MTH26001 - Elementary Number Theory
Name: Nguyen Minh Duc
Student ID: 20202026

ASSIGNMENT 4.

Sec 5.2

Problem 3.

* By Fermat's theorem, we obtain

$$11^{13-1} \equiv 1 \pmod{13} \quad (\because 13 \nmid 11).$$
$$\Rightarrow 11^{12} \equiv 1 \pmod{13}$$
$$\Rightarrow 11^{12n} \equiv 1 \pmod{13}. \quad (1)$$

* Moreover, $11^2 = 121 \equiv 4 \pmod{13}$

$$\Rightarrow 11^6 \equiv 4^3 \equiv 64 \equiv 12 \pmod{13}. \quad (2).$$

* From (1) and (2), $11^{12n+6} \equiv 12 \pmod{13}$.

$$\Rightarrow 11^{12n+6} + 1 \equiv 13 \equiv 0 \pmod{13}.$$
$$\Rightarrow 13 \mid 11^{12n+6} + 1.$$

Problem 10.

(a) Since $p \nmid a$, $p \nmid b$ and p is prime, by Fermat's theorem,

$$\begin{cases} a^p \equiv a \pmod p \\ b^p \equiv b \pmod p \end{cases}$$

However, $a^p \equiv b^p \pmod p$, thus, $a \equiv b \pmod p$.

(b) From (a), $a = b + pk$ $(k \in \mathbb{Z})$

$$\Rightarrow a^p - b^p = (b+pk)^p - b^p = \sum_{i=0}^{p} \binom{p}{i} b^{p-i}(pk)^i - b^p$$
$$\Rightarrow a^p - b^p = b^p + \binom{p}{1} b^{p-1} pk + \sum_{i=2}^{p} \binom{p}{i} b^{p-i}(pk)^i - b^p$$
$$\Rightarrow a^p - b^p = b^{p-1} p^2 k + \sum_{i=2}^{p} \binom{p}{i} b^{p-i}(pk)^i.$$
$$\Rightarrow a^p - b^p = p^2 \left[b^{p-1} k + \sum_{i=2}^{p} \binom{p}{i} b^{p-i} p^{i-2} k^i \right].$$
$$\Rightarrow p^2 \mid a^p - b^p$$
$$\Rightarrow a^p \equiv b^p \pmod{p^2}.$$

Problem 12.

⊛ $\binom{p-1}{k} = \frac{(p-1)!}{k!(p-k-1)!} = \frac{(p-1)(p-2)\dots(p-k)}{k!}$

$\Rightarrow k!\binom{p-1}{k} = (p-1)(p-2)\dots(p-k).$

$\Rightarrow k!\binom{p-1}{k} \equiv (-1)(-2)\dots(-k) \pmod p.$

$\Rightarrow k!\binom{p-1}{k} \equiv (-1)^k k! \pmod p.$ — ①

⊛ Since $p-1 \geq k \Rightarrow p > k \Rightarrow p \nmid 1, 2, \dots k \Rightarrow p \nmid k! \Rightarrow \gcd(p, k!) = 1.$ — ②

⊛ From ① and ②, $\binom{p-1}{k} \equiv (-1)^k \pmod p.$

Problem 13.

⊛ Since p, q are distinct prime, $\gcd(a, pq) = 1 \Rightarrow \gcd(a,p) = \gcd(a,q) = 1.$

$\Rightarrow \begin{cases} a^{p-1} \equiv 1 \pmod p \\ a^{q-1} \equiv 1 \pmod q \end{cases}$ ($\because$ Fermat's theorem).

⊛ Since $p-1 \mid q-1$, $q-1 = k(p-1)$, $k \in \mathbb{Z}$.

$\Rightarrow a^{p-1} \equiv 1 \pmod p \Rightarrow a^{k(p-1)} \equiv 1 \pmod p$

$\Rightarrow a^{q-1} \equiv 1 \pmod p$ — ①

Moreover, $a^{q-1} \equiv 1 \pmod q$ — ②.

⊛ From ① and ②, $\begin{cases} p \mid a^{q-1} - 1 \\ q \mid a^{q-1} - 1 \end{cases} \Rightarrow pq \mid a^{q-1} - 1$

$\Rightarrow a^{q-1} - 1 \equiv 0 \pmod{pq}$

$\Rightarrow a^{q-1} \equiv 1 \pmod{pq}.$

Problem 18.

(a) ⊛ By Fermat's theorem, $a^p \equiv a \pmod p$.

Then, $a^{n-1} = a^{2p-1} = a^{p-1}a^p \equiv a^{p-1}a \pmod p$

$\equiv a^p \equiv a \pmod p$.

$\Rightarrow p \mid a^{n-1} - a.\ \forall a$ — ①

⊛ case 1. a is even, a^{n-1} is also even, hence, $a^{n-1} - a$ is even $\Rightarrow 2 \mid a^{n-1} - a$.

case 2. a is odd, a^{n-1} is also odd, hence $a^{n-1} - a$ is even $\Rightarrow 2 \mid a^{n-1} - a$.

$\Rightarrow 2 \mid a^{n-1} - a\ \forall a$ — ②.

⊛ From ①, ② and $\gcd(2,p) = 1$ ($\because p$ is odd prime), $2p \mid a^{n-1} - a \Rightarrow n \mid a^{n-1} - a$

$\Rightarrow a^{n-1} \equiv a \pmod n$.

(b) let's consider each prime in 195 factorization.

- For $p=3$, if $3 \mid a$ then $3 \mid a^{193}$, thus, $3 \mid a^{193}-a \Rightarrow a^{193} \equiv a \pmod 3$.

  Otherwise, $3 \nmid a$, by Fermat's theorem,

  $$a^2 \equiv 1 \pmod 3 \Rightarrow a^{192} = a^{2\times 96} \equiv 1 \pmod 3.$$
  $$\Rightarrow a^{193} \equiv a \pmod 3.$$

  Hence, $a^{193} \equiv a \pmod 3 \ \forall a$.

- For $p=5$, if $5 \mid a \Rightarrow 5 \mid a^{193} \Rightarrow 5 \mid a^{193}-a \Rightarrow a^{193} \equiv a \pmod 3$.

  Otherwise, $5 \nmid a$, by Fermat's theorem,

  $$a^4 \equiv 1 \pmod 5 \Rightarrow a^{192} = a^{4\times 48} \equiv 1 \pmod 5$$
  $$\Rightarrow a^{193} \equiv a \pmod 5.$$

  Hence, $a^{193} \equiv a \pmod 5 \ \forall a$.

- For $p=13$, if $13 \mid a \Rightarrow 13 \mid a^{193} \Rightarrow 13 \mid a^{193}-a \Rightarrow a^{193} \equiv a \pmod{13}$

  Otherwise, $13 \nmid a$, by Fermat's theorem

  $$a^{12} \equiv 1 \pmod{13} \Rightarrow a^{192} = a^{12\times 16} \equiv 1 \pmod{13}$$
  $$\Rightarrow a^{193} \equiv a \pmod{13}$$

  Hence, $a^{193} \equiv a \pmod{13}$.

- Now, we combine the previous result: $\begin{cases} a^{193} \equiv a \pmod 3 \\ a^{193} \equiv a \pmod 5 \\ a^{193} \equiv a \pmod{13} \end{cases} \forall a.$

By Chinese Remainder theorem,

$$a^{193} \equiv a \pmod{\operatorname{lcm}(3,5,13)}$$
$$\Rightarrow a^{193} \equiv a \pmod{3\times 5\times 13}$$
$$\Rightarrow a^{193} \equiv a \pmod{195}$$
$$\Rightarrow a^{n-2} \equiv a \pmod n.$$

Sec 5.3

Problem 5.

(a) By Wilson's theorem,

$$n \text{ is prime} \Leftrightarrow (n-1)! \equiv -1 \pmod{n}$$
$$\Leftrightarrow (n-1)! \equiv n-1 \pmod{n}$$
$$\Leftrightarrow \frac{(n-1)!}{n-1} \equiv \frac{n-1}{n-1} \pmod{n} \quad (\because \gcd(n, n-1) = 1).$$
$$\Leftrightarrow (n-2)! \equiv 1 \pmod{n}$$

Thus, n is prime iff $(n-2)! \equiv 1 \pmod{n}$

(b) ⊗ For $0 < n < 4$, n is not composite

⊗ For $n = 4$, $(n-2)! \equiv (4-1)! \equiv 3! \equiv 6 \equiv 2 \pmod{4}$.
$\not\equiv 1 \pmod{4}$.

⊗ For $n > 4$, let $n = pq$ ($\because$ n is composite),
where $p, q \in \mathbb{Z}$, and $1 < p, q < n$.

⊗. Since $\gcd(n, n-1) = 1$, $\begin{cases} p \neq n-1 \\ q \neq n-1 \end{cases} \Rightarrow 1 < p, q < n-1$.
$\Rightarrow p, q \mid (n-1)!$.

⊗ If $p \neq q$, they are different factors of $(n-1)!$
$\Rightarrow pq \mid (n-1)! \Rightarrow n \mid (n-1)! \Rightarrow (n-1)! \equiv 0 \pmod{n}$

⊗ If $p = q \Rightarrow n = p^2$.
If $p \geq \frac{n}{2}$, $p^2 \geq \frac{n^2}{4} \Rightarrow 4p^2 \geq n^2 \Rightarrow 4n \geq n^2 \Rightarrow 4 \geq n$.
$\Rightarrow$ contradict the condition $n > 4$.
Then, $p < \frac{n}{2} \Rightarrow 2p < n \Rightarrow 2p \leq n-1$.
Since $p \neq 2p$, they are different factors of $(n-1)!$
$\Rightarrow p(2p) \mid (n-1)! \Rightarrow 2p^2 \mid (n-1)!$
$\Rightarrow p^2 \mid (n-1)!$ ($\because$ $2 \mid (n-1)!$).
$\Rightarrow n \mid (n-1)!$
$\Rightarrow (n-1)! \equiv 0 \pmod{n}$.

Thus, if n is composite, $(n-1)! \equiv 0 \pmod{n}$ except $n = 4$.

Problem 7.

- $p \mid a^p + (p-1)!$.

By Fermat's theorem, $a^p \equiv a \pmod p \quad \forall a$.

By Wilson's Theorem, $-1 \equiv (p-1)! \pmod p$.

$$\Rightarrow -a^p \equiv a(p-1)! \pmod p \Rightarrow a^p \equiv -a(p-1)! \pmod p$$

$$\hookrightarrow a^p + a(p-1)! \equiv 0 \pmod p$$

Thus, $p \mid a^p + a(p-1)!$.

- $p \mid (p-1)!\,a^p + a$.

From previous, $a^p \equiv a \pmod p$

$$(p-1)! \equiv -1 \pmod p$$

$$\Rightarrow a^p(p-1)! \equiv -a \pmod p$$

$$\Rightarrow a^p(p-1)! + a \equiv 0 \pmod p$$

Thus, $p \mid a^p(p-1)! + a$.

Problem 10.

(a) From Wilson's theorem,

$$(p-1)! \equiv -1 \pmod p$$

$$\Rightarrow \left(\frac{p-1}{2}\right)!\left(\frac{p+1}{2}\right)\left(\frac{p+3}{2}\right)\dots(p-1) \equiv -1 \pmod p$$

We have the congruences:

$$p-1 \equiv -1 \pmod p$$
$$p-2 \equiv -2 \pmod p$$
$$\vdots$$
$$\left(\frac{p+1}{2}\right) \equiv -\frac{p-1}{2} \pmod p.$$

Thus, we have: $\left(\frac{p-1}{2}\right)!\left(-\frac{p-1}{2}\right)\left(-\frac{p-3}{2}\right)\dots(-2)(-1) \equiv -1 \pmod p$

$$\Rightarrow \left(\frac{p-1}{2}\right)!\left(\frac{p-1}{2}\right)!(-1)^{\frac{p-1}{2}} \equiv -1 \pmod p.$$

$$\Rightarrow \left[\left(\frac{p-1}{2}\right)!\right]^2(-1)^{\frac{p-1}{2}} \equiv -1 \pmod p.$$

Since $p = 4k+3$, $\frac{p-1}{2} = 2k+1$, then $(-1)^{\frac{p-1}{2}} = -1$. This implies

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv 1 \pmod p.$$

$$\Rightarrow \left[\left(\frac{p-1}{2}\right)!\right]^2 - 1 \equiv 0 \pmod p$$

$$\Rightarrow \left[\left(\frac{p-1}{2}\right)! - 1\right]\left[\left(\frac{p-1}{2}\right)! + 1\right] \equiv 0 \pmod p$$

$$\Rightarrow \left(\frac{p-1}{2}\right)! - 1 \equiv 0 \pmod p \text{ or } \left(\frac{p-1}{2}\right)! + 1 \equiv 0 \pmod p$$

$$\Rightarrow \left(\frac{p-1}{2}\right)! \equiv 1 \pmod p \text{ or } \left(\frac{p-1}{2}\right)! \equiv -1 \pmod p$$

(b) Let $2, 4, 6, \ldots, n$ be all even integers less than p.

$\Rightarrow n = p-1$ ($\because$ p is an odd prime)

This list has $\frac{n}{2} = \frac{p-1}{2}$ elements.

⊗ Consider the product $2\cdot 4\cdot 6 \cdots n$, factoring out 2 of each element; we obtain

$$2\cdot 4\cdot 6\cdots n = 2^{\frac{p-1}{2}}\left(1\cdot 2\cdot 3\cdots\left(\tfrac{n}{2}\right)\right) = 2^{\frac{p-1}{2}}\left(\tfrac{n}{2}\right)! = 2^{\frac{p-1}{2}}\left(\tfrac{p-1}{2}\right)! \text{ — (1)}$$

⊗ Since $p \nmid 2$, by Fermat's theorem, $2^{p-1} \equiv 1 \pmod p$

$$\Rightarrow \left(2^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod p$$

$$\Rightarrow 2^{\frac{p-1}{2}} \equiv \pm 1 \pmod p \text{ — (2)}.$$

⊗ From (1) and (2), we have:

$$2\cdot 4\cdot 6\cdots n = 2^{\frac{p-1}{2}}\left(\tfrac{p-1}{2}\right)! \equiv \pm 1 \pmod p.$$

⊗ Thus, the product of all even integers less than p is congruent modulo p to either 1 or -1.

Problem 11.

⊗ $x^2 \equiv -1 \pmod{29}$.

Since $29 \equiv 1 \pmod 4$, there exists solutions.

From the proof of Theorem 5.5, we obtain the solutions:

$$x \equiv \pm\left(\tfrac{p-1}{2}\right)! \pmod p$$

$$\Rightarrow x \equiv \pm\left(\tfrac{29-1}{2}\right)! \pmod{29}$$

$$\Rightarrow x \equiv \pm 14! \pmod{29}.$$

⊗ $x^2 \equiv -1 \pmod{37}$

Since $37 \equiv 1 \pmod 4$, there exists solutions.

From the proof of Theorem 5.5, we obtain the solutions:

$$x \equiv \pm\left(\tfrac{p-1}{2}\right)! \pmod p$$

$$\Rightarrow x \equiv \pm\left(\tfrac{37-1}{2}\right)! \pmod{37}$$

$$\Rightarrow x \equiv \pm 18! \pmod{37}.$$