Brain Teaser

What’s wrong with this “proof” that \( 2 = 1 \)?

Let \( a \) and \( b \) be integers, such that \( a = b \).

\[
\begin{align*}
& a = b \\
& 2a = a + b \\
& 2a - 2b = a - b \\
& 2(a - b) = (a - b) \\
& 2 = 1 \quad ??
\end{align*}
\]

Add \( a \) to both sides

Subtract \( 2b \) from both sides

Factor left side

Divide both sides by \( (a - b) \)
Introduction to Proofs

• Definitions
• Properties of integers
• Basic strategies of proofs
Odd and Even

• An integer $m$ is even iff there exists an integer $n$, such that $m=2n$

• An integer $m$ is odd iff there exists an integer $n$, such that $m=2n+1$

• Thm (without proof): Every integer is either odd or even
Closure

• Whenever the operations of multiplication, addition, or subtraction are applied to integers, the result is another integer.
  o The set of integers is closed under the operations of multiplication, addition, subtraction.

• Notice: lots of interesting operations are missing from this list
First Proof

• Proposition: The sum of any odd integer with any even integer is an odd integer
  o Proof: let $x=2m$ and $y=2n+1$. Then...
  o $z=x+y=2m+2n+1=2(m+n)+1=2k+1$.
  o ($z$ is an integer---how do we know that?)
  o Thus, for any odd and even integer, their sum is another integer that can be expressed in the form $2k+1$, and thus their sum is odd.
Observations on First Proof

• Use the definitions to express things to reveal fundamental properties

• Use variables that represent any element in the domain.

• Apply rules/properties that are true for every element in the domain.

• The resulting conclusions are true for any element in the domain
Another Proposition

• Proposition: For all integers, if $n^2$ is even, then $n$ is even.

• **A flawed proof:**
  - Let $n^2$ be even. Therefore there is some int $k$ s.t. $n^2 = 2k$
  - Now we can solve: $n = 2(k/n)$
  - Therefore, $n$ is of the form $n = 2m$, where $m = (k/n)$, and therefore $n$ is even.
Another Flawed Proof

- If $n$ is even, then $n=2k$
- Therefore, $n^2=4k^2=2(2k^2)$.
- Integers are closed under mult, and therefore $k^2=m$, where $m$ is an int
- Therefore, $n^2=2m$
- Therefore, $n^2$ is even.
Proof by Contrapositive

• Contrapositive of proposition:
  o If \( n \) is odd, then \( n^2 \) is odd

• Proof:
  o Let \( n=2k+1 \), be odd.
  o Then, \( n^2=(2k+1)^2 \)
    • \( =4k^2+4k+1 \)
    • \( =2(2k^2+2k)+1 \)
    • \( =2m+1 \)
  o And...
    • \( m \) is in integer (why?)
  o Therefore, \( n^2 \) is odd.

• Thus, if \( n \) is odd, then \( n^2 \) is odd.
• By contrapositive, if \( n^2 \) is even, then \( n \) is even.
Factors and Primes

• \( n \in \mathbb{Z} \) is a factor of \( k \in \mathbb{Z} \) \( \iff \exists m \in \mathbb{Z}, \ k = mxn. \)
  
  o In this case we say that \( n \) divides \( k \)
  
  o \textit{divides} symbol to form predicate: \( n \mid k \)

• Every integer has an associated set of factors
  
  o The following predicates are true: \( 1 \mid k, \ klk \)

• \( n \in \mathbb{Z} \) is a prime number \( \iff \exists \) no factors other than 1 and \( n \).
Another Proposition

• $n \in \mathbb{Z}$ is a perfect square $\iff \exists \ m \in \mathbb{Z}, n = m^2$.

• Proposition: for $n > 4, n \in \mathbb{Z}; \ n$ is a perfect square $\Rightarrow n-1$ is not a prime

• Proof?
  o How do we prove an number is not a prime?
  o How can we take advantage of the hypothesis?
Proof

- $n=m^2$
- $\Rightarrow n-1=m^2-1$
- How can we show that $m^2-1$ is not a prime?
  - Factor it!
- $m^2-1=(m+1)(m-1)=a \times b$
  - And $a,b \in \mathbb{Z}$ (why?)
- Also, $a,b \neq (n-1), a,b \neq 1$,
  - Why is this necessary? (taking care of the details)
  - Why is this true?
- $\Rightarrow n-1$ has factors other than $n-1$ and 1
- Therefore is $n-1$ is not a prime.
Rational Numbers

- A number $r \in \mathbb{R}$ is **rational** iff $\exists \ a, b \in \mathbb{Z}$, $r = \frac{a}{b}$.
  - Rational numbers (fractions) can be expressed in many equivalent ways (e.g. $1/2$, $2/4$, $3/6$)
  - The set of rational numbers is sometimes called “$\mathbb{Q}$”

- A number is **irrational** if it is not rational.
Proposition

• For any rational number \( r \), the number \( r+1 \) is also rational
  • State the proposition
    • \( r \in \mathbb{Q} \rightarrow r+1 \in \mathbb{Q} \)
  • Spell out definitions/properties of hypothesis
    o \( r = \frac{a}{b} \)
  • Express the conclusion in terms of hypothesis
    o \( r+1 = \frac{a}{b} + 1 = \frac{a+b}{b} = \frac{c}{b} \),
  • Take care of some details
    o \( c, b \in \mathbb{Z} \), by closure
  • Therefore, \( r+1 \) is rational
Proof Ideas/Guidelines

• What is more difficult?
  o Proving a number is irrational or...
  o Proving a number is rational?

• What about primes?
  o Proving n is prime or not prime?

• Generally (it’s only a guideline) it is difficult to disprove properties that contain “∃”, especially if the domain is large/infinite
Another Proposition (+ Proof)

• Proposition: For any $x \in \mathbb{R}$, if $2x$ is irrational, then $x$ is irrational
  - $2x \in \mathbb{Q}' \rightarrow x \in \mathbb{Q}'$
• Proving irrational can be hard
• Use contrapositive
  - $x \in \mathbb{Q} \rightarrow 2x \in \mathbb{Q}$
• Proof:
  - $x \in \mathbb{Q} \rightarrow x = a/b \rightarrow y=2x=2a/b=k/b$
  - Therefore, $2x$ is rational
Proof by Cases

• Proposition: \( n \in \mathbb{Z} \rightarrow m = n^2 + n \) is even
  
  o We would like to build an expression for \( m \) in a way that reflects odd/even.
  
  • I.e. it should have a factor of two in there somewhere.
Proof Continued...

- Idea: if $n$ is even, then $n=2k \rightarrow m = 4k^2+2k = 2(2k^2+k) = 2b$. $b \in \mathbb{Z} \rightarrow n$ is even.

- If $n$ is odd..

- $n=2k+1 \rightarrow$
  - $m = (2k+1)^2+2k+1$
  - $= 4k^2+4k+1+2k+1$
  - $= 2(2k^2+3k+1)$
  - $= 2b \rightarrow m$ is even
Proof Continued...

• Therefore $n^2+n$ is even for $n \in \mathbb{E}$ or $n \in \mathbb{O}$
• Therefore, $n^2+n$ is even for all integers
• A small technical problem
  o How do we know that all integers are either odd or even?
  o They are
    • But we have not proved that...yet
• $\rightarrow$ Technically, this proof is not correct
The Division Theorem

• For all $a, b \in \mathbb{Z} \land b > 0$, $\exists \ q \in \mathbb{Z}$ (quotient), $r \in \mathbb{Z}$ (remainder), such that
  - $a = b \cdot q + r$, and
  - $0 \leq r < b$

• E.g.
  - $23 = 4 \cdot 5 + 3$
  - $49 = 4 \cdot 10 + 9$
  - $103 = 7 \cdot 14 + 5$
Some More Division

• “Divided by”, the symbol “÷” returns the quotient.
  o 5 ÷ 2 = 2
  o 11 ÷ 3 = 3

• “modulo”, denoted “mod”
  o 5 mod 2 = 1
  o -22 mod 6 = 2
  o 8 mod 11 = 8
Proposition and Proof

• If \( n \) is any integer not divisible by 5, then \( n \) has a square that his of either the form \( 5k+1 \) or \( 5k+4 \).
  
  \[ \forall n \in \mathbb{Z}, (n \mod 5)=0 \rightarrow \exists k \in \mathbb{Z}, (n^2=2k+1) \lor (n^2=2k+4) \]

• Proof by cases
  
  o \( (n \mod 5 = 1) \)
  o \( (n \mod 5 = 2) \)
  o \( (n \mod 5 = 3) \)
  o \( (n \mod 5 = 4) \)
Practice Proofs

• If $a | b$ and $a | c$, then $a | (b + c)$
• If $a | b$ and $a | c$, then $a^2 | (b \cdot c)$
• If $9 | (10^{n-1} - 1)$, then $9 | (10^n - 1)$
Brain Teaser

What’s wrong with this “proof” that $2 = 1$?

Let $a$ and $b$ be integers, such that $a = b$.

\[
\begin{align*}
a &= b \\
2a &= a + b & \text{Add a to both sides} \\
2a - 2b &= a - b & \text{Subtract 2b from both sides} \\
2(a - b) &= (a - b) & \text{Factor left side} \\
2 &= 1 \text{ ??} & \text{Divide both sides by (a - b)}
\end{align*}
\]