Euclid’s little lemma: book 7 proposition 30

**Lemma.** $p$ prime, $x, y$ integer, $p | xy \implies p | x$ or $p | y$.

**Proof.** It suffices to prove for the case when $x, y \geq 0$. The cases where $x$ or $y$ are negative follow by multiplying by $-1$.

Argue by induction on $p$. Base case ($p$): let $p = 2$. Then exists $t$, $xy = pt = 2t$. The product of two odd numbers is odd, so at least one of $x, y$ is not odd, so the lemma holds.

Inductive hypothesis ($p$): let $p > 2$ and assume that the lemma holds for all smaller primes.

Now argue by induction on $xy$. Base case ($xy$): let $xy = 0$. Then at least one of $x, y$ — say $x$ — is 0. $x = 0 = 0p$, so $p | x$, so the lemma holds.

Inductive hypothesis ($xy$): let $xy > 0$ and assume that the lemma holds for $p$ and all smaller values of $xy$.

$p | xy$, so exists $t$, $pt = xy$. Exists $q_x, r_x$ so that $x = pq_x + r_x$, $0 \leq r_x < p$. Exists $q_y, r_y$ so that $y = pq_y + r_y$, $0 \leq r_y < p$.

If $q_x > 0$ then $pt = (pq_x + r_x)y$, so $p(t - qxy) = r_xy$ where $r_x = x - pq_x < x$. So $p | r_xy$, and by hypothesis ($xy$) the lemma holds for $p, r_x, y$, so either $p | y$, and we are done, or $p | r_x$, in which case $p | (r_x + pq_x = x)$, and we are done.

By a similar argument, if $q_y > 0$ then we are done.

So now assume that $q_x = q_y = 0$. Thus $x = r_x < p$, $y = r_y < p$, and since $pt = xy$ we must have $t < p$. Also, $t \neq 1$, for otherwise $p = xy$ and prime $p$ has nontrivial factors $x, y$, contradiction.

So $t \geq 2$, so $t$ has a prime factor $s \leq t < p$, say $t = sv$. Now $pt = psv = xy$, so $s | xy$ and, by hypothesis ($p$), the lemma holds for $s, x, y$, so $s | x$ or $s | y$. By relabelling $x, y$ if necessary, assume that $s | x$, say $sw = x$.

Now $pt = psv = xy = swy$, so $pv = wy$ where $w < x$. By hypothesis ($xy$), the lemma holds for $p, w, y$, so either $p | y$ and we are done, or $p | w$, in which case $p | ws = x$ and we are done.

Thus, by induction on $p$, and then $xy$, the lemma holds. \qed