Afleveringsopgaver 5
Algebra 1, EVU 2011-Aalborg Universitet

These are the exercises that you can hand in, latest 23rd May in the morning. You need not solve them in the same order as they appear.

- Ex A: Consider the group $(\mathbb{Z}/34\mathbb{Z})^*$. Check that $[13] \in (\mathbb{Z}/34\mathbb{Z})^*$. Compute $[13]^{-1}$.
- Ex B: Compute the Cayley table of $(\mathbb{Z}/8\mathbb{Z})^*$. Compare it with the one of $(\mathbb{Z}/4\mathbb{Z}, +)$
- Ex C: Prove that $(\mathbb{Z}/8\mathbb{Z})^*$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Is $(\mathbb{Z}/8\mathbb{Z})^*$ a cyclic group?
- Ex D: Consider an example of RSA in Maple.
- Ex E: Consider an example of ElGamal in Maple.
- Ex F: Prove that $\varphi(n) = \varphi(2n)$ if n is odd.
- Ex G: Prove that $(\mathbb{Z}/13\mathbb{Z})^*$ is cyclic by finding a primitive element.
- Exercises 2.11.1, 2.11.2, 2.11.6, 2.11.7, 2.11.9.
- Ex H: Explain the coset decoding method (section 2.11).
- Ex I: Prove Theorem 3 and Theorem 4 (4) of section 2.11.
- Ex J: Prove that $(\mathbb{Z}/p\mathbb{Z})^*$, with p prime, is a cyclic group.
  - 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 $\mathrm{ord}([a][b]) = mn$
  - 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 $[b] \in (\mathbb{Z}/p\mathbb{Z})^*$
  - 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)
- Ex K: Let $a \in (\mathbb{Z}/p\mathbb{Z})^*$, with p prime. What it the probability that a is a primitive element?
- Exercises and examples from previous lectures.

Med venlig hilsen,

Diego