Inductive step:
   I.H: Assume it works for k
   I.C: Show it works for k+1
2. Proof of Induction (using well-ordered)
3. Strong Induction:
   Inductive step:
   I.H: Assume it works for every k, where k <= n
   I.C: Show it works for n + 1
   Base case(s):
   Analyze based on I.S to find how many base cases we need
   Write down base cases (Note: Don't use any extra base case)

1.5 Divisibility

1. Definition: $a|b$ if $\exists c \in Z$ such that $a.c = b$ given $a, b \in Z$ and $a \neq 0$
2. Properties:
   (A) **Theorem: if $a|b$ and $b|c$, then $a|c$**
   (B) **Theorem: if $a|b$ and $a|c$, then for all $x, y \in Z$, we have $a|(bx+cy)$**

*Warning: Things that might appear true may not be!

3. The Division Algorithm:
   Theorem: Suppose $a, b \in Z$ with $b > 0$
   Then $\exists! r, q \in Z$ such that $a = bq + r$ with $0 \leq r < b$

   Proof: First prove existence by well-ordered, then prove uniqueness
4. Definition of GCD
   (A) Given $a, b \in Z^{\geq 0}$ not both 0
   define gcd(a,b) = largest integer dividing both a, b
   (B) Definition: **a, b are relatively prime (co-prime) if $gcd(a,b) = 1$**
   Theorem: If $a, b \in Z^{\geq 0}$ not both 0, then $\exists x, y \in Z$ such that $gcd(a,b) = ax + by$

CHAPTER 3: PRIMES AND GREATEST COMMON DIVISORS

3.1 Prime Numbers

1. Definition: An integer $n \geq 2$ is prime if its divisors are only 1 and n
   An integer $n \geq 2$ is **composite** if it is not prime
   Meaning $\exists \mathbf{a}, \mathbf{b} \in \mathbf{Z}$ **w/** $\mathbf{1 < a < n, 1 < b < n}$ **and** $\mathbf{n = ab}$
2. Theorems:
   (A) **Every integer $n \geq 2$ has a prime divisor**
   (B) There are infinitely many primes
   (C) **If $n \in Z^{\geq 2}$ is composite then n has a prime divisor $\leq \sqrt{n}$**

3.2 The Distribution of Primes

1. Theorem: **We may find arbitrarily long sequences of consecutive composite integers!**
   $\mathbf{(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1)}$
2. Twin primes: Twin primes are primes two apart (Ex: 3,5 or 41,43)
3. Definition: For $x \in R^{+}$ define $\pi(x) = \#\, primes \leq x$
4. Prime Number Theorem: $\pi(x) \approx \frac{x}{\ln x}$
5. Corollary to PNT: For $x \in Z^{+}$, define $p_n = n^{\text{th}}$ prime. Then, $p_n \approx n \ln n$
6. Prime Conjectures:
   (A) Twin Prime conjecture: There are infinitely many pairs of twin primes
   (B) Legendre conjecture: There exists a prime between squares of any two consecutive integers
   (C) The n^2+1 conjecture: There are infinitely many primes of the form n^2+1
   (D) Goldbach conjecture: Every even int > 2 is the sum of two primes

3.3 Greatest Common Divisor

Theorems: Suppose $a, b \in Z$ not both 0.

1. Let $d = gcd(a,b)$, then $gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$
2. $\boldsymbol{\forall c \in Z,\ gcd(a,b) = gcd(a, b + ca)}$
3. $gcd(a,b) =$ smallest positive linear comb of a and b
4. {Linear combinations of a,b} = {Multiples of gcd(a,b)}
5. $d = gcd(a,b)$ iff (a) $d|a$ and $d|b$ and (b) $\forall c \in Z$, if $c|a$ and $c|b$ then $c|d$

3.4 The Euclidean Algorithm

1. Process: Example: Want gcd(252, 196)
   252 = 1.196 + 56   gcd(196,56)
   196 = 3.56 + 28   gcd(56, 28)
   56 = 2.28 + 0   gcd(28, 0)
   So, gcd(252, 196) = 28
2. Follow up: Find linear combinations of a, b based on that sequence
   28 = 196 - 3.56 = 196 - 3.(252 - 196) = 4.196 - 3.252

3.5 Fundamental Theorem of Arithmetic

1. Theorem: Any integer $n \geq 2$ may be written as a product of powers of primes.
2. Supporting Theorems:
   (A) Suppose p is prime and p|ab, then either p|a or p|b (or both)
   (B) Suppose p is prime and p|$a_1 \ldots a_n$ then there exists i such that p|a_i
   (C) Suppose a|bc and gcd(a,b)=1, then a|c
3. Consequences:
   (A) Theorem: Suppose $a, b \in Z$ with $a, b \geq 2$
   Then a|b iff whenever p^k appears in the prime factorization of a then p^j appears in the prime factorization of b with $j \geq k$
   (B) Theorem: A method of finding all factors of n ≥ 2
   The factors can be obtained by taking any subset of the primes with powers ≤
   (C) Calculation of gcd(a,b) via PF: take min powers of common primes
   (D) Calculation of lcm(a,b) via PF: take max powers of all primes
   (E) Theorem: **gcd(a,b).lcm(a,b) = ab**

CHAPTER 4: CONGRUENCES

4.1 Introduction to Congruences

1.Definition: Suppose $a,b,m \in Z$ with $m \geq 1$

a is congruent/equivalent to b mod m written $\boldsymbol{a \equiv b \bmod m}$ **iff** $\boldsymbol{m|(a-b)}$

2. Basic Properties:
   - (A) $a \equiv b \bmod m$ (Reflexive)
   - (B) if $a \equiv b \bmod m$ then $b \equiv a \bmod m$ (Symmetric)
   - (C) if $a \equiv b \bmod m$ and $b \equiv c \bmod m$ then $a \equiv c \bmod m$ (Transitive)
   - (D) if $a \equiv b \bmod m$ and $c \equiv d \bmod m$
     then $a + c \equiv b + d \bmod m$, $a - c \equiv b - d \bmod m$, $\boldsymbol{ac \equiv bd \bmod m}$
   - (E) **if** $\boldsymbol{a \equiv b \bmod m}$ **and** $\boldsymbol{k \in Z^+}$ **then** $\boldsymbol{a^k \equiv b^k \bmod m}$

3. Theorem: **Suppose** $\boldsymbol{ac \equiv bc \bmod m}$ **then** $\boldsymbol{a \equiv b \bmod \frac{m}{gcd(m,c)}}$

   Corollary: if p is prime and provided p∤c then ac ≡ bc mod p => a ≡ b mod p

4. Congruence Classes and Complete Sets of Residues
   - Definition: A congruence class mod m consists of all integers equivalent mod m
   - A representative of an equivalent class is simply one of the integers in that class
   - Definition: A representative is aka a residue
   - A complete set of residues mod m is a set consisting of one integer from each equivalent class. Such set will have m integers in it.
     Example: CSOR of mod 5 is {0,1,2,3,4} or {0,2,4,6,8}

4.2 Solving Linear Congruences

1. Definition: A linear congruence is a congruence of the form $ax \equiv b \bmod m$
2. $ax \equiv b \bmod m$ has solution(s) iff $gcd(a,m)\,|\,b$ (also # of solns = gcd(a,m))
3. Find the first solution (using Euclidean Algorithm):

   Example: $4x \equiv 6 \bmod 50$

   By E.A, find gcd(4,50) = 2|6 => There exists solution

   also by E.A, (1)50 + (-12)4 = 2

   (3)50 + (-36)4 ≡ 6 mod 50

   4(-36) ≡ 6 mod 50

   4(14) ≡ 6 mod 50

   => x_0 = 14

4. **All solutions have the form** $\boldsymbol{x \equiv x_0 + k\left(\frac{m}{gcd(a,m)}\right) \bmod m}$ with k = 0,1,2,...,gcd(a,m)-1

   Continued example above, gcd(4,50) = 2 => 2 solutions and $\frac{m}{gcd(a,m)} = \frac{50}{2} = 25$

   So, $x \equiv 14 + 25k$ => $x \equiv 14, 39 \bmod 50$

5. Multiplicative Inverses

   Definition: if $gcd(a,m) = 1$ then the unique solution to $ax \equiv 1 \bmod m$ is the multiplicative inverse of a mod m

6. Exponent notation:
   - $a^{-b} \equiv (a^{-1})^b \bmod m$ (provided gcd(a,m) = 1 so it has an inverse)
   - $a^{-b} \equiv \left(a^{b}\right)^{-1} \bmod m$
   - $a^0 \equiv 1 \bmod m$

7. Finalé: mod p = prime, then all of {1,2,...,p-1} have multiplicative inverse
   Otherwise, not obvious. For example, m = 10, then only 1,3,7,9 have m.i

4.3 Chinese Remainder Theorem

Example: $x \equiv 2 \bmod 6$, $x \equiv 4 \bmod 7$, $x \equiv 3 \bmod 25$

Notice, 6,7,25 are pairwise coprime. So, M = (6)(7)(25) = 1050

Then M_1 = (7)(25) = 175 M_2 = (6)(25) = 150 M_3 = (6)(7) = 42

Solve $175y_1 \equiv 1 \bmod 6$ $150y_2 \equiv 1 \bmod 7$ $42y_3 \equiv 1 \bmod 25$

=> y_1 = 1, y_2 = 5, y_3 = 3

=> x = (2)(175)(1) + (4)(150)(5) + (3)(42)(3) = 3728

We can reduce to get $x \equiv 578 \bmod 1050$