SOLUTIONS: PROBLEM SET 9 FROM SECTIONS 4.1 AND 4.2

4.1.22 For $n = 1$, the congruence is an actual equation. For the induction step, we assume that $4^n \equiv 1 + 3n \pmod 9$, and deduce that

$$4^{n+1} \equiv 4 + 12n \equiv 4 + 3n \equiv 1 + 3(n+1) \pmod 9.$$

4.1.28 Using the method in the text, we make the preliminary chart:

$$2^2 = 4$$
$$2^4 = 16$$
$$2^8 = 256 \equiv 21 \pmod{47}$$
$$2^{16} \equiv 18 \pmod{47}$$
$$2^{32} \equiv 42 \pmod{47}$$
$$2^{64} \equiv 25 \pmod{47}$$
$$2^{128} \equiv 14 \pmod{47}$$

We can now complete the computations:

(a) $2^{32} \equiv 42 \pmod{47}$ directly from the chart.
(b) $47 = 32{+}8{+}4{+}2{+}1$, which gives us $2^{47} \equiv 42{\times}21{\times}16{\times}4{\times}2 \equiv 2 \pmod{47}$.
(c) $200 = 128 + 64 + 8$, so that $2^{200} \equiv 14 \times 25 \times 21 \equiv 18 \pmod{47}$.

4.2.2

(a) $x \equiv 10 \pmod 7$
(b) $x \equiv 2, 5, 8 \pmod 9$
(c) $x \equiv 7 \pmod{21}$
(d) There is no solution because $(15, 25)$ does not divide 9.
(e) $x \equiv 812 \pmod{1001}$
(f) $x \equiv 1596 \equiv -1 \pmod{1597}$

4.2.6 There will be solutions provided c is divisible by $(12, 30) = 6$. For each such c there are 6 incongruent solutions.

4.2.8

(a) 7
(b) 9

(c) 8
(d) 6

4.2.16 For $k = 1$, a complete set of residues mod 2^k consists of 1 and 0, of which only 1 satisfies the equation. For $k = 2$, a complete set of residues consists of 0,1,2 and 3, for which only 1 and 3 satisfy the equation. For $k = 3$ a complete set of residues consists of the integers from 0 through 7, and all four odd residues satisfy the equation, while the even ones do not. We now proceed to the general case. Assume $k \geq 3$ and $x^2 \equiv 1 \pmod{2^k}$. Then $2^k | x^2 - 1 = (x-1)(x+1)$. Since 4 cannot divide both $x - 1$ and $x + 1$, but 2 divides both, the only possibilities are $2^{k-1} | x - 1$ or $2^{k-1} | x + 1$. In other words, we have shown that $x^2 \equiv 1 \pmod{2^k}$ if and only if $x \equiv \pm 1 \pmod{2^{k-1}}$, so that $x \equiv \pm 1, \pm 1 + 2^{k-1} \pmod{2^k}$. Since $k \geq 3$, 1 and -1 are incongruent $\pmod{2^{k-1}}$, so these four solutions are distinct.