* R R - 0 8 6 1 / 2 0 0 *

# RR-0861
# Third Year B. Sc. Examination
## March / April – 2010
## Number Theory
**(New Course)**

Time : Hours] [Total Marks : **70**

**સૂચના :**

(૧)

નીચે દર્શાવેલ ☛ નિશાનીવાળી વિગતો ઉત્તરવહી પર અવશ્ય લખવી.
**Fillup strictly the details of ☛ signs on your answer book.**

Name of the Examination :
☛ **T.Y. B.Sc.**

Name of the Subject :
☛ **NUMBER THEORY (NEW)**

☛ Subject Code No. : **0 8 6 1** ☛ Section No. (1, 2,.....) : **NIL**

Seat No. :

Student's Signature

(૨) જમણી તરફની સંખ્યા પૂરા ગુણ દર્શાવે છે.

(૩) પ્રચલિત સંકેતો અનુસરો.

૧ નીચેનાના જવાબો આપો : ૧૦

(૧) જો $a|b$ અને $b \neq 0$ તો સાબિત કરો કે $|a| \leq |b|$.

(૨) $2^{50}$ ને 7 વડે મળતી શેષ શોધો.

(૩) ચાઇનિસ શેષ પ્રમેયનું વિધાન લખો.

(૪) સાબિત કરો કે $n = 2^{k-1}$ સમીકરણ $\sigma(n) = 2n-1$ નું સમાધાન કરે છે.

(૫) $\phi(5040)$ની કિંમત શોધો.

૨ (અ) સાબિત કરો કે ડાયોફેનટાઇન સમીકરણ $ax+by=c$ને ઉકેલ હોય તો અને તો જ $d/c$ જ્યાં $d = \gcd(a,b)$. ૫

(બ) જો કોઈ પૂર્ણાંક $m$ માટે $a/m$ અને $b/m$ તો સાબિત કરો કે $lcm(a,b)/m$. ૪

(ક) $lcm\,(321, 843)$ મેળવો. ૩

**અથવા**

૨ (અ) આપેલ શૂન્ય નહિ હોય તેવા પૂર્ણાંક $a$ અને $b$ માટે, સાબિત કરો કે $\gcd(a, b) = ax + by$ જ્યાં $x, y$ પૂર્ણાંક છે. ૫

(બ) ડાયોફેનટાઈન સમીકરણ $20x + 13y = 200$ નાં બધાં જ ધન ઉકેલો મેળવો. ૪

(ક) યુક્લિડનું પ્રમેય લખો અને સાબિત કરો. ૩

૩ (અ) સાબિત કરો કે અવિભાજ્ય સંખ્યાઓ અનંત છે. ૫

(બ) સાબિત કરો કે $n^2 - 4$ સ્વરૂપની અવિભાજ્ય સંખ્યા ફક્ત 5 છે. ૪

(ક) જો $x$ અને $y$ અયુગ્મ પૂર્ણાંક હોય તો સાબિત કરો કે $x^2 + y^2$ પૂર્ણવર્ગ સંખ્યા હોઈ શકે નહિ. ૩

**અથવા**

૩ (અ) ઇરટોસ્થેનીસ ચાળણીની મદદથી 1થી 200 વચ્ચેની બધી અવિભાજ્ય સંખ્યા મેળવો. ૫

(બ) જો $ca \equiv cb \pmod{n}$ અને $d = \gcd(c, n)$ તો સાબિત કરો કે ૪

$$a \equiv b \left( \bmod \frac{n}{d} \right).$$

(ક) સાબિત કરો કે બધી પૂર્ણાંક સંખ્યા $n > 11$ને બે વિભાજ્ય સંખ્યાના સરવાળા બરાબર લખી શકાય છે. ૩

૪ (અ) ફરમાનું પ્રમેય લખો અને સાબિત કરો. ૫

(બ) ધારો કે ધનપૂર્ણાંક $N$ નું દશાંકી નિરૂપણ ૪

$$N = a_m 10^m + a_{m-1} \cdot 10^{m-1} + \ldots\ldots\ldots + a_1 . 10 + a_0, \quad 0 \le a_k < 10$$

અને $T = a_0 - a_1 + a_2 - \ldots\ldots\ldots + (-1)^m \cdot a_m$ તો સાબિત કરો કે

$11/N \Leftrightarrow 11/T$

(ક) $P(x)=\sum_{k=1}^{n} C_k x^k$ એ પૂર્ણાંક સહગુણકો સાથેનું $x$ નું બહુપદી વિધેય છે. ૩

જો $a \equiv b \pmod{n}$ તો સાબિત કરો કે $P(a) \equiv P(b) \pmod{n}$.

**અથવા**

૪ (અ) વિલ્સનનું પ્રમેય લખો અને સાબિત કરો. ૫

(બ) નીચેની સુરેખ સમશેષ સંહતિ ઉકેલો : ૪

$x \equiv 5 \pmod{6}$, $x \equiv 4 \pmod{11}$ અને $x \equiv 3 \pmod{17}$.

(ક) $2 \cdot (26!)$ને 29 વડે ભાગતા મળતી શેષ શોધો. ૩

૫ (અ) આપેલ ધનપૂર્ણાંક $n$ અને અવિભાજ્ય સંખ્યા $P$ માટે સાબિત કરો કે ૫

$\sum_{k=1}^{\infty} \left[ n \middle| p^k \right]$ એ $n!$ ને નિઃશેષ ભાગી શકે તેવા મહત્તમ ઘાતવાળા $P$ નો ઘાતાંક છે.

(બ) જો $F$ ગુણાત્મક વિધેય છે અને $F(n)=\sum_{d/n} f(d)$ તો સાબિત કરો કે ૪

$f$ પણ ગુણનાત્મક વિધેય છે.

(ક) સાબિત કરો કે પૂર્ણાંક $n$ ના ધન ભાજકોનો ગુણાકાર $n^{T(n)/2}$ બરાબર છે. ૩

**અથવા**

૫ (અ) જો $f$ અને $F$ સાંખ્યિક ગણિતીય વિધેય માટે, $F(n)=\sum_{d/n} f(d)$, ૫

તો સાબિત કરો કે કોઈ પણ પૂર્ણાંક $N$ માટે, $\sum_{n=1}^{N} F(n)=\sum_{k=1}^{N} f(k)[N/k]$.

(બ) જો $n>1$ માટે, $n=P_1^{k_1}\cdot P_2^{k_2}\cdot\ldots\ldots P_r^{k_r}$ અવિભાજ્ય અવયવીકરણ હોય તો સાબિત કરો કે ૪

$$\sigma(n)=\frac{P_1^{k_1+1}-1}{P_1-1}\cdot\frac{P_2^{k_2+1}-1}{P_2-1}\ldots\ldots\ldots\ldots\frac{P_r^{k_r+1}-1}{P_r-1}$$

(ક) બધા જ ધન પૂર્ણાંક $n\geq 1$ માટે સાબિત કરો કે ૩

$$\sum_{d/n,\, d>0}\mu(d)\ =1,\quad \text{જો } n=1$$
$$=0,\quad \text{જો } n>1$$

૬ (અ) જો ધનપૂર્ણાંક $n$ માટે $\gcd(a,n)=1$ હોય તો સાબિત કરો કે ૫

$$a^{\phi(n)}\equiv 1(\bmod n).$$

(બ) સીઝર ગુપ્તલિપિ દ્વારા KDSSB ELUWKGDB ઉત્પન્ન થતાં સંદેશનો મૂળભૂત સંદેશ લખો. ૪

(ક) જો પૂર્ણાંક $n$ ને $r$ જુદાં જુદાં અયુગ્મ અવિભાજ્ય અવયવ હોય તો સાબિત કરો કે $2^r/\phi(n)$. ૩

**અથવા**

૬ (અ) સંદેશ GOLD MEDALનું RSA અલગોરિધમ, જ્યાં $key(n,k)=(2419,3)$ દ્વારા સાંકેતિક ભાષા લખો. ૫

(બ) સીઝર ગુપ્તલિપિનો ઉપયોગ કરીને સંદેશ REPLY NOWની સાંકેતિક ભાષા લખો. ૪

(ક) સાબિત કરો કે $\phi(3n)=3\phi(n)\Leftrightarrow 3/n$. ૩

## ENGLISH VERSION

**Instructions :** (1) As per the instruction no. 1 of page no. 1.
(2) Figures to the right indicate full marks.
(3) Follow usual instructions.

**1** Answer the following : **10**

(1) If $a|b$ and $b \neq 0$, then prove that $|a| \leq |b|$.

(2) Find the remainder when $2^{50}$ is divide by 7.

(3) State the Chinese Remainder Theorem.

(4) Show that $n = 2^{k-1}$ satisfies the equation $\sigma(n) = 2n - 1$.

(5) Calculate $\phi(5040)$.

**2** (a) Show that the linear Diophantine equation $ax + by = c$ has a solution if and only if $d/c$, where $d = \gcd(a, b)$. **5**

(b) Prove that if $m$ is any integer such that $a/m$ and $b/m$ then $lcm(a, b)/m$. **4**

(c) Find $lcm(321, 843)$. **3**

**OR**

**2** (a) Given non zero integers $a$ and $b$, show that $\gcd(a, b) = ax + by$ for some integers $x, y$. **5**

(b) Determine all solutions in positive integers of the Diophantine equation : $20x + 13y = 200$. **4**

(c) State and prove Euclid's lemma. **3**

3 (a) Show that there are infinite number of primes. **5**

(b) Prove that the only prime of the form $n^2-4$ is 5. **4**

(c) If $x$ and $y$ are odd, prove that $x^2+y^2$ cannot be a perfect square. **3**

**OR**

3 (a) Employing the Sieve of Eratosthenes, obtain all the primes between (5) 1 and 200. **5**

(b) If $ca \equiv cb \pmod{n}$ and $d = \gcd(c, n)$ then prove that $a \equiv b \left( \mod \frac{n}{d} \right)$. **4**

(c) Prove that each integer $n > 11$ can be written as the sum of two composite numbers. **3**

4 (a) State and prove Fermat's Little Theorem. **5**

(b) If $N = a_m 10^m + a_{m-1} \cdot 10^{m-1} + \ldots\ldots\ldots + a_1 . 10 + a_0$ be the decimal expansion of the positive integer $N$, $0 \le a_k < 10$ and let $T = a_0 - a_1 + a_2 - \ldots\ldots\ldots + (-1)^m \cdot a_m$. Then prove that $11/N$ if and only if $11/T$. **4**

(c) Let $P(x) = \sum_{k=1}^{n} C_k x^k$ be a polynomial function of $x$ with integral coefficients $c_k$. If $a \equiv b \pmod{n}$, then show that : $P(a) \equiv P(b) \pmod{n}$. **3**

**OR**

4 (a) State and prove Wilson's theorem. **5**

(b) Solve the following set of simultaneous conguences : **4**

$x \equiv 5 (\mathrm{mod}\, 6)$, $x \equiv 4 (\mathrm{mod}\, 11)$ and $x \equiv 3 (\mathrm{mod}\, 17)$.

(c) Find the remainder when $2 \cdot (26!)$ is divided by 29. **3**

5 (a) If $n$ is a positive integer and $p$ a prime, then prove that the exponent of the highest power of $p$ that divides $n!$ is $\sum_{k=1}^{\infty} \left[ n \middle| p^k \right]$. **5**

(b) If $F$ is a multiplicative function and $F(n) = \sum_{d/n} f(d)$, then show that $f$ is also multiplicative. **4**

(c) Show that the product of the positive divisors of an integer $n$ is equal to $n^{T(n)/2}$. **3**

**OR**

5 (a) Let $f$ and $F$ be number theoretic functions such that $F(n) = \sum_{d/n} f(d)$, then prove that for any integer $N$, **5**

$$\sum_{n=1}^{N} F(n) = \sum_{k=1}^{N} f(k)[N/k].$$

(b) If $n = P_1^{k_1} \cdot P_2^{k_2} \cdot \ldots\ldots\ldots P_r^{k_r}$ is the prime factorization of $n > 1$, then prove that **4**

$$\sigma(n) = \frac{P_1^{k_1+1} - 1}{P_1 - 1} \cdot \frac{P_2^{k_2+1} - 1}{P_2 - 1} \ldots\ldots\ldots\ldots \frac{P_r^{k_r+1} - 1}{P_r - 1}.$$

(c) For each positive integer $n \geq 1$, prove that **3**

$$\sum_{d/n,\, d>0} \mu(d) = 1, \quad \text{if } n = 1$$

$$= 0, \quad \text{if } n > 1$$

**6** (a) If $n$ is a positive integer and $\gcd(a, n) = 1$, then prove that $a^{\phi(n)} \equiv 1 \pmod{n}$. **5**

(b) If the Caesar cipher produced KDSSB ELUWKGDB, what is the plaintext message ? **4**

(c) Prove that if the integer $n$ has $r$ district odd prime factors, then $2^r / \phi(n)$. **3**

**OR**

**6** (a) Encrypt the message GOLD MEDAL using the RSA algorithm with $key(n, k) = (2419, 3)$. **5**

(b) Encrypt the message REPLY NOW using the Caeser cipher. **4**

(c) Prove that $\phi(3n) = 3\phi(n) \Leftrightarrow 3/n$. **3**