MATH 178 Homework #2

Tamir Enkhjargal

April 2019

NT

3.

$$73 = 2 * 35 + 3 \tag{1}$$
$$35 = 11 * 3 + 2 \tag{2}$$
$$3 = 1 * 2 + 1 \tag{3}$$
$$1 = 1 * 1 + 0 \tag{4}$$

$$1 = 3 - 1 * 2 \tag{5}$$
$$1 = 3 - 1 * (35 - 11 * 3) \tag{6}$$
$$1 = 12 * 3 - 1 * 35 \tag{7}$$
$$1 = 12 * (73 - 2 * 35) - 1 * 35 \tag{8}$$
$$1 = 12 * 73 - 25 * 35 \tag{9}$$

$$-25 + 73 = 48 \equiv 1 * 35^{-1} (mod\ 73) \tag{10}$$

The gcd(35,73) is 1. 35^{-1} in $\mathbb{Z}/73\mathbb{Z}$ is 48.

Because mod "respects" arithmetic functions, if we were to find $ax * x \equiv 1(mod\ 73)$ is the same as running the mod then multiplying by x again.

$$48 * 48 \equiv 1 * 35^{-1} * 35^{-1} (mod\ 73) \tag{1}$$
$$48^2 \equiv 1 * 35^{-2} (mod\ 73) \tag{2}$$
$$32 \equiv 1 * 35^{-2} (mod\ 73) \tag{3}$$

4.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Table 1: Addition Table in Mod 6

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Table 2: Multiplication Table in Mod 6

5.

Z*	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	7
7	7	5	7	1

Table 3: Modular Multiplication Modulo 8

Z*	1	3	7	9
1	1	3	5	9
3	3	9	1	7
7	5	1	1	3
9	9	7	3	1

Table 4: Modular Mulitplication Modulo 10

6.

After handwriting and brute-forcing through the combinations, the results are:

n	Elements in Range
2	6
3	4
4	3
5	12
6	2
7	12
8	3
9	4
10	6
11	12

Table 5: Table of inputs into $f_n(x)$ and number of elements in ranges Modulo 12

This can be broken down into a single function.

$$\text{Number of Elements in Range} = 12/\text{gcd(n,12)}$$

7.

$$27 \equiv 5(mod\ m) \tag{1}$$
$$\equiv m \mid (27 - 5) \tag{2}$$
$$\equiv m = 22 \tag{3}$$

Therefore, m can be any of its factors, 1, 2, 11, or 22.

8.

Since 13 is a prime number, this means that all numbers between 1-12 have a gcd of 1.

$$(x * 1) \bmod 13 = 1 \qquad x = 1 = 1^{-1} \tag{1}$$
$$(x * 2) \bmod 13 = 1 \qquad x = 7 = 2^{-1} \tag{2}$$
$$(x * 3) \bmod 13 = 1 \qquad x = 9 = 3^{-1} \tag{3}$$
$$(x * 4) \bmod 13 = 1 \qquad x = 10 = 4^{-1} \tag{4}$$
$$(x * 5) \bmod 13 = 1 \qquad x = 8 = 5^{-1} \tag{5}$$
$$(x * 6) \bmod 13 = 1 \qquad x = 11 = 6^{-1} \tag{6}$$
$$(x * 7) \bmod 13 = 1 \qquad x = 2 = 7^{-1} \tag{7}$$
$$(x * 8) \bmod 13 = 1 \qquad x = 5 = 8^{-1} \tag{8}$$
$$(x * 9) \bmod 13 = 1 \qquad x = 3 = 9^{-1} \tag{9}$$
$$(x * 10) \bmod 13 = 1 \qquad x = 4 = 10^{-1} \tag{10}$$
$$(x * 11) \bmod 13 = 1 \qquad x = 6 = 11^{-1} \tag{11}$$
$$(x * 12) \bmod 13 = 1 \qquad x = 12 = 12^{-1} \tag{12}$$