Tutorial 10 Solutions

1. What is $1 + 2 + 3 + 4 + 5$ modulo 2,3,5 ?
   What is $2 \cdot 4 + 4 \cdot 7 + 5 \cdot 3$ modulo $2, 3, 19$?

   Solution. $1 + 2 + 3 + 4 + 5 = 15$ which is $1, 0, 0$ modulo $2, 3, 5$ respectively. $2 \cdot 4 + 4 \cdot 7 + 5 \cdot 3 = 51$ which is $1, 0, 13$ modulo $2, 3, 19$ respectively.

2. Compute the inverses of 3 mod 11, 8 mod 13, and 4 mod 7. Use your answers to solve the equations $3x + 2 = 8$ mod 11, $8x - 3 = 6$ mod 13, $4x = 0$ mod 7.

   Solution. We compute the inverse of 3 mod 11 using the extended Euclidean algorithm.

$$
\begin{array}{rcl}
11 &=& 3(3) + 2 \\
3 &=& 1(2) + 1 \\
--- & - & -------- \\
1 &=& 3 - 2 \\
1 &=& 3 - (11 - 3 \cdot 3) \\
1 &=& 4 \cdot 3 - 11.
\end{array}
$$

   Reducing this equation modulo eleven, we find that the inverse of 3 is 4. Next we compute the inverse of 8 mod 13 using the extended Euclidean algorithm.

$$
\begin{array}{rcl}
13 &=& 1(8) + 5 \\
8 &=& 1(5) + 3 \\
5 &=& 1(3) + 2 \\
3 &=& 1(2) + 1 \\
--- & - & -------- \\
1 &=& 3 - 2 \\
1 &=& 3 - (5 - 3) \\
1 &=& 2 \cdot 3 - 5 \\
1 &=& 2 \cdot (8 - 5) - 5 \\
1 &=& 2 \cdot 8 - 3 \cdot 5 \\
1 &=& 2 \cdot 8 - 3(13 - 8) \\
1 &=& 5 \cdot 8 - 3 \cdot 13.
\end{array}
$$

Reducing this equation modulo thirteen, we find that the inverse of 8 is 5.
Next we compute the inverse of 4 mod 7 using the extended Euclidean algorithm.

$$\begin{array}{rcl} 7 & = & 1(4)+3 \\ 4 & = & 1(3)+1 \\ --- & - & -------- \\ 1 & = & 4-3 \\ 1 & = & 4-(7-4) \\ 1 & = & 2\cdot 4-7. \end{array}$$

Reducing this equation modulo seven, we find that the inverse of 4 is 2.
These inverses allow us to solve the given equations.

$$\begin{array}{rcl} 3x+2 & = & 8 \bmod 11 \\ 4(3x+2) & = & 4(8) \bmod 11 \\ x+8 & = & 32 \bmod 11 \\ x & = & 24 \bmod 11 \\ & = & 2 \bmod 11. \end{array}$$

$$\begin{array}{rcl} 8x-3 & = & 6 \bmod 13 \\ 5(8x-3) & = & 5(6) \bmod 13 \\ x-15 & = & 30 \bmod 13 \\ x & = & 45 \bmod 13 \\ & = & 6 \bmod 13. \end{array}$$

$$\begin{array}{rcl} 4x & = & 0 \bmod 7 \\ 2(4x) & = & 2(0) \bmod 7 \\ x & = & 0 \bmod 7. \end{array}$$

3. Determine the complete solution set for the following systems of equations.

$$(a)\quad \begin{array}{rcl} 4x+2y &=& 2 \\ 5x-3y &=& 1 \quad \text{mod } 7 \end{array} \qquad (b)\quad \begin{array}{rrcl} x & +\,2y &=& 0 \\ 2x & -\,y &=& 0 \quad \text{mod } 3 \end{array}$$

$$(c)\quad \begin{array}{rrrcl} 3x & +\,4y & +\,2z &=& 1 \\ 5x & -\,2y & +\,z &=& 1 \\ x & +\,5y & +\,6z &=& 1 \quad \text{mod } 7 \end{array}$$

Solution.

(a) $$\left[\begin{array}{cc|c} 4 & 2 & 2 \\ 5 & -3 & 1 \end{array}\right] \sim_{2R_1,3R_2} \left[\begin{array}{cc|c} 1 & 4 & 4 \\ 1 & 5 & 3 \end{array}\right] \sim_{R_2-R_1} \left[\begin{array}{cc|c} 1 & 4 & 4 \\ 0 & 1 & 6 \end{array}\right] \sim_{R_1-4R_2} \left[\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & 6 \end{array}\right].$$

(b) $$\left[\begin{array}{cc|c} 1 & 2 & 0 \\ 2 & -1 & 0 \end{array}\right] \sim_{2R_2} \left[\begin{array}{cc|c} 1 & 2 & 0 \\ 1 & 1 & 0 \end{array}\right] \sim_{-R_2+R_1} \left[\begin{array}{cc|c} 1 & 2 & 0 \\ 0 & 1 & 0 \end{array}\right] \sim_{R_1-2R_2} \left[\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & 0 \end{array}\right].$$

(c) $$\left[\begin{array}{ccc|c} 3 & 4 & 2 & 1 \\ 5 & -2 & 1 & 1 \\ 1 & 5 & 6 & 1 \end{array}\right] \sim_{5R_1,3R_2} \left[\begin{array}{ccc|c} 1 & -1 & 3 & 5 \\ 1 & 1 & 3 & 3 \\ 1 & 5 & 6 & 1 \end{array}\right] \sim_{R_2-R_1,R_3-R1} \left[\begin{array}{ccc|c} 1 & -1 & 3 & 5 \\ 0 & 2 & 0 & 5 \\ 0 & 6 & 3 & 3 \end{array}\right]$$

$$\sim_{R_3-3R_2,4R_2} \left[\begin{array}{ccc|c} 1 & -1 & 3 & 5 \\ 0 & 1 & 0 & 6 \\ 0 & 0 & 3 & 2 \end{array}\right] \sim_{R_1+R_2-R_3,5R_3} \left[\begin{array}{ccc|c} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 6 \\ 0 & 0 & 1 & 3 \end{array}\right]$$

4. *Challenge.* For what values of a does $ax = 1$ have a solution modulo 4 ? *Solution.* For $a = 1, 3$ there is a solution; for $a = 1$ the solution is $x = 1$, and for $a = 3$ we can multiply both sides by 3 and have $x = 3$. For $x = 0, 2$ there is no solution.