Algebra 1 (2012)-Aalborg University
Lecture 5, September 20th

5th Lecture: Thursday September 20th, 8:15-12:00.
I will not be present during this lecture.

- Work in groups. Exercises from [Lau], 1.12 (page 41): 17, A, 18, 22, 41, 19.

  Exercise A: Let $N = n_1 n_2$, where n_1 and n_2 are relatively prime. Prove that $X \equiv a \pmod{N}$ if and only if $X \equiv a \pmod{n_1}$ and $X \equiv a \pmod{n_2}$. This exercise is a hint for solving exercise 18.

  Each group can write their solution for exercises 18 and 22, and leave it in my mailbox (just one set of exercises per group). Do not write it with the computer, please. The idea is to practice how to write exercises for the exam. If you cannot solve one exercise completely, hand in whatever you have, how you think that one may solve it ..., in the exam you may get points for an incomplete solution.

- Lecture: This part will consist of self-study in the group rooms. The topics are "Prime numbers" (the parts that we skipped last lecture of section 1.8, pages 19–24, you may also use Wikipedia) and "RSA" (section 1.9 and subsection 1.9.1, pages 24–26, line 13). I have written some slides. Your are welcome to orientate the teacher, by e-mail, about the successes and difficulties during the lecture.

Best regards,

Diego