NATIONAL INSTITUTE OF TECHNOLOGY CALICUT
Department of Computer Science and Engineering
CS6101E-Mathematical Foundations of Computer Science (MFCS)
Common for S1 M. TECH (CS, CSIS, AIDA), Research Scholars
Mid Semester Examinations

DoE: 25-10-2023 | Time: 90 Minutes
Max. Marks: 30

Note: Answer ALL the questions on answer script
Use outcome of the proof of questions if required in another solution

1. Let '*' denoted on $\mathbb{Q}^+$ by $a*b=ab/2$, where $a, b \in \mathbb{Q}^+$. Is $(\mathbb{Q}^+, *)$ a group? Justify. 2M

2. Consider the quotient ring $\mathbb{Z}_2[x]/x^3+x+1$. Find the elements present in the quotient ring. Find the multiplicative inverse of $(x+1)$ if it presents in the quotient ring. Justify, is quotient ring a field? 3M

3. Show that there exist non-negative integers x *and* y such that $x^2 - y^2 = n$ *if and only if* n *is odd or is a multiple of* 4. Show that there is exactly one such representation of n if and only if $n = 1, 4$, an odd prime, or four times a prime. 3M

4. Let $\psi(n)$ *denote the number of integers* $a, 1 \le a \le n$, *for which both* $(a,n) = 1$ *and* $(a+1, n) = 1$. *Show that* $\psi(n) = n\prod_{p|a}\left(1 - \frac{2}{p}\right)$. For what values of n is $\psi(n) = 0$. 3M

5. Prove or disprove that p is an odd prime $\left(\frac{3}{p}\right) = 1$ *if and only if* $p \equiv \pm 1 \pmod{12}$. 3M

6. $x^2 \equiv -66 \pmod{221}$ has ZERO solution or TWO solutions. 4M
(Note. - if moduli is composite, use the Jacobi symbol by expressing moduli as a product of prime powers. The power of the prime rises to the entire term, and terms are separated based on the denominator. ZERO marks will be awarded if you use other methods than Jacobi. To solve Legendre, use other theorems than Euler's criteria.)

7. Let $\phi: G_1 \to G_2$ *be a surjective group homomorphism. Let* H_1 *be a normal subgroup of* G_1 *and suppose that* $\phi(H_1) = H_2$. *Prove or disprove that* $G_1/H_1 \cong G_2/H_2$. 3M

8. Find the Characteristic of the given field $F = \left\{\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, \begin{pmatrix}1 & 1\\1 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\0 & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\1 & 1\end{pmatrix}\right\}$ *with entries from* $\mathbb{Z}_2$. Prove or disprove that it is isomorphic with $\mathbb{Z}_8^*$. 3M

9. Find the ideals in $\mathbb{Z}_{18}$. Which of these ideals are maximal and prime ideals? 3M

10. Prove that, let $p(x) \in \mathbb{Z}[x]$ *be a monic polynomial such that* $p(x)$ *factors into two polynomials* $\alpha(x)$ *and* $\beta(x)$ *in* $\mathbb{Q}[x]$ *where the degree of both* $\alpha(x)$ *and* $\beta(x)$ *are less than the degree of* $p(x)$. *Then* $p(x) = a(x)b(x)$, *where* $a(x)$ *and* $b(x)$ *are monic polynomials in* $\mathbb{Z}[x]$ *with* $\deg \alpha(x) = \deg a(x)$ *and* $\deg \beta(x) = \deg b(x)$ 3M

*****The END*****