Discrete mathematics: Examination rules

Basic rules:

1. To take the exam, you need to obtain credit from the classes (the rules for that are set by the class teacher). Lack of credit (while being graded at all) means that you need to get a classes credit during the June exam-time to be able to take the second term of the exam in September.

2. The exam will consist of 4-6 "practical" tasks similar to ones that you are solving during classes (examples below) and one "theoretical" task - a question about the material of the lecture (again, examples below). Some time before the exam, I am going to present you a list of about 30 questions from which I will choose one as a "theoretical question" for the exam. For my convenience, the exam will be graded on the scale of 0-1200 " small points" and after dividing by 20, they will change into 0-60 " course points".

To pass the course one needs to satisfy the following three conditions:

a) get credit from the classes;

b) obtain at least 50 " course points" from the classes and the exam (in total);

c) obtain at least 20 " course points" from the exam.

Every ten points above 50 gives you +0.5 to the final grade (so for 3.5 you need at least 60 "course points", for 4.0 you need 70, and so on).

During the exam, you should only have a simple calculator, an analog watch and something to write (also something to drink, if necessary) by yourself. In particular, you cannot have anything that could let you contact "the world outside" (e.g. a phone/smartphon/smartwatch/tablet etc.) not to mention any cribs. The consequences for breaking this rule are severe, up to automatically failing the course.

Tasks:

As you can see, the points for the tasks below sum up to more than 1200 points. This is because only some of them will appear in a particular exam (only Task 9 is guaranteed to appear).

1. (100-200 points) Logic: to transform a sentence of everyday speech or a logic gate circuit into a logical expression and then use the truth table to verify the logical value of this expression [Presentation 1a, slides 23-31, Presentation 1b, slides 28-29]

2. (100 points): Find a formula of an inverse function to a given function [Presentation 2, slide 29 - probably in the exam the example will be a bit more advanced]

3. (100-200 points) Provide the ordering of a few sequences (e.g. $a_n = n^2 + n + 1$, $b_n = n \log n$, $c_n = 2^n - n$) by the "Big O" notation prove that the ordering is correct by calculating appropriate limits [Presentation 3b, slides 16-17, 21-23]

4. (200-400 points) 1 or 2 tasks in number theory and cryptology. For example:

Extended Euclidian Algorithm [Presentation 4, slides 17-36] Solving systems of linear congruencies [Presentation 4, slides 60-64 i 76-83] Calculation a value of the Euler-φ function [Presentation 4, slides 86-87] Modular exponentiation with the application of Euler's Theorem [Presentation 4, slide 90] Cryptologic tasks of the type: Which of the pairs $(77, 21)$, $(165, 41)$, $(91, 17)$ can be a public key in the RSA system? Explain why the other two cannot constitute a public key. For the correct pair, calculate the private key, the number of the unit of cyphertext under which the unit of plaintext of number 10 is encrypted and what unit of the plaintext will be decrypted from the unit of cyphertext of number 6. [Presentation 5, slides 24-32].

5. (100-200 points) Prove something by mathematical induction[Presentation 6a, slides 9-13]

6. (200-300 points) Solve a non-homogeneous linear recurrence relation [Presentation 6c, slides 23-25]

7. (200-300 points) 2-3 short tasks in combinatorics: only an answer with a short justification is required. [Presentation 7a: slides 8, 11-12, 17-19, 21, Presentation 7b: slides 5-10, 18, 22-25, 35-40, Presentation 7c: slides 4-5,8-10]

8. (200 points) An algorithm of the graph theory: Which of the presented graphs has an Eulerian path or Eulerian circuit (explain why the other graphs do not)? Use the Fleury's algorithm to find this Eulerian path/circuit. The steps of the algorithm should be presented in the form of a table [Presentation 8b,slides 8, 14-29]. Or: Find a minimal path and its weight in a directed

graph using Dijkstra's algorithm. The steps of the algorithm should be presented in the form of a table[Presentation 8c, slides 24-39].

9. (100 points) A "theoretical" task - at least 2 weeks before the exam I am going to publish a list of about 30 questions. One of them will be chosen for the exam. Examples of such questions:

a) Prove that there are infinitely many prime numbers.

b) What is a recursion algorithm? Provide an example of such an algorithm (preferably from the lecture).

c) Draw one of each examples of a simple, connected graph with 5-7 vertices and 5-12 edges satisfying the following conditions or explain why such a graph does not exist.

I. A hamiltonian graph which is also a tree;

II. A hamiltonian graph which is not eulerian;

III. An eulerian graph which is not hamiltonian;

IV. An eulerian graph which has a separating vertex.