Firas Aboushamalah

250 920 750

CS 2214 Assignment #3

Marc Moreno

Problem 1: Functions and Matrices

1a)

The solution is the following matrix because you have to multiply using the dot product: Using the A matrix (above), and A(x, y), we use the dot product to multiply and receive: (0(x) + 2(y), 3(x) + 0(y)) by removing the zeros, we receive the answer: (2y, 3x).

1b)

The solution is by having A equal all 0 so that every product via the Dot Product results in a 0.

1c)

The solution is the following matrix because you have to multiply using the dot product: Using the A matrix (above), and A(x, y), we use the dot product to multiply and receive: (0(x) + 1(y), 0(x) + 1(y)) by removing the zeros, we receive the answer: (y, y).

1d)

The solution is the following matrix because you have to multiply using the dot product: Using the A matrix (above), and A(x, y), we use the dot product to multiply and receive: (1(x) + 1(y),

-1(x) + 1(y)) by removing the zeros, we receive the answer: (y + x, y - x).

2a) This function is injective because for all (x1, y1) and (x2, y2), F1(x1, y1) = F1(x2, y2). Therefore, y1 = y2 and x1=x2 and so the function is one-to-one.

2b) This is not injective. Because all of the F2(x1, y1) are 0, there is multiple inputs that will give the same output. For example F2(0, 1) = (0, 0) = F2(0, 4). It is not surjective either because there is no preimage for various outputs – for example (1, 1).

2c) This function is not injective because there are different inputs that relinquish the same output. For example, F3(1, 2) = (2, 2) = F3(3, 2). F3 is surjective, however, as every (x’, y’) has a preimage in the domain of F3.

2d) This function is injective because for all (x1, y1) and (x2, y2), F(x1, y1) = F(x2, y2). Therefore, (x1, y1) = (x2, y2). It is surjective as well because not only is there only one solution for every pair of output, there is also a preimage for every possible output that can be achieved.

Problem 2: Chinese Remainder Theorem

1. Prove that the above c satisfies both c ≡ a mod m and c ≡ b mod n.

To prove this, we see that c is congruent to a + (b-a) sm

Therefore, for some number I, c is congruent to a + i\*sm. Moving on, we want to solve

C ≡ a mod m. Therefore, to isolate m with a number i we see c – a.

Problem 3: Solving Congruences

1. 5 x + 9 = 10 mod 77. This can be simplified to 5x = 1 mod 77. However, 5x can be reduced to separate x to be x = 5 mod 77. We now use Euclidian’s Algorithm to achieve the lowest common divisor between 5 and 77. Note: We cannot use the Chinese Remainder Theorem because there are no congruencies with two relative prime numbers.

Therefore, we get:

Gcd(5, 77) = 1

77 = 5 + q + r

77 = 5 \* 15 + 2

5 = 2 \* 2 + 1

1 = 5 – 2(77-5\*15)

1 = 5 – 2 \* 77 + 50-5

1 = 31 \* 5 – 2 \* 77

M = 5 and t = 77

S5 + t77 = 1

Bézout coefficient for 5 and 77 is 31 because 31 is the inverse of 5 mod 77.

1. If m = 77, then the range of x is 0 ≤ x < 77. The two congruences are:

x ≡ 2 mod 7 and x ≡ 3 mod 11. This means that:

M1 = 11 and M2 = 7. (M1 = 11 because it is everything but 7, and M2 is 7 because it is everything but 7).

Y1 ≡ 1 mod 7 and Y2 ≡ 1 mod 11.

Y1 can be reduced so that it is 4y1 ≡ 1 mod 7 which is y1 = 2

Y2 can be reduced so that it is 7y2 = 1 mod 11 which is y2 = 8

Therefore, x = (2 \* 11 \* 2) + (3 \* 7 \* 8) = 44 + 168 = 212. Because 212 is outside of the realm of our limits, we subtract until it gets below 77: 212 – 154 = 58. Therefore x = 58.

1. X + y = 33 mod 77 and x – y = 10 mod 77. The greatest divisor (77, 77) = 1. We can isolate x to be x = 10 + y and now find the number where x = y + 10. This number modulo with 77 must give us our x. If we use x = 60, then by these terms, y must be

x – 10 which gives 110 (x + y) mod 77 = 33 – we confirm that it is correct because of the first constraint where x + y = 33 mod 77.

Problem 4: RSA

1. Compute the product n = p q and Φ(n)

n = p(q)

n = 5(11)

n = 55

Φ(n) = (p – 1) \* (q – 1) = 4 \* 10 = 40

1. Is this choice for of e valid here?

Yes because the lowest divisor is gcd(3, 40) which is 1. The public exponent is 3 which is a prime number and so the public exponent e is a valid choice.

1. Compute d , the private exponent of Alice

D = 27 since 3 \* 27 = 81. 81 is simply 1 mod 40.

1. Encrypt the plain-text M using Alice public exponent. What is the resulting cipher-text C?

C = Me mod n

C = 43 mod 55

C = 64 mod 55

C = 9

5. Verify that Alice can obtain M from C, using her private decryption exponent.

C = Cd mod n

C = 927 mod 55

C = 4