Math 330 • Number Systems
Test 2 Solutions, April 24, 2023 Instructor: Dikran Karagueuzian

1. A sequence $(a_n)_{n=1}^{\infty}$ satisfies $a_1 = a_2 = a_3 = 1$ and $a_{n+1} = a_n + a_{n-1} + a_{n-2}$ for $n \geq 3$. In this problem you will prove by induction that $a_n < 2^n$ for all $n \geq 1$.

   (a) (2 points) Identify a statement $P(n)$ to be proved.

   Solution: Let $P(n)$ be the statement "$a_n < 2^n$".

   (b) (2 points) Complete the base step of the induction.

   Solution: We show that $a_n < 2^n$ for $n = 1, 2, 3$. To see this, observe that $a_1 = 1 < 2 = 2^1$, $a_2 = 1 < 4 = 2^2$, and $a_3 = 1 < 8 = 2^3$.

   (c) (8 points) Complete the induction step.

   Solution: Suppose that $P(k)$ is true for all k such that $1 \leq k \leq n$, where $n \geq 3$. We will show that $P(n+1)$ is also true. We know that $P(n-2)$, $P(n-1)$ and $P(n)$ are true by the induction hypothesis, so we have $a_{n-2} < 2^{n-2}$, $a_{n-1} < 2^{n-1}$, and $a_n < 2^n$.

   Add the three inequalities to get $a_n + a_{n-1} + a_{n-2} < 2^n + 2^{n-1} + 2^{n-2}$. The left-hand-side is a_{n+1} by definition of the sequence. On the right-hand-side we have

   $$2^n + 2^{n-1} + 2^{n-2} = 2^n(1 + \frac{1}{2} + \frac{1}{4}) = 2^n \cdot \frac{7}{4} < 2^n \cdot 2 = 2^{n+1}$$

   Combining these observations, we have $a_{n+1} = a_n + a_{n-1} + a_{n-2} < 2^n + 2^{n-1} + 2^{n-2} < 2^{n+1}$. This proves $P(n+1)$ and completes the induction step.

   (d) (1 point) In your proof, did you use strong induction?

   Solution: Yes.

2. Consider carefully each of the following propositions and attempted proofs. Indicate what is wrong with each attempted proof, if anything. (Some proofs may be correct.) *Hint: you are not being asked whether the propositions themselves are true. You are being asked to find the errors, if any, in the proofs.*

   (a) (5 points) **Proposition:** For any positive integer n, $\sum_{i=1}^{n} i = \frac{1}{2}(n + \frac{1}{2})^2$.

   Attempted Proof. We will prove this by induction. Let $P(n)$ be the statement that $\sum_{i=1}^{n} i = \frac{1}{2}(n + \frac{1}{2})^2$.

   For the base step, a calculation shows that $P(n)$ is true for $n = 1$.

For the induction step, we show that if $P(n)$ is true then $P(n+1)$ is true. This is again a calculation: assuming $P(n)$ we have $\sum_{i=1}^{n} i = \frac{1}{2}(n+\frac{1}{2})^2$. Now

$$\begin{aligned}\sum_{i=1}^{n+1} i &= \frac{1}{2}(n+\frac{1}{2})^2 + (n+1) \\ &= \frac{1}{2}(n^2+n+\frac{1}{4}+2n+2) \\ &= \frac{1}{2}((n^2+2n+1)+(n+1)+\frac{1}{4}) \\ &= \frac{1}{2}((n+1)+\frac{1}{2})^2\end{aligned}$$

This final equality gives us $P(n+1)$, so we have proved $P(n) \Rightarrow P(n+1)$ and the proof is complete.

Solution: The proof is wrong, because the "calculation" referred to in the base step does not show that $P(1)$ is true. In fact $\sum_{i=1}^{1} i = 1$, while $\frac{1}{2}(1+\frac{1}{2})^2 = \frac{9}{8}$.

(b) (5 points) **Proposition:** Any positive integer m factors uniquely into a product of primes.

Attempted Proof. We prove this by strong induction on m.

For the base step, $m = 1$, m has no prime factors and the only possible factorization is $m = 1$.

For the induction step, if m is a prime, then m is its own factorization, and no other factors are possible by definition of prime.

If m is not prime, then m must have a factor l which is less than m, so $m = kl$ for some $k < m$, $l < m$. Now apply the induction hypothesis to k and l: the factorization of m is (factorization of l) $\cdot$ (factorization of k), so again m factors into primes. Since there is only one factorization of l and only one factorization of k, there is only one factorization of m.

Thus m factors uniquely into primes. This completes the induction step and so completes the proof.

Solution: The proof is wrong, because many choices of l may be possible, and even though the (strong) induction hypothesis tells us that the factorization of l is unique, the resulting factorization of m is not unique, because another choice of l might result in a different factorization.

3. Answer the following questions about sets A and B.

(a) (3 points) Is it possible that both $A \in B$ and $A \subseteq B$ are true? (Only a yes or no answer is required.)

Solution: Yes.

(b) (10 points) Give an example of such sets, or a proof that no such sets A and B exist to support your answer to the first part.

Solution: (Many examples are possible.) Let $A = \{1\}$, $B = \{\{1\}, 1\}$.

4. Let X, Y, Z be sets and $f\colon X \to Y$, $g\colon Y \to Z$ be functions.

(a) (4 points) Suppose $g \circ f$ is one-to-one. Must f be one-to-one? Must g be one-to-one? (Only yes/no answers are necessary.)

Solution: Yes, f must be one-to-one. No, g need not be one-to-one.

(b) (10 points) Give proofs or examples to justify your answers to the previous part.

Solution: Suppose that $g \circ f$ is one-to-one. We will show that f is one-to-one. To do this, we must show that, for $x_1, x_2 \in X$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$. So suppose $f(x_1) = f(x_2)$. It follows that $g(f(x_1)) = g(f(x_2))$, so $x_1 = x_2$ since $g \circ f$ is one-to-one.

To see that g need not be one-to-one, let $X = \{1\}$, $Y = \{a, b\}$, $Z = \{y, z\}$. Define f by $f(1) = a$ and g by $g(a) = g(b) = y$. Then $g \circ f$ is one-to-one, but g is not one-to-one.

(c) (4 points) Suppose $g \circ f$ is onto. Must f be onto? Must g be onto? (Only yes/no answers are necessary.)

Solution: No, f need not be onto. Yes g must be onto.

(d) (10 points) Give proofs or examples to justify your answers to the previous part.

Solution: To see that f need not be onto, let $X = \{1\}$, $Y = \{a, b\}$, $Z = \{y\}$. Define f by $f(1) = a$ and g by $g(a) = g(b) = y$. Then $g \circ f$ is onto, but f is not onto.

Suppose that $g \circ f$ is onto. We show that g is onto. To see this, we must show that if $z \in Z$, there is a $y \in Y$ with $g(y) = z$. Since $g \circ f$ is onto, there is an $x \in X$ with $g(f(x)) = z$. Now let $y = f(x) \in Y$, and we have $g(y) = z$ as required.

5. Let X, Y be sets and let $f\colon X \to Y$ be a function.

   (a) (8 points) Suppose that C and D are subsets of Y. Prove that $f^{-1}[C \cap D] = f^{-1}[C] \cap f^{-1}[D]$.

   Solution: By definition, $f^{-1}[C \cap D] = \{x \in X \mid f(x) \in C \cap D\}$. By definition of intersection $f(x) \in C \cap D$ iff $f(x) \in C$ and $f(x) \in D$. Thus $f^{-1}[C \cap D] = \{x \in X \mid f(x) \in C \text{ and } f(x) \in D\}$. Again by definition of intersection ("and") this means $\{x \in X \mid f(x) \in C \text{ and } f(x) \in D\} = \{x \in X \mid f(x) \in C\} \cap \{x \in X \mid f(x) \in D\}$. But this is $f^{-1}[C] \cap f^{-1}[D]$, as required.

   (b) (8 points) Suppose A and B are subsets of X. Either prove that $f[A \cap B] = f[A] \cap f[B]$, or give a counterexample to show that this equality need not be true.

   Solution: This equality need not be true. Suppose that $X = \{1, 2\}$, $Y = \{y\}$, $f(1) = f(2) = y$, and $A = \{1\}$, $B = \{2\}$. Then $A \cap B = \varnothing$, so $f[A \cap B] = \varnothing$, while $f[A] = f[B] = \{y\}$, so $f[A] \cap f[B] = \{y\}$.

   It is instructive to check where an attempted proof that $f[A \cap B] = f[A] \cap f[B]$ along the lines of the previous part fails. We observe that $f[A \cap B] = \{f(x) \mid x \in A \text{ and } x \in B\}$, while $f[A] \cap f[B] = \{f(a) \mid a \in A\} \cap \{f(b) \mid b \in B\}$. In other words, for $f[A] \cap f[B]$, we are allowed to choose two different elements a and b, but for $f[A \cap B]$ we can choose only one element x.

   In the previous part, we were able to make two conditions on one element an intersection of sets, but here there are two elements to contend with, so we can't make $f[A \cap B]$ into the intersection of sets on the other side of the equality.

6. Let $\mathbb{Z}^+$ denote the positive integers and consider the function $f\colon \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$ defined by $f(m, n) = 2^{m-1}(2n - 1)$. In what follows you may use the Fundamental Theorem of Arithmetic (FTA), but you must quote it explicitly if you do.

   (a) (9 points) Is f one-to-one? Prove that your answer is correct.

   Solution: Yes, f is one-to-one. We will show that if $f(m_1, n_1) = f(m_2, n_2)$ then $(m_1, n_1) = (m_2, n_2)$.

   If $f(m_1, n_1) = f(m_2, n_2)$ then $2^{m_1-1}(2n_1 - 1) = 2^{m_2-1}(2n_2 - 1)$. This is an equation of positive integers, and by the FTA the number of factors of 2 in each side of the equation is the same. Since $(2n_1 - 1)$ and $(2n_2 - 1)$ are both odd, they contain no factors of 2, so $m_1 - 1 = m_2 - 1$ and also $m_1 = m_2$ and $2^{m_1-1} = 2^{m_2-1}$. Now we can cancel the factors of 2 to get $(2n_1 - 1) = (2n_2 - 1)$, so $n_1 = n_2$.

Since $m_1 = m_2$ and $n_1 = n_2$, $(m_1, n_1) = (m_2, n_2)$ and so f is one-to-one.

(b) (9 points) Is f onto? Prove that your answer is correct.

Solution: Yes, f is onto. To see that f is onto, we must show for any positive integer z that there exist positive integers m, n with $f(m, n) = z$.

Since z is a positive integer, using the FTA we may write $z = 2^a b$ where b is an odd positive integer and $a \geq 0$. This means b can be written as $2n - 1$ where n is a positive integer and a can be written as $m - 1$ where m is a positive integer. Thus $z = 2^{m-1}(2n - 1) = f(m, n)$, as required.

7. Answer the following questions about arithmetic mod 59.

(a) (7 points) Show that there is a positive integer x such that $x \cdot 47 \equiv 1 \mod 59$.

Solution: Observe that 59 is prime: it's enough to check that 59 is not divisible by $2, 3, 5, 7$. Now $47 < 59$, so $(47, 59) = 1$ and by the linear combination interpretation of gcd, we know there are $x, y \in \mathbb{Z}$ such that $x \cdot 47 + y \cdot 59 = 1$. This means that $x \cdot 47 \equiv 1 \mod 59$. This x could be negative, but we can add a multiple of 59 to x to make it positive without changing the property $x \cdot 47 \equiv 1 \mod 59$.

(b) (12 points) Find a number m in $\{0, 1, 2, \ldots, 58\}$ which is a representative of $[x]_{59}$, i.e. a number such that $m \equiv x \mod 59$.

Solution: The number x in part (a) can be found using the Euclidean Algorithm, so we'll first do that. Notice that $59 = 47 \cdot 1 + 12$, $47 = 12 \cdot 3 + 11$, and $12 = 11 \cdot 1 + 1$. These are all the divisions required by the Euclidean algorithm, so now we trace back through the steps to express 1 as $x \cdot 47 + y \cdot 59$.

From the last step, $1 = 12 - 11$. Now $11 = 47 - 3 \cdot 12$ and $12 = 59 - 47$. Substituting, we get $1 = (59 - 47) - (47 - 3(59 - 47)) = 4 \cdot 59 - 5 \cdot 47 = 236 - 235$. It follows that $x = -5$ satisfies $x \cdot 47 \equiv 1 \mod 59$. The same will be true for any representative of the class $[-5]_{59}$, in particular 54.

Thus the answer is $m = 54$, and we can check $54 \cdot 47 = 2538 = 43 \cdot 59 + 1 \equiv 1 \mod 59$.

(c) (12 points) Find, with proof, the product $3 \cdot 4 \cdot 5 \cdots 56 \cdot 57 \mod 59$. Give an answer in $\{0, 1, 2, \ldots, 58\}$.

Solution: The answer is 30. This can be seen using Wilson's Theorem, or by reproving a simplified version of Wilson's Theorem.

By Wilson's Theorem, $58! \equiv -1 \mod 59$. Our product is very close to being 58!, so we make use of this fact to simplify the computations.

Write z for the product $3 \cdot 4 \cdot 5 \cdots 56 \cdot 57$. Then we have $1 \cdot 2 \cdot z \cdot 58 = 58!$, so $1 \cdot 2 \cdot z \cdot 58 \equiv -1 \mod 59$. Since $58 \equiv -1 \mod 59$, we can cancel the -1s and get $2 \cdot z \equiv 1 \mod 59$. Since 2 is invertible mod 59, by the reasoning of part (a), we have $z \equiv 2^{-1} \mod 59$.

Now observe that $2 \cdot 30 = 60 \equiv 1 \mod 59$, so we have $2^{-1} \equiv 30 \mod 59$. Now by uniqueness of inverse $z \equiv 30 \mod 59$.