CSC165 fall 2017

Mathematical expression: proofs

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

defining, unpacking

existential

universal

notes

$a \quad b$ and $Prime(p)$

statements packed and unpacked

"a divides b": "$\exists k \in \mathbb{Z}, b = ka$, write $a|b$". for $a, b \in \mathbb{Z}$

$\forall n \in \mathbb{N}, n|5 \Rightarrow n|10$

unpack:

$\forall n \in \mathbb{N}, (\exists k_1 \in \mathbb{Z}, 5 = k_1 n) \Rightarrow (\exists k_2 \in \mathbb{Z}, 10 = k_2 n)$

Prime(p): "$p > 1 \wedge \forall n \in \mathbb{N}, n|p \Rightarrow (n=1 \vee n=p)$", for $p \in \mathbb{N}$

unpack

Prime(p): "$p > 1 \wedge \forall n \in \mathbb{N}, (\exists k \in \mathbb{Z}, p = kn) \Rightarrow (n=1 \vee n=p)$" for $p \in \mathbb{N}$

prove 3 18

translate: $\exists k \in \mathbb{Z}, 3k = 18$

discuss: $k = 6$ should work...

proof

Let $k = 6$. # header introduces variables.

Then $3k = 3 \times 6 = 18$ # body, deduces result

There is a real solution to $x^2 + 2x + 3 = 11$

translate: $\exists x \in \mathbb{R}, x^2 + 2x + 3 = 11$

discussion 2 or -4 should work.

Proof Let $x = 2$ # header

Then $x^2 + 2x + 3 = 2^2 + 2 \cdot 2 + 3$

$= 11$ ∎

prove $n^2 + 2n + 5 > 4$ if $n \in \mathbb{N}$

translate: $\forall n \in \mathbb{N}, n^2 + 2n + 5 > 4$

discuss We can see that LHS is always $\geq 5 > 4$

Proof Let $n \in \mathbb{N}$ (arbitrary, fixed natural number)
header

Then $5 > 4$

$n^2 + n + 5 > 4$ # added non-neg amount to LHS

prove $n^2 - 5n > 7$ for most $n \in \mathbb{N}$

translate: $\forall n \in \mathbb{N}, n \geq 7 \Rightarrow n^2 - 5n > 7$

discuss: "for most" becomes "exclude $\{0,1,2,3,4,5,6\}$" after some trial-and-error

Proof Let $n \in \mathbb{N}$. Assume $n \geq 7$ # No need to consider
0,1,2,3,4,5,6 since
$F \Rightarrow ?$ always true

Then $n \geq 7$

$n - 5 \geq 2$

$n^2 - 5n = n(n-5) \geq 2n$ * hold this thought...

Also $n \geq 7$

$2n \geq 14$ **

$n^2 - 5n \geq 2n \geq 14 > 7$ combine * with ** prove $n \quad n+3 \Rightarrow n \quad 3$ for $n \in \mathbb{N}$

<u>translate</u> $\forall n \in \mathbb{N}, (\exists k_1 \in \mathbb{Z}, n+3 = k_1 n) \Rightarrow (\exists k_2 \in \mathbb{Z}, 3 = k_2 n)$

<u>discuss</u> it looks as if all we need is to find the right k_2

<u>want</u> $k_2 n = 3$

discovery direction

$$k_2 n + n = n+3 = k_1 n$$

$$k_2 n = k_1 n - n = (k_1 - 1) n$$

logic direction

use this direction in proof

<u>let $k_2 = k_1 - 1$</u>

we can do this already!

prove $n \quad n+3 \Rightarrow n \quad 3$ for $n \in \mathbb{N}$

Proof: Let $n \in \mathbb{N}$. Assume $\exists k_1 \in \mathbb{Z}$, $n+3 = k_1 n$.

Let k_1 be such a value. Let $k_2 = k_1 - 1$

Then
$$
\begin{aligned}
k_2 n &= (k_1 - 1) n \\
&= k_1 n - n \\
&= n + 3 - n \\
&= 3 \quad \blacksquare
\end{aligned}
$$

generalize $n \quad n + \overset{d}{\cancel{3}} \Rightarrow n \quad \overset{d}{\cancel{3}}$ for $n \in \mathbb{N}$

Insight: There was nothing special about 3 in the previous page. Any $d \in \mathbb{N}$ would work.

Go back and replace "$\forall n \in \mathbb{N}$" with "$\forall n, d \in \mathbb{N}$" and replace "3" with "d". Is the proof still valid?

if Prime(d), then we have

$$\forall n \in \mathbb{N},\ n \mid n+d \Rightarrow n \mid d \Rightarrow n = 1 \vee n = d \quad (\text{defn of Prime}(d))$$

e.g. $n \mid n+5 \Rightarrow n = 1 \vee n = 5$

$n \mid n+7 \Rightarrow n = 1 \vee n = 7 \ \ldots$

prove $m, n \equiv 1 \bmod 3 \Rightarrow mn \equiv 1 \bmod 3$

$a \equiv b \bmod c$: "$c \mid a-b$". For $a, b, c \in \mathbb{Z}$, $c \neq 0$

translate

$\forall m, n \in \mathbb{Z}, (\exists k_1 \in \mathbb{Z}, 3k_1 = m-1) \wedge (\exists k_2 \in \mathbb{Z}, 3k_2 = n-1)$
$\Rightarrow (\exists k_3 \in \mathbb{Z}, mn-1 = 3k_3)$

discuss We have expressions for m and n in terms of k_1 and k_2, so plug them into $mn-1$: $m = 3k_1+1$ $n = 3k_2+1$

$$
\begin{aligned}
mn-1 &= (3k_1+1)(3k_2+1)-1 \\
&= 9k_1k_2 + 3k_1 + 3k_2 + \underline{1-1} \\
&= 3\underbrace{(3k_1k_2 + k_1 + k_2)}
\end{aligned}
$$

let $k_3 =$

logic direction

prove $m, n \equiv 1 \bmod 3 \Rightarrow mn \equiv 1 \bmod 3$

Proof Let $m, n \in \mathbb{Z}$. assume $\exists k_1, k_2 \in \mathbb{Z}$, $3k_1 = m-1$ $\wedge$ $3k_2 = n-1$. Let k_1, k_2 be such values.

Let $k_3 = 3k_1k_2 + k_1 + k_2$.

Then $3k_3 = 9k_1k_2 + 3k_1 + 3k_2$

$= (3k_1+1)(3k_2+1) - 1$

$= mn - 1$ ∎

eg $m = 4$, $n = 10$ $\quad mn = 40 \wedge 3 \mid 40-1$

converse of previous example?

$$\forall m,n \in \mathbb{Z}, (\exists k_3 \in \mathbb{Z}, 3k_3 = mn-1)$$
$$\Rightarrow (\exists k_2 \in \mathbb{Z}, 3k_2 = m-1 \wedge \exists k_1 \in \mathbb{Z}, 3k_1 = n-1)$$

<u>False</u> e.g.

$m = 8$
$n = 11$) $3 \mid 88-1$ # $87 = 3 \times 29$

<u>But</u> $8 \equiv 2 \bmod 3$
$11 \equiv 2 \bmod 3$

...