PS1: Have you looked at all the resources on Quercus?

- Group work advice & resources
- Academic Integrity reminder (in the announcement)

TT1: details page coming soon (this week)

Last time...

Prove: $\forall x \in \mathbb{Z},\ x \mid x+5 \Rightarrow x \mid 5$

Proof header

Let $x \in \mathbb{Z}$. Assume $x \mid x+5$, KNOW

in other words: $\exists k_1 \in \mathbb{Z},\ x+5 = k_1 \cdot x$

Note: From this point on, we can use k_1 in the proof.

WTS: $x \mid 5$, i.e., $\exists k_2 \in \mathbb{Z},\ 5 = k_2 \cdot x$

WANT

Let $k_2 = \underline{k_1 - 1}$ ← concrete value (constant or expression using constants or variables already introduced)

Then, $x+5 = k_1 \cdot x$

$\Rightarrow\quad 5 = k_1 \cdot x - x$

$\Rightarrow\quad \underline{5 = k_2 \cdot x}$ $\square$

ROUGH WORK — NOT part of proof

KNOW	WANT
$x \in \mathbb{Z}$	$k_2 = \underline{?}$
$\exists k_1 \in \mathbb{Z},\ x+5 = k_1 \cdot x$	$5 = k_2 \cdot x$

In general, proof = sequence of (deduction, <u>justification</u>) pairs.

- Every step <u>should</u> be justified, <u>except</u> simple algebra
- Justifications will be one of the following:

1 _ definitions
2 _ external facts } external

3 _ assumptions
4 _ previous deductions } internal

Note: proof above goes through (it is correct) with any integer d in place of 5

$\rightarrow$ proof of $\forall x, d \in \mathbb{Z},\ x \mid x+d \Rightarrow x \mid d$ (*)

Consider (1) $\forall x, p \in \mathbb{Z}^+, \text{Prime}(p) \wedge x \mid x+p \Rightarrow x=1 \vee x=p$

Recall: Prime(p): $p>1 \wedge \forall d \in \mathbb{Z}^+, d \mid p \Rightarrow d=1 \vee d=p$

Proof of (1):

Let $x, p \in \mathbb{Z}^+$. Assume Prime(p) and $x \mid x+p$. 3

Then, by 2 (*), $x \mid p$.

Then, by def. of Prime(p), 1

since 4 $x \mid p$, $x=1$ or $x=p$. $\square$

<u>EX:</u> Prove:

$$\forall d\in\mathbb{N}, \underbrace{\left(\forall a,b\in\mathbb{Z}, d\nmid a \wedge d\nmid b \Rightarrow d\nmid ab\right)}_{P} \Longrightarrow \underbrace{d\le 1 \vee \mathrm{Prime}(d)}_{Q}$$

<u>Idea 1:</u> direct proof

Let $d\in\mathbb{N}$. Assume $\forall a,b\in\mathbb{Z}, d\nmid a \wedge d\nmid b \Rightarrow d\nmid ab$

WTS: $\underline{d\le 1 \vee \mathrm{Prime}(d)}$ difficult, maybe even impossible...

<u>Idea 2:</u> <u>indirect proof</u>

("proof by contrapositive")

instead of proving $P\Rightarrow Q$

prove $\neg Q \Rightarrow \neg P$

$$\forall d \in \mathbb{N}, \ \boxed{\neg Q(d) \Rightarrow \neg P(d)}$$

$$\underline{\forall d \in \mathbb{N}, P(d) \Rightarrow Q(d)}$$

$$\forall d \in \mathbb{N}, \ d > 1 \wedge \neg Prime(d) \Rightarrow \exists a, b \in \mathbb{Z}, \ d \nmid a \wedge d \nmid b \wedge d \mid ab$$

Let $d \in \mathbb{N}$. Assume $d > 1$ and $\neg Prime(d)$

WTS $\exists a, b \in \mathbb{Z}, \ d \nmid a \wedge d \nmid b \wedge d \mid ab$

KNOW	WANT
$d \in \mathbb{N}$	$a = \underline{\ ?\ }$
$d > 1$	$b = \underline{\ ?\ }$
$\neg Prime(d)$	$d \nmid a$
	$d \nmid b$
	$d \mid ab$

$$\underbrace{\cancel{d \le 1}}_{\text{False}} \lor \underbrace{\exists k \in \mathbb{Z}^+, k \mid d \land k \neq 1 \land k \neq d}_{\text{must be True}}$$

$$\underline{\exists m \in \mathbb{Z}, d = k \cdot m}$$