9.1.1 (b) Solve
$$3x^2 + 9x + 7 \equiv 0 \pmod{13}.$$

We first multiply both sides by 4(3). Then

$$4(3)(3x^2+9x+7) = 4 \cdot 3^2 \cdot x^2 + 4 \cdot 3 \cdot 9x + 4 \cdot 3 \cdot 7 = (2 \cdot 3 \cdot x)^2 + 2 \cdot (2 \cdot 3 \cdot x) \cdot 9 + 4 \cdot 3 \cdot 7.$$

We then add $b^2 = 81$ to both sides of the congruence. So

$$(2 \cdot 3 \cdot x)^2 + 2 \cdot (2 \cdot 3 \cdot x) \cdot 9 + 81 + 4 \cdot 3 \cdot 7 \equiv 81 \pmod{13}.$$

Then factoring gives
$$(2 \cdot 3 \cdot x + 9)^2 \equiv 10 \pmod{13}.$$

We then denote $y = 2 \cdot 3 \cdot x + 9$ giving us

$$y^2 \equiv 10 \pmod{13}.$$

Euler's criterion shows 10 is a quadratic residue of 13. We find that $y \equiv 6 \pmod{13}$ or $y \equiv -6 \pmod{13}$. Then we solve the equations $6x \equiv -3 \pmod{13}$ and $6x \equiv -15 \pmod{13}$. From these we obtain that

$$x \equiv 6 \pmod{13} \text{ or } x \equiv 4 \pmod{13}.$$

9.1.4 Show that 3 is a quadratic residue of 23, but a nonresidue of 31.

Observe that 3 is a quadratic residue if and only if $3^{11} \equiv 1 \pmod{23}$ by Euler's criterion. Then

$$\begin{aligned} 3^{11} &= 3^3 \cdot 3^8 \\ &\equiv 4 \cdot 81^2 \pmod{23} \\ &\equiv 4 \cdot 12^2 \pmod{23} \\ &\equiv 4 \cdot 6 \pmod{23} \\ &\equiv 1 \pmod{23}. \end{aligned}$$

Thus 3 is a quadratic residue of 23. To show that 3 is a quadratic nonresidue of 31, we must show that $3^{15} \equiv -1 \pmod{31}$. Then

$$\begin{aligned} 3^{15} &= 27^5 \\ &\equiv -4^4 \pmod{31} \\ &\equiv -1 \pmod{31}. \end{aligned}$$

Thus 3 is a nonresidue of 31.

9.1.7 If $p = 2^k + 1$ is prime, verify that every quadratic nonresidue of p is a primitive root of p.

Suppose $p = 2^k + 1$ is prime. Let a be a quadratic nonresidue of p. Then $a^{\frac{p-1}{2}} \equiv a^{2^{k-1}} \equiv -1 \pmod{p}$. Notice that

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

We want to show that $\phi(p) = 2^k$ is the least positive integer such that

$$a^{\phi(p)} \equiv 1 \pmod{p}$$

holds. Suppose for the sake of contradiction that n is the order of a modulo p and $n < \phi(p)$. Then $n \mid \phi(p)$ and so $n = 2^m$ for some $m < k$. So

$$a^{2^m} \equiv 1 \pmod{p}.$$

If $m = k - 1$, we contradict our hypothesis that $a^{2^{k-1}} \equiv -1 \pmod{p}$. If $m < k - 1$, then

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

which still contradicts our assumption. Thus a must be a primitive root of p.