Homework 1
Solutions

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.

   Proof:
   (a) The elements in $\mathbb{Z}/4\mathbb{Z}$ are $\bar{0}, \bar{1}, \bar{2}, \bar{3}$. It is easy to check that $\bar{0}^2 = \bar{0}$, $\bar{1}^2 = \bar{1}$, $\bar{2}^2 = \bar{0}$ and $\bar{3}^2 = \bar{1}$.
   (b) Since by part (a) squares are always $\bar{0}$ or $\bar{1}$, the sum of squares can never be $\bar{3}$ which shows the statement of part (b).
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 $(a, n) = 1$.

   Proof:
   (a) If a and n are not relatively prime, then there exists $x, m, b \in \mathbb{Z}$ such that $a = mx$ and $n = bx$. This implies in particular that $ba = bmx = mn$ so that $ab \equiv 0 \mod n$. Suppose that there exists a $c \in \mathbb{Z}$ such that $ac \equiv 1 \mod n$. This means that $ac = 1 + kn$ for some k. Multiplying by b amounts to $abc = b + bkn$ or, using $ab = mn$, $b = n(mc - kb)$ so that b is a multiple of n. This contradicts $1 \leq b < n$.
   (b) If a and n are relatively prime, their g.c.d is 1. Hence by the hint there exist $c, m \in \mathbb{Z}$ such that $ca + mn = 1$ which is equivalent to $ac \equiv 1 \mod n$.
   (c) By the previous two parts $\bar{a}$ has a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$ if and only if a and n are relatively prime.
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.

Proof:

(a) Firstly, G is closed under multiplication. Suppose $x, y \in G$ so that $x^n = 1$ and $y^m = 1$ for some $n, m \in \mathbb{Z}^+$. Then $(xy)^{nm} = (x^n)^m(y^m)^n = 1$ so that xy is also in G. Associativity holds by the multiplicative associativity of the complex numbers. The identity is 1 which is certainly in G. If $z \in G$ then $z^n = 1$ for some $n \in \mathbb{Z}^+$. Hence $z^{-1} = z^{n-1}$ which is also in G.

(b) 1 is in G, but $1 + 1$ is not in G since there is no $n \in \mathbb{Z}^+$ such that $2^n = 1$. Hence G is not closed under addition and hence cannot be a group with respect to $+$.

4. Let G be a group. Prove that if $x^2 = 1$ for all $x \in G$ then G is abelian.

   Proof: G is abelian if $xy = yx$ for all $x, y \in G$. Since $xy \in G$ we know that $(xy)(xy) = 1$. Hence xy is the inverse of xy. Note that $(xy)(yx) = x(yy)x = xx = 1$. Hence yx is also the inverse of xy, and since the inverse is unique it follows that $xy = yx$.

5. Let $G = \{a_1, a_2, \dots, a_n\}$ be a finite, abelian group. Prove that $(a_1 \cdots a_n)^2 = 1$.

   Proof: Every element a_i has a unique inverse element. Either the inverse is a_i itself or another element in G. Hence, since G is abelian, $(a_1 \cdots a_n)^2 = 1$.

6. If x is an element of finite order n in the group G, prove that the elements $1, x, x^2, \dots, x^{n-1}$ are all distinct. Deduce that $|x| \leq |G|$.

   Proof: Assume that there are a, b with $0 \leq a < b < n$ such that $x^a = x^b$. This implies that $x^{b-a} = 1$ where $b - a < n$ which contradicts the assumption that x has order n. Since the n elements $1, x, \dots, x^{n-1}$ are all distinct and all in G it follows that $|x| \leq |G|$.

7. Dummit, Foote I.1.2 Exercise 18 (page 28)

   Proof: The group in question is $Y = \langle u, v \mid u^4 = v^3 = 1, uv = v^2u^2 \rangle$.

   (a) The relation $v^3 = 1$ implies $v^2 = v^{-1}$ by multiplication with v^{-1} on both sides.

   (b) Note that $v^2u^3v = (v^2u^2)(uv) = (uv)(v^2u^2) = uv^3u^2 = u^3$. Hence $vu^3 = v(v^2u^3v) = u^3v$ so that v and u^3 commute.

   (c) Since $u^4 = 1$ it follows that $u^9 = u^8u = u$. Hence by (b) $vu = vu^9 = u^3vu^6 = u^6vu^3 = u^9v = uv$ so that u and v commute.

   (d) By the last relation in Y and (c) we have $uv = v^2u^2 = u^2v^2$. Multiplying by $v^{-1}u^{-1}$ on both sides yields $uv = 1$.

(e) By the relations of Y we have $u^4v^3 = 1$. Using (d) this reduces to $u = 1$, and again by (d) $v = 1$. This means that Y is the trivial group.