20P105 (Pages: 2) Name: …….

Reg. No……...

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, NOVEMBER 2020

(CBCSS-PG)

(Regular/Supplementary/Improvement)

CC19 MTH1 C05 – NUMBER THEORY

(Mathematics)

(2019 Admission onwards)

Time: Three Hours Maximum: 30 Weightage

Part A

Answer ***all*** questions. Each question carries 1 weightage.

1. Prove that, for $n \geq 1$, $\Lambda(n)\log n + \sum_{\frac{d}{n}} \Lambda(d)\Lambda\left(\frac{n}{d}\right) = \sum_{\frac{d}{n}} \mu(d) log^2\left(\frac{n}{d}\right)$
2. For every,n ≥ 1 prove that $\sum_{\frac{d}{n}} \lambda(d) = \begin{cases} 1 & if\ n\ is\ a\ square \\ 0 & otherwise \end{cases}$
3. (a) State and prove Legender's Identity.

   (b) Find the highest power of 2 which is contained in (100)!
4. State Shapiro's Tauberian theorem.
5. Show that the asymptotic relation $\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$ implies $\lim_{x\to\infty} \frac{\pi(x)\log \pi(x)}{x} = 1$.
6. Evaluate (−1/p) as Lengendre's symbol.
7. Determine whether 888 is a quadratic residue or non-residue mod 1999.
8. Describe how a signature is sent in RSA.

(8 × 1 = 8 Weightage)

Part B

Answer any ***two*** questions from each unit. Each question carries 2 weightage.

Unit - I

9. (a) If f and g are multiplicative, so is their Dirchlet product f ∗g.

   (b) If both g and f ∗g are multiplicative, then f is also multiplicative.
10. Assume f is multiplicative. Prove that $f^{-1}(n) = \mu(n)f(n)$ for every square free n.
11. State and prove Euler Summation formula.

Unit - II

12. Prove $\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$ implies $\lim_{x\to\infty} \frac{\theta(x)}{x} = 1$
13. State and prove Abel's identity.
14. For $n \geq 1$, the nth prime P_n satisfies the inequalities

$$\frac{1}{6}\, n\log n < P_n < 12\left(n\log n + nlog\frac{12}{e}\right).$$

Unit - III

15. Prove that the Diophantine equation $y^2 = x^3 + k$ has no solution if k has the form $k = (4n-1)^3 - 4m^2$ where m and n are integers such that no prime $p \equiv -1(mod\ 4)$ divides m

16. Solve the system of simultaneous congruence 2x + 3y ≡ 1(mod 26),7x + 8y ≡ 2(mod 26)

17. (a) Explain how to send a signature in RSA cryptosystem?

    (b) Find the inverse of the matrix A = $\begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix} \in M_2(Z\ /\ 26Z)$

(6 × 2 = 12 weightage)

Part C

Answer any ***two*** questions. Each question carries 5 weightage.

18. (a) State and prove Mobius inversion formula.

    (b) For $x \geq 2$, prove that $\sum_{p \leq x} \left[\frac{x}{p}\right] \log p = x \log x + O(x)$.

19. For every integer $n \geq 2$, prove that $\frac{1}{6}\frac{n}{\log n} < \pi(n) < \frac{6n}{\log n}$

20. State and prove Gauss's lemma.

21. (a) Find the cipher text of the plain text 'THANK YOU' using the affine enciphering transformation with key (7,12) in 26-letter alphabet.

    (b) Describe public key cryptosystem and explain RSA cryptosystem with example.

(2 × 5 = 10 Weightage)

****