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. Assume p is a prime number and $1 \leq g \leq p-1$ is a primitive root modulo p. Consider than the DLP with base g^2, and show that $(g^2)^x \equiv a \bmod p$ has a solution x if and only if a is a quadratic residue modulo p. (Quadratic residue means that it is not the zero residue class, and has a square-root modulo p.)

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