Worksheet 9: Modular Arithmetic First Submission

MATH 1700: Ideas in Mathematics

Professor Rimmer

Due: March 31, 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 $1782^{12} + 1841^{12} = 4472^{12}$.

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

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

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

Answer 3.

$$\begin{aligned}
13 &\equiv 6 \bmod 7 \\
13^2 &\equiv 6 \bmod 7 \cdot 6 \bmod 7 \\
6^2 \bmod 7 &\equiv 1 \bmod 7 \\
13^{100} &\equiv 6^{100} \bmod 7 \\
6^{100} \bmod 7 &= (6^2)^{50} \bmod 7 \\
13^{100} &\equiv 1 \bmod 7
\end{aligned}$$

2 Another Theorem of Fermat

Question 4. For each number n from 1 to 4, compute, n^2, n^3, and n^4 mod 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	1 mod 5 = 1	1 mod 5 = 1
2	4 mod 5 = 4	8 mod 5 = 3	16 mod 5 = 1
3	9 mod 5 = 4	27 mod 5 = 2	81 mod 5 = 1
4	16 mod 5 = 1	64 mod 5 = 4	256 mod 5 = 1

All n^4 mod 5 are 1.

Question 5. Repeat the same problem for the numbers 1 through 6, working mod 7.

Answer 5.

n	n^2	n^3	n^4	n^5	n^6
1	1 mod 7 = 1	1 mod 7 = 1	1 mod 7 = 1	1 mod 7 = 1	1 mod 7 = 1
2	4 mod 7 = 4	8 mod 7 = 1	16 mod 7 = 2	32 mod 7 = 4	64 mod 7 = 1
3	9 mod 7 = 2	27 mod 7 = 6	81 mod 7 = 4	243 mod 7 = 5	729 mod 7 = 1
4	16 mod 7 = 2	64 mod 7 = 1	256 mod 7 = 4	1024 mod 7 = 2	4096 mod 7 = 1
5	25 mod 7 = 4	125 mod 7 = 6	625 mod 7 = 2	3125 mod 7 = 3	15625 mod 7 = 1
6	36 mod 7 = 1	216 mod 7 = 6	1296 mod 7 = 1	7776 mod 7 = 6	46656 mod 7 = 1

All n^6 mod 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	1 mod 9 = 1	1 mod 9 = 1	1 mod 9 = 1	1 mod 9 = 1	1 mod 9 = 1	1 mod 9 = 1
2	4 mod 9 = 4	8 mod 9 = 8	16 mod 9 = 7	32 mod 9 = 5	64 mod 9 = 1	128 mod 9 = 2	256 mod 9 = 4
3	9 mod 9 = 0	27 mod 9 = 0	81 mod 9 = 0	243 mod 9 = 0	729 mod 9 = 0	2187 mod 9 = 0	6561 mod 9 = 0
4	16 mod 9 = 7	64 mod 9 = 1	256 mod 9 = 4	1024 mod 9 = 7	4096 mod 9 = 1	16384 mod 9 = 4	65536 mod 9 = 7
5	25 mod 9 = 7	125 mod 9 = 4	625 mod 9 = 1	3125 mod 9 = 7	15625 mod 9 = 4	78125 mod 9 = 1	390625 mod 9 = 7
6	36 mod 9 = 0	216 mod 9 = 0	1296 mod 9 = 0	7776 mod 9 = 0	46656 mod 9 = 0	279936 mod 9 = 0	1679616 mod 9 = 0
7	49 mod 9 = 4	343 mod 9 = 1	2401 mod 9 = 7	16807 mod 9 = 4	117649 mod 9 = 1	823543 mod 9 = 7	5764801 mod 9 = 4
8	64 mod 9 = 1	512 mod 9 = 7	4096 mod 9 = 1	32768 mod 9 = 4	262144 mod 9 = 7	2097152 mod 9 = 1	16777216 mod 9 = 4

n	n^2	n^3	n^4	n^5	n^6	n^7	n^8	n^9	n^{10}
1	1 mod 11 = 1	1 mod 11 = 1	1 mod 11 = 1	1 mod 11 = 1	1 mod 11 = 1	1 mod 11 = 1	1 mod 11 = 1	1 mod 11 = 1	1 mod 11 = 1
2	4 mod 11 = 4	16 mod 11 = 5	64 mod 11 = 9	256 mod 11 = 3	1024 mod 11 = 4	4096 mod 11 = 5	16384 mod 11 = 9	65536 mod 11 = 3	262144 mod 11 = 4
3	9 mod 11 = 9	81 mod 11 = 1	729 mod 11 = 9	6561 mod 11 = 1	59049 mod 11 = 9	531441 mod 11 = 1	4782969 mod 11 = 9	43046721 mod 11 = 1	387420489 mod 11 = 9
4	16 mod 11 = 5	256 mod 11 = 4	4096 mod 11 = 5	65536 mod 11 = 9	1048576 mod 11 = 3	16777216 mod 11 = 4	268435456 mod 11 = 5	4294967296 mod 11 = 9	68719476736 mod 11 = 3
5	25 mod 11 = 3	125 mod 11 = 9	625 mod 11 = 3	3125 mod 11 = 9	15625 mod 11 = 3	78125 mod 11 = 9	390625 mod 11 = 3	1953125 mod 11 = 9	9765625 mod 11 = 3
6	36 mod 11 = 9	216 mod 11 = 1	1296 mod 11 = 9	7776 mod 11 = 1	46656 mod 11 = 9	279936 mod 11 = 1	1679616 mod 11 = 9	10077696 mod 11 = 1	60466176 mod 11 = 9
7	49 mod 11 = 1	343 mod 11 = 9	2401 mod 11 = 1	16807 mod 11 = 9	117649 mod 11 = 1	823543 mod 11 = 9	5764801 mod 11 = 1	40353607 mod 11 = 9	282475249 mod 11 = 1
8	64 mod 11 = 10	512 mod 11 = 5	4096 mod 11 = 10	32768 mod 11 = 5	262144 mod 11 = 10	2097152 mod 11 = 5	16777216 mod 11 = 10	134217728 mod 11 = 5	1073741824 mod 11 = 10
9	81 mod 11 = 7	729 mod 11 = 9	6561 mod 11 = 7	59049 mod 11 = 9	531441 mod 11 = 7	4782969 mod 11 = 9	43046721 mod 11 = 7	387420489 mod 11 = 9	3486784401 mod 11 = 7
10	100 mod 11 = 9	1000 mod 11 = 1	10000 mod 11 = 9	100000 mod 11 = 1	1000000 mod 11 = 9	10000000 mod 11 = 1	100000000 mod 11 = 9	1000000000 mod 11 = 1	10000000000 mod 11 = 9

n	n^2	n^3	n^4	n^5	n^6
1	1 mod 12 = 1	1 mod 12 = 1	1 mod 12 = 1	1 mod 12 = 1	1 mod 12 = 1
2	4 mod 12 = 4	16 mod 12 = 4	64 mod 12 = 4	256 mod 12 = 4	1024 mod 12 = 4
3	9 mod 12 = 9	81 mod 12 = 9	729 mod 12 = 9	6561 mod 12 = 9	59049 mod 12 = 9
4	16 mod 12 = 4	256 mod 12 = 4	4096 mod 12 = 4	65536 mod 12 = 4	1048576 mod 12 = 4
5	25 mod 12 = 1	625 mod 12 = 1	15625 mod 12 = 1	390625 mod 12 = 1	9765625 mod 12 = 1
6	36 mod 12 = 0	1296 mod 12 = 0	46656 mod 12 = 0	279936 mod 12 = 0	1679616 mod 12 = 0
7	49 mod 12 = 1	2401 mod 12 = 1	16807 mod 12 = 1	117649 mod 12 = 1	823543 mod 12 = 1
8	64 mod 12 = 4	4096 mod 12 = 4	262144 mod 12 = 4	16777216 mod 12 = 4	1073741824 mod 12 = 4
9	81 mod 12 = 9	6561 mod 12 = 9	531441 mod 12 = 9	43046721 mod 12 = 9	3486784401 mod 12 = 9
10	100 mod 12 = 4	10000 mod 12 = 4	1000000 mod 12 = 4	100000000 mod 12 = 4	10000000000 mod 12 = 4
11	121 mod 12 = 1	14641 mod 12 = 1	161051 mod 12 = 1	1771561 mod 12 = 1	19487171 mod 12 = 1

n	n^7	n^8	n^9	n^{10}	n^{11}	n^{12}
1	1 mod 12 = 1	1 mod 12 = 1	1 mod 12 = 1	1 mod 12 = 1	1 mod 12 = 1	1 mod 12 = 1
2	4096 mod 12 = 4	16384 mod 12 = 4	65536 mod 12 = 4	262144 mod 12 = 4	1048576 mod 12 = 4	4194304 mod 12 = 4
3	531441 mod 12 = 9	4782969 mod 12 = 9	43046721 mod 12 = 9	387420489 mod 12 = 9	3486784401 mod 12 = 9	31381059609 mod 12 = 9
4	16777216 mod 12 = 4	268435456 mod 12 = 4	4294967296 mod 12 = 4	68719476736 mod 12 = 4	1099511627776 mod 12 = 4	17592186044416 mod 12 = 4
5	244140625 mod 12 = 1	6103515625 mod 12 = 1	152587890625 mod 12 = 1	3814697265625 mod 12 = 1	95367431640625 mod 12 = 1	2384185791015625 mod 12 = 1
6	10077696 mod 12 = 0	60466176 mod 12 = 0	362797056 mod 12 = 0	2176782336 mod 12 = 0	13060694016 mod 12 = 0	78364164096 mod 12 = 0
7	5764801 mod 12 = 1	40353607 mod 12 = 1	282475249 mod 12 = 1	1977326743 mod 12 = 1	13841287201 mod 12 = 1	96889010407 mod 12 = 1
8	68719476736 mod 12 = 4	4398046511104 mod 12 = 4	281474976710656 mod 12 = 4	18014398509481984 mod 12 = 4	1152921504606846976 mod 12 = 4	73786976294838206464 mod 12 = 4
9	31381059609 mod 12 = 9	282429536481 mod 12 = 9	2541865828329 mod 12 = 9	22876792454961 mod 12 = 9	205891132094649 mod 12 = 9	1853020188851841 mod 12 = 9
10	1000000000000 mod 12 = 4	100000000000000 mod 12 = 4	10000000000000000 mod 12 = 4	1000000000000000000 mod 12 = 4	100000000000000000000 mod 12 = 4	10000000000000000000000 mod 12 = 4
11	214358881 mod 12 = 1	2357947691 mod 12 = 1	25937424601 mod 12 = 1	285311670611 mod 12 = 1	3138428376721 mod 12 = 1	34522712143931 mod 12 = 1

I couldn't find a pattern... I'll try to redo these tables for the second submission.

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 $\equiv$ 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 $3d_1 + d_2 + 3d_3 + d_4 + 3d_5 + d_6 + 3d_7 + d_8 + 3d_9 + d_{10} + 3d_{11} + d_{12} \equiv 0 \bmod 10$.

Answer 7.

$$3421054606 \equiv 4 \bmod 7$$

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?

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

$$051000026255 \text{ nor } 050000055265$$

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. $\square$

4 Reflection

What content do I need to review before attempting the worksheet again? Are there any videos I need to rewatch?
I need to review Fermat's Little Theorem, as I do not understand how it can be obtained through the tables I made.

What questions would I like to ask my group during the next class discussion?
What pattern did you find? How did you find it?