Indian Institute of Technology Kharagpur
Department of Computer Science and Engineering

CS60094 Computational Number Theory **Spring 2026**

Class Test 2 **13 April, 11 AM – 12 PM** **Marks = 30**

---

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

---

1. Recall that n is a pseudoprime to base a (with $\gcd(a, n) = 1$) if $a^{n-1} \equiv 1 \pmod{n}$. Let p, q be primes, $n = pq$, $a \in \mathbb{Z}_n^*$ and $d = \gcd(p-1, q-1)$.
   (a) Prove that n is a pseudoprime to base a if and only if $a^d \equiv 1 \pmod{n}$.
   (b) Prove that n is a pseudoprime to exactly d^2 bases in $\mathbb{Z}_n^*$.
   (c) To how many bases in $\mathbb{Z}_n^*$ is n a pseudoprime if $q = 2p - 1$?

   4+4+2 = 10

2. [*Pépin Test*] A *Fermat number* is of the form $f_m = 2^{2^m} + 1$ for some integer $m \geq 0$.
   (a) Prove that the Fermat number f_m for $m \geq 1$ is prime if and only if $3^{(f_m-1)/2} \equiv -1 \pmod{f_m}$.
   (b) Write down pseudocode for a deterministic primality test for Fermat numbers based on the result from Part (a). (You may assume the input is a Fermat number.)
   (c) What is the running time of your algorithm?

   5+2+3 = 10

3. In Pollard's Rho method (for factoring n), we generate a sequence of integers $x_0, x_1, \ldots$ computed using a function $f(x)$ as follows: $x_0 \in \mathbb{Z}_n$ is random and $x_i = f(x_{i-1})$ for all $i \geq 1$. A common choice for f is $f(x) = x^2 - a \pmod{n}$, where $a \in \mathbb{Z}_n \setminus \{0, 2\}$. What happens if a is either 0 or -2? 10