Semestral

Number Theory

Instructor: Ramdin Mawia Marks: **50** Course: M1 **Time:** May 04, 2026; 14:00–17:00.

Part 1

Attempt any TWO problems. Each question carries 12 marks.

1. Prove or disprove (**any two**): **6+6=12**

   i. Let $\varphi(n)$ denote the usual Euler function. Then

   $$\liminf_{n\to\infty} \frac{\varphi(n)}{n} = 0.$$

   ii. Let p be an odd prime and $n \in \mathbb{Z}^+$ be a quadratic nonresidue mod p. Then

   $$\sum_{d|n} d^{(p-1)/2} \equiv 0 \pmod{p}.$$

   iii. Let p be an odd prime and a, b be integers with $p \nmid ab$. Then there is some integer c such that the congruence

   $$aX^2 + bY^2 \equiv c \pmod{p}$$

   does not have a solution.

2. Prove that there are infinitely many primes of the form $8k - 1$. [*Hint.* Let $p_1, ..., p_n$ be primes of the said form. Look at $(p_1 \cdots p_n)^2 - 2$.] **12**

3. Are there positive integers x and y such that $(x^2 + 6)/(3y^2 + 13)$ is also an integer? Give two examples, if any. [You need not give a complete description.] **12**

Please turn over for Part 2

Part 2

Attempt any TWO problems. Each question carries 13 marks.

4. Consider the quadratic field $K = \mathbb{Q}[\sqrt{-3}]$. **13**

   i. Determine the ring of integers $\mathcal{O}_K$ in K.

   ii. Prove that $\mathcal{O}_K$ is a norm-Euclidean domain.

   iii. Show that a prime $\pi \in \mathcal{O}_K$ divides exactly one rational prime $p \in \mathbb{Z}^+$.

   iv. Using this or otherwise, prove that any prime $p \equiv 1 \pmod 6$ can be written in the form $p = a^2 + ab + b^2$ for some integers a and b.

---

5. Let $q > 1$ be an integer and χ be a Dirichlet character mod q, i.e., $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$ is a group homomorphism. Write $G = (\mathbb{Z}/q\mathbb{Z})^\times$. For any integer a, define the *Gauss sum* $\tau_a(\chi) := \sum_{b \in G} \chi(b) e^{2\pi i a b/q}$. Prove the following: **13**

   i. $\tau_a(\chi) = 0$ if $a \equiv 0 \pmod q$ and χ is a nontrivial character, i.e., $\chi(G) \neq \{1\}$.

   ii. $\tau_a(\chi) = \chi(a^{-1})\tau_1(\chi)$ if $\gcd(a, q) = 1$. Here a^{-1} denotes the inverse of a mod q.

   iii. If q is an odd prime and χ is a nontrivial character modulo q, then $|\tau_1(\chi)| = \sqrt{q}$. [*Hint.* Evaluate $\sum_{a=1}^{q} \tau_a(\chi)\overline{\tau_a(\chi)}$ in two ways!]

---

6. Let $\vartheta(x) = \sum_{p \leq x} \log p$, where the sum runs through the primes $p \leq x$. Prove that **13**

$$\sum_{n \leq x} \frac{\vartheta(n)}{n^2} = \log x + O(1).$$

OR

6′. Let $\ell(n) = \mathbb{1}_{\mathbb{P}}(n) \log n$ where $\mathbb{1}_{\mathbb{P}}$ denotes the characteristic function of the primes. Find an asymptotic formula for the sum **13**

$$\sum_{n \leq x} \frac{\ell * \ell(n)}{n}.$$

---

7. Let $\pi_{\text{sq}}(X)$ denote the number of primes $p \leq X$ which can be written in the form $p = n^2 + 1$ for some integer n. Using the Sieve of Eratosthenes-Legendre or otherwise, prove that **13**

$$\pi_{\text{sq}}(X) \ll \frac{X}{\log \log X}$$

as $X \to \infty$. [*Hint.* You may use, without proof, $\sum_{p < z, p \equiv 1 \pmod 4} = \frac{1}{2} \log \log z + O(1)$.]

The End