Indian Institute of Technology Kharagpur
Department of Computer Science and Engineering

CS60094 Computational Number Theory **Spring 2026**

Class Test 1 **16 February, 11 AM – 12 PM** **Marks = 30**

*Answer **any three** questions. State all assumptions you make. Keep your answers concise.*

1. Let $p \in \mathbb{P} \setminus \{2\}$. Prove or Disprove the following.
   (a) $(p-1)! \equiv 1 \pmod{p}$
   (b) The numerator of $\displaystyle\sum_{i=2}^{p-1} \frac{1}{i(i-1)}$ is divisible by p.

   5+5 = 10

2. Let $a, b \in \mathbb{N}$ with $d = \gcd(a,b) = ua + vb$ for some $u, v \in \mathbb{Z}$.
   (a) Demonstrate that u, v are not unique.
   (b) Assume that $(a,b) \neq (1,1)$. Prove that u, v can be chosen to satisfy $|u| \leq b/d$ and $|v| \leq a/d$.

   3+7 = 10

3. (a) Describe an algorithm to compute $a_1^{e_1} a_2^{e_2} a_3^{e_3} \pmod{m}$ that uses only one square-and-multiply loop. Assume e_1, e_2, e_3 have the same size in bits.
   (b) How does your algorithm compare with the naive method where $a_1^{e_1} \pmod{m}$, $a_2^{e_2} \pmod{m}$ and $a_3^{e_3} \pmod{m}$ are computed individually (using square-and-multiply method) and then multiplied modulo m?

   6+4 = 10

4. Consider the following algorithm that takes as input two integers a, n where n is odd and positive.

```
J(a, n)
    set s ← 1.
    repeat forever
        a ← a mod n
        if a = 0
            if n = 1
                return s
            else
                return 0
        compute a', r such that a = 2^r a' and a' is odd
        if r ≢ 0 (mod 2) and n ≢ ±1 (mod 8)
            s ← −s
        if a' ≢ 1 (mod 4) and n ≢ 1 (mod 4)
            s ← −s
        (a, n) ← (n, a')
```

   (a) Show that $\mathsf{J}(a,n)$ correctly computes the Jacobi symbol $\left(\frac{a}{n}\right)$.
   (b) What is the running time of the algorithm?

   6+4 = 10