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

Course Number: MATH F231 (Number Theory) — Examination: End-Semester Test
Date of Examination: 12.05.2023
Maximum Duration: 180 min — Maximum Marks: 90

General Instructions.

1. There are two parts of 45 marks each: Part A is Closed Book; Part B is Open Book.
Part A must be completed latest by 11:00 AM. You may get the question paper for Part B immediately if you submit Part A before 11:00 AM.
2. Calculators are allowed.
3. Symbols have their usual meaning unless stated otherwise.
4. If multiple answers are written for the same question, only the first one will be graded.
5. Justify all answers. You will be graded on the correctness of your solution as well as the quality of your explanation.

Part A

Q1. Let p be a prime and let $a, b \in \mathbb{Z}$ with $\gcd(a, p) = \gcd(b, p) = 1$. Suppose $a^p \equiv b^p \pmod{p}$. Prove that $a \equiv b \pmod{p}$. Hence prove that $a^p \equiv b^p \pmod{p^2}$. **[5]**

Q2. Let p be a prime. For $m \in \mathbb{N}$, let $\mu(p, m)$ denote the value of the Möbius function μ at $\gcd(p, m)$. Prove that

$$\sum_{d|n} \mu(d)\mu(p, d) = \begin{cases} 1 & \text{if } n = 1, \\ 2 & \text{if } n = p^k \text{ for some } k \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$ **[10]**

Q3.

(i) Let $n \geq 2$. Prove that the sum of the positive integers less than n and coprime to n is $\frac{1}{2}n\varphi(n)$. **[4]**

(ii) Let p be a prime. Prove that the product of the $\varphi(p-1)$ primitive roots modulo p is congruent to $(-1)^{\varphi(p-1)}$ modulo p. **[5]**

Q4. Compute $\left(\frac{773}{343}\right)$. **[5]**

Q5. Let a and b be coprime odd positive integers. Suppose $\epsilon, \eta \in \{-1, 1\}$. Prove that

$$\left(\frac{\epsilon a}{b}\right)\left(\frac{\eta b}{a}\right) = (-1)^t,$$

where

$$t = \left(\frac{\epsilon a - 1}{2} \times \frac{\eta b - 1}{2}\right) + \left(\frac{\epsilon - 1}{2} \times \frac{\eta - 1}{2}\right).$$ **[10]**

Q6. Express $\frac{118}{101}$ as a finite simple continued fraction. Hence find a particular solution of the linear Diophantine equation

$$118X - 101Y = -11.$$ **[6]**

ALL THE BEST

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

Course Number: MATH F231 (Number Theory) Examination: End-Semester Test
Date of Examination: 12.05.2023
Maximum Duration: 180 min Maximum Marks: 90

General Instructions.

1. There are two parts of 45 marks each: Part A is Closed Book; Part B is Open Book.
Part A must be completed latest by 11:00 AM. You may get the question paper for Part B immediately if you submit Part A before 11:00 AM.
2. Calculators are allowed.
3. Symbols have their usual meaning unless stated otherwise.
4. If multiple answers are written for the same question, only the first one will be graded.
5. Justify all answers. You will be graded on the correctness of your solution as well as the quality of your explanation.

Part B

Q1. Suppose a is a positive real number such that $a + \frac{1}{a} \in \mathbb{Z}$. Use the Well Ordering Principle to prove that $a^n + \frac{1}{a^n} \in \mathbb{Z}$ for all positive integers n. Do not use PMI/PSI directly. **[8]**

Q2. Let $m \in \mathbb{N}$ and let a be an integer coprime to m. Prove that there exist integers x and y with $1 \leq x, y \leq \sqrt{m}$ such that either $ax - y$ or $ax + y$ is divisible by m.
(Hint: Pigeonhole Principle) **[10]**

Q3. Solve the Diophantine equation
$$X^2 - 16 = Y^3.$$
[13]

Q4. Using the method in the proof of the Chinese Remainder Theorem, find the least positive integer x satisfying the following system of congruences.
$$x \equiv -1 \pmod{125},$$
$$x \equiv -2 \pmod{343}.$$
[7]

Q5. Let $m, n \in \mathbb{N}$ with $m - n \geq 1$ and n odd. Prove that
$$F_{m+n} + F_{m-n} = F_n L_m.$$
Hence prove that $F_{4n} + 1$ is composite for all positive integers n. **[7]**

ALL THE BEST