SM 404/A computational introduction to Number Theory/Term II 2023-24/T2-23-24-SM 404 [#97]

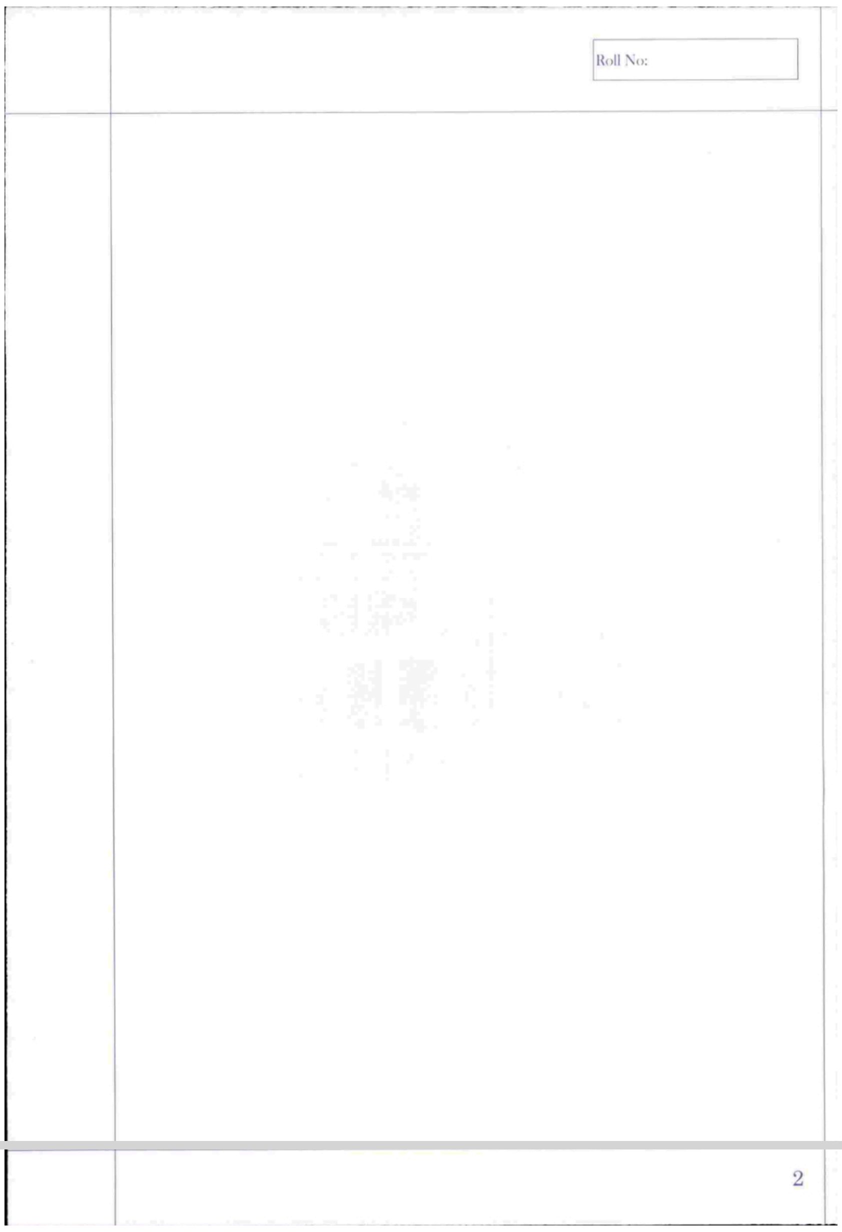
Sarvesh Kumar A [IMT2022521] - sarveshkumar.a@iiitb.ac.in

Test Start Time	3/7/2024, 6:00:00 PM
Marks Scored	30.0 / 50.0
Total Questions	8
Attempted Questions	7
Correct Questions	6
Incorrect Questions	1
Skipped Questions	1
Pending Evaluation	0

Answer Script

Previous Page: 1 / 15 Next

36 %



Previous Page: 1 / 15 Next

List of Sections

Theory questions Marks per question : 5.0 **Marks Scored : 22.0**

Q No.	Q. Type	Status	Marks
1	File Upload	✔	5.0

Hide Answer

Find the smallest positive integer n which is congruent to $(32)^{412}$ mod 7.

Q No.	Q. Type	Status	Marks
2	File Upload	✔	5.0

Hide Answer

If n is a composite positive integer, show that $(n-1)!+1$ is not divisible by n.

Q No.	Q. Type	Status	Marks
3	File Upload	✔	2.0

Hide Answer

Without using a calculator find the remainder when $n=(17)(16)(15)(14)(11)(10)(9)(8)(7)(6)(5)$ is divided by 13.

Evaluator Comments

Explicit calculation is not appreciated.

Q No.	Q. Type	Status	Marks
4	File Upload	✔	5.0

Hide Answer

Find the remainder when $n = 3^{172698304 16891}$ is divided by 5.

5	File Upload	✔	5.0	View Answer

Algorithms-1

Marks per question : 8.0 Marks Scored : 8.0

Q No.	Q. Type	Status	Marks	
1	File Upload	✔	8.0	Hide Answer

Design an algorithm that takes three positive integers $a > b > 1, n > ab$ with $\gcd(a, b) = 1$ and computes **positive** integers $s, t > 0$ such that $as + bt = n$.

Algorithm-2

Marks per question : 9.0 Marks Scored : 0.0

Q No.	Q. Type	Status	Marks	
1	File Upload	⚠	0.0	Hide Answer

Consider an abstract computing machine – let's call it the *addition machine* — with a fixed number of *registers* and capable of performing basic addition and subtraction on integers and a few others to make it 'complete'. Here's the full instruction set of the our addition machine:

- $\texttt{input(n)}$
- $\texttt{m} \leftarrow \texttt{n}$
- $\texttt{m} \leftarrow \texttt{m} + \texttt{n}$
- $\texttt{m} \leftarrow \texttt{m} - \texttt{n}$
- $\texttt{if (m} \geq \texttt{n) then goto(label)}$
- $\texttt{output(x)}$

Show how you can compute $(m \bmod n)$ for any two integers $m > n > 0$ using the addition machine in time $O\left(\log^k\left(\frac{m}{n}\right)\right)$ for a small positive integer k.

User did not attempt this question

Evaluator Comments

Not Answered

Algorithm-3

Marks per question : 8.0 Marks Scored : 0.0

Q No.	Q. Type	Status	Marks	
1	File Upload	✖	0.0	Hide Answer

We know that the asymptotic running time $T(.)$ for both the product $m * n$ and the Extended GCD $\texttt{EGCD}(m, n)$ for any two integers m, n is $O(\texttt{len}(m) * \texttt{len}(n))$. (a) Argue why the actual running time (clock time) for $m * n$ is likely to be significantly faster (by a not-so-small, though bounded, constant factor) than $\texttt{EGCD}(m, n)$. (b) In this context design an algorithm for computing the inverses (modulo n) for a set of numbers $\alpha_1, ..., \alpha_{k+1} \in Z_n^*$ that computes just one inverse directly (presumably using EGCD) along with at most $3k$ products, modulo n. In other words, design an algorithm $\mathcal{A}$ which returns $(\alpha_1^{-1}, ..., \alpha_{k+1}^{-1})$ such that

$$T\left(\mathcal{A}(n, \alpha_1, ..., \alpha_{k+1})\right) \leq T\left(\texttt{EGCD}(\alpha, \beta)\right) + 3k.T\left(\alpha *_{\bmod n} \beta\right)$$

where $\alpha_1, ..., \alpha_{k+1} \in Z_n^*$ and α, β are arbitrary elements of Z_n^*.

Evaluator Comments

The argument for (a) is very loose and for (b) it is incomplete and incorrect.