4.4.1 (b) Solve the linear congruence $5x \equiv 2 \pmod{26}$.

To solve the linear congruence $5x \equiv 2 \pmod{26}$, first notice that this can be written as a Diophantine equation

$$5x - 26n = 2$$

for some $n \in \mathbb{Z}$. Then since the $\gcd(5, 26) = 1$, we can write $1 = 26 + 5(-5)$. Then

$$2 = 26(2) + 5(-10).$$

So $x_0 = -10$ and thus $x = -10 + 26t \equiv -10 \equiv \mathbf{16} \pmod{\mathbf{26}}$, the unique solution as $\gcd(5, 26) = 1$.

4.4.4 (c) Solve the set of simultaneous congruences

$$x \equiv 5 \pmod{6},\ x \equiv 4 \pmod{11},\ x \equiv 3 \pmod{17}.$$

To solve the system of simultaneous congruences, we first construct $n = 6{\cdot}11{\cdot}17 = 1122$. Then $N_1 = 187$, $N_2 = 102$, and $N_3 = 66$. We then solve

$$187x \equiv 1 \pmod{6},\ 102x \equiv 1 \pmod{11},\ 66x \equiv 1 \pmod{17}$$

to obtain x_1, x_2 and x_3. So $187x \equiv 1 \pmod{6}$ implies that $x_1 = 1 \pmod{6}$, $102x \equiv 1 \pmod{11}$ implies that $x_2 = 4 \pmod{11}$, and $66x \equiv 1 \pmod{17}$ implies that $x_3 = 8 \pmod{17}$. Then

$$\bar{x} = 5(187)(1) + 4(102)(4) + 3(66)(8) = 4151 \equiv 785 \pmod{1122}$$

gives the unique solution $x \equiv 785 \pmod{1122}$.

4.4.10 A band of 17 pirates stole a sack of gold coins. When they tried to divide the fortune into equal portions, 3 coins remained. In the ensuing brawl over who should get extra coins, one pirate was killed. The wealth was redistributed, but this time an equal division left 10 coins. Again an argument developed in which another pirate was killed. But now the total fortune was evenly distributed among the survivors. What was the least number of coins that could have been stolen?

We first rewrite the situation as a system of simultaneous congruences. The set is

$$x \equiv 3 \pmod{17},\ x \equiv 10 \pmod{16},\ x \equiv 0 \pmod{15}.$$

We first construct $n = 17 \cdot 16 \cdot 15 = 4080$. Then $N_1 = 240$, $N_2 = 255$, and $N_3 = 272$. We now solve

$$240x \equiv 1 \pmod{17},\ 255x \equiv 1 \pmod{16}.$$

We need not solve $272x \equiv 1 \pmod{15}$ as this term vanishes in the construction of $\bar{x}$. Then $x_1 \equiv 9 \pmod{17}$ and $x_2 \equiv 15 \pmod{16}$. So

$$\bar{x} = 3(240)(9) + 10(255)(15) + 0(272)(x_3) = 44730 \equiv 3930 \pmod{4080}.$$

Thus 3930 coins is the least number of coins stolen.

4.4.13 If $x \equiv a \pmod{n}$, prove that either $x \equiv a \pmod{2n}$ or $x \equiv a + n \pmod{2n}$.

Suppose that $x \equiv a \pmod{n}$. Then $x - a = nk$ for some $k \in \mathbb{Z}$. If k is even then $k = 2m$ for some $m \in \mathbb{Z}$. Then $x - a = m(2n)$ which implies that $x \equiv a \pmod{2n}$. If k is odd then $k = 2m + 1$ for $m \in \mathbb{Z}$. Then $x - a = (2m + 1)n = 2mn + n$. We can rewrite this as $x - (a + n) = m(2n)$ which implies that $x \equiv a + n \pmod{2n}$. Thus if $x \equiv a \pmod{n}$, then either $x \equiv a \pmod{2n}$ or $x \equiv a + n \pmod{2n}$.

4.4.20 (a) Find solutions to

$$5x + 3y \equiv 1 \pmod{7} \tag{1}$$
$$3x + 2y \equiv 4 \pmod{7}. \tag{2}$$

We first solve for y. We take 5 times (2) and subtract it from 3 times (1). This gives

$$y(9 - 10) \equiv 3 - 20 \pmod{7}$$

or

$$y \equiv 17 \equiv 3 \pmod{7}.$$

We then solve for x. We take 3 times (2) and subtract it from 2 times (1). This gives

$$x(10 - 9) \equiv 2 - 12 \pmod{7}$$

or

$$x \equiv -10 \equiv 4 \pmod{7}.$$

Thus the solutions are

$$x \equiv 4 \pmod{7} \quad y \equiv 3 \pmod{7}.$$