ADAMAS UNIVERSITY

END-SEMESTER EXAMINATION : JANUARY 2021

(Academic Session: 2020 – 21)

Name of the Program:	B.Tech in Computer Science and Engineering	**Semester:**	VII
Paper Title :	Number Theory	**Paper Code:**	SMA44101
Maximum Marks :	40	**Time duration:**	3 hrs.
Total No of questions:	8	**Total No of Pages:**	1
(Any other information for the student may be mentioned here)			

Instructions:

Attempt any three questions from **Section A** (each carrying 4 marks); any **Two Questions** from **Section B** (each carrying 10 marks)**.**

Section C is Compulsory (carrying 8 marks)**.**

	Section A (Attempt **any Three)** $\mathbf{3 \times 4 = 12}$	
1	Using the digraphic cipher that sends the plaintext block P_1, P_2 to the ciphertext block C_1, C_2, with $C_1 \equiv 8P_1 + 9P_2 \pmod{26}$ $C_2 \equiv 3P_1 + 11P_2 \pmod{26}$ encrypt the message DO NOT SHOOT THE MESSENGER.	**4**
2	Solve the following congruence $3x^2 + 9x + 7 \equiv 0 (mod\ 13)$.	**4**
3	Decipher the message: RTOLKTOIK, which was encrypted by the transformation, $C \equiv 3P + 24 \pmod{26}$.	**4**
4	Factor 247 using the Pollard Rho method with polynomial $f(x) = x^2 + 1$ and initial guess $x_0 = 1$.	**4**
	Section B (Attempt **any Two)** $\mathbf{2 \times 10 = 20}$	
5	i) Use Gauss's lemma to compute the Legendre symbol $\left(\frac{5}{19}\right)$. ii) For any positive integer k, there are infinitely many primes of the form 4k + 1.	**5+5**
6	i) Using the Generalized Quadratic Reciprocity Law, determine whether the congruence $x^2 \equiv 231 \pmod{1105}$ is solvable. ii) Show that the only prime p for which 3p+1 is a perfect square is p= 5.	**5+5**
7	Using the Diffie-Hellman key agreement protocol, find the common key that can be used by two parties with keys $k_1 = 27$ and $k_2 = 31$ when the modulus is p= 103 and the base r=5.	**10**
	SECTION C is Compulsory $\mathbf{1 \times 8 = 8}$	
8	If the cipher text message: 0504187403470515208823560736046 8 is produced by RSA cipher with e = 5 and n = 2881, find the plaintext message.	**8**