CS 1050 Homework 2 Solutions

1. Theorem 2: $\sqrt{3}$ is not rational.

Proof by contradiction: Assume $\sqrt{3}$ is rational. Then by definition $\sqrt{3} = r/s$ for integers r and s where $s \neq 0$. Divide out all common factors greater than 1 between r and s and call the new values a and b respectively. Thus $\sqrt{3} = a/b$ and by squaring both sides and multiplying both sides by b^2 we get $a^2 = 3b^2$. Since the right-hand side of the equation is divisible by 3, so is a^2 (the left-hand side), and, by Lemma 1, so is a. Since a is divisible by 3, we can rewrite it as $a = 3k$ for integer k. Thus $a^2 = (3k)^2 = 9k^2$ and, combined with the previous equation, $a^2 = 9k^2 = 3b^2$. Mathematical manipulation gives us that $b^2 = 3k^2$ which means b^2 is divisible by 3 as above. Since b^2 is divisible by 3, Lemma 1 tells us that b is divisible by 3 as well. However, we assumed that a and b have no common factors. Thus, we have a contradiction and $\sqrt{3}$ must be irrational. □

2. We need to prove some lemmas before we can complete the proof.

Lemma 2.1: Let a be an integer such that $a = 5k + j$ where j and k are integers and j is from 1 to 4. Then the remainder when a^2 is divided by 5 is non-zero.(Note: This can be split up into four different lemmas, one for each case).

Proof: Assume $a = 5k+j$. Then $a^2 = 25k^2+10kj+j^2 = 5(5k^2+2kj)+j^2$. Since $5(5k^2+2kj)$ is divisible by 5, any non-zero remainder must come from the last term j^2. If $j = 1$ then $j^2 = 1$ and the remainder is 1. If $j = 2$ then $j^2 = 4$ and the remainder is 4. If $j = 3$ then $j^2 = 9$ and the remainder is 4. If $j = 4$ then $j^2 = 16$ and the remainder is 1. In each case, the remainder is non-zero. □

Lemma 2.2: If a is an integer and a^2 is a multiple of 5, then a is also a multiple of 5.

Proof by contradiction: Assume a is an integer and a^2 is a multiple of 5, but a is NOT a multiple of 5. Then a can be written in the form $5k + j$ for integers j and k with j in the range 1 to 4. But from Lemma 2.1 we know that the remainder when a^2 is divided by 5 is non-zero; thus, a^2 is not a multiple of 5 as we had assumed. We can conclude that if a is an integer and a^2 is a multiple of 5, then a is also a multiple of 5. □

Theorem: $\sqrt{5}$ is not rational.

Proof by contradiction: Assume $\sqrt{5}$ is rational. Then by definition $\sqrt{5} = r/s$ for integers r and s where $s \neq 0$. Divide out all common factors between r and s and call the new values a and b respectively. Thus $\sqrt{5} = a/b$ and by squaring both sides and multiplying both sides by b^2 we get $a^2 = 5b^2$. Since the right-hand side of the equation is divisible by 5, so is a^2 (the left-hand side), and, by Lemma 2.2, so is a. Since a is divisible by 5, we can rewrite it as $a = 5k$ for integer k. Thus $a^2 = (5k)^2 = 25k^2$ and, combined with the previous equation, $a^2 = 25k^2 = 5b^2$. Mathematical manipulation gives us $b^2 = 5k^2$ which means b^2 is divisible by 5 as above. Since b^2 is divisible by 5, Lemma 2.2 tells us that b is divisible by 5 as well. However, we assumed that a and b have no common factors. Thus, we have a contradiction and $\sqrt{5}$ must be irrational. □

3. The proof breaks down in one of the lemmas.

Conjecture: Let a be an integer such that $a = 4k + 2$ where k is an integer. Then the remainder when a^2 is divided by 4 is non-zero.

Attempted proof: $a^2 = (4k + 2)^2 = 16k^2 + 16k + 4 = 4(4k^2 + 4k + 1)$. Note that this is evenly divisible by 4. So the conjecture is false.

Our proof method requires that the remainder be non-zero so that we can show that 4 is a factor of both a and b. Because the conjecture is false, we cannot use this proof method. (In fact, because $\sqrt{4}$ is rational, *no* proof that $\sqrt{4}$ is irrational, using any method, can work.)

4 a) **Proof.** Let $z = a^2$ such that z is a multiple of p, where p is a prime number. And z can written as $z = a \cdot a$. By Theorem 3, we know either a is a multiple of p or a is a multiple of p. Thus a is a multiple of p.

b) We just need to give a counterexample. Say, $a = 6$, $p = 9$. Here, $a^2 = 36$ is a multiple of 9, but $a = 6$ is not a multiple of 9. So, we have at least one case where a, p are integers, $p \neq 0, a^2$ is a multiple of p, but a is not a multiple of p.

5 a) $f_1(x) = x$, f_2 and f_3 do not exist, $f_4(x) = 1$.

b) $g(x) = x \ mod \ 5 + 1$.