**CSE439, Fall 2026 Problem Set 5 Due Fri. 11/6, 11:59pm**

The **Second Prelim Exam** will be on **Thursday, Nov. 19** *in class period*. It will cover up through at least section 14.4 and at most section 14.7, depending on the range of a short Assignment 6 which will be due on Friday 11/13. For next week, please read chapter 13 and read chapter 14 up through section 14.4. For the week of Nov. 9–13, continue through section 14.7 and also chapter 18, section 18.1 (only up through Theorem 18.1 and its proof).

———————*-Assignment 5, due Fri. 11/6 "midnight stretchy" on CSE Autolab*———————-

**(1)** Exercise 10.6 on page 105, but described this way: Let $f(x) = y$ be a function with arguments $x$ and values $y$ that are modulo $M = 2^m$. Suppose there is an unknown value $k$ such that whenever $x_2 - x_1$ is a multiple of $2^k$, $f(x_2) = f(x_1)$, and moreover, the function $f$ takes on $2^k$ distinct values. Give a quantum algorithm that computes the value of $k$ in expected time $m^{O(1)}$. (Note that the given conditions of Shor's algorithm do not apply since $M$ is not a product of two odd primes—this is intended to channel Simon's algorithm but with the twist of $f$ being more than 2-to-1. Think of the arguments as $m$-bit binary strings, and consider what $x_2 - x_1$ being a multiple of $2^k$ means then. 30 pts. total)

**(2)** Find the period $r$ of $a = 7$ among integers relatively prime to $M = 33$. Your $r$ will be even. Then show that calculating both $\gcd(M, a^{r/2} - 1)$ and $\gcd(M, a^{r/2} + 1)$ gives the factors of $M$ in this case. (15 pts. total)

**(3)** Exercise 11.1 on page 116. (Bear in mind that $R'$ can be run on other functions $f'$ besides $f$, provided $f'$ also takes and gives values in $[N] = \{0, 1, \ldots, N - 1\}$. 15 pts., for 60 on the set)