1 Homework 1.

1. (Algebraic independence) Suppose G_1 and G_2 are two groups. We say G_1 and G_2 are *algebraically independent* if there are no proper normal subgroups N_1 and N_2 of G_1 and G_2, respectively, such that $G_1/N_1 \simeq G_2/N_2$.

   (a) Prove that G_1 and G_2 are algebraically independent if and only if $G_1 \times G_2$ satisfies the following property: suppose H is a subgroup of $G_1 \times G_2$ and the projection of H to i-th component is G_i for $i = 1, 2$. Then $H = G_1 \times G_2$.

   (b) Suppose G_1 and G_2 are two finite groups and $\gcd(|G_1|, |G_2|) = 1$. Prove that G_1 and G_2 are algebraically independent.

2. Suppose G is a finite group. Suppose for every positive integer n,

$$|\{g \in G \mid g^n = e\}| \leq n,$$

   where e is the neutral element of G. Use the following steps to prove that G is a cyclic group.

   (a) Prove that if there is an element of order d in G, then there are exactly $\phi(d)$ elements of order d in G, where $\phi(d)$ is the Euler ϕ-function.

   (b) For every positive number d, let $\psi(d)$ be the number of elements of G that has order d. Show that $\psi(d) \leq \phi(d)$ and $\psi(d) \neq 0$ implies that $d||G|$.

   (c) Prove that $\psi(d) = \phi(d)$ if d is a positive divisor of $|G|$. Deduce that G is a cyclic group. (Hint. Use the previous step and the fact that $\sum_{d|n} \phi(d) = n$ for every positive integer n.)

   (Remark. Later we will use this result to deduce that the group of units of every finite field is cyclic.)

3. Find the automorphism group of the Cayley graph of $\mathbb{Z}$ with respect to the set $S := \{1, -1\}$. (You have to list the elements of this group, and write the product of every two elements as an element in the given list.)

4. (Symmetries and Diophantine equations) Suppose a and b are non-negative integers. Prove that if $k = \frac{a^2+b^2}{1+ab}$ is an integer, then k is a perfect square. (Hint. We look for some symmetries of the set

$$V := \{(a,b) \in \mathbb{Z}^2 \mid a^2 + b^2 - kab - k = 0\}.$$

View this equation as a quadratic equation in terms of a. Deduce that the sum of two zeros is kb. Thus if $(a,b) \in V$, then $(b, kb-a) \in V$. Hence, multiplication by the matrix $\begin{pmatrix} 0 & 1 \\ -1 & k \end{pmatrix}$ is a *symmetry* of V. Suppose $(a_0, b_0) \in V$, a_0 and b_0 are non-negative, $a_0 \geq b_0$ and a_0 is the smallest such integer. Suppose $b_0 > 0$. Deduce that $kb_0 - a_0 \geq a_0$. Argue why this is a contradiction. Obtain that $b_0 = 0$, and so $k = a_0^2$. Can you use this argument to list all the elements of V?)

(Remark. The idea of using symmetries of an equation in order to find many solutions is extremely useful. An important example is the Markoff equation

$$x^2 + y^2 + z^2 = 3xyz.$$

Clearly $(1,1,1)$ is a solution of the Markoff equation. Using a similar argument as the above problem, we get that if (a,b,c) is a solution of the Markoff equation, then so are $(3bc-a, b, c)$, $(a, 3ac-b, c)$, and $(a, b, 3ab-c)$. Moreover, we can permute the components and change the sign of two of the components. It turns out starting with $(1,1,1)$ using the above mentioned symmetries, one can get all the integer solutions of the Markoff equation.)

5. Recall that an automorphism of a group G is a group isomorphism from G to itself. The set of all the automorphisms of G is denoted by $\mathrm{Aut}(G)$. One can see that $\mathrm{Aut}(G)$ forms a group under the composition of functions. In this problem, we want to prove that $\mathrm{Aut}(C_n) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, where C_n is a cyclic group of order n and $(\mathbb{Z}/n\mathbb{Z})^\times$ is the set of elements of $\mathbb{Z}/n\mathbb{Z}$ that have multiplicative inverse.

   (a) Suppose $C_n = \langle g \rangle$ and $\phi \in \mathrm{Aut}(C_n)$. Suppose $\phi(g) = g^m$. Prove that $\gcd(m,n) = 1$. (Hint. Use the fact that $o(g) = o(\phi(g))$ and $o(g^m) = \frac{o(g)}{\gcd(o(g),m)}$.)

(b) Suppose $\gcd(m, n) = 1$. Prove that $\phi_m : C_n \to C_n, \phi_m(x) := x^m$ is an automorphism of C_n.

(c) Prove that $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(C_n), (m + n\mathbb{Z}) \mapsto \phi_m$ is an isomorphism.