B.A./B.Sc. 5th Semester (Honours) Examination, 2019 (CBCS)

Subject : Mathematics

Paper : BMH5DSE12

(Number Theory)

Time: 3 Hours **Full Marks: 60**

The figures in the margin indicate full marks.

Candidates are required to give their answers in their own words as far as practicable.

Notation and symbols have their usual meaning.

1. Answer *any ten* questions from the following: 2×10=20

(a) Show that 41 divides $2^{20} - 1$.

(b) Show that if $(P-1)! + 1 \equiv 0 \pmod{p}$, then P must be prime.

(c) Find the number of odd positive divisors of 2700.

(d) If p be prime and k be a positive integer, then show that $\phi\left(p^k\right) = p^k\left(1 - \frac{1}{p}\right)$.

(e) If $n > 2$, then show that $\phi(n)$ is an even integer.

(f) Find the highest power of 5 dividing 50!.

(g) In RSA modulus $N \equiv 15$ and encryption exponent $e = 3$, find decryption exponent d.

(h) Show that if $F_n = 2^{2^n} + 1, n > 1, n$ is prime, then 2 is not a primitiv root of F_n.

(i) Let a be an odd integer. Then show that $x^2 \equiv a \pmod{4}$ has a solution if and only if $a \equiv 1 \pmod{4}$.

(j) Give an example to show that $a^2 \equiv b^2 \pmod{n}$ need not imply that $a \equiv b \pmod{n}$.

(k) Find the least positive residues in $3^{36} \pmod{77}$.

(l) Prove that $19^{20} \equiv 1 \pmod{181}$

(m) Find the unit digit of 3^{100} by the use of Fermat's theorem.

(n) Find the remainder when 2 (2 6 !) is divided by 29.

(o) Find φ (5040), where φ is Euler's phi function.

2. Answer *any four* questions from the following: 5×4=20

(a) Find the general solution in integers of the equation $5x + 12y = 80$. Examine if there is a solution in positive integers. 4+1=5

(b) Solve the system of linear congruences $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{7}$. 5

(c) State and prove Möbius inversion formula. 5

(d) If p is a prime number and $d|p-1$, then show that the congruence $x^d - 1 \equiv 0 \pmod{p}$ has exactly d number of solutions. 5

(e) (i) Show that there are primitive roots for $2p^k$, where p is an odd prime and $k \geq 1$.

(ii) Determine all the primitive roots of 3^4. 3+2=5

(f) (i) What do you mean by the Legendre symbol? Explain with an example.

(ii) Let p be an odd prime and let a, b be two integers that are relatively prime to p. Then show that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. 2+3=5

3. Answer *any two* questions from the following: 10×2=20

(a) Prove that the system of linear congruence's $ax + by \equiv r \pmod{n}$, $cx + dy \equiv s \pmod{n}$ has a unique solution modulo n whenever $gcd(ad - bc, n) = 1$. Hence solve the system $7x + 3y \equiv 10 \pmod{16}$, $2x + 5y \equiv 9 \pmod{16}$. 5+5=10

(b) (i) Find the solution $x^2 \equiv 196 \pmod{1357}$.

(ii) Prove that, for $k \geq 3$, the integer 2^k has no primitive roots. 5+5=10

(c) (i) State and prove Chinese Remainder theorem.

(ii) Determine all solutions of the Diophantine equation $24x + 138y = 18$. 5+5=10

(d) (i) For any integer $n \geq 1$, show that $\tau(n) \leq 2\sqrt{n}$.

(ii) Show that $\exists$ no integers n for which $\varphi(n) = \frac{n}{4}$.

(iii) Show that if $gcd(a, n) = gcd(a-1, n) = 1$, then $1 + a + a^2 + \cdots + a^{\varphi(n)-1} \equiv 0 \pmod{n}$. 4+3+3=10

———