Homework 21 Solutions

Problems

1. **Use your power table from arithmetic** $\pmod{13}$ **on HW 20 to compute the following.**

   (a) **What is the 5th root of** $4 \pmod{13}$?

   We want the row whose 5th column is 4, which we find in row $\boxed{10}$.

   (b) **What is the 11th root of** $9 \pmod{13}$?

   Row $\boxed{3}$ has 11th column equal to 9.

2. **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.

3. **The method we know for computing roots** $\pmod{p}$ **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 $\pmod{23}$**;**

   (b) The 5th root of 7 $\pmod{31}$**;**

   (c) The 5th root of 6 $\pmod{33}$**;**

   (d) The 5th root of 4 $\pmod{37}$**.**

   33 is not prime. 5 is not relatively prime to $30 = 31 - 1$

   $1/5 = 9 \pmod{22}$ So $3^{1/5} = 3^9 \pmod{23}$ and you can compute this by the doubling method.

   $1/5 = 29 \pmod{36}$. So $4^{1/5} = 4^{29} \pmod{37}$ and you can compute this by the doubling method.

4. **What is the 15th root of 2** $\pmod{29}$**?**

   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

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