EE2302 Foundations of Information and Data Engineering

Assignment 5 (Solution)

1.

$\times$	**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	105		
1	0	121	a
0	1	105	b
1	-1	16	$c = a - b$
-6	7	9	$d = b - 6c = -6a + 7b$
7	-8	7	$e = c - d = 7a - 8b$
-13	15	2	$f = d - e = -13a + 15b$
46	-53	1	$g = e - 3f = 46\,a - 53b$

Hence, $\gcd(105,121) = 1 = 105\,x + 121\,y$ where $x = -53$ and $y = 46$.

$$x = \left(-53 + \frac{121}{1}\,t\right) = -53 + 121\,\mathrm{t}\,.$$

$$y = \left(46 - \frac{105}{1}t\right) = 46 - 105\,\mathrm{t}\,.$$

b)

67890	12345		
1	0	67890	a
0	1	12345	b
1	-5	6165	$\mathrm{c = a - 5b}$
-2	11	15	$\mathrm{d = b - 2c = -2a + 11b}$

Hence, $\gcd(67890,12345) = 15 = 12345\,x + 67890\,y$ where $x = 11$ and $y = -2$.

$$x = 11 + \frac{67890}{15}t = 11 + 4526\,t.$$

$$y = -2 - \frac{12345}{15}\mathrm{t} = -2 - 823\,t.$$

3. Note that $15^{34} = 15^{16} \times 15^{16} \times 15^{2}$

$15 \bmod 40 = 15$
$15^{2} \bmod 40 = 25$
$15^{4} \bmod 40 = 25$
$15^{8} \bmod 40 = 25$
$15^{16} \bmod 40 = 25$

Hence, $15^{16} \times 15^{16} \times 15^{2} \bmod 40 = 25 \times 25 \times 25 \bmod 40 = 25$

4.

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

$\equiv 8 \bmod 73.$

b) Since $x^{86} \equiv 6 \bmod 29$, x is not divisible by 29, for otherwise $x^{86} \equiv 0 \bmod 29$.
That means, we can apply Fermat's Little Theorem.
Since $86 = 3 \times 28 + 2$, we have $x^{2} \equiv 6 \bmod 29$.
We need to try all possible values between 0 and 28 for x.
The solutions are $x = 8$ or 21.

Remark 1: You may use the following code in SageMath to try all values. Note that the syntax is essentially the same as that of Python. In Python, range(29) generates integers from 0 up to, but not including, 29.

```
for x in range(29):
    if x^2 % 29 == 6:
        print(x)
```

Remark 2: Under mod p, where p is a prime number, a quadratic equation has at most two roots.