CSE 311: Foundations of Computing I
Assignment #6
due: Fri, May 20, 1:30pm

1. *(15 points)* Section 4.3, exercise 26, all parts
2. *(10 points)* Section 4.4, exercise 10
3. *(10 points)* Section 4.4, exercise 22
4. *(5 points)* Chapter 4, Supplementary exercise 12(a) (on page 330)
5. *(16 points)* Section 8.1, exercise 6, all parts. Your answer should be in the form of a table with Y/N in each entry. You don't need to justify your answers.
6. *(10 points)* Section 8.1, exercise 8, both parts
7. *(10 points)* Section 8.1, exercise 14
8. *(24 points)* Let p be a prime, and let $S := [p-1] = \{1, \ldots, p-1\}$. For any $a \in S$, define the relation R on S by $\{(x, y) : x, y \in S \wedge \exists j \in \mathbb{N}(xa^j \equiv y \pmod{p})\}$. In parts (b) and (c), define r to be the smallest positive integer satisfying $a^r \equiv 1 \pmod{p}$.

   (a) Prove that R is an equivalence relation.

   (b) Prove that for $x \in S$, the equivalence class $[x]$ is equal to $\{x, ax \bmod p, a^2x \bmod p, \ldots, a^{r-1}x \bmod p\} = \{xa^j \bmod p : 0 \leq j < r\}$.

   (c) Prove that $r | p-1$. What can you conclude about $a^{p-1} \bmod p$?