Birla Institute of Technology and Science, Pilani (Pilani Campus)
First Semester 2022-23

Course Number: MATH F441 (Discrete Mathematical Structures) Examination: Mid-Semester Test
Date of Examination: 31.10.2022 (Monday) Mode: Closed Book
Maximum Duration: 90 min (2:00-3:30 pm) Maximum Marks: 30

Instructions.

1. Calculators are allowed.
2. For a prime p, the symbols $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{F}_p$ are used interchangeably.
3. If two or more solutions are written for the same question, only the first one will be graded.
4. Answer each question legibly, clearly and concisely. Illegible answers will not be graded.
5. You will be graded on the correctness of your solution as well as the quality of your explanation. Writing the final answer without any justification will lead to no credit.
6. All the results discussed in class should be stated clearly wherever used.

Q1. Describe the symmetries of a non-square rectangle. Construct the 'multiplication' table. **[4]**

Q2. Let p be an odd prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Prove Euler's criterion, i.e.,

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

[5]

Q3. Find the sum of all positive integers < 105 which are coprime to 105. Justify your answer. **[4]**

Q4. Using Chinese Remainder Theorem, determine $f(x) \in \mathbb{F}_2[x]$ such that $\deg(f) < 6$ and

$$f(x) \equiv x^2 + x + 1 \pmod{x^3 + x + 1},$$
$$f(x) \equiv x + 1 \pmod{x^3 + x^2 + 1}.$$

[5]

Q5. Apply the Fast Fourier Transform method to find the product of the polynomials $f(x) = x + 2i$ and $g(x) = (1+i)x - 3$, where i denotes the complex number with $i^2 = -1$. Justify all the steps. **[4]**

Q6. Given the RSA encoding parameters $(n, e) = (133, 25)$, find the private key d and decrypt the message $c = 70$. **[3]**

Q7. Decode the message SKMD encrypted using the encryption matrix

$$\begin{pmatrix} 1 & 2 \\ 5 - 9t & 15 - 18t \end{pmatrix}$$

such that $t = n$ if the nth tuple is being coded. The above matrix is viewed as a matrix over $\mathbb{Z}/26\mathbb{Z}$ and the letters are converted to numbers as:

$$\begin{array}{c} A\ B\ C\ \ldots\ Y\ Z \\ 1\ 2\ 3\ \ldots\ 25\ 26 \end{array}$$

[5]

ALL THE BEST