Your Name:

Duration of the mid-term exam is 90 minutes. There are five problems, worth 50 points, and an extra credit problem, worth 2 points. Show all your work for full credit. Books, notes etc. are prohibited. Calculators are NOT permitted.

1. (i) (6 points) Find $\gcd(1001, 33)$ and write it as a linear combination of the two given integers.

(ii) (2 points) Disprove with a counterexample: If $a^2 \equiv b^2 \pmod{n}$, then $a \equiv b \pmod{n}$.

(iii) (2 points) Prove that if a is an odd integer, then $a^2 \equiv 1 \pmod{8}$.

2. (i) (5 points) Let S be a set, and let $\sim$ be an equivalence relation on S. Prove that each element of S belongs to exactly one of the equivalence classes of S determined by the relation $\sim$.

(ii) (5 points) Consider the set $\mathbb{Z}$ where $x \sim y$ if and only if $2 \mid (x + y)$. Prove that $\sim$ is an equivalence relation on S, and then describe all the elements of $S/\sim$, i.e. find all the equivalence classes.

3. (10 points) Prove that the set of all 8-th roots of unity is a group of order 8 under the usual multiplication of complex numbers. In this problem, I want you to find all the roots and then prove that the set of all roots satisfies the axioms of a group. Also, identify the inverse of each element. You may use the fact that the multiplication of complex numbers is associative.

4. (i) (6 points) Let S be the set of real numbers of the form $a+b\sqrt{2}$, where $a, b \in \mathbb{Q}$ and are not simultaneously zero. Show that S becomes a group under the usual multiplication of real numbers. You may use the fact that the multiplication of real numbers is associative.

(ii) (6 points) Construct the multiplication table for $U(9)$, and prove that $U(9)$ is a group under multiplication modulo 9. Find the inverse and the order of each element of $U(9)$.

5. (i) (4 points) Let G be a group. Prove that if $x^2 = e$ for all $x \in G$, then G is abelian.

(ii) (2 points) Prove or disprove: A group of order 3 contains a self-inverse different from the identity element.

(iii) (2 points) Prove or disprove: A group of order 4 contains two self-inverses different from the identity element.

EXTRA CREDIT PROBLEM For any integer $n > 2$, show that there are at least two elements in $U(n)$ that satisfy $x^2 = 1$.

WORKSHEET