February 22, 2011
Due date: March 24, 2011.

Final exam in Advanced Algebra 83-804

General rules: You are supposed to solve these problems alone without an external help or a cooperation with fellow students. Please write solutions clearly (preferably type) and submit to me via email (listed on my homepage). Try to find short solutions. All statements should be explained. I might ask to explain unclear passages.
The maximal grade is 100.

1. Let p be a prime. Prove that $\mathbb{F}_p^x$ is a cyclic group (here $\mathbb{F}_p^x = \mathbb{F}_p \setminus \bar{0}$ is the multiplicative group of the finite field with p elements; another notation we used for $\mathbb{F}_p$ is $\mathbb{Z}_p$).

Here are steps to follow:

a) (15 pts.) Let $\mathbb{Z}_n$ be the cyclic group of order $n > 1$. Show that if $d|n$ then there is the unique subgroup $C_d \subset \mathbb{Z}_n$ of order d (i.e., $|C_d| = d$). Show that the number of generators of C_d is equal to $\phi(d)$ (ϕ is the Euler function).

Deduce from this the Gauss identity $n = \sum_{d|n} \phi(d)$.

b) (15 pts) Let H be a finite group of order n such that for any $d|n$ the set $H_d \subset H$ of elements $x \in H$ satisfying $x^d = 1$ have at most d elements. Prove that H is cyclic. (Hint: use the Gauss identity from a), and the notion of the order of an element in a group.)

c) (15 pts.) Deduce that $\mathbb{F}_p^x$ is cyclic by applying Lagrange theorem on number of roots of polynomials over $\mathbb{F}_p$.

d) (5 pts.) How many generators are there in the group $\mathbb{F}_p^x$?

Bonus problems: $1\frac{1}{2}$. (10 pts.) Prove that $\mathbb{Z}_{p^2}^x$ is cyclic. (Hint: use the fact that $\mathbb{Z}_p^x$ is cyclic, i.e., it is generated by an *integer* $g \in \mathbb{Z}$, and try to correct it (if needed!) in order to find $g' \in \mathbb{Z}$ generating $\mathbb{Z}_{p^2}^x$.)

$1\frac{3}{4}$. (15 pts.) Check that the proof you constructed in a-b-c in fact proves the following: Let $H \subset F^x$ be a finite subgroup of the multiplicative group of a field F (finite or infinite). Assume that the order $|H| = p^n$ for some prime p and integer $n \geq 1$. Then H is cyclic.

(In fact one can prove that, any finite subgroup of a multiplicative group of a field (finite or infinite) is cyclic.)

2. Let p be a prime number, and $GL(2, \mathbb{F}_p)$ be the group of invertible 2×2 matrices with elements in the field $\mathbb{F}_p$. Consider the following subgroup (called the affine group)

$$Aff(p) = \left\{ \begin{pmatrix} a & b \\ & 1 \end{pmatrix} \mid a \in \mathbb{F}_p^x,\ b \in \mathbb{F}_p \right\} \subset GL(2, \mathbb{F}_p) \ .$$

The operation in the group $Aff(p)$ is the usual multiplication of matrices.

a) (15 pts.) Prove that $Aff(p)$ is solvable. Namely, there are subgroups $G_1 \subset G_2 \subset Aff(p)$ such that G_1 is normal in G_2, G_2 is normal in $Aff(p)$, and quotient groups G_2/G_1 and $Aff(p)/G_2$ are abelian.

b) (15 pts) Let G be a group, and let $a \in G$ be an element.
The set $C_a = \{gag^{-1} \mid g \in G\} \subset G$ of elements is called the conjugacy class of a.

Compute conjugacy classes of $Aff(p)$ and their sizes.

c) (10 pts.) Let $g \in \mathbb{F}_p^x$ be a generator for the multiplicative group of the field $\mathbb{F}_p$ (proven to exist in problem 1). Prove that the set

$$S = \left\{ \begin{pmatrix} g & \\ & 1 \end{pmatrix}, \begin{pmatrix} g^{-1} & \\ & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ & 1 \end{pmatrix} \right\}$$

is a symmetric generating set for $Aff(p)$.

d) (10 pts.) Construct the Cayley graph for $(Aff(p), S)$ with $p = 5$. (Hint: organize elements of $Aff(p)$ in groups.)

Bonus problems: $2\frac{1}{2}$. (5 pts.) Let p be a prime. Consider the subgroup $(\mathbb{F}_p^x)^2 = \{a^2 \mid \in a \in \mathbb{F}_p^x\}$ consisting of squares in the multiplicative group $\mathbb{F}_p^x$. Use results from problem 1 to compute the order of the factor group $|\mathbb{F}_p^x/(\mathbb{F}_p^x)^2|$.

$2\frac{3}{4}$. (5 pts.) Use the problem $2\frac{1}{2}$. to determine conjugacy classes in the special affine group

$$SAff(p) = \left\{ \begin{pmatrix} a & b \\ & a^{-1} \end{pmatrix} \mid a \in \mathbb{F}_p^x,\ b \in \mathbb{F}_p \right\} \subset SL(2, \mathbb{F}_p) \ .$$

Good luck!