

5.23 Prove there is no integer a such that $a \equiv 5 \pmod{14}$ and $a \equiv 3 \pmod{21}$.

Proof. Suppose, for a contradiction, that there is such an integer a . Then there exist integers x and y such that $a = 14x + 5$ and $a = 21y + 3$. Taking the difference of these, we find that

$$14x + 5 - 21y - 3 = 0 \implies 2 = 21y - 14x \implies 2 = 7(3y - 2x) \implies 7|2$$

But this is impossible, because $0 < 2 < 7$. Thus, we have reached a contradiction, so our assumption was false and there is no such integer a . \square

5.55 Prove that there do not exist positive integers a and n such that $a^2 + 3 = 3^n$.

Proof 1. Suppose, for a contradiction, that there exist positive integers a and n such that $a^2 + 3 = 3^n$. Then

$$a^2 = 3(3^{n-1} - 1) \implies 3|a^2 \implies 3|a$$

Thus, $9|a^2$ and so $9|3(3^{n-1} - 1)$. So $3|(3^{n-1} - 1)$. If $n \geq 2$, this is impossible because $3^{n-1} \equiv 0 \pmod{3}$. Therefore, $n = 1$. But this implies that

$$a^2 + 3 = 3 \implies a = 0$$

which contradicts the assumption that a is positive! Therefore, there are no such positive integers a and n . \square

Proof 2. Suppose, for a contradiction, that there exist positive integers a and n such that $a^2 + 3 = 3^n$. If $n = 1$, then $a^2 + 3 = 3 \implies a = 0$, which contradicts the assumption that a is positive. So assume that $n \geq 2$. Then $3^n \equiv 0 \pmod{9}$. Taking both sides of the equation modulo 9, we find that $a^2 \equiv 6 \pmod{9}$. But this is impossible:

$$\begin{array}{lll} 0^2 \equiv 0 \pmod{9} & 1^2 \equiv 1 \pmod{9} & 2^2 \equiv 4 \pmod{9} \\ 3^2 \equiv 0 \pmod{9} & 4^2 \equiv 7 \pmod{9} & 5^2 \equiv 7 \pmod{9} \\ 6^2 \equiv 0 \pmod{9} & 7^2 \equiv 4 \pmod{9} & 8^2 \equiv 1 \pmod{9} \end{array}$$

\square

3. Carefully read the proof (from the class notes or from the book) that $\sqrt{2}$ is irrational. Then prove the following.

- Prove that $\sqrt[3]{5}$ is irrational.
- Prove that $\log_2(5)$ is irrational. (Remember that $\log_a(b)$ is the unique real number such that $a^{\log_a(b)} = b$.)
- (Bonus)** Prove that if n is a positive integer such that $n \geq 2$, then $\sqrt[n]{5/3}$ is irrational.

Proof of (a). Suppose, for a contradiction, that $\sqrt[3]{5}$ is rational. Then there exist integers a, b such that $\sqrt[3]{5} = \frac{a}{b}$. Without loss of generality, a and b are chosen to be positive. Among all possible fractions which equal $\sqrt[3]{5}$, we may also pick the one where a is smallest. Hence, a and b have no common factors except for 1 (as if they did, we could divide out that common factor and get a smaller a).

Then

$$\begin{aligned}\sqrt[3]{5} = \frac{a}{b} &\implies 5 = \frac{a^3}{b^3} &\implies 5b^3 = a^3 \\ &\implies 5|a^3 &\implies 5|a\end{aligned}$$

So let $a = 5c$ for some positive integer c .

$$\begin{aligned}5b^3 = (5c)^3 &\implies 5b^3 = 125c^3 &\implies b^3 = 25c^3 \\ &\implies 5|b^3 &\implies 5|b\end{aligned}$$

But this implies that a and b have 5 as a common factor. This contradicts the fact that a and b have no common factors! Therefore, our assumption that $\sqrt[3]{5}$ was rational was false, so $\sqrt[3]{5}$ is irrational. \square

Proof of (b). Suppose, for a contradiction, that $\log_2(5)$ is rational. Then there exist integers a, b such that $\log_2(5) = \frac{a}{b}$. b must be nonzero, so without loss of generality, b is chosen to be positive. Then

$$\log_2(5) = \frac{a}{b} \implies 5 = 2^{a/b} \implies 5^b = 2^a$$

Since b is positive, this means $5|2^a$. This is impossible, because for any k ,

$$\begin{aligned}a = 4k &\implies 2^a = (2^4)^k \equiv 1^k \pmod{5} \equiv 1 \pmod{5} \\ a = 4k + 1 &\implies 2^a = 2 \cdot (2^4)^k \equiv 2 \cdot 1^k \pmod{5} \equiv 2 \pmod{5} \\ a = 4k + 2 &\implies 2^a = 4 \cdot (2^4)^k \equiv 4 \cdot 1^k \pmod{5} \equiv 4 \pmod{5} \\ a = 4k + 3 &\implies 2^a = 8 \cdot (2^4)^k \equiv 3 \cdot 1^k \pmod{5} \equiv 3 \pmod{5}\end{aligned}$$

\square

Proof of (c). Suppose, for a contradiction, there exists some positive integer $n \geq 2$ such that $\sqrt[n]{5/3}$ is rational. Then $\sqrt[n]{5/3} = \frac{a}{b}$ for some integers a, b . By the same reasoning as in part (a), we can choose a, b such that they are both positive and have no common factors. Then

$$\begin{aligned}\sqrt[n]{5/3} = \frac{a}{b} &\implies \frac{5}{3} = \frac{a^n}{b^n} &\implies 5b^n = 3a^n \\ &\implies 5|a^n &\implies 5|a\end{aligned}$$

So let $a = 5c$ for some integer c .

$$\begin{aligned}5b^n = 3(5c)^n &\implies 5b^n = 3 \cdot 5^n \cdot c^n &\implies b^n = 3 \cdot 5^{n-1} \cdot c^n \\ &\implies 5|b^n &\implies 5|b\end{aligned}$$

But this contradicts the fact that a and b have no common factors! Therefore, our assumption that $\sqrt[n]{5/3}$ is rational was false. \square

4. Prove that between any two real numbers, there are infinitely many rational numbers. (Hint: First prove as a lemma that between any two real numbers, there is at least one rational number.)

Lemma 0.1. *Between any two real numbers, there exists at least one rational number.*

Proof. Let x, y be real numbers, and WLOG $x < y$. Then there exists some natural number n such that $\frac{1}{n} < y - x$. Suppose, for a contradiction, that there is no integer a such that $\frac{a}{n}$ is between x and y . Then, for every integer a , either $\frac{a}{n} \leq x$ or $\frac{a}{n} \geq y$. There are some integers $k < \ell$ such that $\frac{k}{n} \leq x$ and $\frac{\ell}{n} \geq y$, and therefore there must be some integer a such that $k \leq a < \ell$ such that $\frac{a}{n} \leq x < y \leq \frac{a+1}{n}$. Thus

$$\frac{1}{n} = \frac{a+1}{n} - \frac{a}{n} \geq y - \frac{a}{n} \geq y - x > \frac{1}{n}$$

so $\frac{1}{n} > \frac{1}{n}$. This is a contradiction! Therefore, our assumption was incorrect and so there exists some integer a such that $\frac{a}{n}$ is between x and y . This proves the lemma. \square

Proof 1 of Q4. Let x, y be any two real numbers, and WLOG $x < y$. By the lemma, there is at least one rational number between x and y . Suppose for a contradiction that there are only finitely many rational numbers $q_1 < q_2 < \dots < q_n$ between x and y , where $n \in \mathbb{N}$. By assumption, there are no other rational numbers between x and y , and so there are no rational numbers between q_n and y . But this contradicts the lemma! Therefore, our assumption was false and there are infinitely many rational numbers between x and y . \square

Proof 2 of Q4. Let x, y be any two real numbers, and suppose $x < y$. We show by induction on n that there exist at least n rational numbers between x and y .

- Base case: $n = 1$. This is the lemma.
- Inductive step: suppose that there are rational numbers $q_1 < q_2 < \dots < q_n$ between x and y . By the lemma, there is a rational number q_{n+1} between q_n and y . Because $q_{n+1} > q_n$, q_{n+1} is distinct from q_1, q_2, \dots, q_n . Thus, we now have $n + 1$ rational numbers between x and y . This completes the induction.

\square

5. Consider the following proposition.

Proposition 0.2. *Let x be any positive real number. Then for every positive real number y , there is a positive real number z such that $z^x > y$.*

- (a) The following is an invalid proof. Explain why it is invalid.

Proof. Suppose that the statement is false. Then for some x , there is a positive real number y such that for every $z > 0$, $z^x \leq y$. Either $y > 1$ or $y \leq 1$: let us consider these two cases separately.

- If $y > 1$, then set $z = y$ and $x = 2$. Then $z^x = y^2 > y$. But this contradicts the assumption that $z^x \leq y$, so we have a contradiction!

- If $y \leq 1$, then set $z = 2$ and $x = 1$. Then $z^x = 2 > y$. But this contradicts the assumption that $z^x \leq y$, so we have a contradiction!

In each case we reach a contradiction, and so our assumption was incorrect. Therefore, for every positive real number x and every positive real number y , there is a positive real number z such that $z^x > y$. \square

Solution: The real issue is that the given proof chooses x (i.e., proves a $\exists x$ statement). The fact that it proceeds by contradiction is a red herring - if you take out the first two sentences of the given proof, you see it is actually just a direct proof of the statement $\forall y, \exists x \exists z, z^x > y$. Whereas the proposition to be proven is $\forall x \forall y, \exists z, z^x > y$ (which is equivalent to $\forall y \forall x, \exists z, z^x > y$). The proposition to be proven is much more general than what the given argument proves.

- (b) Give a correct proof of the proposition.

Proof. We want to show that for every pair of positive real numbers x and y , there exists a positive real number z such that $z^x > y$. We consider two cases for y .

Case 1: If $y \leq 1$, let $z = 2$. Then no matter what x is, $z^x = 2^x > 2^0 = 1$ and so $z^x > y$.

Case 2: If $y > 1$, let n be some number such that $n > \frac{1}{x}$. Then let $z = y^n$. We thus have

$$z^x = (y^n)^x = y^{nx} > y^1 = y$$

\square

6. Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be a continuous function. Suppose that

$$\exists a, b \in \mathbb{R}, (a < b \wedge f(a) < f(b))$$

and

$$\exists c, d \in \mathbb{R}, (c < d \wedge f(c) > f(d))$$

Use the Intermediate Value Theorem to prove that

$$\exists x, y \in \mathbb{R}, (x < y \wedge f(x) = f(y))$$

Hint: Construct a continuous function $H(t)$ with the property that $H(0) = f(b) - f(a)$ and $H(1) = f(d) - f(c)$. Then use the Intermediate Value Theorem on $H(t)$ over the interval $[0, 1]$.

Proof 1. Consider the function $H : \mathbb{R} \rightarrow \mathbb{R}$ defined by

$$H(t) = f(b(1-t) + dt) - f(a(1-t) + ct)$$

Then $H(t)$ is a function of the one variable t which is continuous, and it satisfies the property that $H(0) = f(b) - f(a) > 0$ and $H(1) = f(d) - f(c) < 0$. Since $H(0) > 0$ and $H(1) < 0$, the IVT tells us that there is some number $s \in [0, 1]$ such that $H(s) = 0$. This means that

$$H(s) = f(b(1-s) + ds) - f(a(1-s) + cs) = 0$$

$$\implies f(b(1-s) + ds) = f(a(1-s) + cs)$$

Since $b > a$, $d > c$, and $0 < s < 1$,

$$b(1-s) + ds > a(1-s) + cs$$

and so we can let $x = a(1-s) + cs$ and $y = b(1-s) + ds$ to satisfy the conditions required. \square

Proof 2. Suppose for a contradiction that there are no such x, y . Then it follows that for every $x, y \in \mathbb{R}$, if $x < y$ then either $f(x) < f(y)$ or $f(x) > f(y)$.

Define a function g by $g(y) = f(y) - f(a)$. Then by assumption, $g(y)$ cannot be zero anywhere on the interval $[b, d]$. Since $g(b) > 0$, the contrapositive version of the IVT tells us that $g(d) > 0$. So $f(d) - f(a) > 0$.

Define a function h by $h(x) = f(d) - f(x)$. Then by assumption, $h(x)$ cannot be zero anywhere on the interval $[a, c]$. Since $h(c) < 0$, the contrapositive version of the IVT tells us that $h(a) < 0$. So $f(d) - f(a) < 0$.

So we have shown that $f(d) - f(a) > 0$ and $f(d) - f(a) < 0$, which is a contradiction! Hence, our assumption was incorrect and there must exist $x, y \in \mathbb{R}$ such that $x < y$ and $f(x) = f(y)$.

\square