Erikson Sodergren CS462-01

1.
    a. 2*3mod13 = 6mod13
    b. 2*8mod7 = 2mod7
    c. 5*1mod11 = 5mod11
    d. 4*4mod15 = 1mod15
2.
    a. 1*5^{-1}mod13 = 1*8mod13 = 8mod13
    b. 1*5^{-1}mod7 = 1*3mod7 = 3mod7
    c. 3*2*5^{-1}mod7 = 3*2*3mod7 = 4mod7
3.
    a.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

    b.

x	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

    c.

+	0	1	2	3	4		x	0	1	2	3	4
0	0	1	2	3	4		0	0	0	0	0	0
1	1	2	3	4	0		1	0	1	2	3	4
2	2	3	4	0	1		2	0	2	4	1	3
3	3	4	0	1	2		3	0	3	1	4	2
4	4	0	1	2	3		4	0	4	3	2	1

    d.

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

   e. In Z_4, 0 and 2 did not have an inverse, while in Z_6, 0, 2, 3 and 4 did not have one. All elements in Z_5 had an inverse because 5 is prime, so no nonzero number smaller than it can have a gcd other than 1.

4. 9 in Z_{11} , 5 in Z_{12}, 8 in Z_{13}
5.
   a. 3*3mod13 = 9mod13
   b. 7*7mod13 = 8mod13
   c. $3^2*3^2*3^2*3^2*3^2$mod13 = 9*9*9*9*9mod13 = 3*3*9mod13 = 3mod13
   d. $(7^2)^{50}$mod13 = 3^{50}mod13 = $(3^{10})^5$mod13 = 3^5mod13 = 81*3mod13 = 9mod13
6. x=5
7. m=4: (1, 3) φ=2, m=5: (1, 2, 3, 4) φ=4, m=9: (1, 2, 4, 5, 7, 8) φ=6, m=26: (1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25) φ=12
8. a^{-1} = 15. X = 15(y-22)
   Pseudocode: convert char to int, put through decryption equation, convert back
   First the sentence and then the evidence said the queen