1. All arithmetic in this question is modulo the safe prime 23.

   (a) Circle the unique $m$ among $-5$ and 5 that is a quadratic residue. Explain. $\boxed{-5}$ 5

   **Solution:** There are 22 invertible elements and 11 quadratic residues. The quadratic residues are those elements whose 11th power is 1. As

   $$5^{11} = 5 \cdot 5^{10} = 5 \cdot 25^5 \equiv 5 \cdot 2^5 = 5 \cdot 32 \equiv 5 \cdot 9 = 45 \equiv -1,$$

   it is not the quadratic residue. It has to be $-5$ because $(-5)^{11} = (-1)^{11}5^{11} \equiv (-1) \cdot (-1) = 1$.

   (b) What is the unique square root of $m$ among the numbers $\{1, 2, \ldots, 11\}$?

   **Solution:** Among quadratic residues, $m^{12} \equiv m$, so its square roots must be $\pm m^6$. Here

   $$(-5)^6 = 25^3 \equiv 2^3 = 8.$$

   The two square roots are $\pm 8$. The sought one is 8.

2. Alice tags a 6-bit message $m = m_L m_R$ by $t = t_L t_R$, with $t_L = F(m_L)$ and $t_R = F(m_R + \texttt{001})$. $F$ is a PRF with 3 bits of input and 3 bits of output whose secret key is shared between Alice and Bob. All addition is mod 2.

   (a) Bob receives the message–tag pair $(\texttt{011011}, \texttt{111101})$ for $F$ given below. Is it valid? **yes** $\boxed{\textbf{no}}$

   | $x$ | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
   |---|---|---|---|---|---|---|---|---|
   | $F(x)$ | 010 | 100 | 110 | 111 | 011 | 101 | 010 | 100 |

   **Solution:** No. Here $m_L = \texttt{011}$ and $m_R = \texttt{011}$. The left half of the tag is $t_L = F(\texttt{011}) = \texttt{111}$. The right half is $t_R = F(\texttt{011} + \texttt{001}) = F(\texttt{010}) = \texttt{110}$. The correct tag is 111110, not 111101. Bob rejects the pair.

   (b) Eve intercepts the valid message–tag pair $(\texttt{010101}, \texttt{101010})$. Construct a forgery for her.

   **Solution:** From the intercepted message–tag pair, Eve learns that $F(\texttt{010}) = \texttt{101}$. The pair

   $$m = \texttt{010011}, \qquad t = \texttt{101101}$$

   is a forgery. Its left tag is $F(\texttt{010}) = \texttt{101}$ and its right tag is $F(\texttt{011} + \texttt{001}) = F(\texttt{010}) = \texttt{101}$.

   There are two other possible forgeries. As Eve also learns that $F(\texttt{101} + \texttt{001}) = \texttt{010}$, the message-tag pairs $(\texttt{100011}, \texttt{010101})$ and $(\texttt{100101}, \texttt{010010})$ are also forgeries. (The fourth possible combination $(\texttt{010101}, \texttt{101010})$ is the intercepted pair itself and doesn't qualify as a forgery.)