Michael Chillemi Hw 1

1. Solve using modular arithmetic
    a) 15*29 mod 13 =
    435 mod 13 = 6
    b) 2 * 29 mod 11 =
    58 mod 11 = 3
    c) 21 * 36 mod 17 =
    273 mod 17 =8
    d) -11 * 59 mod 19 =
    -649 Mod 19 =16
2. Compute the following
    a) ⅛ mod 13 = 0.2
    b) ⅛ mod 7 = 0.2
    c) 3 * ⅖ mod 17 = 1.2

3. Z4

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

a) Z4

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	4	6
3	0	3	6	9

b) Z5

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

2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	6	8
3	0	3	6	9	12
4	0	4	8	12	16

Z6

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	6
2	2	3	4	5	6	7
3	3	4	5	6	7	8
4	4	5	6	7	8	9
5	5	6	7	8	9	10

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	6	8	10

3	0	3	6	9	12	15
4	0	4	8	12	16	20
5	0	5	10	15	20	25

c)

In Z4 the elements that do not have a multiplicative inverse are 2 and 0.

In Z6 the elements that do not have a multiplicative inverse are 2, 3, 4 and 0.

d)

There exist a multiplicative inverse for all non-zero elements in Z5 because 5 is prime and all non-zero elements smaller than 5 are relatively prime to 5.

*	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	8	10	12
3	0	3	6	9	12	15	18
4	0	4	8	12	16	20	24
5	0	5	10	15	20	25	30
6	0	6	12	18	24	30	36

Inverse

$1^{-1} = 1$

$2^{-1} = 4$

$3^{-1} = 5$

$4^{-1} = 2$

$5^{-1} = 3$

$6^{-1} = 6$

e) Z11{0,1,2,3,4,5,6,7,8,9,10}

The multiplicative inverse of 5 in Z11 is 9.

Z12{0,1,2,3,4,5,6,7,8,9,10,11}

The multiplicative inverse of 5 in Z12 is 5.

Z13{0,1,2,3,4,5,6,7,8,9,10,11,12}

The multiplicative inverse of 5 in Z13 is 8.

f) Z21{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20}

$0^2 = 0$

$1^2 = 1$

$2^2 = 4$

$3^2 = 9$

$4^2 = 16$

$5^2 = 25\, r = 4$

$6^2 = 36\, r = 15$

$7^2 = 49\, r = 7$

$8^2 = 64\, r = 1$

$9^2 = 81\, r = 18$

$10^2 = 100\, r = 16$

$11^2 = 121\, r = 16$

$12^2 = 144\, r = 18$

$13^2 = 169\, r = 1$

$14^2 = 196\, r = 7$

$15^2 = 225\, r = 15$

$16^2 = 256\, r = 4$

$17^2 = 289\, r = 16$

$18^2 = 324\, r = 9$

$19^2 = 361\, r = 4$

$20^2 = 400\, r = 1$

4.

a) $7^{100}(mod\ 13)$ =9

b) $2^{197}(mod\ 13)$ =6