CEMC.UWATERLOO.CA | The CENTRE for EDUCATION in MATHEMATICS and COMPUTING

Grade 7/8 Math Circles

November 14/15/16/17, 2022

Modular Arithmetic Solutions

Exercise Solutions

Exercise 1

What are the remainders of the following divisions?

a) $8 \div 3$ b) $-10 \div 7$ c) $95 \div 8$ d) $-274 \div 10$

Exercise 1 Solution

a) Since 6 is the largest multiple of 3 less than or equal to 8, the remainder of $8 \div 3$ is $8 - 6 = 2$.

b) Since -14 is the largest multiple of 7 less than or equal to -10, the reminder of $-10 \div 7$ is $-10 - (-14) = 4$.

c) Since 88 is the largest multiple of 8 less than or equal to 95, the remainder of $95 \div 88$ is $95 - 88 = 7$.

d) Since -280 is the largest multiple of 10 less than or equal to -274, the remainder of $-274 \div 10$ is $-274 - (-280) = 6$.

Exercise 2

Fill in the blank with either $\equiv$ or $\not\equiv$.

a) $14 \_\_\_\ 3 \pmod{8}$ b) $6 \_\_\_\ 9 \pmod{3}$ c) $4 \_\_\_\ 7 \pmod{4}$ d) $5 \_\_\_\ 1 \pmod{2}$

Exercise 2 Solution

a) $14 \div 8$ has remainder 6 while $3 \div 8$ has remainder 3, so $14 \not\equiv 3 \pmod{8}$.

b) $6 \div 3$ has remainder 0 and $9 \div 3$ also has remainder 0, so $6 \equiv 9 \pmod{3}$.

c) $4 \div 4$ has remainder 0 while $7 \div 4$ has remainder 3, so $4 \not\equiv 7 \pmod{4}$.

d) $5 \div 2$ has remainder 1 and $1 \div 2$ also has remainder 1, so $5 \equiv 1 \pmod{2}$.

Exercise 3

Fill in the blank with either $\equiv$ or $\not\equiv$.

a) -4 ___ $3 \pmod{7}$ b) -2 ___ $-7 \pmod{9}$ c) -1 ___ $15 \pmod{5}$ d) 8 ___ $-16 \pmod{3}$

Exercise 3 Solution

a) $(-4) \div 7$ has remainder 3 and $3 \div 7$ also has remainder 3, so $-4 \equiv 3 \pmod{7}$.

b) $(-2) \div 9$ has remainder 7 while $(-7) \div 9$ has remainder 2, so $-2 \not\equiv -7 \pmod{9}$.

c) $(-1) \div 5$ has remainder 4 while $15 \div 5$ has remainder 0, so $-1 \not\equiv 15 \pmod{5}$.

d) $8 \div 3$ has remainder 2 and $(-16) \div 3$ also has remainder 2, so $8 \equiv -16 \pmod{3}$.

Exercise 4

Fill in the blank with either $\equiv$ or $\not\equiv$.

a) 4488 ___ $0 \pmod{17}$ since 4488 is divisible by 17.

b) 7 ___ $7 \pmod{9}$.

c) 564 ___ $5 \pmod{18}$ since 6 is the remainder when 564 is divided by 18.

d) $284 \equiv 5 \pmod{31}$ and 5 ___ $284 \pmod{31}$.

e) $-64 \equiv 118 \pmod{26}$ and $222 \equiv 118 \pmod{26}$, so -64 ___ $222 \pmod{26}$.

Exercise 4 Solution

a) $\equiv$ b) $\equiv$ c) $\not\equiv$ d) $\equiv$ e) $\equiv$

Exercise 5

Observe that $8 \equiv 25 \pmod{17}$, $19 \equiv 2 \pmod{17}$, and $0 \equiv 17 \pmod{17}$. Find an integer k, where $0 \leq k < 17$, which is congruent to the following sums **modulo 17** by using modular addition to simplify the calculations.

a) $25 + 19$ b) $19 + 17$ c) $25 + 19 + 17$ d) $19 + 19 + 17 + 25 + 19 + 19 + 19 + 17$

Exercise 5 Solution

a) $25 + 19 \equiv 8 + 2 \equiv 10 \pmod{17}$. So, $k = 10$.

b) $19 + 17 \equiv 2 + 0 \equiv 2 \pmod{17}$. So, $k = 2$.

c) $25 + 19 + 17 \equiv 8 + 2 + 0 \equiv 10 \pmod{17}$. So, $k = 10$.

d) $19 + 19 + 17 + 25 + 19 + 19 + 19 + 17 \equiv 2 + 2 + 0 + 8 + 2 + 2 + 2 + 0 \equiv 18 \equiv 1 \pmod{17}$. So, $k = 1$.

Note that in each part, k is the remainder when the expression is divided by the modulus.

Exercise 6

Observe that $-3 \equiv 6 \pmod{9}$, $11 \equiv 2 \pmod{9}$, and $9 \equiv 0 \pmod{9}$. Find an integer k, where $0 \leq k < 9$, which is congruent to the following differences **modulo 9** by using modular subtraction to simplify the calculations.

a) $11 - 9$ b) $9 - 11$ c) $(-3) - (-3) - 9 - 11$ d) $11 - 9 - 9 - 11 - 9 - 9 - (-3) - 11$

Exercise 6 Solution

a) $11 - 9 \equiv 2 - 0 \equiv 2 \pmod{9}$. So, $k = 2$.

b) $9 - 11 \equiv 0 - 2 \equiv -2 \equiv 7 \pmod{9}$. So, $k = 7$.

c) $(-3) - (-3) - 9 - 11 \equiv 6 - 6 - 0 - 2 \equiv -2 \equiv 7 \pmod{9}$. So, $k = 7$.

d) $11 - 9 - 9 - 11 - 9 - 9 - (-3) - 11 \equiv 2 - 0 - 0 - 2 - 0 - 0 - 6 - 2 \equiv -8 \equiv 1 \pmod{9}$. So, $k = 1$.

Note that in each part, k is the remainder when the expression is divided by the modulus.

Exercise 7

Observe that $15 \equiv 3 \pmod{4}$, $21 \equiv 1 \pmod{4}$, and $88 \equiv 0 \pmod{4}$. Find an integer k, where $0 \leq k < 4$, which is congruent to the following products **modulo 4** by using modular multiplication to simplify the calculations.

a) 15×21 b) 21×15 c) $88 \times 21 \times 15$ d) $15 \times 15 \times 21 \times 15$

Exercise 7 Solution

a) $15 \times 21 \equiv 3 \times 1 \equiv 3 \pmod{4}$. So, $k = 3$.

b) $21 \times 15 \equiv 1 \times 3 \equiv 3 \pmod{4}$. So, $k = 3$.

c) $88 \times 21 \times 15 \equiv 0 \times 1 \times 3 \equiv 0 \pmod{4}$. So, $k = 0$.

d) $15 \times 15 \times 21 \times 15 \equiv 3 \times 3 \times 1 \times 3 \equiv 27 \equiv 24 + 3 \equiv 3 \pmod{4}$. So, $k = 3$.

Note that in each part, k is the remainder when the expression is divided by the modulus.

Exercise 8

Observe that $23 \equiv 3 \pmod{10}$, $21 \equiv 1 \pmod{10}$, and $1430 \equiv 0 \pmod{10}$. Find an integer k, where $0 \leq k < 10$, which is congruent to the following powers **modulo 10** by using modular exponentiation to simplify the calculations.

a) 23^3 b) 21^8 c) 1430^{33429}

Exercise 8 Solution

a) $23^3 \equiv 3^3 \equiv 27 \equiv 7 \pmod{10}$. So, $k = 7$.

b) $21^8 \equiv 1^8 \equiv 1 \pmod{10}$. So, $k = 1$.

c) $1430^{33429} \equiv 0^{33429} \equiv 0 \pmod{10}$. So, $k = 0$.

Note that in each part, k is the remainder when the expression is divided by the modulus.

Problem Set Solutions

For an extra challenge try to complete all the problems without using a calculator.

1. Fill in the blank with either $\equiv$ or $\not\equiv$.

a) $-3 \underline{\quad\quad} 7 \pmod{5}$ b) $-10 \underline{\quad\quad} 12 \pmod{11}$ c) $3 \underline{\quad\quad} 10 \pmod{4}$
d) $7 \underline{\quad\quad} -43 \pmod{2}$ e) $8 \underline{\quad\quad} 104 \pmod{8}$ f) $89 \underline{\quad\quad} 1 \pmod{9}$

Problem 1 Solution

a) $-3 \div 5$ has remainder 2 and $7 \div 5$ has remainder 2, so $-3 \equiv 7 \pmod{5}$.

b) $-10 \div 11$ has remainder 1 and $12 \div 11$ has remainder 1, so $-10 \equiv 12 \pmod{11}$.

c) $3 \div 4$ has remainder 3 and $10 \div 4$ has remainder 2, so $3 \not\equiv 10 \pmod{4}$.

d) $7 \div 2$ has remainder 1 and $-43 \div 2$ has remainder 1, so $7 \equiv -43 \pmod{2}$.

e) $8 \div 8$ has remainder 0 and $104 \div 8$ has remainder 0, so $8 \equiv 104 \pmod{8}$.

f) $89 \div 9$ has remainder 8 and $1 \div 9$ has remainder 1, so $89 \not\equiv 1 \pmod{9}$.

2. Fill in the blank with either $\equiv$ or $\not\equiv$.

a) $2 \underline{\quad\quad} 47 \pmod{1}$

b) $-2448 \underline{\quad\quad} 39202 \pmod{1}$

c) $a \underline{\quad\quad} b \pmod{1}$ for any integers a and b

Problem 2 Solution

a) $2 \div 1$ has remainder 0 and $47 \div 1$ has remainder 0, so $2 \equiv 47 \pmod{1}$.

b) $-2448 \div 1$ has remainder 0 and $39202 \div 1$ has remainder 0, so $-2448 \equiv 39202 \pmod{1}$.

c) $a \div 1$ has remainder 0 and $b \div 1$ has remainder 0, so $a \equiv b \pmod{1}$ for any integers a and b.

3. List three integers which are congruent to k modulo m given the following values for k and m.

a) $k = 9,\ m = 21$ b) $k = -19,\ m = 3$ c) $k = 87,\ m = 7$

d) $k = 0,\ m = 15$ e) $k = -2,\ m = 2$ f) $k = -11,\ m = 8$

Problem 3 Solution

Responses will vary, below are some examples.

a) $-12,\ 30,\ 51$ b) $-22,\ -16,\ -13$ c) $80,\ 94,\ 101$

d) $-15,\ 15,\ 30$ e) $-4,\ 0,\ 2$ f) $-19,\ -3,\ 5$

4. What is the remainder when...

a) 320×84^7 is divided by 3? b) 22928^3 is divided by 5?

c) 17^{404} is divided by 15? d) $97 - 106^2 + 100^{429}$ is divided by 9?

e) $(19 \times 239) + 282^6$ is divided by 20? f) $1430 \times (11 + 153^{200064})$ is divided by 14?

Problem 4 Solution

a) Observe that $320 \equiv 300 + 18 + 2 \equiv 0 + 0 + 2 \equiv 2 \pmod{3}$ and $84 \equiv 90 - 6 \equiv 0 - 0 \equiv 0 \pmod{3}$.

$$\begin{aligned} 320 \times 84^7 &\equiv 2 \times 0^7 && \pmod{3} \\ &\equiv 2 \times 0^7 && \pmod{3} \\ &\equiv 2 \times 0 && \pmod{3} \\ &\equiv 0 && \pmod{3} \end{aligned}$$

So, 0 is the remainder when 320×84^7 is divided by 3.

b) Observe that $22928 \equiv 22925 + 3 \equiv 0 + 3 \equiv 3 \pmod{5}$.

$$\begin{aligned} 22928^3 &\equiv 3^3 && \pmod{5} \\ &\equiv 27 && \pmod{5} \\ &\equiv 25 + 2 && \pmod{5} \\ &\equiv 0 + 2 && \pmod{5} \\ &\equiv 2 && \pmod{5} \end{aligned}$$

So, 2 is the remainder when 22928^3 is divided by 5.

c) Observe that $17 \equiv 15 + 2 \equiv 0 + 2 \equiv 2 \pmod{15}$.

$$\begin{aligned}
17^{404} &\equiv 2^{404} && \pmod{15}\\
&\equiv 2^{4\times 101} && \pmod{15}\\
&\equiv (2^4)^{101} && \pmod{15}\\
&\equiv 16^{101} && \pmod{15}\\
&\equiv 1^{101} && \pmod{15}\\
&\equiv 1 && \pmod{15}
\end{aligned}$$

So, 1 is the remainder when 17^{404} is divided by 15.

d) Observe that $97 \equiv 90 + 7 \equiv 0 + 7 \equiv 7 \pmod 9$, $106 \equiv 108 - 2 \equiv 0 - 2 \equiv -2 \pmod 9$, and $100 \equiv 99 + 1 \equiv 0 + 1 \equiv 1 \pmod 9$.

$$\begin{aligned}
97 - 107^2 + 100^{429} &\equiv 7 - (-2)^2 + 1^{429} && \pmod 9\\
&\equiv 7 - 4 + 1 && \pmod 9\\
&\equiv 4 && \pmod 9
\end{aligned}$$

So, 4 is the remainder when $97 - 106^2 + 100^{429}$ is divided by 9.

e) Observe that $19 \equiv -1 \pmod{20}$, $239 \equiv 220 + 19 \equiv 0 + (-1) \equiv -1 \pmod{20}$, and $282 \equiv 280 + 2 \equiv 0 + 2 \equiv 2 \pmod{20}$.

$$\begin{aligned}
(19 \times 239) + 282^6 &\equiv ((-1) \times (-1)) + 2^6 && \pmod{20}\\
&\equiv 1 + 64 && \pmod{20}\\
&\equiv 65 && \pmod{20}\\
&\equiv 60 + 5 && \pmod{20}\\
&\equiv 0 + 5 && \pmod{20}\\
&\equiv 5 && \pmod{20}
\end{aligned}$$

So, 5 is the remainder when $(19 \times 239) + 282^6$ is divided by 20

f) Observe that $1430 \equiv 1428 + 2 \equiv 0 + 2 \equiv 2 \pmod{14}$ and $153 \equiv 140 + 13 \equiv 0 + 13 \equiv 13 \equiv -1 \pmod{14}$.

$$\begin{aligned}
1430 \times (11 + 153^{200064}) &\equiv 2 \times (11 + (-1)^{200064}) &&\pmod{14}\\
&\equiv 2 \times (11 + (-1)^{2\times 100032} &&\pmod{14}\\
&\equiv 2 \times (11 + ((-1)^{2})^{100032}) &&\pmod{14}\\
&\equiv 2 \times (11 + 1^{100032}) &&\pmod{14}\\
&\equiv 2 \times (11 + 1) &&\pmod{14}\\
&\equiv 2 \times 12 &&\pmod{14}\\
&\equiv 24 &&\pmod{14}\\
&\equiv 10 &&\pmod{14}
\end{aligned}$$

So, 10 is the remainder when $1429 \times (11 + 153^{200064})$ is divided by 14.

5. What is the last digit of $(391^{283} + 28917 - 283^{4}) \times 85$?

Problem 5 Solution

The last digit of an integer is just the remainder when divided by 10.

$$\begin{aligned}
(391^{283} + 28917 - 283^{4}) \times 85 &\equiv (1^{283} + 7 - 3^{4}) \times 5 &&\pmod{10}\\
&\equiv (1 + 7 - 81) \times 5 &&\pmod{10}\\
&\equiv (1 + 7 - 1) \times 5 &&\pmod{10}\\
&\equiv 7 \times 5 &&\pmod{10}\\
&\equiv 35 &&\pmod{10}\\
&\equiv 5 &&\pmod{10}
\end{aligned}$$

So, the last digit is 5.

6. Gus baked 10 trays of muffins to share with his class. Each tray contained 12 muffins. Gus split the muffins evenly between his 22 classmates and his teacher and then he ate the leftovers. How many muffins did Gus eat?

Problem 6 Solution

Gus split the muffins between 23 people, so we have a modulus of 23. The total number of muffins was 10×12. We have $10 \times 12 \equiv 5 \times 2 \times 12 \equiv 5 \times 24 \equiv 5 \times 1 \equiv 5 \pmod{23}$, so there were 5 leftover muffins which Gus ate.

7. A card game involves removing one random card from a regular deck of 52 cards by each player Then, the remaining cards are dealt between all the players. For each of the following number of players, does each player have the same amount of cards?

a) 2 players b) 3 players c) 5 players d) 13 players

Problem 7 Solution

a) There are 2 players, so $52 - 2 = 50$ cards are dealt between the 2 players. $50 \equiv 0 \pmod{2}$, so each player has the same amount of cards.

b) There are 3 players, so $52 - 3 = 49$ cards are dealt between the 3 players. $49 \equiv 48 + 1 \equiv 0 + 1 \equiv 1 \pmod{3}$, so 1 player will have one more card than there other 2 players.

c) There are 5 players, so $52 - 5 = 47$ cards are dealt between the 5 players. $47 \equiv 45 + 2 \equiv 0 + 2 \equiv 2 \pmod{5}$, so 2 players will have one more card than the other 3 players.

d) There are 13 players, so $52 - 13 = 39$ cards are dealt between the 13 players. $39 \equiv 0 \pmod{13}$, so each player has the same amount of cards.

8. Morgan, Milly, and Baloo are playing a game and need to decide who will go first. They decide that the decision should be random, so the numbers 0, 1, and 2 are all uniquely assigned to the three of them and each of them will hold up a random number of fingers (from 0 to 10) at the same time. Whoever's assigned number is congruent modulo 3 to the total number of fingers held up gets to go first.

Who will go first if Morgan is assigned 0 and holds up 6 fingers, Milly is assigned 1 and holds up 1 finger, and Baloo is assigned 2 and holds up 9 fingers?

Problem 8 Solution

The sum of fingers is $6 + 1 + 9 = 16$. So, we have $16 \equiv 15 + 1 \equiv 0 + 1 \equiv 1 \pmod{3}$ and so Milly will go first.

9. What day of the week were you born on? Work backwards from your last or next birthday.

   Hint: The years 2020, 2016, 2012, 2008, 2004, and 2000 were all leap years, that is, these years contained 366 days instead of 365.

   Once you've found the day of the week, check your answer by looking at a calendar from your birth year.

Problem 9 Solution

Responses will vary. Below is an example using my birthday.

My last birthday was on a Sunday and I turned 20. There have been 5 leap years since I was born so

$$\begin{aligned}
(15 \times 365) + (5 \times 366) &\equiv (1 \times 365) + (-2 \times 366) && \pmod{7}\\
&\equiv (350 + 15) + (-2 \times (350 + 16)) && \pmod{7}\\
&\equiv (0 + 1) + (-2 \times (0 + 2)) && \pmod{7}\\
&\equiv 1 + (-4) && \pmod{7}\\
&\equiv -3 && \pmod{7}\\
&\equiv 4 && \pmod{7}
\end{aligned}$$

And, since we are thinking about the past, this means that I was born four days **before** a Sunday. So, we count backwards from Sunday (Sat, Fri, Thu, Wed) and that means I was born on a Wednesday.

Congruence Classes

Two integers are congruent modulo m if they have the same remainder when divided by a positive integer m. Is there a way to define all integers that are congruent modulo m?

Congruence classes are sets of integers which have the same remainder when divided by a positive integer m. That is, all integers in a congruence class are congruent modulo m. We denote a congruence class as $[a]$ where a is the remainder.

Recall that the remainder of a division, using divisor n, is an integer between 0 and $n-1$. So, congruence classes for modulus m only exist from 0 to $m-1$.

Example

We can organize integers into congruence classes with modulus m by finding which integer from 0 to $m-1$ each integer is congruent with. For example, with modulus 5, we can write the congruences for the integers 1 to 14 as seen below:

$$\begin{array}{lll} 0 \equiv 0 \pmod{5} & 5 \equiv 0 \pmod{5} & 10 \equiv 0 \pmod{5} \\ 1 \equiv 1 \pmod{5} & 6 \equiv 1 \pmod{5} & 11 \equiv 1 \pmod{5} \\ 2 \equiv 2 \pmod{5} & 7 \equiv 2 \pmod{5} & 12 \equiv 2 \pmod{5} \\ 3 \equiv 3 \pmod{5} & 8 \equiv 3 \pmod{5} & 13 \equiv 3 \pmod{5} \\ 4 \equiv 4 \pmod{5} & 9 \equiv 4 \pmod{5} & 14 \equiv 4 \pmod{5} \end{array}$$

Using these congruences, we can organize the integers 1-14 into their respective congruence classes.

- 0, 5, and 10 belong to the same congruence class, $[0] = \{..., -15, -10, -5, 0, 5, 10, 15, ...\}$
- 1, 6, and 11 belong to the same congruence class, $[1] = \{..., -14, -9, -4, 1, 6, 11, 16, ...\}$
- 2, 7, and 12 belong to the same congruence class, $[2] = \{..., -13, -8, -3, 2, 7, 12, 17, ...\}$
- 3, 8, and 13 belong to the same congruence class, $[3] = \{..., -12, -7, -2, 3, 8, 13, 18, ...\}$
- 4, 9, and 14 belong to the same congruence class, $[4] = \{..., -11, -6, -1, 4, 9, 14, 19, ...\}$

10. How many congruence classes are there for each modulus?

a) 1 b) 2 c) 3 d) n where n is any positive integer

Problem 10 Solution

a) There is 1 congruence class for modulus 1: [0].

b) There are 2 congruence classes for modulus 2: [0], [1].

c) There are 3 congruence classes for modulus 3: [0], [1], [2].

d) There are n congruence classes for modulus n: [0], [1], ..., $[n-1]$.

11. What congruence classes exist for the following moduli (plural of modulus)? List 3 numbers that belong to each congruence class.

a) 3 b) 6 c) 1 d) 2

Problem 11 Solution

a) The congruences classes with modulus 3 are [0], [1], and [2].

- -3, 0, and 3 belong to [0]
- -2, 1, and 4 belong to [1]
- -1, 2, and 5 belong to [2]

b) The congruences classes with modulus 6 are [0], [1], [2], [3], [4], and [5].

- -6, 0, and 6 belong to [0]
- -5, 1, and 7 belong to [1]
- -4, 2, and 8 belong to [2]
- -3, 3, and 9 belong to [3]
- -2, 4, and 10 belong to [4]
- -1, 5, and 11 belong to [5]

c) The congruences class with modulus 1 is [0].

- -1, 0, and 1 belong to [0]

d) The congruences classes with modulus 2 are [0] and [1].

- -2, 0, and 2 belong to [0] *Note that all even integers belong to [0] with modulus 2
- -1, 1, and 3 belong to [1] *Note that all odd integers belong to [1] with modulus 2

Modular Addition with Congruence Classes

The basic idea of modular addition is that we are just adding the remainders while multiples of the modulus are ignored. And since congruence classes are defined by their remainders, we can see that if we have two congruence classes, then the sum of two integers where one is from each of the two congruence classes will always be the same no matter which integers were picked from the congruence classes.

Modular Addition with Congruence Classes

Suppose that a and b are integers and that $[a]$ and $[b]$ are two congruence classes with modulus m. We can define modular addition as $[a] + [b] = [s]$ where $a + b \equiv s \pmod{m}$ and $0 \leq s < m$.

We can now build addition tables that will provide us with all the addition results between any congruence classes with a specific modulus. For example, to the right is an addition table for all congruence classes with modulus 7.

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[0]	[1]	[2]	[3]	[4]	[5]

Example

Since $11 \equiv 4 \pmod{7}$ and $8 \equiv 1 \pmod{7}$, $11 + 8 \equiv 4 + 1 \equiv 5 \pmod{7}$.
Similarly, since $18 \equiv 4 \pmod{7}$ and $78 \equiv 1 \pmod{7}$, $18 + 78 \equiv 4 + 1 \equiv 5 \pmod{7}$.

Both 11 and 18 belong to the congruence class [4] and both 8 and 78 belong to the congruence class [1] with modulus 7.

Notice that $11 + 8$ and $18 + 78$ are both congruent to 5 modulo 7. Looking at our above addition table for modulus 7, we can see that $[4] + [1] = [5]$ by finding the row and column intersections as highlighted in the table. This means that the sum of any integer which is congruent to 4 modulo 7 and any integer which is congruent to 1 modulo 7 will be congruent to 5 modulo 7.

12. Perform the following additions on the congruence classes with modulus 7 using the above addition table.

    a) $[3] + [5]$ b) $[5] + [3]$ c) $[2] + [2]$ d) $[6] + [1]$ e) $[0] + [4]$

Problem 12 Solution

a) $[3] + [5] = [1]$

b) $[5] + [3] = [1]$

c) $[2] + [2] = [4]$

d) $[6] + [1] = [0]$

e) $[0] + [4] = [4]$

Modular Multiplication with Congruence Classes

The basic idea of modular multiplication is that we are just multiplying the remainders and multiples of the modulus are ignored. And since congruence classes are defined by their remainders, we can see that if we have two congruence classes, then the product of two integers where one is from each of the two congruence classes will always be the same no matter which integers were picked from the congruence classes.

Modular Multiplication with Congruence Classes

Suppose that a and b are integers and that $[a]$ and $[b]$ are two congruence classes with modulus m. We can define modular multiplication as $[a] \times [b] = [s]$ where $a \times b \equiv s \pmod{m}$ and $0 \leq s < m$.

We can now build multiplication tables that will provide us with all the multiplication results between any congruence classes with a specific modulus. For example, to the right is a multiplication table for all congruence classes with modulus 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]

Example

Since $11 \equiv 4 \pmod{7}$ and $8 \equiv 1 \pmod{7}$, $11 \times 8 \equiv 4 \times 1 \equiv 4 \pmod{7}$.
Similarly, since $18 \equiv 4 \pmod{7}$ and $78 \equiv 1 \pmod{7}$, $18 \times 78 \equiv 4 \times 1 \equiv 4 \pmod{7}$.

Both 11 and 18 belong to the congruence class $[4]$ and both 8 and 78 belong to the congruence class $[1]$ with modulus 7.

Notice that 11×8 and 18×78 are both congruent to 4 modulo 7. Looking at our above multiplication table for modulus 7, we can see that $[4] \times [1] = [4]$ by finding the row and column intersections as highlighted in the table. This means that the product of any integer which is congruent to 4 modulo 7 and any integer which is congruent to 1 modulo 7 will be congruent to 4 modulo 7.

13. Perform the following multiplications on the congruence classes with modulus 7 using the above multiplication table.

a) $[2] \times [5]$ b) $[5] \times [2]$ c) $[3] \times [3]$ d) $[6] \times [1]$ e) $[0] \times [4]$

Problem 13 Solution

a) $[2] \times [5] = [3]$

b) $[5] \times [2] = [3]$

c) $[3] \times [3] = [2]$

d) $[6] \times [1] = [6]$

e) $[0] \times [4] = [0]$