Math 74, Sec. 2, Instructor: Walter Kim
Midterm (50 pts.), Thursday, October 27, 2005

1. (5 pts.) Prove the following formula by induction for $n \in \mathbb{N}$.

$$\sum_{i=0}^{n} r^i = \frac{1 - r^{n+1}}{1 - r}$$

2. (9 pts.) (a) State the Well-Ordering Principle.

2 (con't).

(b) Let n be an integer > 1. Show using the Well-Ordering Principle that n has a least divisor that is > 1.

(c) So by part (b), 15 has a least divisor that is > 1. What is it?

(d) Let n be an integer > 1. By part (b), n has a least divisor > 1, call it d. Prove that d is prime. Prove this by contradiction. (You will have to suppose that d has a divisor c such that $1 < c < d$).

3. (9 pts.) The following is the Linear Congruence Theorem: Let a, b, and m be integers with $m > 1$. Suppose $gcd(a, m) = 1$. Then the linear congruence $ax \equiv b \pmod{m}$ has a unique solution modulo m.

(a) Let x_1 and x_2 be two solutions to the linear congruence $ax \equiv b \pmod{m}$. The Linear Congruence Theorem says that the solution to the linear congruence is unique modulo m. This tells you that x_1 and x_2 are related in what way?

(b) Which numbers in the set $\{0, 1, 2, 3, 4, 5\}$ are solutions to $2x \equiv 4 \pmod{6}$? Why does this not contradict the fact that the Linear Congruence Theorem says that the solution of a linear congruence should be unique?

3 (con't).

(Linear Congruence Theorem): Let a, b, and m be integers with $m > 1$. Suppose $gcd(a, m) = 1$. Then the linear congruence $ax \equiv b \pmod{m}$ has a unique solution modulo m.

(c) Prove the existence of the solution. (You will use Euclid's Divisor Theorem for a and m and multiply the equation you get by b.)

4. (10 pts.) In this exercise we will prove Euclid's Theorem which asserts: There are infinitely many primes. We will prove this by contradiction.

(a) What do we have to suppose in this proof to prove by contradiction?

(Lets start the proof): So now let P be the set of all primes. We can write $P = \{p_1, p_2, \ldots, p_n\}$.

(b) What are the p_i's and how many are there? Why can we say this?

(c) Name some element of P so we know it is nonempty. Why do we need to do this? (It has to do with the next step and M.)

(Continuing the proof): Now let $M = p_1 p_2 \cdots p_n + 1$.

(d) M has a prime divisor. Why? (Write the statement the theorem or proposition that tells us this).

4 (con't).
(e) Let $p_i \in P$. Does $p_i | M$? Prove your answer. (Use Division Theorem, what is the remainder?)

(f) Finish the proof. (There are only a couple sentences left.)

5. (9 pts.) (a) Finish the definition. A subset $J \subset \mathbb{Z}$ is called an ideal of $\mathbb{Z}$ if it satisfies the following three conditions...

(b) Show that $I = \{12s + 18t : s, t \in \mathbb{Z}\}$ is an ideal.

(c) The Principle Ideal Theorem tells us that $I = \{12s + 18t : s, t \in \mathbb{Z}\}$ from part (b) should be of the form $\{kg : k \in \mathbb{Z}\}$ for some g. What is the g for this I?

(d) Is $\mathbb{N}$ an ideal of $\mathbb{Z}$? Prove your answer.