UNIVERSITY OF WATERLOO

Faculty of Mathematics
Waterloo, Ontario N2L 3G1

Centre for Education in
Mathematics and Computing

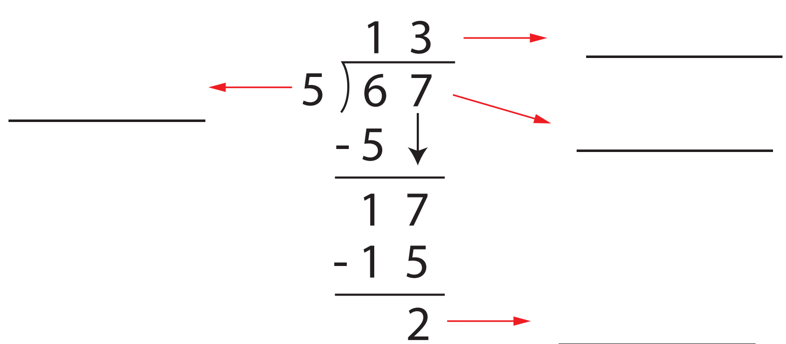
Grade 7/8 Math Circles

November $12^{\text{th}}/13^{\text{th}}/14^{\text{th}}$

Modular Arithmetic

Division

Suppose we want to calculate 67 divided by 5. Here, 67 is the __________ and 5 is the __________. The division would go as follows:



For the example above we can write:

$$\mathbf{67 \div 5 = 13\ R\ 2}$$

Where **R** indicates the remainder.

> **Divisible**
>
> In math, a number is said to be **divisible** by another number if the remainder is 0.

Example: In the example above, 67 is *not divisible* by 5 as the division results in a remainder of 2. However, 65 is divisible by 5 since the division results in a remainder of 0.

Exercise Set 1

For the following, use long division to determine the quotient and remainder as above and determine if the dividend is *divisble* by the divisor.

1. $29 \div 9$

   Quotient: ___________

   Remainder: ___________

   Divisible? _____________

2. $23 \div 8$

   Quotient: ___________

   Remainder: ___________

   Divisible? _____________

3. $37 \div 7$

   Quotient: ___________

   Remainder: ___________

   Divisible? _____________

4. $25 \div 3$

   Quotient: ___________

   Remainder: ___________

   Divisible? _____________

5. $7 \div 5$

   Quotient: ___________

   Remainder: ___________

   Divisible? _____________

6. $63 \div 9$

   Quotient: ___________

   Remainder: ___________

   Divisible? _____________

7. $64 \div 12$

   Quotient: ___________

   Remainder: ___________

   Divisible? _____________

8. $56 \div 11$

   Quotient: ___________

   Remainder: ___________

   Divisible? _____________

9. $32 \div 4$

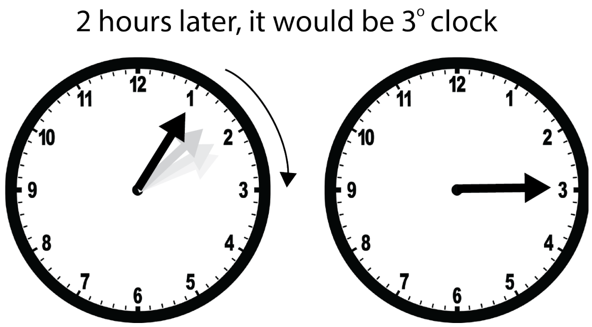
   Quotient: ___________

   Remainder: ___________

   Divisible? _____________

The 12-hour Clock

We know any clock has 12 hours. Suppose the clock reads 1^o clock. In 2 hours, it would be 3^o clock. This is found simply by adding $1 + 2 = 3$.

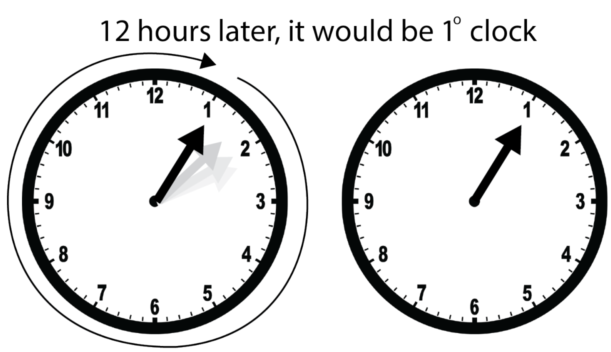


Exercise:

- What time would it be after 12 hours?
- What time would it be after 17 hours?
- What time would it be after 43 hours?

How did you calculate the time in each of the examples above?

Looking at the first exercise, we get $1 + 12 = 13$. In a clock, we may view 13^o clock the same as 1^o clock as $13 - 12 = 1$. Alternatively, you may interpret that shifting 13 hours ahead on a clock is the same as if you were shifting 1 hour ahead so starting from 12^o clock, you'd end up at 1^o clock.



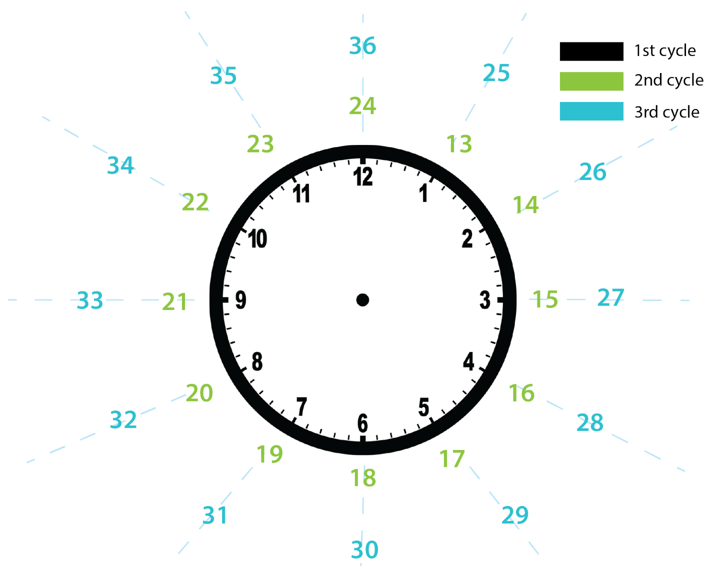
We write this mathematically as:

$$13 \equiv 1 \mod 12$$

We use the ≡ (equivalence) symbol to indicate they mean the same thing on a clock. This means that 13° clock is the same thing as 1° clock in a 12 hour system. The mod 12 indicates the clock cycles every 12 hours.

Similarly, we can add 12 hours again to 13 to get 25° clock. We still understand that it is the same as 1° clock. We write this as

$$25 \equiv 1 \mod 12$$



Exercise. Can you think of anything else that is equal 1° clock. How would you write this mathematically?

Exercise: What is is 17° clock equal to on a 12 hour clock (*the number must be less than 12*). Express your answer mathematically as well.

Modular Arithmetic and Remainder

Sometimes, we are only interested in the *remainder* when we divide two integers.

In these cases we write one of the following:

$$\text{dividend mod divisor} = \text{remainder}$$

$$\text{dividend} \equiv \text{remainder} \mod \text{divisor}$$

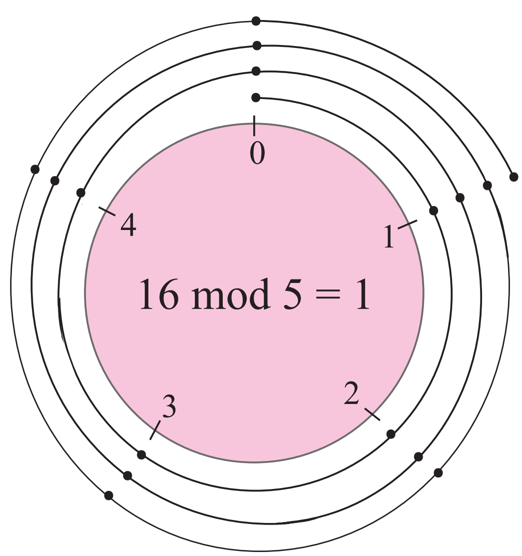
Example: $16 \equiv 1 \mod 5$

We know that $(5 \times 3) + 1 = 16$ so the remainder of dividing 16 by 5 will be 1.

By noticing this, we can visualize the modulo operator by using circles.

We write 0 at the top of a circle and continuing clockwise writing integers 1, 2, ... up to one less than the modulus.

Example: $16 \equiv 1 \mod 5$



We start at 0 and go through 16 numbers in a clockwise sequence 1, 2, 3, 4, 0, 1, 2, 3, 4, 0, 1, 2, 3, 4, 0, 1.

We ended up at **1** so 16 mod 5 = 1 as we mentioned before.

Exercise Set 2

1. Evaluate.

   $38 \equiv$ ______ mod 3 $54 \equiv$ ______ mod 8 $81 \equiv$ ______ mod 10

   $12 \equiv$ ______ mod 6 $73 \equiv$ ______ mod 5 $96 \equiv$ ______ mod 1

   In a clock, we are evaluating with mod 12. Start at 0 on the top and continuing clockwise writing integers 1, 2, ..., 11 which is what a clock looks like.

2. Simplify the following times i.e how would you read it on a clock and write the answer mathematically.

   (a) 15° clock

   (b) 56° clock

   (c) 42° clock

   (d) 48° clock

3. **The 24 Hour Cycle**

   The 12 hour cycle is a time convention where we divide the day into 2 periods: a.m (ante meridiem) and p.m (post meridiem). However, as you may know there are 24 hours in day. If we use the 24 hour system, we do not have to write a.m or p.m after the time.

   Suppose the clock is initially 12^{o} clock (12 p.m). Using a 24 hour system, determine what time it would be after the following amount of hours have passed and express the following in modular relation ($25 \equiv 1 \mod 24$).

   (a) 24 hours

   (b) 37 hours

   (c) 56 hours

   (d) 45 hours

Modular Addition

Going back to the clock example. We already know that

$$13 \equiv 1 \mod 12$$

Question: What if we shift the hour hand by 2 additional hours after 13 hours have passed? Will it be the same time after shifting the hour hand an additional 2 hours after an hour has passed?

Answer: Since shifting 13 hours lands the hour hand in the same position as if it passed by an hour, shifting an additional two hours to both 13 and 1 shift the clock to 3° clock.

$$\begin{aligned} 13 + 2 &\equiv 1 + 2 \mod 12 \\ 15 &\equiv 3 \mod 12 \end{aligned}$$

Modular Addition:

Suppose a, b and m are whole numbers, then

$$(a + b) \equiv (a \mod m + b \mod m) \mod m$$

Example: Suppose we want to find:

$$(14 + 17) \equiv \underline{\qquad} \mod 5$$

Well we know $14 \equiv 4 \mod 5$ and $17 \equiv 2 \mod 5$, then:

$$(14 + 17) \equiv 4 + 2 \mod 5$$

$$(14 + 17) \equiv 6 \mod 5$$

$$(14 + 17) \equiv 1 \mod 5$$

Modular Multiplication

Modular Arithmetic is even more useful when we are dealing with multiplication.

Again, let's start with the clock. Since we already know that

$$13 \equiv 1 \mod 12$$

or in other words, shifting 13 hours ahead is the same as shifting one hour ahead.

$$13 \equiv 1 \mod 12$$
$$13 + 13 \equiv 1 + 1 \mod 12$$
$$13 + 13 + 13 \equiv 1 + 1 + 1 \mod 12$$
$$3 \times 13 \equiv 3 \times 1 \mod 12$$

This makes sense intuitively. Since shifting 13 hours ahead is the same as shifting 1 hour ahead, then shifting 13 hours 3 times should be the same as shifting 3 hours ahead.

Modular Multiplication:

Suppose a, b and m are whole numbers, then

$$(a \times b) \equiv ((a \mod m) \times (b \mod m)) \mod m$$

Example: Suppose we want to find:

$$(12 \times 18) \equiv \underline{\qquad} \mod 5$$

Well we know $12 \equiv 2 \mod 5$ and $18 \equiv 3 \mod 5$, then:

$$(12 \times 18) \equiv 2 \times 3 \mod 5$$
$$(12 \times 18) \equiv 6 \mod 5$$
$$(12 \times 18) \equiv 1 \mod 5$$

To verify, $(5 \times 43) + 1 = 216 = 12 \times 18$ *and the remainder here is 1 as found above.*

Exercise Set 3

1. Simplify the following

   (a) $9+5 \mod 12$

   (b) $13+15 \mod 12$

   (c) $22+14 \mod 10$

   (d) $34+37+64+18 \mod 12$

2. Reduce the expression $90987+7269+2341014+758776 \mod 10$

   Hint: *What is the remainder of any number when you divide by 10?*

3. It is currently 2° clock.

   (a) What time will it be if we shift forward 13 hours 12 times?

   (b) What time will it be after we shift the clock 23 hours ahead 14 times?

4. Reduce the following

   (a) $44 \times 56 \mod 12$

   (b) $41 \times 67 \times 25 \mod 5$

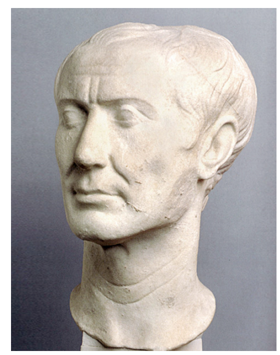
   (c) $2 \times 30 + 4 \times 37 \mod 8$

Caesar Cipher

Cryptography is the study of hidden writing or reading and 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 encrypting 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

The most 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 shifting over every letter of the alphabet by 3 units. Using a shift of 3 letters, here is the cipher that Caesar used:



plaintext	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
ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Now suppose Caesar wants to send the following message:

`CAESAR SALAD IS NAMED AFTER ME AS WELL`

Using the cipher shown earlier, Caesar's encrypted message is:

`FDHVDU VDODG LV QDPH DIWHU PH DV ZHOO`

To decrypt the encrypted message, we replace letters from the ciphertext row with letters from the plaintext row. We can also use the Caeser shift with **different shift numbers.**

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 well call k). To encode our message, we encrypt each letter individually using the formula:

$$\text{coded} \equiv (\text{original} + k) \mod 26$$

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

$$\text{original} \equiv (\text{coded} + 26 - k) \mod 26$$

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.

Complete the encryptions and decryptions below using the following table:

plaintext	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: What do you call a bee that lives in America? Decode **KIR** using $k = 16$.

K is in position 10 so we can use the formula above to find the original letter:
original $\equiv 10 + 26 - 16 \equiv 20 \mod 26$ so the first letter is **U** (20).

I is in position 8 so we can use the formula above to find the original letter:
original $\equiv 8 + 26 - 16 \equiv 18 \mod 26$ so the next letter is **S** (18).

R is in position 17 so we can use the formula above to find the original letter:
original $\equiv 17 + 26 - 16 \equiv 1 \mod 26$ so the next letter is **B** (1).

What do you call a bee that lives in America? ______

Exercise Set 4

Encrypt or decrypt the following messages using the shift number given in parentheses:

a) Welcome to Math Circles! ($k = 5$)

b) Ljw hxd anjm cqrb? ($k = 9$)

c) Modular Arithmetic ($k = 20$)

d) Pnrfne fuvsgf ner fb sha! ($k = 13$)

e) What if I did a Caeser Shift of 26 units on "*Welcome to Math Circles!*"?

Problem Set

1. Evaluate.

(a) $13 \equiv$ ______ $\bmod 1$

(b) $29 \equiv$ ______ $\bmod 3$

(c) $49 \equiv$ ______ $\bmod 5$

(d) $64 \equiv$ ______ $\bmod 8$

(e) $7 \equiv$ ______ $\bmod 6$

(f) $14 \equiv$ ______ $\bmod 2$

(g) $9 \equiv$ ______ $\bmod 6$

(h) $5 \equiv$ ______ $\bmod 9$

(i) $29 \equiv$ ______ $\bmod 4$

(j) $37 \equiv$ ______ $\bmod 7$

(k) $34 \equiv$ ______ $\bmod 8$

(l) $16 \equiv$ ______ $\bmod 2$

2. Evaluate using modular addition.

(a) $124 + 495 \equiv ($ ______ $\bmod 3 +$ ______ $\bmod 3) \bmod 3$

$\equiv$ ______ $\bmod 3$

(b) $89 + 26 \equiv ($ ______ $\bmod 7 +$ ______ $\bmod 7) \bmod 7$

$\equiv$ ______ $\bmod 7$

(c) $76 + 38 \equiv ($ ______ $\bmod 3 +$ ______ $\bmod 3) \bmod 3$

$\equiv$ ______ $\bmod 3$

3. Evaluate using modular multiplication.

   (a) $322 \times 93 \equiv (\_\_\_\_\_\_ \mod 4 \times \_\_\_\_\_\_ \mod 4) \mod 4$

   $\equiv \_\_\_\_\_\_ \mod 3$

   (b) $8 \times 9 \times 10 \equiv (\_\_\_\_\_\_ \mod 6 \times \_\_\_\_\_\_ \mod 6 \times \_\_\_\_\_\_ \mod 6) \mod 6$

   $\equiv \_\_\_\_\_\_ \mod 6$

4. The following questions involves divisibility of 2.

   (a) What are the possible remainders when you divide any number by 2?

   (b) How can you tell by just looking at the number the remainder of any number when divided by 2.

   (c) Using part a and part b, reduce the expression:

$$108 + 2534 + 3976 + 321539 \mod 2$$

5. A litre of milk is 4 cups, and one cake recipe uses 3 cups. If I have 8 litres of milk, how many cakes can I make? And how many cups of milk will be leftover, if any?

6. I bought as many mini-erasers as possible at 25 cents each and spent the rest of my money on paperclips at 3 cents each. How many of each did I buy given that I have \$1.70? Is there anything leftover? *(Assume theres no tax.)*

7. I have 9 trays with 8 muffins each that I divided evenly among 5 of my friends, and I ate the leftovers. How many muffins did each of my friends eat? How many muffins did I eat?

8. If Math Circles started on Tuesday, October 8^{th}, 2019, and lasts for 51 days, what is the last day of Math Circles? (Give the full date.)

   Note that 51 is not the number of classes there are, rather it is the number of days in between the first and last day of Math Circles.

9. Encrypt or decrypt the following messages using a Caesar cipher given the shift number in parentheses.

   (a) I love math jokes! (14)

   (b) Axeeh Phkew (19)

10. For a year n, we can identify if n is a leap year or not if it fulfills the following criteria:

   - The year can be evenly divided by 4;
   - If the year can be evenly divided by 100, it is NOT a leap year, unless;
   - The year is also evenly divisible by 400. Then it is a leap year.

   (a) Was the year 1900 a leap year?

   (b) Was the year 2000 a leap year?

   (c) Is the year 2100 going to be a leap year?

   (d) Is the year 2400 going to be a leap year?

   (e) What year is the next leap year?

11. * If Justin celebrated his 19^{th} birthday on Sunday, February 10^{th}, 2019, what day of the week was he born?

   Hint: *Dont forget to consider leap years. Use your answers from the question above.*

12. * Reduce the following

   (a) $2^{20} \mod 3$

   (b) $5^{10} \mod 3$

   (c) $2^{20} \times 5^{10} \mod 3$

13. *What is the last digit of 3^{729}?

14. * What is the remainder of 1259421 when divided by 9?

   Hint: Notice that $1259421 = 1 \times 10^7 + 2 \times 10^6 + 5 \times 10^5 + \cdots 2 \times 10 + 1$