All problems are of equal value.

1. The primitive operation we added to deterministic algorithms to make them randomized is the \( \text{rand}(k) \) operation, which in 1 operation will return a uniformly random number in the set \( \{0, \ldots, k - 1\} \). In this formalism we are allowed to specify \( k \), and in this problem we will consider what happens when this flexibility is not present.

   (a) Given \( k \geq \ell \geq 2 \), show how one can output a uniformly random number in \( \{0, \ldots, \ell - 1\} \) by only using \( \text{rand}(k) \) as a source of randomness, in \( O(1) \) expected time.

   (b) Given \( k \geq 2 \), show how one can output a uniformly random number in \( \{0, \ldots, k - 1\} \) by only using \( \text{rand}(2) \) as a source of randomness, in \( O(\log k) \) expected time.

2. In lecture it was shown that the family of hash functions \( \mathcal{H}_{k,p} \),

\[
\mathcal{H}_{k,p} = \left\{ h : \mathbb{Z}_p^k \to \mathbb{Z}_p, h(x) = \sum_{i=1}^{k} x_i b_i, b \in \mathbb{Z}_p^k \right\},
\]

is universal for any prime \( p \) and integer \( k \geq 1 \), in that for any \( x \neq y \in \mathbb{Z}_p^k \),

\[
\Pr_{h \in \mathcal{H}_{k,p}} [h(x) = h(y)] = \frac{1}{p},
\]

where \( h \) is taken uniformly from \( \mathcal{H}_{k,p} \). A stronger requirement is that of \( \ell \)-wise independence, which means that for any distinct \( x_1, \ldots, x_\ell \in \mathbb{Z}_p \) and (not necessarily distinct) \( y_1, \ldots, y_\ell \in \mathbb{Z}_p \),

\[
\Pr_{h \in \mathcal{H}_{k,p}} [h(x_1) = y_1 \wedge \cdots \wedge h(x_\ell) = y_\ell] = \frac{1}{p^\ell}.
\]

When \( \ell = 2 \), this is called pairwise independence.

   (a) Show that any family of hash functions that is pairwise independent is also universal.

   (b) Show that \( \mathcal{H}_{k,p} \) is not pairwise independent, for every \( k \) and \( p \).

   (c) Show that hash family \( \mathcal{H}'_{k,p} = \{ h : \mathbb{Z}_p^k \to \mathbb{Z}_p, h(x) = c + \sum_{i=1}^{k} x_i b_i, b \in \mathbb{Z}_p^k, c \in \mathbb{Z}_p \} \) is pairwise independent.

   (d) Show that \( \mathcal{H}'_{k,p} \) is not 3-wise independent, for every \( k \) and \( p \) with \( p^k \geq 3 \).