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 $\{y \in \mathbb{Z} : V_p(y) \geq \frac{\alpha+1}{2}\}$.

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 $\frac{\alpha+1}{2} \leq V_p(y)$.

And obviously, $\forall y : V_p(y) \geq \frac{\alpha+1}{2}$, 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 $\gcd(4a, m) = 1$. 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 $(2ax + b)^2 + (4ac - b^2) \equiv 0 \pmod{m}$.

$\square$