Solutions for Assignment 3

Author: Kartick Kolachala

1. **1.a**

   Multiplicative inverse for GF (29) =
   {DNE, 1, 15, 10, 22, 6, 5, 25, 11, 13, 3, 8, 17, 9, 27, 2,0, 12, 21, 26, 16, 18, 4, 24, 23, 7 19, 14, 28

   1.b

   A = 79, b = 20

   1 = 20 –19

   1 = 20 - 1(79 - 3(20))
   1 = 20 - 79 + 3(20)
   1 = 4(20) - 1(79)

   X = -1, y = 4

   a = 62, b = 3

   1 = 3 - 2
   1 = 3 - 1(62 - 3(20))

   1 = 3 - 62 + 20(3)
   1 = 21(3) - 1(62)

   x = -1, y = 21

   a = 91, b = 22

   1 = 22 - 3.7

   = 22 - (91-22.4).7

   = 22 - (91.7 - 22.28)

   = 22.29 - 91.7

Here, x = -7, y = 29

a = 23, b = 5

1 = 3 - 2.1

= (23-5.4) - (5-3).1

= (23-5.4) - (5-(23-5.4)).1

= (23-5.4) - (5.1-23+5.4)

= (23-5.4) - (5.5-23)

= 2.23 - 5.9

Here, x = 2, y = -5

2. 11^3 = 1331
   Multiples of 11: 1331 / 11 = 121
   Numbers with Inverses: 1331 – 121 = 1210

3. **3.a**
   For this problem, the range will be from 0 to 4, and aj = {0, 1}

   i= 0: f(x) = a0 x^0 ; S1 = {0, 1}

   i= 1: f(x) = a0 x^0 + a1 x^1 ; S2 = {0, x, 1, 1 + x}

   i= 2: f(x) = a0 x^0 + a1 x^1 + a2 x^2 ; S3 = {0, x^2, x, x+x^2, 1, 1 + x^2, 1 + x, 1 + x + x^2}

   i= 3: f(x) = a0 x^0 + a1 x^1 + a2 x^2 + a3 x^3 ; S4 = {0, x^3, x^2, x^2 + x^3, x, x + x^3, x + x^2, x + x^2 + x^3, 1, 1 +

   x^3, 1 + x^2, 1 + x^2 + x^3, 1 + x, 1 + x + x^3, 1 + x + x^2, 1 + x + x^2 + x^3}

   i= 4: f(x) = a0 x^0 + a1 x^1 + a2 x^2 + a3 x^3 + a4 x^4 ; S5 = {0, x^4, x^3, x^3 + x^4, x^2, x^2 + x^4, x^2 + x^3, x^2 + x^3 + x^4, x, x + x^4, x

$+ x^3, x + x^3 + x^4, x + x^2, x + x^2 + x^4, x + x^2 + x^3, x + x^2 + x^3 + x^4, 1, 1 + x^4, 1 + x^3, 1$

$+ x^3 + x^4, 1 + x^2, 1 + x^2 + x^4, 1 + x^2 + x^3, 1 + x^2 + x^3 + x^4, 1 + x, 1 + x + x^4, 1 + x + x^3, 1 + x + x^3 +$

$x^4, 1 + x + x^2, 1 + x + x^2 + x^4, 1 + x + x^2 + x^3, 1 + x + x^2 + x^3 + x^4\}$

S = S1 U S2 U S3 U S4 U S5

$S = \{0, x^4, x^3, x^3 + x^4, x^2, x^2 + x^4, x^2 + x^3, x^2 + x^3 + x^4, x, x + x^4, x + x^3, x + x^3 + x^4, x + x^2, x + x^2 +$

$x^4, x + x^2 + x^3, x + x^2 + x^3 + x^4, 1, 1 + x^4, 1 + x^3, 1 + x^3 + x^4, 1 + x^2, 1 + x^2 + x^4, 1 + x^2 + x^3, 1 + x^2$

$+ x^3 + x^4, 1 + x, 1 + x + x^4, 1 + x + x^3, 1 + x + x^3 + x^4, 1 + x + x^2, 1 + x + x^2 + x^4, 1 + x + x^2 + x^3, 1$

$+ x + x^2 + x^3 + x^4\}$

3.b For this problem, the range will be from 0 to 1, and aj = {0, 1, 2, 3, 4}

i= 0: $f(x) = a0\ x^0$; S1 = {0, 1, 2, 3, 4}

i= 1: $f(x) = a0\ x^0 + a1\ x^1$; S2 = {0, x, 2x, 3x, 4x, 1, 1+ x, 1 + 2x, 1 + 3x, 1 + 4x, 2, 2 + x, 2 + 2x, 2

+ 3x, 2 + 4x, 3, 3 + x, 3 + 2x, 3 + 3x, 3 + 4x, 4, 4 + x, 4 + 2x, 4 + 3x, 4 + 4x}

S = S1 U S2

S = {0, x, 2x, 3x, 4x, 1, 1+ x, 1 + 2x, 1 + 3x, 1 + 4x, 2, 2 + x, 2 + 2x, 2 + 3x, 2 + 4x, 3, 3 + x, 3 +

2x, 3 + 3x, 3 + 4x, 4, 4 + x, 4 + 2x, 4 + 3x, 4 + 4x}

4. 4.a

Here, a = 423, b = 128
r1 = 423 mod 128 = 39; q1 = 3

r2 = 128 mod 39 = 11; q2 = 3
r3 = 39 mod 11 = 6; q3 = 3
r4 = 11 mod 6 = 5; q4 = 1
r5 = 6 mod 5 = 1; q5 = 1
r6 = 5 mod 1 = 0; q6 = 5
Since, gcd(423, 128) = 1, so they are coprime.
Now, find x, y such that x.423 + y.128 = 1
From equation, r = dividend - q.divisor
1 = (6). 1 - 1.(5)
= (39 - 3.11).1 - 1.(11 - 1.6)
= (39).1 - 3.(11) - 1.(11) + 1.(6)
= (423 - 3.128).1 - 4.(11) + 1.(39 - 3.11)
= (423).1 - 3.(128) - 4.(11) + 1.(39) - 3.(11)
= 1.(423) - 3.(128) - 7.(11) + 1.(39)
= 1.(423) - 3.(128) - 7.(128 - 3.39) + 1.(39)
= 1.(423) - 3.(128) - 7.(128) + 21.(39) + 1.(39)
= 1.(423) - 3.(128) - 7.(128) + 22.(39)
= 1.(423) - 10.(128) + 22.(423 - 3.128)
= 1.(423) - 10.(128) + 22.(423) - 66.(128)
= 23.(423) - 76.(128)
x = 23, y = -76

4.b

gcd(588, 210)
Here, a = 588, b = 210
r1 = 588 mod 210 = 168; q1 = 2
r2 = 210 mod 168 = 42; q2 = 1
r3 = 168 mod 42 = 0; q3 = 4
Since, gcd(588, 210) = 42 = d, so they are notcoprime
Find x, y such that x.588 + y.210 = 42
From equation, r = dividend - q.divisor
42 = (210). 1 - 1.(168)
= (210). 1 - 1.(588 - 2.210)
= (210). 1 - 1.(588) + 2.(210)
= -1.(588) + 3.(210)
x = -1, y = 3

4.c.

Here, a = 899, b = 493
r1 = 899 mod 493 = 406; q1 = 1
r2 = 493 mod 406 = 87; q2 = 1
r3 = 406 mod 87 = 58; q3 = 4
r4 = 87 mod 58 = 29; q4 = 1
r5 = 58 mod 29 = 0; q5 = 2
Since, gcd(899, 493) = 29 = d, so they are not coprime.
Find x, y such that x.423 + y.128 = 29
From equation, r = dividend - q.divisor
29 = (87). 1 - 1.(58)
= (493 - 1.406).1 - 1.(406 - 4.87)
= (493).1 - 1.(406) - 1.(406) + 4.(87)
= (493).1 - 2.(406) + 4.(493 - 1.406)
= (493).1 - 2.(406) + 4.(493) - 4.(406)
= (493).5 - 6.(406)
= (493).5 - 6.(899 - 1.493)
= (493).5 - 6.(899) + 6.(493)
= -6.(899) + 11.(493)
x = -6, y = 11

5. **5.a**
   Z *^ {100}}| = {1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33
   37, 39, 41, 43, 47, 49, 51, 53, 57, 59, 61, 63, 67, 69, 71,73, 77, 79, 81, 83,
   87, 89, 91, 93, 97, 99
   |Z *^ {100}}| = 40
   Hence
   3 ^ 1000 mod 100 = 3 ^ {1000 mod 40} mod 100
   3 ^ 20 mod 100

   (3 ^ 15) (3 ^ 5) mod 100

   (3 ^ 10) (3 ^ 45 * 43) mod 100

   (3 ^ 5 (3 ^ 5 mod 100) * 43 * 43)

   19320201 mod 100 = 1

5.b

Z *^ {35}}| = {1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19,*Z*35
22, 23, 24, 26, 27, 29, 31, 32, 33, 34}

|Z *^ {100}}| = 244,800,000,002

Hence,
101 ^ (4,800,000,002) mod 35 = 101 ^ (4,800,000,002 mod 24)mod 35

= 101 ^ 2 mod 35 = 16

5.c

Z * ^ 55 = {1, 2, 3, 4, 6, 7, 8, 9, 12, 13, 14, 16, 17, 18, 19, 21, 23, 24, 26, 27, 28, 29, 31, 32, 34, 36, 37, 38,39, 41, 42, 43, 46, 47, 48, 49, 51, 52, 53, 54}

| Z * ^ 55| = 40

46 ^ 51 mod 55

46 ^ {51 mod 40} mod 55

46 ^ 11 mod 55

= 46

6.

(4 ^ 1536 – 9 ^ 4824) mod 25 should be 0
Now
|Z* 25| = 20
4^ (1536 mod 20) - 9(4824 mod 20) mod 25
(4 ^ 16 – 9^ 4) mod 25
4 ^ 16 mod 25 – 9 ^ 4 mod 25
= 10 hence not divisible

a.

(5 ^ 30000 – 6 ^ 123456) mod 23 should be 0
Hence (5 ^ (30000 mod 22) - 6 ^ (123456 mod 22)) mod 23
5 ^ 14 mod 23 – 6 ^ 14 mod 23 = 4
Not multiple