Algebra 2010-Aalborg University

5th Lecture: Tuesday September 21st, 8:15-12:00 at room G5-112.

- 8:15-8:45 Repetition from last lecture. Factorization of integers. How to compute $\varphi(n)$. RSA (pages 22-29).
- 8:45-10:30 Work in groups. Check that 6 is composite using Fermat's little theorem but the same method of page 27 does not work for 9. Check that 341 is composite using lemma 1.9.4 (page 28). Exercises from [Lau], 1.12 (page 41): 30 (i and ii), 38, 41, 42, 45 (i and ii).
- 10:30-12:00 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 50-58).

Best regards,

Diego Ruano