Some definitions:

12. Let $A[1 \dots n]$ be an array with $n$ different integers. Let $ran(n)$ a randomized function that outputs an integer $i$, $1 \leq i \leq n$ under the uniform distribution. Let us consider the following algorithms

    **Input:** $A[1 \dots n]$
    **from** $i = 1$ **to** $n$ **do**
      swap values $A[i]$ and $A[ran(n)]$

    **Input:** $A[1 \dots n]$
    **from** $i = n$ **downto** $1$ **do**
      swap values $A[i]$ and $A[ran(i)]$

    Do these algorithms output a uniform random permutation? Justify your answer.

13. Consider the following algorithm to generate an integer $r \in \{1, \dots, n\}$: We have $n$ coins labelled $m_1, \dots, m_n$, where the probability that $m_i$ = head is $1/i$. Toss the in order the coins $m_n, m_{n-1}, \dots$ until getting the first head, if the fist head appears with coin $m_i$, the $r = i$. Prove that the previous algorithm yield an integer $r$ with uniform distribution. i.e. the probability of getting any integer $r$ is $1/n$.)

14. Consider the set $S = \{1, \dots, n\}$.

    (a) We generate $X \subseteq S$ as follows: A fair coin is flipped independently for each element of $S$, if the coin lands H, the element is added to $X$, otherwise it is not. Prove that the resulting set $X$ is equally likely to be any one of the $2^n$ possible subsets.

    (b) Suppose $X, Y \subseteq S$ are chosen independently and u.a.r. from all $2^n$ subsets from $S$. Compute $\mathbf{Pr}[X \subseteq Y]$ and $\mathbf{Pr}[X \cup Y = S]$

15. Let $h(x) = x \mod m$ be a hash function, where $m = 2^p - 1$ for some prime number $p$. Let $w$ be a character string corresponding to the representation in radix $2^p$ of a natural number. Prove that, if $w'$ is a string obtained by permuting the symbols in $w$, $h(w') = h(w)$.

16. Consider the family $\mathcal{H}$ of hash functions $h : \{1, 2, 3, 4\} \to \{0, 1\}$ containing the three following functions

    - $h_1(1) = 0, h_1(2) = 1, h_1(3) = 1, h_1(4) = 0$
    - $h_2(1) = 1, h_2(2) = 0, h_2(3) = 1, h_2(4) = 0$
    - $h_3(1) = 1, h_3(2) = 1, h_3(3) = 0, h_3(4) = 0$

    Is $\mathcal{H}$ universal? Justify your answer.

17. There are different operations that we wish to implement on sets of integers. Take into account that in a set there are no repeated elements. Let $a[n]$ and $b[n]$ be arrays holding the elements in two sets $A$ and $B$ with $n$ elements. Provide an exact and a randomized algorithm for each of the following problems.

    (a) Given $a$ and $x \in \mathbb{N}$, are there integers $y, z \in A$ such that $x = y + z$?

    (b) Given $a$ and $b$, is $A = B$?

    Your algorithms should solve the problems in time $\Theta(n \log n)$ and in expected time $O(n)$, respectively.

18. Lucas' theorem says the following: If we have an integer $a$ such that: $a^{n-1} \equiv 1(modn)$, and, for every prime factor $q$ of $n-1$, it is not the case that $a^{(n-1)/q} \equiv 1(modn)$, then n is prime.

    Can this result be used to show that Primality belongs to NP?

19. Consider the following problems:

    - Modular factorial: Given $N$ bits natural numbers $x, y$ compute $x! \mod y$.
    - Smallest prime divisor: Given a $N$ bit natural number $x$, compute the smallest prime divisor of $x$.
    - Factoring: Given a $N$ bit natural number $x$, compute the factorization of $x$ as product of primes.

    (a) Prove that $y$ is prime if and only if, for each integer $x < y$, we have that $\text{mcd}(x!, y) = 1$.

    (b) Show that if Modular factorial can be solved in polynomial time, then Smallest prime divisor and Factoring could be solved in polynomial time.