

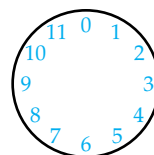


5.4 MODULAR ARITHMETIC

Until the 1800s, whole number arithmetic was done one way. In fact, statements like $8 + 8 = 16$ were thought of as absolute truths. In the 1800s, new types of arithmetic, algebra, and geometry were developed that changed this view of mathematics. Modular arithmetic was one of the new types of arithmetic.

CLOCK ARITHMETIC

Clock arithmetic can be used to introduce modular arithmetic. Consider arithmetic that only uses the numbers on a clock except that 0 replaces 12. The set of numbers for clock arithmetic is: $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$.



Clock arithmetic refers to the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ and the rules for adding, subtracting, multiplying, and dividing these numbers. The symbols for clock arithmetic are $+$, $-$, \times , \div .

What is $8 + 8$ in clock arithmetic? It can't be 16 since there is no number 16. From now on, write $8 + 8$ in mod 12 as $8 \oplus 8$ to distinguish it from $8 + 8$ in base 10.

• EXAMPLE 1

$$8 \oplus 8 = \underline{\hspace{2cm}}$$

SOLUTION

If I start at 8 on the clock and move 8 hours clockwise, where do I end up? At 4. Therefore, $8 \oplus 8 = 4$. ●

LE 1

Compute $4 \oplus 10$ in clock arithmetic.

LE 2

Solve for x in the clock arithmetic system if $x \oplus 10 = 3$.

LE 3

Suppose it is now June (the 6th month).

- What month is 9 months later?
- Write a clock addition equation that supports your answer to part (a).

How would clock subtraction work? Clock subtraction can be defined in terms of addition. For example, $4 \ominus 7 = x$ if and only if $4 = 7 \oplus x$. Subtraction can also be done by counting back on a clock.

• **EXAMPLE**

$$4 \ominus 7 = \underline{\hspace{2cm}}$$

SOLUTION

$4 \ominus 7$ means start at 4 and count back 7.

Where do I end up? 9. So $4 \ominus 7 = 9$.

Check it using addition. Does $7 \oplus 9 = 4$? Yes. ●

LE 4

(a) $6 \ominus 10 = \underline{\hspace{2cm}}$

(b) Write an equivalent addition equation.

LE 5

Suppose it is now April (4th month).

(a) What month is 7 months earlier?

(b) Write a clock subtraction equation that supports your answer to part (a).

Clock multiplication can be defined as repeated addition. For example, $3 \otimes 5 = 5 \oplus 5 \oplus 5 = 3$. Clock division can be defined as the inverse of multiplication. For example, $2 \oslash 3 = n$ if and only if $2 = 3 \otimes n$.

• **EXAMPLE 3**

Compute: (a) $5 \otimes 8$ and (b) $2 \oslash 3$ in clock arithmetic.

SOLUTION

(a) $5 \otimes 8 = 8 \oplus 8 \oplus 8 \oplus 8 \oplus 8 = 4$ or using a clock, $5 \otimes 8 = 40$.
Go 40 hours clockwise from 12 and you end up at 4. So $5 \otimes 8 = 4$.

(b) $2 \oslash 3 = n$ means $3 \otimes n = 2$. The multiples of 3 in clock arithmetic are 3, 6, 9, and 12. So $3 \otimes n = 2$ and $2 \oslash 3 = n$ have no solution. ●

LE 6

Compute $11 \oslash 7$ in clock arithmetic.

LE 7

Starting at midnight, 6 people work back-to-back 5-hour shifts.

(a) What time will the 6 shifts end?

(b) Write a clock multiplication equation that supports your answer to part (a).

MODULAR ARITHMETIC

Modular arithmetic is clock arithmetic extended to include all integers. Any integer is considered equivalent to one of the clock numbers. For example, -10 , 14 , and 26 are equivalent to 2 on the 12-hour clock.

LE 8

(a) List the set of all integers that are equivalent to 2 on the 12-hour clock.

(b) If you subtract 2 from each number in part (a), what set of numbers do you obtain?

LE 8 suggests that the set of equivalent numbers, termed congruent mod 12, and written $\dots \equiv -22 \pmod{12} \equiv -10 \pmod{12} \equiv 2 \pmod{12} \equiv 14 \pmod{12} \equiv \dots$. All these numbers have a remainder of 2 when they are divided by 12, or put differently, any of these numbers minus 2 results in an integer multiple of 12.

Definition: Congruence Mod M

For integers a and b , a is **congruent to b mod M** , written $a \equiv b \pmod{M}$ if and only if $a - b$ is an integer multiple of M where M is a whole number greater than 1.

LE 9

Use this definition to explain why $116 \equiv 8 \pmod{9}$.

Modular arithmetic can be done on other sized “clocks.” Figure 5–5 shows a mod 5 clock. It has 5 numbers.

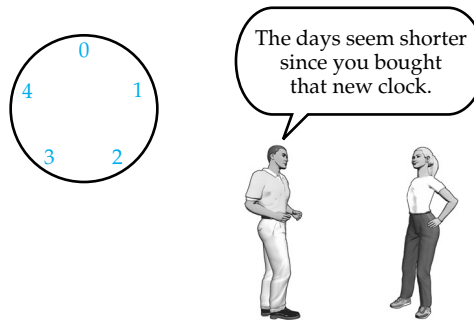


Figure 5–5

In fact, a clock can be made for any counting number beginning with 0 and counting by ones. Such a clock with the M numbers $\{0, 1, 2, \dots, M-1\}$ and rules for addition, subtraction, multiplication, and division comprises a mod M arithmetic system.

LE 10

Explain why $-3 \equiv 12 \pmod{5}$.

LE 11

Complete the following mod 5 addition table.

\oplus	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2					
3					
4					

You can also use the addition table to do mod 5 subtraction.

• **EXAMPLE 4**

Compute $2 \ominus 4$ in mod 5 using the addition table.

SOLUTION

$2 \ominus 4 = \underline{\hspace{2cm}}$ means $4 \oplus \underline{\hspace{2cm}} = 2$. Use the table to find out what number added to 4 will result in 2. Look in the column labeled 4. Go down until you find 2.

\oplus					4
3					2

What number is at the left of the row? 3. So $4 \oplus 3 = 2$ which means $2 \ominus 4 = 3$. ●

LE 12

Compute $3 \ominus 4$ using the mod 5 addition table.

Does mod 5 addition have the same properties as integer addition? For example, is mod 5 addition commutative? Since it is a finite system, it is possible to check every result.

$$\begin{array}{lll}
 \text{Does: } 0 \oplus 0 = 0 \oplus 0? & 1 \oplus 1 = 1 \oplus 1? & 2 \oplus 3 = 3 \oplus 2? \\
 0 \oplus 1 = 1 \oplus 0? & 1 \oplus 2 = 2 \oplus 1? & 2 \oplus 4 = 4 \oplus 2? \\
 0 \oplus 2 = 2 \oplus 0? & 1 \oplus 3 = 3 \oplus 1? & 3 \oplus 3 = 3 \oplus 3? \\
 0 \oplus 3 = 3 \oplus 0? & 1 \oplus 4 = 4 \oplus 1? & 3 \oplus 4 = 4 \oplus 3? \\
 0 \oplus 4 = 4 \oplus 0? & 2 \oplus 2 = 2 \oplus 2? & 4 \oplus 4 = 4 \oplus 4?
 \end{array}$$

Yes, all 15 of these equations are true. So mod 5 addition is commutative.

LE 13

Look at the mod 5 addition table. What pattern of numbers inside the table indicates that addition is commutative? (*Hint*: Compare the location of sums like $2 + 3$ and $3 + 2$.)

What about the identity property?

LE 14

The identity number I for mod 5 addition has the property that for any mod 5 number

$$N, N \oplus I = I \oplus N = N.$$

- (a) What is the identity element I for mod 5 addition described above?
 (b) What patterns in the addition table indicate an identity element?

LE 15

- (a) What is the additive inverse of 3 in mod 5?
 (b) Does every mod 5 number have an additive inverse in mod 5?

Next, investigate mod 5 multiplication.

LE 16

Complete the mod 5 multiplication table below.

\otimes	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0			1	3
3	0		1		
4	0		3		

Use your completed mod 5 multiplication table to answer the following questions.

LE 17

Is mod 5 multiplication commutative?

LE 18

- (a) What is the identity element for mod 5 multiplication?
 (b) What is the multiplicative inverse of 2?

Use the mod 5 multiplication table to solve the following division problem.

LE 19

- (a) Write $3 \oslash 2 = n$ in mod 5 as an equivalent multiplication equation.
 (b) Use the multiplication table to solve for n .

ANSWERS TO SELECTED LESSON EXERCISES

1. 2

2. $x = 5$ 3. (a) March (b) $6 \oplus 9 = 3$ 4. (a) 8 (b) $8 \oplus 10 = 6$ 5. (a) September (b) $4 \ominus 7 = 9$

6. 5

7. (a) 6 AM (b) $5 \otimes 6 = 6$ 8. (a) $\{\dots, -22, -10, 2, 14, \dots\}$
 (b) The integer multiples of 129. $116 - 8$ is an integer multiple of 9.10. $-3 - 12$ is an integer multiple of 5.

12. 4

13. Numbers above and below the diagonal (lower left to upper right) match up

14. (a) 0
 (b) A row and column match the numbers along the outside of the table.

15. (a) 2 (b) Yes

16.

\otimes	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

17. Yes

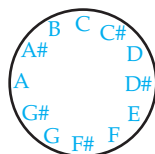
18. (a) 1 (b) 3

19. (a) $n \otimes 2 = 3$ (b) $n = 4$

5.4 HOMEWORK EXERCISES

Basic Exercises

- Compute the following in 12-hour clock arithmetic.
 - $6 \oplus 8$
 - $5 \ominus 7$
 - $4 \otimes 6$
- Suppose it is now November (11th month).
 - What month is 8 months later?
 - Write a 12-hour clock addition equation that supports your answer to part (a).
- You have to take a medication every 6 hours for 5 days starting at 7 AM. Explain why you will never have to take medication between 2 AM and 6 AM.
- A musical scale has 12 half-tones that correspond to the 12-hour clock.



What note is 6 half-tones above A?

- A three-way bulb works with a switch that has settings for off, low, medium, and high. What mod system would be a model for this?
- Compute the following in mod 5.
 - $3 \oplus 4$
 - $2 \ominus 1$
 - $3 \otimes 4$
- Compute the following using the mod 5 multiplication table in the lesson.
 - $3 \oplus 4$
 - $4 \oplus 3$
 - The results to parts (a) and (b) prove that mod 5 division is not _____.

- Write the set of numbers that are congruent to 3 (mod 7).
- Explain why $39 \equiv 4 \pmod{7}$.
- Explain why $19 \equiv 41 \pmod{11}$.
- Construct an addition table for mod 7.
 - Use it to compute $5 \ominus 6$ in mod 7.
 - What is the identity number for mod 7 addition?
- Is mod 7 addition commutative?
- Construct a multiplication table for mod 7.
 - Use it to compute $3 \oplus 2$ in mod 7.
 - What is the identity number for mod 7 multiplication?
- Is mod 7 multiplication commutative?
- Suppose today is Thursday (5th day of the week).
 - What day is 4 days later?
 - Write a mod 7 addition equation that supports your answer to part (a).
- What day of the week is it 100 days after Tuesday?
- Construct an addition table for mod 4.
 - Use it to compute $1 \ominus 2$ in mod 4.
- Is mod 4 addition commutative?
- Construct a multiplication table for mod 4.
 - Use it to compute $2 \oplus 3$ in mod 4.
 - Use it to compute $1 \oplus 2$ in mod 4.
 - Name another division problem in mod 4 that has no answer.

20. Is mod 4 multiplication commutative?
21. Find all integer values of x if $x \ominus 3 \equiv 6 \pmod{8}$.
22. Find all integer values of x if x times $x \equiv 1 \pmod{4}$.
23. Find all integer values of x if $3x \equiv 8 \pmod{7}$.
24. Consider the following problem: "Suppose it is now 6 PM. What time will it be in 1 million hours?"
 (a) Devise a plan.
 (b) Solve the problem.

Extension Exercises

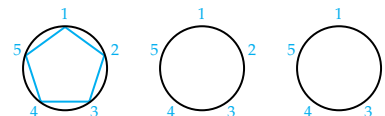
25. Consider the following problem: "What is the last digit of 3^{50} ?"
 (a) Devise a plan.
 (b) Solve the problem.
26. What is the last digit of 8^{27} ?
27. April 5, 2001 was a Thursday. What day of the week was April 5, 2002?
28. Jan. 1, 1994 was a Saturday. What day of the week was Jan. 1, 1997?
29. Jan. 1, 2000 was a Saturday. What is the next year Jan. 1 fell on a weekend?
30. What day of the week is your birthday in the year 2010?
31. The lesson and homework exercises have included mod 4, 5, 7, and 12. The multiplicative identity for all these systems is 1.
 (a) For which of these mods do all nonzero numbers have a multiplicative inverse?
 (b) What property of M determines whether or not all nonzero numbers in mod M have a multiplicative inverse in mod M ?
32. Show that if $a \equiv 0 \pmod{M}$ then M is a factor of a .

33. True or false? a , b , and c are integers and M is a whole number greater than 1. If $ac \equiv bc \pmod{M}$ then $a \equiv b \pmod{M}$. If it's true, give an example. If it's false, give a counterexample.
34. If n is an integer, does $n^p \equiv n \pmod{M}$ for $M \geq 2$? Try the following and state your conclusion.
 (a) Does $n^2 \equiv n \pmod{2}$?
 (b) Does $n^3 \equiv n \pmod{3}$?
 (c) Does $n^4 \equiv n \pmod{4}$?

Labs and Projects

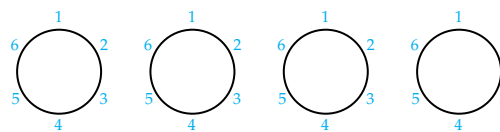
You can obtain some interesting designs by connecting equally spaced points on a mod M clock (actually a circle).

35. First, work with 5 equally spaced points on a circle.



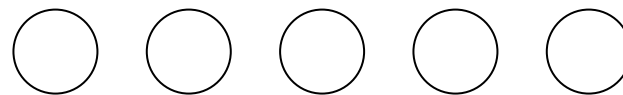
- (a) On the second circle, connect 1 to 3, 2 to 4, 3 to 5, 4 to 1, and 5 to 2.
 (b) On the third circle, connect 1 to 4, 2 to 5, and so on.
 (c) What would you obtain if you connect each point to the point which is 4 places on (such as 1 to 5)?

- 36.



Find all possible designs you can make by connecting points in the same manner as in Exercise 35.

37. (a) Predict how many different patterns you would obtain for 7 equally spaced points.



- (b) Find all possible designs for the 7 points on a circle.

5.4 ANSWERS TO SELECTED HOMEWORK EXERCISES

1. (a) 2 (b) 10 (c) 0
3. It will always be at 7 AM, 1 PM, 7 PM, or 1 AM.
5. mod 4
7. (a) 2 (b) 3 (c) Commutative
9. $39 - 4$ is a multiple of 7.
21. $\dots, -7, 1, 9, 17, \dots$
23. $\dots, -2, 5, 12, 19, \dots$
25. (b) 9
27. Friday
11. (b) 6 (c) 0
13. (b) 5 (c) 1
15. (a) Monday (b) $5 \oplus 4 \equiv 2 \pmod{7}$
17. (b) 3
19. (b) 2 (c) No solution (d) $3 \div 2$
29. 2005
31. (a) 5, 7 (b) M is prime
33. False for $a = 8, b = 4, c = 2, M = 8$