PROBLEM I Use the method in the contexts of this section to judge whether these equations below have solutions.

1. $x^2 \equiv 429 \pmod{563}$
2. $x^2 \equiv 680 \pmod{769}$
3. $x^2 \equiv 503 \pmod{1013}$

where $503, 563, 796, 1013$ are prime.

SOLUTION.

1. $\left(\frac{429}{563}\right) = \left(\frac{3}{563}\right)\left(\frac{11}{563}\right)\left(\frac{13}{563}\right) = (-1)^{\frac{(2+10+12)*562}{4}}\left(\frac{563}{3}\right)\left(\frac{563}{11}\right)\left(\frac{563}{13}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{11}\right)\left(\frac{4}{13}\right) = (-1)(-1)^{\frac{11^2-1}{8}}(1) = 1.$
2. $\left(\frac{680}{769}\right) = \left(\frac{170}{769}\right) = \left(\frac{2}{769}\right)\left(\frac{5}{769}\right)\left(\frac{17}{769}\right) = (-1)^{\frac{769^2-1}{8}+\frac{(4+16)768}{4}}\left(\frac{769}{5}\right)\left(\frac{769}{17}\right) = \left(\frac{4}{5}\right)\left(\frac{4}{17}\right) = 1.$
3. $\left(\frac{503}{1013}\right) = (-1)^{\frac{502\times1012}{4}}\left(\frac{1013}{503}\right) = \left(\frac{7}{503}\right) = (-1)^{\frac{6\times502}{4}}\left(\frac{503}{7}\right) = -\left(\frac{6}{7}\right) = -\left(\frac{-1}{7}\right) = -(-1)^3 = 1.$

$\square$

PROBLEM II Find out the expression of the prime with the quadratic residue -2; Find out the expression of the prime with the non-quadratic residue -2;

SOLUTION. Easy to get that $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(p-1)(p+5)}{8}}$. So $\left(\frac{-2}{p}\right) = 1 \iff 16 \mid (p-1)(p+5) \iff 4 \mid \frac{p-1}{2}\frac{p+5}{2}$. Since $\frac{p+5}{2} - \frac{p-1}{2} = 3 \equiv 1 \mod 2$, we know they can't be all even. So $4 \mid \frac{p-1}{2} \vee 4 \mid \frac{p+5}{2}$, so $p \equiv 1, 3 \mod 8$. So $\left(\frac{-2}{p}\right) = 1 \iff p \equiv 1, 3 \mod 8$, and $\left(\frac{-2}{p}\right) = -1 \iff p \equiv 5, 7 \mod 8$. $\square$

PROBLEM III Assume $n \in \mathbb{N}_+$, $4n+3, 8n+7$ are prime, prove:

$$2^{4n+3} \equiv 1 \pmod{8n+7}$$

Thus, prove that $23 \mid (2^{11}-1), 47 \mid (2^{23}-1), 503 \mid (2^{251}-1)$.

SOLUTION. In fact we don't need $4n+3$ is prime. Since $2^{\frac{8n+7-1}{2}}\left(\frac{2}{8n+7}\right) = (-1)^{\frac{(8n+7)^2-1}{8}} = (-1)^{8n^2+14n+6} = 1$, we easily get that $2^{4n+3} \equiv 1 \mod 8n+7$. We let $n = 2, 5, 62$, then we get $23 \mid (2^{11}-1), 47 \mid (2^{23}-1), 503 \mid (2^{251}-1)$. $\square$

PROBLEM IV Find out the expression of the prime with the quadratic residue ±3; which prime has the non-quadratic residue ±3?

SOLUTION. Assume $p > 3$. Easy to get that $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)$. And $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$. So $\left(\frac{-3}{p}\right) = 1 \iff p \equiv 1 \mod 3$, and $\left(\frac{-3}{p}\right) = -1 \iff p \equiv 2 \mod 3$. And $\left(\frac{3}{p}\right) = 1 \iff (p \equiv 1 \mod 3 \wedge p \equiv 1 \mod 4) \vee (p \equiv 2 \mod 3 \wedge p \equiv 3 \mod 4) \iff p \equiv 1, 11 \mod 12$. So $\left(\frac{3}{p}\right) = 1 \iff p \equiv 1, 11 \mod 12$, and $\left(\frac{3}{p}\right) = -1 \iff p \equiv 5, 7 \mod 12$. $\square$

PROBLEM V Find out the expression of the prime with the minimum non-quadratic residue 3.

SOLUTION. Only need to solve $\left(\frac{2}{p}\right) = 1 \wedge \left(\frac{3}{p}\right) = -1$. Easy to know that $\left(\frac{2}{p}\right) = 1 \iff p \equiv 1, 7 \mod 8$. And from IV we know that $\left(\frac{3}{p}\right) = 1 \iff p \equiv 1, 11 \mod 12$. So finally we get that $p \equiv 1, 23 \mod 24$. So $p \in \mathbb{P}$ with minimum non-quadratic 3 $\iff p \equiv 1, 23 \mod 24$. $\square$