Training Problems #3 - Solutions

Section 4.4:

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 $-8 \equiv 9 \pmod{17}$.

b) We need to find s and t such that $34s + 89t = 1$. Then s will be the desired inverse, since $34s \equiv 1 \pmod{89}$ (i.e., $34s - 1 = -89t$ is divisible by 89). To do so, we proceed as in Example 2. First we go through the Euclidean algorithm computation that $\gcd(34, 89) = 1$:

$$\begin{aligned}
89 &= 2 \cdot 34 + 21 \\
34 &= 21 + 13 \\
21 &= 13 + 8 \\
13 &= 8 + 5 \\
8 &= 5 + 3 \\
5 &= 3 + 2 \\
3 &= 2 + 1
\end{aligned}$$

Then we reverse our steps and write 1 as the desired linear combination:

$$\begin{aligned}
1 &= 3 - 2 \\
&= 3 - (5 - 3) = 2 \cdot 3 - 5 \\
&= 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5 \\
&= 2 \cdot 8 - 3 \cdot (13 - 8) = 5 \cdot 8 - 3 \cdot 13 \\
&= 5 \cdot (21 - 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13 \\
&= 5 \cdot 21 - 8 \cdot (34 - 21) = 13 \cdot 21 - 8 \cdot 34 \\
&= 13 \cdot (89 - 2 \cdot 34) - 8 \cdot 34 = 13 \cdot 89 - 34 \cdot 34
\end{aligned}$$

Thus $s = -34$, so an inverse of 34 modulo 89 is -34, which can also be written as 55.

c) We need to find s and t such that $144s + 233t = 1$. Then clearly s will be the desired inverse, since $144s \equiv 1 \pmod{233}$ (i.e., $144s - 1 = -233t$ is divisible by 233). To do so, we proceed as in Example 2. In fact, once we get to a certain point below, all the work was already done in part (b). First we go through the

Euclidean algorithm computation that $\gcd(144, 233) = 1$:

$$
\begin{aligned}
233 &= 144 + 89 \\
144 &= 89 + 55 \\
89 &= 55 + 34 \\
55 &= 34 + 21 \\
34 &= 21 + 13 \\
21 &= 13 + 8 \\
13 &= 8 + 5 \\
8 &= 5 + 3 \\
5 &= 3 + 2 \\
3 &= 2 + 1
\end{aligned}
$$

Then we reverse our steps and write 1 as the desired linear combination:

$$
\begin{aligned}
1 &= 3 - 2 \\
&= 3 - (5 - 3) = 2 \cdot 3 - 5 \\
&= 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5 \\
&= 2 \cdot 8 - 3 \cdot (13 - 8) = 5 \cdot 8 - 3 \cdot 13 \\
&= 5 \cdot (21 - 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13 \\
&= 5 \cdot 21 - 8 \cdot (34 - 21) = 13 \cdot 21 - 8 \cdot 34 \\
&= 13 \cdot (55 - 34) - 8 \cdot 34 = 13 \cdot 55 - 21 \cdot 34 \\
&= 13 \cdot 55 - 21 \cdot (89 - 55) = 34 \cdot 55 - 21 \cdot 89 \\
&= 34 \cdot (144 - 89) - 21 \cdot 89 = 34 \cdot 144 - 55 \cdot 89 \\
&= 34 \cdot 144 - 55 \cdot (233 - 144) = 89 \cdot 144 - 55 \cdot 233
\end{aligned}
$$

Thus $s = 89$, so an inverse of 144 modulo 233 is 89, since $144 \cdot 89 = 12816 \equiv 1 \pmod{233}$.

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 $63 \mathbf{\ mod\ } 17 = 12$, 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 $k \in \mathbf{Z}$.

12. In each case we multiply both sides of the congruence by the inverse found in Exercise 6 and simplify. Our answers are not unique, of course—anything in the same congruence class works just as well.

a) We found that 55 is an inverse of 34 modulo 89, so $x \equiv 77 \cdot 55 = 4235 \equiv 52 \pmod{89}$. Check: $34 \cdot 52 = 1768 \equiv 77 \pmod{89}$.

b) We found that 89 is an inverse of 144 modulo 233, so $x \equiv 4 \cdot 89 = 356 \equiv 123 \pmod{233}$. Check: $144 \cdot 123 = 17712 \equiv 4 \pmod{233}$.

c) We found that -5 is an inverse of 200 modulo 1001, so $x \equiv 13 \cdot (-5) = -65 \equiv 936 \pmod{1001}$. (We could also leave the answer as -65.) Check: $200 \cdot 936 = 187200 \equiv 13 \pmod{1001}$.

34. Fermat's little theorem tells us that $23^{40} \equiv 1 \pmod{41}$. Therefore $23^{1002} = (23^{40})^{25} \cdot 23^2 \equiv 1^{25} \cdot 529 = 529 \equiv 37 \pmod{41}$.

38. **a)** By Fermat's little theorem we know that $3^4 \equiv 1 \pmod{5}$; therefore $3^{300} = (3^4)^{75} \equiv 1^{75} \equiv 1 \pmod{5}$, and so $3^{302} = 3^2 \cdot 3^{300} \equiv 9 \cdot 1 = 9 \pmod{5}$, so $3^{302} \textbf{ mod } 5 = 4$. Similarly, $3^6 \equiv 1 \pmod{7}$; therefore $3^{300} = (3^6)^{50} \equiv 1 \pmod{5}$, and so $3^{302} = 3^2 \cdot 3^{300} \equiv 9 \pmod{7}$, so $3^{302} \textbf{ mod } 7 = 2$. Finally, $3^{10} \equiv 1 \pmod{11}$; therefore $3^{300} = (3^{10})^{30} \equiv 1 \pmod{11}$, and so $3^{302} = 3^2 \cdot 3^{300} \equiv 9 \pmod{11}$, so $3^{302} \textbf{ mod } 11 = 9$.
b) Since 3^{302} is congruent to 9 modulo 5, 7, and 11, it is also congruent to 9 modulo 385. (This was a particularly trivial application of the Chinese remainder theorem.)

Section 4.5:

18. In each case we just have to compute $x_1 + x_2 + \cdots + x_{10} \textbf{ mod } 9$ The easiest way to do this by hand is to "cast out nines," i.e., throw away sums of 9 as we come to them.
a) $7+5+5+5+6+1+8+8+7+3 \textbf{ mod } 9 = 1$ **b)** 5 **c)** 2 **d)** 0