4/9 Spring 2025, Number Theory II, Test II Sitaraman

Howard University Math Department

EACH 20 POINTS

1. True or False ? Prove if true and provide counterexample or disprove if false.
   (a) In a finite field $\mathbb{F}_p$ of order p a prime, the multiplicative group $\mathbb{F}_p^*$ has a unique subgroup of every order.
   (b) The fundamental solution of Pell's equation $x^2 - Dy^2 = 1$, with $D > 0$ square free integer, is always the fundamental unit of the ring of algebraic integers of $\mathbb{Q}[\sqrt{D}]$.
2. Give five examples of each.
   (a) Algebraic integers in $\mathbb{Q}[\sqrt{3}]$ outside of $\mathbb{Z}$.
   (b) Solutions of $x^2 - 3y^2 = 1$.
3. Prove that for any positive integer n, $\phi(n) = \sum_{d|n} \mu(d) \times \frac{n}{d}$.

   Recall that $\mu(1) = 1$ and if k is a product of distinct primes $p_1 p_2 ... p_m$ then $\mu(k) = (-1)^m$. Otherwise $\mu(k) = 0$.
4. Prove that the square triangular numbers are in 1-1 correspondence with the solutions of $x^2 - 2y^2 = 1$.
5. Using Gaussian integers, prove that if p, q are distinct primes of the form $4k + 1$, then pq can be written as sum of squares in exactly two ways. You may assume that primes of this form are sums of squares. You must explain what role the unique factorization property of Gaussian integers plays in the proof.