9.3 **4** By Theorem 9.2 (page 176),

$$\left(\frac{-2}{p}\right) \equiv (-2)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}(2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}}\left(\frac{2}{p}\right),$$

and we know that $\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \pmod 8 \\ -1, & p \equiv \pm 3 \pmod 8 \end{cases}$.

$p \equiv 1 \pmod 8 \Rightarrow p = 8k+1 \Rightarrow (-1)^{\frac{p-1}{2}} = (-1)^{4k} = +1 \Rightarrow \left(\frac{-2}{p}\right) = \underline{\underline{+1}}$.

$p \equiv -1 \pmod 8 \Rightarrow p = 8k+7 \Rightarrow (-1)^{\frac{p-1}{2}} = (-1)^{4k+3} = -1 \Rightarrow \left(\frac{-2}{p}\right) = \underline{\underline{-1}}$

$p \equiv 3 \pmod 8 \Rightarrow p = 8k+3 \Rightarrow (-1)^{\frac{p-1}{2}} = (-1)^{4k+1} = -1 \Rightarrow \left(\frac{-2}{p}\right) = \underline{\underline{+1}}$

$p \equiv -3 \pmod 8 \Rightarrow p = 8k+5 \Rightarrow (-1)^{\frac{p-1}{2}} = (-1)^{4k+2} = +1 \Rightarrow \left(\frac{-2}{p}\right) = \underline{\underline{-1}}$.

$\blacksquare$

<u>5(a)</u> $p > 3$ an odd prime

As in #4, $\left(\frac{-3}{p}\right) \equiv (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \begin{cases} \left(\frac{p}{3}\right), & p \equiv 1 \pmod 4 \\ -\left(\frac{p}{3}\right), & p \equiv 3 \pmod 4 \end{cases}$

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

$= \left(\frac{p}{3}\right)$ in either case!

Now, as in the proof of Theorem 9.10, $\left(\frac{p}{3}\right) = \begin{cases} 1, & p \equiv 1 \pmod 3 \\ -1, & p \equiv 2 \pmod 3. \end{cases}$

Since p is an odd prime, $p \equiv 1 \pmod 2$. Finally,

$p \equiv 1 \pmod 2$ & $p \equiv 1 \pmod 3 \Longrightarrow p \equiv 1 \pmod 6 \Longrightarrow \left(\frac{p}{3}\right) = +1.$

$p \equiv 1 \pmod 2$ & $p \equiv 2 \pmod 3 \Longrightarrow p \equiv 5 \pmod 6 \Longrightarrow \left(\frac{p}{3}\right) = -1.$

(see next page

$p \equiv 1 \pmod 2$ & $p \equiv 2 \pmod 3$: apply Chinese Remainder Theorem

$$\left.\begin{aligned} 3x &\equiv 1 \pmod 2 \implies x \equiv 1 \\ 2x &\equiv 1 \pmod 3 \implies x \equiv 2 \end{aligned}\right\} \quad p \equiv 3 + 8 = 11 \equiv 5 \pmod 6$$

<u>5(b)</u> There are infinitely many primes of the form $6k+1$.

<u>pf.</u>: Suppose, to the contrary, that there are only finitely many such primes, $p_1, \dots, p_n$, and define $N := (2p_1 \cdots p_n)^2 + 3$.

N is clearly odd, so some odd prime $p \mid N$ and thus

$$(2p_1 \cdots p_n)^2 \equiv -3 \pmod p \implies p \equiv 1 \pmod 6 \text{ by 5(a)}.$$

This implies that $p = p_i$ for some $i \implies p \mid 3 \implies$ contradiction!

$\boxtimes$

9 p, q odd primes satisfying $p = q + 4a$ for some integer a.

Then $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

<u>Lemma</u> $p \equiv q \pmod 4 \Longrightarrow \left(\frac{-q}{p}\right) = \left(\frac{p}{q}\right)$

<u>pf.</u>: $\left(\frac{-q}{p}\right) \equiv (-1)^{\frac{p-1}{2}} q^{\frac{p-1}{2}} \pmod p = (-1)^{\frac{p-1}{2}} \left(\frac{q}{p}\right)$ by Thm. 9.2

and $\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right), & p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{p}{q}\right), & p \equiv 3 \pmod 4 \text{ \underline{and} } q \equiv 3 \pmod 4. \end{cases}$

$p \equiv q \pmod 4 \Longrightarrow (-1)^{\frac{p-1}{2}} \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$. $\blacksquare$

<u>Main result</u>:

$p = q + 4a \Longrightarrow 4a = p - q \equiv -q \pmod p \Longrightarrow a \equiv -q \pmod p$ since $\gcd(p, 4) = 1$.

Then $\left(\frac{a}{p}\right) = \left(\frac{-q}{p}\right) \underbrace{=}_{\text{Lemma}} \left(\frac{p}{q}\right) = \left(\frac{q+4a}{q}\right) = \underbrace{\left(\frac{4}{q}\right)}_{1}\left(\frac{a}{q}\right) = \left(\frac{a}{q}\right)$. $\blacksquare$

14 $x^2 \equiv 11 \pmod{35} \iff \underbrace{x^2 \equiv 11 \pmod{5}}$ and $\underbrace{x^2 \equiv 11 \pmod{7}}$

<u>By inspection</u>: $x \equiv 1, 4 \pmod{5}$ $\qquad$ $x \equiv 2, 5 \pmod{7}$

Now solve pairs of congruences with the Chinese Remainder Theorem:

$$\left.\begin{array}{l} 5y \equiv 1 \pmod{7} \implies y = 3 \\ 7y \equiv 1 \pmod{5} \implies y = 3 \end{array}\right\} \text{ use these repeatedly}$$

$x \equiv 1 \pmod{5}$ & $x \equiv 2 \pmod{7} \implies x \equiv 21 + 30 \equiv 16 \pmod{35}$

$\underline{x \equiv 16 \pmod{35}}$

$x \equiv 1 \pmod{5}$ & $x \equiv 5 \pmod{7} \implies x \equiv 21 + 75 = 96 \equiv 26 \pmod{35}$

$\underline{x \equiv 26 \pmod{35}}$

$x \equiv 4 \pmod{5}$ & $x \equiv 2 \pmod{7} \implies x \equiv 84 + 30 = 114 \equiv 9 \pmod{35}$

$\underline{x \equiv 9 \pmod{35}}$

$x \equiv 4 \pmod{5}$ & $x \equiv 5 \pmod{7} \implies x \equiv 84 + 75 = 159 \equiv 19 \pmod{35}$

$x \equiv 19 \pmod{35}$

<u>15</u> 7 is a primitive root of any prime of the form $p = 2^{4n}+1$:

First, note that $3 \nmid n$; if $n = 3m$, then $2^{4n}+1 = 2^{12m}+1$, a sum of 2 cubes and therefore composite. Next, note that

$2 \equiv 2 \pmod 7$, $2^2 \equiv 4 \pmod 7$, $2^3 \equiv 1 \pmod 7$

$$\Longrightarrow 2^n \equiv 2 \pmod 7 \text{ if } n \equiv 1 \pmod 3,$$

$$2^n \equiv 4 \pmod 7 \text{ if } n \equiv 2 \pmod 3, \text{ and}$$

$$2^n \equiv 1 \pmod 7 \text{ if } n \equiv 0 \pmod 3.$$

Since $p = 2^{4n}+1$ is prime, $n \equiv 1,2 \pmod 3 \Longrightarrow 2^{4n}+1 \equiv 3,5 \pmod 7$.

$$\begin{array}{l} p \equiv 3 \pmod 7 \\ p \equiv 1 \pmod 4 \end{array} \Longrightarrow \left(\frac{7}{p}\right) = \left(\frac{p}{7}\right) = \left(\frac{3}{7}\right) \underbrace{=}_{\text{since } 7,3 \equiv 3 \pmod 4} -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

$$\begin{array}{l} p \equiv 5 \pmod 7 \\ p \equiv 1 \pmod 4 \end{array} \longrightarrow \left(\frac{7}{p}\right) = \left(\frac{p}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \overbrace{\left(\frac{2}{5}\right) = -1}^{\text{since } 5 \equiv 5 \pmod 8}$$

Thus, 7 is a quadratic nonresidue of p, so

$$7^{\frac{p-1}{2}} \equiv -1 \pmod{p} \quad \text{and} \quad 7^{p-1} \equiv 1 \pmod{p}, \text{ i.e.,}$$

7 is a primitive root of p. ∎

$\boxed{9.4}$ 3 Solve $x^2 \equiv 31 \pmod{11^4}$

First, solve $x^2 \equiv 31 \pmod{11} \iff x^2 \equiv 9 \pmod{11} \implies x = 3, 8$

Next: $x = 3 \implies x^2 = 9 \equiv 31 - 2(11) \implies$ solve $2(3)y \equiv 2 \pmod{11} \implies y = 4$

$6y \equiv 2 \pmod{11}$

Then $(3 + 4\cdot 11)^2 = 9 + 2\cdot 3\cdot 4\cdot 11 + 4^2\cdot 11^2$

$$= 31 - 2\cdot 11 + 2\cdot 3\cdot 4\cdot 11 + 4^2\cdot 11^2$$

$$= 31 + \underbrace{(2\cdot 3\cdot 4 - 2)\cdot 11 + 4^2\cdot 11^2}_{\equiv 0 \pmod{11^2}}$$

$$\equiv 31 \pmod{11^2}.$$

Thus, 47 solves $x^2 \equiv 31 \pmod{11^2}$.

$x = 8 \Longrightarrow x^2 = 64 = 31 + 3\cdot 11 \Longrightarrow$ solve $16y \equiv -3 \pmod{11} \Longrightarrow y = 6$

$\Longrightarrow x = 8 + 6\cdot 11 = 8 + 66 = \underline{\underline{74}}$ solves $x^2 \equiv 31 \pmod{11^2}$.

$x = 47$, $x^2 \equiv 31 \pmod{11^2} \Longrightarrow 47^2 = 31 + 18\cdot 11^2 \Longrightarrow$ solve $2\cdot 47y \equiv -18 \pmod{11}$

i.e., $94y \equiv 4 \pmod{11} \Longrightarrow 47y \equiv 2 \pmod{11} \Longrightarrow \underline{\underline{y = 8}}$

$\Longrightarrow x = 47 + 8\cdot 11^2 = 47 + 8\cdot 121 = \underline{\underline{1015}}$ solves $x^2 \equiv 31 \pmod{11^3}$.

$x = 74$, $x^2 \equiv 31 \pmod{11^2} \Longrightarrow 74^2 = 31 + 45\cdot 11^2 \Longrightarrow$ solve $2\cdot 74y \equiv -45 \pmod{11}$

i.e., $148y \equiv 10 \pmod{11} \Longleftrightarrow 74y \equiv 5 \pmod{11} \Longrightarrow y = 2$

$\Longrightarrow x = 74 + 2\cdot 11^2 = \underline{\underline{316}}$ solves $x^2 \equiv 31 \pmod{11^3}$.

$x = 1015$, $x^2 \equiv 31 \pmod{11^3} \Longrightarrow 1015^2 = 31 + 774 \cdot 11^3$

$\Longrightarrow$ solve $2 \cdot 1015 y \equiv -774 \pmod{11} \Longrightarrow \underline{y = 3}$

$\Longrightarrow 1015 + 3 \cdot 11^3 = \underline{\underline{5008}}$ solves $x^2 \equiv 31 \pmod{11^4}$

$x = 316$, $x^2 \equiv 31 \pmod{11^3} \Longrightarrow 316^2 = 31 + 75 \cdot 11^3$

$\Longrightarrow$ solve $2 \cdot 316 y \equiv -75 \pmod{11} \Longrightarrow \underline{y = 7}$

$\Longrightarrow 316 + 7 \cdot 11^3 = \underline{\underline{9633}}$ solves $x^2 \equiv 31 \pmod{11^4}$

<u>Final answer</u>: 5008, 9633 are the solutions!

$\underline{4}$ $x^2+5x+6 \equiv 0 \pmod{5^3}$

$\Longleftrightarrow 4x^2+20x+24 \equiv 0 \pmod{5^3}$

$\Longleftrightarrow (2x+5)^2 \equiv 1 \pmod{5^3}$

So solve $y^2 \equiv 1 \pmod{5^3}$; $y=1$ is obviously one solution.

The other: $y=1 \pmod 5 \Longrightarrow y=1$ or $y \underline{\underline{=}} 4$

$y=4 \Longrightarrow 4^2 = 1+3\cdot 5 \Longrightarrow$ solve $8z \equiv -3 \pmod 5 \Longrightarrow z=4$

$\Longrightarrow 4+4\cdot 5 = 24$ solves $y^2 \equiv 1 \pmod{5^2}$

$y=24 \Longrightarrow 24^2 = 1+23\cdot 5^2 \Longrightarrow$ solve $48z \equiv -23 \pmod 5 \Longrightarrow z=4$

$\Longrightarrow 24+4\cdot 5^2 = 124$ solves $y^2 \equiv 1 \pmod{5^3}$

$2x+5 \equiv 1 \pmod{125} \Longrightarrow \underline{\underline{x=123}}$; $2x+5 \equiv 124 \pmod{125} \Longrightarrow \underline{\underline{x=122}}$

The solutions are $122, 123$.

$$x^2 + x + 3 \equiv 0 \pmod{3^3}$$

$$\Longleftrightarrow 4x^2 + 4x + 12 \equiv 0 \pmod{27} \Longleftrightarrow (2x+1)^2 \equiv 16 \pmod{27}$$

$$2x+1 \equiv 4 \pmod{27} \qquad\qquad 2x+1 \equiv -4 \pmod{27}$$

$$\Longrightarrow 2x \equiv 3 \pmod{27} \qquad\qquad \Longrightarrow 2x \equiv 22 \pmod{27}$$

$$\Longrightarrow \underline{\underline{x = 15}} \qquad\qquad \Longrightarrow \underline{\underline{x = 11}}$$