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 **<u>non-empty</u>** subset has **<u>a least element</u>**
   - Axiom: Z^+ is well-ordered
   - Related Proofs:
     - Prove sqrt(integer) is irrational
     - Prove how induction works
3. Floors and Ceilings
   - $\lfloor x \rfloor$ = floor(x) = largest integer ≤ x
   - $\lceil x \rceil$ = ceil(x) = smallest integer ≥ x

     Alternative definition used for proofs:
   - for $x \in R$ and $n \in Z$, $\lfloor x \rfloor = n$ iff n ≤ x < n+1
   - for $x \in R$ and $n \in Z$, $\lceil x \rceil = n$ iff n-1 < x ≤ 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**
   - Theorem: If S and T are both countable then so is $S \oplus T$
   - Uncountable set example: [0,1] Proof using contradiction

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: $\prod_{j=m}^{n} a_j = a_m . a_{m+1} \ldots a_n$
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 $P(n_o)$ 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 $gcd(a, b) = ax + by$