9.1.1b Solve the quadratic congruence $3x^2 + 9x + 7 \equiv 0 \pmod{13}$
Observe.

$$\begin{aligned}(6x^2+9)^2 &\equiv 81 - 12(7) \pmod{13}\\ &\equiv -3 \pmod{13}\\ &\equiv 10 \pmod{13}\end{aligned}$$

Let $y = 6x^2 + 9$. Then we have,

$$y^2 \equiv 10 \pmod{13} \Rightarrow y^2 - 10 \equiv 0 \pmod{13} \Rightarrow y^2 - 36 \equiv 0 \pmod{13}$$

Thus, $y = 6 \pmod{13}$ or $y = 7 \pmod{13}$

$$\begin{aligned}6x+9 &\equiv 6 \pmod{13}\\ 6x &\equiv -3 \pmod{13}\\ 6x &\equiv 36 \pmod{13}\\ x &\equiv 6 \pmod{13}\end{aligned} \qquad \begin{aligned}6x+9 &\equiv 7 \pmod{13}\\ 6x &\equiv -2 \pmod{13}\\ 12x &\equiv -4 \pmod{13}\\ x &\equiv 4 \pmod{13}\end{aligned}$$

Thus, $x \equiv 4 \pmod{13}$ or $x \equiv 6 \pmod{13}$

9.1.04 Show that 3 is a quadratic residue of 23, but a non-residue of 31.
Observe.

$$\begin{aligned}3^{(23-1)/2} = 3^{11} = 3^2(3^3)^3 = 9(27)^3 &\equiv 9(4)^3 \pmod{23}\\ &\equiv 9(64) \pmod{23}\\ &\equiv 9(-5) \pmod{23}\\ &\equiv -45+46 \pmod{23}\\ &\equiv 1 \pmod{23}\end{aligned}$$

Thus, $3^{(23-1)/2} \equiv \pmod{23} \Rightarrow 3$ is a quadratic residue of 23
Observe.

$$\begin{aligned}3^{(31-1)/2} = 3^{15} = (3^3)^5 = (27)^5 &\equiv (-4)^5 \pmod{31}\\ &\equiv -4^3 \cdot -4^2 \pmod{31}\\ &\equiv 16(-64) \pmod{31}\\ &\equiv 16(-64+62) \pmod{31}\\ &\equiv -32 \pmod{31}\\ &\equiv -1 \pmod{31}\end{aligned}$$

Thus, $3^{(31-1)/2} \equiv -1 \pmod{31} \Rightarrow 3$ is a quadratic non-residue of 31

9.1.07 If $p = 2^k + 1$ is prime, verify that every quadratic non-residue of p is a primitive root of p.
Let a be a quadratic non-residue of p. Then by Euler's Criterion for some $k \in \mathbb{Z}^+$,

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

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

Let n be the order of a modulo p, then $n|2^k$. Notice if $n \neq 2^k$, then $n = 2^r$ for $r < k$. Thus, we have $a^{2^r} \equiv 1 \pmod{p}$. If $r = k-1$, we then have a contradiction from $a^{2^{k-1}} \equiv -1 \pmod{p}$. Otherwise, if $r < k-1$, we then get

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

Which is a contradiction from $a^{2^{k-1}} \equiv -1 \pmod{p}$.
Thus, the order of a must be a primitive root.