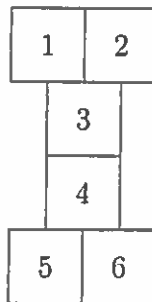


MS-A0401 Foundations of discrete mathematics
Second midterm exam 22.10.2015

Write your name, student number, and other information on every paper!
Calculators or tables are not allowed in this examination!

1. U and V use the RSA-algorithm to communicate with each other. U has the public key (n_U, k_U) and the private key (n_U, d_U) . V has the public key (n_V, k_V) and the private key (n_V, d_V) and both do, of course, keep their private keys secret. In addition they use the hash function h for signing. If now U receives a message, which in encrypted form is x from V and in addition the signature s then what calculations should U do in order to be convinced that V is the sender of the message?

2. With rotations and reflections of the figure below one gets the permutations $p_1 = (1)$, $p_2 = (1\ 6)(2\ 5)(3\ 4)$, $p_3 = (1\ 2)(5\ 6)$, and $p_4 = (1\ 5)(2\ 6)(3\ 4)$.



- (a) What should one show in order to prove that these permutations form a group? (You don't have to do these calculations!)
- (b) Determine the cycle index of this group.
- (c) Determine with the aid of Pólya's theorem in how many, non-equivalent with respect to the action of the group, ways one can colour the squares in the figure using two colours.
- 3.
- (a) Show that if two simple undirected graphs do not have the same chromatic number, then they are not isomorphic.
- (b) Determine the greatest common divisor of the numbers 38 and 48 using the Euclidean algorithm.

Turn over!!

4.

- (a) Draw pictures of all simple undirected non-isomorphic graphs in which there are 4 nodes and which are forests (that is, there is at most one simple path from each node to each other node).
- (b) Determine a Hamilton path in the graph below or explain why one cannot find such a path.

