Monday: 100% increase in office hours, i.e. 1-3 in BA2230...

CSC165 fall 2019

Mathematical expression: more proof, modularity, prime characterization

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

Using Course notes: Proof

linear combinations

$\forall a, b, c, p, q \in \mathbb{Z}, (a \mid b \wedge a \mid c \Rightarrow a \mid (bp + cq))$

discuss if b and c are mults of a, then re-write $bp + cq$ as sum of mults of a, and answer "falls out"

Proof Let $a, b, c, p, q \in \mathbb{Z}$. assume $\exists k_1, k_2 \in \mathbb{Z}$, $b = ak_1$, $c = ak_2$. WTS $\exists k_3 \in \mathbb{Z}$, $ak_3 = bp + cq$.

Let $k_3 = \underline{k_1 p + k_2 q}$.

$$
\begin{aligned}
bp + cq &= ak_1 p + ak_2 q \quad \text{\# assumed...} \\
&= a(k_1 p + k_2 q) \\
&= ak_3 \quad \blacksquare
\end{aligned}
$$

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

$\forall m, n \in \mathbb{Z}, 3 \mid (m-1) \wedge 3 \mid (n-1) \Longrightarrow 3 \mid (mn-1)$

discuss if $m = 3k_1 + 1$ (some k_1) and $n = 3k_2 + 1$ then $mn = 9k_1k_2 + 3k_1 + 3k_2 + 1$

so $mn - 1$ is divisible by 3.

Proof Let $m, n \in \mathbb{Z}$. Assume $\exists k_1, k_2 \in \mathbb{Z}$, $m = 3k_1 + 1 \wedge n = 3k_2 + 1$. Let $k_3 = 3k_1k_2 + k_1 + k_2$

WTS $k_3 \in \mathbb{Z} \wedge mn = 3k_3 + 1$

$mn = (3k_1 + 1)(3k_2 + 1) = 9k_1k_2 + 3k_1 + 3k_2 + 1$

$= 3k_3 + 1$ ■

also $k_3 \in \mathbb{Z}$, sums & mults of ints ...

converse of previous example?

$\forall m, n \in \mathbb{Z},\ 3 \mid (mn-1) \Rightarrow 3 \mid (m-1) \land 3 \mid (n-1)$

False: $\exists m, n \in \mathbb{Z},\ 3 \mid (mn-1) \land [3 \nmid (m-1) \lor 3 \nmid (n-1)]$

e.g. $m = n = 5$

$m, n \in \mathbb{N}^+$ and $m \mid n \Rightarrow m \leq n$

$\forall m, n \in \mathbb{N}^+, \; m \mid n \Rightarrow m \leq n$

discuss: since $m, n > 0$, then $\frac{n}{m} > 0$

and must be integer (assumption)

i.e. $n = km$

so $n/m \geq 1 \Rightarrow m \leq n$

Proof: Let $m, n \in \mathbb{N}^+$. Assume $\exists k \in \mathbb{Z}$,

$n = km$. WTS $m \leq n$.

$k = n/m$ # $m > 0$

$k > 0$ # $m, n > 0$

$k \geq 1$ # $k \in \mathbb{Z}$

$n = mk \geq m$ ■