Homework

1. (from last week) Study the development (and if so desired the paper to referred to) in `https://www.irif.fr/~letouzey//download/examples_CiE2008.v` illustrating different ways to extract a division function. Try to *adapt* (see comments to solutions of last week) at least one of the methods to extract a modulo function (i.e. returning the remainder after the division).

2. Prove that for all natural numbers n there exists a list $[n_1, \ldots, n_k]$ of natural numbers that constitutes a prime factorisation of n, i.e. such that each n_i is prime and such that $n = n_1 \cdot \ldots \cdot n_k$, and extract a program implementing this specification. (For simplicity you may assume that 0 and 1 are 'prime'.)

   You may proceed as follows:

   - First formalise the statement, partitioning it as above (in prime and factorisation).
   - Show that (it is decidable whether) a natural number n is prime or has a non-trivial divisor d, i.e. such that exists n' with $n = d \cdot n'$ and $1 < d, n' < n$.
   - Show that a divisor of a divisor of n is a divisor of n.
   - Show that if d is a non-trivial divisor of n, then $n/d < n$.

   and follow the pattern of the above development for division. (You may freely use that development, and facts about natural numbers in the library, but try to develop the proof yourself).

   - Bonus (may be not so easy): Prove that the prime factorisation is unique up to the order of the elements (and repetitions of 0,1).