

# Cracking the Code – The Mathematics of Cryptanalysis

## Lesson 2 – Modular Arithmetic

### Questions

1. What strategies did you use to decipher Cypher #1?
2. Encrypt the following message using the same code that was used to encrypt Cypher #1:

Ask not for whom the bell tolls.

3. This message was encrypted using the same code that was used to encrypt Cypher #1. Decrypt it.

OLHY

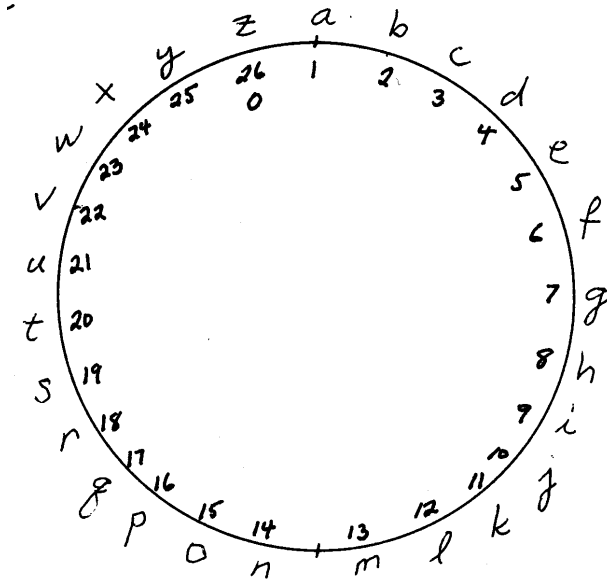
### Notation and Conventions.

- We will use lowercase letters for the English version of each message, called *plaintext*.
- We will use uppercase letters for the encrypted version of each message, called *cyphertext*.
- If we want to indicate that modular arithmetic is to be performed, we notate our work as follows:  $(7+22)(\text{mod } 26) = 3$  or  $7+22 = 3 \pmod{26}$
- We will number the alphabet as follows:

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
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	0

We can think of arithmetic modulo 26 as a circular number system in which numbers wrap around to the beginning when we get to the end of the row. To add 7 to 22, we would move forward 7 spaces from 22, wrapping around when we got to 0 and landing on 3. That's why  $7+22 = 3 \pmod{26}$ .

We can even represent the number system this way:



Now let's think about mod 12 arithmetic.

4. Make a circle for mod 12 arithmetic.

Now let's look at a mod 12 addition table:

+ (mod 12)	1	2	3	4	5	6	7	8	9	10	11	12
1	2	3	4	5	6	7	8	9	10	11	12	1
2	3	4	5	6	7	8	9	10	11	12	1	2
3	4	5	6	7	8	9	10	11	12	1	2	3
4	5	6	7	8	9	10	11	12	1	2	3	4
5	6	7	8	9	10	11	12	1	2	3	4	5
6	7	8	9	10	11	12	1	2	3	4	5	6
7	8	9	10	11	12	1	2	3	4	5	6	7
8	9	10	11	12	1	2	3	4	5	6	7	8
9	10	11	12	1	2	3	4	5	6	7	8	9
10	11	12	1	2	3	4	5	6	7	8	9	10
11	12	1	2	3	4	5	6	7	8	9	10	11
12	1	2	3	4	5	6	7	8	9	10	11	12

Let's look at one entry:  $9+8 \pmod{12} = 5$ . (Make sure you can read this fact from the table. Find the "9 row" and the "8 column." The entry at the intersection of this row and column is 5. Why would the "answer" be 5? Well, if we start at 9 on your circle and go around clockwise 8 spaces, we wrap around to 5.

Notice that 12 behaves in a very interesting way in mod 12 arithmetic.

5. If we add 12 to any number, what do we get?
6. In ordinary addition, what number behaves this way?

For this reason, in mod 12 arithmetic, mathematicians usually replace the symbol 12 with the symbol 0, so that the addition table looks like this:

$+ \pmod{12}$	1	2	3	4	5	6	7	8	9	10	11	0
1	2	3	4	5	6	7	8	9	10	11	0	1
2	3	4	5	6	7	8	9	10	11	0	1	2
3	4	5	6	7	8	9	10	11	0	1	2	3
4	5	6	7	8	9	10	11	0	1	2	3	4
5	6	7	8	9	10	11	0	1	2	3	4	5
6	7	8	9	10	11	0	1	2	3	4	5	6
7	8	9	10	11	0	1	2	3	4	5	6	7
8	9	10	11	0	1	2	3	4	5	6	7	8
9	10	11	0	1	2	3	4	5	6	7	8	9
10	11	0	1	2	3	4	5	6	7	8	9	10
11	0	1	2	3	4	5	6	7	8	9	10	11
0	1	2	3	4	5	6	7	8	9	10	11	0

### Questions Continued

7. Make an addition table for addition mod 26.
8. Make an addition table for addition mod 8.
9.  $(6+7)\pmod{12}$
10.  $(6+6)\pmod{12}$
11.  $(7+7)\pmod{12}$
12.  $(7+19)\pmod{12}$
13.  $(5 \times 7)\pmod{12}$
14.  $(7 \times 7)\pmod{12}$
15.  $(22+7)\pmod{26}$
16.  $(20+6)\pmod{26}$
17.  $(7+7)\pmod{26}$
18.  $(7+19)\pmod{26}$
19.  $(5 \times 7)\pmod{26}$
20.  $(7 \times 7)\pmod{26}$
21. The *additive inverse* of a given number is a number that can be added to the given number to get 0. What is the additive inverse of 5 in mod 12 arithmetic? (Do not use negative numbers!)
22. What is the additive inverse of 2 mod 12?
23. What is the additive inverse of 5 mod 26?

24. What is the additive inverse of  $11 \pmod{26}$ ?
25. Using your circle for mod 12 arithmetic, determine the following.
  - a.  $15 \pmod{12}$
  - b.  $26 \pmod{12}$
  - c.  $53 \pmod{12}$
26. Can you suggest a way to compute these values without consulting the circle?
27. Can you suggest a way to implement this method on a calculator?