1. Use the Euclidean Algorithm to find $(5568, 7266)$, and find a solution to Bezout's identity.

Solution:

\[
\begin{align*}
7266 &= 5568 + 1698 \\
5568 &= 3 \cdot 1698 + 474 \\
1698 &= 3 \cdot 474 + 276 \\
474 &= 276 + 198 \\
276 &= 198 + 78 \\
198 &= 2 \cdot 78 + 42 \\
78 &= 42 + 36 \\
42 &= 36 + 6 \\
36 &= 6 \cdot 6 + 0
\end{align*}
\]

\[
\begin{align*}
5568 &= 3 \cdot 1698 + 474 \\
1698 &= 3 \cdot 474 + 276 \\
474 &= 276 + 198 \\
276 &= 198 + 78 \\
198 &= 2 \cdot 78 + 42 \\
78 &= 42 + 36 \\
42 &= 36 + 6 \\
36 &= 6 \cdot 6 + 0
\end{align*}
\]

2. True or False. If true say why. If false, give a counterexample.

a) $ax \equiv b \mod 77$ has a unique solution mod 77 provided that $(a, 77) | b$. Solution: False. The solution is not unique if $(a, 77) \neq 1$. A counterexample is given by $a = 14$, $b = 7$, where there are 7 solutions, including 6 and 17.

b) If $a \neq 0 \mod 21$, and if $ax \equiv ay \mod 21$, then $x \equiv y \mod \frac{21}{(21, y)}$. Solution: False. A counterexample is given by $a = 3$, $y = 1$ and $x = 8$.

3. Let $a = 2^53^64^75^86^9$ and $b = 2^93^84^55^63^9$. Give prime decompositions for the following:

a) $ab$

b) $[a, b]$

c) $(a, b)$

Solution: Here $a = 2^{28}3^{15}5^8$, $b = 2^{20}3^{11}5^5$, so $ab = 2^{48}3^{26}5^{13}$, $[a, b] = a$ and $(a, b) = b$. 

4. Find all solutions or say why none exist:
   a) \(75x + 100y = 35\). \textbf{Solution:} \((75, 100) = 25 \not| 35\), so there are no solutions.
   
   b) \(75x + 35y = 100\). \textbf{Solution:} \((75, 35) = 5|100\), so solutions exist. We first solve Bezout’s identity for 75 and 35, getting
   \[5 = 75 - 2 \cdot 35.\]
   Multiplying through by 20, we get
   \[100 = 20 \cdot 75 + (-40)35,\]
   The general solution is now given by
   \[
   \begin{cases}
   x = 20 + 7n \\
   y = -40 - 15n
   \end{cases}
   \text{ for } n \in \mathbb{Z}.
   \]

5. Suppose \((a, b) = 40\), \([a, b] = 3600\). What are the possible values for \(a\) and \(b\) (as a pair)?
   \textbf{Solution:} Here, \((a, b) = 2^33^05^1\) and \([a, b] = 2^43^25^2\). Thus, \(a = 2^r3^r5^r\) and \(b = 2^s3^s5^s\), where
   \[
   \begin{align*}
   \min(r_1, s_1) &= 3 & \max(r_1, s_1) &= 4 \\
   \min(r_2, s_2) &= 0 & \max(r_2, s_2) &= 2 \\
   \min(r_3, s_3) &= 1 & \max(r_3, s_3) &= 2.
   \end{align*}
   \]
   We may fix the exponents for one prime in \(a\) and \(b\) and let the others vary. So we fix \(r_1 = 3\) and \(s_1 = 4\).
   
   \textit{Case 1:} \(r_2 = 0\) and \(r_3 = 1\). Here, \(a = 40, b = 3600\).
   \textit{Case 2:} \(r_2 = 0\) and \(r_3 = 2\). Here, \(a = 200, b = 720\).
   \textit{Case 3:} \(r_2 = 2\) and \(r_3 = 1\). Here, \(a = 360, b = 400\).
   \textit{Case 4:} \(r_2 = 2\) and \(r_3 = 2\). Here, \(a = 1800, b = 80\).

6. Find all nonnegative solutions less than the modulus or show why no solutions exist:
   a) \(24x \equiv 22 \mod 150\). \textbf{Solution:} \((24, 150) = 6 \not| 22\), so there are no solutions.
   
   b) \(42x \equiv 24 \mod 150\). \textbf{Solution:} \((42, 150) = 6|24\), so there are solutions. We first divide through by \((42, 150)\), getting
   \[7x \equiv 4 \mod 25.\]
   We now solve Bezout’s identity for 7 and 25, getting
   \[1 = 25 + (-7)7.\]
Thus, the inverse of 7 mod 25 is $-7$. So we multiply (1) by $-7$, getting

\begin{align*}
(2) & \quad -7 \cdot 7x \equiv -7 \cdot 4 \mod 25, \\
(3) & \quad x \equiv -28 \mod 25.
\end{align*}

But $-28 \equiv -3 \equiv 22 \mod 25$, so

\begin{align*}
x & \equiv 22, 22 + 25, 22 + 50, 22 + 75, 22 + 100, 22 + 125 \mod 150 \\
& \equiv 22, 47, 72, 97, 122, 147.
\end{align*}

7. a) What are the elements of $\mathbb{Z}_{18}^\times$?
   
   **Solution:** $\{1, 5, 7, 11, 13, 17\}$.

b) What is the inverse of $13$ in $\mathbb{Z}_{18}^\times$?
   
   **Solution:** Solving Bezout’s identity for 13 and 18, we get
   \begin{align*}
   1 & = -5 \cdot 18 + 7 \cdot 13, \text{ so} \\
   1 & \equiv 7 \cdot 13 \mod 18.
   \end{align*}

   Thus, $13^{-1} = 7$. 