Advanced security ... , training set of problems for 9.06.2010

This is a training set of questions.

1. Consider a directed graph G in which each node has the output degree 1. Let $H(v)$ denote the end of an arc originating in v. Our goal is to find $u \neq u'$ such that $H(u) = H(u')$.

   How to speed up the algorithm by using two processors?

2. Write a BSP-style program for computing an arithmetic expression that corresponds to a full binary tree by 3 processors.

3. Try to speed up computation of $m^d \bmod n$ (RSA encryption) by computing it with two processors.

4. How to speed up matrix multiplication by using more than one processor? Again, formulate a solution as an BSP algorithm.