MTH 26001 - Elementary Number Theory
Student Name: Nguyen Minh Duc
Student ID: 20202026

ASSIGNMENT 7.

Sec 8.2

Problem 1.

(a) ⊗ Since p is odd, $2 \mid p-1$
By ~~coto~~ corollary of Theorem 8.5, the congruence

$$x^2 - 1 \equiv 0 \pmod p$$

has exactly 2 incongruent solutions.

⊗. Cleary, $x \equiv 1 \pmod p$ is a solution as $1^2 - 1 = 0 \equiv 0 \pmod p$.

$x \equiv p-1 \equiv -1 \pmod p$ is also a solution as $(-1)^2 - 1 = 1 - 1 = 0 \equiv 0 \pmod p$.

⊗ Therefore, the only incongruence solutions are 1 and $p-1$.

(b) ⊗ Clearly, $x \equiv 0 \pmod p$ is not a solution.

⊗ Consider $x \equiv 1, 2, \dots, p-1 \pmod p$ and they are coprime with p.

$\Rightarrow \gcd(x, p) = 1$. By Fermat's theorem,

$x^{p-1} \equiv 1 \pmod p$. $\Rightarrow x^{p-1} - 1 \equiv 0 \pmod p$

$\Rightarrow$ There are exactly $p-1$ solutions to $x^{p-1} - 1 \equiv 0 \pmod p$ ~~since~~ and they are

$1, 2, 3, \dots, p-1$ ($\because x \equiv 0 \pmod p$ is cleary not a solution).

⊗ Note that $x^{p-1} - 1 = (x-1)(x^{p-2} + x^{p-3} + \dots + x + 1)$.

Since p is odd, $p \geq 3 \Rightarrow p - 2 > 0$.

⊗ Since $x - 1 \equiv 0 \pmod p$ has exactly one solution $x \equiv 1 \pmod p$.

$\Rightarrow$ There must be $(p-1) - 1 = p-2$ solution for $x^{p-2} + x^{p-3} + \dots + x + 1 \equiv 0 \pmod p$

and they are $2, 3, 4, \dots, p-1$ ~~(∵ x ≡ 1 (mod p) is already solution to x − 1 ≡ 0 (mod p))~~

$x \equiv 1 \pmod p$ cannot be a solution to $x^{p-2} + x^{p-3} + \dots + x + 1 \equiv 0 \pmod p$

since $1^{p-2} + 1^{p-3} + \dots + 1 + 1 = p - 1 \not\equiv 0 \pmod p$.

Therefore, the $p-2$ solutions for $x^{p-2} + x^{p-3} + \dots + x + 1 \equiv 0 \pmod p$

are $x \equiv 2, 3, \dots, p-1 \pmod p$

Problem 4.

(a) Since 3 is a primitive ~~rood~~ root of 43, 3^k, $1 \leq k \leq 42$ are incongruent mod 43

or all integers less than 43 is congruent to 3^k.

~~Since ϕ Since $\phi(43) = 42$, $ord_{43}(3^k)$~~

Now, $ord_{43}(3) = \phi(43) = 42$, $ord_{43}(3^k) = \dfrac{42}{\gcd(k, 42)} = 6$.

$\Rightarrow \gcd(k, 42) = 7$.

$\Rightarrow k = 7$ or 35.

$\Rightarrow 3^7$ and 3^{35} have order 6 mod 43.

~~Now~~
Now, $3^7 \equiv 3^3 \times 3^4 \equiv 27 \times 81 \equiv 27 \times (-5) \equiv -135 \equiv 37 \pmod{43}$

$$3^{35} \equiv 3^{14} \times 3^{15} \times 3^{2} \equiv (3^7)^2 \times (3^7)^2 \times 3^4 \times 3^2 \equiv 37^2 \times 37^2 \times (-5) \times 9 \pmod{43}$$
$$\equiv (-6)^2 \times (-6)^2 \times (-45) \pmod{43}$$
$$\equiv 36 \times 36 \times (-2) \pmod{43}$$
$$\equiv (-7)(-7)(-2) \pmod{43}$$
$$\equiv -98 \pmod{43}$$
$$\equiv 7 \pmod{43}$$

There are 7 and 37 have order 6 mod 43.

(b) Similarly, $\frac{42}{\gcd(k,42)} = 21 \Rightarrow \gcd(k,42) = 2.$

$\Rightarrow k \in \{2, 2^2, 2^3, 2^4, 2^5, 2\times 5, 2\times 11, 2\times 13, 2\times 17, 2\times 19, 2^2\times 5, 2^3 \times 5\}.$

$\Rightarrow$ Numbers to consider: $3^2, 3^4, 3^8, 3^{10}, 3^{16}, 3^{20}, 3^{22}, 3^{26}, 3^{32}, 3^{34}, 3^{38}, 3^{40}$.

$$\left.\begin{aligned} 3^2 &\equiv 9 \\ 3^4 &\equiv 81 \equiv 38 \equiv -5 \\ 3^8 &\equiv (-5)^2 \equiv 25 \\ 3^{10} &\equiv 25 \times 9 \equiv 225 \equiv 10 \end{aligned}\right) \bmod 43 \quad \left.\begin{aligned} 3^{16} &\equiv 25^2 \equiv 23 \\ 3^{20} &\equiv 23 \times 38 \equiv 14 \\ 3^{22} &\equiv 14 \times 9 \equiv 40 \\ 3^{26} &\equiv 10 \times 23 \equiv 230 \equiv 15 \end{aligned}\right) \bmod 43 \quad \left.\begin{aligned} 3^{32} &\equiv 40 \times 10 \equiv 400 \equiv 13 \\ 3^{34} &\equiv 31 \\ 3^{38} &\equiv 17 \\ 3^{40} &\equiv 24 \end{aligned}\right) \bmod 43$$

Thus, 9, 10, 13, 14, 15, 17, 23, 24, 25, 31, 38, 40 all have order 21 mod 43.

Problem 6.

(a) By Fermat's theorem, $r^{p-1} \equiv 1 \pmod p \Rightarrow r^{p-1} - 1 \equiv 0 \pmod p$

Since p is odd, $p-1$ is even, then, $r^{p-1} - 1 = (r^{\frac{p-1}{2}} - 1)(r^{\frac{p-1}{2}} + 1) \equiv 0 \pmod p$.

If $r^{\frac{p-1}{2}} - 1 \equiv 0 \pmod p$, then since $\frac{p-1}{2} < p-1$, r won't have order $p-1$ mod p

$\Rightarrow r^{\frac{p-1}{2}} + 1 \equiv 0 \pmod p \Rightarrow r^{\frac{p-1}{2}} \equiv -1 \pmod p$.

(b) Assume rr' is another primitive root.

From part (a), $\left.\begin{aligned} r^{\frac{p-1}{2}} &\equiv -1 \pmod p \\ r'^{\frac{p-1}{2}} &\equiv -1 \pmod p \end{aligned}\right\} \Rightarrow (rr')^{\frac{p-1}{2}} \equiv 1 \pmod p$

But $\frac{p-1}{2} < p-1$, this contradicts assumption rr' is another primitive root.

Hence, rr' is not a primitive root.

(c) WLOG, assume that $1 \le r' \le p-1$.

If $r' \equiv 0 \pmod p$ Then $rr' \not\equiv 1 \pmod p$.

This implies $\gcd(r', p) = 1$.

Consider $(r')^k$ for $1 \le k \le p-1$.

If $k < p-1$ and $(r')^k \equiv 1 \pmod p$ then

$$1 \equiv 1^k \equiv (rr')^k \equiv r^k (r')^k \equiv r^k \pmod p,$$

contradicts r is primitive root mod p.

~~Hence, $k \ge p-1 \Rightarrow k = p-1$.~~

Hence $k = p-1$ or $(r')^k \not\equiv 1 \pmod p$, $1 \le k < p-1$

$$\Rightarrow \begin{cases} (r')^k \equiv (r')^{p-1} \equiv (r')^{p-1} r^{p-1} \equiv (r'r)^{p-1} \equiv 1 \pmod p \\ (r')^k \not\equiv 1, (1 \le k < p-1) \end{cases}$$

and $\gcd(r', p) = 1$.

Thus, r' is primitive root of p by definition.

Problem 7.

- Note that $n > 2$ and $2 \mid n$, $\varphi(n) \ge 2$.
- Let r be primitive root of $p \Rightarrow r^1, r^2, \dots, r^{p-1}$ are congruent to $1, 2, \dots, p-1$ in some order. and they are all incongruent to each other.

  Since $p > 3$, there are at least 3 elements on this list.
- Let $r' = r^{p-2} \Rightarrow r'$ and r are incongruent.

  $$r'r = r^{p-2} \cdot r = r^{p-1} \equiv 1 \pmod p$$
- Applying Problem 6(c), r' is a primitive root, which completes the proof.

Problem 11.

- r is primitive root $\Rightarrow r^1, r^2, \dots, r^{p-1}$ are congruent to $1, 2, \dots, p-1$ in some order

  $\Rightarrow$ other primitive root has the form r^k where $1 \le k \le p-1$.
- Note that ~~gcd(k,p~~ r^k will have order $p-1$ if $\gcd(k, p-1) = 1$.

  $\Rightarrow 1 \le k < p-1$.
- Let the $\varphi(p-1)$ primitive root of ~~x~~ p be $r^{k_1}, r^{k_2}, \dots, r^{k_{\varphi(p-1)}}$.

  $\Rightarrow$ The product is: $r^{k_1} r^{k_2} \dots r^{k_{\varphi(p-1)}} = r^{k_1 + k_2 + \dots + k_{\varphi(p-1)}}$

  By Theorem 7.7, $k_1 + k_2 + \dots + k_{\varphi(p-1)} = \frac{1}{2}(p-1)\varphi(p-1)$

  $$\Rightarrow r^{k_1} r^{k_2} \dots r^{k_{\varphi(p-1)}} = r^{1/2(p-1)\varphi(p-1)}$$

  By Theorem 7.4, $2 \mid \varphi(p-1)$, then $r^{1/2(p-1)\varphi(p-1)} \equiv (r^{p-1})^{1/2\varphi(p-1)} \equiv 1^{1/2\varphi(p-1)} \equiv 1 \pmod p$

  Since $\frac{1}{2}\varphi(p-1) \ge 1$ for $p > 2$.
- Now, since $2 \mid \varphi(p-1)$, $(-1)^{\varphi(p-1)} \equiv 1 \pmod p$.

  Therefore, $r^{k_1 + k_2 + \dots + k_{\varphi(p-1)}} \equiv (-1)^{\varphi(p-1)} \equiv 1 \pmod p$.

~~Prob~~

$\boxed{\text{Sec } 8.4}$

Problem 3.

(a) $x^{12} \equiv 13 \pmod{17}$, $\gcd(13,17)=1$.

$\Rightarrow 12\,ind_3 x \equiv ind_3 13 \pmod{16}$

$\Rightarrow 12\,ind_3 x \equiv 4 \pmod{16}$, $\gcd(12,16)=4$.

$\Rightarrow$ 4 incongruent solution.

Dividing by 4: $3\,ind_3 x \equiv 1 \pmod 4$

$\Rightarrow ind_3 x \equiv 3, 7, 11$ or 15.

$\Rightarrow x = 10, 11, 7, 6$ from table.

$\Rightarrow x \equiv 6, 7, 10, 11 \pmod{17}$

(b) $8x^5 \equiv 10 \pmod{17}$, $\gcd(10,17)=1$.

$\Rightarrow ind_3 8 + 5\,ind_3 x \equiv ind_3 10 \pmod{17}$

$\Rightarrow 10 + 5\,ind_3 x \equiv 3 \pmod{16}$

$\Rightarrow 5\,ind_3 x \equiv -7 \pmod{16}$, $\gcd(5,16)=1$.

$\Rightarrow 15\,ind_3 x \equiv -21 \pmod{16}$

$\Rightarrow -ind_3 x \equiv -21 \pmod{16}$

$\Rightarrow ind_3 x \equiv 21 \equiv 5 \pmod{16}$

$\Rightarrow x = 5$ from table.

$\Rightarrow x \equiv 5 \pmod{17}$

(c) $9x^8 \equiv 8 \pmod{17}$, $\gcd(8,17)=1$.

$\Rightarrow ind_3 9 + 8\,ind_3 x \equiv ind_3 8 \pmod{16}$

$\Rightarrow 2 + 8\,ind_3 x \equiv 10 \pmod{16}$

$\Rightarrow 8\,ind_3 x \equiv 8 \pmod{16}$, $\gcd(8,16)=8$.

$\Rightarrow ind_3 x \equiv 1 \pmod 2$

$\Rightarrow ind_3 x = 1, 3, 5, 7, 9, 11, 13, 15$

$\Rightarrow ind_3 x = 1, 3, 5, 7, 9, 11, 13, 15 \pmod{17}$

$\Rightarrow x \equiv 3, 10, 5, 11, 14, 7, 12, 6 \pmod{17}$

(d) $7^x \equiv 7 \pmod{17}$, $\gcd(7, 17) = 1$.

$\Rightarrow x\,\mathrm{ind}_3 7 \equiv \mathrm{ind}_3 7 \pmod{16}$

$\Rightarrow 11x \equiv 11 \pmod{16}$, $\gcd(11, 16) = 1$

$\Rightarrow x \equiv 1 \pmod{16}$

Problem 4.

⊗ Let $x \equiv 3^{24} \times 5^{13} \pmod{17}$, $\gcd(1, 17) = 1$.

$\Rightarrow \mathrm{ind}_3 x \equiv 24\,\mathrm{ind}_3 3 + 13\,\mathrm{ind}_{13} 5 \pmod{16}$

$\Rightarrow \mathrm{ind}_3 x \equiv 24 \times 1 + 13 \times 5 \pmod{16}$

$\Rightarrow \mathrm{ind}_3 x \equiv 89 \equiv 9 \pmod{16}$.

$\Rightarrow x \equiv 14 \pmod{17}$ from table.

⊗ Thus, $3^{24} \times 5^{13} \bmod 17 = 14$.

Problem 5.

⊗ Let $x = \mathrm{ind}_{r'} a \pmod{p}$

$y = \mathrm{ind}_r a \pmod{p}$

$z = \mathrm{ind}_{r'} r \pmod{p}$

⊗ From definition, $\begin{cases} (r')^x \equiv a \pmod{p} \\ r^y \equiv a \pmod{p} \\ (r')^z \equiv r \pmod{p} \Rightarrow (r')^{zy} \equiv r^y \pmod{p}. \end{cases}$

$\Rightarrow (r')^x \equiv r^y \equiv (r')^{zy} \equiv a \pmod{p}$

By Theorem 8.2, $x \equiv zy \pmod{p}$

$\Rightarrow \mathrm{ind}_{r'} a \equiv (\mathrm{ind}_r a)(\mathrm{ind}_{r'} r) \pmod{p-1}$.