Worksheet 9: Modular Arithmetic Second Submission

MATH 1700: Ideas in Mathematics

Professor Rimmer

Due: April 5, 2023 **Denny Cao**

1 Warm-Up Problems

Question 1. If today is Friday, what day of the week will it be 3724 days from now?

Answer 1. $3724 \bmod 7 = 0$, so it will be Friday.

Question 2. A famous episode of The Simpsons displays the equation

$$1782^{12} + 1841^{12} = 4472^{12}$$

Indeed, if your calculator is not very precise, and you add 1782^{12} to 1841^{12} and take the twelfth root, you will see 4472^{12}, but that is a rounding error! In fact, Fermat's Last Theorem (claimed by Fermat around 1637, and finally proven by Wiles and Taylor in 1994) states that for whole numbers a, b, c, and n, the equation

$$a^n + b^n = c^n$$

can only be true when $n = 2$. (See the above equation, with $n = 12$, must be false.). Reduce mod 2 to show that $1782^{12} + 1841^{12} \neq 4472^{12}$.

Answer 2.

Proof. Assume for purposes of contradiction that $1782^{12} + 1841^{12} = 4472^{12}$.

$$\begin{aligned}
1782^{12} \bmod 2 &= (1782 \bmod 2)^{12} \bmod 2 = 0^{12} \bmod 2 = 0 \\
1841^{12} \bmod 2 &= (1841 \bmod 2)^{12} \bmod 2 = 1^{12} \bmod 2 = 1 \\
4472^{12} \bmod 2 &= (4472 \bmod 2)^{12} \bmod 2 = 0^{12} \bmod 2 = 0 \\
\implies 0 + 1 = 0 \;&⨳
\end{aligned}$$

We reach a contradiction, which means that $1782^{12} + 1841^{12} \neq 4472^{12}$. □

Question 3. Compute $13^{100} \bmod 7$.

Answer 3.

$$\begin{aligned}
13 &\equiv 6 \bmod 7 \\
13^{100} &\equiv (6 \bmod 7)^{100} \bmod 7 \\
&\equiv 6^{100} \bmod 7 \\
6 &\equiv -1 \bmod 7 \\
6^{100} &\equiv (-1 \bmod 7)^{100} \bmod 7 \\
&\equiv 1 \bmod 7 \\
13^{100} &\equiv 1 \bmod 7 \implies 13^{100} \bmod 7 = 1
\end{aligned}$$

2 Another Theorem of Fermat

Question 4. For each number n from 1 to 4, compute, n^2, n^3, and $n^4 \bmod 5$. Make a table of your results. Do you notice anything surprising?

Answer 4.

n	n^2	n^3	n^4
1	1 mod 5	1 mod 5	1 mod 5
2	4 mod 5	3 mod 5	1 mod 5
3	4 mod 5	2 mod 5	1 mod 5
4	1 mod 5	4 mod 5	1 mod 5

All $n^4 \bmod 5$ **are** 1.

Question 5. Repeat the same problem for the numbers 1 through 6, working $\bmod 7$.

Answer 5.

n	n^2	n^3	n^4	n^5	n^6
1	1 mod 7	1 mod 7	1 mod 7	1 mod 7	1 mod 7
2	4 mod 7	1 mod 7	2 mod 7	4 mod 7	1 mod 7
3	2 mod 7	6 mod 7	4 mod 7	5 mod 7	1 mod 7
4	2 mod 7	1 mod 7	4 mod 7	2 mod 7	1 mod 7
5	4 mod 7	1 mod 7	4 mod 7	3 mod 7	1 mod 7
6	1 mod 7	6 mod 7	1 mod 7	6 mod 7	1 mod 7

All $n^6 \bmod 7$ **are** 1.

Question 6. Repeat this problem for 9, 11 and 13. (You do not need to include a table for 13 with your first submission, only your second submission.) How large should the exponents be before you discover a similar pattern? Does the pattern continue to hold for all odd numbers? Make a guess about when this pattern does and doesn't hold.

Answer 6.

n	n^2	n^3	n^4	n^5	n^6	n^7	n^8
1	1 mod 9	1 mod 9	1 mod 9	1 mod 9	1 mod 9	1 mod 9	1 mod 9
2	4 mod 9	8 mod 9	7 mod 9	5 mod 9	1 mod 9	2 mod 9	4 mod 9
3	0 mod 9	0 mod 9	0 mod 9	0 mod 9	0 mod 9	0 mod 9	0 mod 9
4	7 mod 9	1 mod 9	4 mod 9	7 mod 9	1 mod 9	4 mod 9	7 mod 9
5	7 mod 9	8 mod 9	4 mod 9	2 mod 9	1 mod 9	5 mod 9	7 mod 9
6	0 mod 9	0 mod 9	0 mod 9	0 mod 9	0 mod 9	0 mod 9	0 mod 9
7	4 mod 9	1 mod 9	7 mod 9	4 mod 9	1 mod 9	7 mod 9	4 mod 9
8	1 mod 9	8 mod 9	1 mod 9	8 mod 9	1 mod 9	8 mod 9	1 mod 9

n	n^2	n^3	n^4	n^5	n^6	n^7	n^8	n^9	n^{10}
1	1 mod 11	1 mod 11	1 mod 11	1 mod 11	1 mod 11	1 mod 11	1 mod 11	1 mod 11	1 mod 11
2	4 mod 11	8 mod 11	5 mod 11	10 mod 11	9 mod 11	7 mod 11	3 mod 11	6 mod 11	1 mod 11
3	9 mod 11	5 mod 11	4 mod 11	1 mod 11	3 mod 11	9 mod 11	5 mod 11	4 mod 11	1 mod 11
4	5 mod 11	9 mod 11	3 mod 11	1 mod 11	4 mod 11	5 mod 11	9 mod 11	3 mod 11	1 mod 11
5	3 mod 11	4 mod 11	9 mod 11	1 mod 11	5 mod 11	3 mod 11	4 mod 11	9 mod 11	1 mod 11
6	3 mod 11	7 mod 11	9 mod 11	10 mod 11	5 mod 11	8 mod 11	4 mod 11	2 mod 11	1 mod 11
7	5 mod 11	2 mod 11	3 mod 11	10 mod 11	4 mod 11	6 mod 11	9 mod 11	8 mod 11	1 mod 11
8	9 mod 11	6 mod 11	4 mod 11	10 mod 11	3 mod 11	2 mod 11	5 mod 11	7 mod 11	1 mod 11
9	4 mod 11	3 mod 11	5 mod 11	1 mod 11	9 mod 11	4 mod 11	3 mod 11	5 mod 11	1 mod 11
10	1 mod 11	10 mod 11	1 mod 11	10 mod 11	1 mod 11	10 mod 11	1 mod 11	10 mod 11	1 mod 11

n	n^2	n^3	n^4	n^5	n^6	n^7	n^8	n^9	n^{10}	n^{11}	n^{12}
1	1 mod 13	1 mod 13	1 mod 13	1 mod 13	1 mod 13	1 mod 13	1 mod 13	1 mod 13	1 mod 13	1 mod 13	1 mod 13
2	4 mod 13	8 mod 13	3 mod 13	6 mod 13	12 mod 13	11 mod 13	9 mod 13	5 mod 13	10 mod 13	7 mod 13	1 mod 13
3	9 mod 13	1 mod 13	3 mod 13	9 mod 13	1 mod 13	3 mod 13	9 mod 13	1 mod 13	3 mod 13	9 mod 13	1 mod 13
4	3 mod 13	12 mod 13	9 mod 13	10 mod 13	1 mod 13	4 mod 13	3 mod 13	12 mod 13	9 mod 13	10 mod 13	1 mod 13
5	12 mod 13	8 mod 13	1 mod 13	5 mod 13	12 mod 13	8 mod 13	1 mod 13	5 mod 13	12 mod 13	8 mod 13	1 mod 13
6	10 mod 13	8 mod 13	9 mod 13	2 mod 13	12 mod 13	7 mod 13	3 mod 13	5 mod 13	4 mod 13	11 mod 13	1 mod 13
7	10 mod 13	5 mod 13	9 mod 13	11 mod 13	12 mod 13	6 mod 13	3 mod 13	8 mod 13	4 mod 13	2 mod 13	1 mod 13
8	12 mod 13	5 mod 13	1 mod 13	8 mod 13	12 mod 13	5 mod 13	1 mod 13	8 mod 13	12 mod 13	5 mod 13	1 mod 13
9	3 mod 13	1 mod 13	9 mod 13	3 mod 13	1 mod 13	9 mod 13	3 mod 13	1 mod 13	9 mod 13	3 mod 13	1 mod 13
10	9 mod 13	12 mod 13	3 mod 13	4 mod 13	1 mod 13	10 mod 13	9 mod 13	12 mod 13	3 mod 13	4 mod 13	1 mod 13
11	4 mod 13	5 mod 13	3 mod 13	7 mod 13	12 mod 13	2 mod 13	9 mod 13	8 mod 13	10 mod 13	6 mod 13	1 mod 13
12	1 mod 13	12 mod 13	1 mod 13	12 mod 13	1 mod 13	12 mod 13	1 mod 13	12 mod 13	1 mod 13	12 mod 13	1 mod 13

The pattern returns when we mod by 11. As such, this pattern does not hold for all odd numbers; it only holds for prime numbers.

3 Check Digits

Question 7. U.S. postal money orders have a 10-digit serial number plus an additional check digit. The check digit is a number between 0 and 6, which is congruent to the serial number mod 7. That is, serial number ≡ check digit mod 7. Find the check digit for the serial number below. You may use your computer as a calculator.

$$3421054606\_$$

(Note that the postal money orders do *not* compute check digits the same way that we say in the videos, but instead in the way described above.)
Recall that the formula for 12-digit UPC codes $d_1d_2d_3d_4d_5d_6d_7d_8d_9d_{10}d_{11}d_{12}$ is $3d_1 + d_2 + 3d_3 + d_4 + 3d_5 + d_6 + 3d_7 + d_8 + 3d_9 + d_{10} + 3d_{11} + d_{12} \equiv 0 \text{ mod } 10$.

Answer 7.

$$3421054606 \equiv 4 \text{ mod } 7$$

The check digit is 4. □

Question 8. The paper that this worksheet was originally printed on came in a package of 500 sheets with the UPC code below. What was the last digit?

$$84235605541\_$$

Answer 8.

$$\begin{aligned}3(8)+4+3(2)+3+3(5)+6+3(0)+5+3(5)+4+3(1)+x &\equiv 0 \bmod 10\\ 4+4+6+3+5+6+0+5+5+4+3+x &\equiv 0 \bmod 10\\ 45+x &\equiv 0 \bmod 10\\ x &\equiv 5 \bmod 10\end{aligned}$$

The last digit is 5. □

Question 9. The correct UPC for a product is

051000025265

Explain why neither

051000026255 nor 050000055265

register as errors.

Answer 9. *Proof.* Neither 051000026255 nor 050000055265 register as errors because the method used to check the UPCS, $3d_1+d_2+3d_3+d_4+3d_5+d_6+3d_7+d_8+3d_9+d_{10}+3d_{11}+d_{12} \equiv 0 \bmod 10$, is true for all 3 codes.

For 051000026255:
The difference between the correct UPC of 051000025265 and 051000026255 is that the 9th and 11th digits are switched. However, as the method to check the digits multiplies the 9th and 11th digits by 3, the resulting sum of the UPC check is the same. As the check sum with 051000025265 is divisible by 10, the check sum with 051000026255 is also divisible by 10, and thus the UPC is valid.
We can confirm this by using the method to check the UPC:

$$\begin{aligned}3(0)+5+3(1)+0+3(0)+0+3(0)+2+3(6)+2+3(5)+5 &\overset{?}{\equiv} 0 \bmod 10\\ 0+5+3+0+0+0+0+2+18+2+15+5 &\overset{?}{\equiv} 0 \bmod 10\\ 0+5+3+0+0+0+0+2+8+2+5+5 &\overset{?}{\equiv} 0 \bmod 10\\ 30 &\equiv 0 \bmod 10\end{aligned}$$

For 050000055265:
The difference between the correct UPC of 051000025265 and 050000055265 is that the 3rd digit is replaced with a 0, and the 8th digit is replaced with a 5. With the correct UPC, the check sum multiplies the 3rd digit by 3 and the 8th digit by 1, resulting in a sum of 5 for the two digits. With 050000055265, the check sum multiplies the 3rd digit by 3 and the 8th digit by 3, resulting in a sum of 15 for the two digits. As the rest of the digits remain the same, the check sums for both UPCs are the same. As the check sum with 051000025265 is divisible by 10, the check sum with 050000055265 is also divisible by 10, and thus the UPC is valid.

We can confirm this by using the method to check the UPC:

$$\begin{aligned} 3(0)+5+3(0)+0+3(0)+0+3(0)+5+3(5)+2+3(6)+5 &\overset{?}{\equiv} 0 \bmod 10 \\ 0+5+0+0+0+0+0+5+5+2+8+5 &\overset{?}{\equiv} 0 \bmod 10 \\ 30 &\equiv 0 \bmod 10 \end{aligned}$$

Thus, 050000055265 is a valid UPC.

As both of these UPCs are valid, they do not register as errors. □

4 Reflection

Identify at least one wrong or failed idea that turned out to be helpful or enlightening in some way. For instance, that idea might have helped you solve a problem, or it may have been the start of a conversation that improved your understanding more generally. You can list one of your own ideas, or an idea that originated with a classmate. (Please give your classmate credit!)
For quesiton 6, I initially could not find a pattern, but after checking with Larry Huang, I realized that I had just made mistakes in my calculations! After redoing the table, I was able to find the pattern.