Math 581 Problem Set 9

1. Let m and n be relatively prime positive integers.
(a) Prove that $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ as RINGS. (Hint: First Isomorphism Theorem)
(b) Show by example that part (a) may be false if m and n are not assumed to be relatively prime.
(c) Prove that if one has rings R and S and $R \cong S$ as rings, then $R^\times \cong S^\times$ as groups under multiplication, i.e., the units in the rings are isomorphic as groups.
(d) Prove that if R and S are rings, then $(R \times S)^\times \cong R^\times \times S^\times$ as groups under multiplication.
(e) Use part (d) to conclude that $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$.
(f) Now let $m = p$ and $n = q$ for some primes p and q. Prove that the order of the group $(\mathbb{Z}/pq\mathbb{Z})^\times$ is $(p-1)(q-1)$.
(g) Prove that if $\gcd(a, pq) = 1$, then $a^{(p-1)(q-1)} \equiv 1 (\operatorname{mod} pq)$.

2. Let N be a subgroup of G such that $[G : N] = 2$. Prove that N is a normal subgroup of G.

3. Show that every element in $\mathbb{Q}/\mathbb{Z}$ has finite order. (Recall you showed last homework that there are infinitely many elements in $\mathbb{Q}/\mathbb{Z}$.)

4. Let p be an odd prime.
(a) Show that $a^2 \equiv b^2 (\operatorname{mod} p)$ if and only if $a \equiv b (\operatorname{mod} p)$ or $a \equiv -b (\operatorname{mod} p)$.
(b) Show that $\varphi : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ defined by $\varphi(a) = a^2$ is a group homomorphism whose image is a subgroup H of index 2. (Hint: Use part (a) to determine the kernel of φ and use the first isomorphism theorem.)
(b) Define $\psi : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$ by

$$\psi(a) = \begin{cases} +1, & \text{if } a \text{ is a square in } \mathbb{Z}/p\mathbb{Z} \\ -1, & \text{otherwise.} \end{cases}$$

Prove that ψ is a group homomorphism. (Hint: Consider the quotient group $(\mathbb{Z}/p\mathbb{Z})^\times / H$.)
(c) Conclude that if neither a nor b is a square in $\mathbb{Z}/p\mathbb{Z}$, then their product ab is a square in $\mathbb{Z}/p\mathbb{Z}$. (We used this result last term when showing there was a polynomial that was irreducible but reducible modulo every prime p.)

5. If N is a normal subgroup of G and if every element of N and G/N has finite order, prove that every element of G has finite order.

6. Let $G = \mathbb{R} \times \mathbb{R}$.
(a) Show that $N = \{(x, y) | x = -y\}$ is a normal subgroup of G.
(b) Describe the quotient group G/N.

7. Prove that $\mathbb{R}^\times / \langle -1, 1 \rangle \cong \mathbb{R}_{>0}$ where $\mathbb{R}_{>0}$ is the group of positive real numbers.

8i. Let G be the set of all matrices of the form

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

where $a, b, c \in \mathbb{Q}$.
(a) Show that G is a group under matrix multiplication.
(b) Find the center $Z(G)$ of G and show it is isomorphic to $\mathbb{Q}$.
(c) Show that $G/Z(G) \cong \mathbb{Q} \times \mathbb{Q}$.