Re-Exam for Algebra 1 at Aalborg University
For 3. semester Mat
Friday, February 22nd 2013, 10:30–14:30.

You are allowed to use books and your notes. However calculators, computers, pdas, tablets, ebooks or phones are not allowed.
A reasoned explanation should follow the solution of the exercises. Moreover, the intermediate steps leading to the solution should also be written down. You can write the exam in Danish or English.
The percentage following each exercise number stands for the exercise's value in the final mark. There are 4 exercises.

Exercise 1 *(15%)* Consider the RSA cryptosystem with public key $N = pq$, where $p = 5$ and $q = 11$.

1. Prove that $e = 3$ is a valid encryption exponent.
2. Find the decryption exponent d for $e = 3$.
3. Encrypt the message $X = 5$ using the encryption exponent $e = 3$.

Exercise 2 *(35%)*

1. Let $\sigma = (1\ 5)(3\ 4) \in S_5$. Compute the number of inversions of σ and write σ as a product of the minimal number of simple transpositions.
2. Determine whether each of the following subsets of the symmetric group S_4, is a subgroup of S_4:
   - $A = \{e, (1\ 2), (1\ 2\ 3), (3\ 4\ 1)\}$
   - $B = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$
   - $C = \{e, (1\ 3), (1\ 2\ 3\ 4), (2\ 4), (1\ 4)\}$
   - $D = \{e, (1\ 2)\}$
3. Consider the following subgroup of S_4 (you do not have to prove that it is a subgroup):

$$H = \{\varepsilon, (1\ 2), (3\ 4), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\}$$

   Let $\sigma = (1\ 3\ 2\ 4)$ and $\eta = (1\ 2)$.

   - Prove that $|\sigma| = 4$, $|\eta| = 2$ and $\sigma\eta\sigma = \eta$.
   - Write a group isomorphism from the dihedral group D_4 to H (One has that $D_4 = \{1, a, a^2, a^3, b, ba, ba^2, ba^3\}$, where $|a| = 4$, $|b| = 2$ and $aba = b$).

Exercise 3 *(20%)*

1. How many elements are there of order 7 in $\mathbb{Z}/30\mathbb{Z}$?
2. Write down all the elements of order 5 in $\mathbb{Z}/30\mathbb{Z}$.
3. How many subgroups are there of order 5 in $\mathbb{Z}/30\mathbb{Z}$?. Write down the subgroups of order 5 in $\mathbb{Z}/32\mathbb{Z}$.
4. How many elements of $(\mathbb{Z}/13\mathbb{Z})^*$ are generators of $(\mathbb{Z}/13\mathbb{Z})^*$? (hint: you do not need to compute them).

Exercise 4 *(30%)* Let $G = \langle g \rangle$ with $\text{ord}(g) = 20$, and let $H = \langle g^4 \rangle$.

1. Is H a normal subgroup in G?
2. Compute G/H.
3. Write the composition table of G/H.
4. Compute the order of every element in G/H. Is G/H a cyclic group?

Husk at skrive jeres fulde navn på hver side af besvarelsen. Nummerer siderne, og skriv antallet af afleverede ark på 1. side af besvarelsen. God arbejdslyst.