Birla Institute of Technology & Science, Pilani
Second Semester, 2017-18
Comprehensive Examination (Closed Book)

Course Name: MATH F231 (Number Theory) **Date: May 5, 2018 (Saturday)**
Max. Time: 180 Minutes **Max. Marks: 45**

Note:1. Answer all sub-parts together.
2. Start new question from fresh page.
3. Symbols have their usual meaning.
4. Please write END at the end of the answer script.

Q1. State and prove the Euler's theorem. **[4]**

Q2. Prove that ϕ is a multiplicative function. **[6]**

Q3. Prove or disprove:
(a) The sum of two primitive roots modulo an odd prime p is a primitive root of p.
(b) If $p \equiv 3\ (mod\ 8)$ is an odd prime and a is a quadratic non residue of p then $2a$ is a quadratic residue of p.
(c) 17 is a quadratic residue of 33.
(d) For an odd positive integer a, $a^{2^n} \equiv 1 \pmod{2^{n+2}}$, for $n \geq 1$.
(e) The only solution of $\phi(mn) = \phi(m) + \phi(n)$, $m, n \in \mathbb{N}$ are $(2,2), (3,4)$ and $(4,3)$.
(f) The linear system $x \equiv 3 \pmod 4$, $x \equiv 4 \pmod 5$, $x \equiv 4 \pmod 6$ has unique solution modulo 60. **[3x6=18]**

Q4. State and prove the Euler's criterion for a least positive residue modulo an odd prime p to be a quadratic residue of p. Hence, conclude whether a primitive root modulo an odd prime p can be a quadratic residue of p or not ? **[6]**

Q5. State and prove the Gauss' lemma and use it to check whether 6 is a quadratic residue of 19 or not ? **[6]**

Q6. Prove that a positive real number is rational iff it can be written as a finite simple continued fraction. **[5]**

*******END*******