A SOLUTION TO 5.4(C) WITHOUT PRIME FACTORIZATION

I will use a lemma which appears as Exercise 7.1 in the book. The location of that exercise in Chapter 7 may make you think you *have* to prove it using prime factorization. You do not.

Lemma. *If* $\gcd(a,b)=1$ *and* $a \mid bc$ *then* $a \mid c$.

Proof of the Lemma. By Bézout's Identity, we can find $x, y \in \mathbb{Z}$ such that $ax+by=1$. Multiply both sides by c, obtaining $a(cx)+(bc)y=c$. By hypothesis, $a \mid bc$, so we can find $q \in \mathbb{Z}$ such that $aq=bc$. By substitution, then, $a(xc)+(aq)y=c$. The left side factors as $a(xc+qy)=c$. By definition, $a \mid c$. □

Exercise. Show that for any natural numbers m, n we have $mn = \gcd(m,n)\operatorname{lcm}(m,n)$.

Proof of the Exercise. For convenience, write $g=\gcd(m,n)$ and $\ell=\operatorname{lcm}(m,n)$. Choose a,b,c,d such that $m=ag$, $n=bg$, $\ell=cm$, and $\ell=dn$.

First we claim that $\gcd(a,b)=1$. By Bézout's Identity, there exist $x,y \in \mathbb{Z}$ such that $mx+ny=g$. Rewrite this as $(ag)x+(bg)y=g$, and divide to obtain $ax+by=1$. Bézout's Identity states that the $\gcd(a,b)$ is the smallest natural that can be written in that form, and 1 is the smallest natural, period, so $\gcd(a,b)=1$, as claimed.

Next we claim that $ac=bd$. Recall that $cm=\ell=dn$. By substitution

$$c(ag)=d(bg). \tag{1}$$

Dividing show that $ac=bd$, as claimed.

We have $ac=bd$, but also $\gcd(a,b)=1$. By the Lemma above, $a \mid d$ and $b \mid c$. Choose q, r such that $d=aq$ and $c=br$. Substitute into 1, obtaining $(br)(ag)=(aq)(bg)$. Division gives us $r=q$.

We claim $\gcd(q,r)=1$. To see why, let $s=\gcd(q,r)$. Recall that q and r divide c and d, so s also divides c and d. Recall that $cm=\ell=dn$, or $cm=dn$; if $s \neq 1$, we could divide both sides by s, obtaining a *smaller* common multiple of m and n. This would contradict the definition of ℓ as the *least* common multiple, so it must be that $1=s=\gcd(q,r)$, as claimed.

We have $r=q$ and $\gcd(q,r)=1$. This is possible only if $r=q=1$. By substitution, $\ell=cm=(br)(ag)=abg$.

Again by substitution, $g\ell=g(abg)=(ag)(bg)=mn$, as claimed. □