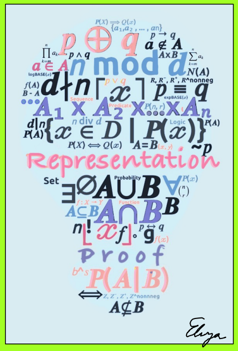
Discrete Structures



Lecture 7: Introduction to number theory

Susan L. Epstein

HUNTER

1

Last time

★ **Predicate calculus extends logical representation**

- How to translate multiply quantified statements from logic to English and from English to logic
- How to construct and negate multiply quantified predicate statements
- Valid arguments in FOPC
- Basic formal proof structures
- Proof by cases

2

Today's outline

- Formal verbal proof (review)
- Integers
- Rational numbers
- Divisibility

Definitions and prior theorems guide proofs

Fall 2023 CSCI 150 3/26

3

Proof skeleton

Theorem: (copy the statement here)

Proof:

Let/Assume/Suppose: Name variables and state what they stand for

be general: any state any assumptions

We must show that…

multiple grammatically correct sentences

Clarify your logic with a reason for every assertion Thus Then

Therefore So Hence Consequently It follows that

By definition of By substitution Because Since

Display equations and inequalities clearly

QED

Fall 2023 CSCI 150 4/26

4

Proof by cases skeleton

Theorem: If A_1 or A_2 or… or A_n then C.

Proof:

Let/Assume/Suppose: Name variables and state what they stand for
be general: any state any assumptions

We must show that C is true in each of the following cases:
Case 1: If A_1 then C.
Case 2: If A_2 then C.
…
Case n: If A_n then C

Clarify your logic with a reason for every assertion
Display equations and inequalities clearly

Thus C is true regardless of which is the case.

QED

5

Today's outline

- ✓ Formal verbal proof (review)
- Integers
- Rational numbers
- Divisibility

6

Assumptions

- Appendix A
- Properties of equality for objects A, B, C

  reflexivity: $A = A$
  symmetry: if $A = B$ then $B = A$
  transitivity: if $A = B$ and $B = C$ then $A = C$

- Closure: Set S is closed under operation $\circ$ iff $\forall x, y \in S,\ x \circ y \in S$

  $\boldsymbol{Z}$ is closed under addition, subtraction, and multiplication

- $\nexists\, \boldsymbol{x} \in \boldsymbol{Z}\ 0 < x < 1$

Fall 2023 CSCI 150 7/26

7

Kinds of integers

- $n \in \boldsymbol{Z}$ is even iff $\exists k \in \boldsymbol{Z}$ such that $n = 2k$ 30 516
- $n \in \boldsymbol{Z}$ is odd iff $\exists k \in \boldsymbol{Z}$ such that $n = 2k + 1$ 899 -5
- Parity of integer = even or odd
- $n \in \boldsymbol{Z}$ is prime iff $n > 1$ and $\forall r, s \in \boldsymbol{Z}^+$ such that $n = rs$ and either $r = 1$ and $s = n$ or $r = n$ and $s = 1$

  7 97 20981

- $n \in \boldsymbol{Z}$ is composite iff $n > 1$ and $\exists\, r, s \in \boldsymbol{Z}^+$ such that $n = rs$ and $1 < r < n$ and $1 < s < n$ 6 95 20983

Fall 2023 CSCI 150 8/26

8

Disproof and proof for universals

$$\forall x \in D, P(x) \rightarrow Q(x)$$

- Disproof: show that it is false by $\exists x \in D, \sim(P(x) \rightarrow Q(x)) \equiv P(x) \wedge \sim Q(x)$
  Simply display a counterexample
  All primes are odd numbers
  $\forall a, b \in \boldsymbol{R}$, if $a^4 = b^4$ then $a = b$
- Exhaustive proof: for **finite** D, proof by $|D|$ cases (one for each $x \in D$)
  $\forall n \in \boldsymbol{Z}$, if n is even and $6 \leq n \leq 18$ then n can be written as the sum of 2 primes
  You could do this for D but not for **all** integers.

Fall 2023 CSCI 150 9/26

9

Generalization from the generic particular

$$\forall x \in D, P(x) \rightarrow Q(x)$$

- Generic particular = arbitrarily chosen example from D that represents a specific but unknown element
  For all integers m, if $m > 1$ then $0 < 1/m < 1$
  Let m be any integer greater than 1. We must show that
  $0 < 1/m < 1$ generic particular
- Proof by generalization from the generic particular: use a generic particular that satisfies $P(x)$ and show that it satisfies $Q(x)$
- Use existential instantiation to name distinct objects

  If n is even then it is twice some integer. We can name that integer.

  "by definition of even there is some integer k such that $n = 2k$"

Fall 2023 CSCI 150 10/26

10

Proof by the generic particular skeleton

Theorem: (copy statement of the form $\forall x \in D, P(x) \rightarrow Q(x)$ here)

Proof:

Let x be any particular but arbitrarily chosen element in D that satisfies $P(x)$.

We must show that x satisfies $Q(x)$.

Clarify your logic with a reason for every assertion
Display equations and inequalities clearly

QED

Fall 2023 CSCI 150 11/26

11

Proofs about existence

- Assertion of existence: $\exists x \in D \ni Q(x)$ is true iff some $x \in D$ makes $Q(x)$ true
- An equivalent and usually easier approach is to prove its negation $\sim(\exists x \in D \ni Q(x)) \equiv \forall x \in D \sim Q(x)$ by generalization from the generic particular
- Constructive proofs
  - Find an $x \in D$

    $Q(x)$ =∃ an even integer n that can be written in two ways as a sum of two prime numbers $17 + 3 = 20 = 13{+}7$
  - Or provide directions to find an $x \in D$ that satisfies $Q(x)$

    For $r, s \in \boldsymbol{Z}$, ∃ an integer k such that $22r + 18s = 2k$

    use $k = 11r + 9s$
- Nonconstructive proofs
  - Show an axiom or previously proved theorem guarantees $\exists x \in D$
  - Or assume $\nexists x \in D$ and show that that leads to a contradiction

Fall 2023 CSCI 150 12/26

12

Today's outline

- ✓ Formal verbal proof
- ✓ Integers
- Rational numbers
- Divisibility

Rational numbers and decimals

- Rational number $r \in \boldsymbol{Q} \leftrightarrow (\exists a, b \in \boldsymbol{Z}, r = a/b$ and $b \neq 0)$
  - a and b are not unique $\frac{3}{5} = \frac{24}{40}$
- Any terminating decimal number is rational $1.6 = \frac{16}{10}$ $.0008 = \frac{8}{10000}$
- Many rational numbers are repeating decimals $\frac{1}{3} = 0.333\ldots$
- Non-terminating, non-repeating decimals are real but not rational π e
- Zero product property: $\forall r, s \in \boldsymbol{Q}, r \neq 0, s \neq 0$ then $rs \neq 0$

Theorems, axioms and corollaries

- Axiom = statement assumed or accepted without proof
- Theorem = statement that is or can be proved

  Theorem: $\forall x \in \boldsymbol{Z}, x \in \boldsymbol{Q}$
- Corollary = somewhat less significant statement immediately deducible from a theorem

  Theorem: The sum of any 2 rational numbers is rational.

  Corollary: Twice a rational number is rational.

Fall 2023 CSCI 150 15/26

15

Equivalent definitions

- Equivalent definition: $\Leftrightarrow$
- $[n \in \boldsymbol{Z}$ is even$] \Leftrightarrow [\exists k \in \boldsymbol{Z}$ such that $n = 2k]$
- If n is a particular even integer, it has the form $2k,\ k \in \boldsymbol{Z}$

  Given a value with the form $2k,\ k \in \boldsymbol{Z}$ you can deduce that it is even
- $[n \in \boldsymbol{Z}$ is odd$] \Leftrightarrow [\exists k \in \boldsymbol{Z}$ such that $n = 2k+1]$

  If n is a particular odd integer, it has the form $2k+1,\ k \in \boldsymbol{Z}$

  Given a value with the form $2k+1,\ k \in \boldsymbol{Z}$ you can deduce that it is odd
- $[n \in \boldsymbol{Z}$ is prime$] \Leftrightarrow$

  $(n > 1) \wedge \forall r, s \in \boldsymbol{Z}^{+}(n = rs) \rightarrow [(r = 1, s = n) \oplus (r = n, s = 1)] \Leftrightarrow$

  $(n > 1) \wedge \forall r, s \in \boldsymbol{Z}^{+}(n = rs) \rightarrow (r = 1, s = n) \vee (r = n, s = 1) \wedge (\boldsymbol{r} \neq \boldsymbol{s})$
- $[n \in \boldsymbol{Z}$ is composite$] \Leftrightarrow$

  $(n > 1) \wedge \exists\, r, s \in \boldsymbol{Z}^{+}(n = rs) \wedge (1 < r < n) \wedge (1 < s < n)$

Fall 2023 CSCI 150 16/26

16

Disproof by counterexample

- Form for disproof
  - **Statement:**
  - **Counterexample: Let**

Statement: $\forall a, b \in \boldsymbol{R}$ if $a^{42} = b^{42}$ then $a = b$
Counterexample: Let $a = 1, b = -1$. Then $a^{42} = 1 = b^{42}$ but $a \neq b$ because $1 \neq -1$.

Any questions?

Fall 2023 CSCI 150 17/26

17

Today's outline

✓ Formal verbal proof
✓ Integers
✓ Rational numbers
- Divisibility

Fall 2023 CSCI 150 18/26

18

Definitions

- For $n, d \in \boldsymbol{Z}, d \neq 0$`, n is divisible by d iff $\exists m \in \boldsymbol{Z}$ such that $n = md$
- Equivalent phrasing
  - n is divisible by d
  - n is a multiple of d
  - d is a factor of n
  - $d|n \equiv d$ is a divisor of n
  - d divides n
- $\forall n, d \in \boldsymbol{Z}, d|n \iff \exists k$ such that $n = dk$
- $\forall n, d \in \boldsymbol{Z}, d \nmid n \iff n/d \notin \boldsymbol{Z}$

Warning: $x|y \not\Leftrightarrow x/y$

Fall 2023 CSCI 150 19/26

19

Proof skeleton

Theorem: (copy the statement here)

Proof:

Let/Assume/Suppose: Name variables and state what they stand for

be general: any state any assumptions

We must show that…

multiple grammatically correct sentences

Clarify your logic with a reason for every assertion Thus Then

Therefore So Hence Consequently It follows that

By definition of By substitution Because Since

Display equations and inequalities clearly

QED

Fall 2023 CSCI 150 20/26

20

A proof with divisibility

Theorem (T20 in Appendix A): $\forall a, b \in \boldsymbol{R}$, if $a < b$ and $c > 0$, then $ac < bc$.
Theorem (T25 in Appendix A): $\forall a, b \in \boldsymbol{R}, ab > 0 \rightarrow (a, b \in \boldsymbol{R}^{+}) \vee (a, b \in \boldsymbol{R}^{-})$
Theorem: $\forall a, b \in \boldsymbol{Z}^{+}\ a|b \rightarrow a \leq b$
Proof: generic particulars
Let a, b be any positive integers such that $a|b$.
We must show that $a \leq b$.
Since $a|b, \exists k$ such that $b = ak$ by definition of |.
Because $a, b \in \boldsymbol{Z}^{+} \subset \boldsymbol{R}$, by T25, $ab, k \in \boldsymbol{Z}^{+}$and by definition of $\boldsymbol{Z}^{+}$,

$$1 \leq k$$

Because a positive multiplier preserves inequality (T20 in Appendix A), multiplying both sides by a yields

$$a \leq ak = b$$

Thus $a \leq b$.
QED
Corollary: The only divisors of 1 are +1 and -1. (**why?**)

Fall 2023 CSCI 150 21/26

21

Divisibility is transitive

Theorem: $\forall x, y, z \in \boldsymbol{Z}, (x|y) \wedge (y|z) \rightarrow x|z$

Proof: generic particulars

Let x, y, z be any integers such that $x|y$ and $y|z$.

We must show that $x|z$ or equivalently that $\exists k \in \boldsymbol{Z}$ such that $z = kx$.

Then by definition of divisibility, $\exists a, b \in \boldsymbol{Z}$ such that $y = ax$ and $z = by$.

By substitution $z = by = b(ax) = (ba)x$.

Because $\boldsymbol{Z}$ is closed under multiplication, $ba \in \boldsymbol{Z}$.

Then for $k = ba$, $z = kx$ and $x|z$.

QED

Fall 2023 CSCI 150 22/26

22

A divisibility disproof

Statement: $\forall m, n \in \boldsymbol{Z}$, if $m|n$ and $n|m$ then $m = n$.

Counterexample: $m = 7, n = -7$

Where did that come from?

If $m|n$ then by definition $\exists a$ such that $ma = n$

Similarly, if $n|m$ then by definition $\exists b$ such that $nb = m$.

By substitution of nb for m in $ma = n$, $nba = n$ and dividing both sides by n, $ba = 1$. By the corollary on slide 22 the only divisors of 1 are $+1$ and -1. There are 3 cases.

Case 1: $a = b = 1$ so $m = n$.

Case 2: $a = b = -1$ $m = n$.

Case 3: One of a and b is 1 and the other is -1. Then m can be any integer and n is $-m$.

Comment: $\forall m, n \in \boldsymbol{Z}$ does not state $m \neq n$. Don't assume they are distinct!

Unique factorization theorem

Theorem: For every integer $n > 1$ there is a positive integer k and distinct primes $p_1, p_2, \ldots, p_k$ and positive integers $e_1, e_2, \ldots, e_k$ such that

$$n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$$

This factorization is unique up to the order in which the primes are written.

$$15000 = 5^4 2^3 3^1$$

Standard factored form of $n > 1$ is $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ where $p_1, p_2, \ldots, p_k$ are distinct primes and $p_1 < p_2 < \cdots < p_k$

$$15000 = 2^3 3^1 5^4$$

Proof is outlined in §5.4 and §8.4

Proof methods (so far)

Truth table

Sequence of statements with reasons

Valid argument forms (modus ponens, modus tollens,…)

Method of exhaustion

Predicate logic (quantification, existence, uniqueness)

Proof by cases

Generalization from the generic particular

Fall 2023 CSCI 150 25/26

25

What you should know

- ★ **Definitions and prior theorems guide proofs**
- What a good verbal proof looks like
- A counterexample produces a simple disproof
- How to work with odd, even, prime, composite, and rational numbers
- The unique factorization theorem

Next up: ***Proofs with number theory***

Time to finish up that Opening sheet!

Problem set 7,8 is due on Monday, October 2 at 11PM

Fall 2023 CSCI 150 26/26

26

PLEASE check your submissions

- **We want you to learn** so we carefully grade **thousands** of answers in 48-72 hours.
- It is **your responsibility** to ensure that Gradescope displays your answers correctly.
- **Look at the way we see your submission when we grade it**
  https://help.gradescope.com/article/axm932lptr-student-view-submission
- Remember to
  - Scan the first page
  - Do not skip a page or scan one twice
  - Check to see that your answers are in the right place.
  - Use our template, not an imitation.

If you still need help with the templates, speak with your recitation instructor or come to my office hours and speak with me.

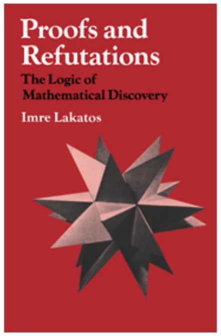
Thanks for your cooperation!

27

Proofs and Refutations

If you find this material fascinating, I recommend

Proofs and Refutation by Imre Lakatos (1976)



Fall 2023 CSCI 150

28