Homework 1

due October 9, 2001 in class

1. (a) Prove that the squares of the elements in $\mathbb{Z}/4\mathbb{Z}$ are just $\bar{0}$ and $\bar{1}$.
   (b) Prove that for any integers a and b the sum a^2+b^2 never leaves a remainder of 3 when divided by 4.
2. Let $n \in \mathbb{Z}$, $n > 1$ and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$.
   (a) Prove that if a and n are not relatively prime, there exists an integer b with $1 \leq b < n$ such that $ab \equiv 0 \mod n$ and deduce that there cannot be an integer c such that $ac \equiv 1 \mod n$.
   (b) Prove that if a and n are relatively prime then there is an integer c such that $ac \equiv 1 \mod n$ (use the fact that the g.c.d. of two integers is a $\mathbb{Z}$-linear combination of the integers).
   (c) Conclude that $(\mathbb{Z}/n\mathbb{Z})^\times$ is the set of elements $\bar{a}$ of $\mathbb{Z}/n\mathbb{Z}$ with $(a, n) = 1$.
3. Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$.
   (a) Prove that G is a group under multiplication (called the group of roots of unity in $\mathbb{C}$).
   (b) Prove that G is not a group under addition.
4. Let G be a group. Prove that if $x^2 = 1$ for all $x \in G$ then G is abelian.
5. Let $G = \{a_1, a_2, \ldots, a_n\}$ be a finite, abelian group. Prove that $(a_1 \cdots a_n)^2 = 1$.
6. If x is an element of finite order n in the group G, prove that the elements $1, x, x^2, \ldots, x^{n-1}$ are all distinct. Deduce that $|x| \leq |G|$.
7. Dummit, Foote I.1.2 Exercise 18 (page 28)