

Coursework II
Oliver Kullmann, November 24, 2008

Deadline: December 8, 2008 Submission only at the student's office.

This course works constitutes 10% of the overall marks for CS_232.

The possible marks for individual exercises sum up to 165, with 100 marks for basic exercises; results over 100 will be capped. Obviously, you do not need to do all exercises, but you should at least read through them and understand them enough, so that all exercises seem plausible to you.

When handing in your course work, please state clearly on top of your first sheet the module code, your name and student number, "Coursework II" and the date. For each single exercise, state the exercise number together with the heading for the exercise. Please answer clearly, and in complete sentences. Write legibly!

When using external sources, then you must make references (even for the lecture script)! The complete coursework must be written in its entirety by you. If you are using material from the scripts of previous years, then you must thoroughly rephrase it in your own words.

Since we cannot return your coursework to you, please keep a *copy for yourself*.

1 Graph colouring (30 marks)

1. Determine the chromatic number of graphs from the following graph classes, and prove your answer:
 - (a) the complete graphs K_n for $n \geq 2$, where one edge has been removed;
 - (b) forests.

[10 marks]

2. For a graph G denote by $\Delta(G)$ the maximal vertex degree.

- (a) Show that $\chi(G) \leq \Delta(G) + 1$.
- (b) Can we also (efficiently) find such a colouring?
- (c) And are there graphs with $\chi(G) = \Delta(G) + 1$?

[10 marks]

3. Design an "intelligent" algorithm (in pseudo-code) for solving the k -colouring problem (whether a graph is k -colourable or not), and discuss the potential savings compared to the algorithm simply enumerating all possible (potential) colourings.

[10 marks]

2 The Euclidean algorithm (50 marks)

Basic exercises

1. Compute the Euclidean sequence and the Euclidean extension sequence for the following pairs of numbers a, b ; in each case state explicitly how to represent $\gcd(a, b)$ as a linear combination of a and b :
 - (a) 66, 55
 - (b) 113, 63
 - (c) 255, 187
 - (d) 104, 116
 - (e) 1001, 338.

[20 marks]

More advanced exercises

2. Find worst-case examples for the Euclidean algorithm, that is, a recipe for producing pairs of numbers a, b such that the Euclidean algorithm needs maximally many steps before termination. Explain your choice. [10 marks]
3. Regarding the extended Euclidean algorithm and the sequences x_0, x_1, \dots and y_0, y_1, \dots , show that we have $x_0 \geq 0, x_1 \leq 0, x_2 > 0, x_4 < 0, x_5 > 0$ and so on, as well as $y_0 \leq 0, y_1 \geq 0, y_2 < 0, y_4 > 0, y_5 < 0$ and so on (compare the remarks in the script).

[20 marks]

3 Modular arithmetic (45 marks)

1. Explain how modular addition, subtraction and multiplication works, showing also some example calculations.

[10 marks]

2. Assume that the multiplication table of \mathbb{Z}_n is given. How then can we easily determine elements which are invertible (multiplicatively), and find their inverses in the positive cases?

[5 marks]

3. Decide, which of the following elements are invertible, and if they are, then show the inverse and how to compute it:

- (a) 7 in \mathbb{Z}_{17}
- (b) 18 in \mathbb{Z}_{38}
- (c) 121 in \mathbb{Z}_{158}
- (d) 10 in \mathbb{Z}_{19}
- (e) 4008 in \mathbb{Z}_{4009} .

[10 marks]

4. Compute the following exponentiations (show your calculations; use a pocket calculator; hint: not in all cases the binary expansion of the exponent is actually needed):

- (a) $\text{pow}_3(2, 36291928392133)$
- (b) $\text{pow}_{16}(7, 105)$
- (c) $\text{pow}_{100000}(20, 10000000)$
- (d) $\text{pow}_{119}(64, 238)$
- (e) $\text{pow}_{131}(97, 11401)$.

[20 marks]

4 Cryptography (40 marks)

In the following we assume $p = 59$, $q = 67$, and thus $n = 59 \cdot 67 = 3953$ and $N = \varphi(n) = 58 \cdot 66 = 3828$. As encryption key we use $e = 1117$.

1. Encrypt the plaintext message $m = 3600$, and show that decryption gives back the original message (show your computations).

[15 marks]

2. Decrypt the ciphertext message $c = 2566$, and show that encryption of the resulting plaintext gives back the ciphertext (show your computations).

[15 marks]

3. Discuss possibilities how to break RSA.

[10 marks]