

Thm 1.5 Let p be an integer with $p \neq 0, \pm 1$. Then p is prime if and only if p has the property:

Whenever $p|bc$ then $p|b$ or $p|c$

Step 1 Let p be a prime number

So I know:
 $p \neq 0, \pm 1$

And if $d|p$ then $d = \pm 1$ or $d = \pm p$

Let $b, c \in \mathbb{Z}$ such that $p|bc$

so $bc = pr$ for some $r \in \mathbb{Z}$

~~Suppose $p|a$ p does not divide a~~

↑ didn't need it

Let $(p, b) = e$

$e|p$ $e|b$

$$e = pv + bu$$

either

$$e = \pm 1$$

$$\pm 1 = pv + bu$$

$$\pm c = cpv + cbu$$

$$\pm c = cpv + prv$$

$$\pm c = p(cv + ru)$$

$$p|c$$

or

$$e = \pm p$$

$$b = en$$

$$b = \pm p \cdot n$$

so

$$p|b$$

Suppose P is not prime

Let d be a divisor of p ,
 $p = dt$

then $p|dt$ ($p \cdot 1 = d \cdot t$)

Using the property:

Since $p|dt$, then

$p|d$ OR $p|t$

Since $p = dt$, $-p \leq d \leq p$

because $p|d$ $-d \leq p \leq d$

then $d = \pm p$

making $t = \pm 1$ (because $p = dt$)

CONTRADICTION \rightarrow Therefore p is prime