Full name	Andrew ID

21-127 Test 3

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 least element of a set A with a partial order $\preccurlyeq$. **[5]**

(b) find (without proof) an upper bound, lower bound, least element, greatest 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) $A = \{\frac{n}{1+n} : n \in \mathbb{N}\}$ with respect to the order $\leq$.

(ii) $B = \{a - b : a, b \in \mathbb{R}, 1 < a \leq 2 \wedge 3 \leq b < 4\}$ with respect to the order $\leq$.

Suggested solutions:

(a) A least element ℓ of A satisfies $\forall a \in A, \ell \preceq a$.

(b) (i) Upper bound = Supremum = 1; No greatest element because the supremum $1 \notin A$ (no solution for $n/(1+n) = 1$); Lower bound = Infimum = Least element = 0.

(ii) Upper bound = Supremum = Greatest element = -1; Lower bound = Infimum = -3; No least element because the infimum $-3 \notin B$ (any $a - b > 1 - 4 = -3$).

More space for (Q1)

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

(b) Let $\mathscr{F}$ be the set of all functions $f : \mathbb{N} \to \mathbb{N}$. Use Cantor's diagonal argument to prove that $\mathscr{F}$ is uncountable. **[10]**

Suggested solutions:

(a) A set X is finite if there exists $n \in \mathbb{N}$ and a bijection $f : [n] \to X$.

(b) Suppose $\mathscr{F}$ is countable. We can write $\mathscr{F} = \{f_n : n \in \mathbb{N}\}$ where each $f_n : \mathbb{N} \to \mathbb{N}$. Define $g : \mathbb{N} \to \mathbb{N}$ via the following: If $n \in \mathbb{N}$, then $g(n) = f_n(n) + 1$. g is distinct from each f_n because their values differ at n. But g is a function from $\mathbb{N}$ to $\mathbb{N}$ so it is in $\mathscr{F}$. It must be one of the f_n's, contradiction. Therefore $\mathscr{F}$ is uncountable.

More space for (Q2)

3. (a) State Bézout's Lemma. **[5]**

(b) Let $p, q \in \mathbb{N}$ be two primes such that $p < q$. Prove that p^2 has a multiplicative inverse modulo q^3. **[10]**

Suggested solutions:

(a) Let $a, b, c \in \mathbb{Z}$. The following are equivalent:

(i) There exists $x, y \in \mathbb{Z}$ such that $ax + by = c$;

(ii) $\gcd(a, b) \mid c$.

(b) We first show that $\gcd(p, q^3) = 1$. Since $p < q$ are primes, $\gcd(p, q) = 1$ (any common factor c of p, q must divide p, so $c = 1$ or $c = p$; similarly c divides q, so $c = 1$ or $c = q$). By Bézout's Lemma, there exists $x, y \in \mathbb{Z}$ such that $px + qy = 1$. Cubing the equation gives $p^3x^3 + 3p^2x^2qy + 3pxq^2y^2 + q^3y^3 = 1$. We can rewrite it as $p(p^2x^3 + 3px^2qy + 3xq^2y^2) + q^3(y^3) = 1$. Bézout's Lemma implies $\gcd(p, q^3) = 1$.

From the previous paragraph, we know there exist $u, v \in \mathbb{Z}$ such that $pu + q^3v = 1$. Squaring the equation gives $p^2u^2 + 2puq^3v + q^6v^2 = 1$. We can rewrite it as $p^2u^2 + q^3(2pu + q^3v^2) = 1$. Bézout's Lemma implies $\gcd(p^2, q^3) = 1$. Therefore p^2 has a multiplicative inverse modulo q^3.

Alternative method:

Since $p < q$ are primes, $\gcd(p, q) = 1$. By Bézout's Lemma, there exists $x, y \in \mathbb{Z}$ such that $px + qy = 1$. Taking the fourth power of the equation, we have

$$p^4x^4 + 4p^3x^3qy + 6p^2x^2q^2y^2 + 4pxq^3y^3 + q^4y^4 = 1$$
$$p^2(p^2x^4 + 4px^3qy + 6x^2q^2y^2) + q^3(4pxy^3 + qy^4) = 1$$

Bézout's Lemma implies $\gcd(p^2, q^3) = 1$. Therefore p^2 has a multiplicative inverse modulo q^3.

Alternative method:

Since $p < q$ are primes, $\gcd(p, q) = 1$. Suppose $d = \gcd(p^2, q^3) \geq 2$. Then there exist $x, y \in \mathbb{N}$ such that $p^2 = dx$ and $q^3 = dy$. Since $q \mid q^3 \mid dy$, by Euclid's Lemma either $q \mid d$ or $q \mid y$. We cannot have $q \mid d$ because d would be equal to $q > p$, contradicting $d \mid p$. Therefore $q \mid y$. We can rewrite $q^3 = dy$ as $q^2 = dy'$ for some $y' \in \mathbb{N}$. Iterating this twice more, we have $1 = dy'''$ for some $y''' \in \mathbb{N}$. This is a contradiction because $dy''' \geq 2y''' \geq 2$.

More space for (Q3)

4. (a) Let a, x, p be nonzero integers. Define the statement: $x \equiv a \bmod p$. **[5]**

(b) Let p be a prime number. Prove that, for all $x \in \mathbb{Z}$, **[10]**

$$x^2 \equiv 1 \bmod p \text{ if and only if } x \equiv 1 \bmod p \text{ or } x \equiv -1 \bmod p$$

Suggested solutions:

(a) $p \mid (x-a)$. (Or there exists $q \in \mathbb{Z}$ such that $x - a = pq$.)

(b) If $x \equiv \pm 1$, then $x^2 \equiv (\pm 1)^2 = 1$.
Conversely, if $x^2 \equiv 1$, then $p \mid (x^2 - 1) = (x-1)(x+1)$. By Euclid's Lemma, either $p \mid x-1$ or $p \mid x+1$. In other words $x \equiv \pm 1$.

More space for (Q4)

5. (a) State the Fundamental Theorem of Arithmetic **[5]**

(b) Let $p, q \in \mathbb{N}$ be two distinct primes. Prove that for any $a \in \mathbb{Z}$, $pq \mid a^2 \Rightarrow pq \mid a$. **[10]**

Suggested solutions:

(a) Let $a \in \mathbb{Z}$ be a nonzero nonunit ($a \notin \{-1, 0, 1\}$). There exists $k \geq 1$, primes $p_1, \ldots, p_k$ such that

$$a = p_1 \times \cdots \times p_k.$$

The expression is unique up to signs and a reordering of the primes.

(b) Assume $pq \mid a^2$. Then $p \mid a^2$. By Euclid's Lemma, $p \mid a$. Similarly, $q \mid a$. There are $u, v \in \mathbb{Z}$ such that $pu = a$ and $qv = a$. Since p, q are distinct primes, $\gcd(p, q) = 1$. There exist $x, y \in \mathbb{Z}$ such that $px + qy = 1$. Multiplying the whole equation by a, we have

$$\begin{aligned} pxa + qya &= a \\ pxqv + qypu &= a \\ pq(xv + yu) &= a \end{aligned}$$

Therefore $pq \mid a$.

Alternative method:

If $a = 0$, then trivially $pq \mid a$. Since $pq \mid a^2$, a^2 cannot be a unit ($a^2 \neq \pm 1$). Therefore a cannot be a unit either ($a \neq \pm 1$). By part (a), we can write $a = p_1 \times \cdots \times p_k$ as above. Then

$$a^2 = p_1 \times p_1 \times \cdots \times p_k \times p_k$$

where each p_i appears twice. Since $p \mid pq \mid a^2$, we have $p \mid a^2$. By Euclid's Lemma, $p \mid p_i$ for some i. Similarly, $q \mid p_j$ for some j. These i, j are distinct because a single p_i cannot have two distinct prime factors. Since $a = p_1 \times \cdots \times p_k$ and p_i, p_j appear as distinct terms in the product, we know $p_i p_j \mid a$. Combining with $pq \mid p_i p_j$, we can conclude that $pq \mid a$.

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