Midsemestral

Number Theory

Instructor: Ramdin Mawia Marks: **30** Course: M1 **Time:** February 23, 2024; 10:00–13:00.

Attempt any FIVE problems. Each question carries 6 marks.

1. i. Let $n > 2$ be a positive integer such that $\varphi(n) | n - 1$. Prove that n is squarefree. **2**

   ii. Let p be an odd prime. Prove that **4**

$$1^n + 2^n + \cdots + (p-1)^n \equiv \begin{cases} 0 \pmod{p} & \text{if } p-1 \nmid n, \\ -1 \pmod{p} & \text{if } p-1 | n. \end{cases}$$

2. Let $p = m + n + 3$ be a prime with $m, n \in \mathbb{N}$. Prove that **6**

$$(m! + (m+1)!)\,(n! + (n+1)!) \equiv (-1)^m \pmod{p}.$$

3. State whether the following statements are true or false, with brief but complete justifications: **6**

   i. The equation $3X^2 + 5Y^2 = 7Z^2$ has no nontrivial solutions in integers.

   ii. For every positive integer n, 3 is a primitive root for 7^n.

4. Describe all primes p for which 7 is a quadratic nonresidue. **6**

5. Let p be an odd prime and q be a prime such that $p \equiv 1 \pmod{q}$. Let ν be the highest power of q dividing $p-1$; i.e., $q^\nu | p-1$ but $q^{\nu+1} \nmid p-1$. Write $R_j = \{x^{q^j} : x \in \mathbb{Z}/p\mathbb{Z}\} \subset \mathbb{Z}/p\mathbb{Z}$. Show that for all $j \geqslant \nu$, we have $R_j = R_\nu$. That is, the polynomials $X^{q^j} \in \mathbb{Z}/p\mathbb{Z}[X]$ take the same set of values for $j \geqslant \nu$. **6**

6. State and prove the Möbius inversion formula. Use it to show that the following two formulas are equivalent:[5] **6**

   - $\tau(mn) = \sum_{d|(m,n)} \mu(d)\tau(m/d)\tau(n/d)$ for all positive integers m and n.
   - $\tau(m)\tau(n) = \sum_{d|(m,n)} \tau(mn/d^2)$ for all positive integers m and n.

   Here, τ is the usual divisor-counting function, and (m, n) denotes the gcd of m and n.

7. Are there nonzero integers x, y, z such that **6**

$$3x^2 + 13y^2 = z^2?$$

   If yes, find all of them. If not, justify.

8. Show that, for $x \geqslant 2$ we have **6**

$$\sum_{p \leqslant x} \frac{\log^2 p}{p} = \frac{1}{2}\log^2 x + O(\log x).$$

9. Prove that **6**

$$\left| \sum_{n \leqslant x} \frac{\mu(n)}{n} \right| < 1.$$

   for all $x \geqslant 2$, where μ is the Möbius function. [*Hint.* Look at $\sum_{n \leqslant x} \mu(n) \left[\frac{x}{n}\right]$ first.]

[5] You are ***not*** asked to prove that the two formulas are correct (which they are)! "Equivalent" means one is true if and only if the other is true.