Introduction to mathematical cryptography
Homework problems
Week 6

11. Let p be an odd prime, and assume g is a primitive root modulo p, i.e. for any $a \in \mathbf{F}_p^\times$ there exists a solution to the discrete logarithm problem $g^x \equiv a \bmod p$. For any such a, denote by $\log_g a$ the smallest positive solution, i.e. the smallest positive integer x satisfying $g^x \equiv a \bmod p$. Prove that
    (a) for any $a, b \in \mathbf{F}_p^\times$, $\log_g(ab) \equiv \log_g a + \log_g b \bmod (p-1)$,
    (b) for any $a \in \mathbf{F}_p^\times, n \in \mathbf{N}$, $\log_g(a^n) \equiv n \log_g a \bmod (p-1)$.
12. Let p be an odd prime and let g be a primitive root modulo p i.e. for any $a \in \mathbf{F}_p^\times$ there exists a solution to the discrete logarithm problem $g^x \equiv a \bmod p$. For any such a, denote by $\log_g a$ the smallest positive solution, i.e. the smallest positive integer x satisfying $g^x \equiv a \bmod p$. Prove that a has a square root modulo p if and only if its discrete logarithm $\log_g a$ is even.

Note: Please provide complete arguments everywhere.