Solutions to HW Set 2

Math 1350

Section 2.2

1. These are the tables for multiplication mod 5,8,9,11, respectively. The rows and columns for 0,1 are omitted. These are always 0 and identity, respectively.

mod 5 ×	2	3	4
2	4	1	3
3	1	4	2
4	3	2	1

mod 8 ×	2	3	4	5	6	7
2	4	6	0	2	4	6
3	6	1	4	7	2	5
4	0	4	0	4	0	4
5	2	7	4	1	6	3
6	4	2	0	6	4	2
7	6	5	4	3	2	1

mod 9 ×	2	3	4	5	6	7	8
2	4	6	8	1	3	5	7
3	6	0	3	6	0	3	6
4	8	3	7	2	6	1	5
5	1	6	2	7	3	8	4
6	3	0	6	3	0	6	3
7	5	3	1	8	6	4	2
8	7	6	5	4	3	2	1

mod 11 ×	2	3	4	5	6	7	8	9	10
2	4	6	8	10	1	3	5	7	9
3	6	9	1	4	7	10	2	5	8
4	8	1	5	9	2	6	10	3	7
5	10	4	9	3	8	2	7	1	6
6	1	7	2	8	3	9	4	10	5
7	3	10	6	2	9	5	1	8	4
8	5	2	10	7	4	1	9	6	3
9	7	5	3	1	10	8	6	4	2
10	9	8	7	6	5	4	3	2	1

Because 8,9 are not prime their multiplication tables contain elements which multiply together to give multiples of 8,9 respectively. For example, in mod 8, when we multiply 4 and 6 we get a multiple of 8, since $4 = 2^2$ and $6 = 2 \cdot 3$, so $4 \cdot 6 \equiv 0 \pmod 8$.

2. a. $23 \equiv -3(\text{mod } 26)$, and $3 \cdot 9 \equiv 1(\text{mod } 26)$, so

$$-9 \equiv 17 = 23^{-1}(\text{ mod } 26).$$

b. $8 \equiv -5(\text{mod } 13)$, $(-5)^4 \equiv (-1)^2 \equiv 1(\text{mod } 13)$, so

$$(-5)^3 \equiv -125 \equiv 5 = 8^{-1}(\text{ mod } 13).$$

c. 5

d. 59 (note $(x-1)^2 = x^2 - 2x + 1 \equiv 1(\text{mod } x)$, for all x).

3. (a) 4

   (b) 4

   (c) 2

   (d) 3

   (e) 7

   (f) 24 (see 2.(d) for a quick way to solve this)

6. (a) modulus 10 we have, $3^{-1} \equiv 7$, $9^{-1} \equiv 9$, and 1,3,7,9 are the only elements with inverses, being relatively prime to 10.

   (b) read from table in 1.

4. (a) $3a \equiv 5 (\text{mod } 26)$, so $a = 19$, $b = 13$.

   (b) $2b \equiv 10 (\text{mod } 26)$, so $b = 5$ or $b = 18$. The second forces a contradiction, so $b = 5$, $a = 14$.

8. IMAGINATION IS MORE IMPORTANT THAN KNOWLEDGE

9. In mod 26 we have the equations

$$19a + b = 7$$

$$14a + b = 4$$

so $5a = 3$ giving $a = 11$, $b = 6$. Then $y = 11x + 6$ is the encipherment formula and so using the fact that $11^{-1} \equiv 19 (\text{mod } 26)$ we compute the decipherment formula as

$$x = 19y + 16$$

which yields the decrypted

IFYOU BOWAT ALLBO WLOW.

I.e.,“if you bow at all bow low”

10. A little trial and error give K coming from T and P coming from S, so that the decipherment formula is $x = 5y + 21$, which yields

PROSPERITY IS NOT WITHOUT MANY FEARS AND DISTASTES

AND ADVERSITY IS NOT WITHOUT COMFORTS AND HOPES

(with the missing letter ’S’ in distastes added back in!!)