Solutions 3

\#1 Find a primitive root modulo 17.

It is always reasonable to test 2 as a candidate first. By Fermat’s little theorem and by Lagrange’s theorem, 
\(2^d = 1 \mod 17\) is possible only for divisors \(d\) of \(17 - 1\). That is, if 2 is not a primitive root then one of 
\(2^1, 2^2, 2^4, 2^8\) will be 1 \(\mod 17\), and vice-versa. Computing: \(2^1 = 2 \neq 1, 2^2 = 4 \neq 1, 2^4 = 16 = -1 \neq 1,\) and 
then \(2^8 = (2^4)^2 = (-1)^2 = 1\). Thus, 2 is not a primitive root \(\mod 17\).

Then try 3 as candidate: \(3^1 = 3 \neq 1, 3^2 = 9 \neq 1, 3^4 = (3^2)^2 = 81 = 13 \neq 1, 3^8 = (3^4)^2 = 13^2 = 169 = 16 \neq 1\). So, by Fermat’s little theorem and Lagrange’s theorem, the order of 3 must be 16, so 3 is a primitive root \(\mod 17\).

\#2 Show that \(f(x) = x^3\) is a homomorphism \(\mathbb{Z}/7^\times \to \mathbb{Z}/7^\times\).

What must be checked is that \(f(xy) = f(x)f(y)\). In the present example,

\[
\begin{align*}
f(xy) &= (xy)^3 = x^3y^3 \quad \text{(because } \mathbb{Z}/7^\times \text{ is abelian)} \\
&= f(x) \cdot f(y)
\end{align*}
\]

Thus, this \(f\) is a homomorphism.

\#3 What is the kernel of the homomorphism in \#2?

The kernel \(\ker f\) of the homomorphism \(f\) from \#2 is, by definition,

\[
\ker f = \{g \in \mathbb{Z}/7^\times : f(g) = 1\}
\]

In this very small example we may as well use brute force: \(1^3 = 1\), so 1 is in the kernel. \(2^3 = 1\), so 2 is in 
the kernel. \(3^3 = 6\), so 3 is not in the kernel. \(4^3 = 1\), so 4 is in the kernel. \(5^3 = 6\), so 5 is not in the kernel. 
And \(6^3 = 6\), so 6 is not in the kernel. Thus, \(\ker f = \{1, 2, 4\}\).