Ciphers and Number Theory 5

1. For $n = 989$ show how to convert the message `abandon all hope` into suitable blocks made up of elements of $\mathbb{Z}_n$.

2. Each of the following functions is suggested as a possible affine cipher in $\mathbb{Z}_{989}$. For each function, explain whether it is suitable for use as an affine cipher, and if it is then encode the message given in Q1.

   (a) $f(x) = 23x + 147$.

   (b) $g(x) = 24x + 239$.

3. For each encoded message in Q2, show how to decode it, and how to convert it back into a sequence of letters.

4. Calculuate directly $\phi(24)$.

5. Give a reduced residue system mod 24 such that all elements are divisible by 7.

6. Verify Euler's theorem when $a = 11$ and $n = 24$.

7. Given a sequence of numbers $x_1, \ldots, x_t$ in $\mathbb{Z}_n$ we can consider them as a vector $(x_1, \ldots, x_t)$ in $\mathbb{Z}_n^t$. For example, if $x_1 = 3$, $x_2 = 5$, $x_3 = 8$ in $\mathbb{Z}_{10}$ we can consider the vector $\mathbf{v} = (3, 5, 8)$ in $\mathbb{Z}_{10}^3$. We can now look for functions $f : \mathbb{Z}_n^t \longrightarrow \mathbb{Z}_n^t$ which can be used as ciphers.

   (a) Fix a vector $\mathbf{a} = (a_1, \ldots, a_t) \in \mathbb{Z}_n^t$ and consider the function

   $$f(\mathbf{x}) = \mathbf{x} + \mathbf{a}.$$

      i. When does this function have an inverse, and what is it?

      ii. Let $n = 26$ and $\mathbf{a} = (11, 7, 13)$. Show how to use this function f to encode the message `elephant`.

      iii. We have already seen this kind of cipher in Chapter 1; what it is called?

   (b) More generally, fix some $t \times t$ matrix A with entries in $\mathbb{Z}_n$, and $\mathbf{a}$ as above, and consider the function

   $$f(\mathbf{x}) = \mathbf{x}A + \mathbf{a}.$$

      i. Show that the inverse of f is given by $g(\mathbf{z}) = (\mathbf{z} - \mathbf{a})A^{-1}$.

      ii. Calculuate $f(\mathbf{x})$ if $n = 26$, $A = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$, $\mathbf{a} = (4, 7)$ and $\mathbf{x} = (11, 6)$ and verify that g is indeed the inverse of f.

      iii. Show that in general g exists if and only if $\det A$ is invertible in $\mathbb{Z}_n$.

   When f is invertible this gives what is called a *Hill cipher* from $\mathbb{Z}_n^t$ to $\mathbb{Z}_n^t$.