MATH 220 Homework 10

Xander Naumenko

November 28, 2021

Question 1. We will use proof by contradiction so suppose not, i.e. suppose that $\exists a \in \mathbb{N}$ s.t. $\equiv 2 \mod 6$ and $a \equiv 7 \mod 9$. Then $\exists m, n$ s.t.

$$a = 6m + 2 = 9n + 7 \implies 6m - 9n = 5 \implies 3(2m - 3n) = 5$$

Clearly 5 isn't divisible by 3 so this is impossible, so the only possibility is that our original assumption was wrong and no such a exists. $\square$

Question 2. As the hint suggests, consider the equation modulo 4. When doing so we get that

$$y^2 \equiv 3 \mod 4$$

There are two possible cases: either y could be even or odd. If it is even then $\exists a \in \mathbb{Z}$ s.t. $y^2 = (2a)^2 = 4a^2 \equiv 0 \mod 4$, and if it is odd then $\exists b \in \mathbb{Z}$ s.t. $y^2 = (2b+1)^2 = 4(b^2+b)+1 \equiv 1 \mod 4$. In either case it is not possible that $y^2 \equiv 3 \mod 4$ which is a necessary condition for the original equation to have solutions, so no such $x, y \in \mathbb{Z}$ exist. $\square$

Question 3a. We will use proof by contradiction so suppose that the inverse wasn't unique. Then there are two functions f_1^{-1}, f_2^{-1} such that they are both inverses of f but $\exists y_1 \in Y$ s.t. $f_1^{-1}(y_1) \neq f_2^{-1}(y_1)$. We proved in class that if f permits an inverse then it must be bijective, and the definition of the inverse implies

$$f(f_1^{-1}(y_1)) = x_1 = f(f_2^{-1}(y_1))$$

The injectivity of f implies then that $f_1^{-1}(x_1) = f_2^{-1}(x_1)$, but this contradicts the assumption that the two inverses were unique. Thus that assumption must have been incorrect and only one inverse function exists. $\square$

Question 3b. We will first show that $f^{-1} \circ g^{-1}$ is an inverse, and by part a it is also the unique inverse. For any $y \in Y$, we have that

$$f^{-1} \circ g^{-1}(g \circ f(x)) = f^{-1}(g^{-1}(g(f(x)))) = f^{-1}(f(x)) = x$$

Thus $f^{-1} \circ g^{-1}$ fulfills the definition of being an inverse, so it must be unique by part a. $\square$

Question 4. We will use proof by contradiction, so suppose not. Then $\exists a \in \mathbb{Z}, b \in \mathbb{N}, \gcd(a, b) = 1$ s.t. $\sqrt[3]{25} = \frac{a}{b}$. Expanding we get that

$$25 = (\frac{a}{b})^3 \implies a^3 = 25b^3$$

Since $5|25b^3$, this means that $5|a^3$ as well. Since 5 is prime this means that $5|a \implies \exists c \in \mathbb{Z}$ s.t. $a = 5c$. Plugging this in again we get

$$125c^3 = 25b^3 \implies b^3 = 5c^3$$

Using the exact same logic as before $5|b$, but this contradicts our assumption that $gcd(a,b) = 1$. Thus our assumption must be wrong and $\sqrt[3]{25} \notin \mathbb{Q}$. $\square$

Question 5. Proof by contradiction: suppose that it was a perfect square, i.e. suppose that $\exists l \in \mathbb{N}$ s.t. $l^2 = 2n$. Then we would have

$$l = \sqrt{2n} = \sqrt{2}\sqrt{n} = m\sqrt{2}$$

By assumption l and m are natural numbers, and in class we proved that $\sqrt{2} \notin \mathbb{Q} \implies \sqrt{2} \notin \mathbb{N}$. Thus the left side is a natural number and the right side isn't, clearly violating equality. The only possibility is that our original assumption was false and $2n$ isn't a perfect square. $\square$

Question 6. To show it is bijective we will show that it is injective and surjective. For surjective, let $m \in \mathbb{Z}$. If m is even then choose $n = m - 7$ which is odd, and we have that $f(n) = f(m - 7) = m - 7 + 7 = m$. If m is odd then choose $n = -m - 3$ which is even, and we have that $f(n) = f(-m-3) = m - 3 + 3 = m$. Thus $\forall m \in \mathbb{Z}, \exists n \in \mathbb{Z}$ s.t. $f(n) = m$, so f is surjective.

For injective, Let $n_1, n_2 \in \mathbb{Z}$. Suppose $f(n_1) = f(n_2)$, we will show that $n_1 = n_2$. There are three cases: the two numbers are both odd, both even or one of each. If they are both even, then we have that

$$f(n_1) = -n_1 + 3 = f(n_2) = -n_2 + 3 \implies n_1 = n_2$$

If they are both odd, then we have that

$$f(n_1) = n_1 + 7 = f(n_2) = n_2 + 7 \implies n_1 = n_2$$

If one is odd and one is even, without loss of generality assume that n_1 is the even one. Then we get that

$$f(n_1) = f(2m_1) = -2m + 1 = f(n_2) = f(m_2 + 1) = 2m_2 + 8 = 2(m_2 + 4)$$

The left side is odd and the right side is even, so it is not possible that n_1 has different parity then n_2. Thus all possible cases are either not possible or agree with $n_1 = n_2$, so f is injective. Since it is both injective and surjective it is bijective.

For the inverse, it is the following:

$$f^{-1}(m) = \begin{cases} -m-3 & m \text{ odd} \\ m-7 & m \text{ even} \end{cases}$$

To show that this is the case, let $m \in \mathbb{Z}$. Then if m is even we have that $m - 7$ is odd and

$$f^{-1}(f(m)) = f^{-1}(m-7) = m$$

If m is odd then $-m - 3$ is even and we have

$$f^{-1}(f(m)) = f^{-1}(-m-3) = m$$

Thus f^{-1} is the inverse. $\square$

Question 7a. Expanding we get

$$f \circ f \circ f \circ f(x) = f \circ f(1 - \frac{1}{x}) = f(1 - \frac{1}{1-\frac{1}{x}}) = f(1 - \frac{x}{x-1}) = 1 - \frac{1}{1 - \frac{x}{x-1}}$$

$$= 1 - \frac{x-1}{-1} = x = i_A$$

Question 7b. First, note that $i_A = x$ is a bijective function on A. This means that for every $y \in A, \exists x \in A$ s.t. $\exists z \in A$ s.t. $g \circ g(y) = x$ and $g(x) = y$, which is the definition of being surjective.

For injectivity, we will use proof by contradiction so suppose g wasn't injective. Then we have that $\exists x_1, x_2 \in A$ s.t. $g(x_1) = g(x_2)$ and $x_1 \neq x_2$. Using the identity for g we know that $g(g(g(x_1))) = g(g(g(x_2)))$ and $g(g(g(x_1))) = x_1$ and $g(g(g(x_2))) = x_2$. This would imply that $x_1 = x_2$ which contradicts our assumption, so it must be that g is injective as well. Since g is injective and surjective this means that g is bijective. $\square$

Question 7c. By part a f is bijective, so it must have an inverse. the inverse is the following: $f^{-1}(x) = \frac{1}{1-x}$. Plugging in we have $f^{-1}(f(x)) = 1 - \frac{1}{\frac{1}{1-x}} = x$ so it is an inverse, and by question 3 it is the unique inverse. $\square$

Question 8. We will use proof by contradiction, so suppose that such an integer k exists that is rational. Then we would have that $\exists a \in \mathbb{Z}, b \in \mathbb{N}$ s.t. $\gcd(a, b) = 1$ and $\sqrt{k} = \frac{a}{b}$. Then we have that

$$k = \frac{a^2}{b^2} \implies a^2 = kb^2$$

Then $k|a^2$. Since k isn't a perfect square it must have a prime factor p with an odd degree, since if all prime factors had even degrees it would be a perfect square. Then $p|a^2$, and since $p|k$ with odd degree it means that $p|a$ as well. Then we have that $\exists c \in \mathbb{Z}$ s.t. $a = cq$. Then we have that $kb^2 = q^2c^2$. Since k is divisible by an odd number of q either $q|b$ or $q|c$. In the latter case we can repeat this process, and since k this process will eventually terminate and the former case will occur. When this happens we have that $q|b$, which contradicts our assumption that $\gcd(a, b) = 1$ and thus no such k exists. $\square$