Some comments on the recent homework.

7.6 # 7. Let m, n be positive integers with $n \mid m$. Prove that the natural surjective ring projection $\phi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is also surjective on the units: $\phi^* : (\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$.

Students suggested several good options for solutions. Notice that the problem says, in fact, that the *group* homomorphism $\phi^* : (\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$ is well-defined and surjective. We should comment that the ring homomorphism ϕ is well-defined: If $\bar{x} = \bar{x}' \in \mathbb{Z}/m\mathbb{Z}$, then $x = x' + mk$ for some integer k. Moreover, $\phi(\bar{x}) = x \mod n$ and $\phi(\bar{x}') = x' \mod n \equiv (x + km) \mod n \equiv x \mod n = \phi(\bar{x})$.

Notice also that the group homomorphism ϕ^* is also well-defined by a problem from your homework (7.3 # 17) which proves that $\phi^*\big((\mathbb{Z}/m\mathbb{Z})^*\big) \subseteq (\mathbb{Z}/n\mathbb{Z})^*$. It remains to prove that the map ϕ^* is surjective: if $\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^*$, then there exists an element $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^*$ with $\phi^*(\bar{a}) = \bar{x}$.

Here is one solution for this problem:

Solution: Let $\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^*$. Assume first that if p is a prime dividing m, then $p \mid n$ too. That is, assume if p prime, $p \mid m \implies p \mid n$. Now since $\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^*$, x and n are relatively prime, i.e. $(x, n) = 1$. However, since n and m have exactly the same prime divisors, we have that $(x, m) = 1$ too. Thus, taking $\bar{a} = \bar{x} \in (\mathbb{Z}/m\mathbb{Z})^*$, then $\phi^*(\bar{a}) = \bar{x} \in (\mathbb{Z}/n\mathbb{Z})^*$ since $n \mid m$.

Now assume that there is at least one prime q such that $q \mid m$, but $q \nmid n$. Factor m so that $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r} Q$, where each prime $p_i \mid n$, but for each prime q_j with $q_j \mid Q$, we have $q_j \nmid n$. Notice that Q and n are relatively prime.

By the Chinese Remainder Theorem, there exists an integer $a \in \mathbb{Z}$ so that

$$\begin{aligned} a &\equiv x \mod n, \\ a &\equiv 1 \mod Q. \end{aligned}$$

Consider $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})$ and notice $\phi(\bar{a}) = \bar{x}$ by the first equivalence. Notice further that if p is any prime with $p \mid m$, then p must divide either n or Q. Moreover, if $p \mid n$, then $p \nmid a$ by the first congruence, and if $p \mid Q$, then $p \nmid a$ by the second congruence. We conclude that $(a, m) = 1$ and so $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^*$. Thus, the map ϕ^* is surjective. $\square$