Problem 1. Let \( n \in \mathbb{N} \). If there exists a primitive element modulo \( n \), then there exist \( \varphi(\varphi(n)) \) many.

Problem 2. \textit{(properties of the discrete logarithm)} We examine the properties of the discrete logarithm.

a) Compute the discrete logarithm of 18 and 1 in the group \( \mathbb{Z}_{79}^* \) with generator 3 (by trial and error if necessary).

b) How many tryings would be necessary to determine the discrete logarithm in the worst case?

Problem 3. \textit{(prove Proposition 7.5)} Prove Proposition 7.5 from the lecture, which gives a possibility to generate a primitive element modulo \( n \):

Let \( p > 3 \) be prime, \( p - 1 = \prod_{i=1}^{k} p_i^{l_i} \) the prime factorization of \( p - 1 \). Then,

\[
a \in \mathbb{Z}_p^* \text{ is a primitive element modulo } p \iff a^{\frac{p-1}{p_i}} \not\equiv 1 \pmod{p} \text{ for all } i \in \{1, \ldots, k\}.
\]