Inspection
$an \equiv bk+1$

CS 435 HW3 - Anish Abraham

Prime #s b/w 2-100

a) 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97 ⇒ 25

b) 2a) $7623 = 3^2 \cdot 7^1 \cdot 11^2$ & $7425 = 3^3 \cdot 5^2 \cdot 11^1 \Rightarrow 3^2 \cdot 11 = \boxed{99 = GCD}$

b) on page 4

3a)

i	1	2	3	4	5	6	7	8	9	10
$i^{-1} \bmod 11$	1	6	4	3	9	2	8	7	5	10

b)

i	1	2	3	4	5	6	7	8	9	10	11	12	13
$i^{-1} \bmod 14$	1	–	5	–	3	–	–	–	11	–	9	–	13

4)

a	b	c=(a/b)	r = a mod b
121 (1,0)	37 (0,1)	3	$10 = 121 - 3 \cdot 37$ (1,−3)
37 (0,1)	10 (1,−3)	3	$7 = 37 - 3 \cdot 10$ (−3,10)
10 (1,−3)	7 (−3,10)	1	$3 = 10 - 7 \cdot 1$ (4,−13)
7 (−3,10)	3 (4,−13)	2	$1 = 7 - 2 \cdot 3$ (−11,36)

$GCD(121, 37) = 1 = (-11) \cdot 121 + 36 \cdot 37$

$37^{-1} \bmod 121 = 36$

5) $x^{-1} \bmod n = x^{\phi(n)-1} \bmod n$ a) inv 5 mod 17

$x=5, n=17 \rightarrow n$ is prime $\phi(n) = p-1 = \phi(17) = 16 \rightarrow 5^{-1} \bmod 17 = 5^{15} \bmod 17$

$\equiv (5^3)^5 \bmod 17$

$\rightarrow = ((125 \bmod 17)^5) \bmod 17 = 6^5 \bmod 17$

$= (125)^5 \bmod 17$

$= (6^2)^2 \cdot 6 \bmod 17$

$= [(6^{2 \cdot 2} \bmod 17)(6 \bmod 17)] \bmod 17$

$= [([(6^2 \bmod 17)^2] \bmod 17) \cdot 6] \bmod 17 = [([(36 \bmod 17)^2] \bmod 17) \cdot 6] \bmod 17$

$\rightarrow = ((2^2 \bmod 17) \cdot 6) \bmod 17 = ((4 \bmod 17) \cdot 6) \bmod 17$

$= 4 \cdot 6 \bmod 17 = 24 \bmod 17 \boxed{= 7}$

b) inv 5 mod 21 $\Rightarrow x=5; n=21 \rightarrow \phi(n) = (p-1)(q-1) = (2)(6) = 12 = \phi(21)$

$= 5^n \bmod 21 \rightarrow 5^1 = 5 \bmod 21 = 5, \; 5^2 = 25 \bmod 21 = 4, \; 5^4 = (5^2)^2 \bmod 21 = 16 \bmod 21 = 16$

$5^8 = (5^4)^2 \bmod 21 = 16^2 \bmod 21 = 256 \bmod 21 = 4$

$5^n = 5^{8+2+1} = 4(4)(5) \bmod 21 = 80 \bmod 21 \boxed{= 17}$

a)

i	1	2	3	4	5	6	7	8	9	10	11	12	13
b) $5^i \bmod 14$	5	10	1	6	11	2	7	12	3	8	13	4	9

b)

i	1	2	3	4	5	6	7	8	9	10	11	12	13
$6^i \bmod 14$	6	12	4	10	2	8	0	6	12	4	10	2	8

Result not permutation of $(1, 2, \ldots, 13)$ b/c $GCD(6, 14) \neq 1$.

c)

$i \in \mathbb{Z}_{14}^*$	1	3	5	9	11	13
$3^i \bmod 14$	3	9	1	13	5	11
5^i "	5	1	11	3	13	9
9^i "	9	13	3	11	1	5
11^i "	11	5	13	1	9	3
13^i "	13	11	9	5	3	1

7)

i	1	2	3	4	$5 = p-2$	$6 = p-1$
$2^i \bmod 7$	2	4	1	2	4	1
3^i "	3	2	6	4	5	1
4^i "	4	2	1	4	2	1
5^i "	5	4	6	2	3	1
6^i "	6	1	6	1	6	1

7) a) given $b = p-1$ shows Permutation where $x^{p-1} \bmod p = 1$

b) column $5 = p-2$ gives inverse of each x value. P. is prime, $\phi(p) = p-1$, $\therefore x^{p-2} = x^{\phi(p)-1} = x^{-1} \pmod p$

8)

i	1	2	3	$4 = \phi(n)$	5
$1^i \bmod 10$	1	1	1	1	1
$3^i \bmod 10$	3	9	7	1	3
7^i "	7	9	3	1	7
9^i "	9	1	9	1	9

$\phi(n)$ Theorem says for every $x \in \mathbb{Z}_n^*$, $x^{\phi(n)} \bmod n = 1$. $\phi(n) = 4$ w/ whole column equal to 1.

b) column $5 = \phi(n)+1$, where values equal x proved by corollary 1.

c) column $3 = \phi(n)-1$ creates $x^{-1} \bmod n$ where columns $(3, 4, 5)$ produce $(x^{-1}, 1, x)$ respectively.

9) i | 1 | 2 | 3 | 4 | $S = \phi(n)+1$

$1^i \bmod 10$	1	1	1	1	1
2^i	2	4	8	6	2
3^i	3	9	7	1	3
4^i	4	6	4	6	4
5^i	5	5	5	5	5
6^i	6	6	6	6	6
7^i	7	9	3	1	7
8^i	8	4	2	6	8
$9^i \bmod 10$	9	1	9	1	9

9) a) column S shows Thmb which is for every positive integer $x < n$ (every row) col S shows $x^{\phi(n)+1} \bmod n = x$

b) col 4 shows Euler's thm where if $x \in Z_n^*$, then $x^{\phi(n)} \bmod n = 1$ which explains column 4 showing value of 1 for rows 1, 3, 7, 9.

c) val in col 4 cannot be 1 for any $x \in Z_n^*$ due to the reason if col 4 shows a value of 1 for any n, this means $x^4 \bmod n = 1$. This implies $x^3 \bmod n = x^{-1}$. However from 3 we know x has no inverse if $\gcd(x,n) \neq 1 \Rightarrow$ means $x \in Z_n^*$. $\therefore x^4 \bmod n \neq 1$ for any $x \in Z_n^*$

Encryption: $(x = 2169) \Rightarrow y = x^5 \bmod n = 2169^{13} \bmod 2747 = 223$

10 a) Computation of power:

Power i	square	mod 2747	x · n	mod 2747
13	4,020,020	1,164	2,524,716	223
6	6,553,600	2,005	2,005	2,005
3	4,704,561	1,697	3,680,793	2,560
1				2,169

b) Decryption: $z = y^b \bmod n = 223^{2437} \bmod 2747 = 2169$

Computation of latter exponentiations:

power	square	mod 2747	b · x	mod 2747
2437	50276	54	13157	2169
1218	151476	174	174	174
609	1656369	2615	546525	421
304	1519441	1287	1287	1287
152	1004089	1349	1349	1349
76	212521	1002	1002	1002
38	1552516	461	461	461
19	115336	215	47605	1246
9	151471	174	35502	341
4	30089	426	421	426
2	49729	283	283	283
1				283

2b)

a	b	q = ⌊a/b⌋	r = a − qb = ama + bmb
7623	7425	1	198
(1,0)	(0,1)		(1,−1)
7425	198	37	99
(0,1)	(1,−1)		(−37,38)
198	99	2	0
(1,−1)	(−37,38)		
99	0		
(−37,38)			

GCD(7623, 7425)

= 99 = −37a + 38b

s = −37, t = 38