Cs 2214b- Assignment3

Student Name: MingCong, Zhou
Student Number: 250945414
Student Account: mzhou272

Assignment #3
Due: Mar. 5, 2017, by 23:55
Submission: on the OWL web site of the course

Problem 1 (Functions and matrices) *[30 marks]* Consider the set of ordered pairs (x, y) where x are y are real numbers. Such a pair can be seen as a point in the plane equipped with Cartesian coordinates (x, y).

1. For each of the following functions F_1, F_2, F_3, F_4, determine a (2×2)-matrix A so that the point of coordinates $(x \quad y)$ is sent to the point $(x' \quad y')$ when we have

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix} \tag{1}$$

where

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{2}$$

(a) $F_1(x, y) = (2y, 3x)$
(b) $F_2(x, y) = (0, 0)$
(c) $F_3(x, y) = (y, y)$
(d) $F_4(x, y) = (y + x, y - x)$

1. $A = \begin{pmatrix} 0 & 2 \\ 3 & 0 \end{pmatrix}$
2. $A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$
3. $A = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$
4. $A = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$

2. Determine which of the above functions F_1, F_2, F_3, F_4 is injective? sur-jective? Justify your answer.

1. F1 is injective: Indeed, for all (X1, Y1) and (X2, Y2), if F1(X1, Y1) = F1(X2, Y2) holds then we have (2 * Y1, 3 * X1) = (2 * Y2, 3 * X2) that is, 2Y1 = 2Y2 and 3X1 = 3X2, thus (X1, Y1) = (2 * X2, 3 * Y2), which exactly means that F1 is injective. F1 is surjective: Indeed, every (x', y') has a pre-image by F1, namely (2y', 3x'), since F1(y', x') = (1/2x', 1/3y') holds.
2. F2 is not injective, for all (x,y) the result through F2 is always (0,0). That is not one to one. F2 is not surjective: Indeed, (1,1) has no pre-image by F2
3. F3 is not injective For all x, F(x,y) point to the same point which is the (y,y). This is not one to one. F3 is not surjective, because when (1,0) there is no pre-image for it.
4. F4 is injective: For all (X1, Y1) and (X2,Y2), if F4(X1,X2) = F4(X2,Y2) holds then we have (Y1 + X1, Y1 - X1) = (Y2 + X2, Y2 - X2) that is Y1 + X1 = Y2 + X2 and Y1 - X1 = Y2 - X2, which exactly means that F1 is injective. F4 is surjective every (x', y') can find at least one preimage by F4.

Problem 2 (Chinese Remaindering Theorem) *[20 marks]* Let m and n be two relatively prime integers. Let $s, t \in \mathbb{Z}$ be such that $s\,m + t\,n = 1$. The *Chinese Remaindering Theorem* states that for every $a, b \in \mathbb{Z}$ there exists $c \in \mathbb{Z}$ such that

$$(\forall x \in \mathbb{Z}) \qquad \begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases} \quad \Longleftrightarrow \quad x \equiv c \mod m\,n \tag{3}$$

where a convenient c is given by

$$c \;=\; a + (b-a)\,s\,m = b + (a-b)t\,n \tag{4}$$

1. Prove that the above c satisfies both $c \equiv a \mod m$ and $c \equiv b \mod n$.
2. Let $x \in \mathbb{Z}$. Prove that if $x \equiv c \mod m\,n$ holds then $x \equiv a \mod m$ and $x \equiv b \mod n$ both hold as well.
3. Let $x \in \mathbb{Z}$. Prove that if both $x \equiv a \mod m$ and $x \equiv b \mod n$ hold then so does $x \equiv c \mod m\,n$.

Solution 2

1. By theorem 4 from text, "The integers a and are congruent modulo m if and only if there is an integer k such a = b + km". In this case a = "c", b = "a" and k = "b+k". Therefore c and a are congruent modulo m, c ≡ a mod m. At the same strategy, c ≡ b mod n as well(c = b + (a-b)tn).
2. ∵ x ≡ c mod mn holds

   ∴by theorem 4: x = mnk + c //we denote that as "A"

   recall:

   c = a + (b — a) s m = b + (a — b)t n

   substituting c into "A" can get two formulas

   x =a + mnk + (b — a) s m and x = b + mnk + (a — b)t n

   Simplifying the above two formulas:

   x =a + m[nk + (b — a) s] and x = b + n[mk + (a — b)t]

   denote "nk + (b — a) s" as k1 and "mk + (a — b)t" as k2:

   x =a + mk1 and x = b + nk2

   which satisfy theorem 4 again:

   therefore: x ≡ a mod m and x ≡ b mod n
3. ∵x ≡ a mod m and x ≡ b mod n

   ∴x = mk + a and x = nj + b

   Substituting mk+a into x ≡ b mod n:

   mk+a ≡ b mod n

   mk ≡ b-a mod n (denote this as "GG")

   ∵sm + tn = 1, we multiply both side by mod n, we can get:

   ∴sm mod n + tn mod n = 1 mod n

   by simplifying the above formula we can get:

   sm mod n = 1 mod n

   which is equivalent to:

   sm ≡ 1 (mod n)

   therefore s is the inverse of m modulo n.

   multiply both side of "GG" by its inverse:

   s * mk ≡ s * (b-a) mod n

   k ≡ s (b-a) mod n

   x = [s (b-a) mod n]m + a //assume s (b-a) < n

   then x = a + (b-a) sm = c

   therefore:

   x ≡ c mod m n

Problem 3 (Solving congruences) *[30 marks]*

1. Find all integers x such that $0 \leq x < 77$ and $5x + 9 = 10 \mod 77$. Justify your answer.
2. Find all integers x such that $0 \leq x < 77$, $x \equiv 2 \mod 7$ and $x \equiv 3 \mod 11$. Justify your answer.
3. Find all integers x and y such that $0 \leq x < 77$, $0 \leq y < 77$, $x + y = 33 \mod 77$ and $x - y = 10 \mod 77$. Justify your answer.

Solution 3

1. We have $5 \times 31 \equiv 1 \bmod 77$. That is, 31 is the inverse of 5 modulo 77. We multiply by 31 each side of:

$$5x + 9 \equiv 10 \bmod 77$$

leading to:

$$x + 31 \times 9 \equiv 31 \times 10 \bmod 15,$$

that is:

$$x \equiv 31(10 - 9) \bmod 15,$$

which finally yields:

$$x \equiv 1 \bmod 15.$$

2. We apply the Chinese Remainder Theorem (as stated in Assignment 2). We have $m = 7$, $n = 11$, $a = 2$, $b = 3$.

   We need s and t such that $s\, m + t\, n = 1$, hence we can choose $s = -3$ and $t = 2$. Then, we have

$$c \equiv a + (b - a)\, s\, m \equiv 2 + (3 - 2) \times (-3) \times 7 \equiv -19 \bmod 15.$$

3. We eliminate y in order to solve for x first.
   x + y = 33 mod 77
   x − y = 10 mod 77.
   adding the two side by side get:
   2x = 43 mod 77
   the inverse of 2 mod 77 is 39
   2x ≡ 43 mod 77
   multiplying both side by its inverse:
   x ≡ 60 mod 77
   Substituting x with 60 into x + y = 33 mod 77 yields
   y ≡ 27 mod 77

Problem 4 (RSA) *[20 marks]* Let us consider an RSA Public Key Crypto System. Alice selects 2 prime numbers: $p = 5$ and $q = 11$. Alice selects her public exponent $e = 3$ and sends it to Bob. Bob wants to send the message $M = 4$ to Alice.

1. Compute the product $n = p\,q$ and $\Phi(n)$
2. Is this choice for of e valid here?
3. Compute d , the private exponent of Alice.
4. Encrypt the plain-text M using Alice public exponent. What is the resulting cipher-text C?
5. Verify that Alice can obtain M from C, using her private decryption exponent.

Solution 4

1. n = pq = 5 * 11 = 55
   Φ(55) = 40

2. Exponent e is relatively prime to (p-1)(q-1)
   therefore gcd(e,(p-1)(q-1)) must equal 1
   gcd(e,4*10) = gcd(3,40) = 1
   therefore this choice of e is valid here.

3. This must be satisfied:
   ed ≡ 1(mod (p-1)(q-1))
   Substituting:
   3d ≡ 1 (mod 40)
   the inverse of 3 is 27
   d ≡ 27 mod 40

4. C must satisfied:
   C = m^e (mod N)
   C = 4^3(mod 55) = 9

5. m' = c^d mod N
   = 9^27 mod 55
   = 4
   = M