Note 2: PROOFS

- proof = finite sequence of steps (logical deductions) which estabilishes the truth of desired statement
- axioms = postulates
  - accepted without proof

NOTATION AND BASIC FACTS

- set of integers is closed under addition and multiplication
  - set of natural numbers too
  - sum or product of two integers is an integer
- a divides b ($a \mid b$) iff there is an integer q such that $b = aq$
- natural number is prime if it is divisible only by 1 and itself
- notation $:=$ indicates definition
  - $q := 6$ defines variable q as having value 6

DIRECT PROOF

- starts by assuming $P(x)$ for generic value of x and eventually concludes $Q(x)$ through chain of implications
- → $\boxed{EX}$: Let $0 < n < 1000$ be an integer. If sum of digits of n is divisible by 9, then n is divisible by 9.
  - equivalent to $(\forall n \in \mathbb{Z}^+)(n < 1000) \Rightarrow$ (sum divisible by 9 $\Rightarrow n$ divisible by 9)
  - PROOF: $n = 100a + 10b + c$ ($n = abc$ in decimal)
    - assume that sum is divisible by 9: $a + b + c = 9k$

      $n = 100a + 10b + c = 9k + 99a + 9b = 9(k + 11a + b)$

      → n is divisible by 9
    - converse is also true

      $n = 9l \Rightarrow 100a + 10b + c = 9l \Rightarrow 99a + 9b + (a+b+c) = 9l$

      $\Rightarrow a + b + c = 9(l - 11a - b)$

PROOF BY CONTRAPOSITION

- $P \Rightarrow Q$ is equivalent to $\neg Q \Rightarrow \neg P$
- $\boxed{EX}$: Let n be $\mathbb{N}$. If n^2 is even, n is even
  - PROOF: Assume n is odd, then n^2 is odd.

    $n = 2k + 1$

    $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ → odd

- $\boxed{EX}$: Suppose we place n object into k boxes. If $n>k$, then at least one box must contain more than one object.
  - PROOF: Suppose all boxes contain at most one object. We have to show that then $n \leq k$

    $n = n_1 + n_2 + \ldots + n_k$

    - we know that each n_i is at most 1

      $n_1 + n_2 + \ldots + n_k \leq 1+1+1+\ldots+1$

      $n_1 + n_2 + \ldots + n_k \leq k$

      $n \leq k$

- PROOF BY CONTRADICTION
  - assume the claim you want to prove is false, then you show that this leads to nonsense (contradiction)
    - → conclude that your claim must be true
  - to prove P, assume $\neg P \Rightarrow \ldots \Rightarrow R \Rightarrow \ldots \neg R$
    - conclusion $\neg P \Rightarrow \neg R \wedge R$ (contradiction)
      - → P holds
    - $\neg P \Rightarrow$ False contrapositive True $\Rightarrow P$
  - $\boxed{EX}$: There are infinitely many prime numbers.
    - PROOF: note that every natural number greater than 1 has a prime factor
      - suppose there are finitely many prime numbers (k)

        $p_1, p_2, \ldots, p_k$

        $Q = p_1 \cdot p_2 \cdots p_k + 1$

        - we know Q has prime factor p
          - → $p_1, \ldots, p_k$ are all primes, p must be one of them
            - p divides $p_1 p_2 \ldots p_k = r$
              - → $p | Q$ and $p | r$ but $p | (Q-r)$:
                - because $Q-r=1$, $p \leq 1$
                  - → p is not prime (contradiction)
  - $\boxed{EX}$: $\sqrt{2}$ is irrational
    - PROOF: Assume $\sqrt{2}$ is rational

      $\sqrt{2} = \frac{a}{b}$ where a and b have no common factor other than 1

      $2 = \frac{a^2}{b^2} \Rightarrow a^2 = 2b^2 \Rightarrow a^2$ must be even $\Rightarrow a = 2c$

      $\Rightarrow 2b^2 = 4c^2 \Rightarrow b^2 = 2c^2 \Rightarrow b$ is even $\Rightarrow a, b$ have common factor (contradiction)

- **PROOF BY CASES**
  - $\boxed{EX}$: There exist irrational numbers x and y such that x^y is rational
    - PROOF: demonstrate single x and y such that x^y is rational
      - let $x=\sqrt{2}$ and $y=\sqrt{2}$
        - → case $\sqrt{2}^{\sqrt{2}}$ is rational
          - yields our claim
        - → case $\sqrt{2}^{\sqrt{2}}$ is irrational
          - let $x=\sqrt{2}^{\sqrt{2}}$ and $y=\sqrt{2}$

            $x^y=(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}=\sqrt{2}^{\sqrt{2}\cdot\sqrt{2}}=\sqrt{2}^2=2$
          - we obtained rational number from two irrationals
      - since one of two cases must hold, statement is true
  - non-constructive proof
    - prove that X exists without revealing what X is
  - useful for proving inequalities
    - such as triangle inequality $x,y\in\mathbb{R}$ $|x+y|\leq|x|+|y|$
- **COMMON ERRORS WHEN USING PROOFS**
  - when writing proofs, don't assume the claim you want to proof
  - never forget to consider case where your variables take on the value 0
  - be careful when mixing negative numbers and inequalities
    - multiplying inequality by negative number flips the direction of inequality
- **STYLE AND SUBSTANCE IN PROOFS**
  - theorem, lemma