Theory of Computation

Solutions to Homework 4

Problem 1. Please calculate $\phi(313716)$ and $77^{192960} \bmod 313716$. (You need to write down the steps explicitly. Providing merely the final result is not satisfactory.)

Sol. Note that $313716 = 2^2 \times 3 \times 13 \times 2011$ and

$$\phi(n) = 313716 \times \frac{1}{2} \times \frac{2}{3} \times \frac{12}{13} \times \frac{2010}{2011} = 96480.$$

By the Fermat-Euler theorem (Corollary 56),

$$(77^{96480})^2 = 77^{96480} = \mathbf{1} \mod 313716.$$

Problem 2. Show that NP = co-NP if there exists an NP-complete language that belongs to co-NP.

Proof. Suppose X is NP-complete and $X \in$ co-NP. Let a polynomial-time NTM M decide X. For any language $Y \in$ NP, there is a reduction R from Y to X because X is NP-complete. Now, $X \in$ co-NP implies $Y \in$ co-NP by the closeness of reduction; hence

$$\text{NP} \subseteq \text{co-NP}.$$

On the other hand, suppose $Y \in$ co-NP. Then there is a reduction R' from $\bar{Y}$ to X because $\bar{Y} \in$ NP and X is NP-complete. As a result, for all input strings x,

$$x \in \bar{Y} \text{ iff } \mathrm{R}'(x) \in X.$$

This implies $\bar{Y} \in$ co-NP by the closeness of reduction and the assumption of $X \in$ co-NP. Consequently, $Y \in$ NP and

$$\text{co-NP} \subseteq \text{NP}.$$

Thus, NP = co-NP.