Homework 30 Solutions

1. (a) **Find a multiplicative generator for arithmetic** (mod 17)**.**

   The only method we've discussed for finding generators is trial and error. Fortunately, 17 is a relatively small number, so that shouldn't be too hard. We start by trying 2. We have

   $$2^2 \equiv 4$$
   $$2^3 \equiv 8$$
   $$2^4 \equiv 16 \equiv -1$$

   where all of these equivalences are taken (mod 17). This means that $2^8 \equiv 1 \pmod{17}$, so 2 can't be a generator. Next we try 3. We have

   $$3^2 \equiv 9 \qquad 3^6 \equiv 15$$
   $$3^3 \equiv 27 \equiv 10 \qquad 3^7 \equiv 45 \equiv 11$$
   $$3^4 \equiv 30 \equiv 13 \qquad 3^8 \equiv 33 \equiv 16$$
   $$3^5 \equiv 39 \equiv 5$$

   where all of these equivalences are taken (mod 17). At this point, we can conclude that $\boxed{3}$ is a generator. The reason is that we know the next 8 powers of 3 are just the negatives of the numbers we've computed above. Hence the first time that a power of 3 is congruent to 1 is $3^16 \equiv 1 \pmod{17}$. As discussed in lecture, this means that 3 is a generator.

   (b) **How many numbers** (mod 17) **have a cube root (note: you don't have to list these numbers, just say how many there are), and how many cube roots does each such number have?**

   We see that 3 is relatively prime to $16 = 17 - 1$. Therefore, our "old" method of using Euler's theorem to find an x such that $a^{1/3} \equiv a^x \pmod{17}$. Since this method works for all non-zero a, we conclude that every number has a cube root (mod 17). Further, we know that this method always gives unique roots, so we can conclude that every number has exactly one cube root (mod 17). (We are ignoring zero, since it always has just one root, namely itself.)

   (c) **How many numbers** (mod 17) **have a 4th root (note: you don't have to list these numbers, just say how many there are), and how many 4th roots does each such number have?**

   In this case, 4 divides 16, so our "old" method certainly doesn't apply. Instead, we know that 3 is a generator. Therefore, we know that 3^4, 3^8, 3^{12}, and 3^{16} all have 4th roots. Consider 3^4. We know that one 4th root is 3, and we can find others by adding multiples of 4 to the exponent (because $4 \cdot 4 = 16$, so taking the 4th power will still gives 3^4, by Fermat's theorem). So 3, 3^5, 3^9, and 3^13 are all 4th roots of 3^4. Moreover, the same idea allows us to find four 4th roots for 3^8, 3^{12}, and 3^{16}. This means that each of these 4 numbers has four 4th roots. Finally, we see that this accounts for all 16 non-zero numbers (mod 17), and thus there can't be any more fourth roots. We conclude that there are 4 numbers which have 4th roots (mod 17), and that each of these numbers has exactly four 4th roots. (Again, we ignore zero.)

2. **Exactly one of the numbers 2, 3, 5 is a multiplicative generator** (mod 31)**. Which is it?**

   We know that $2^5 = 32$, and therefore $2^5 \equiv 1 \pmod{31}$. So 2 can't be a generator. Similarly, we have that

   $$5^3 \equiv 125 \equiv 1 \pmod{31},$$

so cannot be a generator. By process of elimination, we must have that $\boxed{3}$ is a generator.

Of course, this relies on us believing the question when it asserts that one of these numbers is a generator. If we wish to confirm that 3 is a generator, we can compute that

$$\begin{aligned}
3^2 &\equiv 9 & 3^9 &\equiv -33 \equiv -2 \\
3^3 &\equiv 27 \equiv -4 & 3^{10} &\equiv -6 \\
3^4 &\equiv -12 & 3^{11} &\equiv -18 \equiv 13 \\
3^5 &\equiv -36 \equiv -5 & 3^{12} &\equiv 39 \equiv 8 \\
3^6 &\equiv -15 & 3^{13} &\equiv 24 \equiv -7 \\
3^7 &\equiv -45 \equiv -14 & 3^{14} &\equiv -21 \equiv 10 \\
3^8 &\equiv -42 \equiv -11 & 3^{15} &\equiv 30 \equiv -1
\end{aligned}$$

where all of these equivalences are taken (mod 31). At this point, we can conclude that 3 is a generator, by the same reasoning as in problem 1 a).