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

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

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 \( \exists k_3 \in \mathbb{Z}, \)

Let \( k_3 = \frac{k_1 p + k_2 q}{a} \).

\( bp + cq = ak_1 p + ak_2 q \) \( \Rightarrow \)

\( = a(k_1 p + k_2 q) \)

\( = ak_3 \)
prove $m, n \equiv 1 \mod 3 \Rightarrow mn \equiv 1 \mod 3$

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

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

So $mn - 1$ is divisible by 3.

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

WTS $\exists k_3 \in \mathbb{Z}$ s.t. $mn = 3k_3 + 1$

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

$\Rightarrow 3k_3 + 1$

also $k_3 \in \mathbb{Z}$, sum of multis of ints...
converse of previous example?

\[ \forall m, n \in \mathbb{Z}, \, 3 \mid (mn - 1) \implies 3 \mid (m - 1) \land 3 \mid (n - 1) \]

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

E.g. \( m = n = 5 \)
\( m, n \in \mathbb{N}^+ \text{ and } m \mid n \Rightarrow m \leq n \)

\[ \forall m, n \in \mathbb{N}^+, \ m \mid n \Rightarrow m \leq n \]

discuss since m, n \geq 0, then \( \frac{n}{m} \geq 0 \)

and must be integer

i.e. \( n = km \) (assumption)

So \( n/m \geq 1 \Rightarrow m \leq n \)

Proof let \( m, n \in \mathbb{N}^+ \) assume \( \exists k \in \mathbb{Z}, \)

\[ n = km, \text{ WTS } m \leq n. \]

\[ k = \frac{n}{m} \]

\( m > 0 \)

\( k > 0 \)

\( k \geq 1 \)

\( k \in \mathbb{Z} \)

\[ n = m \cdot k \geq m \]