

Theorem

if p is prime

and $p \mid ab$

Then either $p \mid a$ or

$p \mid b$ (or possibly both)

Proof: if $p|a$, were done,

so assume $p \nmid a$, and

look $\gcd(p, b)$

only possibilities are $1, p$
since p is prime.

It can't be 1 (why?)
(see next slide)

$$\therefore \gcd(p, b) = p$$

So $p \mid b$.

BWOC
Suppose $\gcd(p, b) = 1$

Then $\exists s, t$ sth

$$sp + tb = 1$$

$$\Rightarrow asp + atb = a$$

but then $p|asp$ and $p|atb$ since
we know $p|ab$

thus $p|asptatb$, and so

$$p|a.$$

But we were assuming $p \nmid a$,
so this is a contradiction,
so our original statement
that $\gcd(p, b) = 1$ must
be false.

Theorem: P is prime.

if $p \mid a_1 a_2 \cdots a_r$ then

P divides a_i for at least one i .

Proof by induction on r .

Base case true when $r = 1$

(obvious).

true when $r = 2$ by the preceding theorem.

So now assume if

$p \mid a_1 \cdots a_{r-1}$ then p divides
at least one of a_i for
 $1 \leq i \leq r-1$.

and consider if

$$p \mid \underbrace{a_1 \cdots a_{r-1}}_A \cdot \underbrace{a_r}_B$$

this \Rightarrow $p \mid AB$

so by previous theorem

$$p \mid A \quad \text{or} \quad p \mid B$$

So $p \mid a_1 \dots a_{r-1}$ or $p \mid a_r$



or $p \mid a_r$

by induction

$p \mid a_i$ for at least
one i with $1 \leq i \leq r-1$

Thus $p \mid a_i$ for at least one i
with $1 \leq i \leq r$ ✓