Algebra 1 (2012)-Aalborg University
Lecture 7, September 18th

7th Lecture: Thursday September 27th, 8:15-12:00 at room G5-112.

- 8:15-8:45 Repetition from last lecture. Chinese remainder theorem. How to compute $\varphi(n)$. RSA (pages 16–17 + 22–29).
- 8:45-10:45 Work in groups. Exercises from [Lau], 1.12 (page 41): A, 18, B, C, D, 30 (i and ii), 41, 38, 42, 45 (i and ii).

  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.

  Exercise B: Check that 6 is composite using Fermat's little theorem but the same method of page 27 does not work for 9.

  Exercise C: Check that 341 is composite using lemma 1.9.4 (page 28).

  Exercise D: Check that 561 is a Carmichael number but it is not a strong pseudoprime.
- 10:45-12:00 Lecture: Groups. Groups and congruences. The composition table. Associativity. The first non-abelian group. Uniqueness of neutral and inverse elements. Multiplication by $g \in G$ is bijective. Examples of groups (pages 50-57).

Best regards,

Diego