1. Let $\mathbb{Z}_n = \{0, \ldots, n-1\}$, and let $e$ be a non-zero element of $\mathbb{Z}_n$.

   (a) Show that if $\gcd(e, n) = 1$, then there exists a unique element $d$ of $\mathbb{Z}_n$ with 
   $ed \equiv 1 \pmod{n}$. (The element $d$ is called the multiplicative inverse of $e$ in $\mathbb{Z}_n$.)

   (b) Conversely, show that if $e$ has a multiplicative inverse in $\mathbb{Z}_n$, then $\gcd(e, n) = 1$.

   Hint: use the fact (from Workshop 1) that $\gcd(e, n) = 1$ if and only if the function $f : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ given by $f : a \mapsto ea$ is one-to-one.

2. (a) Show that 2 is a primitive element of $\mathbb{Z}_{11}$.

(b) Let $f$ be the function from $\mathbb{Z}_{31}$ to $\mathbb{Z}_{31}$ given by

   $$f : x \mapsto 3^x \pmod{31}$$

   (where 3 is a primitive element of $\mathbb{Z}_{31}$).

   i. Evaluate $f(5)$.

   ii. Find $x$ given that $f(x) = 4$.

(c) Let $f$ be the function from $\mathbb{Z}_{73}$ to $\mathbb{Z}_{73}$ given by

   $$f : x \mapsto 5^x \pmod{73}$$

   (where 5 is a primitive element of $\mathbb{Z}_{73}$). EITHER

   i. evaluate $f(7)$, OR

   ii. find $x$ given that $f(x) = 19$.

   (The two choices are worth the same number of marks.)
3. Let $C$ be the binary $(4,2)$-code $\{0000, 1011, 0110, 1101\}$.

(a) Find a parity check matrix $H$ for $C$.
(b) Construct a standard array for $C$.
(c) Give a table of coset leaders and their syndromes for $C$.
(d) Use syndrome decoding to decode

i. 1111
ii. 0111
iii. 1110

4. Let $C$ be the ternary code with parity check matrix

$$H = \begin{pmatrix}
0 & 1 & 1 & 0 \\
1 & 2 & 0 & 1 \\
1 & 2 & 0 & 1 
\end{pmatrix}.$$

Give a table of coset leaders and their syndromes for $C$. Use syndrome decoding to decode

(a) 0110
(b) 2222
(c) 2012

5. **Bonus Question**

Is there a self-dual ternary $(6,3)$-code? If so, give an example. If not, give a proof.