SOLUTIONS FOR ASSIGNMENT-3

HUMESH REDDY VENKATAPURAM **CS 525: INTRO TO CRYPTO**

1) Multiplicative inverses:

(a) Find the set of multiplicative inverses in GF (23).

(b) Use the Extended Euclidean algorithm to find multiplicative inverses of (20 mod 79), (3 mod 62), (22 mod 91), and (5 mod 23).

Answer:

(a) GF(23) = {1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22}

Here N = 23

In the context of modular arithmetic, for an integer a that is not divisible by the modulus N, its multiplicative inverse is a^{-1}. So,

$a.a^{-1} \cong 1 \bmod N$

$1 \times 1 \equiv 1 \bmod 23$ -> Inverse of 1 is 1

$2 \times 12 \equiv 1 \bmod 23$ -> Inverse of 2 is 12

$3 \times 8 \equiv 1 \bmod 23$ -> Inverse of 3 is 8

…… so on ……

The multiplicative inverse in GF (23) are:

a a^{-1}

1 -> 1

2 -> 12

3 -> 8

4 -> 6

5 -> 14

6 -> 4

7 -> 10

8 -> 3

9 -> 18

10 -> 7

11 -> 21

12 -> 2

13 -> 16

14 -> 5

15 -> 20

16 -> 13

17 -> 19

18 -> 9

19 -> 17

20 -> 15

21 -> 11

22 -> 22

0 doesn't have a multiplicative inverse in any field. Because it is undefined

(b) i) Need to use the Extended Euclidean algorithm to find multiplicative inverses of (20 mod 79)

To find the multiplicative inverse of a modulo b, we are looking for an integer x such as:

$a.x \equiv 1 \bmod b$

In this case, a = 20 and b = 79

The Extended Euclidean Algorithm is a method for determining the coefficients x and y such that:

ax + by = gcd (a,b)

Let's use this formula: dividend =divisor * quotient + Remainder

$remainder_1$ = 20 mod 79 = (20) $quotient_1$ = 0

$remainder_2$ = 79 mod 20 = (19) $quotient_2$ = 3

$remainder_3$ = 20 mod 19 = (1) $quotient_3$ = 1 ---------------- This is the GCD because the remainder is 1 (1)

$remainder_4$ = 19 mod 1 = (0) $quotient_4$ = 19

Now,

Let's try {remainder = dividend - (divisor * quotient)}

From (1) (Can see the above steps)

1 = 20 mod 19

1 = 20 - (19) * 1

= 20 – 1 (79 – (20) * 3)

= 20 – 79 + 3 * (20)

= 4(20) – 79

= 4(20) + (-1)79

Therefore, the above equation is in the form of ax + by = 1

So, **x = 4 and y = -1**

ii) Need to use the Extended Euclidean algorithm to find multiplicative inverses of (3 mod 62).

To find the multiplicative inverse of a modulo b, we are looking for an integer x such as:

a.x ≡ 1 mod b

In this case, a = 3 and b = 62

The Extended Euclidean Algorithm is a method for determining the coefficients x and y such that:

ax + by = gcd (a,b)

Let's use this formula: dividend =divisor * quotient + Remainder

$remainder_1$ = 3 mod 62 = 3 $quotient_1$ = 0

$remainder_2$ = 62 mod 3 = 2 $quotient_2$ = 20

$remainder_3$ = 3 mod 2 = 1 $quotient_3$ = 1 ------------------ This is the GCD because the remainder is 1 – (2)

$remainder_4$ = 2 mod 1 = 0 $quotient_4$ = 2

Now,

Let’s try {remainder= dividend - (divisor * quotient)}

From (2) (Can see the above steps)

1 = 3 - (2) * 1

= 3 – 1 [62 – 20 * (3)]

= 3 – 62 + 20 * (3)

= 21 (3) – 1 (62)

Therefore, the above equation is in the form of ax + by = 1

So, **x = 21 and y = -1**

iii) Need to use the Extended Euclidean algorithm to find multiplicative inverses of (22 mod 91).

To find the multiplicative inverse of a modulo b, we are looking for an integer x such as:

a.x ≡ 1 mod b

In this case, a = 22 and b = 91

The Extended Euclidean Algorithm is a method for determining the coefficients x and y such that:

ax + by = gcd (a,b)

Let's use this formula: dividend =divisor * quotient + Remainder

$remainder_1$ = 22 mod 91 = 22 $quotient_1$ = 0

$remainder_2$ = 91 mod 22 = 3 $quotient_2$ = 4

$remainder_3$ = 22 mod 3 = 1 $quotient_3$ = 7 --------------- This is the GCD because the remainder is 1 – (3)

$remainder_4$ = 3 mod 1 = 0 $quotient_4$ = 3

Now,

Let's try {remainder= dividend - (divisor * quotient)}

From (3) (Can see the above steps)

1 = 22 (1) - (3) * 7

= 22 - ((91 – 22 * (4)) 7)

= 22 – 7 * (91) + 28 * (22)

= 29(22) – 7(91)

Therefore, the above equation is in the form of ax + by = 1

So, **x = 29 and y = -7**

iv) Need to use the Extended Euclidean algorithm to find multiplicative inverses of (5 mod 23)

To find the multiplicative inverse of a modulo b, we are looking for an integer x such as:

a.x ≡ 1 mod b

In this case, a = 22 and b = 91

The Extended Euclidean Algorithm is a method for determining the coefficients x and y such that:

ax + by = gcd (a,b)

Let's use this formula: dividend =divisor * quotient + Remainder

$remainder_1 = 5 \bmod 23 = 5$ $quotient_1 = 0$

$remainder_2 = 23 \bmod 5 = 3$ $quotient_2 = 4$

$remainder_3 = 5 \bmod 3 = 2$ $quotient_3 = 1$

$remainder_4 = 3 \bmod 2 = 1$ $quotient_4 = 1$---------------- This is the GCD because the remainder is 1 – (4)

$remainder_5 = 2 \bmod 1 = 0$ $quotient_5 = 2$

Now,

Let's try {remainder= dividend - (divisor * quotient)}

From (4) (Can see the above steps)

1 = 3 - (2) * 1

= 3 - (5 - (3) (1)) * (1)

= 3 - (5 – 3) = 3 - (5 + 3)

= 2 (3) - 5

= 2 (23) -2 (5) (4) - 5

= 2 (23) - 5 (8) - 5

= 5(-9) + 23(2)

Therefore, the above equation is in the form of ax + by = 1

So, **x = -9 and y = 2**

X = -9 is the multiplicative inverse of 5 modulo 23. However, since we want a positive inverse, we can add the modulus 23 to -9, which gives:

X = -9 + 23 = 14

2) How many integers modulo 11^3 have inverses? You may find the following theorem useful.

The theorem states that an integer a has a multiplicative inverse modulo N if and only if gcd(a, N) = 1. This suggests that a and N have no factors in common other than 1. In other words, a and N are relatively prime.

One method we can use extended Euclidean algorithm. This one can find the GDC of two integers., which states for any integers a and b, which exist integers x and y as:

ax + by = gcd(a,b)

We'd want to know how many numbers modulo 11^3 have inverses.

let N = 11^3 = 1331 (range 0 < a < 1331 and b is 11^3)

If gcd (a, 11^3) = 1, then we have:

ax + 11^3y = 1

Taking this equation modulo 11^3, we get:

ax ≡ 1 (mod11^3)

This indicates that x is the modulo 11^3 multiplicative inverse.

So we just need to count how many a values in the range 0 < a < 11^3 with gcd(a, 11^3) = 1.

This may be accomplished by examining each value of a and using the extended Euclidean method.

We may also use a shortcut by observing that gcd(a, 11^3) = 1 if and only if a is not divisible by 11.

This is because 11 is the only prime factor of 11^3. As a result, we may exclude all multiples of 11 from the range 0 to 11^3 and count the remaining numbers.

$$11^3 - 1 - \frac{11^3}{11} = \frac{10}{11} \cdot (11^3 - 1) = \frac{10}{11} \cdot (1330) = 1210$$

As a result, using this strategy, there are 1210 numbers modulo 11^3 that have inverses.

3) Find the set of polynomials in GF (2^4) and GF (5^2)?

The notation of GF is given as a GF (p^n)

Here the 2^4 and 5^2 are not in the form of where p is prime. Therefore, such fields are not typical.

If it meant GF (2^4) and GF (5^2):

GF (2^4):

It has 16 elements (2 * 2 * 2 * 2 = 16)

The M is 4

F(x)= $a_{m-1} x^{m-1} + a_{m-2} x^{m-2}$ ………….$a_{m-n} x^{m-n}$

It is represented as polynomials of degree less than 4 with the coefficients in GF(2) which are 0 and 1. So the polynomials for GF(2^4) is:

= {0,1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1, x^3, x^3+1, x^3+x, x^3+x+1, x^3+x^2, x^3+x^2+1, x^3+x^2+x, x^3+x^2+x+1}

GF (5^2):

It has 25 elements (5 * 5 = 25)

The M is 2

$F(x)= a_{m-1} x^{m-1} + a_{m-2} x^{m-2}$ ....$a_{m-n} x^{m-n}$

It is represented as polynomials of degree less than 2 with the coefficients in GF (5) which are 0, 1, 2, 3, 4. So the polynomials for GF (5^2) is:

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

4) We worked out a few examples of Euclid's algorithm and the extended Euclidean

algorithm in class. Use that as a reference to solve the following:

(a) Find d = gcd(423, 128). Are they co-prime? Find integers x, and y, such that d = x · 423 + y · 128.

(b) Find d = gcd(588, 210). Are they co-prime? Find integers x, y, such that d = x · 588 + y · 210.

(c) Find d = gcd(899, 493). Are they co-prime? Find integers x, and y, such that d = x · 899 + y · 493.

a) d = gcd(423, 128)

The Extended Euclidean Algorithm is a method for determining the coefficients x and y such that:

423 mod 128

ax + by = d

Let's use this formula: dividend =divisor * quotient + Remainder

$remainder_1$ = 423 mod 128 = 39 $quotient_1$ = 3

$remainder_2$ = 128 mod 39 = 11 $quotient_2$ = 3

$remainder_3$ = 39 mod 11 = 6 $quotient_3$ = 3

$remainder_4$ = 11 mod 6 = 5 $quotient_4$ = 1

$remainder_5$ = 6 mod 5 = 1 $quotient_5$ = 1-------- This is the GCD because the remainder is 1 – (5)

$remainder_6$ = 5 mod 1 = 0 $quotient_6$ = 5

Are they co-prime? Yes, they are co-primes.

Now,

Let’s try {remainder= dividend - (divisor * quotient)}

From (5) (Can see the above steps)

1 = 6−1 * (5)

=6−1(11−1(6))

=2 * (6) − 1 * (11)

=2(39−3 * (11)) − 1(11)

=2(39) − 7(11)

=2(39) − 7(128−3 * (39))

=23(39) − 7(128)

=23(423−3(128)) − 7(128)

=23(423) − 76(128)

Therefore, the above equation is in the form of ax + by = 1

So, **x = 23 and y = -76 and d = 1**

1 = 23 * 423 + (-76) * 128

b) d = gcd(588, 210)

The Extended Euclidean Algorithm is a method for determining the coefficients x and y such that:

588 mod 210

ax + by = d

Let's use this formula: dividend =divisor * quotient + Remainder

$remainder_1$ = 588 mod 210 = 168 $quotient_1$ = 2

$remainder_2$ = 210 mod 168 = 42 $quotient_2$ = 1------------------------------ Here the GCD is not 1 – (6)

$remainder_3$ = 168 mod 42 = 0 $quotient_3$ = 4

Are they co-prime? No, they are not co-primes.

Now,

Let’s try {remainder= dividend - (divisor * quotient)}

From (6) (Can see the above steps)

42 = 210 − 1 * (168)

$= 210 - 1(588 - 2 * (210))$

$= 3(210) - 1(588)$

Therefore, the above equation is in the form of ax + by = d

So, **x = -1 and y = 3 and d = 42**

42 = (-1) * 558 + (3) * 210

c) d = gcd(899, 493)

The Extended Euclidean Algorithm is a method for determining the coefficients x and y such that:

899 mod 493

ax + by = d

Let's use this formula: dividend =divisor * quotient + Remainder

$remainder_1 = 899 \bmod 493 = 406$ $quotient_1 = 1$

$remainder_2 = 493 \bmod 406 = 87$ $quotient_2 = 1$

$remainder_3 = 406 \bmod 87 = 58$ $quotient_3 = 4$

$remainder_4 = 87 \bmod 58 = 29$ $quotient_4 = 1$------------------------- Here the GCD is not 1 – (7)

$remainder_5 = 58 \bmod 29 = 0$ $quotient_5 = 2$

Are they co-prime? No, they are not co-primes.

Now,

Let's try {remainder= dividend - (divisor * quotient)}

From (7) (Can see the above steps)

$29 = 87 - 1 * (58)$

$= 87 - 1(406 - 4(87))$

$= 5(87) - 1(406)$

$= 5(493 - 1 * (406)) - 1(406)$

$= 5(493) - 6(406)$

$= 5(493) - 6(899 - 1(493))$

$= 11(493) - 6(899)$

Therefore, the above equation is in the form of ax + by = d

So, **x = -6 and y = 11 and d = 29**

42 = (-6) * 899 + (11) * 493

5) Compute the following using the Chinese remainder theorem, or the group-order rule. You may also use the modular arithmetic rules in "numTheoryI.pdf".

(a) 3^{1000} mod 100

(b) $101^{4,800,000,002}$ mod 35

(c) 46^{51} mod 55

(a) Here n=100

$|Z^*_{100}| = Z^*_2 * Z^*_5$

According to the above step, I eliminated multiples of 2 and 5 in the 100. So, the remaining are:

$|Z^*_n|$={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} = {40}

Now,

- $3^{1000 \text{ mod } 40}$ mod 100 (Here 1000 mod 40 = 0)
- 3^0 mod 100 ($3^0 = 1$)
- **1 mod 100 = 1**

(b) Here n=35

$|Z^*_{35}| = Z^*_5 * Z^*_7$

According to the above step, I eliminated multiples of 5 and 7 in the 35. So, the remaining are:

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

Now,

- $101^{4,800,000,002 \text{ mod } 24}$ mod 35 (Here 4,800,000,002 mod 24 = 2)
- 101^2 mod 35 (101^2 = 10201)
- 10201 mod 35 = **16**

(c) Here n=55

$|Z^*_{55}| = Z^*_5 * Z^*_{11}$

According to the above step, I eliminated multiples of 5 and 11 in the 55. So, the remaining are:

$|Z^*_n|$={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} = {40}

Now,

- $46^{51 \bmod 40} \bmod 55$ – (51 mod 40 = 11)
- $46^{11} \bmod 55$
- $(46^5 * 46^5 * 46) \bmod 55$ – (Here I am using formula – a*b mod n= (a mod n * b mod n) mod n)
- $(46^5 \bmod 55 * 46^5 \bmod 55 * 46 \bmod 55) \bmod 55$ – ($46^5 \bmod 55$ – 21 and 46 mod 55 - 46)
- (21 * 21 * 46) mod 55
- 20286 mod 55 = **46**

6) Is $(4^{1862} – 9^{3206})$ divisible by 25?

Now,

$4^{1862} \bmod 25 – 9^{3206} \bmod 25$

$|Z^*_{25}| = Z^*_5$ (Now removing the multiple of 5)

According to the above step, I eliminated multiples of 25. So, the remaining are:

$|Z^*_n|$={1,2,3,4,6,7,8,9,11,12,13,14,16,17,18,19,21,22,23,24} = {20}

I am dividing a = $4^{1862} \bmod 25$ and b = $9^{3206} \bmod 25$

a - $4^{1862 \bmod 20} \bmod 25$ (1862 mod 20 = 2)

- $4^2 \bmod 25$
- 16 mod 25

a – **16**

b - $9^{3206 \bmod 20} \bmod 25$ (3206 mod 20 = 6)

- $9^6 \bmod 25$ (9^6 = 531441)
- 531441 mod 25

b - **16**

$4^{1862} \bmod 25 – 9^{3206} \bmod 25$ = **16 – 16**

= **0**

- Is (4^{1862} – 9^{3206}) divisible by 25? Yes, it is divisible.

7) Is the difference between $5^{30,000}$ and 6^{887543} a multiple of 23?

($5^{30,000}$ - 6^{887543}) mod 23 = $5^{30,000}$ mod 23 - 6^{887543} mod 23

First, I am doing for $5^{30,000}$ mod 23:

$|Z^*_{23}| = Z^*_{23}$ (Now removing the multiple of 23)

According to the above step, I eliminated multiples of 23. So, the remaining are:

$|Z^*_n|$= {1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22} = {22}

- $5^{30,000 \text{ mod } 22}$ mod 23 (30000 mod 22 - 14)
- 5^{14} mod 23
- (5^7 * 5^7) mod 23
- (5^7 mod 23 * 5^7 mod 23) mod 23 - (Here I am using formula – a*b mod n= (a mod n * b mod n) mod n)
- (78125 mod 23 * 78125 mod 23) mod 23 – (5^7 – 78125 and 78125 mod 23 - 17)
- (17 * 17) mod 23
- 289 mod 23 = **13**

Second, I am doing this for 6^{887543} mod 23:

$|Z^*_{23}| = Z^*_{23}$ (Now removing the multiple of 23)

According to the above step, I eliminated multiples of 23. So, the remaining are:

$|Z^*_n|$= {1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22} = {22}

- $6^{887543 \text{ mod } 22}$ mod 23 (887543 mod 22 - 19)
- 6^{19} mod 23
- (6^6 * 6^6 * 6^6 * 6) mod 23 (Here I am using formula – a*b mod n= (a mod n * b mod n) mod n)
- (6^6 mod 23 * 6^6 mod 23 * 6^6 mod 23 * 6 mod 23) mod 23
- (12 * 12 * 12 * 6) mod 23
- (10368) mod 23 = **18**

Now,

$5^{30,000}$ mod 23 - 6^{887543} mod 23 = 13 – 18 = -5

- Is the difference between $5^{30,000}$ and 6^{887543} a multiple of 23? -5 is not a multiple of 23.