Last time...

Prove $\forall d \in \mathbb{N},\ Atomic(d) \Rightarrow Prime(d) \vee d \leq 1$

where

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

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

$\nmid$: does not divide

Note: $Atomic(d) \Rightarrow Prime(d) \vee d \leq 1$

$\equiv$ $\neg Atomic(d) \vee \neg(d > 1) \vee Prime(d)$

$\equiv$ $\neg(Atomic(d) \wedge d > 1) \vee Prime(d)$

$\equiv$ $d > 1 \wedge Atomic(d) \Rightarrow Prime(d)$

is logically equivalent to

Indirect proof: contrapositive

$\forall d \in \mathbb{N}, \neg Prime(d) \Rightarrow d \leq 1 \vee \neg Atomic(d)$

Proof header

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

WTS: $d \leq 1 \vee \neg Atomic(d)$

ROUGH WORK

KNOW

$d \in \mathbb{N}$

$\neg Prime(d)$

WANT

$d \leq 1 \vee \neg Atomic(d)$

expand definitions

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

$d \leq 1 \vee$
$\exists a, b \in \mathbb{Z}, d \nmid a \wedge d \nmid b \wedge d \mid ab$

Note: one assumption is a disjunction
$(d \leq 1 \vee \exists k \in \mathbb{Z}^+, \ldots)$

Proof by Cases

- When we know (assumption or definition or previous deduction or external fact) a statement of the form $A \vee B$
- Break up proof into cases

- Case 1: Assume A (no info about B)
  ... prove conclusion ... (about A)
- Case 2: Assume B (no info about A) same conclusion!
  ... prove conclusion ...
- Therefore, the conclusion holds (in all cases).

In this situation (back to example)

- Case 1: Assume $d \leq 1$
  Then, $d \leq 1 \vee \exists a,b \in \mathbb{Z}, d \nmid a \wedge d \nmid b \wedge d \mid ab$
- Case 2: Assume $\exists k \in \mathbb{Z}^+, k \mid d \wedge k \neq 1 \wedge k \neq d$
  Then, $k \neq 1$, $k \neq d$, $k \mid d$, i.e., $\exists m \in \mathbb{Z}, d = km$

WTS: $d \leq 1 \vee \exists a,b \in \mathbb{Z}, d \nmid a \wedge d \nmid b \wedge d \mid ab$

aim: prove the second half of the $\vee$

Let $a =$ _____

Let $b =$ _____

WTS: $d \nmid a$

$d \nmid b$

$d \mid ab$

WANT

$k \neq 1 \quad k \neq d$

$d = km$

$k \in \mathbb{Z}^+ \quad m \in \mathbb{Z}$

KNOW

DETAILS: worksheet #7 ...

What about converse of original statement?

$\forall d \in \mathbb{N}, \text{Prime}(d) \Rightarrow$ [$d > 1$] $\wedge$ [$\text{Atomic}(d)$]

WANTED

Proof header

Let $d \in \mathbb{N}$. Assume Prime(d).

KNOWN

By def., this means:

$d > 1 \wedge \forall k \in \mathbb{Z}^+, k \mid d \Rightarrow k = 1 \vee k = d$

W.T.S.: $\forall a, b \in \mathbb{Z}, d \nmid a \wedge d \nmid b \Rightarrow d \nmid ab$

Let $a, b \in \mathbb{Z}$. Assume $d \nmid a$ and $d \nmid b$

WTS: $d \nmid ab$

We require additional "tools" (facts)

Key idea: put the facts together to show

d is prime $\wedge$ $d \nmid a$

$\Rightarrow$ $\exists r_1, s_1 \in \mathbb{Z}$, $r_1 d + s_1 a = 1$