Full name	Andrew ID

21-127 Test 3 (Practice)

Wednesday, 19 April 2023

Please read the following instructions carefully before the test begins.

Before the test

- Do not open the test until instructed to do so.
- Write your full name and Andrew ID in the boxes at the top of this page.
- Place your Carnegie Mellon University ID card face-up in front of you.
- Turn off your electronic devices (e.g. phone, tablet, laptop, calculator), and store any devices, notes or books out of sight (e.g. in a closed bag).

During the test

- Write clearly and legibly with a pen or pencil that is dark enough to be readable when scanned.
- You must justify all answers and claims with mathematical proof, unless otherwise specified.
- If you continue a solution on one of the extra pages (pages 12–13), you should clearly indicate in your solution the page number where it is continued.
- You may not use notes, books, other reference materials, calculators or electronic devices on this test.
- You may not communicate with others or attempt to look at other students' work during the test.
- If you require assistance, please raise your hand and wait for a proctor to come to you.
- If you need to leave the classroom (e.g. to use the bathroom), please raise your hand, show your CMU ID card to a proctor, and leave your belongings in the classroom.
- If you finish the test with 5 minutes or more remaining, you may turn in your test and leave the classroom discreetly; otherwise, please remain seated until the test ends.

After the test

- Stop working immediately when you are instructed to do so.
- Turn in all 14 pages of this test; if you tore out any pages, put them back in their correct positions.

Do not write on this page

1. (a) Write the definition of a supremum and an infimum of a set A with a partial order **[5]**

(b) find (without proof) an upper bound, lower bound, least element, most element, supremum, and infimum for the following sets, if they exist. If any of these didn't exist, prove that they don't. **[10]**

(i) $A = \{\frac{1}{n} : n \in \mathbb{N} \wedge n \neq 0\}$ with respect to the order $\leq$.

(ii) $B = \{X \subseteq \mathbb{N} : |X| = 2\}$ with respect to the order $\subseteq$

Suggested solutions:

(a) Let $A \subseteq X$, R be the partial order on X. The supremum s of A satisfies:

- $s \in X$;
- s is an upper bound of A: For any $x \in X$, xRs;
- For any other upper bound u of A, sRu.

The infimum i of A satisfies:

- $i \in X$;
- i is a lower bound of A: For any $x \in X$, iRx;
- For any other lower bound l of A, lRi.

(b) (i) Upper bound: 10; Lower bound: 0; No least element: for any $n \in \mathbb{N}$, $1/(n+1) < 1/n$; Greatest element = Supremum: 1; Infimum = 0.

(ii) Upper bound = Supremum = $\mathbb{N}$; Lower bound = Infimum = $\emptyset$; No least element: the lower bound must be the empty set which is of size 0; No greatest element: any upper bound contains $\mathbb{N}$ which has infinitely many elements.

More space for (Q1)

2. (a) Define what it means for a set to be uncountable **[5]**

(b) Let $A = \{X \subseteq \mathbb{Q} : X \text{ is finite }\}$. Prove that A is countable. **[10]**

Suggested solutions:

(a) X is uncountable when there does not exist an injection $f : X \to \mathbb{N}$.

(b) For $i \in \mathbb{N}$, let $A_i = \{X \in A \mid |X| = i\}$. Then $A = \bigcup_{i \in \mathbb{N}} A_i$. It suffices to show each A_i is countable. We prove this by finding an injection $g : A_i \to \mathbb{Q}^i$ because $\mathbb{Q}^i$ is countable. Let $B \in A_i$. Order the elements of B in increasing order $x_1 < x_2 < \cdots < x_i$. Then $g(B) = (x_1, \ldots, x_i)$.

More space for (Q2)

3. (a) Define the $\gcd(a,b)$ for two integers a and b **[5]**

(b) Let a and b be two natural numbers. Show that if $\gcd(a,b) = 1$ then $\gcd(a,b^2) = 1$. **[10]**

Suggested solutions:

(a) $d = \gcd(a,b)$ when $d \mid a$, $d \mid b$ and for any $c \in \mathbb{Z}$ such that $c \mid a$ and $c \mid b$, we have $c \mid d$.

(b) Since $\gcd(a,b) = 1$, there are $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Squaring both sides gives $a^2x^2 + b^2y^2 + 2abxy = a(ax^2 + 2bxy) + b^2(y^2) = 1$. Therefore $\gcd(a,b^2) \mid 1$. Since $\gcd(a,b^2)$ is non-negative, it must be 1.

More space for (Q3)

4. (a) Define the multiplicative inverses modulo n **[5]**

(b) Let $n > 4$ be an integer. Prove that if n is not a prime, then $(n-1)! \equiv 0 \mod n$ **[10]**

(c) Give an example to show that the above statement is not true for primes **[5]**

Suggested solutions:

(a) x is the multiplicative inverse of a modulo n if $ax \equiv 1 \mod n$.

(b) If n is not a prime, then there are a, b between 2 and $n-1$ such that $n = ab$. If $a \neq b$, then they appear as distinct terms in $\{1, \ldots, n-1\}$. Then $ab = n \mid (n-1)!$. If $a = b$, then $a^2 = n > 4$. Hence $a \geq 3$ and $n \geq 3a$. Then a and $2a$ are distinct terms in $\{1, \ldots, n-1\}$. As a result, $n = a^2 \mid a(2a) \mid (n-1)!$.

(c) Let $n = 7$. $(n-1)! = 720$ is not divisible by 7.

More space for (Q4)

5. (a) State Canter's diagonal argument and explain how it is used to prove that a given set is uncountable **[5]**

(b) Show that $\{0,1\} \times \mathbb{N}$ is countable by defining a bijection between $\{0,1\} \times \mathbb{N}$ and $\mathbb{N}$. **[10]**

Suggested solution:

(a) To prove X is uncountable, it suffices to prove that any $f : \mathbb{N} \to X$ cannot be surjective. Find an element $b \in X$ that disagrees with every $f(n)$, where $n \in \mathbb{N}$.

(b) Let $f : \{0,1\} \times \mathbb{N} \to \mathbb{N}$ be defined by $f(0,n) = 2n$ and $f(1,n) = 2n+1$ for $n \in \mathbb{N}$.

More space for (Q5)

If you use this page to continue a solution to a question, please clearly indicate on the first page of your solution where it is continued (this is page 12).

If you use this page to continue a solution to a question, please clearly indicate on the first page of your solution where it is continued (this is page 13).

Do not write on this page