Student Number: [redacted] Name: Bryan Hoang

1. (10 points)

(a) **Answer:**

Proof. If a and b are cubic residues modulo p, then $p \nmid a$ and $p \nmid b$. Thus, $p \nmid ab$. We also have that $\exists\, c, d \in \mathbb{Z}$ such that

$$a \equiv c^3 \pmod p \qquad \text{and} \qquad b \equiv d^3 \pmod p.$$

It then follows that with $ab \in \mathbb{Z}$, $ab \equiv (cd)^3 \pmod p$. Therefore, ab is a cubic residue modulo p. □

(b) **Answer:**

Example. Let $p = 7$, $a \equiv 2 \pmod p$, and $b \equiv 4 \pmod p$. Then $ab \equiv 3 \pmod p$. But

$$\begin{aligned} 1^3 &\equiv 1 \pmod p \\ 2^3 &\equiv 1 \pmod p \\ 3^3 &\equiv 6 \pmod p \\ 4^3 &\equiv 1 \pmod p \\ 5^3 &\equiv 6 \pmod p \\ 6^3 &\equiv 6 \pmod p \\ (ab)^3 &\equiv 1 \pmod p. \end{aligned}$$

Therefore, a, b, and ab are not cubic residues modulo p.

(c) **Answer:**

Proof.

Part 1. ($\Rightarrow$) First, let's suppose that a is a cubic residue modulo p. Then $\exists b \in \mathbb{Z} : a \equiv b^3 \pmod p$. We also have that since g is a primitive root modulo p, $\exists c \in \mathbb{Z} : b \equiv g^c \pmod p$. Let $x = \log_g(a)$. Then

$$\begin{aligned} &\begin{cases} g^x \equiv a \pmod p \\ a \equiv b^3 \pmod p \end{cases} \\ \Rightarrow\ & g^x \equiv b^3 \pmod p \\ & g^x \equiv (g^c)^3 \pmod p \\ & g^x \equiv g^{3c} \pmod p \\ \Rightarrow\ & x = 3c \\ \Rightarrow\ & 3 \mid x \\ \Rightarrow\ & 3 \mid \log_g(a). \end{aligned}$$

Part 2. ($\Leftarrow$) Next, suppose that $3 \mid \log_g(a)$. Then $\exists b \in \mathbb{Z} : \log_g(a) = 3b$. Letting $x = \log_g(a)$, we have

$$\begin{aligned} g^x &\equiv a \pmod p \\ g^{3b} &\equiv a \pmod p \\ (g^b)^3 &\equiv a \pmod p \\ c^3 &\equiv a \pmod p && \text{where } c \equiv g^b \pmod p \text{ as } g \text{ is a primitive root} \end{aligned}$$

Thus, a is a cubic residue modulo p.

□

(d) **Answer:**

Proof. Let $p \equiv 2 \pmod 3$, let $a \in \mathbb{Z}$, and let g be a primitive root modulo p. Since $p \equiv 2 \pmod 3$, then

Student Number: [redacted] Name: Bryan Hoang

$\exists b \in \mathbb{Z} : p = 3b + 2$. By Fermat's Little Theorem, it follows that

$$\begin{aligned} g^{p-1} &= g^{3b+1} \\ &\equiv 1 \pmod{p} \\ \Rightarrow g^{6b+2} &\equiv 1 \pmod{p}. \end{aligned}$$

Also since g is a primitive root modulo, $\exists c \in \mathbb{Z} : a = g^c \pmod{p}$. Then by the previous two results,

$$a \equiv g^c \equiv g^{c+3b+1} \equiv g^{c+6b+2} \pmod{p}.$$

Exactly one of the elements in the set $\{c, c + 3b + 1, c + 3b + 2\}$ is divisible by 3. Let $x = \log_g(a)$ denote this element. Then $3 \mid x$. By part (c), we have that a is cube modulo p. $\square$