On the multiplicative group mod n
MAT347

Let n be a positive integer. Let us call U_n the group of invertible elements mod n. In other words:

$$U_n := (\mathbb{Z}/n\mathbb{Z})^\times$$

with operation product. Things you already know (and you can prove):

1. Aut $Z_n \cong U_n$ and you know what the explicit isomorphism is.
2. $|U_n| = \varphi(n)$, the Euler function of n.
3. If p is a prime and $m \geq 1$, then $\varphi(p^m) = p^m - p^{m-1}$.

Here are some results that we will be able to prove in Chapter 9 (without using any extra group theory) but which will be useful now. You are welcome to use any of these without proof in your classifications of finite groups:

4. If p is prime, then U_p is cyclic.
5. More generally, if p is an odd prime and $m \geq 1$, then U_{p^m} is cyclic.
6. If a and b are relatively prime, then $U_{ab} \cong U_a \times U_b$.