Math 3110: Worksheet on Congruences

March 8, 2019

1 Multiplication Tables

Finish the multiplication tables.

Mod 4

	0	1	2	3
0	0	0	0	0
1	0			
2	0			
3	0			

Mod 5

	0	1	2	3	4
0					
1					
2					
3					
4					

Mod 6

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Mod 7

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Mod 8

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Mod 9

	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

Mod 10

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

2 Multiplicative Inverses

We use the notation $\mathbb{Z}/n\mathbb{Z}$ for the integers modulo n, which has n elements, usually denoted $0, 1, 2, 3, \ldots, n-1$ (the "natural representatives").

Definition 1. *Let $n \in \mathbb{Z}$. We say that $a \in \mathbb{Z}/n\mathbb{Z}$ and $b \in \mathbb{Z}/n\mathbb{Z}$ are* multiplicative inverses *if $ab \equiv 1 \pmod{n}$. We say that b is the* multiplicative inverse *of a and we say that a is invertible. We write a^{-1} for the multiplicative inverse of a, if it exists.*

1. Give examples of multiplicative inverses modulo 7, 9 and 10. (Hint: see tables on first page.)

2. Find $5^{-1} \pmod{9}$. (Hint: use tables.)

3. For which moduli $4, 5, 6, 7, 8, 9, 10$ is 5 invertible?

4. Which elements modulo 9 are invertible?

5. Which elements modulo 9 are not invertible?

6. By looking at invertible and non-invertible elements in all the tables, form a conjecture about when elements are invertible.

   Theorem 1 (Conjecture)**.** *Let $a, n \in \mathbb{Z}$. Then a is invertible modulo n if and only if*

3 Solving Linear Congruences

1. Solve $3x \equiv 1 \pmod{7}$. (Hint: use the tables.)

2. Explain why solving $ax \equiv b \pmod{n}$ is the same as solving the linear Diophantine equation $ax + ny = b$.

3. Rewrite $11x \equiv 1 \pmod{13}$ as a linear Diophantine equation.

4. Solve the linear Diophantine equation. (The full set of solutions, please.)

5. Solve $11x \equiv 1 \pmod{13}$. (Hint: see the previous item.)

6. Find the multiplicative inverse of 11 modulo 13. (Hint: see the previous item.)

7. Find the multiplicative inverse of 13 modulo 11. (Hint: see the third-to-previous item (the Diophantine equation solution).)

8. Solve $11x \equiv 2 \pmod{13}$. (Hint: this isn't much extra work at all; don't start over.)

9. State the correct theorem:

   Theorem 2. *Let $a, b, n \in \mathbb{Z}$. Then $ax \equiv b \pmod{n}$ has at least one solution if and only if*

10. Explain why this theorem is true.

4 How many solutions?

1. Consider the linear congruence $3x \equiv 6 \pmod{15}$. Rewrite it as a linear Diophantine equation.

2. Find the full set of solutions to the linear Diophantine equation.

3. Solve $3x \equiv 6 \pmod{15}$. How many solutions are there?

4. State the correct theorem:

   Theorem 3. *Let $a, b, n \in \mathbb{Z}$. If $ax \equiv b \pmod{n}$ has any solutions, the number of solutions it has is exactly*

5. Explain why this theorem is true.

5 Using multiplicative inverses

1. Verify that 37 is the multiplicative inverse of 13 modulo 40.

2. Solve $13x \equiv 10 \pmod{40}$ by using the previous item (not by using a Diophantine equation).

3. State the correct theorem:

   Theorem 4. *Let $a, b, n \in \mathbb{Z}$. If a is invertible modulo n, the congruence $ax \equiv b \pmod{n}$ has exactly one solution, namely*

4. Explain why this theorem is true.

5. Give an interesting ($a \neq 0$) example that illustrates that $ax \equiv ay \pmod{n}$ does not always imply $x \equiv y \pmod{n}$.

6. Using the first item in this section (about the inverse of 13 modulo 40), explain why $13x \equiv 13y \pmod{40}$ implies $x \equiv y \pmod{40}$.

7. State the correct theorem:

   Theorem 5. *Let $a, x, y, n \in \mathbb{Z}$. Suppose $ax \equiv ay \pmod{n}$. If , then $x \equiv y \pmod{n}$.*

8. Explain why this theorem is true.

6 Power tables

Finish the power tables.

Mod 4

x	x^2	x^3	x^4	x^5	x^6	x^7	x^8
0	0	0	0	0	0	0	0
1	1	1					
2	0	0					
3	1	3					

Mod 5

x	x^2	x^3	x^4	x^5	x^6	x^7	x^8
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2							
3							
4	1	4	1	4	1	4	1

Mod 6

x	x^2	x^3	x^4	x^5	x^6	x^7	x^8
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	4	2	4	2	4	2	4
3	3	3	3	3	3	3	3
4	4	4	4	4	4	4	4
5	1	5	1	5	1	5	1

Mod 7

x	x^2	x^3	x^4	x^5	x^6	x^7	x^8
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	4	1	2	4	1	2	4
3	2	6	4	5	1	3	2
4	2	1	4	2	1	4	2
5	4	6	2	3	1	5	4
6	1	6	1	6	1	6	1

Mod 8

x	x^2	x^3	x^4	x^5	x^6	x^7	x^8
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	4	0	0	0	0	0	0
3	1	3	1	3	1	3	1
4	0	0	0	0	0	0	0
5	1	5	1	5	1	5	1
6	4	0	0	0	0	0	0
7	1	7	1	7	1	7	1

Mod 9

x	x^2	x^3	x^4	x^5	x^6	x^7	x^8
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	4	8	7	5	1	2	4
3	0	0	0	0	0	0	0
4	7	1	4	7	1	4	7
5	7	8	4	2	1	5	7
6	0	0	0	0	0	0	0
7	4	1	7	4	1	7	4
8	1	8	1	8	1	8	1

Mod 10

x	x^2	x^3	x^4	x^5	x^6	x^7	x^8
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	4	8	6	2	4	8	6
3	9	7	1	3	9	7	1
4	6	4	6	4	6	4	6
5	5	5	5	5	5	5	5
6	6	6	6	6	6	6	6
7	9	3	1	7	9	3	1
8	4	2	6	8	4	2	6
9	1	9	1	9	1	9	1

7 The order of an element

Definition 2. *Let $a, n \in \mathbb{Z}$. Let x be the smallest positive integer such that $a^x \equiv 1 \pmod{n}$, if it exists. Then we say x is the* order *of a modulo n.*

1. Using the tables on the previous page, compute the order of 2 modulo 7.

2. Using the tables on the previous page, compute the order of 3 modulo 7.

3. Give the full list of elements together with their orders for all elements modulo 7.

4. Explain why the increasing powers of any element (the rows in the tables) form a periodic sequence that goes on forever. ('Periodic' means it repeats the same pattern over and over.)

5. Highlight or mark the rows corresponding to invertible elements on the previous page.

6. Highlight or mark the columns where all invertible rows show a '1'. This is a power where all invertible elements, to that power, become 1. For example, modulo 10, this happens first in column 4. Let us call this first occurence a function f and so we write $f(10) = 4$. Compute $f(4)$, $f(5)$, ..., $f(10)$.

7. Can you guess what the function f is?

8. Conjecture the correct statement for this theorem:

   Theorem 6 (Conjecture)**.** *Let a be invertible modulo n. Then, for $x =$, we have $a^x \equiv 1 \pmod{n}$.*

9. Why might this be true?