Midsemestral

Number Theory

Instructor: Ramdin Mawia | Marks: **30** | Course: M1 | **Time:** February 27, 2026; 14:00–17:00.

Attempt any FOUR problems. Each question carries 8 marks.

1. Prove or disprove (**any two**): **4+4=8**

   i. There are infinitely many positive integers n for which the congruence

   $$(x^2-3)(x^2-5)(x^2-15) \equiv 0 \pmod{n}$$

   is not solvable.

   ii. For all positive integers a and n, the congruence $a^n \equiv a^{n-\varphi(n)} \pmod{n}$ holds.

   iii. There is an integer x such that $7x^2 + 2x + 1 \equiv 0 \pmod{127}$.

   iv. The integral domain $\mathbb{Z}[\sqrt{-14}]$ is a UFD.

2. Prove that there are infinitely many primes of the form $6k+1$. [*Hint.* Let $p_1, \ldots, p_n$ be primes of the said form. Apply the QRL to a prime factor of $4(p_1 \cdots p_n)^2 + 3$.] **8**

3. Are there integers x and y such that $(x^2-11)/(11y^2-3)$ is also an integer? **8**

4. Consider the quadratic field $K = \mathbb{Q}[\sqrt{-7}]$. **8**

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

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

   iii. Using this or otherwise, find all solutions of the Diophantine equation

   $$X^3 = Y^2 + Y + 2$$

   in rational integers.

5. Describe all solutions to the Diophantine equation **8**

   $$4X^2 + 9Y^2 = 36Z^2$$

   in rational integers.

6. Let A be an integral domain with field of fractions K, and let L/K be an algebraic extension. Suppose A is integrally closed in K. Prove that an element $\alpha \in L$ is integral over A if and only if its minimal polynomial over K has all its coefficients in A. **8**