57. (a) Clearly $p = 2$ doesn't satisfy this.

- If $p \equiv 1 \pmod 8$, then we have
$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) = 1 \cdot 1 = 1$$
- If $p \equiv 3 \pmod 8$, then we have
$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) = (-1) \cdot (-1) = 1$$
- If $p \equiv 5 \pmod 8$, then we have
$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) = 1 \cdot (-1) = -1$$
- If $p \equiv 7 \pmod 8$, then we have
$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) = (-1) \cdot 1 = -1.$$

Therefore, we have $\left(\frac{-2}{p}\right) = 1$ if and only if $p \equiv 1, 3 \pmod 8$.

(b) Let's first find all the primes $p \equiv 1 \pmod 4$ satisfying the equation. For $p \equiv 1 \pmod 4$, by the Law of Quadratic Reciprocity, we have
$$\left(\frac{7}{p}\right) = 1 \iff \left(\frac{p}{7}\right) = 1 \iff p \equiv 1, 2, 4 \pmod 7.$$
Combining $\pmod 4$ and $\pmod 7$ congruences, we find
$$p \equiv 1, 9, 25 \pmod{28}.$$
Next,we deal with the case $p \equiv 3 \pmod 4$ similarly. By the Law of Quadratic Reciprocity, we have
$$\left(\frac{7}{p}\right) = 1 \iff \left(\frac{p}{7}\right) = -1 \iff p \equiv 3, 5, 6 \pmod 7.$$
Combining $\pmod 4$ and $\pmod 7$ congruences, we find
$$p \equiv 3, 19, 27 \pmod{28}.$$
Clearly $p = 2$ satisfies the equation as well. Therefore, we have $\left(\frac{7}{p}\right) = 1$ if and only if $p \equiv 1, 3, 9, 19, 25, 27 \pmod{28}$ or $p = 2$.

58. We begin with writing
$$\left(\frac{814}{2003}\right) = \left(\frac{2}{2003}\right) \cdot \left(\frac{11}{2003}\right) \cdot \left(\frac{37}{2003}\right).$$

- From the fact that
$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8 \\ -1 & \text{if } p \equiv 3, 5 \pmod 8 \\ 0 & \text{if } p = 2, \end{cases}$$
we have $\left(\frac{2}{2003}\right) = -1$.
- Using the Law of Quadratic Reciprocity,
$$\left(\frac{11}{2003}\right) = -\left(\frac{2003}{11}\right) = -\left(\frac{1}{11}\right) = -1.$$

- Using the Law of Quadratic Reciprocity again,

$$\left(\frac{37}{2003}\right)=\left(\frac{2003}{37}\right)=\left(\frac{5}{37}\right)=\left(\frac{37}{5}\right)=\left(\frac{2}{5}\right)=-1.$$

Therefore, we have

$$\left(\frac{814}{2003}\right)=\left(\frac{2}{2003}\right)\cdot\left(\frac{11}{2003}\right)\cdot\left(\frac{37}{2003}\right)=(-1)\cdot(-1)\cdot(-1)=-1.$$

59. (a) Let g be a primitive root modulo p, then $\{g^2, g^4, g^6, \cdots, g^{p-1}\}$ will be the set of all quadratic residues. Then, we have

$$g^2+g^4+\cdots+g^{p-1}\equiv\frac{g^{p+1}-g^2}{g^2-1}\equiv 0 \pmod p$$

because

$$p+1\equiv 2 \pmod{p-1}\Longrightarrow g^{p+1}\equiv g^2 \pmod p\Longrightarrow p \text{ divides } g^{p+1}-g^2$$

while

$$p>3\Longrightarrow g^2\not\equiv 1 \pmod p\Longrightarrow p\nmid g^2-1.$$

(b) One can use a similar technique with the previous part, but we will show a different method here.
We know that if a is a quadratic residue, then so is $a^{-1} \pmod p$. By pairing up every quadratic residue with its inverse, we will get some product equivalent to $1 \pmod p$. However, 1 and -1 cannot be paired up since they are their own inverses.
If $p\equiv 3 \pmod 4$, then -1 is not a quadratic residue and therefore the product will still be $1 \pmod p$.
If $p\equiv 1 \pmod 4$, then -1 is a quadratic residue and therefore the product will be changed to $-1 \pmod p$.
Finally, note that this is same as $(-1)^{\frac{p+1}{2}} \pmod p$.

60. Let's write $m=\frac{p+1}{4}+n(n+1)$, then we have

$$4m=p+1+4n^2+4n\equiv 4n^2+4n+1\equiv(2n+1)^2 \pmod p.$$

If $4m$ is not a unit modulo p, i.e. divisible by p, then m is also divisible by p.
Assume $4m$ is a unit modulo p now. Then $4m\equiv(2n+1)^2 \pmod p$ is a quadratic residue modulo p and hence

$$\left(\frac{4m}{p}\right)=1\Longrightarrow\left(\frac{4}{p}\right)\cdot\left(\frac{m}{p}\right)=1\Longrightarrow\left(\frac{m}{p}\right)=1.$$

61. First we note that the first congruence doesn't have ay solution for $p=2$ and both of the congruences have solutions for $p=3$ and $p=11$. Assume now that $p\neq 2,3,11$. We have

$$x^2-x+3\equiv 0 \pmod p\Longrightarrow 4x^2-4x+12\equiv 0 \pmod p\Longrightarrow(2x-1)^2+11\equiv 0 \pmod p\Longrightarrow\left(\frac{-11}{p}\right)=1,$$

which gives $\left(\frac{-99}{p}\right)=1$, i.e. there exists an integer a such that $a^2+99\equiv 0 \pmod p$. Clearly, we can choose a as an odd integer by considering $a+p$ instead of a if necessary. Writing $a=2y-1$, we have

$$(2y-1)^2+99\equiv 0 \pmod p\Longrightarrow 4y^2-4y+100\equiv 0 \pmod p\Longrightarrow y^2-y+25\equiv 0 \pmod p.$$

Note: The idea is that the solubility of both of the given congruences is more or less equivalent to -11 being a quadratic residue modulo p.

62. (a) Suppose $p\neq 3$. Then

$$\begin{aligned}-3\equiv(2n)^2 \pmod p&\Longrightarrow\left(\frac{-3}{p}\right)=1\\&\Longrightarrow\left(\frac{-1}{p}\right)\cdot\left(\frac{3}{p}\right)=1\\&\Longrightarrow(-1)^{\frac{p-1}{2}}\cdot(-1)^{\frac{p-1}{2}}\cdot\left(\frac{p}{3}\right)=1\\&\Longrightarrow\left(\frac{p}{3}\right)=1\\&\Longrightarrow p\equiv 1 \pmod 3.\end{aligned}$$

(b) Assume there are finitely many of them, say $p_1, p_2, \cdots, p_k$, and consider $m = 4(p_1 p_2 \cdots p_k)^2 + 3$. By the previous part, m must be divisible by 3 or p_i for some i, but obviously that's not possible because

$$m \equiv 3 \not\equiv 0 \pmod{p_i} \text{ and } m \not\equiv 0 \pmod{3}.$$

63. 43 is a quadratic residue modulo 923 if and only the congruence

$$x^2 \equiv 43 \pmod{923}$$

has a solution. By the Chinese Remainder Theorem, we can rewrite it as the combination of two congruences

$$x^2 \equiv 43 \pmod{13}$$

and

$$x^2 \equiv 43 \pmod{71}.$$

The first congruence has a solution because

$$\left(\frac{43}{13}\right) = \left(\frac{4}{13}\right) = 1$$

and similarly the second congruence also has a solution since

$$\left(\frac{43}{71}\right) = -\left(\frac{71}{43}\right) = -\left(\frac{28}{43}\right) = -\left(\frac{7}{43}\right) = \left(\frac{43}{7}\right) = \left(\frac{1}{7}\right) = 1.$$

Therefore, 43 is indeed a quadratic residue modulo 923. Moreover, both of the congruences have two solutions and by the Chinese Remainder Theorem, the original congruence

$$x^2 \equiv 43 \pmod{923}$$

has 4 solutions in $\mathbb{Z}_{923}$.

64. See `https://number.subwiki.org/wiki/Smallest_quadratic_nonresidue_is_less_than_square_root_plus_one`