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 $p^\alpha \mid y^2$. $\square$

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 $\gcd(4a, m) = 1$. $ax^2 + bx + c \equiv 0 \pmod{m}$ has solutions $\iff$ $(2ax + b)^2 + (4ac - b^2) \equiv 0 \pmod{m}$ has solutions. $\implies$:$y^2 + 4ac - b^2 \equiv 0 \pmod{m}$, 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 $(2ax + b)^2 + (4ac - b^2) \equiv 0 \pmod{m}$. $\impliedby$: $(2ax + b)^2 + (4ac - b^2) \equiv 0 \pmod{m}$ has solution x, then $2ax + b$ is the solution of $ax^2 + bx + c \equiv 0 \pmod{m}$, same way as above. $\square$

PROBLEM III Find out all the squared remainder and non quadratic 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. $\square$

PROBLEM IV

1. Use the conclusion in the former 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_1x_2 is quadratic residue, x_1x_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.

SOLUTION.

1. Obviously, 1 is quadratic residue of p. Consider function $f : \mathbb{Z}_p \setminus \{0\} \to \mathbb{Z}_p \setminus \{0\}, i \to i^2$. When $p > 2$, if every elements in $\mathbb{Z}_p \setminus \{0\}$ is quadratic residue, then f is bijective. But $1 \not\equiv -1 \pmod{p}$ and $f(-1) \equiv f(1) \equiv 1 \pmod{p}$, then f is not surjective, contradiction! Then there must exist non-quadratic residue of p.

2. Assume $x_1 \equiv y_1^2, x_2 \equiv y_2^2 \pmod p$, then $x_1x_2 \equiv y_1^2y_2^2 \pmod p$. Then x_1x_2 is quadratic residue. Since $y_1 \not\equiv 0 \pmod p$, then $\exists z$ such that $y_{1z} \equiv 1 \pmod p$. If $x_1x_3 \equiv t^2 \pmod p), \exists t$. Then $x_3 \equiv z^2x_1x_3 \equiv (zt)^2 \pmod p$, contradiction!

3. Recall f, we only need to prove $|f(\mathbb{Z}_p \backslash \{0\})| = \frac{p-1}{2}$. For every $x \in f(\mathbb{Z}_p \backslash \{0\})$, consider $x \equiv y^2 \pmod p$. Then $\exists y$ such that $x \equiv y^2 \pmod p$. If $y_1^2 \equiv y_2^2 \equiv \pmod p$, then $p \mid (y_1+y_2)(y_1-y_2)$, then $y_2 \equiv \pm y_1 \pmod p$. Then $|f^{-1}(x)| \leq 2$. On the other hand, easy to prove that $y \not\equiv 0 \pmod p \to y \not\equiv -y \pmod p$, and $x \equiv y^2 \pmod p \to x \equiv (-y)^2 \pmod p$. So $|f^{-1}(x)| = 2$. Then
$$\sum_{x \in f(\mathbb{Z}_p \backslash \{0\})} 2 = \sum_{x \in f(\mathbb{Z}_p \backslash \{0\})} \sum_{y \in \mathbb{Z}_p, x \equiv y^2} 1 = \sum_{y \in \mathbb{Z}_p \backslash \{0\}} \sum_{x \equiv y^2} 1 = \sum_{y \in \mathbb{Z}_p \backslash \{0\}} 1 = p-1$$
Therefore, $|f(\mathbb{Z}_p \setminus \{0\})| = \frac{p-1}{2}$.

$\square$

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
$$P = \frac{(z+\sqrt{\alpha})^\alpha + (z-\sqrt{\alpha})^\alpha}{2}, Q = \frac{(z+\sqrt{\alpha})^\alpha - (z-\sqrt{\alpha})^\alpha}{\sqrt{\alpha}},$$
$$z^2 \equiv \alpha \pmod p, QQ' \equiv 1 \pmod{p^\alpha}.$$

SOLUTION. First, if $x^2 \equiv a \pmod{p^\alpha}$ has solution, then $z^2 \equiv a \pmod p$ has solution. So we only need to prove that if $z^2 \equiv a \pmod p$ has solution, then $\pm PQ'$ is the solution of $x^2 \equiv a \pmod{p^\alpha}$. Easy to get that $P + \sqrt{a}Q = (z+\sqrt{a})^\alpha$ and $P - \sqrt{a}Q = (z-\sqrt{a})^\alpha$. So $P^2 - aQ^2 = ((z+\sqrt{a})(z-\sqrt{a}))^\alpha = (z^2-a)^\alpha$. Since $z^2 \equiv a \pmod p$, we know $p \mid z^2 - a$, so $p^\alpha \mid P^2 - aQ^2$. So $P^2 \equiv aQ^2 \pmod p$. So $x^2 \equiv P^2Q'^2 \equiv aQ^2Q'^2 \equiv a \pmod p$. $\square$

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

SOLUTION. Easy to know that $x^2 \equiv \prod_{i=1}^{2m} i \prod_{i=1}^{2m} i \equiv \prod_{i=1}^{2m} i (-1)^{2m} \prod_{i=1}^{2m} -i \equiv \prod_{i=1}^{4m} i \pmod p$. So we only need to prove that for $p \in \mathbb{P} \land p \neq 2, (p-1)! \equiv -1 \mod p$. It is obvious by Wilson's Theorem. $\square$