# Theory of Computation

## Solutions to Homework ~~3~~

**Problem 1.** Show that if NP $\neq$ coNP, then NP $\neq$ NL. (Hint: The Immerman-Szelepscényi theorem implies NL = coNL.)

*Proof.* If NP = NL, then coNP = coNL = NL by the Immerman-Szelepscényi theorem. Hence coNP = NL = NP, a contradiction. $\square$

**Problem 2.** Let $k$ be a positive integer which is not a multiple of 13. Show that if $k^5 = 1 \bmod 13$, then $k = 1 \bmod 13$. (Hint: Fermat's little theorem implies $k^{12} = 1 \bmod 13$.)

*Proof.* By applying Euclid's algorithm, $1 = -2 \cdot 12 + 5 \cdot 5$. Hence $k \equiv k^{-2\cdot 12 + 5\cdot 5} \bmod 13$. Since $k^{12} \equiv 1 \bmod 13$ by Fermat's little theorem and $k^5 \equiv 1 \bmod 13$, $k \equiv 1 \bmod 13$. $\square$