B. MATH (HONS.) IST YEAR
MID-SEMESTER EXAM
ELEMENTARY NUMBER THEORY
13TH OCTOBER, 2022
TOTAL MARKS - 30

Instruction to students. Please present your solutions as clearly as possible. Any theorem/result that you use directly should be clearly stated/mentioned.

(1) (i) Consider the equivalence relation ρ on $\mathbb{Z}$ given by $a\rho b$ iff 5 divides $a^2 - b^2$. Find the corresponding partition of $\mathbb{Z}$. (3)
(ii) Find all the equivalence relations on $S = \{1, 2, 3\}$. (3)

(2) If p is a prime and $n \in \mathbb{Z}$ such that p divides $(4n^2 + 1)$, then show that $p \equiv 1 \pmod 4$. Hence prove that there are infinitely many primes of the form $(4k + 1)$. $(3 + 3)$

(3) (i) If H is a subgroup of a group G, show that for any $g \in G$, $K = gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ is a subgroup of G. (2)
(ii) If H is the only subgroup of order n in a group G, then prove that $gHg^{-1} = H$. (3)

(4) (i) For $m \geqslant 2$, let $T_m = \{x^2 (\text{mod} m)\}$ be the set of squares modulo m. If $\gcd(m, n) = 1$, show that $|T_{mn}| = |T_m||T_n|$. (6)
Hint : Consider the natural map $T_{mn} \longrightarrow T_m \times T_n$. Use the Chinese Remainder Theorem.
(ii) If p is an odd prime, then show that the number of non-zero squares in $\mathcal{U}_p$ is $\dfrac{p-1}{2}$ ($\mathcal{U}_p = \{[a] \in \mathbb{Z}_p \mid \gcd(a, p) = 1\}$). (3)
Hint : $\mathcal{U}_p$ is cyclic.

OR

(5) (i) Show that for any positive integer N, there exists a multiple of N that consists of only 0's and 1's. (3)
Hint : Use the Pigeonhole Principle.
(ii) For all positive integers n, let $a_n = 2^{2^n} + 1$. Show that $\gcd(a_m, a_n) = 1 \ \forall\ m \neq n$. (3)
(iii) Show that if $a,\ b \in \mathbb{N}$ with $\gcd(a, b) = 1$, then show that there exist $m,\ n \in \mathbb{Z}$ such that $a^m + b^n \equiv 1 (\text{mod } ab)$. (3)
Hint : Use Euler's Theorem.

(6) Using the identity $2^{2.3^{n-1}} \equiv 1 + 3^n \pmod{3^{n+1}}$ (no proof needed) or otherwise, show that 2 is a primitive root of $3^n\ \forall\ n \geqslant 1$. (4)