Euclid's Lemma

Euclid's Lemma says that primes divide separately, that is:
If a p prime divides an ab product then p divides at least one member. Formally:

$$p \mid ab \quad \rightarrow \quad p \mid a \quad \vee \quad p \mid b$$

The importance of this Lemma is that it easily proves the Fundamental Theorem of Arithmetic or Unique Prime Factorization Theorem. This claims that $P_1 P_2 \ldots P_M = Q_1 Q_2 \ldots Q_N$ equal prime products allow only same members except in other order. Now if this wasn't true then dividing both sides with P_1 if it's not on the other side then with P_2 if it's not there, and so on, we would get some remaining $p_1 p_2 \ldots p_m = q_1 q_2 \ldots q_n$ that have no common members at all. But Euclid's Lemma refutes such.
Indeed, for example p_1 must be dividing q_1 or $q_2 \ldots q_n$. In the first case p_1 is same as q_1 in the second it divides $q_2 \ldots q_n$ where we can repeat the argument and so finally we get that p_1 appears on the other side too.

The crucial step to prove Euclid's Lemma easily, is to see an other way what it says:
For any p prime, the set of those ab products where p divides neither a nor b but p divides ab, is an empty set. It is empty because if we form the same sets of ab products for general d numbers instead of p, then a claim is true about d that can not be true for primes.
This claim is that the minimal ab products in the sets are such that both a and b divide d.
Indeed, then since neither a nor b can be d or 1, already one dividing d means that d is composite.

We prove our claim about the minimal ab in two steps. First we show that if either member say b were bigger than d then we had a smaller b' so that the new smaller ab' is similar as ab. Then that if b is smaller than d but it wouldn't divide d then again we had a smaller b'.
For the first case our b' is quite simply $b - d$. Indeed, $ab' = a(b - d) = ab - ad$ is again dividable by d. But b' is still not. In the second case it's not enough to subtract b from d because the result wouldn't necessarily be smaller than b. We have to subtract it as many m times it is possible, in other words we must form the $d - mb = b'$ remainder.
Then $ab' = a(d - mb) = ad - amb$ so is again dividable by d. But b' itself is not.

Surprisingly, we can avoid Euclid's Lemma and refute prime factorizations with members not appearing on the other side in an other way too.
The trick is to regard the first such $F = p_1 p_2 \ldots p_m = q_1 q_2 \ldots q_n$.
Changing sides we can assume $p_1 < q_1$. Then replacing q_1 in the right side with p_1, it becomes $p_1 q_2 \ldots q_n < F$, so we can subtract it from both decompositions:
$p_1 p_2 \ldots p_m - p_1 q_2 \ldots q_n = q_1 q_2 \ldots q_n - p_1 q_2 \ldots q_n$. So :
$p_1 (p_2 \ldots p_m - q_2 \ldots q_n) = q_2 \ldots q_n (q_1 - p_1)$
Decomposing the bracketed numbers into primes too, we get prime factorizations of both sides:

$$p_1 r_1 \ldots r_j = q_2 \ldots q_n s_1 \ldots s_k$$

These two prime factorizations are of a smaller than F number so should be mere rearrangements. We show that this is not the case, proving that F couldn't exist at all!
Indeed, p_1 appears on the left but it can not on the right. Because the q-s were all different by assumption and the s-s all divide $q_1 - p_1$ while p_1 can not because it doesn't divide q_1.