Homework 23 Solutions

1. **The method we have used for computing roots** $\pmod n$ **can be applied to only part (c) of the following three problems. Explain why it fails for the first two problems, and solve the third.**

   (a) **The 4th root of** $4 \pmod{77}$**;**
   Since $77 = 11 \cdot 7$, we see that $\phi(77) = (11-1)(7-1) = 60$. It's clear that 4 and 60 are not relatively prime, and thus our method does not apply. (More specifically, we won't be able to solve $4x + 60y = 1$.)

   (b) **The 7th root of** $7 \pmod{77}$**;**
   In this case, 7 and 77 are not relatively prime, and our method does not apply. (In particular, Euler's theorem doesn't apply, and that's the whole basis of our approach.)

   (c) **The 13th root of** $13 \pmod{77}$**.**
   Here we see that 60 and 13 are relatively prime, as are 13 and 77, so our method will apply. We begin with the Euclidean algorithm:

$$\begin{aligned} 60 &= 4 \cdot 13 + 8 \\ 13 &= 8 + 5 \\ 8 &= 5 + 3 \\ 5 &= 3 + 2 \\ 3 &= 2 + 1 \end{aligned}$$

   Running it backwards, we have

$$\begin{aligned} 1 &= 3 - 2 \\ 1 &= 3 - (5-3) = -5 + 2 \cdot 3 \\ 1 &= -5 + 2(8-5) = 2 \cdot 8 - 3 \cdot 5 \\ 1 &= 2 \cdot 8 - 3(13-8) = -3 \cdot 13 + 5 \cdot 8 \\ 1 &= -3 \cdot 13 + 5(60 - 4 \cdot 13) = 5 \cdot 60 - 23 \cdot 13 \end{aligned}$$

   So we see that $13^{1/13} \equiv 13^{-23} \equiv 13^{37} \pmod{77}$. We could use successive squaring to evaluate $13^{37} \pmod{77}$, but in this case using the Chinese remainder theorem works well. Recalling that $7 = 11 \cdot 7$, we first need to compute $13^{37} \pmod{11}$ and $13^{37} \pmod 7$. Note that, by Fermat's theorem, $13^{37} \equiv 13^7 \pmod{11}$. We have that

$$\begin{aligned} 13 &\equiv 2 \pmod{11}, \\ 13^2 &\equiv 4 \pmod{11}, \\ 13^4 &\equiv 5 \pmod{11}, \\ 13^7 &\equiv 13^4 \cdot 13^2 \cdot 13 \equiv 5 \cdot 4 \cdot 2 \equiv 7 \pmod{11}. \end{aligned}$$

   Thus $13^{37} \equiv 7 \pmod{11}$. On the other hand, $13^{37} \equiv -1^{37} \equiv -1 \equiv 6 \pmod 7$. Next we need to find $x \pmod{77}$ such that $x \equiv 7 \pmod{11}$ and $x \equiv 6 \pmod 7$. This is the same as saying that $x = 7 + 11y$ and $x = 6 + 7z$ for some numbers y and z. Setting these equal, we want to solve $7 + 11y = 6 + 7z$, which simplifies to $11(-y) + 7z = 1$. Since the multiples of 11 are easy to compute, it's not too hard to guess a solution, namely $-y = -5,\ z = 8$. (Of course, the Euclidean algorithm would also work.) Plugging this back into our equations for x, we see that $13^{37} \equiv x \equiv \boxed{62} \pmod{77}$.

2. (a) **Compute** $3^{917} \pmod{140}$**.**

We start by noting that $140 = 14 \cdot 10 = 2^2 \cdot 5 \cdot 7$. Applying our method for computing ϕ gives

$$\phi(140) = 140 \cdot \frac{1}{2} \cdot \frac{4}{5} \cdot \frac{6}{7} = 2^2 \cdot 5 \cdot 7 \cdot \frac{1}{2} \cdot \frac{4}{5} \cdot \frac{6}{7} = 2 \cdot 4 \cdot 6 = 48.$$

Since 3 and 140 are relatively prime, Euler's theorem allows us to write $3^{917} \equiv \left(3^{48}\right)^{19} \cdot 3^5 \pmod{140}$. Finally, $3^5 \equiv 243 \equiv \boxed{103} \pmod{140}$.

(b) **Compute** $4^{1125} \pmod{105}$**.**

We see that $105 = 3 \cdot 5 \cdot 7$, and thus

$$\phi(105) = 105 \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot 67 = 2 \cdot 4 \cdot 6 = 48.$$

Since 4 and 105 are relatively prime, Euler's theorem allows us to write $4^{1125} \equiv \left(4^{48}\right)^{23} \cdot 4^{21} \pmod{105}$. Then we compute

$$\begin{aligned} 4^2 &\equiv 16 \\ 4^4 &\equiv 256 \equiv 46 \\ 4^8 &\equiv 2116 \equiv 16 \\ 4^{16} &\equiv 46 \end{aligned}$$

where all of these congruences are $\pmod{105}$. Thus,

$$4^{21} \equiv 4^{16} \cdot 4^4 \cdot 4 \equiv 46 \cdot 46 \cdot 4 \equiv 16 \cdot 4 \equiv \boxed{64} \pmod{105}.$$

3. **Find a number** x **such that** $x \equiv 3 \pmod{11}$ **and** $x \equiv 5 \pmod{15}$**.**

These two congruences are equivalent to requiring that $x = 3 + 11y$ and $x = 5 + 15z$ for some numbers y and z. Setting these equal gives $3 + 11y = 5 + 15z$, which simplifies to $11y + 15(-z) = 2$. The Euclidean algorithm gives

$$\begin{aligned} 15 &= 11 + 4 \\ 11 &= 2 \cdot 4 + 3 \\ 4 &= 3 + 1. \end{aligned}$$

Running it backwards gives

$$\begin{aligned} 1 &= 4 - 3 \\ 1 &= 4 - (11 - 2 \cdot 4) = -11 + 3 \cdot 4 \\ 1 &= -11 + 3(15 - 11) = 3 \cdot 15 - 4 \cdot 11. \end{aligned}$$

To get a combination which equal 2, we need to multiply this last line by 2. This gives $6 \cdot 15 - 8 \cdot 11 = 2$, and thus we can take $y = -8$, $-z = 6$. Using this in the above gives $x = \boxed{-85}$. If we prefer a positive answer, we recall that the Chinese remainder theorem says that the answer is unique in arithmetic $\pmod{165}$, and thus $-85 \equiv \boxed{80} \pmod{165}$ is another possible answer.