Algebra 1 (2011)-Aalborg University
Lecture 17, November 16th

17th Lecture: Wednesday November 16th, 8:15-12:00 at room G5-112.
I will not be present during this lecture. The group G3-112 will be responsible for the lecture.

- 8:15-8:45 Repetition from last lectures. Group G3-112 will give this lecture. Order of a group element, cyclic groups and Groups and numbers (pages 72–78).
- 8:45-11:45 Work in groups and Lecture.
  - Exercise 28 in [Lau]
  - Self-study of ElGamal encryption system, section 4.5.2 in [Lau] (page 160) and Wikipedia. ElGamal can be defined using a cyclic group (as it is described in Wikipedia), however in [Lau], it is described for the cyclic group $\mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^*$. I have prepared some slides as well. Remark: ElGamal is nowadays used in practice using *elliptic curves*: it has smaller key sizes and faster operations. New standards are coming.
  - We have not seen yet that $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group. We have computed it for some concrete values of p, for instance for $p = 13$ in exercise 28. Exercise A: Write a Maple program that, given a prime p, finds a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. In this way, we have that $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group for that value of p (we will get a general proof in Exercise E). You can find some help for Maple in the slides for lecture 6 and in Mapleprimes.
  - Exercise B: Answer briefly to the following questions about ElGamal:
    1. How are the public and private keys generated?
    2. How does the sender encrypt a message?
    3. How does the receiver decrypt a message?
    4. How can the receiver be sure that he/she will recover the original message?
    5. Why cannot an encrypted message be decrypted without the private key?
  - Exercise C: Compute in Maple an example of ElGamal using the group $\mathbb{F}_p^*$, encrypt a message and then decrypt it.
  - Exercise D: We have seen in section 2.7 in [Lau] that $G = \mathbb{Z}/p\mathbb{Z}$, with p prime, is a cyclic group. Therefore, one could use this group for ElGamal. However, Is ElGamal secure for this choice of G?
  - Exercise E: One can prove that $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group for p prime. Prove that $(\mathbb{Z}/p\mathbb{Z})^*$, with p prime, is a cyclic group. Hints for solving the exercise:
    1. Prove that for $[a], [b] \in (\mathbb{Z}/p\mathbb{Z})^*$, with $\text{ord}([a]) = m$, $\text{ord}([b]) = n$ and $gcd(m, n) = 1$, one has that $\text{ord}([a][b]) = mn$
    2. Let $[a] \in (\mathbb{Z}/p\mathbb{Z})^*$ with $m = \text{ord}([a])$ as high as possible. Prove that $\text{ord}([b]) \mid m$ for every $[b] \in (\mathbb{Z}/p\mathbb{Z})^*$

3. Prove that for every $[b] \in (\mathbb{Z}/p\mathbb{Z})^*$ one has that $[b]^m = [1]$ and conclude that $m = p-1$ (hint: a polynomial of degree s can have at most s roots)

Each group can write their solution for exercises C, D and E and leave it in my mailbox (just one set of exercises per group). You can print exercise C and/or email me your Maple Worksheet. Exercise E is a bit difficult.

- 11:45-12:00 Common discussion in the lecture room directed by group G3-112. At the end of the lecture, group G3-112 will orientate the teacher, by e-mail, about the concrete successes and difficulties during the lecture.

Best regards,

Diego