Proof Must Have

- Statement of what is to be proven.
- "Proof:" to indicate where the proof starts
- Clear indication of flow
- Clear indication of reason for each step
- Careful notation, completeness and order
- Clear indication of the conclusion

Number Theory - Ch 3 Definitions

- \( \mathbb{Z} \) --- integers
- \( \mathbb{Q} \) - rational numbers (quotients of integers)
  - \( r \in \mathbb{Q} \iff \exists a, b \in \mathbb{Z}, (r = a/b) \land (b \neq 0) \)
- Irrational = not rational
- \( \mathbb{R} \) --- real numbers
- superscript of + --- positive portion only
- superscript of - --- negative portion only
- other superscripts: \( \mathbb{Z}^{\text{even}}, \mathbb{Z}^{\text{odd}}, \mathbb{Q}^{>5} \)

- "closure" of these sets for an operation
Integer Definitions

- **even integer**
  \[ n \in \mathbb{Z}^{even} \iff \exists k \in \mathbb{Z} \ n = 2k \]

- **odd integer**
  \[ n \in \mathbb{Z}^{odd} \iff \exists k \in \mathbb{Z} \ n = 2k+1 \]

- **prime integer (\( \mathbb{Z}^{\geq 1} \))**
  \[ n \in \mathbb{Z}^{prime} \iff \forall r,s \in \mathbb{Z}^+, \ (n=r\times s) \rightarrow (r=1) \vee (s=1) \]

- **composite integer (\( \mathbb{Z}^{>1} \))**
  \[ n \in \mathbb{Z}^{composite} \iff \exists r,s \in \mathbb{Z}^+, \ n=r\times s \quad (r \neq 1) \wedge (s \neq 1) \]

Constructive Proof of Existence

If we want to prove:

- \( \exists n \in \mathbb{Z}^{even}, \exists p,q, r,s \in \mathbb{Z}^{prime} \ n = p+q \land n = r+s \land p \neq r \land p \neq s \land q \neq r \land q \neq s \)
  
  - let \( n=10 \)
    - \( n \in \mathbb{Z}^{even} \) by definition of even
  
  - Let \( p = 5 \) and the \( q = 5 \)
    - \( p,q \in \mathbb{Z}^{prime} \) by definition of prime
    - \( 10 = 5+5 \)
  
  - Let \( r = 3 \) and \( s = 7 \)
    - \( r,s \in \mathbb{Z}^{prime} \) by definition of prime
    - \( 10 = 3+7 \)
  
  - and all of the inequalities hold
Methods of Proving
Universally Quantified Statements

• Method of Exhaustion
  – prove for each and every member of the domain
  – $\forall r \in \mathbb{Z}^+ \text{ where } 23 < r < 29 \rightarrow \exists p, q \in \mathbb{Z}^+ (r = p \cdot q \land (p \leq q))$

• Generalizing from the "generic particular"
  – suppose x is a particular but arbitrarily chosen element of the domain
  – show that x satisfies the property
  – i.e. $\forall r \in \mathbb{Z}, \ r \in \mathbb{Z}^{\text{even}} \rightarrow r^2 \in \mathbb{Z}^{\text{even}}$

Examples of Generalizing from the "Generic Particular"

• For any pair of integers where the first of them is even, the product of those integers is also even.
  – $\forall m, n \in \mathbb{Z}, \ m \in \mathbb{Z}^{\text{even}} \rightarrow m \cdot n \in \mathbb{Z}^{\text{even}}$

• The product of any two odd integers is also odd.
  – $\forall m, n \in \mathbb{Z}^{\text{odd}}, \ m \cdot n \in \mathbb{Z}^{\text{odd}}$

• The product of any two rationals is also rational.
  – $\forall m, n \in \mathbb{Q}, \ m \cdot n \in \mathbb{Q}$
Disproof by Counter Example

- \( \forall r^2 \in \mathbb{Z}^+ \rightarrow r \in \mathbb{Z}^+ \)
- Counter Example: \( r^2 = 9 \land r = -3 \)
  - \( r^2 \in \mathbb{Z}^+ \) since \( 9 \in \mathbb{Z}^+ \) so the antecedent is true
  - but \( r \notin \mathbb{Z}^+ \) since \( -3 \notin \mathbb{Z}^+ \) so the consequent is false
  - this means the implication is false for \( r = -3 \) so this is a valid counter example
- When a counter example is given you must always justify that it is a valid counter example by showing the algebra (or other interpretation needed) to support your claim

Division definitions

- \( d \mid n \leftrightarrow \exists k \in \mathbb{Z}, n = d \times k \)
- \( n \) is divisible by \( d \)
- \( n \) is a multiple of \( d \)
- \( d \) is a divisor of \( n \)
- \( d \) divides \( n \)

- standard factored form
  - \( n = p_1^{e_1} \times p_2^{e_2} \times p_3^{e_3} \times \ldots \times p_k^{e_k} \)
Proof by Contrapositive

For all positive integers, if \( n \) does not divide a number to which \( d \) is a factor, then \( n \) can not divide \( d \).

\[ \forall n, d, c \in \mathbb{Z}^+, \ n \nmid dc \rightarrow n \nmid d \]
Proof by Contrapositive

For all positive integers, if \( n \) does not divide a number to which \( d \) is a factor, then \( n \) can not divide \( d \).

\[ \forall n, d, c \in \mathbb{Z}^+, \ n \nmid dc \rightarrow n \nmid d \]
\[ \forall n, d, c \in \mathbb{Z}^+, \ n \mid d \rightarrow n \mid dc \]

proof:

more integer definitions

- div and mod operators
  - \( n \div d \) --- integer quotient for \( \frac{n}{d} \)
  - \( n \mod d \) --- integer remainder for \( \frac{n}{d} \)
  - \((n \div d = q) \land (n \mod d = r) \iff n = d \cdot q + r\)
    where \( n \in \mathbb{Z}^{\geq 0}, \ d \in \mathbb{Z}^+, \ r \in \mathbb{Z}, \ q \in \mathbb{Z}, \ 0 \leq r < d \)

- relating “mod” to “divides”
  - \( d \mid n \iff 0 = n \mod d \)
  - \( 0 \equiv_d n \)

- equivalence in a mod
  - \( x \equiv_d y \iff d|\,(x-y) \quad \text{[note: their remainders are equal]} \)
  - sometimes written as \( x \equiv_y \mod d \) meaning \( x \equiv y \mod d \)
Quotient Remainder Theorem

\( \forall n \in \mathbb{Z} \setminus \forall d \in \mathbb{Z}^+ \exists q, r \in \mathbb{Z} \)

\[ (n = dq + r) \land (0 \leq r < d) \]

Proving definition of equiv in a mod by using the quotient remainder theorem

Prove that if \([m \equiv_d n]\), then \([d|n-m]\)

where \(m, n \in \mathbb{Z}\) and \(d \in \mathbb{Z}^+\)

Proofs using this definition

• \( \forall m \in \mathbb{Z}^+ \setminus \forall a, b \in \mathbb{Z} \)

\[ a \equiv_m b \iff \exists k \in \mathbb{Z} \setminus a = b + km \]

• \( \forall m \in \mathbb{Z}^+ \setminus \forall a, b, c, d \in \mathbb{Z} \)

\[ a \equiv_m b \land c \equiv_m d \rightarrow a + c \equiv_m b + d \]
Floor and Ceiling Definitions

• n is the floor of x where $x \in \mathbb{R} \land n \in \mathbb{Z}$
  \[ \lfloor x \rfloor = n \iff n \leq x < n+1 \]
• n is the ceiling of x where $x \in \mathbb{R} \land n \in \mathbb{Z}$
  \[ \lceil x \rceil = n \iff n-1 < x \leq n \]

Floor/Ceiling Proofs

• $\forall x, y \in \mathbb{R} \ [x+y] = [x] + [y]$

• $\forall x \in \mathbb{R} \ \forall y \in \mathbb{Z} \ [x+y] = [x] + y$
Proof by Division into Cases

• The floor of \( \frac{n}{2} \) is either
  a) \( \frac{n}{2} \) when \( n \) is even
  or  b) \( \frac{n-1}{2} \) when \( n \) is odd

• \( \forall n \in \mathbb{Z} \ 3 \mid n \rightarrow n^2 \equiv_3 1 \)

Prime Factored Form

\[ n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdot \ldots \cdot p_k^{e_k} \]

• Unique Factorization Theorem (Theorem 3.3.3)
  – given any integer \( n > 1 \)
  – \( \exists k \in \mathbb{Z}, \exists p_1, p_2, \ldots, p_k \in \mathbb{Z}_{\text{prime}}, \exists e_1, e_2, \ldots, e_k \in \mathbb{Z}^+ \)
   where the \( p \)’s are distinct and any other expression of \( n \) is identical to this except maybe in the order of the factors

• Standard Factored Form
  – \( p_i < p_{i+1} \)
  • \( \exists m \in \mathbb{Z}, 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot m = 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \)
    – Does \( 17 \mid m \) ??
Steps Toward Proving the Unique Factorization Theorem

• Every integer greater than or equal to 2 has at least one prime that divides it

• For all integers greater than 1, if \( a \mid b \), then \( a \mid (b+1) \)

• There are an infinite number of primes

Using the Unique Factorization Theorem

• Prove that the \( \sqrt{3} \notin \mathbb{Q} \)

• Prove:
  \[
  \forall a \in \mathbb{Z}^+ \forall q \in \mathbb{Z}_{\text{prime}} \quad q \mid a^2 \rightarrow q \mid a
  \]
Summary of Proof Methods

• Constructive Proof of Existence
• Proof by Exhaustion
• Proof by Generalizing from the Generic Particular
• Proof by Contraposition
• Proof by Contradiction
• Proof by Division into Cases

Errors in Proofs

• Arguing from example for universal proof.
• Misuse of Variables
• Jumping to the Conclusion (missing steps)
• Begging the Question
• Using "if" about something that is known