You may use the following theorem for free on the homework. We strongly encourage you to understand the proof.

**Theorem** (Euclid's lemma)**.** *Assume that $p$ is prime. Assume $a, b \in \mathbb{Z}$ and $a > 1$ and $b > 1$. Assume $p \mid ab$ and $p \nmid a$. Then $p \mid b$.*

*Proof.* Integers $a$ and $b$ have prime factorizations. We express them as follows.

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$$
$$b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_n^{\beta_n}$$

Therefore, the prime factorization of $ab$ is a product of the $p_i$'s and the $q_j$'s (see Remark 1). Since $p \mid ab$, we have $kp = ab$ for some integer $k > 0$. Now the prime factorization of $kp$ contains the prime $p$ raised to an appropriate power (see Remark 1). Moreover, the prime factorization of $kp$ is unique. Therefore, $p$ must be equal to one of the primes in the prime factorization of $ab$. Since, $p \neq p_i$ for any $i$ (since $p \nmid a$), it follows that $p = q_j$ for some $j$. Therefore $p \mid b$. □

**Remark 1.**

1. *While the prime factorization of $ab$ is certainly a product of the $p_i$'s and the $q_j$'s, it is not necessarily equal to*
$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} q_1^{\beta_1} q_2^{\beta_2} \cdots q_n^{\beta_n}$$
*This is because $p_i$ may be equal to $q_j$ for some $i, j$. In that case, those terms can be combined.*

2. *If $k = 1$, then the prime factorization of $kp = p$. If $k > 1$, then $k$ has a prime factorization. Some of the primes in the prime factorization of $k$ may be $p$, hence the prime factorization of $kp$*
$$= \textit{ product of primes } \cdot p^t$$
*for some integer $t \geq 1$. Moral of the story, the prime factorization of $kp$ contains $p$.*