MTH26001- Elementary Number Theory.

Name: Nguyen Minh Duc

Student ID: 20202026

Quiz 3.

Problem 1.

- Since $50 = 2 \times 5^2$, 50 has a primitive root.
- ~~$\varphi(5)$~~ $\varphi(50) = \varphi(2)\varphi(5^2) = 1 \times 20 = 20$.

$3^1 \equiv 1 \pmod{50}$

$3^2 = 9 \pmod{50}$

$3^4 \equiv 9 \times 3^2 \equiv 81 \equiv 31 \pmod{50}$

$3^5 \equiv 3^4 \times 3^1 \equiv 31 \times 3 \equiv 93 \equiv 43 \pmod{50}$

$3^{10} \equiv 3^5 \times 3^5 \equiv 43 \times 43 \equiv 1849 \equiv 49 \pmod{50}$

$3^{20} \equiv 3^{10} \times 3^{10} \equiv 49 \times 49 \equiv 2401 \equiv 1 \pmod{50}$

$\Rightarrow$ 3 is a primitive root of 50.

- Since $\gcd(3, 50) = 1$, $3^3 \equiv 27 \pmod{50}$ is also a primitive root of 50.
- Thus, two primitive root of 50 is 3 and 27.

Problem 2.

- For $p = 3$, $7^{\frac{3-1}{2}} = 7^1 = 7 \equiv 1 \pmod 3$

$\Rightarrow$ 7 is a quadratic ~~root~~ residue of 3

$\Rightarrow \left(\frac{7}{3}\right) = 1$.

~~For p=5~~

- For $p = 5$, $7^{\frac{5-1}{2}} = 7^2 = 49 \equiv 4 \equiv -1 \pmod 5$

$\Rightarrow$ 5 is not a quadratic residue of 5)

$\Rightarrow \left(\frac{7}{3}\right) = -1$.

⊛ For $p > 7$, $\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right)$

$$\equiv p^{\frac{7-1}{2}} \pmod 7$$

$$\equiv p^3 \pmod 7$$

$p \bmod 7$	0	1	2	3	4	5	6
$p^3 \bmod 7$	0	1	1	-1	1	-1	1

Since any odd prime $p > 7$ is of the form $7k+3$ or $7k+5$,

$$p^3 \equiv -1 \pmod 7.$$

~~⇔ p is not a q.r.~~

$\Rightarrow \left(\frac{p}{7}\right) = -1$, $p > 7$

$\Rightarrow \left(\frac{7}{p}\right) = -1$, $p > 7$.