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

ASSIGNMENT 8.

Sec 9.1

Problem 1.

(a) $x^2+7x+10 \equiv 0 \pmod{11}$.

$\Leftrightarrow 4x^2+4\cdot 7\cdot x+40 \equiv 0 \pmod{11}$

$\Leftrightarrow 4x^2+2\cdot 7\cdot(2x)+7^2 \equiv 7^2-40 \pmod{11}$

$\Leftrightarrow (2x+7)^2 \equiv 9 \pmod{11}$.

Since $9^{\frac{11-1}{2}} = 9^5 \equiv 1 \pmod{11}$, the equation has solutions.

Note that $3^2 = 9 \equiv 9 \pmod{11}$

Hence, $2x+7 \equiv \pm 3 \pmod{11}$ ($\because$ 11 is prime).

$\Leftrightarrow \left[\begin{array}{l} 2x+7 \equiv 3 \pmod{11} \\ 2x+7 \equiv -3 \pmod{11} \end{array}\right. \Leftrightarrow \left[\begin{array}{l} 2x \equiv -4 \pmod{11} \\ 2x \equiv -10 \pmod{11} \end{array}\right.$

$\Leftrightarrow \left[\begin{array}{l} x \equiv -2 \equiv 9 \pmod{11} \\ 2x \equiv 1 \pmod{11} \Rightarrow 10x \equiv 5 \pmod{11} \Rightarrow x \equiv -5 \pmod{11} \Rightarrow x \equiv 6 \pmod{11} \end{array}\right.$

Thus, solutions are $x \equiv 6, 9 \pmod{11}$.

(b) $3x^2+9x+7 \equiv 0 \pmod{13}$

$\Leftrightarrow (6x+9)^2 \equiv 9^2-4\cdot 3\cdot 7 \pmod{13}$

$\Leftrightarrow (6x+9)^2 \equiv -3 \equiv 10 \pmod{13}$

Since $10^{\frac{13-1}{2}} = 10^6 \equiv 1 \pmod{13}$, the equation has solutions.

Note that $10 \equiv 10+2\cdot 13 \equiv 36 \pmod{13}$

Hence, $6x+9 \equiv \pm 6 \pmod{13}$.

$6x+9 \equiv 6 \pmod{13}$

$\Leftrightarrow 6x \equiv -3 \equiv 36 \pmod{13}$

$\Leftrightarrow x \equiv 6 \pmod{13}$

$6x+9 \equiv -6 \pmod{13}$

$\Leftrightarrow 6x \equiv -15 \equiv -2 \pmod{13}$

$\Leftrightarrow 12x \equiv -4 \pmod{13}$

$\Leftrightarrow -x \equiv -4 \pmod{13}$

$\Leftrightarrow x \equiv 4 \pmod{13}$.

Therefore, the solutions are $x \equiv 4, 6 \pmod{13}$

(c) $5x^2+6x+1 \equiv 0 \pmod{23}$

$\Leftrightarrow (10x+6)^2 \equiv 6^2 - 4\cdot5\cdot1 \pmod{23}$

$\Leftrightarrow (10x+6)^2 \equiv 16 \pmod{23}$

Since $16^{\frac{23-1}{2}} = 16^{11} \equiv 1 \pmod{23}$, the equation has solutions.

Note that $(\pm 4)^2 \equiv 16 \pmod{23}$

Hence, $10x+6 \equiv \pm 4 \pmod{23}$

$10x+6 \equiv 4 \pmod{23}$	$10x+6 \equiv -4 \equiv 19 \pmod{23}$
$\Leftrightarrow 10x \equiv -2 \pmod{23}$	$\Leftrightarrow 10x \equiv 13 \pmod{23}$
$\Leftrightarrow 20x \equiv -4 \pmod{23}$	$\Leftrightarrow 20x \equiv 26 \equiv 3 \pmod{23}$
$\Leftrightarrow -3x \equiv -4 \pmod{23}$	$\Leftrightarrow -3x \equiv 3 \pmod{23}$
$\Leftrightarrow -24x \equiv -32 \equiv -9 \pmod{23}$	$\Leftrightarrow x \equiv -1 \pmod{23}$
$\Leftrightarrow -x \equiv -9 \pmod{23}$	$\Leftrightarrow x \equiv 22 \pmod{23}$.
$\Leftrightarrow x \equiv 9 \pmod{23}$	

Thus, the solutions are $x \equiv 9, 22 \pmod{23}$.

Problem 2.

⊛ Consider $6x^2+5x+1=0 \Leftrightarrow x = \frac{-5 \pm \sqrt{5^2-4\cdot6\cdot1}}{2\cdot6}$

$\Leftrightarrow x = -\frac{1}{2}, -\frac{1}{3} \notin \mathbb{Z}$.

This implies $(2x+1)(3x+1)=0$.

$\Rightarrow (2x+1)(3x+1) \equiv 0 \pmod{p}$.

⊛ Now, $6x^2+5x+1 \equiv (2x+1)(3x+1) \equiv 0 \pmod{p}$.

$\Rightarrow 2x+1 \equiv 0 \pmod{p}$ or $3x+1 \equiv 0 \pmod{p}$.

⊛ If $p=2$, then $3x+1 \equiv 0 \pmod{2}$

$\Leftrightarrow 3x \equiv -1 \pmod{2} \Leftrightarrow x \equiv 1 \pmod{2}$.

Check: $6x^2+5x+1 \equiv 6(1)^2+5(1)+1 \equiv 12 \equiv 0 \pmod{2}$.

$\Rightarrow x \equiv 1 \pmod{2}$ is a solution. — ①

⊛ If p is an odd prime, then $2x+1 \equiv 0 \pmod{p}$

$\Leftrightarrow 2x \equiv -1 \equiv p-1 \pmod{p}$.

Note that $\gcd(2,p)=1$, there exists unique solution

$x \equiv 2^{-1}(p-1) \pmod{p}$,

which is also a solution for the original congruence. — ②.

⊛ From ① and ②, there is a solution for $6x^2+5x+1 \equiv 0 \pmod{p}$ for every prime p.

Scanned with CamScanner

Problem 4.

* Consider: $3^{\frac{23-1}{2}} \equiv 3^{11} \equiv 3^2(3^3)^3 \equiv 9(27)^3 \equiv 9(4)^3 \equiv 9\cdot 64 \equiv 9(-5) \pmod{23}$

$$\equiv -45 \pmod{23}$$
$$\equiv 1 \pmod{23}$$

$\Rightarrow$ 3 is a quadratic residue of 23.

* Consider: $3^{\frac{31-1}{2}} \equiv 3^{15} \equiv (3^3)^5 \equiv 27^5 \equiv (-4)^5 \equiv -4^3\cdot 4^2 \equiv (-64)\cdot 16 \pmod{31}$

$$\equiv (-2)\cdot 16 \pmod{31}$$
$$\equiv -32 \pmod{31}$$
$$\equiv -1 \pmod{31}$$

$\Rightarrow$ 3 is a ~~non~~ quadratic nonresidue of 31.

Problem 7.

* Let q be a quadratic nonresidue of $p \Rightarrow a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

Since $p = 2^k + 1$ is prime, $k \geq 1$ and $p-1 = 2^k \Rightarrow \frac{p-1}{2} = 2^{k-1}$.

This implies $q^{\frac{p-1}{2}} \equiv q^{2^{k-1}} \equiv -1 \pmod p$ —— (1).

$\Rightarrow (q^{2^{k-1}})^2 \equiv q^{2^k} \equiv 1 \pmod p$.

Note that $\varphi(p) = p - 1 = 2^k$ ($\because p$ is prime).

* Let $n = ord_p(q) \Rightarrow n \mid 2^k$.
* If $n \neq 2^k$ then $n = 2^r$ where $0 \leq r < k$.

$\Rightarrow q^{2^r} \equiv 1 \pmod p$. —— (2).

* If $r = k-1$ then $q^{2^{k-1}} \equiv 1 \pmod p$, contradicts (1).
* If $r < k-1$ then squaring (2), $k-1-r$ times,

$$(q^{2^r})^2 \equiv q^{2\cdot 2^r} \equiv q^{2^{r+1}} \equiv 1 \pmod p.$$
$$\Rightarrow (q^{2^{r+1}})^2 \equiv q^{2\cdot 2^{r+1}} \equiv q^{2^{r+2}} \equiv 1 \pmod p$$
$$\Rightarrow (q^{2^{k-2}})^2 \equiv q^{2\cdot 2^{k-2}} \equiv q^{2^{k-1}} \equiv 1 \pmod p,$$

which contradicts (1).

* Therefore $n = 2^k$, which implies a is primitive root of p.

Sec 9.2

Problem 3.

- Recall that there are $\frac{p-1}{2}$ quadratic residues of p and $\frac{p-1}{2}$ quadratic nonresidues of p.
- If q is a ~~quadratic~~ quadratic residue of p, it cannot be a primitive root since $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ and $\frac{p-1}{2} < p-1 = \phi(p)$.
- If r is a primitive root of p, it must be congruent to a quadratic ~~nor~~ nonresidue of p.
- Let S be the set of quadratic nonresidues of $p \Rightarrow |S| = \frac{p-1}{2}$.

  $\Rightarrow$ ~~root~~ $r \equiv x$ ~~for~~ $\pmod p$ for some ~~for~~ $x \in S$.
- By corollary of Theorem 8.6, there are $\phi(p-1)$ primitive roots of p

  $\Rightarrow$ There are $\phi(p-1)$ elements of S are primitive roots of p.

  $\Rightarrow$ There are $\frac{p-1}{2} - \phi(p-1)$ elements of S are not primitive root of p.

Problem 4(a)

$x^2 + py + a = 0$, $\gcd(a, p) = 1$.

- Suppose the equation has a solution, then.

  $$x^2 + a = -yp \Rightarrow x^2 + a \equiv 0 \pmod p \Rightarrow x^2 \equiv -a \pmod p$$

  This implies $(-a)$ is a quadratic residue of $p \Rightarrow \left(\frac{-a}{p}\right) = 1$. — ①
- If $\left(\frac{-a}{p}\right) = 1$ then $(-a)$ is a quadratic residue of p

  $\Rightarrow x^2 \equiv -a \pmod p$ has a solution.

  $\Rightarrow x^2 = -a - yp$ has a solution

  $\Rightarrow x^2 + yp + a = 0$ has a solution. — ②.
- From ① and ②, the equation has solutions iff $\left(\frac{-a}{p}\right) = 1$.

Problem 7.

- Note that $\gcd(a,p)=1$, then $\exists a': a'a \equiv 1 \pmod p$. for $1 \le a \le p-2$.
- $a \in [1,p-2]$ and $a' \in [1,p-2]$. Note that it's not $p-1$ since if $a'=p-1$, $a(p-1)\equiv 1 \pmod p \Rightarrow ap-a \equiv -a \equiv 1 \pmod p \Rightarrow a+1 \equiv 0 \equiv p \pmod p \Rightarrow a \equiv p-1 \pmod p$ $\Rightarrow a = p-1$, a contradiction ↯.
- . Also, if $a'a_1 \equiv 1 \pmod p$ and $a'a_2 \equiv 1$ then $a_1a' \equiv a_2a' \pmod p$
  $\Rightarrow a_1a' = a_2a'$
  $\Rightarrow a_1 = a_2$.
- As a runs from $1 \to p-2$, each a' from $1 \to p-2$ is represented only once.
- As a runs from $1 \to p-2$, $1+a'$ runs from $2 \to p-1$.
- Now, $a'a \equiv 1 \pmod p \Rightarrow a + aa' \equiv a+1 \pmod p$

$$\Rightarrow a(1+a') \equiv a+1 \pmod p$$
$$\Rightarrow a^2(1+a') \equiv a(a+1) \pmod p$$
$$\Rightarrow \left(\frac{a(a+1)}{p}\right) = \left(\frac{a^2(1+a')}{p}\right) = \left(\frac{1+a'}{p}\right)$$
$$\Rightarrow \sum_{a=1}^{p-2}\left(\frac{a(a+1)}{p}\right) = \sum_{a'=2}^{p-1}\left(\frac{1+a'}{p}\right)$$
$$= \sum_{a=2}^{p-1}\left(\frac{a'}{p}\right)$$
$$= \sum_{a=2}^{p-1}\left(\frac{a}{p}\right)$$
$$= \sum_{a=1}^{p-1}\left(\frac{a}{p}\right) - \left(\frac{1}{p}\right)$$
$$= 0 - 1 \quad (\because \text{Theorem } 9.4).$$
$$= -1.$$

Problem 8.

(a) Since p, q are odd, $\gcd(2,q)=1$

Since $\varphi(q) = q-1 = 2p$, Order of -4 must be $1, 2, p$ or $2p$. mod q.

- If $-4 \equiv 1 \pmod q$ then $5 \equiv 0 \pmod q \Rightarrow q \mid 5$ but $q > 5$ since p is odd
  $\Rightarrow$ contradiction.
- If $(-4)^2 \equiv 1 \pmod q$ then $15 \equiv 0 \pmod q \Rightarrow q \mid 15 \Rightarrow q = 3$ or 5 but $q > 5$ since p is odd
  $\Rightarrow$ contradiction.
- If $(-4)^p \equiv 1 \pmod q$. Now, $(-4)^p = (-4)^{\frac{q-1}{2}} \equiv 1 \pmod q$ ($\because$ 4 is a quadratic residue)
  $\Rightarrow \left(\frac{-4}{q}\right) = 1$ —— ①.

However, $\left(\frac{-4}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{2}{q}\right)\left(\frac{2}{q}\right)$.

Now, $\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}} = (-1)^{p} = -1$ ($\because p$ is odd).

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

if $p \equiv 1 \pmod 4$ then $p = 4k+1 \Rightarrow q = 8k+3$.

$\Rightarrow q \equiv 3 \pmod 8$

$\Rightarrow \left(\frac{2}{q}\right) = 1$.

$\Rightarrow \left(\frac{-4}{q}\right) = (-1)(1)(1) = -1$, contradicts 1.

if $p \equiv 3 \pmod 4$, then $p = 4k+3 \Rightarrow q = 8k+7$.

$\Rightarrow q \equiv 7 \pmod 8 \Rightarrow q \equiv -1 \pmod 8$

$\Rightarrow \left(\frac{2}{q}\right) = 1$

$\Rightarrow \left(\frac{-4}{q}\right) = (-1)(1)(1) = -1$, contradicts 1.

This means $(-4)^p \not\equiv \pmod q$, so order of -4 mod q is not p.

Therefore, $\text{ord}_q(-4) = 2p = q-1 = \phi(q)$.

$\Rightarrow -4$ is the primitive root of $q = 2p+1$.

(b) Consider $\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{2}{p}\right)$

$= (1)\underbrace{(\pm 1)(\pm 1)}_{\text{The same}}$ ($\because$ corollary of theorem 9.2)

$= 1$.

$\Rightarrow -4$ is a quadratic residue of p. — 1

Since $\gcd(4,p) = 1$ then

$x^2 \equiv \frac{p-1}{4} \pmod p \Leftrightarrow 4x^2 \equiv p-1 \pmod p$

$\Leftrightarrow (2x)^2 \equiv -1 \pmod p$

This congruence has solutions by corollary of theorem 9.2.

$\Rightarrow x^2 \equiv \frac{p-1}{4} \pmod p$ has a solution.

$\Rightarrow \frac{p-1}{4}$ is a quadratic residue of p — 2.

From 1 and 2, -4 and $\frac{p-1}{4}$ both are quadratic residues of p.