PROBLEM I When p is prime, $p > 2, A \mid p^{\alpha}$, find all the solution of $y^2 \equiv A \pmod{p^{\alpha}}$.

SOLUTION . Since $A \mid p^{\alpha}$, then it is equal to find the solution of $y^2 \equiv 0 \pmod{p^{\alpha}}$. Next, we will prove that the solution of $y^2 \equiv 0 \pmod{p^{\alpha}}$ are $\{y \in \mathbb{Z} : V_p(y) \geq \frac{\alpha}{2}\}$.

Let $y = \prod_{r \in P} r^{V_r(y)}$, where P is all the prime, $V_r(n) = \min\{k \in \mathbb{N} : r^k \mid n\}, r \in P, n \in \mathbb{Z}$. If $p^{\alpha} \mid y^2 = \prod_{r \in P} r^{2V_r(y)}$, then $V_p(y) \geq 1$ and $\alpha \mid 2V_p(y)$. So $\frac{\alpha}{2} \leq V_p(y)$.

And obviously, $\forall y : V_p(y) \geq \frac{\alpha}{2}$, then $V_p(y^2) = 2V_p(y) \geq \alpha$, then $p^{\alpha} \mid y^2$. □

PROBLEM II Prove:

$$ax^2 + bx + c \equiv 0 \pmod{m}, \gcd(2a, m) = 1$$

has solution. $\iff$

$$x^2 \equiv q \pmod{m}, q = b^2 - 4ac$$

has solutions, which can infer the solution of $ax^2 + bx + c \equiv 0 \pmod{m}$.

SOLUTION . Since $\gcd(2a, m) = 1$, then $2 \nmid m, a \nmid m$, then $\gcd(4a, m) = 1$. So the solution of $ax^2 + bx + c \equiv 0 \pmod{m} \iff$ it is the solution of $(2ax + b)^2 + (4ac - b^2) \equiv 0 \pmod{m} \implies y^2 + 4ac - b^2 \equiv 0 \pmod{m}$, where $y \equiv 2ax + b \pmod{m}$. Since $\gcd(2a, m) = 1$, then the solution of $y^2 + 4ac - b^2 \equiv 0 \pmod{m}$ y, we let $x \equiv A(y - b) \pmod{m}$, where $A(2a) \equiv 1 \pmod{m}$, x is the solution of $(2ax + b)^2 + (4ac - b^2) \equiv 0 \pmod{m}$.

□

PROBLEM III Find out all the squared remainder and non squared remainder of 37.

SOLUTION . By the Theorem 2 on page 65 of text book, we can get that $\{k^2 + 37t : 1 \leq k \leq 18, t \in \mathbb{Z}\} = \{k + 37t : t \in \mathbb{Z}, k \in A\}$, where $A := \{1, 4, 9, 16, 25, 36, 12, 27, 7, 26, 10, 33, 21, 11, 3, 34, 30, 28\}$ are squared remainder. And $\{k + 37t : t \in \mathbb{Z}, k \in B\}$, where $B = \mathbb{N}^+ \cap [0, 36] \setminus A$ are non squared remainder. □

PROBLEM IV

1. Use the conclusion in the formar chapters, prove: there must exist quadratic residue and non quadratic residue in the reduced residue system of p.

2. Assume x_1, x_2 are quadratic residues, X_3 is non quadratic residue: prove $x_1 x_2$ is quadratic residue, $x_1 x_3$ is non quadratic residue.

3. Apply the conclusions above, prove that both the quadratic residue and the non quadratic residue in the reduced residue system of p have $\frac{p-1}{2}$ elements.

PROBLEM V Prove: the solution of $x^2 \equiv a \pmod{p^{\alpha}}, \gcd(\alpha, p) = 1$ is $x \equiv \pm PQ' \pmod{p^{\alpha}}$, where

$$P = \frac{(z + \sqrt{\alpha})^{\alpha} + (z - \sqrt{\alpha})^{\alpha}}{2}, Q = \frac{(z + \sqrt{\alpha})^{\alpha} - (z - \sqrt{\alpha})^{\alpha}}{\sqrt{\alpha}},$$

$$z^2 \equiv \alpha \pmod{p}, QQ' \equiv 1 \pmod{p^{\alpha}}.$$

PROBLEM VI Prove the solution of $x^2 + 1 \equiv 0 \pmod{p}, p = 4m + 1$ is $x \equiv \pm 1 \cdot 2 \cdot \cdots \cdot (2m) \pmod{p}$.