Algebra 1 (2011)-Aalborg University
Lecture 20, November 24th

20th Lecture: Thursday November 24th, 12:30-16:15 at room G5-112.

I will not be present during this lecture. The group G3-117 will be responsible for the lecture.

- 12:30-13:00 Repetition. Group G3-117 will give this lecture. The topics are: Euclidean algorithm. Cyclic groups and ElGamal cryptosystem (10–12, 74–76 and 160)
- 13:00-16:00 Work in groups.
  - Self-study of the cryptosystem Knapsack (Merkle-Hellman), see Knapsack in Wikipedia, based in the Knapsack problem. I have prepared some slides as well (see the web page). Knapsack is very fast and elegant, but was broken in 1982. However, there have been several improvements that have also been broken (in the 80's and 90's). It is not considered secured nowadays but it would be very nice to get an improvement.
  - Exercise A: Answer briefly to the following questions about Knapsack:
    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 B: Compute an example of Knapsack, encrypt a message and then decrypt it. You can use Maple.
  - Exercise C: With the notation of section 1.5 in [Lau], prove that $r_{i+2} < r_i/2$. This exercise estimates the number of iterations in the Euclidean algorithm (it shows that the remainders become smaller quite fast). Hints for solving the exercise:
    1. Prove that if $2r_{i+1} \leq r_i$, then $r_{i+2} < r_{i+1} \leq r_i/2$ (ok)
    2. Prove that if $2r_{i+1} > r_i$, then $r_{i+2} = r_i - r_{i+1}$ (then ...)
  - Exercise D: Compute in Maple an example of ElGamal (see lecture 17) using the group $\mathbb{F}_p^*$, encrypt a message and then decrypt it.
  - Exercise E: 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? (Hint: is it difficult to compute the "equivalent operation of the logarithm" for the sum?)
  - Exercise F: 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 $\mathrm{ord}([a]) = m$, $\mathrm{ord}([b]) = n$ and $gcd(m, n) = 1$, one has that $\mathrm{ord}([a][b]) = mn$
2. Let $[a] \in (\mathbb{Z}/p\mathbb{Z})^*$ with $m = \mathrm{ord}([a])$ as high as possible. Prove that $\mathrm{ord}([b]) \mid m$ 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, E and F and leave it in my mailbox (just one set of exercises per group).

- 16:00-16:15 Common discussion in the lecture room directed by group G3-117. At the end of the lecture, group G3-117 will orientate the teacher, by e-mail, about the concrete successes and difficulties during the lecture.

Best regards,

Diego