Homework 21 Solutions

Problems

Here is the table of powers modulo 13 that you computed on HW 20:

x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}	x^{11}	x^{12}
1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	3	6	12	11	9	5	10	7	1
3	9	1	3	9	1	$\boxed{3}$	9	1	3	$\boxed{9}$	1
4	3	12	9	10	1	4	3	12	9	10	1
5	12	8	1	5	12	8	1	5	12	8	1
6	10	8	9	2	12	7	3	5	4	11	1
7	10	5	9	11	12	6	3	8	4	2	1
8	12	5	1	8	12	5	1	8	12	5	1
9	3	1	9	3	1	9	3	1	9	3	1
10	9	12	3	$\boxed{4}$	1	10	9	12	3	4	1
11	4	5	3	7	12	2	9	8	10	6	1
12	1	12	1	12	1	12	1	12	1	12	1

1. **Use the table of powers** $\pmod{13}$ **to compute the following:**
   - **(a) What is the 5th root of 4** $\pmod{13}$**?**
   - **(b) What is the 11th root of 9** $\pmod{13}$**?**
   - **(c) What is the 7th root of** 3 $\pmod{13}$**?**

   We find the 4 in the 5th column of the table. It appears in row 10, so

   $$4^{1/5} \equiv 10 \pmod{13}.$$

   We find the 9 in the 11th column of the table. It appears in row 3, so

   $$9^{1/11} \equiv 3 \pmod{13}.$$

   We find the 3 in the 7th column of the table. It appears in row 3, so

   $$3^{1/7} \equiv 3 \pmod{13}.$$

2. - **(a) How many 8th roots does** 9 **have** $\pmod{13}$**? How many 8th roots does** 3 **have** $\pmod{13}$**? How many 8th roots does** 7 **have** $\pmod{13}$**?**
   - **(b) How many 9th roots does** 8 **have** $\pmod{13}$**? How many 9th roots does** 6 **have** $\pmod{13}$**? How many 9th roots does** 5 **have** $\pmod{13}$**?**
   - **(c) What is the greatest common divisor of** 8 **and** $13-1$**?**
   - **(d) What is the greatest common divisor of** 9 **and** $13-1$**?**

   We look in the column for x^8, and find 9 and 3 four times each, and don't find 7. So 9 has $\boxed{\text{four}}$ 8th roots, 3 has $\boxed{\text{four}}$ 8th roots, and 7 has $\boxed{\text{zero}}$ 8th roots.

   Similarly, in the column for x^9, 8 and 5 appear three times each, while 6 does not appear. So 8 has $\boxed{\text{three}}$ 9th roots, 6 has $\boxed{\text{zero}}$ 9th roots and 5 has $\boxed{\text{three}}$ 9th roots.

   The gcd of 8 and 12 is $\boxed{4}$, corresponding to the fact that one quarter of nonzero numbers modulo 13 will have an 8th root, and each one that does will have 4.

   The gcd of 9 and 12 is $\boxed{3}$, corresponding to the fact that one third of the nonzero numbers modulo 13 will have a 9th root, and each one that does will have 3.

3. **Suppose I tell you that 39847418273263 is prime, and that**

$$5441662622048^{19} \equiv 2673482^{19} \pmod{39847418273263}.$$

Note that $2^{19} = 524288$**. How many 19th roots of 524288 are there** $\pmod{39847418273263}$**, and why?**

There are $\boxed{19}$ 19th roots of 524288. There is at least one, since 2 is a 19th root. Moreover, we know that there must be at least two since we've exhibited another number with duplicate 19th roots. But the number of 19th roots must be the gcd of 19 and 39847418273262, which must be either 1 or 19 (since it is a divisor of 19). So there must be 19 19th roots.

4. **The goal of this exercise is to compute** $5^{82} \pmod{103}$ **using the method outlined in Section 18.2 of the textbook.**

(a) **Write** 82 **as a sum of powers of 2. What is the largest power of 2 appearing?**

The largest power of 2 less than or equal to 82 is 64. We write

$$82 = 64 + 18,$$

and then repeat the process with 18. This yields

$$82 = \boxed{64 + 16 + 2}.$$

The largest power of 2 appearing is $\boxed{64}$.

(b) **Compute** $5^2 \pmod{103}$**. Compute** $5^4 \pmod{103}$**. Compute** $5^8 \pmod{103}$**. Keep going until you've computed 5 raised to the largest power of 2 appearing in part (a).**

$$\begin{aligned}
5^1 &= \boxed{5} \\
5^2 &= \boxed{25} \\
5^4 &= (5^2)^2 = 25^2 = 625 \equiv \boxed{7} \pmod{103} \\
5^8 &= (5^4)^2 \equiv 7^2 = \boxed{49} \pmod{103} \\
5^{16} &= (5^8)^2 \equiv 49^2 = 2401 \equiv \boxed{32} \pmod{103} \\
5^{32} &= (5^{16})^2 \equiv 32^2 = 1024 \equiv \boxed{-6} \pmod{103} \\
5^{64} &= (5^{32})^2 \equiv (-6)^2 = \boxed{36} \pmod{103}
\end{aligned}$$

(c) Use part (a) to write 5^{82} as a product of the numbers you computed in part (b). Multiply these out $\pmod{103}$ in order to find the final answer.

We have

$$\begin{aligned}
5^{82} &= 5^{64+16+2} \\
&= 5^{64} \cdot 5^{16} \cdot 5^2 \\
&\equiv 36 \cdot 32 \cdot 25 \\
&\equiv \boxed{63} \pmod{103}
\end{aligned}$$