Martin Schlichenmaier
Université du Luxembourg

Mathematical Foundations

Exercise sheet 1

1. Let $\mathbb{F}_{23}$ be the finite field with 23 elements. For $\bar{5} = 5 \bmod 23$ calculate its inverse element with respect to the multiplication by using Euclid's algorithm (e.g. via expressing the $gcd(n, m)$ as integer combination of n and m).

2. (a) Let $a = a_n a_{n-1} \dots a_1 a_0$ be the presentation of a number a by a decimal expansion. Show (using residue calculus) that $3|a$ if and only if $3|(\sum_{i=1}^{n} a_i)$.
(b) Find a corresponding rule for the divisibility by 9.

3. Determine up to isomorphy all groups of order less or equal 5. Are these groups abelian?

4. Let S_3 be the group of bijective maps from $\{1, 2, 3\}$ to $\{1, 2, 3\}$. Give all elements of this group. Calculate the order of the elements and find all subgroups of S_3. Is this group abelian?

5. Let $\varphi(n)$ be Euler's phi-function which is defined as the number of elements in $\mathbb{Z}_n^*$, the group of units in the ring $\mathbb{Z}_n$. Show that for p and q prime, one has

$$\varphi(p) = (p-1), \qquad \varphi(p \cdot q) = (p-1)(q-1).$$

The web-page of the course: `http://www.cu.lu/~schliche/cours-mics`