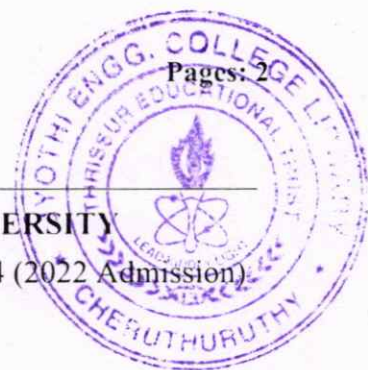


Reg No.: _____

Name: _____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Fourth Semester B.Tech (Hons.) Degree Examination June 2024 (2022 Admission)

**Course Code: CST292****Course Name: Number Theory**

Max. Marks: 100

Duration: 3 Hours

PART A*(Answer all questions; each question carries 3 marks)*

Marks

- | | | |
|----|--------------------------------------------------------------------------------|---|
| 1 | Show that $\mathbb{Z}_5 - \{0\}$ under multiplication modulo 5 forms a group. | 3 |
| 2 | Apply Euclidean Algorithm to find the GCD of (4278, 8602). | 3 |
| 3 | What do you mean by prime factorization? Find the prime factors of 100 and 76. | 3 |
| 4 | Show that 11 is prime using Wilson's theorem. | 3 |
| 5 | Outline the concept of Carmichael number. Give an example. | 3 |
| 6 | Define Primitive root with example. | 3 |
| 7 | Describe Dirichlet product and its properties. | 3 |
| 8 | What does the law of quadratic reciprocity state? | 3 |
| 9 | State Pell's equation | 3 |
| 10 | What are Gaussian integers? Give examples. | 3 |

PART B*(Answer one full question from each module, each question carries 14 marks)***Module -1**

- | | | |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 11 | a) Describe the properties of modular arithmetic and modulo operator. Apply modulo reduction to compute the least absolute residue of $19 * 14 \pmod{23}$. | 7 |
| | b) Find the general solution of the Diophantine equation $21x + 13y = 45$. | 7 |
| 12 | a) Apply Euclidean algorithm to find out the GCD(1492,1066) and express it in terms of Bezout's identity. | 7 |
| | b) Explain Extended Euclidean algorithm. Find the multiplicative inverse of 23 mod 100. | 7 |

Module -2

- | | | |
|----|-----------------------------------------------------------------------------------------------------|---|
| 13 | a) State the linear congruence theorem and use it to solve the congruence $12x \equiv 48 \pmod{18}$ | 7 |
|----|-----------------------------------------------------------------------------------------------------|---|

- b) Explain the concept of Fermat's factorization theorem and use it to factorize the number 3811 7
- 14 a) State Chinese Remainder Theorem. Solve the linear system 9
- $$x \equiv 2 \pmod{3}$$
- $$x \equiv 3 \pmod{5}$$
- $$x \equiv 2 \pmod{7}$$
- b) Use Fermat's Little theorem to find the solution of: 5
- i. $3^{31} \pmod{7}$ (2 marks)
- ii. $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \pmod{7}$ (3 marks)

Module -3

- 15 a) Mention the merits and demerits of asymmetric key encryption. Also explain the challenges faced in public key crypto systems. 6
- b) Solve the polynomial power congruence $x^3 + 4x \equiv 4 \pmod{343}$ (hint: $343=7^3$) 8
- 16 a) Define Euler's Totient function and using prime factorization compute $\phi(666)$ & $\phi(1976)$. 8
- b) Verify that 5 is a primitive root of U_7 and hence show that it generates elements of U_7 . 6

Module -4

- 17 a) State Euler's criterion for quadratic residues and use it to determine if 3 is a quadratic residue of 29. 6
- b) Find the value of the Legendre symbol: $(4699|4703)$. *Hint:* [4703 is prime and 4699 is composite] 8
- 18 a) State the law of reciprocity for Jacobi symbols. Evaluate Jacobi symbols $(55|273)$ and $(364|935)$ 7
- b) Solve the quadratic congruence: $3x^2 - 4x + 7 \equiv 0 \pmod{13}$ 7

Module -5

- 19 a) Express the integer 247 as sums of four squares. 7
- b) Define a Gaussian integer. Factorize the Gaussian integer $(-19 + 43i)$ 7
- 20 a) Express $225|157$ as a finite simple continued fraction. 7
- b) Find all solutions of the Pell's equation $x^2 - 2y^2 = 1$ 7
