M.1 Consider the following predicate P: *Between any two positive perfect squares there's always a prime.* Express $\neg P$ using quantifier and relation symbols, without using 'not' anywhere in your statement (implicitly or explicitly). [*Aside: empirically P seems to be true, but no one has been able to prove it.*]

BASED ON: Problem **4.7** from the HW.

STRATEGY. The first thing to do is to rewrite P with explicit quantifiers and relations:

$$\forall x, y \in \{\text{positive perfect squares}\},\ \exists p \in \{\text{primes}\} \text{ such that } x < p < y.$$

To negate this, we add 'Not' in front of it:

$$\nexists\, x, y \in \{\text{positive perfect squares}\},\ \exists p \in \{\text{primes}\} \text{ such that } x < p < y.$$

How do we interpret this? There must be some positive perfect squares x and y with no primes between them. Making the quantifiers and relations explicit:

$$\exists x, y \in \{\text{positive perfect squares}\} \text{ such that } \nexists p \in \{\text{primes}\} \text{ with } x < p < y.$$

Another way to express this:

$$\exists x, y \in \{\text{positive perfect squares}\} \text{ such that } \forall p \in \{\text{primes}\},\ p \notin (x, y).$$

None of these ways of writing $\neg P$ are valid solutions to this problem, because they all involve a 'not'. In words, one could get away from the not like this:

There's a pair of positive perfect squares such that all the integers between them are composite.

Below are some ways to write this using quantifier and relation symbols.

SOLUTION 1. $\exists m, n \in \mathbb{Z}_{>0}$ such that $\mathbb{Z} \cap (m^2, n^2) \subseteq \{\text{composites}\}$.

SOLUTION 2. $\exists m, n \in \mathbb{Z}_{>0}$ such that $\{\text{primes}\} \cap (m^2, n^2) = \emptyset$.

SOLUTION 3. $\exists n \in \mathbb{Z}_{>0}$ such that $\mathbb{Z} \cap (n^2, (n+1)^2) \subseteq \{\text{composites}\}$.

SOLUTION 4. $\exists n \in \mathbb{Z}_{>0}$ such that $\forall k \in \mathbb{Z} \cap (n^2, (n+1)^2)$, k is composite.

SOLUTION 5. $\exists n \in \mathbb{Z}_{>0}$ such that $k \in \mathbb{Z} \cap (n^2, (n+1)^2) \implies k$ is composite.

SOLUTION 6. $\exists m, n \in \mathbb{Z}_{>0}$ such that $m < n$ and $\forall p \in \{\text{primes}\}$, $p < m^2$ or $p > n^2$.

ERROR 1. Using $\mathbb{Z}^2_{>0}$ to denote perfect squares.

ERROR 2. Writing $(x, y) \in S$ for some set consisting of numbers (as opposed to ordered pairs).

ERROR 3. Using $\mathbb{Z}$ or $\mathbb{Z}_{\geq 0}$ instead of $\mathbb{Z}_{>0}$

ERROR 4. Writing relations in the form $x \in \{x \in \mathbb{Z} : \text{constraints}\}$.

ERROR 5. Writing a set in the form $\{\mathbb{Z}_{>0} : x < n < y\}$.

ERROR 6. Writing $\{\mathbb{Z}\}$ or $\{\mathbb{Z}_{>0}\}$.

ERROR 7. Writing "$\forall a < n < b$" to mean "$\forall n \in (a, b)$".

ERROR 8. Expressing a composite as mn with $m, n \in \mathbb{Z} \setminus \{0\}$.

ERROR 9. Writing '$\exists x^2$ such that...'.

ERROR 10. Writing ':' outside of set notation.

ERROR 11. Writing more than one ':' or 's.t.' symbols.

GRADING NOTE 1. A correct solution using only words (i.e. no quantifier or relation symbols) earns 3 points.

GRADING NOTE 2. Using {positive perfect squares} or {perfect squares} maximizes the score at 4 points.

GRADING NOTE 3. The incorrect interpretation of $\neg P$ as saying '*Between any two positive perfect squares there are only composites*' is worth at most 2 points (if translated correctly into quantifier and relation symbols).

GRADING NOTE 4. The incorrect interpretation of $\neg P$ as saying '*There exist two positive perfect squares between which there exists a composite*' is worth at most 2 points (if translated correctly into quantifier and relation symbols).

GRADING NOTE 5. The incorrect interpretation of $\neg P$ as saying '*For all positive perfect squares there exists a composite between them*' is worth 1 point.

M.2 The goal of this problem is to give an alternative proof that $\sqrt{2}$ is irrational (so for this problem you should forget about the proof we did in class!). Let $\mathcal{A} := \{n \in \mathbb{Z}_{>0} : n\sqrt{2} \in \mathbb{Z}\}$.

Lemma: $0 < \sqrt{2} - 1 < 1$.
Proof: If $\sqrt{2} \leq 1$, then $2 \leq 1$, which is false. Thus, $\sqrt{2} > 1$. If $\sqrt{2} \geq 2$, then $2 \geq 4$, which is false. Thus $\sqrt{2} < 2$. Putting these two inequalities together yields $1 < \sqrt{2} < 2$, from which the claim immediately follows. QED

(a) Prove that if $k \in \mathcal{A}$, then $(\sqrt{2} - 1)k \in \mathcal{A}$.

SOLUTION. Given $k \in \mathcal{A}$, we know that

$$(*) \qquad k \in \mathbb{Z}_{>0}$$

and

$$(\dagger) \qquad k\sqrt{2} \in \mathbb{Z}.$$

Let's prove that $(\sqrt{2} - 1)k \in \mathcal{A}$:

i. Equation $(*)$ combined with the lemma imply that $(\sqrt{2} - 1)k > 0$.
ii. Since $(\sqrt{2} - 1)k = k\sqrt{2} - k$, equations $(*)$ and $(\dagger)$ imply that $(\sqrt{2} - 1)k \in \mathbb{Z}$.
iii. We have $(\sqrt{2} - 1)k\sqrt{2} = 2k - k\sqrt{2} \in \mathbb{Z}$ by equations $(*)$ and $(\dagger)$.

Putting these together, we conclude that $(\sqrt{2} - 1)k \in \mathcal{A}$ as claimed. QED

ERROR 1. Only verifying that $(\sqrt{2} - 1)k\sqrt{2} \in \mathbb{Z}$.

ERROR 2. You can **never** assume the thing you're trying to prove (because then your proof is over!). For example

- If proving $\sqrt{2} > 1$, you may not assume $\sqrt{2} > 1$.
- If proving that $(\sqrt{2} - 1)k \in \mathcal{A}$, you may not assume that $(\sqrt{2} - 1)k \in \mathcal{A}$.

ERROR 3. An 'equation' **always** has an $=$ sign. Otherwise, it's merely an 'expression' or 'quantity'.

ERROR 4. Never write $\implies$ unless the clause preceding the symbol actually implies the clause following the symbol.

ERROR 5. $\mathcal{A}$ does not guarantee that whenever n is an integer, $n\sqrt{2}$ is an integer.

ERROR 6. *Since $\sqrt{2}$ isn't an integer, $k\sqrt{2}$ isn't an integer.* This is already assuming $\sqrt{2}$ is irrational!

ERROR 7. *Since $\sqrt{2} - 1$ isn't an integer, $k(\sqrt{2} - 1)$ isn't an integer.* This is already assuming $\sqrt{2} - 1$ (and hence $\sqrt{2}$) is irrational!

ERROR 8. Writing $n \in \{\mathbb{Z}\}$; the set $\mathbb{Z}$ is already a set.

ERROR 9. If $k \in \mathcal{A}$, that does *not* imply that $k = n\sqrt{2}$ for some integer n.

ERROR 10. Using the n from the definition of $\mathcal{A}$ as though it's a thing. More generally, you should **never** use the same variable simultaneously in the definition of a set and for an object outside the set.

ERROR 11. Please stop using the $\therefore$ symbol; use $\implies$ instead.

GRADING NOTE 1. One point for each of i, ii, iii above.

GRADING NOTE 2. One point total for explicitly writing both $(*)$ and $(\dagger)$.

GRADING NOTE 3. One point for clear and logical proof exposition.

GRADING NOTE 4. Automatic 0 if irrationality of $\sqrt{2}$ is used.

GRADING NOTE 5. If misinterpretation of $\mathcal{A}$ happens where $k \in \mathcal{A}$ implies $k = n\sqrt{2}$, total of parts (a) and (b) cannot exceed 5 points.

(b) Use part (a) to show that the set $\mathcal{A}$ must be empty. [*Hint: warm up by using (a) to prove that* $1 \notin \mathcal{A}$.]

STRATEGY. It's not hard to show that $1 \notin \mathcal{A}$, but my hint was to use part (a) to show this. Well, if $1 \in \mathcal{A}$, then (a) would imply that $\sqrt{2}-1 \in \mathcal{A}$. But this cannot be, since $\sqrt{2}-1 < 1$ while $\mathcal{A}$ consists of positive integers. The key observation is that multiplying by $\sqrt{2}-1$ makes a number strictly smaller. On the other hand, starting with a positive integer, we cannot create an infinite chain of smaller positive integers.

BASED ON: Our proof that every integer ≥ 2 has a prime factor!

SOLUTION 1. Suppose $\mathcal{A}$ is nonempty; let m be its least element. (This exists by the Well-Ordering principle, but since we didn't cover this before the exam began it isn't necessary to explicitly state this.) Then $(\sqrt{2}-1)m \in \mathcal{A}$ by part (a). On the other hand, by the Lemma, $(\sqrt{2}-1)m < m$! This contradicts the minimality of m. Hence, $\mathcal{A}$ must be empty. QED

SOLUTION 2. Suppose $\mathcal{A}$ is nonempty, and pick any $n \in \mathcal{A}$. By (a) we know that $n_1 := (\sqrt{2}-1)n \in \mathcal{A}$; note that $1 \leq n_1 < n$. Again by (a) we see that $n_2 := (\sqrt{2}-1)n_1 \in \mathcal{A}$, and as before $1 \leq n_2 < n_1$. We can continue this process indefinitely, obtaining an infinite sequence of positive integers $n > n_1 > n_2 > \cdots \geq 1$. But this is impossible. Thus, $\mathcal{A}$ must have been empty after all. QED

SOLUTION 3. Suppose $\mathcal{A}$ is nonempty, and pick any $n \in \mathcal{A}$. By (a) we know $(\sqrt{2}-1)n \in \mathcal{A}$. Applying (a) again yields $(\sqrt{2}-1)^2 n \in \mathcal{A}$. Applying (a) again yields $(\sqrt{2}-1)^3 n \in \mathcal{A}$. Continuing in this fashion, we get infinitely many elements in $\mathcal{A}$ of the form $(\sqrt{2}-1)^k n \in \mathcal{A}$. Summing all these elements produces

$$n + (\sqrt{2}-1)n + (\sqrt{2}-1)^2 n + (\sqrt{2}-1)^3 n + \cdots = \frac{n}{1-(\sqrt{2}-1)}$$

which is finite. However, the sum of infinitely many positive integers is infinite. QED

ERROR 1. Writing $(\sqrt{2}-1)n \leq n$ and then following correct argument doesn't work.

ERROR 2. Asserting (without proof) that $\sqrt{2} \notin \mathbb{Z}$.

ERROR 3. *Since* $\sqrt{2}$ *isn't an integer,* $k\sqrt{2}$ *isn't an integer.* This is already assuming $\sqrt{2}$ is irrational!

ERROR 4. *Since* $\sqrt{2}-1$ *isn't an integer,* $k(\sqrt{2}-1)$ *isn't an integer.* This is already assuming $\sqrt{2}-1$ is irrational!

ERROR 5. Writing $n \in \{n \in \mathbb{Z}_{\geq 0} : \textit{constraints}\}$.

ERROR 6. If $\mathcal{A}$ is nonempty, that does **not** mean that its smallest element must be 1!

ERROR 7. A non-integer times a non-integer *can* be an integer!

ERROR 8. An integer times a non-integer *can* be an integer!

ERROR 9. Using the n in the definition of $\mathcal{A}$ as though it's a thing.

GRADING NOTE 1. Automatic 0 if (a) isn't used.

GRADING NOTE 2. Automatic 0 if irrationality of $\sqrt{2}$ is used.

GRADING NOTE 3. The hint is just a hint – verifying that $1 \notin \mathcal{A}$ isn't necessary in the proof.

GRADING NOTE 4. Two points for explicitly stating the idea of finding the least element of $\mathcal{A}$.

GRADING NOTE 5. Two points for explicitly stating somewhere that $(\sqrt{2}-1)n < n$.

GRADING NOTE 6. One point for clear proof exposition.

GRADING NOTE 7. If the general argument isn't there, but $1 \notin \mathcal{A}$ is proved using (a), this earns 2 points.

(c) Use part (b) to prove that $\sqrt{2} \notin \mathbb{Q}$. [*Your answer should be very short!*]

BASED ON: Recall that $\mathcal{A} = \{n \in \mathbb{Z}_{>0} : n\sqrt{2} \in \mathbb{Z}\}$; this looks a lot like HW problem **5.1(f)**.

SOLUTION. If $\sqrt{2} \in \mathbb{Q}$, then we could write $\sqrt{2} = \frac{a}{b}$ for some $a \in \mathbb{Z}$ and $b \in \mathbb{Z}_{>0}$. But then $b \in \mathcal{A}$, which can't happen since $\mathcal{A} = \emptyset$! Contradiction. QED

ERROR 1. Writing $\sqrt{2} = \frac{a}{b}$ but then using the undefined variable k.

ERROR 2. Using that *rational* $\times$ *rational* = *rational* (this doesn't directly apply, since $\mathcal{A}$ deals with integers specifically).

ERROR 3. Using words without making them precise, e.g. *Because $\mathcal{A}$ is empty there are no integers one can multiply $\sqrt{2}$ by to get an integer, so $\sqrt{2} \notin \mathbb{Q}$.*

GRADING NOTE 1. Automatic 0 if irrationality of $\sqrt{2}$ is used in the proof.

GRADING NOTE 2. Maximum of four points if $\mathcal{A}$ isn't explicitly mentioned anywhere.

GRADING NOTE 3. Three points if correct argument but it's asserted that $\sqrt{2} = \frac{a}{b}$ and both a and b must belong to $\mathcal{A}$.

M.3 We define a new logical connective as follows:

$$P \uparrow Q := \neg(P \wedge Q).$$

This connective is cool because it can be used to replace all the other standard ones, as you'll see below.

(a) The proposition $P \uparrow P$ is logically equivalent to a very familiar expression. Which one?

STRATEGY. $P \uparrow P := \neg(P \wedge P)$. But P and P should be the same as P!

SOLUTION. Claim: $P \uparrow P \equiv \neg P$.
Proof: Consider the truth table:

P	$P \wedge P$	$\neg(P \wedge P)$	$\neg P$
T	T	F	F
F	F	T	T

ERROR 1. := means 'is defined to be'.

GRADING NOTE 1. One point for the claim, one point for any justification.

(b) Express $\implies$ in terms of $\uparrow$. (In other words, write down an expression that's purely in terms of P's, Q's, and $\uparrow$'s that is logically equivalent to $P \implies Q$.) Prove the logical equivalence with a truth table.

STRATEGY. We know from HW problem **3.6** that

$$P \implies Q \equiv (\neg P) \vee Q.$$

We can 'factor out' the $\neg$ to get

$$P \implies Q \equiv (\neg P) \vee Q \equiv \neg\big(P \wedge (\neg Q)\big).$$

Now the right hand side looks a lot like the $\uparrow$ of two propositions:

$$P \implies Q \equiv \neg\big(P \wedge (\neg Q)\big) \equiv P \uparrow (\neg Q).$$

Finally, in part (a) we figured out how to express negation in terms of $\uparrow$: $\neg Q \equiv Q \uparrow Q$.

$$P \implies Q \equiv P \uparrow (\neg Q) \equiv P \uparrow (Q \uparrow Q).$$

SOLUTION 1. Claim: $P \implies Q \equiv P \uparrow (Q \uparrow Q)$.
Proof: First let's write down a truth table for $A \uparrow B$ for reference:

A	B	$A \uparrow B$
T	T	F
T	F	T
F	T	T
F	F	T

With this in hand, we can write the truth table for $P \uparrow (Q \uparrow Q)$ with ease:

P	Q	$Q \uparrow Q$	$P \uparrow (Q \uparrow Q)$	$P \implies Q$
T	T	F	T	T
T	F	T	F	F
F	T	F	T	T
F	F	T	T	T

SOLUTION 2. Claim: $P \implies Q \equiv (P \uparrow Q) \uparrow P$
Proof:

P	Q	$P \uparrow Q$	$(P \uparrow Q) \uparrow P$	$P \implies Q$
T	T	F	T	T
T	F	T	F	F
F	T	T	T	T
F	F	T	T	T

ERROR 1. The symbol $A \uparrow B \uparrow C$ is not well-defined! This is because $\uparrow$ isn't associative:

$$(A \uparrow B) \uparrow C \not\equiv A \uparrow (B \uparrow C).$$

GRADING NOTE 1. $\uparrow$ is commutative: $X \uparrow Y \equiv Y \uparrow X$. Thus, for example, $P \uparrow (P \uparrow Q)$ is a solution (since this is equivalent to the second solution given above).

GRADING NOTE 2. 2 points for claim, 3 points for table. Table must show (at least in a rudimentary way) how the expression with the $\uparrow$ was computed.

(c) Express $\wedge$ in terms of $\uparrow$, and prove with a truth table.

STRATEGY. We have $P \uparrow Q := \neg(P \wedge Q)$. Thus $P \wedge Q \equiv \neg(P \uparrow Q)$. But we've figured out how to express $\neg$ in terms of $\uparrow$.

SOLUTION 1. Claim: $P \wedge Q \equiv (P \uparrow Q) \uparrow (P \uparrow Q)$.
Proof: Recall the truth table for $A \uparrow B$ for reference:

A	B	$A \uparrow B$
T	T	F
T	F	T
F	T	T
F	F	T

Now we can verify our claim:

P	Q	$P \uparrow Q$	$(P \uparrow Q) \uparrow (P \uparrow Q)$	$P \wedge Q$
T	T	F	T	T
T	F	T	F	F
F	T	T	F	F
F	F	T	F	F

ERROR 1. Using $\neg$ in your answer.

GRADING NOTE 1. $\uparrow$ is commutative: $X \uparrow Y \equiv Y \uparrow X$. Thus, for example, $P \uparrow (P \uparrow Q)$ is a solution (since this is equivalent to the second solution given above).

GRADING NOTE 2. 2 points for claim, 3 points for table. Table must show (at least in a rudimentary way) how the expression with the $\uparrow$ was computed.

GRADING NOTE 3. 3 points for using $\neg$ in the answer.

(d) Express $\vee$ in terms of $\uparrow$, and prove with a truth table.

STRATEGY. By 'factoring out' a $\neg$, we have

$$P \vee Q \equiv \neg\big((\neg P) \wedge (\neg Q)\big)$$

which looks an awful lot like the definition of $\uparrow$.

SOLUTION 1. Claim: $P \vee Q \equiv (P \uparrow P) \uparrow (Q \uparrow Q)$
Proof:

P	Q	$P \uparrow P$	$Q \uparrow Q$	$(P \uparrow P) \uparrow (Q \uparrow Q)$	$P \vee Q$
T	T	F	F	T	T
T	F	F	T	T	T
F	T	T	F	T	T
F	F	T	T	F	F

ERROR 1. First error

GRADING NOTE 1. $\uparrow$ is commutative: $X \uparrow Y \equiv Y \uparrow X$. Thus, for example, $P \uparrow (P \uparrow Q)$ is a solution (since this is equivalent to the second solution given above).

GRADING NOTE 2. 2 points for claim, 3 points for table. Table must show (at least in a rudimentary way) how the expression with the $\uparrow$ was computed.

(e) Rewrite the proposition $P \wedge \big((\neg Q) \implies (P \vee Q)\big)$ purely in terms of P's, Q's, and $\uparrow$'s. You don't need a truth table for this one. [*Hint: Use (a)-(d) to make your life easier! The main take-away from this part is that* any *boolean expression can be expressed in terms of just* $\uparrow$.]

STRATEGY. In the previous parts of the problem we figured out how to write $\neg$, $\implies$, $\vee$, and $\wedge$ in terms of $\uparrow$:

$$\neg A \equiv A \uparrow A \qquad A \wedge B \equiv (A \uparrow B) \uparrow (A \uparrow B)$$
$$A \implies B \equiv A \uparrow (B \uparrow B) \qquad A \vee B \equiv (A \uparrow A) \uparrow (B \uparrow B)$$

Now we just substitute these in!

Alternatively, we have

$$P \wedge \big((\neg Q) \implies (P \vee Q)\big) \equiv P \wedge \big(\neg(\neg Q) \vee (P \vee Q)\big) \equiv P \wedge \big(Q \vee (P \vee Q)\big) \equiv P \wedge (P \vee Q) \equiv P.$$

(This can easily be verified with a truth table as well.)

SOLUTION 1. $P \wedge \big((\neg Q) \implies (P \vee Q)\big) \equiv P$.

SOLUTION 2. $P \wedge \big((\neg Q) \implies (P \vee Q)\big) \equiv (P \uparrow P) \uparrow (P \uparrow P)$.

SOLUTION 3. $P \wedge \big((\neg Q) \implies (P \vee Q)\big) \equiv (P \uparrow P) \uparrow (P \uparrow Q)$.

ERROR 1. Because $\uparrow$ isn't associative, it's crucial to put the parentheses in the right place.

GRADING NOTE 1. Out of 5 points total

(f) Find a formula expressing $\#(P \uparrow Q)$ in terms of $\#P$ and $\#Q$.

STRATEGY. The $\uparrow$ operator is defined in terms of $\neg$ and $\wedge$. And we saw in class that $\#(A \wedge B) = \#A \cdot \#B$ and $\#(\neg A) = 1 - \#A$. More precisely:

$$\#(P \uparrow Q) = \#\big(\neg(P \wedge Q)\big) = 1 - \#(P \wedge Q) = 1 - \#P \cdot \#Q.$$

SOLUTION 1. Claim: $\#(P \uparrow Q) = 1 - \#P \cdot \#Q$.
Proof: Translating our previous truth table into numerical values, we have

$\#P$	$\#Q$	$\#(P \uparrow Q)$	$1 - \#P \cdot \#Q$
1	1	0	0
1	0	1	1
0	1	1	1
0	0	1	1

ERROR 1. $\equiv$ is used for logical expressions; $=$ is used for numbers. The two don't mix (e.g. $\neg(\#P)$ doesn't make sense).

GRADING NOTE 1. 1 point for correct answer, 1 point for any justification.

M.4 A *perfect cube* is any real number of the form a^3 for some $a \in \mathbb{Z}$. Prove that $n^3 + 2$ is a perfect cube if and only if $n = -1$.

STRATEGY. This is very similar to the problem we considered in class and on the HW (problem **4.2**), except with squares replaced by cubes. Writing $n^3 + 2 = a^3$ and rearranging leads to $a^3 - n^3 = 2$, so to follow the model from the square case we need to factor $a^3 - n^3$. The hint gives this in the special case $a = 1$. Actually, the hint also gives the general case:

$$\begin{aligned} a^3 - n^3 &= a^3\left(1 - \left(\frac{n}{a}\right)^3\right) = a^3\left(1 - \frac{n}{a}\right)\left(1 + \frac{n}{a} + \frac{n^2}{a^2}\right) = a\left(1 - \frac{n}{a}\right)a^2\left(1 + \frac{n}{a} + \frac{n^2}{a^2}\right) \\ &= (a - n)(a^2 + an + n^2). \end{aligned}$$

With this in hand, the rest of the problem becomes similar to previous problems.

SOLUTION 1. ($\Longleftarrow$) If $n = -1$, then $n^3 + 2 = 1$ which is a perfect cube.
($\Longrightarrow$) Suppose $n^3 + 2$ is a perfect cube, say $n^3 + 2 = a^3$. Then

$$2 = a^3 - n^3 = (a - n)(a^2 + an + n^2).$$

Since the right hand side is the product of two integers, and 2 is prime, there are only four options: one of the factors is 1 and the other is 2, or one of the factors is -1 and the other is -2. We handle this in a unified way by writing

$$a - n = x$$
$$a^2 + an + n^2 = y.$$

Then $x^2 = a^2 - 2an + n^2$, so

$$y - x^2 = 3an.$$

In particular, we need $y - x^2$ to be a multiple of 3 to even hope for a solution. This rules out the cases $x = 1$ and $x = -2$. Note that in both of the remaining two cases we have $y - x^2 = -3$, which translates into the condition $an = -1$; this implies $n = -a$, whence $a = \frac{x}{2}$. The case $x = -1$ is therefore impossible, and the case $x = 2$ yields $a = 1$ and $n = -1$.
In summary, if $n^3 + 2$ is a perfect cube, then $n = -1$. QED

SOLUTION 2. Note that $n^3 + 2 = a^3$ implies that n is even iff a is even. This simplifies Solution 1: either way $a - n$ must be even, whence $a - n = \pm 2$ and $a^2 + an + n^2 = \pm 1$.

SOLUTION 3. A different approach starts off the same way, but shows that $a^3 - n^3$ is large once $|n| \geq 2$.

Lemma. If $a < n$ then $a^3 < n^3$.

Claim. If $a^3 - n^3 > 0$ and $|n| \geq 2$ then $a^3 - n^3 \geq 7$.
Proof. Since $a^3 - n^3 > 0$, we see that $a \neq n$. The Lemma above implies $a > n$. We consider two cases.
(i) If $a = n + 1$, then

$$a^3 - n^3 = (n+1)^3 - n^3 = 3n^2 + 3n + 1 \geq 3|n|^2 - 3|n| + 1 = 3|n|(|n| - 1) + 1 \geq 7.$$

(ii) If $a \geq n + 2$, then $an \geq 0$ (since $|n| \geq 2$). Thus

$$a^2 + an + n^2 = (a - n)^2 + 3an \geq 4.$$

It follows that

$$a^3 - n^3 = (a - n)(a^2 + an + n^2) \geq 8.$$

In either case, the claim is satisfied. QED

Proof of Lemma. Given $a < n$. The statement is trivial if either of a or n is zero, so henceforth we assume that $an \neq 0$. If a and n have the different signs, then $an < 0$, whence

$$a^2 + an + n^2 = (a + n)^2 - an > 0;$$

if a and n have the same sign, then $an > 0$, whence

$$a^2 + an + n^2 = (a - n)^2 + 3an > 0.$$

Either way we deduce that $a^2 + an + n^2 > 0$, whence

$$a^3 - n^3 = (a - n)(a^2 + an + n^2) < 0$$

QED

Error 1. Getting $a^3 - n^3 = -2$.

Error 2. If $(a-n)(a^2+an+n^2) = 2$ that does *not* imply that $\frac{a-n}{2} = 1 = a^2+an+n^2$.

Error 3. Difference between n^3+2 and $(n+1)^3$ is $3n^2+3n-1$.

Error 4. Assuming that for any integer x we have $x^3 > x$.

Error 5. Arguments can be made based on the derivative, but these need to be made very carefully and explicitly to be rigorous.

Error 6. Concluding that $n - a = \pm 1$ or ± 2, but then *using* that n must be ± 1 or ± 2.

Error 7. Asserting without proof that $n^2 - n = 1$ has no integer solution.

Error 8. Asserting without proof that $n^3 + 2 = a^3 \implies a > n$.

Error 9. Asserting that consecutive cubes are closer together than non-consecutive cubes.

Error 10. Asserting that $n^3 - a^3 = (n-a) \cdot \dfrac{n-a^3}{n-a}$

Error 11. Writing the forwards case in a convoluted enough way that you don't notice that you did the reverse case twice. If you plug in -1 in both directions... you probably made this error.

Error 12. Finding multiple possible cases for a and n, but only pursuing the one that gives $n = -1$.

Error 13. Making a sequence of complicated algebraic maneuvers to translate $n^3 + 2 = a^3$ into... $n^3 + 2 = a^3$ written in another form (e.g. $n^3 + 1 = a^3 - 1$).

Error 14. Writing contradictory statements (e.g. $a = 1$ and $a + 1 = -1$).

Error 15. Making the assertion (without proof) that $a^2 + an + n^2 > 0$.

Error 16. Don't write QED unless you've proved something.

Error 17. $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ is the set of ordered triples of integers, not the set of perfect cubes.

Error 18. Giving no indication at all of how you solved a pair of simultaneous equations. (You don't have to say much, but at least a little bit, e.g. "Substituting $a = n+2$ into the first equation and using the quadratic formula, we find that blah blah blah".)

Grading note 1. One point for reverse implication.

Grading note 2. In Solutions 1 or 2: one point for writing $(a-n)(n^2+an+a^2) = 2$, three points for the rest of the argument.

Grading note 3. In Solution 3: one point for proving $a > n$, one point for handling the case $a = n+1$, two points for handling the case $a \geq n+2$.

Grading note 4. Purely empirical (i.e. unproved) assertions that the distance between cubes grows is worth 1 point.

M.5 Let $\mathcal{A}$ denote the set of all real numbers in $(0,1)$ that can be expressed as a finite decimal. Thus, for example, $\frac{1}{3} \notin \mathcal{A}$ (because $\frac{1}{3} = 0.3333...$), whereas $\frac{1}{4} \in \mathcal{A}$ (because $\frac{1}{4} = 0.25$). Is $\mathcal{A}$ countable? If yes, prove with an enumeration of the set. If no, prove why not.

STRATEGY. The key epiphany here is the distinction between *infinite* and *arbitrarily long* decimals. The set $\mathcal{A}$ contains arbitrarily long decimals, but no infinite ones.

SOLUTION 1. $\mathcal{A}$ is countable, because we can enumerate it. One way to enumerate $\mathcal{A}$ is to list (in increasing order) all the elements of $\mathcal{A}$ with a single digit after the decimal point (i.e. $0.1, 0.2, 0.3, \ldots, 0.9$), then the elements of $\mathcal{A}$ with two digits (i.e. $0.01, 0.02, 0.03, \ldots, 0.99$), then the elements with three digits, etc. Since for any $n \in \mathbb{Z}_{>0}$ there are only finitely many elements of $\mathcal{A}$ with n digits, and any $\alpha \in \mathcal{A}$ has some finite number of digits, this enumeration will reach an arbitrary $\alpha \in \mathcal{A}$ after a finite number of steps.

SOLUTION 2. $\mathcal{A}$ is countable, because it's a subset of $\mathbb{Q}$ which we know to be countable. The reason we know it's a subset is because any finite decimal must be rational:

$$0.a_1a_2\cdots a_k = \frac{a_1a_2\cdots a_k}{10^k}$$

The enumeration we can give is the same one as we had for $\mathbb{Q}$, sweeping up and down diagonals (and ignoring all rational entries that have infinite decimal expansions).

SOLUTION 3. $\mathcal{A}$ is countable, because we can explicitly describe its elements as a countable set. As in the solution above, we know all elements of $\mathcal{A}$ are rational. Moreover, the only rational numbers with finite decimal expansions are those with denominators of the form 2^a5^b for some $a, b \in \mathbb{Z}_{>0}$. Thus an enumeration might be ordered in the denominator by fixed sum $a + b$, and in the numerator by increasing order.

SOLUTION 4. $\mathcal{A}$ is countable. An enumeration is as follows: for any positive integer, write it in standard decimal form, say

$$a_1a_2\cdots a_n$$

where each a_i is a digit and $a_1 \neq 0$. Associate to this the number $0.a_na_{n-1}\cdots a_2a_1$. This is a finite decimal, so it lives in $\mathcal{A}$. Every finite decimal is enumerated (just reverse its digits). Finally, no two integers are associated to the same element of $\mathcal{A}$, since if they were, they would have to agree in every digit.

SOLUTION 5. The cube of $\frac{a}{2^b5^c}$.

ERROR 1. The set $\mathcal{A}$ is *not* the same as $(0,1)$!

ERROR 2. The enumeration $0.n$ is the n-th number doesn't work; 0.1 and 0.01 go to the same place.

ERROR 3. To prove $\mathcal{A}$ is countable, you must show that $\mathcal{A}$ is infinite.

ERROR 4. In class we proved that $(0,1)$ is uncountable. This proof doesn't work here because the new number created isn't in $\mathcal{A}$ – it has infinitely many digits!

ERROR 5. Showing that the above proof doesn't work for $\mathcal{A}$ doesn't prove that $\mathcal{A}$ is countable – it just shows that that proof doesn't apply!

ERROR 6. If you claim all elements of $\mathcal{A}$ are rational, you must prove that.

ERROR 7. There is no smallest or largest element of $(0,1)$. There's also no element 'just to the right of' $1/2$, or any other number.

ERROR 8. There are many elements of $\mathcal{A}$ that don't look like $\frac{a}{2^n}$.

ERROR 9. $\mathcal{A}$ has elements that aren't of the form $\frac{1}{d}$ with d a divisor of 10^n.

GRADING NOTE 1. One point for answer.

GRADING NOTE 2. Two points for enumeration.

GRADING NOTE 3. Two points for justification for why the enumeration works.

GRADING NOTE 4. Arguing that $\mathcal{A}$ is a subset of $\mathbb{Q}$ and is therefore countable (without giving an enumeration) is worth at most three points.

GRADING NOTE 5. No need to discuss abstractions if you give a very concrete enumeration (e.g. Solution 1).

M.6 Suppose a function $f : \mathbb{Z} \to \mathbb{R}$ satisfies two nice properties:

- $f(1) \neq 0$, and
- $f(a+b) = f(a) + f(b)$ for all $a, b \in \mathbb{Z}$.

(a) Prove that $f(n) = 0$ if and only if $n = 0$.

STRATEGY. First we prove that $f(0) = 0$. Now comes the tricky part. This is **NOT** enough to deduce that $f(n) = 0$ implies $n = 0$... at least, not until you prove injectivity of f.

SOLUTION. As usual with if and only if proofs, we proceed in both directions.
($\Longleftarrow$) We have $f(0) = f(0+0) = f(0) + f(0)$. Subtracting $f(0)$ from both sides yields $f(0) = 0$.
($\Longrightarrow$) Suppose $f(n) = 0$. There are three cases to consider:

- If $n = 0$, we're done.
- If $n > 0$ then $n = \underbrace{1 + 1 + \cdots + 1}_{n}$, so $f(n) = \underbrace{f(1) + f(1) + \cdots + f(1)}_{n} = nf(1)$. Since $n > 0$ and $f(1) \neq 0$, we see that $f(n) \neq 0$ in this case.
- If $n < 0$, then the same argument as above applies to show that $f(n) = -nf(-1)$. To conclude, we need to know that $f(-1) \neq 0$. But this follows immediately from $f(-1) + f(1) = f(0) = 0$ and the fact that $f(1) \neq 0$.

This concludes the proof. QED

ERROR 1. The letters a and b aren't things. They just signify that f of a sum is the same as the sum of the f values at those inputs.

ERROR 2. We do not yet know that $f(a-b) = f(a) - f(b)$. (This follows from part (b), however.)

ERROR 3. Proving $f(n) = 0 \implies f(0) = 0$ does *not* prove that $f(n) = 0 \implies n = 0$!

ERROR 4. When manipulating equations in the proof of ($\Longleftarrow$), be careful not to accidentally replace 0 by $f(0)$: this is what you're trying to prove!

ERROR 5. If $f(x) = -f(y)$ that doesn't imply that $x = -y$ (unless you already know injectivity!).

ERROR 6. Some folks used (b) by accident, e.g. when writing $f(n) = -(f(1) + f(1) + \cdots + f(1))$ for negative n.

ERROR 7. If you used part (b) to do this, you have to make sure you didn't use part (a) to solve part (b)!

ERROR 8. Faulty argument: $0 = 0 \cdot f(1) = f(0 \cdot 1) = f(0)$.

ERROR 9. You cannot use injectivity in this part! In particular, just because $f(0) = 0$ doesn't imply that $f(n)$ can't be 0 for some nonzero n.

ERROR 10. Some of you wrote $f(n) = 2f(n/2)$. This only makes sense if n is divisible by 2 (since f only takes integer inputs).

ERROR 11. Expressions like $f(0) \implies f(1) + f(-1)$ don't mean anything.

ERROR 12. f is not necessarily increasing. (It's possible that $f(1) < 0$.)

ERROR 13. Asserting (without proof) that $f(n) = nf(1)$ earns 1 point.

ERROR 14. If $n < 0$, then $f(n) = \underbrace{-1 + -1 + \cdots + -1}_{-n}$.

GRADING NOTE 1. ($\Longleftarrow$) is worth 2 points

GRADING NOTE 2. ($\Longrightarrow$) is worth 3 points

(b) Prove that $f(-n) = -f(n)$ for every $n \in \mathbb{Z}$.

STRATEGY. The key here is to realize that the second property of f can work in two different ways: you pick a and b first and then compute $f(a+b)$ in terms of $f(a)$ and $f(b)$, or you can pick a number n and break it up as $n = a + b$ and then apply the property.

SOLUTION. Pick any $n \in \mathbb{Z}$. We have $f(n) + f(-n) = f(0) = 0$ by (a). It follows that $f(-n) = -f(n)$. QED

ERROR 1. a and b aren't things.

ERROR 2. You cannot assume your claim in the proof of the claim! In particular, you cannot assume that $f(a-b) = f(a) - f(b)$.

(c) Prove that f must be injective.

STRATEGY. The strategy for proving injectivity is always the same: *assume* that $f(x) = f(y)$, and try to *deduce* that $x = y$.

SOLUTION 1. Suppose $f(x) = f(y)$. Then applying (b),

$$0 = f(x) - f(y) = f(x) + f(-y) = f(x - y).$$

By (a), this implies $x - y = 0$. But this means $x = y$. QED

SOLUTION 2. From part (a) we know that $f(0) = 0$ and $f(n) = nf(1)$ for all $n \in \mathbb{Z}_{>0}$. By part (b) we deduce that for any $n \in \mathbb{Z}_{<0}$ we have $f(n) = -f(-n) = -(-n)f(1) = nf(1)$. Thus, we deduce that

$$f(n) = nf(1) \qquad \forall n \in \mathbb{Z}.$$

In particular, if $f(x) = f(y)$ then $xf(1) = yf(1)$, and since $f(1) \neq 0$ we deduce that $x = y$. QED

ERROR 1. You're not trying to prove that $f(x) = f(y)$ here; you're trying to prove that whenever $f(x) = f(y)$, it must follow that $x = y$.

ERROR 2. You may not assume that f is injective to prove that f is injective! In other words, at no time in your proof are you allowed to make a deduction of the form $f(m) = f(n)$, therefore $m = n$.

ERROR 3. f is not necessarily an increasing function; it might be a decreasing function.

ERROR 4. Just because $\mathbb{R}$ has a larger cardinality than $\mathbb{Z}$ doesn't guarantee that f is injective. For example, the function $g : \mathbb{Z} \to \mathbb{R}$ defined by $g(n) := 0$ for all n isn't injective.

GRADING NOTE 1. Asserting that $f(n) = nf(1)$ for all n, but only proving it for positive n, earns three points (assuming injectivity is proved correctly using this).

(d) Is f surjective? Prove your answer.

STRATEGY. $\mathbb{Z}$ is countable, $\mathbb{R}$ isn't!

SOLUTION 1. No: if f were surjective, then by (c) it would be a bijection between $\mathbb{Z}$ and $\mathbb{R}$. But we know that $\mathbb{R}$ is uncountable, whereas $\mathbb{Z}$ is countable, so there cannot be any bijection between them.

SOLUTION 2. No: we found earlier that for any $n \in \mathbb{Z}$, $f(n) = nf(1)$. I claim that $\frac{1}{2}f(1)$ is not an output of f. Indeed, suppose $f(x) = \frac{1}{2}f(1)$; then $xf(1) = \frac{1}{2}f(1)$, whence $x = \frac{1}{2}$. But f only take inputs from $\mathbb{Z}$! Thus, f is not surjective.

ERROR 1. It's not enough to give an example of an f that's not surjective. Maybe there's another example that is!

ERROR 2. It's not enough to simply assert that any function from a countable set to an uncountable one cannot be surjective – we never proved this fact.

ERROR 3. To receive full credit, a solution of type Solution 2 requires a proof that the given output is impossible.

ERROR 4. '$\mathbb{R}$ is uncountable, because you can always create a new α within $\mathbb{R}$'... no, this just tells you that $\mathbb{R}$ is *infinite*.

GRADING NOTE 1. Example of f that's not surjective earns 2 points.

M.7 Prove that $(0,1] \approx (0,1)$ by giving an explicit function producing a one-to-one correspondence. (Here $(0,1]$ means the set $\{x \in \mathbb{R} : 0 < x \leq 1\}$.)

STRATEGY. The heart of the problem is: where does the 1 go? Well, if I forced you to pick, you'd probably say 1/2. OK, so where does 1/2 go? Again, if I were to force you, you might say 1/4. But then...

SOLUTION 1. Let $\mathcal{A} := \left\{\frac{1}{2^n} : n \in \mathbb{Z}_{\geq 0}\right\}$, and consider the function $f : (0,1] \to (0,1)$ defined by

$$f(x) = \begin{cases} \frac{x}{2} & \text{if } x \in \mathcal{A} \\ x & \text{if } x \notin \mathcal{A}. \end{cases}$$

It's clear that f is a function, and that all of its outputs live in $(0,1)$.
Lemma. $x \in \mathcal{A}$ if and only if $f(x) \in \mathcal{A}$.
Proof. The forward direction is trivial (by the definition of f). Now suppose $x \notin \mathcal{A}$. Then $f(x) = x$ by definition, whence $f(x) \notin \mathcal{A}$. The contrapositive of this is: if $f(x) \in \mathcal{A}$, then $x \in \mathcal{A}$. QED
I claim f is bijective. As usual, we prove this in two steps:
f injective: Suppose $f(x) = f(y)$. Since they are equal, either both $f(x)$ and $f(y)$ live in $\mathcal{A}$ or neither does. In the former case, x and y must both live in $\mathcal{A}$, in which case $\frac{x}{2} = f(x) = f(y) = \frac{y}{2}$ and we deduce that $x = y$. If neither $f(x)$ nor $f(y)$ lives in $\mathcal{A}$, then $x, y \notin \mathcal{A}$, whence $x = f(x) = f(y) = y$. Thus, in either situation we conclude that $x = y$, so f must be injective.
f surjective: Pick an arbitrary $y \in (0,1)$. Set

$$x := \begin{cases} 2y & \text{if } y \in \mathcal{A} \\ y & \text{otherwise.} \end{cases}$$

I claim that $f(x) = y$. Indeed, if $x \in \mathcal{A}$ then $y \in \mathcal{A}$, whence $x = 2y$ and $f(x) = f(2y) = y$. If, on the other hand, $x \notin \mathcal{A}$, then $y \notin \mathcal{A}$, whence $x = y$ and $f(x) = x = y$. In either case, $f(x) = y$, and we see that f must be surjective.

ERROR 1. ∞ isn't a number!
ERROR 2. No such thing as a number 'infinitesimally close to' 1/2 or 1.
ERROR 3. Be careful: is your function injective?

GRADING NOTE 1. Two points for explicit function, clearly defined.
GRADING NOTE 2. One point for injective proof.
GRADING NOTE 3. One point for surjective proof.
GRADING NOTE 4. One point for checking its a function as claimed.