Introduction to mathematical cryptography
Homework problems
Week 7

13. Assume p is a prime number and $1 \leq g, h \leq p-1$ are primitive roots modulo p. Show that if there is an algorithm which solves the DLP with base g in polynomial time, then there is an algorithm which solves the DLP with base h in polynomial time.

14. Prove that 1729 is a Carmichael number, i.e. (a) 1729 is not a prime; and (b) for every $a \in \mathbf{Z}$, $a^{1729} \equiv a \bmod 1729$ holds.

Note: Please, provide complete arguments everywhere, and explain how you arrived at your answer/solution. Giving the result without explanation leads to score deduction.