This week not all problems are in the book.

(i) Do problems 27, 28, 29 and 30 of Section 20.

(ii) **The groups** $G_n$.

Let $G_n \subset \mathbb{Z}/(n)$ denote the set of integers modulo $m$ that are relatively prime to $n$. Its order is $\varphi(n)$.

1. Prove that if $m$ and $n$ are relatively prime, then $G_{mn} = G_m \times G_n$.
2. Prove that $G_{2^k}$ for $k \geq 2$ is isomorphic to $C_2 \times C_{2^{k-2}}$.
3. Prove that for an odd prime $p$, $G_{p^k}$ for $k \geq 1$ is isomorphic to $C_{p-1} \times C_{p^{k-1}}$.
4. The above three statements determine the structure of $G_n$ for all $n > 0$.

Make a table of the structures of $G_n$ for $n \leq 30$. (The answer to problem 20.7 is in the back of the book, and it shows the order of each group.)

5. The following statements were proved in class.

- If an integer $a$ is not divisible by 2 or 3, then $a^2$ is congruent to one modulo 24.
- If an integer $a$ is not divisible by 2, 3 or 5, then $a^4$ is congruent to one modulo 240.

Find and prove the best possible congruence of the same type for sixth powers. It should say that if $a$ is not divisible by certain primes, then $a^6$ is congruent to one modulo a certain number $n$, which is product of powers of those primes. The number $n$ should be as largest integer for which this is true.

6. Do the same for 8th powers.

(iii) Do problems 2, 12, 13, 14, 16 of Section 21.