Re-Exam for Algebra 1 at Aalborg University

For 3. semester Mat

Thursday, March 1st 2012, 8:15–12:15.

You are allowed to use books and your notes. However calculators, computers, pdas 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.

Exercise 1 *(15%)* Solve the following system of congruences in X,

$$\begin{aligned} X &\equiv 1 \pmod 2 \\ X &\equiv 0 \pmod 3 \\ X &\equiv 2 \pmod 7 \end{aligned}$$

Exercise 2 *(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. Encrypt the message $X = 4$ using the encryption exponent $e = 3$.

3. Find the decryption exponent d for $e = 3$.

Exercise 3 *(15%)*

1. Compute the order of the permutation $\sigma = (1\ 2\ 3)(3\ 4\ 5)(5\ 6\ 1)$ (hint: the cycles are not disjoint).

2. Compute the sign of the previous permutation σ.

Exercise 4 *(20%)*

1. How many elements are there of order 11 in $\mathbb{Z}/32\mathbb{Z}$?

2. Write down all the elements of order 8 in $\mathbb{Z}/32\mathbb{Z}$.

3. How many subgroups are there of order 8 in $\mathbb{Z}/32\mathbb{Z}$?. Write down the subgroups of order 8 in $\mathbb{Z}/32\mathbb{Z}$.

4. How many elements of $(\mathbb{Z}/11\mathbb{Z})^*$ are generators of $(\mathbb{Z}/11\mathbb{Z})^*$? (hint: you do not need to compute them).

Exercise 5 *(20%)* Let $G = D_3 = \{e, a, a^2, b, ba, ba^2\}$, where $\operatorname{ord}(a) = 3$, $\operatorname{ord}(b) = 2$ and $aba = b$. Let $H = \langle a \rangle$.

1. Prove that H is a normal subgroup in G.

2. Write the composition table for G/H.

Exercise 6 *(15%)* Prove that for $n \geq 3$, the center of S_n is $\{e\}$, i.e. $Z(S_n) = \{e\}$.

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.