Homework 21 Solutions

1. **The goal of this problem is to find the 11th root of 5** $\pmod{29}$**.**

   (a) **Find a number** k **such that** $11k \equiv 1 \pmod{28}$**. (Caution: for this part, we are working** $\pmod{28}$**).**
   Since $k \equiv 1/11 \pmod{28}$, we run the Euclidean algorithm.

   $$\begin{aligned} 28 &= 2 \cdot 11 + 6 \\ 11 &= 6 + 5 \\ 6 &= 5 + 1. \end{aligned}$$

   Doing it backwards gives

   $$\begin{aligned} 1 &= 6 - 5 \\ 1 &= 6 - (11 - 6) = -11 + 2 \cdot 6 \\ 1 &= -11 + 2(28 - 2 \cdot 11) = 2 \cdot 28 - 5 \cdot 11. \end{aligned}$$

   We conclude that $k \equiv -5 \equiv \boxed{23} \pmod{28}$.

   (b) **Compute** $5^k \pmod{29}$**. Why is this number the 11th root of 5** $\pmod{29}$**?**
   We wish to compute $5^{23} \pmod{29}$. We have

   $$\begin{aligned} 5^2 &\equiv 25 \equiv -4, \\ 5^4 &\equiv 16 \equiv -13, \\ 5^8 &\equiv 169 \equiv 24 \equiv -5, \\ 5^{16} &\equiv 25 \equiv -4. \end{aligned}$$

   Using this, we see that

   $$5^{23} \equiv 5^{16} \cdot 5^4 \cdot 5^2 \cdot 5 \equiv -4 \cdot (-13) \cdot (-4) \cdot 5 \equiv 52 \cdot (-20) \equiv -6 \cdot 9 \equiv -54 \equiv \boxed{4} \pmod{29}.$$

   Alternatively, we could use that $5^{23} \equiv 5^{-5} \equiv (1/5)^5 \pmod{29}$. Since it's easy to see that $1/5 \equiv 6 \pmod{29}$, it suffices to compute $6^5 \pmod{29}$. We have

   $$\begin{aligned} 6^2 &\equiv 36 \equiv 7, \\ 6^4 &\equiv 49 \equiv 20 \equiv -9, \\ 6^5 &\equiv -9 \cdot 6 \equiv -54 \equiv \boxed{4}. \end{aligned}$$

   Why is 5^{23} the 11th root of 5 $\pmod{29}$? Well, we know that

   $$\left(5^{23}\right)^{11} \equiv 5^{-5} \equiv 5^{1-2 \cdot 28} \equiv 5 \pmod{29}$$

   where we've used the results of our Euclidean algorithm from part (a) and Fermat's theorem. Since $\left(5^{23}\right)^{11} \equiv 5 \pmod{29}$, it follows that $5^{1/11} \equiv 23 \pmod{29}$.

   (c) **Check that your answer to part (b) is correct by raising it to the 11th power and seeing if you get 5.**
   We want to compute $4^{11} \pmod{29}$. We have

   $$\begin{aligned} 4^2 &\equiv 16 \equiv -13, \\ 4^4 &\equiv 169 \equiv 24 \equiv -5, \\ 4^8 &\equiv 25 \equiv -4. \end{aligned}$$

   Using this, we have

   $$4^{11} \equiv 4^8 \cdot 4^2 \cdot 4 \equiv -4 \cdot (-13) \cdot 4 \equiv -16 \cdot (-13) \equiv 13 \cdot (-13) \equiv -169 \equiv \boxed{5} \pmod{29}.$$

   So we do get 5, confirming that we did the previous parts correctly.

2. **The method we discussed in today's lecture and reviewed in the previous problem (and which is discussed in Chapter 19 of the book) for computing roots** (mod p) **can be applied to only 2 of the following 4 problems. Say which 2 can be solved by this method, and solve them. Also, explain why our method fails in the other 2 cases.**

   (a) **The 5th root of 3** (mod 23)**;**
   We check that 23 is prime and that 5 and $22 = 23 - 1$ are relatively prime. Since this is the case, we can apply our method. The Euclidean algorithm gives

$$\begin{aligned} 22 &= 4 \cdot 5 + 2, \\ 5 &= 2 \cdot 2 + 1. \end{aligned}$$

   Running it backwards shows that

$$\begin{aligned} 1 &= 5 - 2 \cdot 2, \\ 1 &= 5 - 2 \cdot (22 - 4 \cdot 5) = -2 \cdot 22 + 9 \cdot 5. \end{aligned}$$

   Thus $3^{1/5} \equiv 3^9 \pmod{23}$. To compute $3^9 \pmod{29}$, we first compute that

$$\begin{aligned} 3^2 &\equiv 9, \\ 3^4 &\equiv 81 \equiv 12, \\ 3^8 &\equiv 144 \equiv 6. \end{aligned}$$

   Thus

$$3^{1/5} \equiv 3^9 \equiv 3^8 \cdot 3 \equiv 6 \cdot 3 \equiv \boxed{18} \pmod{23}.$$

   (b) **The 5th root of 7** (mod 31)**;**
   We see that 5 and $30 = 31 - 1$ are not relatively prime. Thus our method does not apply.

   (c) **The 5th root of 6** (mod 33)**;**
   It's clear that 33 is not prime. Thus our method does not apply.

   (d) **The 5th root of 4** (mod 37)**.**
   We see that 37 is prime and that 5 and 36 are relatively prime, so our method applies. The Euclidean algorithm gives

$$36 = 7 \cdot 5 + 1.$$

   Running it backwards shows that

$$1 = 36 - 7 \cdot 5.$$

   Thus $4^{1/5} \equiv 4^{-7} \equiv 4^{29} \pmod{37}$. Computing $4^{29} \pmod{37}$, we have

$$\begin{aligned} 4^2 &\equiv 16, \\ 4^4 &\equiv 256 \equiv 34 \equiv -3, \\ 4^8 &\equiv 9, \\ 4^{16} &\equiv 81 \equiv 7. \end{aligned}$$

   Finally, we have

$$4^{29} \equiv 4^{16} \cdot 4^8 \cdot 4^4 \cdot 4 \equiv 7 \cdot 9 \cdot (-3) \cdot 4 \equiv -27 \cdot 28 \equiv 10 \cdot (-9) \equiv -90 \equiv \boxed{21}.$$

3. **What is the 15th root of 2** (mod 29)**?**

Since 29 is prime and 15 and 28 are relatively prime, our method applies. The Euclidean algorithm gives

$$\begin{aligned} 28 &= 15 + 13, \\ 15 &= 13 + 2, \\ 13 &= 6 \cdot 2 + 1. \end{aligned}$$

Running it backwards, we have

$$\begin{aligned} 1 &= 13 - 6 \cdot 2, \\ 1 &= 13 - 6(15 - 13) = -6 \cdot 15 + 7 \cdot 13, \\ 1 &= -6 \cdot 15 + 7(28 - 15) = 7 \cdot 28 - 13 \cdot 15. \end{aligned}$$

Thus $2^{1/15} \equiv 2^{-13} \equiv 2^{15} \pmod{29}$. To compute $2^{15} \pmod{29}$, we first compute

$$\begin{aligned} 2^2 &\equiv 4, \\ 2^4 &\equiv 16 \equiv -13, \\ 2^8 &\equiv 169 \equiv 24 \equiv -5, \\ 2^{16} &\equiv 25 \equiv -4. \end{aligned}$$

Here we've gone up to $2^{16} \pmod{29}$ because we know that $1/2 \equiv 15 \pmod{29}$, and thus

$$2^{15} \equiv 1/2 \cdot 2^{16} \equiv 15 \cdot (-4) \equiv -60 \equiv \boxed{27} \pmod{29}.$$