Indian Institute of Technology Dharwad

Introduction to Number Theory (MA-403)

Final Exam. Date: 18 November, 2022

Timing: **10:00am to 1:00 PM**
Instructors : N.S.N Sastry and Amlan Barua

Autumn 2022-23
Max mark: **100**

Answer all questions. Your answers and proofs should be <u>clear</u> and <u>complete</u>. Incomplete answers will be ignored. Write your Registration number <u>clearly</u>.

1. (a) Find the gcd $d = (a, b)$ if $a = 225$ and $b = 157$. Find integers m and n such that $d = ma + nb$ (8+7)

2. (a) Show that, for $a, n \in \mathbb{Z}^{>1}$, if $a^n - 1$ is a prime, then $a = 2$ and n is a prime. (6)

3. (a) If p is an odd prime, show that $p^2 \equiv 1 \pmod{24}$ (7)
   (b) Find <u>all</u> integers such that $n \equiv 3 \pmod 5$, $n \equiv 1 \pmod 4$, $n \equiv 2 \pmod 3$. (7)

4. (a) Write the binary expansions of 164. (7)
   (b) Use (a) to find $a \in \mathbb{Z}$ such that $0 \le a < 51$ and $3^{164} \equiv a \pmod{51}$. (8)

5. For $n \in \mathbb{N}$, let $Z_n^* = \{a \in \mathbb{N} : 1 \le a \le n, (a, n) = 1\}$
   (a) When is $x \in Z_n^*$ called a primitive root $\pmod n$. (4)
   (b) Find all primitive roots $\pmod n$ for $n = 14$. (6)
   (c) For $3 \in Z_{14}^*$, find $d \in Z_{14}^*$ such that $3d \equiv 1 \pmod{14}$. (5)

6. (a) When is $a \in Z_n^*$ called a quadratic residue $\pmod n$. (4)
   (b) Is 38 a quadratic residue $\pmod{43}$? (6)
   (c) Calculate the following :
      (i) The Euler's ϕ-function $\phi(720)$.
      (ii) Möbius function $\mu(2022)$.

(iii) The Legendre symbol $\left(\frac{36}{109}\right)$.

(4+4+7)

7. (a) Give an example of a polynomial in X of degree 3 with coefficients in $\mathbb{F}_3$ and irreducible over $\mathbb{F}_3$. Prove that it is irreducible over $\mathbb{F}_3$. **(10)**