





J3. Template (Type in this one)

 Help Videos	Use OneNote App How to use OneNote App for hand written solutions	 Camera

Cryptology and Modular Arithmetic

Activity		Download/Link	Deadline
 JOURNAL	A. Cryptology B. Modular Arithmetic C. Algorithm	Journal 3: Upload pdf Journal 3: Accuracy Check	Upload pdf Mon 8th Nov 5pm Accuracy Test Monday 8th Nov 5pm
	 (100%)	 Mastery Quiz 3	Friday 5th November 5pm

A. Cryptology: Ciphers

Question 1

Complete the following statements

Cryptology is the study of codes, or the art of writing and solving them.

Encryption performed on plaintext using an algorithm is called a Cipher

Question 2

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	26

- i. **Chris** wants to encrypt his name with a **Caesar Cipher** using a shift of 9, what will his name look like after he encrypts it?

	3	8	18	9	19
	+9	+9	+9	+9	+9
	12	17	27	18	28

12	17	1	18	2
l	q	a	r	b

- ii. A student wants to encrypt the message “see you later” using a **Vigenere Cipher** and the keyword “**maths**”. What will her message say?


S E E	Y O U	L A T E R
19 5 5	25 15 21	12 1 20 5 18
M A T	H S M	A T H S M
13 1 20	8 19 13	1 20 8 19 13
32 6 25	33 34 34	13 21 28 24 31
6 6 25	7 8 8	13 21 2 24 5
F f y	G H H	M U B X E

ff y ghh mubxe

B. Modular Arithmetic

Question 3: Mod Calculations

A. Find the solutions to the following modular arithmetic questions (Show working out)

	(i) $36 \bmod 10$	(ii) $-18 \bmod 5$	(iii) $243 \bmod 8$
	$36/10 = 3.6$ $3.6 - 3 = 0.6$ $0.6 * 10 = 6.0$	$-18 + 5 = -13$ $-13 + 5 = -8$ $-8 + 5 = -3$ $-3 + 5 = 2$	$243/8 = 30.375$
			$30.375 - 30 = 0.375$
			$0.375 * 8 = 3.0$

B. If today is Thursday, what day of the week will it be 100 days later?

$$100/7 = 14.2857$$

$$14.2857 - 14 = 0.2857$$

$$0.2857 * 7 = 1.9999$$

$$1.9999 \approx 2.0$$

Thursday + 2 Days = Saturday

Saturday

Question 4: Mod Tables

A. Complete the following modular arithmetic tables in your journal:

(i) Addition mod 5 (create table)

+Mod5	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$$5 \text{ MOD } 5 = 0$$

$$6 \text{ MOD } 5 = 1$$

$$7 \text{ MOD } 5 = 2$$

$$8 \text{ MOD } 5 = 3$$

Using table what is the

(ii) Additive inverses of 1 mod 5	$1 + 4 = 5 \text{ MOD } 5 = 0$ 4
(ii) Additive inverses of 2 mod 5	$2 + 3 = 5 \text{ Mod } 5 = 5 \text{ } 0$ 3
(ii) Additive inverses of 3 mod 5	$3 + 2 = 5 \text{ Mod } 5 = 5 \text{ } 0$ 2
(iv) Additive inverses of 4 mod 5	$4 + 1 = 5 \text{ Mod } 5 = 5 \text{ } 0$ 1

B. Complete the following modular arithmetic tables in your journal:

(ii) Multiplication mod 5 (create table)

*Mod5	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

$$6 \text{ MOD } 5 = 1$$

$$8 \text{ MOD } 5 = 3$$

$$9 \text{ MOD } 5 = 4$$

$$12 \text{ MOD } 5 = 2$$

$$16 \text{ MOD } 5 = 1$$

Using table what is the

(ii) Multiplicative inverse of 1 mod 5	$1*1= 1 \text{ MOD } 5 = 1$ 1
(ii) Multiplicative inverse of 2 mod 5	$2*3= 6 \text{ MOD } 5 = 1$ 3
(ii) Multiplicative inverse of 3 mod 5	$3*2= 6 \text{ MOD } 5 = 1$ 2
(iv) Multiplicative inverse of 4 mod 5	$4*4= 16 \text{ MOD } 5 = 1$ 4

C. Logic and Algorithms

Question 5:

A. Write out the steps of Euclidean Algorithm

1. Set up a division problem where a is bigger than b.
2. $a / b = c$ with remainder R.
3. Do the division.
4. Then replace a with b.
5. Continue the process until $R = 0$.
6. This will give you GCD.

B. Use the Euclidean Algorithm to find the greatest common divisor of **2,322** and **654**.



[Find gcd (2322, 654)]. All workings must be shown.

A/B	WORKINGS	Reminder
2322/654	$3.5505 - 3 = 0.5505$ $0.5505 * 654 = 360.027$	360
$654/360 = 1.8167$	$1.8167 - 1 = 0.8167$ $0.8167 * 360 = 294.012$	294
$360/294 = 1.2245$	$1.2245 - 1 = 0.2245$ $0.2245 * 294 = 66.003$	66
$294/66 =$	$4.4545 - 4 =$	30

<i>4.4545</i>	<i>0.4545</i> <i>0.4545*66=</i> <i>29.997</i>	
<i>66/30=2.2</i>	<i>2.2 -2=0.2</i> <i>0.2*30=6</i>	<i>6</i>
<i>30/6=5</i>	<i>5-5=0</i> <i>0*6=0</i>	<i>0</i>

GCD = 6