# THE AMERICAN COLLEGE, MADURAI

(An Autonomous Institution Affiliated to Madurai Kamaraj University)
Re-accredited (2nd Cycle) by NAAC with Grade "A", CGPA – 3.46 on a 4-point scale

## Backlog Arrear Examination, March 2021

**PGM 4437** **TIME:3HRS**
**NUMBER THEORY** **MARK:75**

---

Answer Any **FIVE** Questions 5x15=75

1. State and prove Euclidean algorithm and hence find the $gcd\ g$ of 2689 and 4001. Also find the integers $x$ and $y$ such that $g = 2689x + 4001y$.

2. (i) State and prove Wilson's theorem.
   (ii) Let $p$ denote a prime. Then prove that $x^2 \equiv -1(mod\ p)$ has solutions if and only if $p = 2$ or $p \equiv 1(mod\ 4)$.

3. (i) State and prove Chinese Remainder Theorem.
   (ii) Find the least positive integer $x$ such that $x \equiv 5(mod\ 7)$, $x \equiv 7(mod\ 11)$, and $x \equiv 3(mod\ 13)$.

4. **(i)** Let $f(x)$ $be$ a fixed polynomial with integral coefficients, and for any positive integer $m$ let $N(m)$ denote the number of solutions of the congruence $f(x) \equiv 0\ (mod\ m)$. Prove that if $m = m_1 m_2$ where $(m_1, m_2) = 1$, then $N(m) = N(m_1)N(m_2)$.
   **(ii)** Find all roots of $f(x) \equiv 0\ (mod\ 189)$, given that $189 = 3^3.7$, that the roots (mod 27) are 4, 13, and 22, and that the roots (mod 7) are 0 and 6.

5. Let $p$ be an odd prime. Then prove the following:
   (i) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2}(mod\ p)$
   (ii) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
   (iii) $a \equiv b(mod\ p)$ implies that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
   (iv) If $(a, p) = 1$ then $\left(\frac{a^2}{p}\right) = 1, \left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$.

6. **(i)** Prove that if $p, q$ are distinct odd primes, then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\{(p-1)/2\}\{(q-1)/2\}}$
   **(ii)** Is the congruence $x^2 \equiv -42\ (mod\ 61)$ solvable?

7. If $f(n) = \sum_{d|n} \mu(d)\, F(n/d)$ for every positive integer $n$, then prove that $F(n) = \sum_{d|n} f(d)$.