

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

- **Z** --- integers
 - **Q** - rational numbers (quotients of integers)
 - $r \in \mathbf{Q} \leftrightarrow \exists a, b \in \mathbf{Z}, (r = a/b) \wedge (b \neq 0)$
 - Irrational = not rational
 - **R** --- real numbers
 - superscript of ⁺ --- positive portion only
 - superscript of ⁻ --- negative portion only
 - other superscripts: $\mathbf{Z}^{\text{even}}$, $\mathbf{Z}^{\text{odd}}$, $\mathbf{Q}^{>5}$
-
- "closure" of these sets for an operation
 - Z closed under what operations?

Integer Definitions

- even integer
 - $n \in \mathbf{Z}^{\text{even}} \leftrightarrow \exists k \in \mathbf{Z}, n = 2k$
- odd integer
 - $n \in \mathbf{Z}^{\text{odd}} \leftrightarrow \exists k \in \mathbf{Z}, n = 2k+1$
- prime integer ($\mathbf{Z}^{>1}$)
 - $n \in \mathbf{Z}^{\text{prime}} \leftrightarrow \forall r,s \in \mathbf{Z}^+, (n=r*s) \rightarrow (r=1) \vee (s=1)$
- composite integer ($\mathbf{Z}^{>1}$)
 - $n \in \mathbf{Z}^{\text{composite}} \leftrightarrow \exists r,s \in \mathbf{Z}^+, n=r*s \wedge (r \neq 1) \wedge (s \neq 1)$

Constructive Proof of Existence

If we want to prove:

- $\exists n \in \mathbf{Z}^{\text{even}}, \exists p, q, r, s \in \mathbf{Z}^{\text{prime}} n = p+q \wedge n = r+s$
 $\wedge p \neq r \wedge p \neq s \wedge q \neq r \wedge q \neq s$

– let $n=10$

- $n \in \mathbf{Z}^{\text{even}}$ by definition of even

– Let $p = 5$ and the $q = 5$

- $p, q \in \mathbf{Z}^{\text{prime}}$ by definition of prime
- $10 = 5+5$

– Let $r = 3$ and $s = 7$

- $r, s \in \mathbf{Z}^{\text{prime}}$ 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
 - $\forall r \in \mathbf{Z}^+$ where $23 < r < 29 \rightarrow \exists p, q \in \mathbf{Z}^+ (r = p * q) \wedge (p \leq q)$
- 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. $\forall r \in \mathbf{Z}, r \in \mathbf{Z}^{\text{even}} \rightarrow r^2 \in \mathbf{Z}^{\text{even}}$

Examples of Generalizing from the "Generic Particular"

- The product of any two odd integers is also odd.
 - $\forall m, n \in \mathbf{Z}, [(m \in \mathbf{Z}^{\text{odd}} \wedge n \in \mathbf{Z}^{\text{odd}}) \rightarrow m * n \in \mathbf{Z}^{\text{odd}}]$
- The product of any two rationals is also rational.
 - $\forall m, n \in \mathbf{Q}, m * n \in \mathbf{Q}$

Disproof by Counter Example

- $\forall r \in \mathbf{Z}, r^2 \in \mathbf{Z}^+ \rightarrow r \in \mathbf{Z}^+$
- Counter Example: $r^2 = 9 \wedge r = -3$
 - $r^2 \in \mathbf{Z}^+$ since $9 \in \mathbf{Z}^+$ so the antecedent is true
 - but $r \notin \mathbf{Z}^+$ since $-3 \notin \mathbf{Z}^+$ 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

- $d \mid n \leftrightarrow \exists k \in \mathbf{Z}, n = d * k$
- n is divisible by d
- n is a multiple of d
- d is a divisor of n
- d divides n

-
- standard factored form

$$- n = p_1^{e_1} * p_2^{e_2} * p_3^{e_3} * \dots * p_k^{e_k}$$

Proof using the Contrapositive

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

Proof using the 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 using the 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 $\frac{n}{d}$
 - $n \text{ div } d$ --- integer quotient for $\frac{n}{d}$
 - $n \text{ mod } d$ --- integer remainder for $\frac{n}{d}$
 - $(n \text{ div } d = q) \wedge (n \text{ mod } d = r) \leftrightarrow n = d * q + r$
where $n \in \mathbf{Z}^{\geq 0}$, $d \in \mathbf{Z}^+$, $r \in \mathbf{Z}$, $q \in \mathbf{Z}$, $0 \leq r < d$
- relating “mod” to “divides”
 - $d | n \quad \leftrightarrow \quad 0 = n \text{ mod } d$
 $\quad \quad \quad \leftrightarrow \quad 0 \equiv_d n$
- definition of equivalence in a mod
 - $x \equiv_d y \leftrightarrow d | (x - y)$ [note: their remainders are equal]
 - sometimes written as $x \equiv y \text{ mod } d$ meaning $(x \equiv y) \text{ mod } d$

Quotient Remainder Theorem

$$\forall n \in \mathbb{Z} \quad \forall d \in \mathbb{Z}^+ \quad \exists q, r \in \mathbb{Z}$$

$$(n = dq + r) \wedge (0 \leq r < d)$$

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

This means

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

- $\forall m \in \mathbb{Z}^+ \quad \forall a, b \in \mathbb{Z}$

$$a \equiv_m b \leftrightarrow \exists k \in \mathbb{Z} \quad a = b + km$$

- $\forall m \in \mathbb{Z}^+ \quad \forall a, b, c, d \in \mathbb{Z}$

$$a \equiv_m b \wedge c \equiv_m d \rightarrow a + c \equiv_m b + d$$

Proof by Division into Cases

$$\forall n \in \mathbb{Z} \ 3 \nmid n \rightarrow n^2 \equiv_3 1$$

Floor and Ceiling Definitions

- n is the floor of x where $\mathbf{x \in R \wedge n \in Z}$

$$\lfloor x \rfloor = n \iff n \leq x < n+1$$

- n is the ceiling of x where $\mathbf{x \in R \wedge n \in Z}$

$$\lceil x \rceil = n \iff n-1 < x \leq n$$

Floor/Ceiling Proofs

- $\forall x, y \in \mathbf{R} \lfloor x+y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$
- $\forall x \in \mathbf{R} \forall y \in \mathbf{Z} \lfloor x+y \rfloor = \lfloor x \rfloor + y$

Proof by Division into Cases (again)

- The floor of $(n/2)$ is either
 - a) $n/2$ when n is even
 - or b) $(n-1)/2$ when n is odd

Prime Factored Form

$$n = p_1^{e_1} * p_2^{e_2} * p_3^{e_3} * \dots * p_k^{e_k}$$

- Unique Factorization Theorem (Theorem 3.3.3)

- given any integer $n > 1$

- $\exists k \in \mathbb{Z}, \exists p_1, p_2, \dots, p_k \in \mathbb{Z}^{\text{prime}}, \exists e_1, e_2, \dots, e_k \in \mathbb{Z}^+,$

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

- $p_i < p_{i+1}$

- $\exists m \in \mathbb{Z}, 8 * 7 * 6 * 5 * 4 * 3 * 2 * m = 17 * 16 * 15 * 14 * 13 * 12 * 11 * 10$

- Does $17 | m$??

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 $a|b$, then $a \nmid (b+1)$
- There are an infinite number of primes

Using the Unique Factorization Theorem

- Prove that the

$$\sqrt{3} \notin \mathbb{Q}$$

- Prove:

$$\forall a \in \mathbb{Z}^+ \forall q \in \mathbb{Z}^{\text{prime}} \quad q|a^2 \rightarrow q|a$$

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