1. Prove that if $a, b, c$ are integers for which $b \mid a$ and $b \mid (a - c)$, then $b \mid c$.

Solution: Assume that $b \mid a$ and $b \mid (a - c)$. Then by definition there exist integers $k$ and $q$ with $a = bq$ and $a - c = bk$. Since we need to show that $b$ is a factor of $c$, we start by solving the second equation for $c$. Then $c = a - bk$, and we can substitute for $a$ to get $c = bq - bk = b(q - k)$. This shows that $c$ has $b$ as a factor, and so $b \mid c$, as required.

2. Find gcd(7605, 5733), and express it as a linear combination of 7605 and 5733.

Solution: Use the matrix form of the Euclidean algorithm:

\[
\begin{bmatrix}
1 & 0 & 7605 \\
0 & 1 & 5733
\end{bmatrix} \sim \begin{bmatrix}
1 & -1 & 1872 \\
0 & 1 & 5733
\end{bmatrix} \sim \begin{bmatrix}
1 & -1 & 1872 \\
-3 & 4 & 117
\end{bmatrix} \sim \begin{bmatrix}
49 & -65 & 0 \\
-3 & 4 & 117
\end{bmatrix}.
\]

Thus gcd(7605, 5733) = 117, and $117 = (−3) \cdot 7605 + 4 \cdot 5733$.

3. Find the prime factorizations of 1275 and 495 and use them to find gcd(1275, 495).

Solution: You can compare Problem 1.1.42, which was to be solved using the Euclidean algorithm. We can begin factoring 1275 by factoring out a 5. Continuing, we obtain $1275 = 5 \cdot 255 = 5^2 \cdot 51 = 3 \cdot 5^2 \cdot 17$. Next, we have $495 = 5 \cdot 99 = 5 \cdot 9 \cdot 11 = 3^2 \cdot 5 \cdot 11$. Thus gcd(1275, 495) = $3 \cdot 5$, while lcm[1275, 495] = $3^2 \cdot 5^2 \cdot 11 \cdot 17$.

4. Find $\varphi(1275)$ and $\varphi(495)$.

Solution: We can use the prime factorizations found in Problem 3. By Proposition 1.4.8 we have $\varphi(1275) = 3 \cdot 5^2 \cdot 17 \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{16}{17} = 5 \cdot 2 \cdot 4 \cdot 16 = 640$ and $\varphi(495) = 3^2 \cdot 5 \cdot 11 \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{10}{11} = 3 \cdot 2 \cdot 4 \cdot 10 = 240$.

5. Solve the congruence $24x \equiv 168 \pmod{200}$.

Solution: First we find that gcd(24, 200) = 8, and 8 \mid 168, so the congruence has a solution. The next step is to reduce the congruence by dividing each term by 8, which gives $24x \equiv 168 \pmod{200}$. To solve the congruence $3x \equiv 21 \pmod{25}$ we could find the multiplicative inverse of 3 modulo 25. Trial and error shows it to be $−8$, we can multiply both sides of the congruence by $−8$, and proceed with the solution.

\[
\begin{align*}
24x & \equiv 168 \pmod{200} \\
3x & \equiv 21 \pmod{25} \\
−24x & \equiv −168 \pmod{25} \\
x & \equiv 7 \pmod{25}
\end{align*}
\]

The solution is $x \equiv 7, 32, 57, 82, 107, 132, 157, 182 \pmod{200}$.
6. Find the additive order of 168 modulo 200.

Solution: According to the definition of the additive order of a number, we need to solve $168x \equiv 0 \pmod{200}$. Since $\gcd(168, 200) = 8$, we get $21x \equiv 0 \pmod{25}$. This leads to $x \equiv 0 \pmod{25}$, and therefore the the additive order of 168 is 25.

7. Solve the system of congruences $2x \equiv 9 \pmod{15}$, $x \equiv 8 \pmod{11}$.

Solution: Write $x = 8 + 11q$ for some $q \in \mathbb{Z}$, and substitute to get $16 + 22q \equiv 9 \pmod{15}$, which reduces to $7q \equiv -7 \pmod{15}$, so $q \equiv -1 \pmod{15}$. This gives $x \equiv -3 \pmod{11 \cdot 15}$.

8. Find $[50]^{-1}_{501}$ and $[51]^{-1}_{501}$, if possible (in $\mathbb{Z}^\times_{501}$).

Solution: We need to use the Euclidean algorithm.

\[
\begin{bmatrix}
1 & 0 & 501 \\
0 & 1 & 50 \\
\end{bmatrix} \leadsto \begin{bmatrix}
1 & -10 & 1 \\
0 & 1 & 50 \\
\end{bmatrix} \leadsto \begin{bmatrix}
1 & -10 & 1 \\
-50 & 501 & 0 \\
\end{bmatrix}
\]

Thus $[50]^{-1}_{501} = [-10]_{501} = [491]_{501}$.

\[
\begin{bmatrix}
1 & 0 & 501 \\
0 & 1 & 51 \\
\end{bmatrix} \leadsto \begin{bmatrix}
1 & -9 & 42 \\
0 & 1 & 51 \\
\end{bmatrix} \leadsto \begin{bmatrix}
1 & -9 & 42 \\
-1 & 10 & 9 \\
\end{bmatrix} \leadsto \begin{bmatrix}
5 & -11 & 6 \\
-1 & 10 & 9 \\
\end{bmatrix}
\]

Now we can see that the gcd is 3, so $[51]_{501}$ is not a unit in $\mathbb{Z}^\times_{501}$.

9. List the elements of $\mathbb{Z}^\times_{15}$. For each element, find its multiplicative inverse, and find its multiplicative order.


To compute the multiplicative order of $[8]$, we can rewrite it as $[2]^3$, and then it is clear that the first positive integer $k$ with $([2]^3)^k = [1]$ is $k = 4$, since $3k$ must be a multiple of 4. (This can also be shown by rewriting $[8]$ as $[-7]$.) Similarly, $[11] = [-4]$ has multiplicative order 2, and $[13] = [-2]$ has multiplicative order 4.

10. Show that $3^n + 4^n - 1$ is divisible by 6, for any positive integer $n$.

Solution: We have $3^n + 4^n - 1 \equiv 1^n + 0^n - 1 \equiv 0 \pmod{2}$ and $3^n + 4^n - 1 \equiv 0^n + 1^n - 1 \equiv 0 \pmod{3}$. Since 2 and 3 are relatively prime, it follows that 6 is a divisor of $3^n + 4^n - 1$. 