Student Number: 20053722 Name: Bryan Hoang

4. (10 points)

(a) **Answer:**

Proof.

$$\begin{cases} x = a \\ x = b \end{cases}$$
$$\Rightarrow g^a \equiv h \equiv g^b \pmod{p}$$
$$\Rightarrow g^{a-b} \equiv 1 \pmod{p} \tag{1}$$

But since g is a primitive root,

$$\operatorname{ord}(g) = p - 1 \tag{2}$$
$$\Rightarrow p - 1 \mid a - b \qquad \text{by (1) and (2)}$$
$$\Rightarrow a \equiv b \pmod{p-1}.$$

□

The proven result implies that $\log_g(h)$ is well-defined up to adding or subtracting multiples of $p-1$, showing that the map (2.1) on page 63 is indeed well-defined.

(b) **Answer:**

Proof. Let $h_1, h_2 \in \mathbb{F}_p^8$. Starting with the LHS, we have

$$\begin{aligned} g^{\log_g(h_1 h_2)} &\equiv h_1 h_2 \pmod{p} \\ &\equiv g^{\log_g(h_1)} g^{\log_g(h_2)} \pmod{p} \\ &\equiv g^{\log_g(h_1)+\log_g(h_2)} \pmod{p} \\ \Rightarrow \log_g(h_1 h_2) &\equiv g^{\log_g(h_1)+\log_g(h_2)} \pmod{p-1}. \end{aligned}$$

□

(c) **Answer:**

Proof. Let $h \in \mathbb{F}_p^8$. Starting with the RHS, we have

$$\begin{aligned} g^{n \log_g(h)} &= \left(g^{\log_g(h)}\right)^n \\ &\equiv h^n \pmod{p} \\ &\equiv g^{\log_g(h^n)} \pmod{p} \\ \Rightarrow n \log_g(h) &\equiv \log_g(h^n) \pmod{p-1}. \end{aligned}$$

□