Name: Connor Raymond Stewart
Student Number: 10104125

MATH 3101 Assignment 4:

(1)

a) Write out the addition table for $\mathbb{Z}_7$:

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

b) Write out the multiplication table for $\mathbb{Z}_7$:

×	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[0]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[0]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[0]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[0]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[0]	[6]	[5]	[4]	[3]	[2]	[1]

c) Write out the multiplication table for $\mathbb{Z}_7$, indexed in the order [0],[1],[3],[2],[6],[4],[5]:

×	[0]	[1]	[3]	[2]	[6]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[3]	[2]	[6]	[4]	[5]
[3]	[0]	[3]	[2]	[6]	[4]	[5]	[1]
[2]	[0]	[2]	[6]	[4]	[5]	[1]	[3]
[6]	[0]	[6]	[4]	[5]	[1]	[3]	[2]
[4]	[0]	[4]	[5]	[1]	[3]	[2]	[6]
[5]	[0]	[5]	[1]	[3]	[2]	[6]	[4]

What difference can be noticed between this table & the table from part b:

In table b, the non-[0] entries form a Palindromic Pattern over the diagonals:

i.e. 3,4,3 & 4,6,6,4

In table c, the diagonals form rows of the same number (for the non-[0] entries):

i.e. 2,2,2 & 6,6,6,6

Thus:

the difference is that the table has diagonal entries of the same number for the non-zero rows/columns (i.e. not column one or row one).

② Find the multiplicative inverse of $[33]$ in $\mathbb{Z}_{58}$:

We first find x given:

$[33][x]=[1]$ in the set of $\mathbb{Z}_{58}$

We get:

$33x \equiv 1 \pmod{58}$

We observe that $(33,58)=1$, so we must increment 1 by multiples of 33:

We will use the euclidean Algorithm:

$58 = 33q_0 + r_1$

$\hookrightarrow 58 = 33(1) + 25 \quad [q_0=1, r_1=25]$

$33 = 25q_1 + r_2$

$\hookrightarrow 33 = 25(1) + 8 \quad [q_1=1, r_2=8]$

$25 = 8q_2 + r_3$

$\hookrightarrow 25 = 8(3) + 1 \quad [q_2=3, r_3=1]$

$8 = (1)q_3 + r_4$

$\hookrightarrow 8 = (1)(8) + 0 \quad [q_3=8, r_4=0]$

Write the inequalities:

$58 = 33(1) + 25 \rightarrow 25 = 58 - 33$

$33 = 25(1) + 8 \rightarrow 8 = 33 - 25$

$25 = 8(3) + 1 \rightarrow 1 = 25 - 8 \cdot 3$

Form this:

$1 = 25 - 8 \cdot 3$

$= 25 - (3)(33-25)$

$= (58-33) - (3)(33-(58-33))$

$= \cancel{58 - 33 - (3)(33) + (3)(58) - (3)(33)}$

$= 4(58) - 7(33) \equiv (33)(-7) \pmod{58}$

Thus:

$\boxed{x=-7}$

All Solutions must thereby be given by $x \equiv -7 \pmod{58}$, or simply $x \equiv 51 \pmod{58}$

Therefore; $[33]^{-1} = [51]$

③ Since a Caesar Cipher is a map between the alphabet & a "shifted" alphabet a the aphabet, & Caesar's Cipher was mapped a to D:

	a from the alphabet → D in Cipher
See Figure 2.4 from text for visual.	b → E
	c → F
	⋮
	V → Y
	W → Z
	X → A
	Y → B
	Z → C

Note, the letters j, u, & w were NOT in the Roman Alphabet used by Caesar. Thus ~~the Alphabet had only 23 letters.~~

$f(x) = x + 3 \pmod{26}$

thus, $f^{-1}(x) = x - 3 \pmod{26}$

Also, Caesar didn't encrypt Spaces with his Cipher.

So, Given "YHQL YLGL YLFL": (use Zero indexing)

Cipher text →	Y	H	Q	L		Y	L	G	L	Y	L	F	L
translate to # →	24	7	16	11		24	11	6	11	24	11	5	11
$f^{-1}(x) = x - 3 \bmod 26$ →	21	4	13	8		21	8	3	8	21	8	2	8
Plane text →	V	E	N	I		V	I	D	I	V	I	C	I

thus, we get the following Plane text:

"VENI VIDI VICI"

④ Use a translation cipher on the following data:

Alphabet:

a-z, —, ', ., ', ? } B

0-25, 26, 27, 28, 29, 30 }

K=21, message = "what's up, doc", n=31

Encipher:

$f(x) = x + K \bmod n$

$f(x) = x + 21 \bmod 31$

plaintext →	w	h	a	t	'	s	—	u	p	,	—	d	o	c
translate to B →	22	7	0	19	29	18	26	20	15	27	26	3	14	2
$f(x)=x+21 \bmod 31$ →	12	28	21	9	19	8	16	10	5	17	16	24	4	23
translate from B →	m	.	v	j	t	i	q	k	f	r	q	y	e	x

thus, we get the following message:

"m.vjtiqkfrqyex" → ciphertext

Inverse Mapping:

$f^{-1}(x) = x - K \bmod n$

$f^{-1}(x) = x - 21 \bmod 31$

Thus:

ciphertext → m.vjtiqkfrqyex

inverse mapping → $f^{-1}(x) = x - 21 \bmod 31$

(5) use an affine cipher on the following:

$a=15$ & $b=22$, message = "Houston, we have a problem.", $n=31$

a-z, —, ', ., ', !, ? } 13

0-25, 26, 27, 28, 29, 30

Encipher:

$f(x) = ax+b \bmod n$

$f(x) = 15x+22 \bmod 31$

Plaintext → Houston,_we_have_a_problem.

translate to B → 7 14 20 18 19 14 13 27 26 22 4 26 7 0 21 4 26 0 26 15 17 14 1 11 4 12 28

f(x)=15x+22 mod 31 → 3 15 12 13 28 15 0 24 9 11 20 9 3 22 27 20 9 22 9 30 29 15 6 1 20 16 8

translate from B → d p m n . p a y j l u j d w , u j w j ? ' p g b u q i

Inverse Mapping:

$(15, 31) = 1$

$f^{-1}(x) = 29x - (29)(22) \bmod 31$

$\hookrightarrow 1 = 29 \cdot 15 \bmod 31$

$f^{-1}(x) = 29x + 2(22) \bmod 31$

$\hookrightarrow 2 = -29 \bmod 31$

$f^{-1}(x) = 29x + 13 \bmod 31$

Thus:

dpmn.pqyjlujdw,ujwj?'pgbuqi

Thus:

Ciphertext → dpmn.pqyjlujdw,ujwj?'pgbuqi

inverse mapping → $f^{-1}(x) = 29x+13 \bmod 31$

⑥ Determine if the following statements are true or false. Justify your responses:

a) $18 = 10 \pmod 8$:

We Know:

$10 \pmod 8 \equiv 18 \pmod 8$ Since

↳ $10 - 18 = K(8)$, $K \in \mathbb{Z}$ (theorm 2.22 of text)

let $K = -1$:

$-8 = (-1)(8)$

$-8 = -8$

True

∴ It's true that $10 \pmod 8 \equiv 18 \pmod 8$

∴ $10 \pmod 8 = 18$ So $18 = 18$

∴ True

b) $[8] \in \mathbb{Z}_9$:

$\mathbb{Z}_9 = \{[0], [1], [2], [3], [4], [5], [6], [7], [8]\}$

$[8] \in \mathbb{Z}_9$ as $[8]$ is in the above ($8 < 9$ so it's in the above set)

↳ Thus $[8]$ is an included class

∴ True

c) $4 \in \mathbb{Z}_7$:

$\mathbb{Z}_7 = \{[0], [1], \ldots, [6], [7]\}$

the Set $\mathbb{Z}_7$ Consists of classes, however 4 is a number

↳ ∴ $4 \notin \mathbb{Z}_7$

∴ False

d) Every nonzero element $x \in \mathbb{Z}$ has a multiplicative inverse in $\mathbb{Z}$:

The multiplicative inverse is the number which when multiplied by x gives 1, the multiplicative identity.

Suppose $\mathbb{Z}$ has the multiplicative inverse:

let a be a nonzero integer

let b be a multiplicative inverse to a, $b \in \mathbb{Z}$

then:

$a \cdot b = 1$ So $b = 1/a$, however $1/a$ is not an integer, & $b = \frac{1}{a}$

thus $b \notin \mathbb{Z}$

However, above we say $b \in \mathbb{Z}$. This is a contradiction, b can't be both an integer & not an integer at the same time.

∴ False