1. for $p=2$ the quadratic has a solution $x \equiv 1 \pmod 2$ as

$$6(1)^2+5(1)+1 \equiv 6+6 \equiv 12 \overset{\checkmark}{\equiv} 0 \pmod 2$$

thus we can consider only odd primes p WLOG

via the law of quadratic reciprocity we can prove the existence of solutions for the remaining odd primes via the equivalent congruence

$$6x^2+5x+1 \equiv 0 \pmod p.$$

$$(2ax+b)^2 \equiv (b^2-4ac) \pmod p$$

$$y^2 \equiv (5^2-4\cdot 6\cdot 1) \equiv 1 \pmod p$$

and $\gcd(1,p)=1 \ \forall p \in \mathbb{Z}^+$.

Because 1 raised to any power is 1 itself theorem 9.1 (Euler's criterion) can be used as to show there are solutions to the system as 1 is a quadratic residual. Additionally there exist trivial solutions of $y \equiv -1 \pmod p$ and $y \equiv 1 \pmod p$

$$(1)^{(p-1)/2} = 1 \equiv 1 \pmod p$$

And thus, because the equivalent congruence has solutions the original does too.

2. By definition, the set of all quadratic residues mod p is $\{1^2, 2^2, \ldots, (p-1)^2\}$ however as a result of the congruence $x^2 \equiv (x-p)^2 \pmod p$, the last $\frac{p-1}{2}$ are congruent to the first $\frac{p-1}{2}$, leaving the smallest set as $\{1^2, 2^2, \ldots, (\frac{p-1}{2})^2\}$ #

3. Via theorem 9.1

a. because $\gcd(3,23)=1$ and $3^{((23-1)/2)} \equiv 3^{11} \equiv 1 \pmod{23}$ theorem 9.1 tells us that 3 is a quadratic residue of 23

b. because $\gcd(3,31)=1$ we can use theorem 9.1 and $3^{\frac{31-1}{2}} \equiv 3^{15} \equiv 30 \equiv -1 \pmod{31}$ to prove that 3 is a quadratic non-residue of 31.

4. a is quadratic residue of odd prime p.

A. according to Euclids criterion, a is a quadratic residue of an odd prime p iff

$$a^{(p-1)/2} \equiv 1 \pmod p$$

thus giving it an order of $(p-1)/2$ mod p which is lower than the $\phi(p) = p-1$ it would need to be a primitive root of p.

Therefore by contradiction, a cannot be a primitive root of p. #

b. $p \equiv 3 \pmod 4 \Rightarrow x = \pm a^{(p+1)/4}$ solves $x^2 \equiv a \pmod p$

if we assume that $a \neq p$ to avoid trivial solutions gcd(a, p) = 1 allowing us to use gauss's criterion

$$x^2 \equiv a^{(p-1)/2} \pmod p$$

$$x \equiv \pm a^{(p-1)/4} \pmod p$$

if $\gcd(a,p) \neq 1$ then it must be $\gcd(a,p) = p$ by definition of primes and thus $x \equiv \pm a^{(p+1)/4} \equiv 0 \equiv p^2$ and thus also the solution.

5. a. $(19/23) = (-4/23) = (-1/23)(4/23) = \left((-1)^{\frac{23-1}{2}}\right)(2^2/23) = -1 \cdot 1 = -1$

b. $(-23/59) = (36/59) = (6^2/59) = 1$

because 15 is odd power

c. $(29/31) = (-2/31) \equiv (-2)^{\frac{31-1}{2}} \equiv -(2^{15}) \equiv -32768 \equiv -1 \pmod{31}$

d. $(18/43) = (-25/43) = (-1/43)\cancel{(5^2/43)} = (-1)^{\frac{43-1}{2}} = (-1)^{21} = -1$

6. a. $(8/11)$

$S = \{8\cdot1, 8\cdot2, 8\cdot3, 8\cdot4, 8\cdot5\}$

$= \{8, 16, 24, 32, 40\}$ $\qquad 11/2 = 5.5$

$\equiv \{8, \cancel{5}, \cancel{2}, 10, 7\} \pmod{11}$

3 exceed $5.5 = 11/2$

$\therefore (8/11) = (-1)^3 = -1$

b. $(7/13)$

$S = \{7\cdot1, 7\cdot2, 7\cdot3, 7\cdot4, 7\cdot5, 7\cdot6\} = \{7, 14, 21, 28, 35, 42\}$

$\equiv \{7, \cancel{1}, 8, \cancel{2}, 9, \cancel{3}\} \pmod{13}$

3 exceed $13/2 = 6.5$

$\therefore (7/13) = (-1)^3 = -1$

c. $(5/19)$

$S = \{5\cdot1, 5\cdot2, 5\cdot3, 5\cdot4, 5\cdot6, 5\cdot7, 5\cdot8, 5\cdot9\} = \{5, 10, 15, 20, 25, 30, 35, 40, 45\}$

$\equiv \{\cancel{5}, 10, 15, \cancel{1}, \cancel{6}, 11, 16, \cancel{2}, \cancel{7}\} \pmod{19}$

4 exceed $19/2 = 9.5$

$\therefore (5/19) = (-1)^4 = 1$