Give arguments to all solutions. List all collaborators.

Warmup

1. To check authenticity of documents from MATEMATIK AB one uses the public key $n = 221$, $e = 7$. Check authenticity of a document with signature 208 1 45 112 208 1 45 76 54. (One uses $A = 1, \dots, Z = 26$, space $= 27$.)

2. Biggs 13.5.3

3. Biggs 20.10.1

4. Show that $\mathbb{Z}_n^*$ (with multiplication as operation) is a group.

5. If G is a group, show that the following sets are subgroups of G:

   (a) $\{x \in G \mid ax = xa\}$ where a is a fixed element of G. (The centraliser of a)

   (b) $\{x \in G \mid ax = xa \text{ for all } a \in G\}$. (The center of G)

   (c) $\{x^n \mid n \in \mathbb{Z}\}$. (The cyclic subgroup generated by x)

6. There are two different (non-isomorphic) groups of order 4. Construct the group table for each of these. Find two subgroups of S_4 that are isomorphic to these.

7. How many finite subgroups are there in $\mathbb{R}^*$ with operation multiplication?

8. Show that if G is a group, then a has the same order as a^{-1} for all $a \in G$.

9. Let M be the group $\{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} | n \in \mathbb{Z}\}$, with matrix multiplication as operation. Show that M is isomorphic to $\mathbb{Z}$ under addition.

10. If G is a group with an even number of elements, show that there is an element $a \neq 1$ such that $a^2 = 1$.

11. Suppose that $a^2 = 1$ for each element a in a group G. Show that G is abelian.

The exercises below are to be handed in
Tuesday October 10, 13.15 at the latest.

1. Use the RSA system with $n = 33 = 3 \cdot 11$. Put $A = 1, \ldots, Z = 26$, space $= 27$.
   (a) Let the encryption key be $e = 3$. Encrypt DISCRETE MATHEMATICS.
   (b) Determine the decryption key d and decrypt the message 19 1 4 12 26.
2. Biggs 20.10.3 and 20.10.4
3. Let G be an abelian group and a and b two elements in G of order r and s, respectively, where r and s are coprime, that is, the greatest common divisor of r and s is 1. What can be said about the order of ab?

   Show (by an example) that if G is non-abelian then we cannot say anything about the order of ab, that is, the order of ab is not a function of r and s.
4. Biggs 20.8.4 and 20.8.5
5. Biggs 20.10.12

Bonus problems (no collaboration)

6. How many elements in the cyclic group C_r are generators, that is have order r?
7. Show that the symmetric group S_5 has no subgroup of order 15.