HOMEWORK 4 – IN PROGRESS

For this week, please answer the following questions from the text. I've copied the problem itself below and the question numbers for your convenience.

(1) (2.3) Let g be a primitive root for $\mathbb{F}_p$.

(a) Suppose that $x = a$ and $x = b$ are both integer solutions to the congruence $gx = h \mod p$. Prove that $a = b \mod (p-1)$. Explain why this implies the map (2.1) on page 65 is well-defined.

(b) Prove that

$$\log_g(h_1 h_2) = \log_g(h_1) + \log_g(h_2)$$

for all $h_1, h_2 \in \mathbb{F}_p$.

(c) Prove that

$$\log_g(h^n) = n \log_g(h)$$

for all $h \in \mathbb{F}_p$ and $n \in \mathbb{Z}$.

(2) (2.4) Compute the following discrete logarithms:

(a) $\log_2(13)$ for the prime 23, i.e., $p = 23$, $g = 2$, and you must solve the the congruence $2^x = 13 \mod 23$.

(b) $\log_{10}(22)$ for the prime $p = 47$.

(c) $\log_6 27(608)$ for the prime $p = 941$. (Hint: Look in the second column of Table 2.1 on page 66.)