Indian Statistical Institute
M. Math II year
Number Theory
September 15, 2018

Mid Sem exam Time : 3 hours 40 points

1. Prove that:

   (a). [3 points] For positive integers m and n, the g.c.d of $2^m - 1$ and $2^n - 1$ is $2^{(m,n)} - 1$, where (m, n) is the g.c.d of m and n.

   (b). [2 points] If $2^n + 1$ is an odd prime, then n is a power of 2.

2. [5 points] Given any positive integer k, prove that there are k consecutive integers each divisible by a square > 1. (Hint: Use Chinese remainder theorem.)

3. [4+1 points] Let $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$. Prove that $\mathbb{Z}[i]$ is a Euclidean domain. Find the units in $\mathbb{Z}[i]$.

4. [5 points] Prove that if p is a prime, then there exists $(p-1)\phi(p-1)$ primitive roots modulo p^2.

5. [5 points] Use quadratic reciprocity law to find the primes $p > 2$, such that the congruence

$$x^2 + x + 1 \equiv 0 \pmod{p}$$

   have solutions.

6. Let $p \equiv 1 \pmod{4}$.

   (a). [2 points] Show that a is a quadratic residue *modulo* m iff $p - a$ is a quadratic residue *modulo* m.

   (b). [2 points] Find the sum of all quadratic residues of p.

   (c). [3 points] Show that $\displaystyle\sum_{a=1}^{p-1} a \left(\frac{a}{p}\right) = 0$.

7. Let $p = 2^{2^n} + 1$ be prime. Show that

   (a). [3 points] Every quadratic non-residue *modulo* p is a primitive root *modulo* p.

   (b). [2 points] 3 is a primitive root *modulo* $p > 3$.

8. [3 points] Let $p = a^2 + 4b^2$ be prime. Show that $\left(\frac{a}{p}\right) = 1$.