Introduction To Modular Arithmetic

Olga Radko
radko@math.ucla.edu

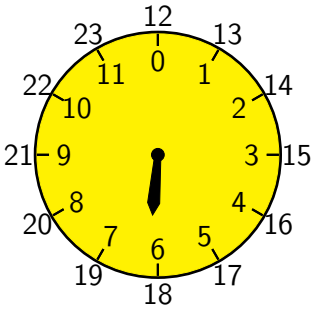
Oleg Gleizer
oleg1140@gmail.com

Warm Up Problem

It takes a grandfather's clock 30 seconds to chime 6 o'clock. Assuming that the time of each chime is negligible compared to the time intervals between the chimes, how much time would it take the clock to chime 12?

Clock Arithmetic or a Circle as a Number Line

One way to turn a circle into a number line is to divide it into twelve equal parts. In this case, one step is usually called one hour.



Notice that 0 coincides with 12, and as the hour hand moves to the right, 1 coincides with 13, 2 with 14, and so on. The hour hand rotates clockwise which corresponds with numbers increasing when moving to the right on a number line. However, 12 is equivalent to 0 on this circle, which can be written as follows:

$$12 \equiv 0 \pmod{12}.$$

This can be read as *12 is congruent to 0 modulo 12.* The usual " = " sign is reserved for the straight number line; we use " $\equiv$ " on the circle instead. The symbol "mod 12" tells us that the circle is divided into 12 equal parts, so that 12 coincides with 0, 13 with 1, etc. In the new notation we have:

$$12 \equiv 0 \pmod{12}, \qquad 13 \equiv 1 \pmod{12}, \quad \ldots \quad 23 \equiv 11 \pmod{12}$$

1. Please reduce the following numbers in modular arithmetic.

   (a) $18 \equiv$ (mod 12)

   (b) $25 \equiv$ (mod 12)

   (c) $36 \equiv$ (mod 12)

2. Recall that if you move to the left of 0 on a number line, you get negative numbers. Similarly, going in the opposite direction (counterclockwise) on the number circle, we get to negative numbers in modular arithmetic. For example,

   $$-1 \equiv 11 \pmod{12}, \qquad -25 \equiv 10 \pmod{12}.$$

   Use this to reduce the following numbers in mod 12 arithmetic (note that all answers must be between 0 and 11).

   (a) $-2 \equiv$ (mod 12)

   (b) $-4 \equiv$ (mod 12)

   (c) $-19 \equiv$ (mod 12)

3. We can also divide the clock into 60 equal parts. Depending on the situation, a unit step is called either a minute or a second. All of the numbers living on this number circle are considered modulo 60. More specifically, $60 \equiv 0$ (mod 60), which corresponds to the fact that there are 60 minutes in an hour (or 60 seconds in a minute).

   Reduce the following numbers in mod 60 arithmetic.

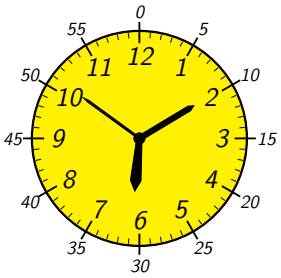
   (a) $72 \equiv$ (mod 60)

   (b) $135 \equiv$ (mod 60)

   (c) $-15 \equiv$ (mod 60)

   (d) $-80 \equiv$ (mod 60)

4. What is the time, in hours, minutes, and seconds, on the clock below?



- Notice that since $60 = 12 \times 5$, the same marks can be used to indicate a whole number of hours and a number of minutes which is a multiple of 5. (For example, the 4 hour mark is the same as the 20 minute mark).

The 24-Hour Clock

There are 24 hours in a day, so one more standard way to turn a circle into a number line is to divide it into 24 equal parts. The US military uses the 24 hour clock. The following is a photograph of the 24 hour clock from the USS (United States Ship) *Mullinex*.

USS *Mullinnix* 24-hour clock.[2]

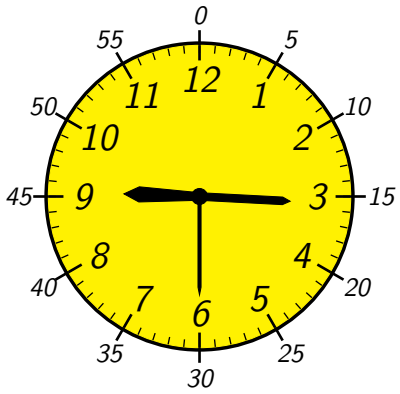
[1]See its homepage at `http://www.ussmullinnix.org/`

[2]Downloaded from `http://www.ussmullinnix.org/MuxMemorabilia.html`

Since 60 is not a multiple of 24, we can't use the same marks on the face of a 24 hour clock for minutes and hours (look at the minute marks on the face of the 24 hour clock).

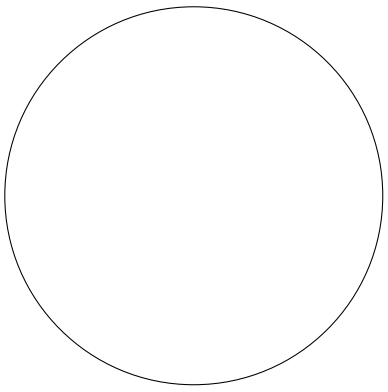
5. What time does the USS Mullinex clock show on the previous page?

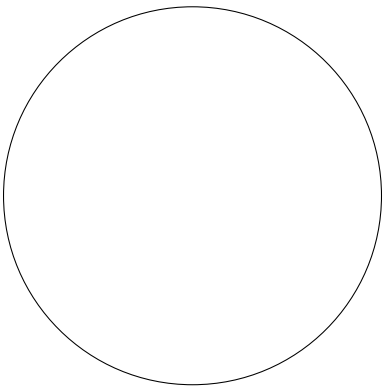
6. What is the time on the clock shown below?



If this time is in P.M, how would the military call this time?

7. On the left, draw the 12 hour clock showing 7 : 15 P.M. On the right, draw the military clock showing the same time.





Modular Arithmetic

In addition to clock analogy, one can view modular arithmetic as *arithmetic of remainders.*

For example, in mod 12 arithmetic, all the multiples of 12 (i.e., all the numbers that give remainder 0 when divided by 12) are equivalent to 0. In the modular arithmetic notation, this can be written as

$$12 \times n \equiv 0 \pmod{12} \text{ for any whole number } n.$$

Similarly, all numbers that give remainder 1 when divided by 12 are equivalent to 1. In other words,

$$12 \times n + 1 \equiv 1 \pmod{12} \text{ for any whole number } n.$$

Recall that any whole number a can be uniquely written in the form

$$a = 12 \times n + r$$

where r is one of the numbers 0, 1, ..., 11. Notice that r is the remainder of the division of a by 12. Therefore, $a \equiv r \pmod{12}$. For example,

$$-50 = -5 \times 12 + 10, \text{ which implies } -50 \equiv 10 \pmod{12},$$

$$40 = 3 \times 12 + 4, \text{ which means } 40 \equiv 4 \pmod{12}.$$

8. Write the following numbers in the form $a = 12 \times n + r$. Use this to reduce the given numbers in mod 12 arithmetic.

   (a) $45 = \_\_ \times 12 + \_\_$,

   $45 \equiv \_\_ \pmod{12}$.

   (b) $80 =$

   (c) $-18 =$

   (d) $-61 =$

9. Reduce the following negative numbers in mod 12 arithmetic.

   (a) $-11 \equiv$ (mod 12)

   (b) $-10 \equiv$ (mod 12)

   (c) $-9 \equiv$ (mod 12)

   (d) $-3 \equiv$ (mod 12)

   (e) $-2 \equiv$ (mod 12)

   (f) $-1 \equiv$ (mod 12)

   (g) What do you notice? If you are given a negative number between -12 and -1, how do you reduce it in mod 12 arithmetic? Why is this true?

   (h) Using your answer to part (g), complete the following formula

   $$-k \equiv \qquad \text{(mod 12)}$$

   where $k = 1, ..., 11$.

10. Similarly to how we used 12 and 60 as a modulus for modular arithmetic, any positive integer can be used. Moreover, we can define operations of addition and multiplication in the modular arithmetic:

    - To add two numbers in modular arithmetic, add them in the ordinary sense and then reduce (if necessary) in modular arithmetic;
    - To multiply two numbers in modular arithmetic, multiply them in the ordinary sense and then reduce (if necessary) in modular arithmetic;

    Fill in the addition and multiplication tables below in mod n, where $n = 4$, $n = 5$, and $n = 7$. Be sure to reduce all the numbers in the appropriate mod arithmetic.

(a) $n = 4$

+	0	1	2	3
0				
1				
2				
3				

x	0	1	2	3
0				
1				
2				
3				

(b) $n = 5$:

+	0	1	2	3	4
0					
1					
2					
3					
4					

x	0	1	2	3	4
0					
1					
2					
3					
4					

(c) $n = 7$:

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

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

11. Addition and multiplication are straightforward operations. Solving problems involving subtraction can be a little more difficult. We know that subtraction is the operation opposite to addition. For example, in the ordinary arithmetic, to subtract 3 from 4 means to find a number c such that $4 = 3 + c$. More generally,

$$a - b = c \quad \text{means that } a = b + \_\_.$$

Subtraction in the modular arithmetic is defined in a similar way.

Solve the following subtraction problems in modular arithmetic.

(a) $2 - 3 \equiv \qquad \pmod 4$

(b) $3 - 6 \equiv \qquad \pmod 7$

(c) $1 - 2 \equiv \qquad \pmod 3$

Now check your answers using addition in modular arithmetic.

(a) $2 \equiv 3 + \_\_ \pmod 4$

(b) $3 \equiv 6 + \_\_ \pmod 7$

(c) $1 \equiv 2 + \_\_ \pmod 3$

12. Division is the operation opposite to multiplication. For example, in ordinary arithmetic, to divide 3 by 4 means to need to find a number c such that $c \times 4 = 3$. Similarly, in modulo 7, to divide 3 by 4 means to find a number c such that:

$$c \times 4 \equiv 3 \pmod{7}.$$

c must be equivalent to one of the numbers 0, 1, 2 ..., 6 in mod 7. Using the multiplication table you made problem 10(c), we see that $c \equiv 6 \pmod{7}$. Thus, we write

$$3 \div 4 \equiv 6 \pmod{7}$$

This is true because $6 \times 4 \equiv 3 \pmod{7}$.

Please solve the following division problems in modular arithmetic (remember to use the tables you made).

(a) $1 \div 2 \equiv$ (mod 7)

(b) $1 \div 4 \equiv$ (mod 7)

(c) $2 \div 3 \equiv$ (mod 7)

(d) $4 \div 5 \equiv$ (mod 7)

(e) $5 \div 6 \equiv$ (mod 7)

(f) $1 \div 3 \equiv$ (mod 5)

(g) How could you solve part (f) without using the tables? (Hint: Use the fact that in mod arithmetic, 1 can be replaced by any number which gives remainder 1 when divided by 5)

Zero Divisors

13. In regular arithmetic, we know that if a product of two numbers is zero, then at least one of the numbers is zero. In modular arithmetic, this is not always the case.

    (a) Find two non-zero numbers in mod 4 arithmetic such that their product is 0.

    (b) Find two non-zero numbers in mod 6 arithmetic such that their product is 0.

    When the product of two non-zero numbers is equivalent to zero in modular arithmetic, these numbers are called *zero divisors*.

14. If x and y are zero divisors in mod n, where x and y can be the numbers 0, ..., $n-1$, what can be said about the value of $x \times y$?

15. Find all zero divisors in mod 12 arithmetic. Explain your answer.

16. Are there any zero divisors in mod 7 arithmetic? Explain your answer.

More Problems

17. If a biology experiment begins at $7:00$ A.M and runs for 80 hours, at what time will it end?

18. Cory's birthday lies on a Monday this year. What day of the week will his birthday be on in 2016?

19. Reduce the following numbers using modular arithmetic:

    (a) $136283 \times 192758237582389 \equiv \qquad \pmod 2$

    (b) $19342347328 + 1894837483 \equiv \qquad \pmod{10}$

    (c) $1934232 \times 1894837480 \equiv \qquad \pmod{10}$

20. Suppose hot dog buns come in packages of 34, and hot dogs come in packages of 8.

(a) What is the smallest number of packages of hot dogs and hot dog buns Ivy should buy if she doesn't want to have left-over hot dogs or left-over hot dog buns? (Assume that hot dogs can't be eaten without a bun, or vice versa).

(b) Suppose that hot dog buns come in packages of 33. What is the smallest number of packages of hot dogs and hot dog buns Ivy should buy now?

(c) Now assume hot dog buns come in packages of n. Write expressions that show how many packages of hot dog buns Ivy should buy. Note that there will be two expressions: one where the reduced form of n in mod 8 is divisible by 8, and one where it is not.