Caballero Huesca Carlos Eduardo Homework 1.

1. Modular Arithmetic.

a). $-81 \bmod 7503$

$7503 - 81 = 7422$

$$\begin{array}{r} 7503 \\ -\ \ 81 \\ \hline 7422 \end{array}$$

b). $-7503 \bmod 81$

$81 - (7503 \bmod 81)$

$81 - 51 = 30$

$$\begin{array}{r|l} & 92 \\ \hline 81 & 7503 \\ & \ \ 213 \\ & \ \ \ \ 51 \end{array}$$

c). $-100 \bmod 24$

$24 - (100 \bmod 24)$

$24 - 4 = 20$

$$\begin{array}{r|l} & \ \ 4 \\ \hline 24 & 100 \\ & \ \ 04 \end{array}$$

d). $-5303 \bmod 63$

$63 - (5303 \bmod 63)$

$63 - 11 = 52$

$$\begin{array}{r|l} & \ \ 84 \\ \hline 63 & 5303 \\ & \ \ 263 \\ & \ \ \ \ 11 \end{array}$$

e). $-3 \bmod 1111$

$1111 - 3 = 1108$

2. a) $Z_5 = \{0 \dots 4\}$

*	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$a \times b \bmod n$

when Z_5 has an inverse?

$1 * 1 \bmod 5 = 1$

$2 * 3 \bmod 5 = 1$

$3 * 2 \bmod 5 = 1$

$4 * 4 \bmod 5 = 1$

b) $Z_8 = \{0 \ldots 7\}$

*	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	4	2
7	7	6	5	4	3	2	1

When Z_8 has an inverse (

1 * 1 MOD 8 = 1
3 * 3 MOD 8 = 1
5 * 5 MOD 8 : 1
7 * 7 MOD 8 is 1.

c). $Z_{11} = \{0 \ldots 10\}$

*	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

When Z_{11} has an inverse?

1 * 1 MOD 11 = 1
2 * 6 MOD 11 = 1
3 * 4 MOD 11 = 1
4 * 3 MOD 11 = 1
5 * 9 MOD 11 = 1
6 * 2 MOD 11 = 1
7 * 8 MOD 11 = 1
8 * 7 MOD 11 = 1
9 * 5 MOD 11 = 1
10 * 10 MOD 11 = 1

d). $Z_{14} = \{0 \ldots 13\}$

*	1	2	3	4	5	6	7	8	9	10	11	12	13
1	1	2	3	4	5	6	7	8	9	10	11	12	13
2	2	4	6	8	10	12	0	2	4	6	8	10	12
3	3	6	9	12	1	4	7	10	13	2	5	8	11
4	4	8	12	2	6	10	0	4	8	12	2	6	10
5	5	10	1	6	11	2	7	12	3	8	13	4	9
6	6	12	4	10	2	8	0	6	12	4	10	2	8
7	7	0	7	0	7	0	7	0	7	0	7	0	7
8	8	2	10	4	12	6	0	8	2	10	4	12	6
9	9	4	13	8	3	12	7	2	11	6	1	10	5
10	10	6	2	12	8	4	0	10	6	2	12	8	4
11	11	8	5	2	13	10	7	4	1	12	9	6	3
12	12	10	8	6	4	2	0	12	10	8	6	4	2
13	13	12	11	10	9	8	7	6	5	4	3	2	1

14
28
42
56
70
84
98

When Z_{14} has an inverse

1 * 1 MOD 14 = 1
3 * 5 MOD 14 = 1
5 * 3 MOD 14 = 1
9 * 11 MOD 14 = 1
11 * 9 MOD 14 = 1
13 * 13 MOD 14 = 1

99 mod 14

e). $\mathbb{Z}_{13} = \{0, \ldots, 12\}$ When $\mathbb{Z}_{13}$ has an inverse

*	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	4	6	8	10	12	1	3	5	7	9	11
3	3	6	9	12	2	5	8	11	1	4	7	10
4	4	8	12	3	7	11	2	6	10	1	5	9
5	5	10	2	7	12	4	9	1	6	11	3	8
6	6	12	5	11	4	10	3	9	2	8	1	7
7	7	1	8	2	9	3	10	4	11	5	12	6
8	8	3	11	6	1	9	4	12	7	2	10	5
9	9	5	1	10	6	2	11	7	3	12	8	4
10	10	7	4	1	11	8	5	2	12	9	6	3
11	11	9	7	5	3	1	12	10	8	6	4	2
12	12	11	10	9	8	7	6	5	4	3	2	1

13
26
39
52
65
78
91
104

$1 * 1 \bmod 13 = 1$
$2 * 7 \bmod 13 = 1$
$3 * 9 \bmod 13 = 1$
$4 * 10 \bmod 13 = 1$
$5 * 8 \bmod 13 = 1$
$6 * 11 \bmod 13 = 1$
$7 * 2 \bmod 13 = 1$
$8 * 5 \bmod 13 = 1$
$9 * 3 \bmod 13 = 1$
$10 * 4 \bmod 13 = 1$
$11 * 6 \bmod 13 = 1$
$12 * 12 \bmod 13 = 1$

When an element in $\mathbb{Z}_n$ has an inverse?

→ $1 * 1 \bmod n$
→ $(n-1) * (n-1) \bmod n$

- In n impar

→ $\left(\frac{n+1}{2}\right) * 2 \bmod n$

→ Always there're (n+1) elements

3. Find the intenger x such that

$5 * x \bmod 13 = 1$

$5 * 8 \bmod 13$

$40 \bmod 13 = 1$

13
26
→ 39 ←
52

$$13 \overline{)40}^{\,3}$$
01

$\boxed{x = 8}$

4. Find the integer x such that 5 *

$5 * X \bmod 7 = 1$

7

$\rightarrow 14 \leftarrow$

21

$5 * 3 \bmod 7$

$15 \bmod 7$

$$7 \overline{)\,15}^{\,2}$$

1

$\boxed{X = 3}$ //

5. Compute $3 * 2 / 5 \bmod 7$

$\frac{6}{5} \bmod 7$

$6 \bmod 7 = 5X$

$X = \frac{6}{5}$ //

6. Compute $(19 + 1/5) * 3 - 4/3 \bmod 11$

$3\left(19 + \frac{1}{5}\right) - \frac{4}{3} \bmod 11$

$3\left(\frac{96}{5}\right) - \frac{4}{3} \bmod 11$

$(a*b) \bmod n$

$\frac{288}{5} - \frac{4}{3} \bmod 11 =$

$= (a \bmod n) * (b \bmod n)$

$\frac{844}{15} \bmod 11 \therefore \bmod\left((56 \bmod 11) * \left(\frac{4}{15} \bmod\right) 11\right)$

$(1)\left(\frac{4}{15}\right) \bmod 11$

$56 + \frac{4}{15}$

$4 \bmod 11 = 15X$

$X = \frac{4}{15}$

$(1)\left(\frac{4}{15}\right) = \frac{4}{15}$ //

1