PS1: check out all these resources (all on Quercus)

- TA office hours
- Group work advice & resources
- Read the announcements!
  (Especially "Problem Set 1 Information")

Last week...

- We proved $\forall x \in \mathbb{Z},\ x \mid x+5 \Rightarrow x \mid 5$
- In this proof, the constant 5 did not play a special role.
- So same proof with constant d in place of 5 proves the generalization

$$\forall x, d \in \mathbb{Z},\ x \mid x+d \Rightarrow x \mid d$$ (Fact 1)

Recall the definition of predicate Prime(p):
(where $p \in \mathbb{N}$)

$$p > 1 \wedge \left(\forall d \in \mathbb{Z}^+, \; d \mid p \Rightarrow d = 1 \vee d = p \right)$$

Variation:

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

Proof: Let $x, p \in \mathbb{N}$.

Assume Prime(p) and $x \mid x + p$.

By fact 1, we know $x \mid p$.
($x, p \in \mathbb{Z}$ and $x \mid x+p$ by assumption)
By definition of Prime(p),
$x \mid p \Rightarrow x = 1 \vee x = p$. □

Generally, in a proof, we have a sequence of (deduction, justification) pairs. The justifications fall into 4 categories:

- definitions } external
- external facts } external
- assumptions } internal
- previous deductions } internal

Example:

- True/~~False~~? $\forall a,b \in \mathbb{Z},\ 2 \nmid a \wedge 2 \nmid b \Rightarrow 2 \nmid ab$

  Proof? Exercise...

- Can we generalize?

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

  This is ~~false~~:

  $\neg \forall d,a,b \in \mathbb{Z},\ d \nmid a \wedge d \nmid b \Rightarrow d \nmid ab$

  $\exists d,a,b \in \mathbb{Z},\ \neg(d \nmid a \wedge d \nmid b \Rightarrow d \nmid ab)$

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

  pick $d=4,\ a=6,\ b=10$

Variation:

$\forall d \in \mathbb{N}$, $(\forall a, b \in \mathbb{Z}, d \nmid a \wedge d \nmid b \Rightarrow d \nmid ab)$

$\Rightarrow (d \leq 1 \vee \text{Prime}(d))$

Let's prove it!

- Direct proof? (assume hypothesis, try to prove conclusion)
  doesn't work...
- Indirect proof (proof by contrapositive)
  to prove $A \Rightarrow B$, prove $\neg B \Rightarrow \neg A$

Contrapositive:

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

Proof header:

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

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

KNOW

$d \in \mathbb{N}$

$d > 1$

$\neg \text{Prime}(d)$

$d \leq 1 \vee \exists k \in \mathbb{Z}^+, (k \mid d \wedge k \neq 1 \wedge k \neq d)$

must be True

$d \leq 1$ ↓ False

expanded: $\exists m \in \mathbb{Z}, d = km$

WANT

$a = \_\_?\_\_$

$b = \_\_?\_\_$

$d \nmid a$

$d \nmid b$

$d \mid ab$

DETAILS? ⇝ worksheet 7!