This question paper contains **2** printed pages]

SB—95—2022

FACULTY OF SCIENCE

B.Sc. (Third Year) (Sixth Semester) EXAMINATION

MAY/JUNE, 2022

(New/CBCS Pattern)

MATHEMATICS

Paper XVII

(Elementary Number Theory)

(Thursday, 16-06-2022) **Time : 10.00 a.m. to 12.30 p.m.**

Time— 2½ *Hours* *Maximum Marks*—40

N.B. :— (*i*) Attempt *all* questions.

(*ii*) Figures to the right indicate full marks.

1. Given integers a and b, with $b > 0$. show that there exist unique integers q and r satisfying $a = qb + r$, $0 \le r < b$. Also find the gcd (12378, 3054) using Euclidean algorithm. 15

Or

(*a*) If p is prime and $p \mid a_1.a_2 \ldots\ldots a_n$, then prove that $p \mid ak$ for some k, where $1 \le k \le n$. 8

(*b*) Show that for given integers a and b not both of which are zero, there exist x and y such that $\gcd(a, b) = ax + by$. 7

2. Define congruence modulo n. Let $n > 1$ be fixed and a, b, c, d be arbitrary integers, then prove that : 15

(*i*) If $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$

(*ii*) If $q \equiv b \pmod n$ and $c \equiv d \pmod n$, then $(a + c) \equiv (b + d) \pmod n$ & $ac \equiv bd \pmod n$

P.T.O.

(*iii*) If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for any positive integer k.

Or

(*a*) Prove that the linear congruence $ax \equiv b \pmod{n}$ has a unique solution if and only if $d \mid b$ where $d = gcd(a, n)$. If $d \mid b$, then it has d mutually incongruent solutions modulo n. 8

(*b*) State and prove Fermat's theorem. 7

3. Attempt any *two* of the following : 10

(*a*) Show that if a and b are integers, not both zero then the set $T = \{ax + by \mid x, y \text{ are integers}\}$ is precisely the set of all multiples of $d = gcd(a, b)$. 10

(*b*) Prove that the number $\sqrt{2}$ is irrational.

(*c*) Show that $2^{20} \equiv 1 \pmod{41}$.

(*d*) If p is prime, prove that $(p - 1)! \equiv -1 \pmod{p}$.