EE2302 Foundations of Information Engineering

Assignment 5 (Solution)

1.

×	**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

a) No, because in the row corresponding to "3", there is no "1" in all entries. (By number theory, this is so because gcd (3,6) $\neq$ 1.)

b) Yes. The multiplicative inverse of 5 is 5, since $5 \times 5 \equiv 1 \pmod 6$ as can be observed from the table.

2.

a)

121	107		
1	0	121	a
0	1	107	b
1	-1	14	$c = a - b$
-7	8	9	$d = b - 7c$
8	-9	5	$e = c - d$
-15	17	4	$f = d - e$
23	-26	1	$g = e - f$

Hence, $\gcd(105,121) = 1 = 107\,x + 121\,y$ where $x = -26$ and $y = 23$.

$x = \left(-26 + \frac{121}{1}\,t\right) = -26 + 121\,\text{t}\,.$

$y = \left(23 - \frac{107}{1}t\right) = 23 - 107\,\text{t}\,.$

b)

575	345		
1	0	575	a
0	1	345	b
1	-1	230	$\text{c} = \text{a} - \text{b}$
-1	2	115	$\text{d} = \text{b} - \text{c}$

Hence, $\gcd(575, 345) = 115 = 575\,x + 345\,y$ where $x = -1$ and $y = 2$.

$x = -1 + \frac{345}{115}t = -1 + 3t.$

$y = 2 - \frac{575}{115}t = 2 - 5t.$

3. Note that $13^{26} = 13^{16} \times 13^{8} \times 13^{2}$

$13 \bmod 40 = 13$
$13^{2} \bmod 40 = 9$
$13^{4} \bmod 40 = 1$
$13^{8} \bmod 40 = 1$
$13^{16} \bmod 40 = 1$

Hence, $13^{16} \times 13^{16} \times 13^{2} \bmod 40 = 1 \times 1 \times 9 \bmod 40 = 9$

4.

Note that 73 is prime and 73 does not divide 9.
Then, by Fermat's Little Theorem $9^{73-1} \equiv 1 \bmod 73$.
Since 794=72*11+2, we have $9^{794} \equiv (9^{72})^{11}\, 9^{2} \bmod 73$.

Hence, $9^{794} \equiv 9^{2} \bmod 73$

$\equiv 8 \bmod 73$.