test #1: time/place → see course web site

coverage

September 5th → October 1st

- logic
- quantifiers
- proof
- number theory

form

- some short answer
- some proof/disproof

CSC165 fall 2019

Mathematical expression: contradiction, induction

Danny Heap
csc165-2019-09@cs.toronto.edu
BA4270 (behind elevators)
Web page:
http://www.teach.cs.toronto.edu/~heap/165/F19/
416-978-5899

Using Course notes: Proof

Computer Science
UNIVERSITY OF TORONTO

contradiction specializes contrapositive

$P_1 \wedge P_2 \wedge \cdots \wedge P_k \Rightarrow Q$

P_i — previously known facts

$\neg Q \Rightarrow \neg P_1 \vee \neg P_2 \vee \neg P_3 \vee \cdots \vee \neg P_k$

<u>technique</u> assume $\neg Q$

follow logical deductions, all valid, until I encounter some $\neg P_i$! → ← contradiction

Since $\neg Q$ leads to contradiction, Q is true.

infinitude of primes

Let $P = \{n : n \in \mathbb{N} \wedge \text{Prime}\}$.

Claim $|P| = \infty$. $\forall k \in \mathbb{N}, |P| \neq k$. Assume,

for sake of contradiction $\exists k \in \mathbb{N}, |P| = k$.

i.e. $P = \{p_1, p_2, p_3, \ldots, p_k\}$. Let

$m = p_1 \cdot p_2 \cdot p_3 \cdots p_k + 1$.   # $m = 2 \times 3 \times \cdots \times p_k + 1$

$m > 1$

$\exists p \in \mathbb{N}, \text{Prime}(p) \wedge p \mid m$ # CSC236 fact

$p \in P$ # $p = p_i$, some $1 \le i \le k$

$p \mid m - 1$

$p \mid 1 \cdot m - 1 \cdot (m-1)$ # linear combs

$p \mid 1 \rightarrow \Leftarrow$ contradiction!! # $p > 1$

Since assuming P finite leads to contradiction, P is infinite ∎

induction $\simeq$ "and so on..."

$7^n \equiv 1 \pmod 6$

$7^0 - 1 = 0 = 6 \times 0$ ✓

$7^1 - 1 = 6 = 6 \times 1$ ✓

$7^2 - 1 = 48 = 6 \times 8$ ✓

$7^3 - 1 = 342 = 6 \times 57$ ✓

$\vdots$

want to prove

$\forall n \in \mathbb{N}, 7^n \equiv 1 \pmod 6$

statements as dominoes

" all dominoes fall "

" turn the crank "

$7^0 \equiv 1 \pmod 6$ $7^1 \equiv 1 \pmod 6$ $7^2 \equiv 1 \pmod 6$ $7^3 \equiv 1 \pmod 6$ $7^4 \equiv 1 \pmod 6$ $7^5 \equiv 1 \pmod 6$ … "etc."

If domino n falls
so does domino
n+1

$7^0 \equiv 1 \pmod 6$ $7^1 \equiv 1 \pmod 6$ $7^2 \equiv 1 \pmod 6$ $7^3 \equiv 1 \pmod 6$ $7^4 \equiv 1 \pmod 6$ $7^5 \equiv 1 \pmod 6$ … "etc."

induction format

define convenient predicate

$P(n)$: ~~~ n ~~~, for $n \in \mathbb{N}$

do not ever, ever, ..., ever quantify n in definition.

- predicate
- base case — $P(0)$, show this.
- inductive step

$\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$

$P(0) \wedge$

conclude $\forall n \in \mathbb{N}, P(n)$