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

SOLUTION . Since $p^\alpha \mid A$, then it is equal to find the solution of $y^2 \equiv 0 \pmod{p^\alpha}$. Easy to prove that $p^\alpha \mid y^2 \iff p^{\lceil \frac{\alpha}{2} \rceil} \mid y$. So all the solutions are $y = kp^{\lceil \frac{\alpha}{2} \rceil}, k \in \mathbb{Z}$. $\square$

PROBLEM II Prove:

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

$\iff$

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

SOLUTION . Since $\gcd(2a, m) = 1$, we can get $\gcd(4a, m) = 1$. So $ax^2 + bx + c \equiv 0 \mod m \iff (2ax+b)^2 \equiv b^2 - 4ac \mod m$. Let $y = 2ax+b$, and let t satisfy $2at \equiv 1 \mod m$, then $x \equiv t(y-b) \mod m$. So the two equation has solution at same condition, and $ax^2 + bx + c \equiv 0 \mod m \iff x \equiv t(y-b) \mod m \wedge y^2 \equiv b^2 - 4ac \mod m$. $\square$

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

SOLUTION . Only need to calculate $\{m^2 \mod 37 : m \in \mathbb{Z}, 1 \leq m \leq 18\}$.
They are $\{1, 4, 9, 16, 25, 36, 12, 27, 7, 26, 10, 33, 21, 11, 3, 34, 30, 28\}$. So squared remainder of 37 are $\{1, 4, 9, 16, 25, 36, 12, 27, 7, 26, 10, 33, 21, 11, 3, 34, 30, 28\}$, and non-squared remainder of 37 are $\{2, 5, 6, 8, 13, 14, 15, 17, 18, 19, 20, 22, 23, 24, 29, 31, 32, 35\}$. $\square$

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, where $p \in \mathbb{P} \wedge p \neq 2$.
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 $1 \equiv 1^2 \mod p$, so 1 is quadratic residue. Consider the function $f : \mathbb{Z}_p \setminus \{0\} \to \mathbb{Z}_p \setminus \{0\}, i \mapsto i^2$. If every element is quadratic residue, then f is surjective. Then f is bijective. But since $p > 2$, we know $1 \not\equiv -1 \mod p$ and $f(1) \equiv 1 \equiv f(-1) \mod p$, contradiction! So there must exist non-quadratic residue of p.
2. Assume $x_1 \equiv y_1^2, x_2 \equiv y_2^2 \mod p$, then $x_1x_2 \equiv y_1^2y_2^2 \mod p$, so x_1x_2 is quadratic residue. Since $y_1 \not\equiv 0 \mod p$, we know there exists z such that $y_1z \equiv 1 \mod p$. So if $x_1x_3 \equiv t^2 \mod p$ for some t, then $x_3 \equiv z^2x_1x_3 \equiv (zt)^2 \mod p$, contradict to x_3 is non-quadratic.

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

PROBLEM V Prove: the solution of $x^2 \equiv a \pmod{p^\alpha}, \gcd(a, p) = 1$ 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 $x^2 \equiv a \mod p^\alpha$ has solution, then $z^2 \equiv a \mod p$ has solution. So we only need to prove that if $z^2 \equiv a \mod p$ has solution, then $\pm PQ'$ is solution of $x^2 \equiv a \mod p^\alpha$. 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 $z^2 \equiv a \mod p$, we know $p \mid z^2 - a$, so $p^\alpha \mid P^2 - aQ^2$. So $P^2 \equiv aQ^2 \mod p$. So $x^2 \equiv P^2 Q'^2 \equiv aQ^2 Q'^2 \equiv a \mod p$. □

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 $x^2 \equiv \prod_{i=1}^{2m} i \prod_{i=1}^{2m} i \equiv \prod_{i=1}^{2m} i (-1)^{2m} \prod_{i=1}^{2m} -i \equiv \prod_{i=1}^{4m} i \mod p$. 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. □