Applied Algebra

Instructions Please write your name in the upper right-hand corner of the page. Use complete sentences, along with any necessary supporting calculations, to answer the following questions.

1. Find an integer x such that $100x \equiv 7 \mod 433$.

   Solution. The strategy is to use the Euclidean algorithm to find the multiplicative inverse of $100 \mod 433$. Here is the calculation via the matrix method.

   $$\begin{pmatrix} 1 & 0 & 433 \\ 0 & 1 & 100 \end{pmatrix} \xrightarrow{R1 \to R1 - 4R2} \begin{pmatrix} 1 & -4 & 33 \\ 0 & 1 & 100 \end{pmatrix} \xrightarrow{R2 \to R2 - 3R1} \begin{pmatrix} 1 & -4 & 33 \\ -3 & 13 & 1 \end{pmatrix}$$

   The conclusion from the calculation is that $-3 \times 433 + 13 \times 100 = 1$. In other words, the numbers 13 and 100 are multiplicative inverses $\mod 433$. Therefore multiplying the original congruence by 13 shows that $x \equiv 13 \times 7 \mod 433$, or $x \equiv 91 \mod 433$.

2. In $\mathbb{Z}_8$ there are eight elements: the congruence classes $[0]$, $[1]$, ..., $[7]$. How many of these eight elements have multiplicative inverses in $\mathbb{Z}_8$?

   Solution. We know from class (or from Theorem 1.4.3 on page 43) that the congruence class $[a]$ is invertible in $\mathbb{Z}_8$ if and only if $\gcd(a, 8) = 1$. Since 2 is the only prime divisor of 8, the odd values of a are the ones for which $\gcd(a, 8) = 1$. Thus there are exactly four invertible elements in $\mathbb{Z}_8$: namely, $[1]$, $[3]$, $[5]$, and $[7]$.