UWO CS2214 Feb. 25, 2019

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) $F_4(x, y) = (y + x, y - x)$

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

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

$$(\forall x \in \mathbb{Z}) \qquad \left\{ \begin{array}{ll} x \equiv a & \bmod\ m \\ x \equiv b & \bmod\ n \end{array} \right. \qquad \Longleftrightarrow \qquad x \equiv c \quad \bmod\ m\,n \tag{3}$$

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 $x \equiv c \mod m\,n$.

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.

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.