Notes about divisibility:

* if $d \mid a$ and $d \mid b$, then $d \mid a+b$.

"there exists"

Why? Since $d \mid a$, $\exists\, k \in \mathbb{Z}$ s.t. $a = dk$.
Since $d \mid b$, $\exists\, \ell \in \mathbb{Z}$ s.t. $b = d\ell$.

But then, $a+b = dk + d\ell = d(k+\ell)$.

But $k+\ell \in \mathbb{Z}$, b/c $k, \ell \in \mathbb{Z}$.

Then by defn of divisibility, $d \mid a+b$. ✓

* However, $d \mid a+b \not\Rightarrow d \mid a$ and $d \mid b$.

counterexample: $2 \mid 6$ but $2 \nmid 1$ and $2 \nmid 5$.
$6 = 1 + 5$

But, if $d \mid a+b$ and $d \mid a$, then $d \mid b$.

b/c $b = \underbrace{(a+b)} - \underbrace{a}$

apply *.

Euclid's Lemma Sps p is prime and $p \mid ab$. Then $p \mid a$ or $p \mid b$ (possibly both).

Remarks:

1. WARNING: not guaranteed to be true if p not prime.

   Ex $6 \mid \underset{3 \cdot 8}{24}$ but $6 \nmid 3$ and $6 \nmid 8$.

2. Sometimes this is how mathematicians define prime numbers.

proof of Euclid's lemma: Sps p prime and $p \mid ab$. Sps $p \nmid a$.

"need to show"
(NTS: $p \mid b$)

Since p is prime and $p \nmid a$, $\gcd(a, p) = 1$.

Thus, $1 = as + pt$ for some integers s, t.

Therefore $b = abs + pbt$. But since $p \mid ab$ and $p \mid p$, we have $p \mid abs$ and $p \mid pbt$. Therefore, $p \mid abs + pbt$, i.e. $p \mid b$. ✓

Fundamental Theorem of Arithmetic

Every integer greater than 1 is a prime or a unique product of primes. The only difference b/w two factorizations is the order in which primes appear.