UNIVERSITY OF
WATERLOO

Faculty of Mathematics
Waterloo, Ontario N2L 3G1

Centre for Education in
Mathematics and Computing

Grade 6 Math Circles

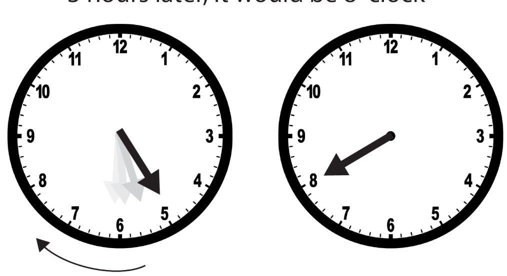
October 14^{th}, 2020

Modular Arithmetic

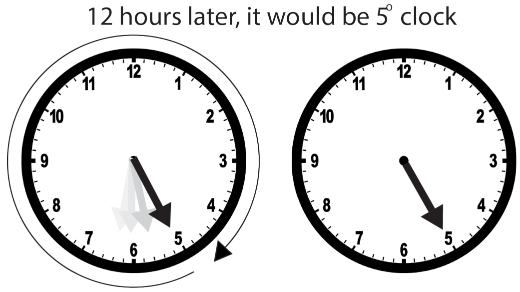
Modular Arithmetic is a system of arithmetic for integers that deals primarily with operations and applications regarding remainders. In this system, numbers "cycle" or repeat when reaching a certain value, called the **modulus**. We will begin to analyze what this means by referring to a tool we use everyday, a clock!

The 12-hour Clock

Let's look at a 12-hour analog clock. Suppose the clock reads 5 o'clock. **After 3 hours**, the clock would read 8 o'clock. This is found by simply adding 5 + 3 = 8.



What time would it be after 12 hours? **After 12 hours**, it would be 5 o'clock since a clock cycles back to the same time every 12 hours. However if we add 5 and 12 normally, we get 5 + 12 = 17. But 17 isn't on the clock! What happened?



On a clock, the numbers go from 1 to 12, but when we get to 13 o'clock, it becomes 1 o'clock again. So 13 becomes 1, 14 becomes 2, 15 becomes 3, and so on. Every time we go past 12 on the clock we start counting the hours at 1 again. Thus we may view 17 o'clock as the same as 5 o'clock.

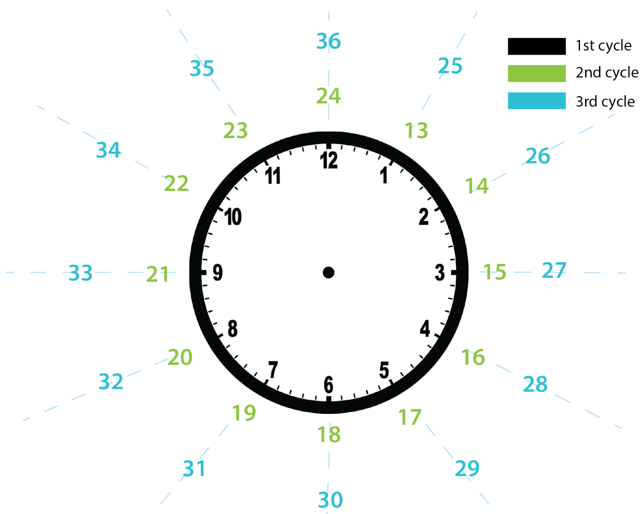
We write this mathematically as:

$$17 = 5 \mod 12$$

We use the modular operator "mod" to indicate they mean the same thing on a clock. This means that 17 o'clock is the same thing as 5 o'clock in a 12 hour system. The mod **12** indicates the clock cycles every 12 hours.

Similarly, we can add 12 hours again to 17 to get 29 o'clock. We still understand that it is the same as 5 o'clock. We write this as

$$29 = 5 \mod 12$$

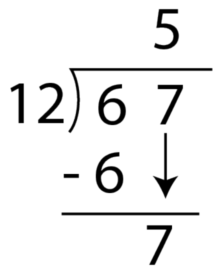


Exercise. Can you think of anything else that is equal 5 o'clock. How would you write this mathematically?

Exercise. What is 31 o'clock equal to on a 12 hour clock (the number must be less than 12)?

Remainder and Modular Arithmetic

Example. Suppose we want to calculate 67 divided by 12. Can you recall how to calculate this using long divison?



Here 67 is not divisible by 12 as the division results in a remainder of 7. However, if we were to use the number 60, we get that it is divisble by 12 since the division results in a remainder of 0.

But how is this related to Modular Arithmetic? Well, there is actually a nice relationship between Modular Arithmetic and long division. Using modulo notation we can write our above example as:

$$\underset{\text{dividend}}{67} = \underset{\text{remainder}}{7} \mod \underset{\text{divisor}}{12}$$

The modular operator (mod) simply says, given two integers (x and n), it produces the remainder (r) when the first number (x) is divided by the second number (n). More generally,

$$\underset{\text{dividend}}{x} = \underset{\text{remainder}}{r} \mod \underset{\text{divisor}}{n}$$

In our example above, 12 is the **divisor**, 67 is the **dividend**, and 7 is **remainder**. Therefore, we can say that 67 has a remainder of 7 when divided by 12, and can be expressed in modulo notation as $67 = 7 \mod 12$.

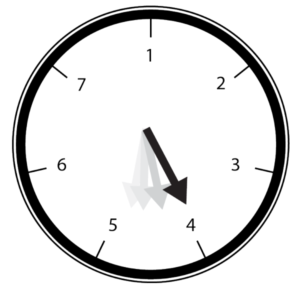
Here is an example on how to use long divison to help you refresh your memory!

Long Division Example Video: *https://youtu.be/tasL5er0Pj4*

Applications of Modular Arithmetic

There are many other things in our lives that repeat or cycle after a certain amount of time - days of the week, months of a year, degrees in a circle, seasons in a year. We can also use modular arithmetic for events that repeat. If the length of the cycle is n, we refer to it as **modulo** n.

For example, since a clock cycles every 12 hours, we refer to it as modulo 12. In a circle where one full revolution is 360 degrees, it is modulo 360. Since a week has 7 days we refer to it as modulo 7.



Examples:

1. Today is Wednesday, what day of the week will it be:
   (a) 165 days from now? (b) 365 days from now?

2. I celebrated my 21st birthday on Saturday, October 3rd, 2020. On what day of the week was I born? (Don't forget about leap years!). **Hint: There are 6 leap years that occured since I was born.**

Solution:

1. Questions 1 Video Solution: *https://youtu.be/-qtgwPZBL3Q*

   (a) There are 7 days in our week, so we will be working in mod 7. Remember, we can simply use the remainder to find which day it is. The number 7 divides into 165 a total of 23 times with 4 left over. We can write this as $165 = 4 \bmod 7$. Since today is Wednesday, after 23 weeks it will be Wednesday again, and 4 days after that it will be Sunday. So 165 days from now it will be Sunday.

   (b) Using the same approach as the previous example we get $365 = 1 \bmod 7$. Since today is Wednesday, 1 day from now will be Thursday.

2. Question 2 Video Solution: *https://youtu.be/hH7_ToP9mgY*

   $21 \times 365 = 7665$. Leap years occured in 2020, 2016, 2012, 2008, 2004, and 2000 so we add 6 more days to get total of 7671 days. $7671 = 6 \bmod 7$, and remember since we are looking into to past we are going **backwards** 6 days from Saturday, therefore I was born on a Sunday.

Modular Addition

Going back to the clock example. We already know that

$$17 = 5 \mod 12$$

Question: What if we shift the hour hand by 2 additional hours after 17 hours have passed? Will it be the same time after shifting the hour hand an additional 2 hours after 5 hours have passed?

Answer: Since shifting 17 hours lands the hour hand in the same position as if 5 hours have passed, shifting an additional two hours to both 17 and 5 shift the clock to 7 o'clock.

$$\begin{aligned} 17 + 2 &= 5 + 2 \mod 12 \\ 19 &= 7 \mod 12 \end{aligned}$$

Modular Addition Rule: Suppose a, b and n are whole numbers, then

$$(a + b) \text{ mod } n = (a \text{ mod } n + b \text{ mod } n) \text{ mod } n$$

Example. Simplify (13 + 15) mod 12

Modular Addition Example Video Solution: *https://youtu.be/sOD0XoJeNXg*

Solution 1. We add 13 and 15 together first and get 28. We find that the number 12 divides into 28 a total of 2 times with 4 left over. We can write this as

$$(13 + 15) = 28 = 4 \mod 12$$

Solution 2. Alternatively, we can find the remainder of 13 and 15 separately. This makes calculations easier because we are dealing with smaller numbers. This proves especially important as we deal with bigger numbers. First we note that

$$13 = 1 \mod 12$$

$$15 = 3 \mod 12$$

Therefore

$$(13 + 15) \text{ mod } 12 \; = 1 + 3 = 4 \mod 12$$

Exercise. Reduce the expression $90987 + 7269 + 2341014 + 758776 \mod 10$
Hint: What is the remainder of any number when you divide by 10?

Cryptography: Shift Ciphers

Cryptography is the study of reading or writing secret messages or codes. The word cryptography comes from the Greek word *kryptos* ($\kappa\rho\upsilon\tau\varsigma$) meaning hidden and *graphein* ($\gamma\rho\alpha\phi\omega$) meaning writing. Before we get any further, let's learn some terminology:

> **Encryption**: The process of concealing normal text such that only authorized parties, such as the sender and receiver, can read it.
>
> **Decryption**: The process of decoding encrypted text back into its original text.

A famous cipher is the **Caesar Cipher** and it is named after, as you may have guessed, Julius Caesar. What did he use this cipher for? To communicate with his army! It would not turn out so well if Caesar's enemies were able to intercept and read his messages. Caesar was able to encrypt his messages by using modular arithmetic!

If we assign each letter of the alphabet a number from 0 to 25 (ex. A=0, B=1, C=2, etc...), a shift cipher can be used to encode and decode messages with a known shift number (which we'll call k).

To encode our message, we encrypt each letter individually using the formula:

$$\textbf{coded} = \textbf{(original} + k\textbf{)(mod 26)}$$

If we are given an encoded message and a shift number, we can decrypt the letters using the formula:

$$\textbf{original} = \textbf{(coded + 26 -} \ k\textbf{)(mod 26)}$$

Why do we add 26? This step will ensure we will not have to work with negative dividends. Infact we can actually add *any multiple* of 26, as we are only concerned about remainders.

letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
position	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Example. Encode the message "MATH" using $k = 20$

Solution. M is in position 12 so we can use the formula above to find the coded letter:
coded $= 12 + 20 = 32$ which is $32 = 6 \mod 26$, so the first letter is **G** (6).

A is in position 0:
coded $= 0 + 20 = 20$ which is $20 = 20 \mod 26$ so the second letter is **U** (20).

T is in position 19:
coded $= 19 + 20 = 39$ which is $39 = 13 \mod 26$ so the third letter is **N** (12).

Lastly, H is in position 7:
coded $= 7 + 20 = 27$ which is $27 = 1 \mod 26$ so the fourth letter is **B** (1).

Thus our coded message is "**GUNB**".