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

Format of the submission. You must submit a **single** file which must be in **PDF** format. All other formats (text or Miscrosoft word format) will be **ignored** and considered as **null**. You are strongly encouraged to type your solutions using a text editor. To this end, we suggest the following options:

1. Miscrosoft word and convert your document to PDF
2. the typesetting system LaTeX; see `https://www.latex-project.org/` and `https://en.wikipedia.org/wiki/LaTeX#Example` to learn about LaTeX; see `https://www.tug.org/begin.html` to get started
3. using a software tool for typing mathematical symbols, for instance `http://math.typeit.org/`
4. using a Handwriting recognition system such as those equipping tablet PCs

Hand-writing and scanning your answers is allowed but not encouraged:

1. if you go this route please use a scanning printer and **do not take a picture of your answers with your phone**,
2. if the quality of the obtained PDF is too poor, your submission will be **ignored** and considered as **null**.

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? surjective? Justify your answer.

Solution 1

1. $A = \begin{pmatrix} 0 & 2 \\ 3 & 0 \end{pmatrix}$. If $(2y_1, 3x_1) = (2y_2, 3x_2)$ holds then we have $(x_1, y_1) = (x_2, y_2)$, hence F_1 is injective. F_1 is also surjective since we have $F_1^{-1}(x', y') = (\frac{y'}{3}, \frac{x'}{2})$.
2. $A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Since F_2 maps every point (x, y) to $(0, 0)$, it is clear that F_2 is neither injective, nor surjective.
3. $A = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$. Since every point of the form $(x, 0)$ is mapped to $(0, 0)$, it is clear that F_3 is not injective. Since $(1, 2)$ cannot have a pre-image by F_3, it is clear that F_3 is not surjective either.
4.
5. $A = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$. If $(y_1 + x_1, y_1 - x_1) = (y_2 + x_2, y_2 - x_2)$ holds, we have

$$y_1 + x_1 = y_2 + x_2 \quad \text{and} \quad y_1 - x_1 = y_2 - x_2.$$

Adding these two equations side by side yields $2y_1 = 2y_2$ and thus $y_1 = y_2$. Subtracting them side by side yields $2x_1 = 2x_2$ and thus $x_1 = x_2$. Therefore, we have proved that $F_4(x_1, y_1) = F_4(x_2, y_2)$ implies $(x_1, y_1) = (x_2, y_2)$, hence F_4 is injective. F_4 is also surjective since we have $F_1^{-1}(x', y') = (\frac{x'-y'}{2}, \frac{x'+y'}{2})$.

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

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

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. Observe that Relation (4) implies

$$c \equiv a \mod m \qquad \text{and} \qquad c \equiv b \mod n. \tag{5}$$

2. Assume that $x \equiv c \mod m\,n$ holds. This implies

$$x \equiv c \mod m \qquad \text{and} \qquad x \equiv c \mod n \tag{6}$$

   Thus Relations (5) and (6) lead to

$$x \equiv a \mod m \qquad \text{and} \qquad x \equiv b \mod n \tag{7}$$

3. Conversely
   - $x \equiv a \mod m$ implies $x \equiv c \mod m$ that is m divides $x - c$ and
   - $x \equiv b \mod n$ implies $x \equiv c \mod n$ that is n divides $x - c$.

   Since m and n are relatively prime it follows that $m\,n$ divides $x - c$.

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. $x = 31 \mod 77$.
2. $x = 58 \mod 77$.
3. $x = 60 \mod 77$ and $y = 50 \mod 77$.

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. We have $n = pq = 55$ and $\Psi(n) = (p-1)(q-1) = 4 \times 10 = 40$.
2. We have $\gcd(3, 40) = 1$, hence $e = 3$ is a valid choice (note that 3 is a prime number, any way).
3. Alice private exponent d satisfies $de = 1 \mod \Psi(n)$, hence $3d = 1 \mod 40$, which gives $d = 27$ since $3 \times 27 = 81 = 1 + 2 \times 40$.
4. Bob send: $C = M^e \mod n = 4^3 \mod 55 = 64 \mod 55 = 9$.
5. Alice receives C and computes $C^d \mod n = 9^{27} \mod 55 = 4$.