Sample Solutions on HW15 (*6 exercises in total*)

Sec. 4.4 6(a)(d), 10, 14, 20, 24

6(a) The first step of the procedure in Example 1 yields $17 = 8 \cdot 2 + 1$, which means that $17 - 8 \cdot 2 = 1$, so -8 is an inverse. We can also report this as 9, because $-8 \equiv 9 \pmod{17}$.

6(d) The first step in the Euclidean algorithm calculation is $1001 = 5 \cdot 200 + 1$. Thus $-5 \cdot 200 + 1001 = 1$, and -5 (or 996) is the desired inverse.

10 We know from Exercise 6 that 9 is an inverse of 2 modulo 17. Therefore if we multiply both sides of this equation by 9 we will get $x \equiv 9 \cdot 7 \pmod{17}$. Since 63 mod 17 = 12, the solutions are all integers congruent to 12 modulo 17, such as 12, 29, and -5. We can check, for example, that $2 \cdot 12 = 24 \equiv 7 \pmod{17}$. This answer can also be stated as all integers of the form $12 + 17k$ for $k \in Z$.

14 Adding 12 to both sides of the congruence yields $12x^2 + 25x + 12 \equiv 0 \pmod{11}$. (We chose something to add that would make the left-hand side easily factorable and the right-hand side equal to 0.) This is equivalent to $(3x + 4)(4x + 3) \equiv 0 \pmod{11}$. Because there are no non-zero divisors of 0 modulo 11, this congruence is true if and only if either $3x + 4 \equiv 0 \pmod{11}$ or $4x + 3 \equiv 0 \pmod{11}$. (This would have been more complicated modulo a non-prime modulus, because there would be nonzero divisors of 0.)
We solve these linear congruences by inspection (guess and check) or using the Euclidean algorithm to find inverses of 3 and 4 (or using computer algebra software), to yield $x = 6$ or $x = 2$.

20 Since 3, 4, and 5 are pairwise relatively prime, we can use the Chinese remainder theorem. The answer will be unique modulo $3 \cdot 4 \cdot 5 = 60$. Using the notation in the text, we have $a_1 = 2$, $m_1 = 3$, $a_2 = 1$, $m_2 = 4$, $a_3 = 3$, $m_3 = 5$, $m = 60$, $M_1 = 60/3 = 20$, $M_2 = 60/4 = 15$, $M_3 = 60/5 = 12$. Then we need to find inverses y_i of Mi modulo m_i for $i = 1, 2, 3$. This can be done by inspection (trial and error), since the moduli here are so small, or systematically using the Euclidean algorithm (as in Example 2); we find that $y_1 = 2$, $y_2 = 3$, and $y_3 = 3$. Thus our solution is $x = 2 \cdot 20 \cdot 2 + 1 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 = 233 \equiv 53 \pmod{60}$. So the solutions are all integers of the form $53 + 60k$, where k is an integer.

24 By definition, the first congruence can be written as $x = 2t + 1$ where t is an integer. Substituting this expression for x into the second congruence tells us that $2t + 1 \equiv 2 \pmod{3}$, which can easily be solved to show that $t \equiv 2 \pmod{3}$. From this we can write $t = 3u + 2$ for some integer u. Thus $x = 2t + 1 = 2(3u + 2) + 1 = 6u + 5$. Next we have $6u + 5 \equiv 3 \pmod{5}$, which we solve to get $u \equiv 3 \pmod{5}$, so $u = 5v + 3$. Thus $x = 6(5v + 3) + 5 = 30v + 23$. For the last congruence we have $30v + 23 \equiv 4 \pmod{11}$; solving this is a little harder but trial and error or the applying the methods of Example 2 and Example 3 shows that $v \equiv 10 \pmod{11}$. Therefore $x = 30(11w + 10) + 23 = 330w + 323$. So our solution is all integers congruent to 323 modulo 330. We check our answer by confirming that $323 \equiv 1 \pmod{2}$, $323 \equiv 2 \pmod{3}$, $323 \equiv 3 \pmod{5}$, and $323 \equiv 4 \pmod{11}$.