9.1 | 3(a) For an odd prime p, its quadratic residues are the unique elements (mod p) of $\{1^2, 2^2, \ldots, (p-1)^2\}$. Note that $(p-k)^2 = p^2 - 2kp + k^2 \equiv k^2 \pmod{p}$, so that $1^2 \equiv (p-1)^2$, $2^2 \equiv (p-2)^2$, ..., up to $\left(\frac{p-1}{2}\right)^2 \equiv \left(\frac{p+1}{2}\right)^2 \pmod{p}$. We also know that p has exactly $\left(\frac{p-1}{2}\right)$ quadratic residues, so they are congruent to $\{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\}$. ∎

3(b) quadratic residues of 17:

$1^2 \equiv 1$; $2^2 \equiv 4$; $3^2 \equiv 9$; $4^2 \equiv 16$; $5^2 \equiv 25 \equiv 8$; $6^2 \equiv 2$;

$7^2 \equiv 15$; $8^2 \equiv 13$ $\longrightarrow$ $\{1, 2, 4, 8, 9, 13, 15, 16\}$ ←

---

5 a: quadratic residue of the odd prime p

(a) Euler's criterion $\Rightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod p$, so the order of a is $< p-1 \Rightarrow a$ is not a primitive root of p. ∎

(b) Note that $p-a \equiv -a \pmod p$. check 2 cases:

$p \equiv 1 \pmod 4 \Rightarrow p = 4k+1 \Rightarrow \frac{p-1}{2} = 2k \Rightarrow (-a)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \equiv 1 \pmod p$,

so $-a$ is a quadratic residue of p. (Euler's criterion)

$p \equiv 3 \pmod 4 \Rightarrow p = 4k+3 \Rightarrow \frac{p-1}{2} = 2k+1 \Rightarrow (-a)^{\frac{p-1}{2}} = -a^{\frac{p-1}{2}} \equiv -1 \pmod p$,

so $-a$ is a quadratic nonresidue of p. ∎

(c) $p \equiv 3 \pmod 4 \Rightarrow p = 4k+3 \Rightarrow \frac{p+1}{4} = k+1$, $\frac{p+1}{2} = 2(k+1)$, even.

Then $x = \pm a^{\frac{p+1}{4}} \Rightarrow x^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} \cdot a \equiv a \pmod p$,

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

so $x^2 \equiv a \pmod p$. ∎

11 (a) 2 is a primitive root of 19

quadratic residues of 19: $\{2^2, 2^4, 2^6, \ldots, 2^{18}\}$

reduce mod 19: $2^2 \equiv 4$, $2^4 \equiv 16$, $2^6 \equiv 7$, $2^8 \equiv 9$, $2^{10} \equiv 17$,

$2^{12} \equiv 11$, $2^{14} \equiv 6$, $2^{16} \equiv 5$, $2^{18} \equiv 1$

$\Rightarrow \{1, 4, 5, 6, 7, 9, 11, 16, 17\}$

(b) quadratic residues of 29: 2 is a primitive root (see page 156),

so they are $2^2 \equiv 4$, $2^4 \equiv 16$, $2^6 \equiv 6$, $2^8 \equiv 24$, $2^{10} \equiv$ [redacted] 9,

$2^{12} \equiv 7$, $2^{14} \equiv 28$, $2^{16} \equiv 25$, $2^{18} \equiv 13$, $2^{20} \equiv 23$,

$2^{22} \equiv 5$, $2^{24} \equiv 20$, $2^{26} \equiv 22$, $2^{28} \equiv 1$

$\Rightarrow \{1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28\}$

quadratic residues of 31: 3 is a primitive root, so they are

[redacted], [redacted], [redacted] $3^2 \equiv 9$, $3^4 \equiv 19$, $3^6 \equiv 16$, $3^8 \equiv 20$, $3^{10} \equiv 25$,

$3^{12} \equiv 8$, $3^{14} \equiv 10$, $3^{16} \equiv 28$, $3^{18} \equiv 4$, $3^{20} \equiv 5$, $3^{22} \equiv 14$, $3^{24} \equiv 2$, $3^{26} \equiv 18$,

$3^{28} \equiv 7$, $3^{30} \equiv 1 \Rightarrow \{1, 4, 5, 2, 8, 9, 10, 7, 14, 16, 18, 19, 20, 25, 28\}$

9.2 3 If p is an odd prime, its primitive roots are quadratic nonresidues; there are $\frac{p-1}{2}$ quadratic nonresidues and $\varphi(\varphi(p)) = \varphi(p-1)$ primitive roots, so $\frac{p-1}{2} - \varphi(p-1)$ of the quadratic nonresidues are not primitive roots.

4(a) p an odd prime, $\gcd(a,p)=1$ (as usual!)

$\left(\frac{-a}{p}\right) = 1 \iff -a$ is a quadratic residue, so there exists an x s.t. $x^2 \equiv -a \pmod p \iff x^2 + a = py$ for some y

$\iff x^2 - py + a = 0 \iff x^2 + p(-y) + a = 0$.

↑ call this y!

4(b) $\left(\frac{+2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \pmod 8 \\ -1, & p \equiv \pm 3 \pmod 8 \end{cases}$

Thus, $x^2 + 7y - 2 = 0$ has integer solutions iff $p \equiv \pm 1 \pmod 8$.

7 For each a with $\gcd(a,p)=1$, let a' be the unique solution of $aa' \equiv 1 \pmod p$. Then

$$\left(\frac{a(a+1)}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a+1}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a+aa'}{p}\right) = \left(\frac{a^2}{p}\right)\left(\frac{1+a'}{p}\right) = \left(\frac{1+a'}{p}\right),$$

so $$\sum_{a=1}^{p-2}\left(\frac{a(a+1)}{p}\right) = \sum_{a'=1}^{p-2}\left(\frac{1+a'}{p}\right) = \underbrace{\left(\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\right)}_{0} - \left(\frac{1}{p}\right) = -1.$$

□

12 $r^2 r^4 \cdots r^{p-1} = r^{2+4+\cdots+(p-1)} = r^{2(1+2+\cdots\frac{p-1}{2})} = r^{2(\frac{p-1}{2}\cdot\frac{p+1}{2}\cdot\frac{1}{2})}$

$= r^{\frac{p^2-1}{4}}$ = product of quadratic residues

$r \cdot r^3 \cdot \ldots \cdot r^{p-2} = r^{1+3+\cdots+(p-2)} = r^{(\frac{p-1}{2})^2}$ since $p-2 = 2(\frac{p-1}{2})-1$

= product of quadratic nonresidues