Handout for Section 8.2 (part 2)

1. Read Example 8.3 that shows how to find all integers with order 6 modulo 31.

   We know there are 4 \phi(6)=2 such integers \equiv 6 \mod 6. To find these integers, we will first find a primitive root \equiv 1 \mod 31.

   There are \phi(\phi(31))=\phi(30)=8 primitive roots \equiv 1 \mod 31.

   Finding one by trial and error: Since \(2^5 \equiv 1 \mod 31\),

   2 cannot be a primitive root \equiv 1 \mod 31.

   How about 3?

   We need to show \(3^k \equiv 1 \mod 31\) for \(k=\phi(31)=30\), \& \(k<30\) i.e., \(k=1,2,3,5,6,10,15\).

   & then show that \(3^{30} \equiv 1 \mod 31\) which is true by Fermat.

   It turns out 3 is a primitive root \equiv 1 \mod 31.

   Now, to find integers of order 6 modulo 31, we need to look in the set of integers less than 31 that are coprime to 31. By Thm. 8.4, this set is given by \(\{3, 3^2, 3^3, \ldots, 3^{30}\}\).

   Now, \(\text{ord}_{31}(3^k) = \text{ord}(3) = \frac{30}{\gcd(k, \phi(31))} = \frac{30}{\gcd(k, 30)}\)

   This equals 6 if \(\gcd(k, 30)=5\), i.e., \(k=5 \& 25\).

   So, \(3^5 \equiv \ldots \equiv 26 \mod 31\) \& \(3^{25} \equiv \ldots \equiv 6 \mod 31\) are the only integers having order 6 modulo 31.

2. Now, use the same method to find all positive integers less than 61 that have order 4 modulo 61.
   (Hint: 2 is a primitive root \equiv 1 \mod 61)