write test: pen, pencil, paint

CSC165 fall 2017

Mathematical expression: contradiction, induction

Danny Heap
csc16517f@cs.toronto.edu
BA4270 (behind elevators)
Web page:
http://www.teach.cs.toronto.edu/~heap/165/F17/
416-978-5899

Using Course notes: Proof

Outline

notes

contradiction specializes contrapositive

Theorem 2.3

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

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

often don't know which P_k matters, so follow our nose until the false comes out.

infinitude of primes

2, 3, 5, 7, 11,

<u>Claim</u> There are infinitely many primes

<u>Proof (by contradiction)</u>

Let $P = \{n \mid n \in \mathbb{N} \wedge Prime(n)\}$. Let $k \in \mathbb{N}$.
assume (for sake of contradiction) that $|P| = k$.
That is $P = \{p_1, p_2, \ldots, p_k\}$. Let $n = p_1 \times p_2 \times \cdots \times p_k + 1$
Since $n > 1$, there is a prime factor of n, let p
be such a prime factor $p \in P$, so $p \mid n-1$, also,
p divides n by construction. So $p \mid (n-(n-1)) = 1$.
Thus $p > 1 \wedge p \mid 1$ $\rightarrow\leftarrow$ contradiction.

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

$7^n \equiv 1 \pmod 6$

$7^0 - 1 = 1 - 1 = 0 = 0 \times 6$

$7^0 \equiv 1 \pmod 6$

$7^1 - 1 = 6 = 1 \times 6$

$7^1 \equiv 1 \pmod 6$

$7^2 \equiv 1 \times 1 = 1 \pmod 6$

$7^3 \equiv 7 \cdot 7^2 \equiv 1 \cdot 1 \pmod 6$

$7^4 \equiv 7 \cdot 7^3 \equiv 1 \cdot 1 \pmod 6$

turn the crank

go another step

dominoes

statements as dominoes

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

$7^0 - 1 = 0 \times 6$ ✓

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

induction format

$P(n)$: ~~~ n ~~~

never, ever, ... do: quantify n in predicate (or else)

- predicate
- base case — $7^0 - 1 = 6 \cdot 0$
- inductive step — $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$

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

$P(n): 6 \mid 7^n - 1$ — want to show $\forall n \in \mathbb{N}, P(n)$

Proof (mathematical induction)

base case $7^0 - 1 = 1 - 1 = 0 = 6 \times 0$. So $6 \mid 7^0 - 1$. So, $P(0)$ is true.

Inductive step: Let $k \in \mathbb{N}$. Assume $P(k)$, that is $\exists y_k \in \mathbb{N}, 7^k - 1 = 6y_k$ (def of $\mid$). Let y_k be such a value. Let $y_{k+1} = 7y_k + 1$.

Must show that $6 \mid 7^{k+1} - 1$.

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

Then

$$
\begin{aligned}
7^{k+1}-1 &= 7(7^k-1)+6 \\
&= 7(6y_k)+6 \quad \left(\text{by IH } P(k)\right) \\
&= 6(7y_k)+6 \\
&= 6(7y_k+1) \\
&= 6y_{k+1} \qquad \blacksquare
\end{aligned}
$$

discover, then prove sum of first n numbers result

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

$$n \quad n-1 \quad n-2 + \cdots + 2 + 1$$

$$n+1 + n+1 + \cdots \quad n+1 \to \frac{n(n+1)}{2}$$

– △ numbers $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

$P(n)$: "The sum of integers from 0 to n is $\frac{n(n+1)}{2}$"

discover, then prove sum of first n numbers result

Proof (math induction) | Try $Q(k) = P(k+1)$

base case $\sum_{i=0}^{0} i = 0 = \frac{0(0+1)}{2}$, so $P(0)$ is true ✓

Inductive step Let k be an arbitrary, fixed element of $\mathbb{N}$. Assume $P(k)$, that is $\sum_{i=0}^{k} i = \frac{k(k+1)}{2}$. Want to show $\sum_{i=0}^{k+1} i = \frac{(k+1)(k+2)}{2}$.

Then,

$$\sum_{i=0}^{k+1} i = \left(\sum_{i=0}^{k} i\right) + k+1$$

$$= \frac{k(k+1)}{2} + k+1 \quad \text{(by IH inductive Hypoth)}$$

$$=$$

discover, then prove sum of first n numbers result

$$\cdots = \frac{k(k+1) + 2(k+1)}{2}$$

$$= \frac{(k+2)(k+1)}{2} = \frac{(k+1)(k+2)}{2} \quad \blacksquare$$

discover, prove sum of first n cubes result

$0^3 = 0$

$0^3 + 1^3 = 1$

$0^3 + 1^3 + 2^3 = 9$

$0^3 + 1^3 + 2^3 + 3^3 = 36$

Claim

$P(n)$: $\sum_{i=0}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$

modular multiplication for more than pairs

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

Proof (induction)

base case $\sum_{i=0}^{0} i^3 = 0 = \left(\frac{0(0+1)}{2}\right)^2$. So $P(0)$ ✓

Inductive Step Let $k \in \mathbb{N}$. Assume the IH $P(k)$, that is: $\sum_{i=0}^{k} i^3 = \frac{k^2(k+1)^2}{4}$. Want to show $\sum_{i=0}^{k+1} i^3 = \frac{(k+1)^2(k+2)^2}{4}$.

modular multiplication for more than pairs

So,
$$\sum_{i=0}^{k+1} i^3 = \left[\sum_{i=0}^{k} i^3\right] + (k+1)^3$$

$$= \frac{k^2(k+1)^2}{4} + (k+1)^3 \quad (\text{by IH})$$

$$= \frac{k^2(k+1)^2 + 4(k+1)^3}{4}$$

$$= \frac{(k^2+4(k+1))(k+1)^2}{4}$$

$$= \frac{(k^2+4k+4)(k+1)^2}{4}$$

$$= \frac{(k+2)^2(k+1)^2}{4} \quad \blacksquare$$

$(k+2)^2$

k^2+4k+4

Notes

$$(k+1)^3 = k^3 + 3k^2 + 3k + 1$$

(binom Theorem)

(it turns out we won't need this ...)