Cryptography I, homework sheet 1

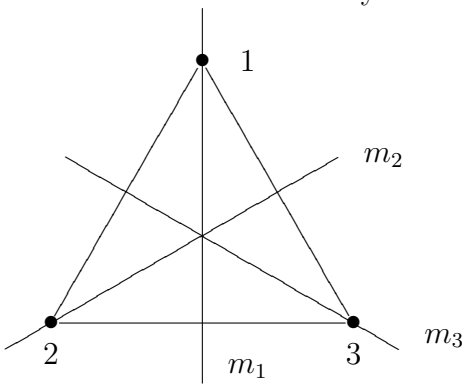
Due: 23 September 2011, 10:45

1. Consider the subset $\mathbb{Z}[i]$ of the complex numbers given by

$$\mathbb{Z}[i] = \{a + bi \in \mathbb{C} | a, b \in \mathbb{Z}\}.$$

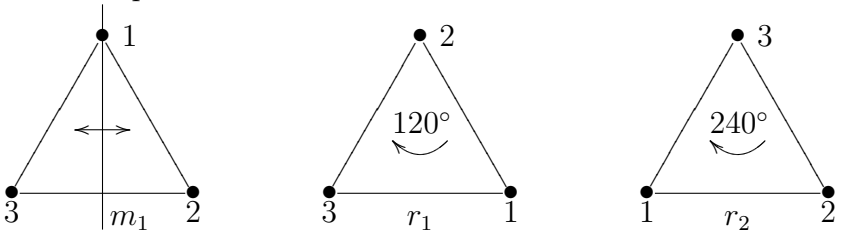
Show that $\mathbb{Z}[i]$ is a subgroup of $(\mathbb{C}, +)$.

2. This exercise if about the symmetry group of the equilateral triangle.



Symmetry operations of the equilateral triangle are maps that do not change the shape of the triangle. There are 6 different such maps:
id: identity map,
m_1: reflection in axis through 1,
m_2: reflection in axis through 2,
m_3: reflection in axis through 3,
r_1: rotation by 120° mapping 1 to 3,
r_2: rotation by 240° mapping 1 to 2.

For example:



To determine whether the set of symmetry operations on the equilateral triangle forms a group with respect to composition first write a table with all results of composing two transformations. For maps we write $r_1 \circ m_1$ if first m_1 and then r_1 is executed. The table is to be read as follows: each table entry is the result of performing the operation stated in same row in the leftmost column first, followed by the one in the same column in the top row. E.g. $r_1 \circ m_1$ is found in the row of m_1 and the column of r_1 and equals m_2.

(a) Show that this gives a group; you do not need to prove associativity.

(b) Find all subgroups. State the order of the group and all its subgroups.

(c) Compute the order of r_1 and m_3.