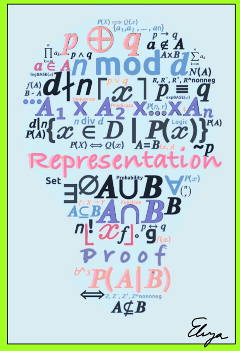
Discrete Structures



Lecture 8: Proofs with number theory

Susan L. Epstein

HUNTER

1

Last time

- ⭐ **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

2

Today's outline

- Important proofs by cases
- Floors and ceilings
- Proofs by contradiction and contraposition

More concepts support more proofs

3

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

4

Another proof with divisibility

Theorem P (proved in Lecture 7): $\forall a, b \in \mathbf{Z}^+ \; a|b \rightarrow a \le b$

Theorem (T12 in Appendix A): $\forall a, b \in \mathbf{R}, (-a)(-b) = ab$

Theorem The only divisors of 1 are $+1$ and -1. USE those definitions!

Proof: generic particular

Let $n \in \mathbf{Z}$ such that $n|1$. We must show that the only divisors of 1 are $+1$ and -1. Since $1 = 1 \cdot 1$ and $1 = -1 \cdot -1$, both 1 and -1 are divisors of 1.

Since $n|1, \exists k \in \mathbf{Z}$ such that $1 = nk$ by definition of |.

Since $1 \in \mathbf{Z}^+$, by T25, there are 2 cases. n and k are either both positive or both negative. ($n = 0$ is not a case because 0 cannot divide any number.)

Case 1: n and k are both positive.

By theorem P, $n \le 1$. Since $n > 0$ and $n \in \mathbf{Z}, 0 < n \le 1$ and so $n = 1$.

Case 2: n and k are both negative.

By T12, $1 = nk = (-n)(-k)$ so $-n|1$. Since $-n > 0$, $-n$ is a positive integer divisor of 1, and by Case 1, $-n = 1$ and $n = -1$.

Thus the only divisors of 1 are $+1$ and -1 regardless of which is the case.

QED

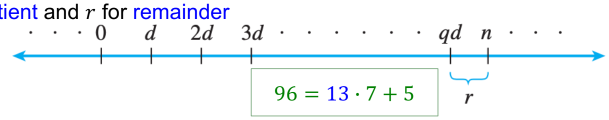
5

The quotient-remainder theorem

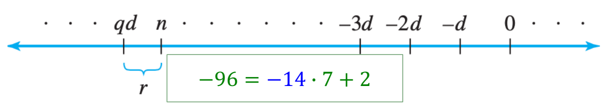
Theorem: For any $n \in \mathbf{Z}$ and any $d \in \mathbf{Z}^+$ there exists **unique** $q, r \in \mathbf{Z}$ such that

$$n = dq + r \qquad \text{and} \qquad 0 \le r < d$$

- q for quotient and r for remainder
- If $n > 0$



- If $n < 0$



- Proof (much) later
- Very useful corollary: Any integer is either even or odd. **why?**

6

div and *mod*

- For any $n \in \boldsymbol{Z}$ and any $d \in \boldsymbol{Z}^+$, $n \text{ div } d$ = integer quotient when n is divided by d $\quad 365 \; div \; 7 \; = 52$
- aka **for $n \in \boldsymbol{Z}^+$ only,** div (Pascal), / (C, C++,Java), /:: (Python)
- For any $n \in \boldsymbol{Z}^+$ and any $d \in \boldsymbol{Z}^+$, $n \bmod d$ = nonnegative integer remainder when n is divided by d
  - mod stands for modulo $\quad 365 \; mod \; 7 \; = 1$
  - aka **for $n \in \boldsymbol{Z}^+$ only,** mod (Pascal), % (C, C++, Java, Python),

$$n \text{ div } d = q \text{ and } n \bmod d = r \quad \Leftrightarrow \quad n = dq + r$$

- Nice computational applications: $365 = \; 52 \cdot 7 + 1$
  - If this year and next year are not leap years and your birthday falls on a Thursday, next year it will be on a Friday
  - Generalization: number the days of the week from Sunday = 0

    $nextWeekday \; = \; (todayWeekday \; + \; daysFromNow) \; mod \; 7$
- n is divisible by d iff $n \bmod d \; = 0$
- Both mod and div are functions defined on $\boldsymbol{Z} \times \boldsymbol{Z}$

Fall 2023 CSCI 150 7/27

7

The parity property

Theorem: Any 2 consecutive integers have opposite parity.

Proof: generic particular USE those definitions!

Let m be any integer. The next consecutive integer is then $m + 1$.

We must show that both m and $m + 1$ have opposite parity, There are 2 cases: m is even or m is odd,

Case 1: m is even. Then $\exists \; k \in \boldsymbol{Z}$ such that $m = 2k$.

Then $m + 1 = 2k + 1$ and $m + 1$ is odd, that is, of opposite parity.

Case 2: m is odd. Then $\exists \; k \in \boldsymbol{Z}$ such that $m = 2k + 1$.

Then $m + 1 = 2k + 1 + 1 = 2k + 2 = 2(k + 1)$.

Since $\boldsymbol{Z}$ is closed under addition, $k + 1 \in \boldsymbol{Z}$, and $m + 1$ is even, that is of opposite parity.

Thus any 2 consecutive integers have opposite parity regardless of which is the case.

QED

Fall 2023 CSCI 150 8/27

8

Square of an odd integer

generic particular

Theorem: The square of any odd integer has the form $8k+1$ for some integer k.
Proof: Let n be any odd integer.
We must show that n^2 has the form $8k+1$ for some $k \in \boldsymbol{Z}$.
By definition, $\exists m \in \boldsymbol{Z}$ such that $n = 2m+1$. USE those definitions!
By the quotient-remainder theorem, $\exists q \in \boldsymbol{Z}$ such that n can be written as one of: $4q, 4q+1, 4q+2$, or $4q+3$. Because $4q$ and $4q+2$ are even, we need only show that n^2 has the form $8k+1$ for $4q+1$ and $4q+3$.
Case 1: $n = 4q+1$ for some $q \in \boldsymbol{Z}$.
Then $n^2 = 16\,q^2 + 8q + 1 = 8(2q^2+q)+1$. Let $k = (2q^2+q)$. Since $\boldsymbol{Z}$ is closed under addition and multiplication and $q \in \boldsymbol{Z}, k \in \boldsymbol{Z}$ and satisfies the condition.
Case 2: $n = 4q+3$ for some $\in \boldsymbol{Z}$.
Then $n^2 = 16\,q^2 + 24q + 9 = 8(2q^2+3q+1)+1$. Let $k = (2q^2+3q+8)$.
Since $\boldsymbol{Z}$ is closed under addition and multiplication and $q \in \boldsymbol{Z}, k \in \boldsymbol{Z}$ and satisfies the condition.
Thus the theorem is true regardless of which is the case.
QED

9

Preparation for an important theorem (1)

T23 (in Appendix A): If $a < b$ and $c < 0$, then $ac > bc$.
Lemma = proved statement that supports proof of a theorem

Absolute value $|x| = \begin{cases} x \text{ if } x \geq 0 \\ -x \text{ if } x < 0 \end{cases}$

generic particular

Lemma 1: For all $r \in \boldsymbol{R}, -|r| \leq r \leq |r|$. USE those definitions!
Let r be any real number. There are 2 cases: $r \geq 0$ and $r < 0$.
We must show that in both cases $-|r| \leq r \leq |r|$.
Case 1: $r \geq 0$. If so then by definition $|r| = r, -r < 0$ (by T23) and substitution into $-|r| \leq r \leq |r|$ asserts that $-r \leq r \leq r$ which is true.
Case 2: $r < 0$. If so then by definition $|r| = -r, -r \geq 0$ (by T23) and substitution into $-|r| \leq r \leq |r|$ asserts that $--r \leq r \leq -r \equiv r \leq r \leq -r$ by T23, which is true.
Thus the lemma is true regardless of which is the case.
QED

10

Preparation for an important theorem (2)

$|x| = \begin{cases} x \text{ if } x \geq 0 \\ -x \text{ if } x < 0 \end{cases}$

Lemma 2: For all $r \in \boldsymbol{R}, |-r| = |r|$

generic particular

Let r be any real number. There are 3 cases: $r > 0, r = 0$, and $r < 0$.

We must show that in all 3 cases $|-r| = |r|$. USE those definitions!

Case 1: $r > 0$. If so, then by definition of absolute value and by T23 $-r < 0, |-r| = - -r = r,$ and $|-r| = |r|$.

Case 2: $r = 0$. If so, then by definition $-r = 0, |-r| = |-0| = 0, |0| = 0$ and $|-r| = |r|$.

Case 3: $r < 0$. If so, then by definition of absolute value and by T23 $-r > 0, |-r| = - -r = r$, and $|-r| = |r|$.

Thus Lemma 2 is true regardless of which is the case.

QED

Fall 2023 CSCI 150 11/27

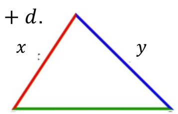
11

The triangle inequality

T26 (in Appendix A): If $a < c$ and $b < d$, then $a + b < c + d$.

Lemma 1: For all $r \in \boldsymbol{R}, -|r| \leq r \leq |r|$

Lemma 2: For all $r \in \boldsymbol{R}, |-r| = |r|$



Theorem: For all $x, y \in \boldsymbol{R}, |x + y| \leq |x| + |y|$

Proof: generic particulars

Let x, y be any real numbers. Then either $x + y \geq 0$ or $x + y < 0$.

We must show that in both cases $|x + y| \leq |x| + |y|$.

Case 1: $x + y \geq 0$. Then by definition of absolute value $|x + y| = x + y$ and by Lemma 1, $x \leq |x|$ and $y \leq |y|$.

Then by T26, $|x + y| = x + y \leq |x| + |y|$. USE those definitions!

Case 2: $x + y < 0$. Then by definition of absolute value $|x + y| = -(x + y) = -x - y$ and by Lemmas 1 and 2, $-|x| \leq x \leq |x|$ and $-|y| \leq y \leq |y|$. By T26, $|x + y| = -x - y \leq |x| + |y|$.

Thus the theorem is true regardless of which is the case.

QED

Fall 2023 CSCI 150 12/27

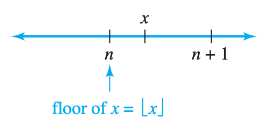
12

Today's outline

- ✓ Important proofs by cases
- Floors and ceilings
- Proofs by contradiction and contraposition

13

Definitions



Let $x \in \boldsymbol{R}$. Recall

- Floor $\lfloor x \rfloor$ of x is largest integer $\le x$

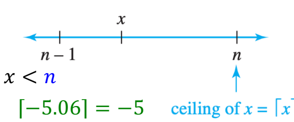
  If $\lfloor x \rfloor = n \in \boldsymbol{Z}$, $n \le x < n + 1$

  $\lfloor 3.1 \rfloor = 3$ $\lfloor 2.9999 \rfloor = 2$ $\lfloor -5.06 \rfloor = -6$

- Ceiling $\lceil x \rceil$ of x is smallest integer $\ge x$

  If $\lceil x \rceil = n \in \boldsymbol{Z}$, $n - 1 \le x < n$

  $\lceil 3.1 \rceil = 4$ $\lceil 2.9999 \rceil = 3$ $\lceil -5.06 \rceil = -5$



- For $k \in \boldsymbol{N}$, $\lfloor k \rfloor =?$
- For $k \in \boldsymbol{N}$, $\lceil k \rceil =?$
- For $k \in \boldsymbol{N}$, $\left\lfloor k + \frac{1}{2} \right\rfloor =?$
- For $k \in \boldsymbol{N}$, $\left\lceil k + \frac{1}{2} \right\rceil =?$

14

A proof about floors

Theorem: For all real numbers x and for all integers m, $\lfloor x+m \rfloor = \lfloor x \rfloor + m$

Proof: generic particulars

Let x be any real number and let m be any integer.

We must show that $\lfloor x+m \rfloor = \lfloor x \rfloor + m$. USE those definitions!

By definition of floor, for some $n \in \boldsymbol{Z}$, $n \le x < n+1$ and $n = \lfloor x \rfloor$.

Adding m throughout yields $n+m \le x+m < n+m+1$.

Because $\boldsymbol{Z}$ is closed under addition, $n+m \in \boldsymbol{Z}$ and $n = \lfloor x \rfloor$.

By substitution into $n+m \le x+m < n+m+1$,

$$\lfloor x \rfloor + m \le x+m < \lfloor x \rfloor + m + 1.$$

By definition of floor, $\lfloor x+m \rfloor = \lfloor x \rfloor + m$.

QED

15

Another proof about floors

Theorem: For any integer n, $\left\lfloor \frac{n}{2} \right\rfloor = \begin{cases} \frac{n}{2} \text{ if } n \text{ is even} \\ \frac{n-1}{2} \text{ if } n \text{ is odd} \end{cases}$ USE those definitions!

Proof: generic particular

Let n be any integer. By the quotient-remainder theorem, n is even or odd.

We must show that if n is even, $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n}{2}$ and if n is odd $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n-1}{2}$.

Case 1: n is even.

By definition of even, $\exists k \in \boldsymbol{N} \ni n = 2k$ and $\left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor \frac{2k}{2} \right\rfloor = \lfloor k \rfloor = k$ since $k \in \boldsymbol{N}$.

Case 2: n is odd.

By definition of odd, $\exists k \in \boldsymbol{N} \ni n = 2k+1$.

Because $k \in \boldsymbol{N}$, $\left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor \frac{2k+1}{2} \right\rfloor = \left\lfloor \frac{2k}{2} + \frac{1}{2} \right\rfloor = \left\lfloor k + \frac{1}{2} \right\rfloor = k$ and $k \le k + \frac{1}{2} < k+1$.

Since $\frac{n-1}{2} = \frac{2k+1-1}{2} = \frac{2k}{2} = k$, $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n-1}{2}$.

Thus the theorem is true regardless of which is the case.

QED

16

Another floor proof

Theorem: For any integer n and any positive integer d, if $q = \left\lfloor \frac{n}{d} \right\rfloor$ and $r = n - d\left\lfloor \frac{n}{d} \right\rfloor$ then $n = dq + r$ and $0 \le r < d$.

Proof: generic particulars

Let n be any integer, $d \in$ any positive integer, $q = \left\lfloor \frac{n}{d} \right\rfloor$ and $r = n - d\left\lfloor \frac{n}{d} \right\rfloor$.

We must show that $n = dq + r$ and $0 \le r < d$.

By substitution, $dq + r = d\left\lfloor \frac{n}{d} \right\rfloor + n - d\left\lfloor \frac{n}{d} \right\rfloor = n$ so $n = dq + r$.

Since $q = \left\lfloor \frac{n}{d} \right\rfloor$, $q < \frac{n}{d} < q + 1$, multiplying by d gives $dq < n < dq + d$ and subtracting dq yields $0 \le n - dq < d$.

Substituting $dq + r$ for n gives $0 \le dq + r - dq < d$ and $0 \le r < d$.

QED

Any questions?

Fall 2023 CSCI 150 17/27

17

Today's outline

- ✓ Important proofs by cases
- ✓ Floors and ceilings
- Proofs by contradiction and contraposition

Fall 2023 CSCI 150 18/27

18

Proof by contradiction skeleton

Theorem: If premises then conclusion.

Proof:

Assume: the conclusion is false.

We will show that this assumption logically leads to a contradiction.

…

Contradiction.

Because the assumption led to a contradiction, its negation is true.

QED

Fall 2023 CSCI 150 19/27

19

There is no greatest integer

Theorem: There is no greatest integer.

Proof:

Assume there is a greatest integer n.

We will show that this assumption logically leads to a contradiction.

By definition of $\boldsymbol{N}$, if $n \in \boldsymbol{N}$, $m = n + 1 \in \boldsymbol{N}$ and since $n + 1 > n$, $m > n$ and n is not the greatest integer.

USE those definitions!

Contradiction.

Because the assumption led to a contradiction, there is no greatest integer.

QED

Fall 2023 CSCI 150 20/27

20

No integer can be both even and odd

Theorem: No integer can be both even and odd.

Proof:

USE those definitions!

Assume there is some integer n that is both even and odd.

We will show that this assumption logically leads to a contradiction.

By definition of even, there is some $k \in \boldsymbol{N}$ such that $n = 2k$.

By definition of odd, there is some $l \in \boldsymbol{N}$ such that $n = 2l + 1$. It follows that $2k = 2l + 1, 2k - 2l = 1, and\ k - l = \frac{1}{2}$.

Since $\boldsymbol{N}$ is closed under subtraction, $k - l \in \boldsymbol{N}$ but $\frac{1}{2} \notin \boldsymbol{N}$.

Contradiction.

Because the assumption led to a contradiction, no integer can be both even and odd.

QED

Fall 2023 CSCI 150 21/27

21

Proof by contraposition skeleton

Theorem: $\forall x \in D$, if $P(x)$ then $Q(x)$.

Proof:

Consider the contrapositive: $\forall x \in D$, if $Q(x)$ is false then $P(x)$ is false.

We will show that the contrapositive is true.

Assume that for some $x \in D$, $Q(x)$ is false.

Show that this proves $P(x)$ is false

Because the assumption showed $P(x)$ is false, the contrapositive is true and the theorem is true..

QED

Fall 2023 CSCI 150 22/27

22

A proof by contraposition

Theorem: For all integers n, if n^2 is even then n is even.

Proof:

USE those definitions!

Consider the contrapositive: For all integers n, if n is odd then n^2 is odd.

We will show that the contrapositive is true.

Uses the generic particular too!

generic particular

Let n be any particular but arbitrarily chosen odd integer.

Then for some $k \in \boldsymbol{Z}, n = 2k + 1$ and
$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$
Because $2, k, 1 \in \boldsymbol{Z}$ and $\boldsymbol{Z}$ is closed under multiplication and addition, n^2 is an odd integer.
Because the assumption showed n^2 is odd, the contrapositive is true and the theorem is true..

QED

Fall 2023 CSCI 150 23/27

23

Proof by contradiction skeleton

Theorem: (copy the statement here)

Proof:

Assume: the negation of the conclusion

We will show that this assumption logically leads to a contradiction.

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

Contradiction. Because the assumption led to a contradiction, negation of the assumption.

QED

Fall 2023 CSCI 150 24/27

24

The same statement proved by contradiction

Theorem: For all integers n, if n^2 is even then n is even.

Proof:

USE those definitions!

Assume n^2 is even but n is odd.

We will show that this assumption logically leads to a contradiction.

Let $n \in \boldsymbol{Z}$ be an odd integer. Then by definition of odd, for some $k \in \boldsymbol{Z}$,

$n = 2k + 1$ and $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ and n^2 is odd.

Contradiction.

Because the assumption led to a contradiction, n is even.

QED

25

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

Proof by contradiction

Proof by contraposition

26

What you should know

More concepts support more proofs

- How to do proofs by cases, contradiction, contraposition
- The parity property
- The triangle property
- How to prove with floors, ceilings, primes

Any questions?

Next up: *Sequences and recursion*

Time to finish up that Opening sheet!

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

Fall 2023 CSCI 150 27/27

27