BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, PILANI
First Semester 2023-24
MATH F441 (Discrete Mathematics Structure)
Comprehensive Examination (Closed Book)
Part-B

Date: December 12, 2023 Time: 120 Minutes Max. Marks: 30

Q.1. Show that if in a BIBD (v, b, r, k, λ), b is divisible by r, then $b \geq v + r - 1$. [5]

Q.2. In the (15, 7) BCH code which can correct up to the two errors suppose $R = (010000011000000)$ is the received message. Then find the correct message with justification. [5]

Q.3. Let $\mathbb{F} = \{\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}\}$ is a finite field with n elements, s.t. $\alpha_0 = 0$ and $\alpha_1 = 1$, then show that there is $n - 1$ MOLS exist. [5]

Q.4. Prove that if $\alpha \in \mathbb{Z}_p$, is primitive, α^t is quadratic residue mod p iff t is even. [5]

Q.5. For a (b, v, r, k, λ)-BIBD with incidence matrix A show that $AA^{\mathrm{T}} = (r - \lambda)I + \lambda J$, where I is identity matrix and J is matrix with all entries as "1" of order $v \times v$. [5]

Q.6. How many ways are there to color the vertices of a square with m colors, up to the rotation of the square? Justify. [5]

SET-X

BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, PILANI
First Semester 2023-24
MATH F441 (Discrete Mathematics Structure)
Comprehensive Examination (Closed Book)
Part-A (Quiz)

Date: December 12, 2023 **Time: 60 Minutes** **Max. Marks: 15**

Name: **Id. No.**

*Write all the answers in the boxes below only, answer written anywhere else will not be checked. Any cross cutting overwriting will be considered as question not attempted. Each question carries 1 Mark and no negative marks for wrong answer.

Q.No.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Ans.															

Q.1. Select true statement for mutually orthogonal Latin square(MOLS) from the following:
[A] There are $p - 1$ MOLS of prime order p
[B] There are $\varphi(n)$ MOLS of order n for all n
[C] There are exactly 5 MOLS of order 6
[D] There are $n!$ MOLS of order n for all n

Q.2. Let H be a Hadamard matrix of order n, then which of the following is false:
[A] $HH^{T} = nI$ [B] $det\,(H) = n^{(n/2)}$ [C] $trace$ (H) = 0 [D] None of these

Q.3. ABC is an equilateral triangle. We wish to color each of the three vertices A, B and C by one out of n possible distinct colors. Furthermore, two colorings are considered identical if we can obtain one from the other by rotating or reflecting the triangle. Number of distinct colorings are:
[A] ${}^{n}C_3$ [B] $n(n + 1)(n + 2)/6$ [C] n^3 [D] $n^2(n + 1)^2/4$

Q.4. Let $v = 7$ and $k = 5$, then the minimum value of b for a (b, v, r, k, λ) BIBD to exist:
[A] 7 [B] 20 [C] 21 [D] 35

Q.5. If in RSA algorithm $n = 221$ and $e = 35$, then $d = ?$
[A] 11 [B] 13 [C] 17 [D] 19

Q.6. Finite field $\mathbb{F}$ with $|\mathbb{F}| = 16$ has how many elements of order 5?
[A] 5 [B] 8 [C] 0 [D] 4

Q.7. How many distinct irreducible monic factors of $f(x) = x^5 + x^4 + 1$ over $\mathbb{Z}_2$:
[A] 1 [B] 2 [C] 3 [D] 5

Q.8. The value of Legendre symbol $\left(\frac{101}{1987}\right)$ is:
[A] -1 [B] 0 [C] 1 [D] 2

Q.9. Which of the following polynomial is reducible over $\mathbb{Z}_3$:

[A] $x^3 - x + 1$ [B] $x^3 - x - 1$ [C] $x^3 - x^2 - 1$ [D] $x^3 - x^2 + x + 1$

Q.10. Let $a = x + 1$ be a non-zero element of the finite field $\mathbb{Z}_3[x]/\langle x^2 + 1\rangle$, then inverse of a is:

[A] a [B] a^3 [C] a^5 [D] a^7

Q.11. The solution of the system of congruence $x \equiv 3 \ (mod\ 5)$ and $x \equiv 5 \ (mod\ 7)$ is:

[A] $x \equiv 33 \ (mod\ 35)$ [B] $x \equiv 29 \ (mod\ 35)$ [C] $x \equiv 27 \ (mod\ 35)$ [D] $x \equiv 23 \ (mod\ 35)$

Q.12. Which of the following (v, k, λ) symmetric BIBD does exist:

[A] (76, 25, 8) [B] (67, 12, 2) [C] (64, 21, 6) [D] (56, 24, 7)

Q.13. For the integers $\mathbb{Z}$, with the subtraction (–) operator, which group axiom is satisfied:

[A] Associativity [B] Existence of identity [C] Commutativity [D] Closure

Q.14. The number of distinct second-degree monic polynomials of the form $x^2 + ax + b$ $(b \neq 0)$ over GF (16) is:

[A] 240 [B] 225 [C] 120 [D] 256

Q.15. The complement of a (v, k, λ)-difference set is:

[A] not necessarily a difference set [B] also a (v, k, λ)-difference set

[C] a $(v, v - k, \lambda)$-difference set [D] a $(v, v - k, v - 2k + \lambda)$-difference set

*** All the Best ***

SET-Y

BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, PILANI
First Semester 2023-24
MATH F441 (Discrete Mathematics Structure)
Comprehensive Examination (Closed Book)
Part-A (Quiz)

Date: December 12, 2023 **Time: 60 Minutes** **Max. Marks: 15**

Name: **Id. No.**

*Write all the answers in the boxes below only, answer written anywhere else will not be checked. Any cross cutting overwriting will be considered as question not attempted. Each question carries 1 Mark and no negative marks for wrong answer.

Q.No.	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Ans.															

Q.1. Which of the following polynomial is reducible over $\mathbb{Z}_3$:
[A] $x^3 - x + 1$ [B] $x^3 - x^2 + x + 1$ [C] $x^3 - x^2 - 1$ [D] $x^3 - x - 1$

Q.2. The complement of a (v, k, λ)-difference set is:
[A] a $(v, v - k, v - 2k + \lambda)$-difference set [B] also a (v, k, λ)-difference set
[C] a $(v, v - k, \lambda)$-difference set [D] not necessarily a difference set

Q.3. Let $a = x + 1$ be a non-zero element of the finite field $\mathbb{Z}_3[x]/<x^2 + 1>$, then inverse of a is:
[A] a [B] a^3 [C] a^5 [D]a^7

Q.4. If in RSA algorithm $n = 221$ and $e = 35$, then $d = ?$
[A] 11 [B] 13 [C] 17 [D] 19

Q.5. Finite field $\mathbb{F}$ with $|\mathbb{F}| = 16$ has how many elements of order 5?
[A] 5 [B] 8 [C] 0 [D] 4

Q.6. Let $v = 7$ and $k = 5$, then the minimum value of b for a (b, v, r, k, λ) BIBD to exist:
[A] 7 [B] 20 [C] 21 [D] 35

Q.7. The value of Legendre symbol $\left(\frac{101}{1987}\right)$ is:
[A] -1 [B] 0 [C] 1 [D] 2

Q.8. Select true statement for mutually orthogonal Latin square(MOLS) from the following:
[A] There are $\varphi(n)$ MOLS of order n for all n [B] There are $p - 1$ MOLS of prime order p
[C] There are exactly 5 MOLS of order 6 [D] There are $n!$ MOLS of order n for all n

Q.9. *ABC* is an equilateral triangle. We wish to color each of the three vertices *A*, *B* and *C* by one out of *n* possible distinct colors. Furthermore, two colorings are considered identical if we can obtain one from the other by rotating or reflecting the triangle. Number of distinct colorings are:
[A] ${}^{n}C_3$ [B] $n(n + 1)(n + 2)/6$ [C] n^3 [D] $n^2(n + 1)^2/4$

Q.10. The solution of the system of congruence $x \equiv 3 \ (mod\ 5)$ and $x \equiv 5 \ (mod\ 7)$ is:
[A] $x \equiv 33 \ (mod\ 35)$ [B] $x \equiv 29 \ (mod\ 35)$ [C] $x \equiv 27 \ (mod\ 35)$ [D] $x \equiv 23 \ (mod\ 35)$

Q.11. Which of the following (v, k, λ) symmetric BIBD does exist:
[A] (76, 25, 8) [B] (67, 12, 2) [C] (64, 21, 6) [D] (56, 24, 7)

Q.12. For the integers $\mathbb{Z}$, with the subtraction (–) operator, which group axiom is satisfied:
[A] Associativity [B] Existence of identity [C] Commutativity [D] Closure

Q.13. The number of distinct second-degree monic polynomials of the form $x^2 + ax + b$ $(b \neq 0)$ over GF (16) is:
[A] 240 [B] 225 [C] 120 [D] 256

Q.14. Let *H* be a Hadamard matrix of order *n*, then which of the following is false:
[A] $trace$ (H) = 0 [B] $det\ (H) = n^{(n/2)}$ [C] $HH^{T} = nI$ [D] None of these

Q.15. How many distinct irreducible monic factors of $f(x) = x^5 + x^4 + 1$ over $\mathbb{Z}_2$:
[A] 1 [B] 2 [C] 3 [D] 5

*** All the Best ***