Proof by Contradiction

I think we've seen enough geometry for now. Our next mathematical topic will be number theory. But there are also logical issues to discuss.

One of the most important methods of proof is called "proof by contradiction". As an example, I will prove the second oldest theorem in mathematics (after the Pythagorean Theorem).

Theorem: The square root of 2 is not a ratio of whole numbers.

Proof: Assume for contradiction that $\sqrt{2}$ is a ratio of whole numbers. In this case, we can write

$$\sqrt{2} = \frac{a}{b}$$

in "lowest terms"

(i.e., where a and b are whole numbers with no common factors except ± 1).

Now we can square both sides to get

$$2 = \frac{a^2}{b^2}$$

$$\Longrightarrow \quad a^2 = 2b^2.$$

This implies that a^2 is even, and hence a is even (as we proved last week). That is, there exists a whole number k such that $a = 2k$. Substituting this into our equation gives

$$\begin{aligned} a^2 &= 2b^2 \\ (2k)^2 &= 2b^2 \\ 4k^2 &= 2b^2 \\ 2k^2 &= b^2. \end{aligned}$$

This implies that b^2 is even, and hence b is even, i.e., there exists a whole number ℓ such that $b = 2\ell$.

Since $a = 2k$ and $b = 2l$ we conclude that a and b have common factor 2.

But this is impossible because we already know that a and b have no common factors except ± 1.

Since our original assumption (that $\sqrt{2}$ is a ratio of whole numbers) leads to a contradition, we conclude that it was false, i.e., $\sqrt{2}$ is not a ratio of whole numbers.

//

What do you you make of that proof? Do you find it convincing?

Let's discuss the logic behind it. In this class our logic will follow two rules.

Rule 1 ("excluded middle")

Any given mathematical statement is either T or F (not both and not neither).

Statements without this property are not "mathematical statements".

Examples:

- "$0 = 1$" is a math. statement
- "Today is a nice day" is <u>not</u>.

Rule 2 ("material implication")

T flows along arrows $\Longrightarrow$.

In other words,

$T \Rightarrow T$, $F \Rightarrow T$, $F \Rightarrow F$, $T \Rightarrow F$.

✓ ✓ ✓ ✗

That's all.

///

We can rephrase the rules in the more formal language of "truth tables"

Rule 1: Every math. statement P has an opposite statement $\neg P$ (read "not P") with the opposite truth value.

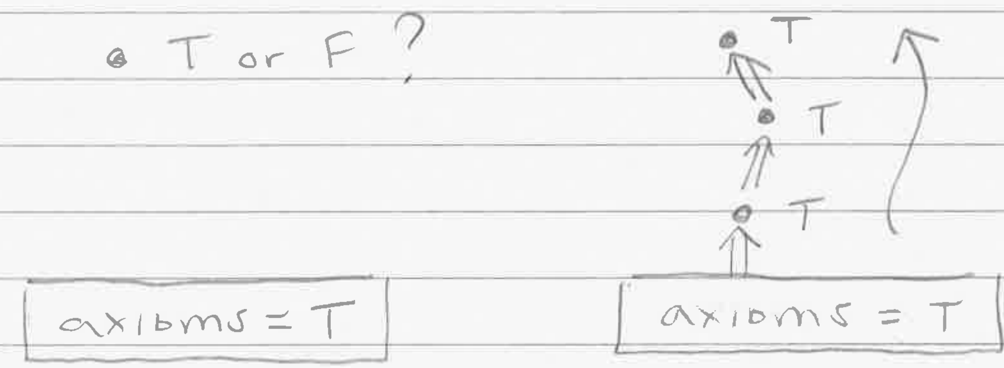
P	$\neg P$
T	F
F	T

Rule 2: The arrow $\Rightarrow$ is a function that sends an ordered pair of truth values to a truth value as follows

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

"Only $T \Rightarrow F$ is false because the T isn't flowing properly."

This explains my earlier schematic diagram of a proof:



"The axioms are the source of T. To prove a mathematical statement we drill down until we hit the axioms; then the T flows up."

But the axioms are also the source of F. We get an interesting duality by putting Rules 1 & 2 together.

☆ Logical Principle ("the contrapositive")

F flows <u>backwards</u>. In other words, the statements $P \Longrightarrow Q$ and $\neg Q \Longrightarrow \neg P$ are <u>logically equivalent</u>.

We don't need to take this as a Rule because we can "prove" it.

"Proof": We can combine the truth tables from Rules 1 & 2 to get

P	Q	$\neg Q$	$\neg P$	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$
T	T	F	F	T	T
T	F	T	F	F	F
F	T	F	T	T	T
F	F	T	T	T	T

"Only $T \Rightarrow F$ is false." Since the last two columns are the same we see that $P \Rightarrow Q$ and $\neg Q \Rightarrow \neg P$ always have the same truth value. In other words, they are

<u>logically equivalent</u>.

[Remark: This is much easier than trying to justify the contrapositive using verbal reasoning, right?]

Logic for Mathematicians

Last time I used the method of contradiction to prove that $\sqrt{2}$ is "irrational", i.e., not a ratio of whole numbers

Then I stated the rules of logic we will use in this class

Recall:

Rule 1 ("excluded middle").

A mathematical statement is either T or F (not both, not neither). In other words, if P is a math statement then it has an opposite statement $\neg P$ defined by

P	$\neg P$
T	F
F	T

Rule 2 ("material implication").

"T flows along arrows"

In other words, for all math. statements P & Q we have

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

"only $T \Rightarrow F$ is false because the T isn't flowing properly."

From these two rules we derived the following.

☆ Logical Principle ("the contrapositive").

"F flows backwards".

In other words, for all math statements P & Q the statements

$$P \Rightarrow Q \quad \& \quad \neg Q \Rightarrow \neg P$$

are logically equivalent.

"Proof":

P	Q	$P \Rightarrow Q$	$\neg Q$	$\neg P$	$\neg Q \Rightarrow \neg P$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

The 3rd and 6th columns are equal. ///

Now let me explain how we <u>use</u> the contrapositive in mathematics. Its main application is the method of <u>proof by contradiction</u>.

Here's how it works:

Suppose we want to prove statement P. If we can build a sequence of arrows from $\neg P$ to a false statement

$$\neg P \Longrightarrow Q_1 \Longrightarrow Q_2 \Longrightarrow \cdots \Longrightarrow Q_k = F$$

then the F will flow backwards and tell us that $\neg P = F$, hence $P = T$.

In practice this means that we start by <u>assuming</u> $\neg P$ and show that this logically leads to a contradiction.

This is exactly what we did when we proved that $\sqrt{2}$ is irrational.

Here's a schematic diagram of the proof:

Let $P =$ "$\sqrt{2}$ <u>is</u> rational",

$\neg P =$ "$\sqrt{2}$ is <u>not</u> rational".

We showed that

$\neg P$

$\Downarrow$

$\sqrt{2} = a/b$ for some whole numbers a & b with no common factor

$\Downarrow$

$a = 2k$ for some whole number k

$\Downarrow$

$b = 2l$ for some whole number l

$\Downarrow$

a & b have common factor 2

F

We conclude that $\neg P = F$, hence $P = T$.

[Remark: We say that this proof is *indirect* because it doesn't say anything about what $\sqrt{2}$ *is*; only what it is *not*.

To say what $\sqrt{2}$ is (e.g. $\sqrt{2} = 1.41421\cdots$) would require some ideas from the mathematical subject of analysis (see MTH 433, 533/534).]

Now let's practice our skills by trying to prove that $\sqrt{3}$ is irrational.

[I won't write "Proof:" yet because we're just doing rough work at this point.]

Assume for contradiction that $\sqrt{3}$ is rational. Then we can write $\sqrt{3} = a/b$ where a & b are integers (i.e. "whole numbers") with no common factor. Square both sides to get

$$3 = a^2/b^2$$

$$\implies 3b^2 = a^2.$$

Now what? If a^2 is a multiple of 3 then what does this tell us about a? Is a also a multiple of 3? If so, how could we prove it?

We want to prove that

$$a^2 \text{ is multiple of } 3 \implies a \text{ is multiple of } 3.$$

Maybe it will be easier to prove the (Logically equivalent) contrapositive statement

$$a \ \underline{\text{not}} \text{ multiple of } 3 \implies a^2 \ \underline{\text{not}} \text{ multiple of } 3.$$

So <u>assume</u> that a is <u>not</u> a multiple of 3.

Wait, it's hard to begin a proof with a negative statement. We need to turn this into a positive statement

" If a is <u>not</u> a multiple of 3, then

$$a = \dots \quad "$$

Actually there are two separate ways for the number a to be <u>not</u> a mutiple of 3.

Case 1 : $a = 3k+1$ for some integer k.
Case 2 : $a = 3k+2$ for some integer k.

In case 1 we have

$$\begin{aligned} a^2 &= (3k+1)^2 \\ &= 9k^2 + 6k + 1 \\ &= 3(3k^2+2k) + 1, \end{aligned}$$

which is <u>not</u> a multiple of 3 (it has remainder 1 when divided by 3).

In case 2 we have

$$\begin{aligned} a^2 &= (3k+2)^2 \\ &= 9k^2 + 12k + 4 \\ &= 3(3k^2+4k+1) + 1, \end{aligned}$$

which is also <u>not</u> a multiple of 3.

Putting both cases together gives

a <u>not</u> multiple of 3 $\Longrightarrow$ a^2 <u>not</u> multiple of 3

hence

a^2 is multiple of 3 $\Longrightarrow$ a <u>is</u> multiple of 3.

///

Back to the proof: we had

$$3b^2 = a^2.$$

Thus a^2 is a multiple of 3 and hence a is a multiple of 3, say $a = 3k$. We can substitute to get

$$3b^2 = (3k)^2$$
$$3b^2 = 9k^2$$
$$b^2 = 3k^2.$$

Thus b^2 is a multiple of 3, hence so is b. Say $b = 3l$.

Now we have $a = 3k$ & $b = 3l$. But this contradicts the fact that a and b have no common factors (except ± 1).

This completes the rough work. Now we're ready to go back and write the proof nicely...

[but not today.]

Jargon for Mathematicians

Last time we did the rough work to show that $\sqrt{3}$ is irrational. Now we'll write a polished proof.

But first, let me introduce some convenient notation.

Notation:

- If S is a set (i.e. a collection of things) we write "$x \in S$" to mean that x is one of the things in the collection. We say

"$x \in S$" = "x is a member (or an element) of S".

[I guess "$\in$" stands for "element"...]

- Our favorite sets are sets of numbers:

$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$

is the set of natural numbers.

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

is the set of integers. ["Z" is for "Zahlen", i.e., "numbers".]

$\mathbb{Q}$ is the set of fractions of integers. We call this the set of rational numbers.

["rational" is for "ratio"; "Q" is for "quotient".]

$\mathbb{R}$ is the set of real numbers, i.e., numbers that have a decimal expansion.

[Note that $\sqrt{3} \in \mathbb{R}$. We want to show that $\sqrt{3} \notin \mathbb{Q}$.]

- If A and B are sets, we write "$A \subseteq B$" to mean that every element of A is also an element of B. We say

"$A \subseteq B$" = "A is a <u>subset</u> of B"

For example, we have

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}.$$

- Suppose we want to say that <u>every</u> element of a set satisfies some given property.

Let S be a set and for each element $x \in S$ let $P(x)$ be some mathematical statement about x. Then we define the notations

"$\forall x \in S, P(x)$" = "The statement $P(x)$ holds for <u>all</u> elements $x \in S$"

$\wr$

"$\exists x \in S, P(x)$" = "There exists an element $x \in S$ such that the statement $P(x)$ holds"

["$\forall$" is for "All"; "$\exists$" is for "Exists".]

For example, we have

"$A \subseteq B$" = "$\forall x \in A, x \in B$"
= "for all $x \in A$ we have $x \in B$".

- Given two integers $m, n \in \mathbb{Z}$ we will write

"$m \mid n$" = "$\exists k \in \mathbb{Z}, n = mk$"
= "there exists an integer k such that $n = mk$".

In this case we say that "m divides n" or "n is divisible by m".

$\int$

For practice, you should prove that

"$\forall n \in \mathbb{Z},\ n \mid 0$"

"$\forall n \in \mathbb{Z},\ 1 \mid n$"

are true statements.

Now I think we're ready to write a polished proof. First we will prove a lemma (i.e., a "little helper theorem").

Lemma: For all $n \in \mathbb{Z}$ we have

$$3 \mid n^2 \implies 3 \mid n.$$

Proof: We will prove the contrapositive statement

$$3 \nmid n \implies 3 \nmid n^2.$$

So assume that $3 \nmid n$. There are two ways this can happen:

Case 1: $\exists k \in \mathbb{Z}$ such that $n = 3k+1$.
In this case we have

$$\begin{aligned} n^2 &= (3k+1)^2 \\ &= 9k^2 + 6k + 1 \\ &= 3(3k^2 + 2k) + 1, \end{aligned}$$

and hence $3 \nmid n^2$ [we'll prove this later; right now it's OK if it just seems true.].

Case 2: $\exists k \in \mathbb{Z}$ such that $n = 3k+2$.
In this case we have

$$\begin{aligned} n^2 &= (3k+2)^2 \\ &= 9k^2 + 12k + 4 \\ &= 3(3k^2 + 4k + 1) + 1, \end{aligned}$$

and hence $3 \nmid n^2$.

In either case we have shown that $3 \nmid n^2$, as desired.

///

Now for the main result.

Theorem: $\sqrt{3} \notin \mathbb{Q}$.

Proof: Assume for contradiction that $\sqrt{3} \in \mathbb{Q}$. Then $\exists\, a, b \in \mathbb{Z}$ such that

- $\sqrt{3} = a/b$
- $\nexists\, d > 1$ such that $d \mid a$ and $d \mid b$.

Square both sides to get

$$3 = a^2/b^2$$
$$3b^2 = a^2.$$

Since $3 \mid a^2$ the lemma implies $3 \mid a$, say $a = 3k$ with $k \in \mathbb{Z}$. Now substitute to get

$$3b^2 = a^2$$
$$3b^2 = (3k)^2$$
$$3b^2 = 9k^2$$
$$b^2 = 3k^2.$$

Since $3 \mid b^2$, the Lemma implies that $3 \mid b$, say $b = 3l$ where $l \in \mathbb{Z}$.

But now we have $3 \mid a$ and $3 \mid b$, which contradicts the fact that a & b have no common divisor greater than 1.

We conclude that our original assumption, that $\sqrt{3} \in \mathbb{Q}$, is false.

QED.

De Morgan's Laws

Last time we gave a polished proof that $\sqrt{3} \notin \mathbb{Q}$. On HW 2 you will give a similar proof that $\sqrt{5} \notin \mathbb{Q}$.

In fact, the following more general statement is true.

☆ Theorem: Let d be an integer. Then

$$\sqrt{d} \notin \mathbb{Z} \implies \sqrt{d} \notin \mathbb{Q}.$$

That is, if d is not the square of an an integer then its square root is irrational. ///

Unfortunately, we don't have the technology to prove this yet.

In particular, I have not yet told you the formal definition (i.e. the axioms) of the set $\mathbb{Z}$. I will do this soon but first we need a bit more logical technology.

So far we have learned two "logical functions" $\neg$ & $\Rightarrow$ defined by the truth tables

P	$\neg P$
T	F
F	T

&

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

These functions are all we really need, but it is <u>convenient</u> to define two more auxiliary functions called

$$\vee \quad \& \quad \wedge .$$

$\Downarrow$

They are defined by the truth tables

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

&

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

The technical names are "logical disjunction" ($\vee$) and "logical conjunction" ($\wedge$), but we usually just say

"$P \vee R$" = "P or R"
"$P \wedge R$" = "P and R".

Does that make any sense to you? Here's the reasoning:

- "P or Q" = T means that at <u>least</u> <u>one</u> of P or Q is true.

- "P and Q" = T means that <u>both</u> P and Q are true.

This can be generalized to define the disjunction and conjunction of any family of statements.

Let I be an index set and for each index $i \in I$ consider a statement P_i.

Then we define the disjunction

$$\text{``}\bigvee_{i \in I} P_i\text{''} := \text{``}\exists\, i \in I,\ P_i\text{''}$$

= "There <u>exists</u> an index i such that P_i holds."

and the conjunction

$$\text{``}\bigwedge_{i \in I} P_i\text{''} := \text{``}\forall\, i \in I,\ P_i\text{''}$$

= "The statement P_i holds for <u>all</u> indices i".

[Does this agree with the definitions for two statements?

"$P_1 \vee P_2$" = "There exists <u>some</u> $i \in \{1,2\}$ such that P_i holds"

$\Downarrow$

" $P_1 \wedge P_2$ " = " The statement P_i holds for <u>all</u> $i \in \{1,2\}$ ".

Yes. It agrees.]

We saw how $\neg$ interacts with $\Longrightarrow$ (via the "contrapositive"). How does $\neg$ interact with $\vee$ and $\wedge$?

We need to find the opposite of the statement

" The statement P_i holds for <u>all</u> indices i. "

... After some thinking, we believe that the opposite statement is

" There <u>exists</u> some index i such that the statement P_i does <u>not</u> hold. "

Ok, so how do we say this in symbols ?

we have

$$\neg\left(\forall i \in I, P_i\right) = \exists i \in I, \neg P_i$$

In other words, we have

(*) $$\neg\left(\bigwedge_{i \in I} P_i\right) = \bigvee_{i \in I} (\neg P_i)$$

Taking $\neg$ of both sides gives

$$\bigwedge_{i \in I} P_i = \neg\left(\bigvee_{i \in I} (\neg P_i)\right)$$

and then substituting $Q_i = \neg P_i$ (hence $P_i = \neg Q_i$) gives

(**) $$\bigwedge_{i \in I} (\neg Q_i) = \neg\left(\bigvee_{i \in I} Q_i\right)$$

The statements (*) and (**) are called <u>de Morgan's Laws</u>.

For poseterity, let's write (*) and (**) down in the case of two statements.

☆ Logical Principle ("de Morgan's laws"):

For all statements P and Q we have

- $\neg(P \vee Q) = (\neg P) \wedge (\neg Q)$
- $\neg(P \wedge Q) = (\neg P) \vee (\neg Q)$.

[You will prove one of these on HW2.1 using a truth table.]

OK, so what? These logical principles are often helpful in proving mathematical theorems.

Example: Let $m, n \in \mathbb{Z}$. Prove that

"mn is odd" $\Rightarrow$ "m is odd or n is odd".

Let P = "mn is odd"
Q = "m is odd"
R = "n is odd".

We want to prove $P \Rightarrow (Q \vee R)$.

How?

Instead we will prove the contrapositive

$$\neg(Q \vee R) \Longrightarrow \neg P$$

Using de Morgan's law, this is the same as

$$(\neg Q \wedge \neg R) \Longrightarrow \neg P$$

In other words,

"m and n are both even" $\Longrightarrow$ "mn is even".

Proof: Suppose m and n are both even, say $m = 2k$ and $n = 2l$ for some $k, l \in \mathbb{Z}$. Then we have

$$\begin{aligned} mn &= (2k)(2l) \\ &= 2(2kl), \end{aligned}$$

which is even.

QED.

Now what about the converse statement?

" $\forall m, n \in \mathbb{Z}$ we have

(m is odd or n is odd) $\Longrightarrow$ (mn is odd) "

I claim that this statement is FALSE.
How can we prove it?

We need two principles.

1. Let S be a set and for each element x, let $P(x)$ & $Q(x)$ be logical statements. Then by de Morgan's Law we have

$$\neg \text{"} \forall x \in S, \ P(x) \Longrightarrow Q(x) \text{"}$$

$$= \text{"} \exists x \in S, \ \neg \left(P(x) \Longrightarrow Q(x) \right) \text{"}.$$

i.e., ¬ " for all x, $P(x)$ implies $Q(x)$ "

= " There exists some x such that $P(x) \Rightarrow Q(x)$ is False. ".

(2) What does it mean to say that

$$P \Rightarrow Q \text{ is False ?}$$

On the HW2 you will use a truth table to show that

$$(P \Rightarrow Q) = (\neg P) \vee Q.$$

Then combining this with de Morgan's Law gives

$$\begin{aligned} \neg(P \Rightarrow Q) &= \neg\left((\neg P) \vee Q\right) \\ &= (\neg\neg P) \wedge (\neg Q) \\ &= P \wedge (\neg Q) \end{aligned}$$

i.e. " $P \Rightarrow Q$ is false " means that

" P is true and Q is false. " //

By combining (1) & (2) we obtain

$\downarrow$

$\neg$ " $\forall x \in S,\ P(x) \Rightarrow Q(x)$ "

$=$ " $\exists x \in S,\ P(x) \wedge \neg Q(x)$ ".

Now let's apply it to our problem.

The opposite of

$\forall m,n \in \mathbb{Z}$, (m or n is odd) $\Rightarrow$ (mn is odd)

is

$\exists m,n \in \mathbb{Z}$, (m or n is odd) but (mn is even).

To prove that such integers m, n exist
I just have to give you one example:

take $m = 1$ & $n = 2$.

Then (m or n is odd) is true
but (mn is odd) is false.

///

Moral: To <u>dis</u>prove a universal ($\forall$) statement we need only provide a single ($\exists$) counterexample.

Another Practice Problem.

Prove that $\forall m, n \in \mathbb{Z}$ we have

$$(mn \text{ even}) \Longleftrightarrow (m \text{ or } n \text{ is even}).$$

Let $P =$ "mn is even"
$Q =$ "m is even"
$R =$ "n is even".

We want to prove $P \Leftrightarrow (Q \vee R)$, and this requires two separate proofs.

<u>Proof of $P \Rightarrow (Q \vee R)$:</u>

Instead we will prove the contrapositive

$$\neg(Q \vee R) \Longrightarrow \neg P$$
$$(\neg Q \wedge \neg R) \Longrightarrow \neg P$$
$$(m \text{ <u>and</u> } n \text{ are odd}) \Longrightarrow (mn \text{ is odd}).$$

We have proved this many times. ✓

Proof of $(Q \vee R) \Rightarrow P$:

To prove (m or n is even) $\Rightarrow$ (mn is even) we need to prove two separate cases.

Case 1: If m is even then $m = 2k$ for some $k \in \mathbb{Z}$ and hence

$$mn = (2k)n = 2(kn) \text{ is even } \checkmark.$$

Case 2: If n is even then $n = 2l$ for some $l \in \mathbb{Z}$ and hence

$$mn = m(2l) = 2(ml) \text{ is even } \checkmark.$$

This completes the proof.

QED.

More formally, we can use a truth table to show for all statements P, Q, R that

$$\big((P \vee Q) \Rightarrow R\big) = \big(\underbrace{(P \Rightarrow R)}_{\text{Case 1}} \wedge \underbrace{(Q \Rightarrow R)}_{\text{Case 2}}\big).$$

Since our Boolean functions involve 3 inputs P, Q, R there will be $8 = 2^3$ in our table:

P	Q	R	$P \vee Q$	$(P \vee Q) \Rightarrow R$	$P \Rightarrow R$	$Q \Rightarrow R$	$(P \Rightarrow R) \wedge (Q \Rightarrow R)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	F
T	F	T	T	T	T	T	T
T	F	F	T	F	F	T	F
F	T	T	T	T	T	T	T
F	T	F	T	F	T	F	F
F	F	T	F	T	T	T	T
F	F	F	F	T	T	T	T

Note that the 5th & 8th columns are the same.

A truth table is not very fun but it always works.

Introduction to Induction

There is just one more proof technique that we need to discuss, called

Induction.

I'll introduce it with an example. My experience shows that students never fully grasp induction on the first try, so we will return to the idea many times in this course.

Example: Try to prove that

$$\log_2(3) \text{ is irrational.}$$

I will assume that there exists a real number $x = \log_2(3)$ with the property that

$$2^x = 3$$

Now let's assume for contradiction that $x = a/b$ for some $a, b \in \mathbb{Z}$, so we have

$$2^{a/b} = 3.$$

Raise both sides to the power of b to get

$$\left(2^{a/b}\right)^b = 3^b$$
$$2^a = 3^b.$$

Since a & b are whole numbers I claim that this is a contradiction.

Indeed, since $x > 0$ we may assume W.L.O.G. ("without loss of generality") that $a \geq 1$ and $b \geq 1$. Then

2^a is an <u>even</u> number

because $2^a = 2(2^{a-1})$, where 2^{a-1} is an integer.

But I claim that

3^b is not an even number.

It's easy to see why this is true but it's kind of hard to prove it. The idea is that

- 3^b is a product of 3's
- 3 is odd
- odd times odd is odd,
- therefore 3^b is odd.

To actually make this work we need a technique called induction. I'll show you how it works.

Lemma: 3^n is odd for all $n \geq 1$.

Proof by Induction on n:

There are two steps:

Step 1: Note that $3^1 = 3$ is odd. ✓

Step 2: Let's assume that 3^n is odd for some integer $n \geq 1$, then we have

$$3^{n+1} = \underbrace{3^n \times 3}_{\text{odd} \times \text{odd}},$$

which implies that 3^{n+1} is also odd. This completes the proof QED.

What? Here's the intution. We want to show that the sequence of integers

$$3, 3^2, 3^3, 3^4, \ldots$$

is odd forever. Step 1 tells us that sequence starts off being odd and Step 2 tells us that the sequence never stops being odd.

That's good enough.

Semi-Review for Exam1

For review please see the provided practice exams and solutions.

Today I will do a semi-review.

Let A & B be sets. Recall that

$$\text{"}A \subseteq B\text{"} = \text{"}\forall x \in A,\ x \in B\text{"}.$$

In this case we say that A is a <u>subset</u> of B.

Q: What does it mean to say that A is <u>not</u> a subset of B?

A: $\text{"}A \not\subseteq B\text{"} = \neg\text{"}A \subseteq B\text{"}$

$$= \neg\text{"}\forall x \in A,\ x \in B\text{"}$$

$$= \text{"}\exists x \in A,\ x \notin B\text{"}$$

["there exists an element of A that is not in B".]

Now let $\mathcal{U}$ be some "universal set" [containing everything we might want to talk about], and let $A \subseteq \mathcal{U}$ and $B \subseteq \mathcal{U}$ be subsets of $\mathcal{U}$.

In this case there is another way to say "$A \subseteq B$":

$$\text{"}A \subseteq B\text{"} = \text{"}\forall x \in \mathcal{U},\ x \in A \Rightarrow x \in B\text{"}$$

Then computing the negation gives

$$\begin{aligned} \text{"}A \not\subseteq B\text{"} &= \neg\text{"}A \subseteq B\text{"} \\ &= \neg\text{"}\forall x \in \mathcal{U},\ x \in A \Rightarrow x \in B\text{"} \\ &= \text{"}\exists x \in \mathcal{U},\ x \in A \not\Rightarrow x \in B\text{"}. \end{aligned}$$

But what the heck does $\not\Rightarrow$ mean?!

On HW2 Problem 1 you used a truth table to show that for all statements P & Q we have

$$\text{"}P \Rightarrow Q\text{"} = \text{"}\neg P \vee Q\text{"}.$$

Then we can apply de Morgan's law to compute the negation:

$$
\begin{aligned}
(P \not\Rightarrow Q) &= \neg(P \Rightarrow Q) \\
&= \neg(\neg P \vee Q) \\
&= (\neg\neg P) \wedge (\neg Q) \\
&= P \wedge \neg Q .
\end{aligned}
$$

OK, whatever...
Let's apply this to analyze the statement "$A \not\subseteq B$".

$$
\begin{aligned}
(A \not\subseteq B) &= \neg(A \subseteq B) \\
&= \neg(\forall x \in \mathcal{U},\ x \in A \Rightarrow x \in B) \\
&= (\exists x \in \mathcal{U},\ x \in A \not\Rightarrow x \in B) \\
&= (\exists x \in \mathcal{U},\ x \in A \wedge x \notin B) .
\end{aligned}
$$

[Here we used $P = (x \in A)$ & $Q = (x \in B)$ so that $(P \not\Rightarrow Q) = (P \wedge \neg Q)$.].

In other words, "$A \not\subseteq B$" means that there exists a thing x in the universe such that x is in A but not in B.

Does that make sense?

Finally, here is an induction review problem

Induction Problem:

For all integers $n \geq 0$ prove that

$$6 \mid (2n^3 + 3n^2 + n).$$

In other words, prove that there exists an integer $k \in \mathbb{Z}$ such that

$$6 \cdot k = 2n^3 + 3n^2 + n.$$

Proof:

Base Case: Let $n = 0$. Then the statement $6 \mid 0$ is true.

(Indeed, just take $k = 0$.)

Induction Step: For all $n \geq 0$ we will prove that

$$6 \mid (2n^3 + 3n^2 + n) \Longrightarrow 6 \mid \left(2(n+1)^3 + 3(n+1)^2 + (n+1)\right).$$

[Remark: Here we are proving infinitely many arrows $\Longrightarrow$, one for each $n \geq 0$.]

So consider any $n \geq 0$ and assume that

$$6 \mid (2n^3 + 3n^2 + n)$$

i.e., assume $\exists k \in \mathbb{Z}$, $2n^3 + 3n^2 + n = 6k$.
In this case we have

$$2(n+1)^3 + 3(n+1)^2 + (n+1)$$

$$= 2(\cancel{n^3} + 3n^2 + 3n + 1) + 3(\cancel{n^2} + 2n + 1) + (\cancel{n} + 1)$$

$$= (2n^3 + 3n^2 + n) + 6n^2 + 6n + 2 + 6n + 3 + 1$$

$$= 6k + 6n^2 + 6n + 6$$

$$= 6(k + n^2 + n + 1),$$

which implies that $6 \mid \left(2(n+1)^3 + 3(n+1)^2 + (n+1)\right)$

as desired.

This completes the proof.