(7 pages) Reg. No. : ....

Code No. : 10296 E **Sub. Code : AMMA 63**

B.Sc. (CBCS) DEGREE EXAMINATION, APRIL 2023.

Sixth Semester

Mathematics — Core

NUMBER THEORY

(For those who joined in July 2020 only)

Time : Three hours Maximum : 75 marks

PART A — ($10 \times 1 = 10$ marks)

Answer ALL questions.

Choose the correct answer :

1. If a and b are any positive integers, then there exist a positive n such that $n\,a \ge b$ by
   (a) Well ordering principle
   (b) Archimedean property
   (c) Finite Induction principle
   (d) Binomial theorem

2. For $n \ge 1$, $\frac{1.3.5....(4n-1)}{[1.3.5....(2n-1)]^2}\binom{2n}{n}$.
   (a) $\binom{4n}{2n}$
   (b) $\binom{4n}{n}$
   (c) $\binom{2n}{n}$
   (d) $\binom{4n}{3n}$

3. Match for integers a, b, c

(i)	$a \mid 1$	(1)	$a \mid c$
(ii)	$a \mid b$ and $b \mid a$	(2)	$a = \pm 1$
(iii)	$a \mid b$ and $c \mid d$	(3)	$a = \pm b$
(iv)	$a \mid b$ and $b \mid c$	(4)	$ac \mid bd$

   (a) (i) – 2, (ii) – 3, (iii) – 1, (iv) – 4
   (b) (i) – 2, (ii) – 3, (iii) – 4, (iv) – 1
   (c) (i) – 1, (ii) – 2, (iii) – 3, (iv) – 4
   (d) (i) – 2, (ii) – 4, (iii) – 3, (iv) – 1

4. If a and b are integers, with $b \neq 0$, then there exist unique integers q and r such that $a = qb + r$ where the value of r is
   (a) $0 \le r \le |b|$ (b) $0 \le r \le |a|$
   (c) $0 \le r < |b|$ (d) $0 < r < |b|$

5. If p is a prime and $p \mid ab$, then ————
   (a) $p \mid a$ and $p \mid b$ (b) $p \nmid a$ and $p \nmid b$
   (c) $p \mid a$ or $p \mid b$ (d) none of these

6. There is an infinite number of primes of the form ————
   (a) $4n$ (b) $4n+1$
   (c) $4n+2$ (d) $4n+3$

7. Which of the following is true?
   (i) $-56 \equiv 9 \pmod 7$
   (ii) $-11 \equiv 9 \pmod 7$
   (a) (i) alone
   (b) (ii) alone
   (c) (i) and (ii) both true
   (d) both false

8. If 'a' is a solution of $p(x) \equiv 0 \pmod n$ and $a \equiv b \pmod n$, then ————
   (a) b is also a solution
   (b) b need not be a solution
   (c) b is sometime a solution
   (d) the value of b is undetermined

9. By Fermat's method factorize 119143 which is ————
   (a) $352^2 - 69^2$
   (b) $(352+69)(352-69)$
   (c) $421 . 283$
   (d) All the above

10. If p is a prime, then ———— for integer a
   (a) $a^p \equiv 1 \pmod p$
   (b) $a^p \equiv a \pmod p$
   (c) $a^p \equiv 0 \pmod p$
   (d) $a^p \not\equiv a \pmod p$

PART B — (5 × 5 = 25 marks)

Answer ALL questions choosing either (a) or (b).

11. (a) State and prove Archimedean property.

Or

(b) Prove by mathematical induction

$1^2 + 2^2 + 3^2 + ... + n^2 = \frac{n(2n+1)(n+1)}{6}$.

12. (a) If $K > 0$, prove that $gcd(Ka, Kb) = K gcd(a, b)$.

Or

(b) Find the $gcd(12378, 3054)$.

13. (a) Prove that $\sqrt{2}$ is irrational.

Or

(b) If the $n>2$ terms of the arithmetic progression $P, P+d, P+2d, ... P+(n-1)d$ n are all prime numbers, then the common difference d is divisible by every prime 'q' $q<n$.

14. (a) If $ca \equiv cb \pmod{n}$, prove that $a \equiv b \pmod{n/d}$, where $d = gcd(c, n)$.

Or

(b) The linear congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d|b$, where $d = gcd(a, n)$. If $d|b$, prove that if has d mutually in congruent solutions modulo n.

15. (a) State and prove Fermat's little theorem.

Or

(b) Illustrate Fermat's method by finding factor of 119143.

PART C — (5 × 8 = 40 marks)

Answer ALL questions choosing either (a) or (b).

16. (a) State and prove Binomial theorem.

Or

(b) Illustrate a proof of second principle of finite induction for lucas sequence 1, 3, 4, 7, 11, 18, 29, 47, 76...

17. (a) State and prove Division algorithm.

Or

(b) State and prove Euclidean Algorithm.

18. (a) There are an infinite number of primes.

Or

(b) State and prove fundamental theorem of Arithmetic.

19. (a) State and prove Chinese remainder theorem.

Or

(b) Let $n>0$ be fixed and a, b, c, d be arbitrary integers then prove the following properties.

(i) $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$

(ii) $a \equiv a \pmod{n}$

(iii) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$

(iv) If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$.

20. (a) State and prove Wilson theorem.

Or

(b) If P is a prime, prove that $a^p \equiv a \pmod{p}$ for any integer a.

———————