PROBLEM I Find the number of all the intergal solution of equations as follow:

1. $x^2 \equiv 3766 \pmod{5987}$;
2. $x^2 \equiv 3149 \pmod{5987}$. Where 5987 is a prime.

SOLUTION. 1.

$$\begin{aligned}
\left(\frac{3766}{5987}\right) &= \left(\frac{2^3}{5987}\right)\left(\frac{471}{5987}\right) = \left(\frac{2}{5987}\right)(-1)^{\frac{5986}{2}\frac{470}{2}}\left(\frac{5987}{471}\right) \\
&= (-1)^{\frac{5987^2-1}{8}}(-1)\left(\frac{5987}{471}\right) = \left(\frac{-136}{471}\right) = \left(\frac{2}{471}\right)\left(\frac{17}{471}\right)\left(\frac{-1}{471}\right) \\
&= (-1)^{\frac{471^2-1}{8}}(-1)^{\frac{471-1}{2}\frac{17-1}{2}}\left(\frac{471}{17}\right)(-1)^{\frac{471-1}{2}} \\
&= -\left(\frac{-5}{17}\right) = -(-1)^{16}\left(\frac{5}{17}\right) \\
&= -\left(\frac{17}{5}\right) = -\left(\frac{2}{5}\right) = -(-1)^{\frac{5^2-1}{8}} = -(-1)^3 = 1
\end{aligned} \tag{1}$$

Since 5987 is prime, then $x^2 \equiv 3766 \pmod{5987}$ has 2 solutions.

2.

$$\begin{aligned}
\left(\frac{3149}{5987}\right) &= \left(\frac{-311}{5987}\right) = \left(\frac{-1}{5987}\right)\left(\frac{311}{5987}\right) = (-1)^{\frac{5987-1}{2}}\left(\frac{78}{311}\right) \\
&= -\left(\frac{2}{311}\right)\left(\frac{3}{311}\right)\left(\frac{13}{311}\right) = -(-1)^{\frac{311^2-1}{8}}(-1)^{\frac{310}{2}\frac{2}{2}}\left(\frac{311}{3}\right)(-1)^{\frac{310}{2}\frac{12}{2}}\left(\frac{311}{13}\right) \\
&= \left(\frac{2}{3}\right)(-1)\left(\frac{-1}{13}\right) = (-1)^{\frac{3^2-1}{8}}(-1)(-1)^{\frac{13-1}{2}} = 1
\end{aligned} \tag{2}$$

Since 5987 is prime, then $x^2 \equiv 3149 \pmod{5987}$ has 2 solutions.

$\square$

PROBLEM II

1. When the equation has solutions, apply theorm 1 in section 2 to find the solution of $x^2 \equiv a \pmod{p}, p = 4m+3$.
2. When the equation has solutions, apply theorem 1 in section 2 and section 3 to find the solution of $x^2 \equiv a \pmod{p}, p = 8m+5$.
3. If the equation $x^2 \equiv a \pmod{p}, p = 8m+1$ has solutions, and N is non quadratic residue. Give one way to solve the equation above.

1. Since the equation has solution, we know that $a^{\frac{p-1}{2}} \equiv 1 \mod p$. So $a^{2m+1} \equiv 1 \mod p$. So $a^{2m+2} \equiv a \mod p$. So $(a^{m+1})^2 \equiv a \mod p$. So the solution is $x \equiv \pm a^{m+1} \mod p$.
2. Since the equation has solution, we know that $a^{\frac{p-1}{2}} \equiv 1 \mod p$, then $a^{4m+2} \equiv 1 \mod p$. So $a^{2m+1} \equiv \pm 1 \mod p$. If $a^{2m+1} \equiv 1 \mod p$, then we have $(a^{m+1})^2 \equiv a \mod p$, so $x \equiv \pm a^{m+1} \mod p$. Else, since $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = -1$, we have $2^{4m+2} \equiv -1 \mod p$. So $2^{4m+2}a^{2m+2} \equiv a \mod p$. So $x \equiv \pm 2^{2m+1}a^{m+1} \mod p$.

3. For the same reason, we easily get that $a^{4m} \equiv 1 \mod p$ and $N^{4m} \equiv -1 \mod p$. We can find the solution by following method:

   (a) let $x = 4m, y = 0$.

   (b) if $2 \nmid x$, goto 3e.

   (c) If $a^{\frac{x}{2}} N^{\frac{y}{2}} \equiv 1 \mod p$, then let $x = \frac{x}{2}, y = \frac{y}{2}$. If $a^{\frac{x}{2}} N^{\frac{y}{2}} \equiv -1 \mod p$, then let $x = \frac{x}{2}, y = \frac{3y}{2}$.

   (d) goto 3b.

   (e) Now we have $2 \nmid x, 2 \mid y, a^x N^y \equiv 1 \mod p$. So $x \equiv a^{\frac{x+1}{2}} N^{\frac{y}{2}} \mod p$.

   It is easy to prove that this method can end because every turn the calue of $v_2(x)$ will -1. And easy to prove that $2 \mid y$ because we can use MI to prove that $v_2(y) > v_2(x)$.

PROBLEM III Solve the following equations

1. $x^2 \equiv 59 \pmod{125}$.
2. $x^2 \equiv 41 \pmod{64}$.

SOLUTION. 1. First solve $x^2 \equiv 4 \mod 5$. Solution is $x \equiv \pm 2 \mod 5$. Second solve $x^2 \equiv 9 \mod 25$, assume $x = 5y \pm 2$, easy to get that $x \equiv \pm 3 \mod 25$. Finally solve $x^2 \equiv 59 \mod 125$ and assume $x = 25y \pm 3$. Easily $x \equiv \pm 53 \mod 125$. So the solution is $x \equiv \pm 53 \mod 125$.

2. Easy to find that $x \equiv \pm 13, \pm 19 \mod 64$.

□

PROBLEM IV

1. Prove equation $x^2 \equiv 1 \pmod{m}$ and $(x+1)(x-1) \equiv 0 \pmod{m}$ are equal.
2. Apply 1 to give one way of finding all the solutions of $x^2 \equiv 1 \pmod{m}$.

SOLUTION. 1. Obviously because $x^2 - 1 = (x+1)(x-1)$.

2. We can solve the equation by this way:

   (a) Dissolve m into product of primes, write $m = 2^\alpha \prod_{i=1}^{n} p_i^{\alpha_i}$.

   (b) For $p_i^{\alpha_i}$, easy to get that solution of $x^2 \equiv 1 \mod p_i^{\alpha_i}$ is $x \equiv \pm 1 \mod p_i^{\alpha_i}$.

   (c) For 2^α, if $\alpha \geq 1$, we need to find solution of $x^2 \equiv 1 \mod 2^\alpha$. When $\alpha = 1$, the solution is $x \equiv 1 \mod 2$. When $\alpha = 2$, the solution is $x \equiv 1, 3 \mod 4$. When $\alpha \geq 3$, the solution is $x \equiv \pm 1, \pm(2^{\alpha-1} + 1) \mod 2^\alpha$.

   (d) Use Chinese Reminder Theorem to find all the solution of $x^2 \equiv 1 \mod m$.

□