CMPSC 464: Introduction to the Theory of Computation **(Date: 10/12/2022)**

Recitation #6 Solution

Instructor: Dr. Young Kun Ko *TAs:*

Problem 1

HW 3 problem.

Problem 2

- M = "On input $\langle a, b, c, p\rangle$, where $a, b, c, p \in \mathbb{N}$:
  1. $r \leftarrow 1$.
  2. Let $b = (b_1 \cdots b_k)_2$, where $b_i \in \{0, 1\}$, for $i = 1, 2, \cdots k$.
  3. For $i = 1, \cdots k$:
     If $b_i == 0$: $r \leftarrow (r^2 \% p)$.
     Else: $r \leftarrow (a r^2 \% p)$.
  4. If $r \equiv c \pmod p$, accept. O.w., reject."

Proof of correctness: Notice that if $a \equiv r \pmod p$, then $a^2 \equiv r^2 \pmod p$. We repeatedly use this property. If $b_i = 0$, we just shift the the exponent one the right, which means raise to the power of two. If $b_i = 1$, we shift the exponent to the right and multiply everything with a. This because:

$$\begin{cases} a^{(10)} = \left(a^{(1)}\right)^2. \\ a^{(11)} = a^{(10)+(1)} = a^{(10)} \cdot a^{(1)} = \left(a^{(1)}\right)^2 \cdot a. \end{cases}$$

Running time: The loop runs for k iterations and in each iteration we do poly-time operation. Therefore M decides $MODEXP$ in polynomial time. Hence $MODEXP \in \mathcal{P}$.