Euclid's Lemma

Let p be a prime number and assume that p | ab where a, b $\in \mathbb{Z}$. Then, p | a or p | b.

Proof.

If p is prime, then the only numbers that divide p are p and 1.
Therefore, if p $\nmid$ a, then gcd(p, a) = 1.
Then by Bézout's identity, $\exists$ some s, t $\in \mathbb{Z}$ such that as + pt = 1.
Then b(1) = b(as + pt) = abs + ptb.
Now:
b = b * as + b * pt
Recall that p | ab and p | p
So, p | ab * s and p | p * tb
Thus, p | (abs + ptb)
Therefore, p | b

p $\nmid$ b $\Rightarrow$ p | a is similar.

Therefore, p | a or p | b

□