Discrete Mathematics

(Proof Techniques)

Class Notes

January 2025

What is a proof?

Definition

- A proof is a method for establishing the truth of a statement.

Rigor	Truth type	Field	Truth teller
0	Word of God	Religion	God/Priests
1	Authoritative truth	Business/School	Boss/Teacher
2	Legal truth	Judiciary	Law/Judge/Law makers
3	Philosophical truth	Philosophy	Plausible argument
4	Scientific truth	Physical sciences	Experiments/Observations
5	Statistical truth	Statistics	Data sampling
6	Mathematical truth	Mathematics	Logical deduction

What is a mathematical proof?

Definition

- A mathematical proof is a verification for establishing the truth of a proposition by a chain of logical deductions from a set of axioms

Concepts

1. Proposition

   Covered in sufficient depth in logic
2. Axiom

   An axiom is a proposition that is assumed to be true

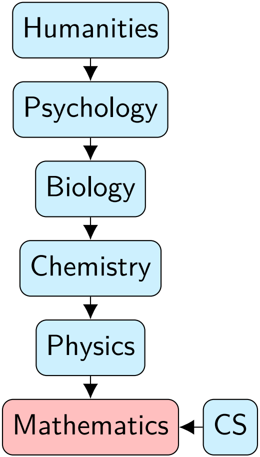
   Example: For mathematical quantities a and b, if $a = b$, then $b = a$
3. Logical deduction

   We call this process – the axiomatic method

   We will cover several proof techniques in this chapter

Why care for mathematical proofs?

- The current world ceases to function without math proofs
- (My belief) Reduction tree showing subjects that possibly could be expressed or understood in terms of other subjects



Methods of mathematical proof

Statements	Method of proof
Proving existential statements	Constructive proof
(Disproving universal statements)	Non-constructive proof
Proving universal statements	Direct proof
(Disproving existential statements)	Proof by mathematical induction
	Well-ordering principle
	Proof by exhaustion
	Proof by cases
	Proof by contradiction
	Proof by contraposition
	Computer-aided proofs

Introduction to number theory

Definition

- Number theory is the branch of mathematics that deals with the study of integers

Numbers	Set
Natural numbers ($\mathbb{N}$)	$\{1, 2, 3, \ldots\}$
Whole numbers ($\mathbb{W}$)	$\{0, 1, 2, \ldots\}$
Integers ($\mathbb{Z}$)	$\{0, \pm 1, \pm 2, \pm 3, \ldots\}$
Even numbers ($\mathbb{E}$)	$\{0, \pm 2, \pm 4, \pm 6, \ldots\}$
Odd numbers ($\mathbb{O}$)	$\{\pm 1, \pm 3, \pm 5, \pm 7, \ldots\}$
Prime numbers ($\mathbb{P}$)	$\{2, 3, 5, 7, 11, \ldots\}$
Composite numbers ($\mathbb{C}$)	{Natural numbers (> 1) that are not prime}
Rational numbers ($\mathbb{Q}$)	{Ratio of integers with non-zero denominator}
Real numbers ($\mathbb{R}$)	{Numbers with infinite decimal representation}
Irrational numbers ($\mathbb{I}$)	{Real numbers that are not rational}
Complex numbers ($\mathbb{S}$)	{real $+ i \cdot$ real}

Even and odd numbers

Definitions

- An integer n is even iff n equals twice some integer; Formally, for any integer n,

$$n \text{ is even} \Leftrightarrow n = 2k \text{ for some integer } k$$

- An integer n is odd iff n equals twice some integer plus 1; Formally, for any integer n,

$$n \text{ is odd} \Leftrightarrow n = 2k + 1 \text{ for some integer } k$$

Examples

- Even numbers: $0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, \ldots$
- Odd numbers: $1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, \ldots$

Rational and irrational numbers

Definitions

- A real number r is rational iff it can be expressed as a ratio of two integers with a nonzero denominator;
  Formally, if r is a real number, then

$$r \text{ is rational} \Leftrightarrow \exists \text{ integers } a, b \text{ such that } r = \frac{a}{b} \text{ and } b \neq 0$$

- A real number r is irrational iff it is not rational

Examples

- Rational numbers:
  $10, -56.47, 10/13, 0, -17/9, 0.121212\ldots, -91, \ldots$
- Irrational numbers:
  $\sqrt{2}, \sqrt{3}, \sqrt{2}^{\sqrt{2}}, \pi, \phi, e, \pi^2, e^2, 2^{1/3}, \log_2 3, \ldots$
- Open problems:
  It's not known if $\pi + e, \pi e, \pi/e, \pi^e, \pi^{\sqrt{2}}$, and $\ln \pi$ are irrational

Divisibility

Definitions

- If n and d are integers, then n is divisible by d, denoted by $d|n$, iff n equals d times some integer and $d \neq 0$;
  Formally, if n and d are integers

$$d|n \Leftrightarrow \exists \text{ integer } k \text{ such that } n = dk \text{ and } d \neq 0$$

- Instead of "n is divisible by d," we can say:
  n is a multiple of d, or
  d is a factor of n, or
  d is a divisor of n, or
  d divides n (denoted by $d|n$)
- Note: $d|n$ is different from d/n

Examples

- Divides: $1|1, 10|10, 2|4, 3|24, 7| - 14, \ldots$
- Does not divide: $2 \nmid 1, 10 \nmid 1, 10 \nmid 2, 7 \nmid 10, 10 \nmid 7, 10 \nmid -7, \ldots$

Quotient-Remainder theorem

Theorem

- Given any integer n and a positive integer d, there exists an integer q and a whole number r such that

$$n = qd + r \text{ and } r \in [0, d-1]$$

Examples

- Let $n = 6$ and $d \in [1, 7]$

Num. (n)	Divisor (d)	Theorem	Quotient (q)	Rem. (r)
6	1	$6 = 6 \times 1 + 0$	6	0
6	2	$6 = 3 \times 2 + 0$	3	0
6	3	$6 = 2 \times 3 + 0$	2	0
6	4	$6 = 1 \times 4 + 2$	1	2
6	5	$6 = 1 \times 5 + 1$	1	1
6	6	$6 = 1 \times 6 + 0$	1	0
6	7	$6 = 0 \times 7 + 6$	0	6

Prime numbers

Num.	Factorization	Prime?
2	$2 = 1 \times 2 = 2 \times 1$	✓
3	$3 = 1 \times 3 = 3 \times 1$	✓
4	$4 = 1 \times 4 = 4 \times 1 = 2 \times 2$	✗
5	$5 = 1 \times 5 = 5 \times 1$	✓
6	$6 = 1 \times 6 = 6 \times 1 = 2 \times 3 = 3 \times 2$	✗
7	$7 = 1 \times 7 = 7 \times 1$	✓
8	$8 = 1 \times 8 = 8 \times 1 = 2 \times 4 = 4 \times 2$	✗
9	$9 = 1 \times 9 = 9 \times 1 = 3 \times 3$	✗
10	$10 = 1 \times 10 = 10 \times 1 = 2 \times 5 = 5 \times 2$	✗
11	$11 = 1 \times 11 = 11 \times 1$	✓
12	$12 = 1 \times 12 = 12 \times 1 = 2 \times 6 = 6 \times 2 = 3 \times 4 = 4 \times 3$	✗
13	$13 = 1 \times 13 = 13 \times 1$	✓
14	$14 = 1 \times 14 = 14 \times 1 = 2 \times 7 = 7 \times 2$	✗
15	$15 = 1 \times 15 = 15 \times 1 = 3 \times 5 = 5 \times 3$	✗
16	$16 = 1 \times 16 = 16 \times 1 = 2 \times 8 = 8 \times 2 = 4 \times 4$	✗
17	$17 = 1 \times 17 = 17 \times 1$	✓

Prime numbers

Definitions

- A natural number n is prime iff $n > 1$ and it has exactly two positive divisors: 1 and n
- A natural number n is composite iff $n > 1$ and it has at least three positive divisors, two of which are 1 and n
- A natural number n is a perfect square iff it has an odd number of divisors
- A natural number n is not a perfect square iff it has an even number of divisors

Examples

- Perfect squares: $1, 4, 9, 16, 25, \ldots$
- Not perfect squares: $2, 3, 5, 6, 7, 8, 10, \ldots$

Prime numbers

Definitions

- A natural number n is prime iff $n > 1$ and for all natural numbers r and s, if $n = rs$, then either r or s equals n; Formally, for each natural number n with $n > 1$,

$$n \text{ is prime} \Leftrightarrow \forall \text{ natural numbers } r \text{ and } s, \text{ if } n = rs \text{ then } n = r \text{ or } n = s$$

- A natural number n is composite iff $n > 1$ and $n = rs$ for some natural numbers r and s with $1 < r < n$ and $1 < s < n$; Formally, for each natural number n with $n > 1$,

$$n \text{ is composite} \Leftrightarrow \exists \text{ natural numbers } r \text{ and } s, \text{ if } n = rs \text{ and } 1 < r < n \text{ and } 1 < s < n$$

Unique prime factorization of natural numbers

n	Unique prime factorization
2	2
3	3
4	2^2
5	5
6	2×3
7	7
8	2^3
9	3^2
10	2×5
11	11
12	$2^2 \times 3$
13	13
14	2×7
15	3×5

n	Unique prime factorization
16	2^4
17	17
18	2×3^2
19	19
20	$2^2 \times 5$
21	3×7
22	2×11
23	23
24	$2^3 \times 3$
25	5^2
26	2×13
27	3^3
28	$2^2 \times 7$
29	29

n	Unique prime factorization
30	$2 \times 3 \times 5$
31	31
32	2^5
33	3×11
34	2×17
35	5×7
36	$2^2 \times 3^2$
37	37
38	2×19
39	3×13
40	$2^3 \times 5$
41	41
42	$2 \times 3 \times 7$
43	43

- What is the pattern?

Unique prime factorization of natural numbers

Definition

- Any natural number $n > 1$ can be uniquely represented as a product of as follows:

$$n = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_k^{e_k}$$

  such that $p_1 < p_2 < \cdots < p_k$ are primes in $[2, n]$, $e_1, e_2, \ldots, e_k$ are whole number exponents, and k is a natural number.
- The theorem is also called fundamental theorem of arithmetic
- The form is called standard factored form

Some terms

Definitions

- Absolute value of real number x, denoted by $|x|$ is
  $$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$
- Triangle inequality. For all real numbers x and y,
  $|x + y| \leq |x| + |y|$
- Floor of a real number x, denoted by $\lfloor x \rfloor$ is
  $\lfloor x \rfloor =$ unique integer n such that $n \leq x < n + 1$
  $\lfloor x \rfloor = n \Leftrightarrow n \leq x < n + 1$
- Ceiling of a real number x, denoted by $\lceil x \rceil$ is
  $\lceil x \rceil =$ unique integer n such that $n - 1 < x \leq n$
  $\lceil x \rceil = n \Leftrightarrow n - 1 < x \leq n$

Some terms

Definitions

- Given an integer n and a natural number d,
  n div $d =$ integer quotient obtained when n is divided by d,
  n mod $d =$ whole number remainder obtained when n is divided by d.
- Symbolically,
  n div $d = q$ and n mod $d = r \Leftrightarrow n = dq + r$
  where q and r are integers and $0 \leq r < d$.

Properties of a proof

Properties

- Concise (not unnecessarily long)
- Clear (not ambiguous)
- Complete (no missing intermediate steps)
- Logical (every statement logically follows)
- Rigorous (uses mathematical expressions)
- Convincing (does not raise questions)
- The way a proof is presented might be different from the way the proof is discovered.

Direct Proof

Even + odd = odd

Proposition

- Sum of an even integer and an odd integer is odd.

Even + odd = odd

Proposition

- Sum of an even integer and an odd integer is odd.

Proof

- Suppose a is even and b is odd. Then

$$\begin{aligned}
&a + b \\
&= (2m) + b && \text{(defn. of even, } a = 2m \text{ for integer } m\text{)} \\
&= (2m) + (2n + 1) && \text{(defn. of odd, } b = 2n + 1 \text{ for integer } n\text{)} \\
&= 2(m + n) + 1 && \text{(taking 2 as common factor)} \\
&= 2p + 1 && (p = m + n \text{ and addition is closed on integers)} \\
&= \text{odd} && \text{(defn. of odd)}
\end{aligned}$$

Problems for practice

Prove the following propositions:

- Even + even = even
- Even + odd = odd
- Odd + odd = even
- Even × integer = even
- Odd × odd = odd

n is odd $\Rightarrow$ n^2 is odd

Proposition

- The square of an odd integer is odd.

n is odd $\Rightarrow n^2$ is odd

Proposition

- The square of an odd integer is odd.

Proof

- Prove: If n is odd, then n^2 is odd.

  n is odd

$$
\begin{aligned}
&\Longrightarrow\ n = (2k+1) && \text{(defn. of odd, } k \text{ is an integer)}\\
&\Longrightarrow\ n^2 = (2k+1)^2 && \text{(squaring on both sides)}\\
&\Longrightarrow\ n^2 = 4k^2 + 4k + 1 && \text{(expanding the binomial)}\\
&\Longrightarrow\ n^2 = 2(2k^2 + 2k) + 1 && \text{(factoring 2 from first two terms)}\\
&\Longrightarrow\ n^2 = 2j + 1 && \text{(let } j = 2k^2 + 2k\text{)}\\
&\qquad \text{(} j \text{ is an integer as mult. and add. are closed on integers)}\\
&\Longrightarrow\ n^2 \text{ is odd} && \text{(defn. of odd)}
\end{aligned}
$$

Odd = difference of squares

Proposition

- Every odd integer is equal to the difference between the squares of two integers

Odd = difference of squares

Proposition

- Every odd integer is equal to the difference between the squares of two integers

Workout

- Write a formal statement.
  $\forall$ integer k, $\exists$ integers m, n such that
  $(2k+1) = m^2 - n^2$.
- Try out a few examples.

$$\begin{aligned} 1 &= 1^2 - 0^2 & \qquad -1 &= 0^2 - (-1)^2 \\ 3 &= 2^2 - 1^2 & -3 &= (-1)^2 - (-2)^2 \\ 5 &= 3^2 - 2^2 & -5 &= (-2)^2 - (-3)^2 \\ 7 &= 4^2 - 3^2 & -7 &= (-3)^2 - (-4)^2 \end{aligned}$$

- Find a pattern.
  $(k+1)^2 - k^2 = (k^2 + 2k + 1) - k^2 = 2k + 1 =$ odd

Odd = difference of squares

Proposition

- Every odd integer is equal to the difference between the squares of two integers.

Proof

- Any odd integer can be written as $(2k+1)$ for some integer k.
- We rewrite the expression as follows.

  $2k + 1$

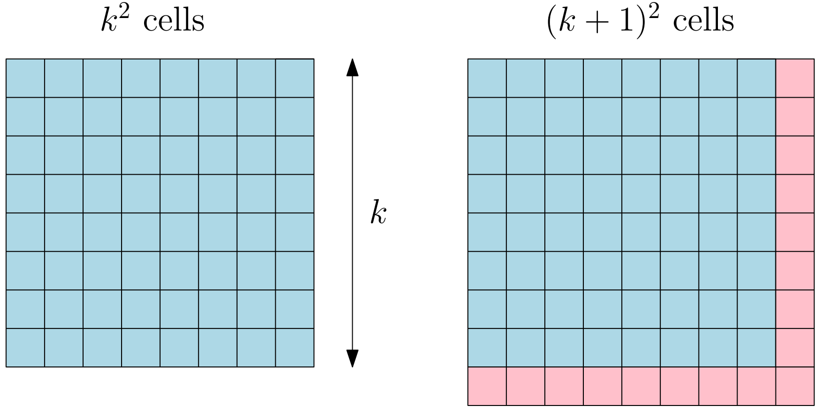
  $= (k^2 + 2k + 1) - k^2$ (adding and subtracting k^2)

  $= (k + 1)^2 - k^2$ (write the first term as sum)

  $= m^2 - n^2$ (set $m = k + 1$ and $n = k$)

  The term m is an integer as addition is closed on integers.
- So, every odd integer can be written as the difference between two squares.

Odd = difference of squares



k^2 cells

k

$(k+1)^2$ cells

If $a|b$ and $b|c$, then $a|c$

Proposition

- (Transitivity) For integers a, b, c, if $a|b$ and $b|c$, then $a|c$.

If $a|b$ and $b|c$, then $a|c$

Proposition

- (Transitivity) For integers a, b, c, if $a|b$ and $b|c$, then $a|c$.

Proof

- Formal statement.
  $\forall$ integers a, b, c, if $a|b$ and $b|c$, then $a|c$.
- c

$$\begin{aligned}
&= bn && (b|c \text{ and definition of divisibility})\\
&= (am)n && (a|b \text{ and definition of divisibility})\\
&= a(mn) && (\text{multiplication is associative})\\
&= ak && (\text{let } k = mn \text{ and multiplication is closed on integers})\\
&\implies a|c && (\text{definition of divisibility and } k \text{ is an integer})
\end{aligned}$$

Summation

Proposition

- $1 + 2 + 3 + \cdots + n = n(n+1)/2.$

Summation

Proposition

- $1 + 2 + 3 + \cdots + n = n(n+1)/2$.

Proof

- Formal statement. $\forall$ natural number n, prove that $1 + 2 + 3 + \cdots + n = n(n+1)/2$.
- $S = 1 + 2 + 3 + \cdots + n$

  $\implies S = n + (n-1) + (n-2) + \cdots + 1$

  (addition on integers is commutative)

  $\implies 2S = \underbrace{(n+1) + (n+1) + (n+1) + \cdots + (n+1)}_{n \text{ terms}}$

  (adding the previous two equations)

  $\implies 2S = n(n+1)$ (simplifying)

  $\implies S = n(n+1)/2$ (divide both sides by 2)

Proof by Negation

$2^{999} + 1$

Proposition

- $2^{999} + 1$ is prime.

$2^{999} + 1$

Proposition

- $2^{999} + 1$ is prime.

Workout

- Trying out a few examples is not possible here.
- When is a number prime?

  A number that is not composite is prime.
- When is a number composite?

  A number is composite if we can factorize it.
- How do you check if a number can be factorized?

  Check whether the number satisfies an algebraic formula that can be factored.

  It seems like the given number can be represented as $a^3 + b^3$.

$2^{999} + 1$

Proposition

- $2^{999} + 1$ is prime.

Solution

- False! $2^{999} + 1$ is composite.
- $2^{999} + 1$

$$
\begin{aligned}
&= (2^{333})^3 + 1^3 && \text{(terms represented as cubes)} \\
&= a^3 + b^3 && \text{(set } a = 2^{333}\text{, } b = 1\text{)} \\
&= (a+b)(a^2 - ab + b^2) && \text{(factorize } a^3 + b^3\text{)} \\
&= (2^{333} + 1)(2^{666} - 2^{333} + 1) && \text{(substituting } a \text{ and } b \text{ values)} \\
&= \text{composite}
\end{aligned}
$$

$n^2 + 3n + 2$

Proposition

- There is a natural number n such that $n^2 + 3n + 2$ is prime.

$n^2 + 3n + 2$

Proposition

- There is a natural number n such that $n^2 + 3n + 2$ is prime.

Workout

- Write a formal statement.
  $\exists$ natural number n such that $n^2 + 3n + 2$ is prime.
- Try out a few examples.

$1^2 + 3(1) + 2 = 6$	composite
$2^2 + 3(2) + 2 = 12$	composite
$3^2 + 3(3) + 2 = 20$	composite
$4^2 + 3(4) + 2 = 30$	composite
$5^2 + 3(5) + 2 = 42$	composite

- Find a pattern.
  It seems like $n^2 + 3n + 2$ is always composite.

$n^2 + 3n + 2$

Proposition

- There is a natural number n such that $n^2 + 3n + 2$ is prime.

Solution

- False!
- Proving that the given statement is false is equivalent to proving that its negation is true.

  Negation. $\forall$ natural number n, $n^2 + 3n + 2$ is composite.
- $$\begin{aligned} & n^2 + 3n + 2 \\ &= n^2 + n + 2n + 2 && \text{(split } 3n\text{)} \\ &= n(n+1) + 2(n+1) && \text{(taking common factors)} \\ &= (n+1)(n+2) && \text{(distributive law)} \\ &= \text{composite} && (n+1 > 1 \text{ and } n+2 > 1) \end{aligned}$$

Polynomial root

Proposition

- If $x^3 - 7x^2 + x - 7 = 0$, then $x = 7$.

Polynomial root

Proposition

- If $x^3 - 7x^2 + x - 7 = 0$, then $x = 7$.

Proof

- Substitute $x = 7$ in the expression to get $7^3 - 7(7^2) + 7 - 7 = 0$. As x satisfies the equation, $x = 7$.

Polynomial root

Proposition

- If $x^3 - 7x^2 + x - 7 = 0$, then $x = 7$.

Proof

- Substitute $x = 7$ in the expression to get $7^3 - 7(7^2) + 7 - 7 = 0$. As x satisfies the equation, $x = 7$.

- Incorrect! What's wrong?

Polynomial root

Proposition

- If $x^3 - 7x^2 + x - 7 = 0$, then $x = 7$.

Polynomial root

Proposition

- If $x^3 - 7x^2 + x - 7 = 0$, then $x = 7$.

Proof

- False!
- A polynomial equation of degree n has n roots.
  So, the polynomial equation $x^3 - 7x^2 + x - 7 = 0$ has 3 roots.
- We factorize the expression.
  $$\begin{aligned} & x^3 - 7x^2 + x - 7 \\ &= x^2(x-7) + (x-7) && \text{(taking } x^2 \text{ factor from first two terms)} \\ &= (x-7)(x^2+1) && \text{(taking } (x-7) \text{ factor)} \\ &= (x-7)(x+i)(x-i) && \text{(factorizing } (x^2+1)\text{)} \\ & && \text{(this is because } (x+i)(x-i) = (x^2 - i^2) = (x^2+1)\text{)} \end{aligned}$$
  So, the three roots to the equation $x^3 - 7x^2 + x - 7 = 0$ are $x = 7$, $x = -\sqrt{-1}$, and $x = \sqrt{-1}$.

Polynomial root

Proposition

- If $x^3 - 7x^2 + x - 7 = 0$, then $x = 7$.

Proof (continued)

- Exactly one of the three roots is $x = 7$. Hence, we have

$$x = 7 \implies x^3 - 7x^2 + x - 7 = 0$$

$$x^3 - 7x^2 + x - 7 = 0 \;\not\Longrightarrow\; x = 7$$

Polynomial root

Proposition

- If x is a real number and $x^3 - 7x^2 + x - 7 = 0$, then $x = 7$.

Polynomial root

Proposition

- If x is a real number and $x^3 - 7x^2 + x - 7 = 0$, then $x = 7$.

Proof

- We factorize the expression.
  $x^3 - 7x^2 + x - 7$
  $= x^2(x-7) + (x-7)$ (taking x^2 factor from first two terms)
  $= (x-7)(x^2+1)$ (taking $(x-7)$ factor)
  $= (x-7)(x+i)(x-i)$ (factorizing (x^2+1))
  (this is because $(x+i)(x-i) = (x^2 - i^2) = (x^2+1)$)
  So, the three roots to the equation $x^3 - 7x^2 + x - 7 = 0$ are $x = 7$, $x = -\sqrt{-1}$, and $x = \sqrt{-1}$.
  As x has to be a real number, $x = 7$.

Proof by Counterexample

$a = b$

Proposition

- For all real numbers a and b, if $a^2 = b^2$, then $a = b$.

$a = b$

Proposition

- For all real numbers a and b, if $a^2 = b^2$, then $a = b$.

Solution

- False! Counterexample: $a = 1$ and $b = -1$.
  In this example, $a^2 = b^2$ but $a \neq b$.

$a = b$

Proposition

- For all real numbers a and b, if $a^2 = b^2$, then $a = b$.

Solution

- False! Counterexample: $a = 1$ and $b = -1$.
  In this example, $a^2 = b^2$ but $a \neq b$.

Proposition

- For all nonzero integers a and b, if $a|b$ and $b|a$, then $a = b$.

$a = b$

Proposition

- For all real numbers a and b, if $a^2 = b^2$, then $a = b$.

Solution

- False! Counterexample: $a = 1$ and $b = -1$.
  In this example, $a^2 = b^2$ but $a \neq b$.

Proposition

- For all nonzero integers a and b, if $a|b$ and $b|a$, then $a = b$.

Solution

- False! Counterexample: $a = 1$ and $b = -1$.
  In this example, $a|b$ and $b|a$, however, $a \neq b$.

$2^n + 1$

Proposition

- $2^n + 1$ is prime for any natural number n.

$2^n + 1$

Proposition

- $2^n + 1$ is prime for any natural number n.

Workout

- Write a formal statement.
  $\forall$ natural number n, $2^n + 1$ is prime.
- Try out a few examples.

$2^1 + 1 = 3$	prime
$2^2 + 1 = 5$	prime
$2^3 + 1 = 9 = 3^2$	composite

- Find a pattern.
  $2^n + 1$ can be either prime or composite.

$2^n + 1$

Proposition

- $2^n + 1$ is prime for any natural number n.

Workout

- Write a formal statement.
  $\forall$ natural number n, $2^n + 1$ is prime.
- Try out a few examples.

$$2^1 + 1 = 3 \qquad \text{prime}$$
$$2^2 + 1 = 5 \qquad \text{prime}$$
$$2^3 + 1 = 9 = 3^2 \qquad \text{composite}$$

- Find a pattern.
  $2^n + 1$ can be either prime or composite.

Solution

- False! Counterexample: $n = 3$
  When $n = 3$, then $2^n + 1 = 2^3 + 1 = 9 = 3^2$ is composite.

$n^2 + n + 41$

Proposition

- $n^2 + n + 41$ is prime for any whole number n.

$n^2 + n + 41$

Proposition

- $n^2 + n + 41$ is prime for any whole number n.

Workout

- Write a formal statement.
  $\forall$ whole number n, $n^2 + n + 41$ is prime.
- Try out a few examples.

$0^2 + 0 + 41 = 41$	prime
$1^2 + 1 + 41 = 43$	prime
$2^2 + 2 + 41 = 47$	prime
$3^2 + 3 + 41 = 53$	prime
$4^2 + 4 + 41 = 61$	prime
$5^2 + 5 + 41 = 71$	prime

- Find a pattern.
  It seems like $n^2 + n + 41$ is always prime.

$n^2 + n + 41$

Proposition

- $n^2 + n + 41$ is prime for any whole number n.

$n^2 + n + 41$

Proposition

- $n^2 + n + 41$ is prime for any whole number n.

Solution

- False!
- Formal statement. $\forall$ whole numbers n, $n^2 + n + 41$ is prime.
- Counterexample: 41.
  $(41^2 + 41 + 41 = 41(41 + 1 + 1) = 41 \times 43)$
- Another counterexample: 40.
  $(40^2+40+41 = 40(40+1)+41 = 40\times 41+41 = 41(40+1) = 41 \times 41)$

$x/(y+z)+y/(x+z)+z/(x+y)$

Proposition

- $\frac{x}{y+z}+\frac{y}{x+z}+\frac{z}{x+y}=4$ has no positive integer solutions.

$x/(y+z)+y/(x+z)+z/(x+y)$

Proposition

- $\frac{x}{y+z}+\frac{y}{x+z}+\frac{z}{x+y}=4$ has no positive integer solutions.

Workout

- Write a formal statement.
  $\forall\ x,y,z\in\mathbb{N},\ x/(y+z)+y/(x+z)+z/(x+y)\neq 4.$
- Try out a few examples.

(x,y,z)	$x/(y+z)+y/(x+z)+z/(x+y)=4$?
$(1,1,1)$	$1/2+1/2+1/2=1.5\neq 4$
$(1,2,1)$	$1/3+2/2+1/3=1.666\cdots\neq 4$
$(1,2,3)$	$1/5+2/4+3/3=1.7\neq 4$
$(1,10,100)$	$1/110+10/101+100/11=9.199\cdots\neq 4$

- Find a pattern.
  It seems like there are no $+$ve integers satisfying the property.

$x/(y+z) + y/(x+z) + z/(x+y)$

Proposition

- $\frac{x}{y+z} + \frac{y}{x+z} + \frac{z}{x+y} = 4$ has no positive integer solutions.

Solution

- False!
- Counterexample:

$$\begin{aligned}
x = {} & 154476802108746166441951315019919837485664325669 \\
& 565431700026634898253202035277999 \\
y = {} & 368751317941299998271978115652254748254929799689 \\
& 71970996283137471637224634055579 \\
z = {} & 373612677928697257861252602371390152816537558161 \\
& 613618621437993378423467772036
\end{aligned}$$

12111111111111111111111111111111111111111111

Proposition

- For whole numbers n, $12\underbrace{11\cdots1}_{n\text{ terms}}$ is composite.

12111111111111111111111111111111111111111

Proposition

- For whole numbers n, $12\underbrace{11\cdots1}_{n\text{ terms}}$ is composite.

Workout

- Try out a few examples.

(n, Number)	Factorization
$(0, 12)$	3×4
$(1, 121)$	11×11
$(2, 1211)$	7×173
$(3, 12111)$	33×367
$(4, 121111)$	281×431
$(5, 1211111)$	253×4787

- Find a pattern.
  It seems like the sequence of numbers is composite.

121111111111111111111111111111111111111111

Proposition

- For whole numbers $n \geq 0$, $12\underbrace{11\cdots1}_{n \text{ terms}}$ is composite.

Solution

- False!
- Smallest counterexample: $n = 136$.

$$\begin{aligned}12{,}&1111111111, 1111111111, 1111111111, 1111111111,\\ &1111111111, 1111111111, 1111111111, 1111111111,\\ &1111111111, 1111111111, 1111111111, 1111111111,\\ &1111111111, 111111 \text{ is prime.}\end{aligned}$$

Proof by Contraposition

n^2 is odd $\Rightarrow$ n is odd

Proposition

- If n^2 is odd, then n is odd.

n^2 is odd $\Rightarrow$ n is odd

Proposition

- If n^2 is odd, then n is odd.

Proof

- Seems very difficult to prove directly.
  Contraposition: If n is even, then n^2 is even.
  n is even
  $\Longrightarrow$ $n = 2k$ (defn. of even, k is an integer)
  $\Longrightarrow$ $n^2 = (2k)^2$ (squaring on both sides)
  $\Longrightarrow$ $n^2 = 4k^2$ (simplifying)
  $\Longrightarrow$ $n^2 = 2(2k^2)$ (factoring 2)
  $\Longrightarrow$ $n^2 = 2j$ (let $j = 2k^2$)
  (j is an integer as mult. is closed on integers)
  $\Longrightarrow$ n^2 is even (defn. of even)

n is odd $\Leftrightarrow$ n^2 is odd

Proposition

- The square of an integer is odd if and only if the integer itself is odd.

n is odd $\Leftrightarrow$ n^2 is odd

Proposition

- The square of an integer is odd if and only if the integer itself is odd.

Workout

- Write a formal statement.
  $\forall$ integer n, n^2 is odd $\Leftrightarrow$ n is odd.
- Try out a few examples.

Odd numbers	Even numbers
$(1, 1)$	$(0, 0)$
$(3, 9)$	$(2, 4)$
$(5, 25)$	$(4, 16)$
$(7, 49)$	$(6, 36)$

- Pattern. It seems that the proposition is true.

n is odd $\Leftrightarrow$ n^2 is odd

Proposition

- The square of an integer is odd if and only if the integer itself is odd.

Proof

There are two parts in the proof.

1. Prove that if n is odd, then n^2 is odd.
   Direct proof
2. Prove that if n^2 is odd, then n is odd.
   Proof by contraposition

n is odd $\Leftrightarrow n^2$ is odd

Corollary

- Prove that the fourth power of an integer is odd if and only if the integer itself is odd.

n is odd $\Leftrightarrow n^2$ is odd

Corollary

- Prove that the fourth power of an integer is odd if and only if the integer itself is odd.

Proof

- We have

$$\begin{aligned} & n \text{ is odd} \Leftrightarrow n^2 \text{ is odd} && \text{(previous theorem)} \\ \Longrightarrow\ & n^2 \text{ is odd} \Leftrightarrow n^4 \text{ is odd} && \text{(previous theorem used on } n^2\text{)} \\ \Longrightarrow\ & n \text{ is odd} \Leftrightarrow n^4 \text{ is odd} && \text{(transitivity of biconditional)} \end{aligned}$$

n is odd $\Leftrightarrow n^2$ is odd

Corollary

- Prove that the fourth power of an integer is odd if and only if the integer itself is odd.

Proof

- We have

  n is odd $\Leftrightarrow n^2$ is odd (previous theorem)

  $\implies n^2$ is odd $\Leftrightarrow n^4$ is odd (previous theorem used on n^2)

  $\implies n$ is odd $\Leftrightarrow n^4$ is odd (transitivity of biconditional)

Problem

- Suppose k is a whole number. Prove that an integer n is odd if and only if n^{2^k} is odd.

n^2 is even $\implies$ n is even

Proposition

- For all integers n, if n^2 is even, then n is even.

n^2 is even $\implies$ n is even

Proposition

- For all integers n, if n^2 is even, then n is even.

Proof

- Contrapositive. For all integers, if n is odd, then n^2 is odd.
- $n = 2k + 1$ (definition of odd number)

  $\implies n^2 = (2k+1)^2$ (squaring both sides)

  $\implies n^2 = 4k^2 + 4k + 1$ (expand)

  $\implies n^2 = 2(2k^2 + 2k) + 1$ (taking 2 out from two terms)

  $\implies n^2 = 2m + 1$ (set $m = 2k^2 + 2k$)

  (m is an integer as multiplication is closed on integers)

  $\implies n^2 =$ odd (definition of odd number)
- Hence, the proposition is true.

Polynomial root

Proposition

- If $x^3 - 7x^2 + x - 7 = 0$, then $x \neq 10$.

Polynomial root

Proposition

- If $x^3 - 7x^2 + x - 7 = 0$, then $x \neq 10$.

Proof

- Contrapositive. If $x = 10$, then $x^3 - 7x^2 + x - 7 \neq 0$
  Substitute $x = 10$ in the expression.
  We get $10^3 - 7(10^2) + 10 - 7 = 1000 - 700 + 10 - 7 = 303 \neq 0$.
  That is, $x = 10$ does not satisfy $x^3 - 7x^2 + x - 7 = 0$ equation.
  Hence, the contraposition is correct which implies that the original statement is correct.

$n \nmid ab \implies n \nmid a$ **and** $n \nmid b$

Proposition

- Let $a, b, n \in \mathbb{Z}$. If $n \nmid ab$, then $n \nmid a$ and $n \nmid b$.

$n \nmid ab \implies n \nmid a$ **and** $n \nmid b$

Proposition

- Let $a, b, n \in \mathbb{Z}$. If $n \nmid ab$, then $n \nmid a$ and $n \nmid b$.

Proof

- Contrapositive. Let $a, b, n \in \mathbb{Z}$. If $n|a$ or $n|b$, then $n|ab$.
- $n|a$

  $$\begin{aligned} &\implies a = nc && \text{(for some } c \in \mathbb{Z}\text{)} \\ &\implies ab = (nc)b = n(cb) && \text{(multiply by } b\text{)} \\ &\implies n|ab && \text{(definition of divisibility)} \end{aligned}$$

- $n|b$

  $$\begin{aligned} &\implies b = nd && \text{(for some } d \in \mathbb{Z}\text{)} \\ &\implies ab = a(nd) = n(ad) && \text{(multiply by } a\text{)} \\ &\implies n|ab && \text{(definition of divisibility)} \end{aligned}$$

- Hence, the proposition is true.

$n^2 - 6n + 5$ **is even** $\implies$ n **is odd**

Proposition

- Let $n \in \mathbb{Z}$. If $n^2 - 6n + 5$ is even, then n is odd.

$n^2 - 6n + 5$ is even $\implies$ n is odd

Proposition

- Let $n \in \mathbb{Z}$. If $n^2 - 6n + 5$ is even, then n is odd.

Proof

- Contrapositive. If n is even, then $n^2 - 6n + 5$ is odd.
- n is even

  $\implies$ $n = 2a$ for some integer a (defn. of even)

  $\implies$ $n^2 - 6n + 5 = (2a)^2 - 6(2a) + 5$ (substitute $n = 2a$)

  $\implies$ $n^2 - 6n + 5 = 2(2a^2) - 2(6a) + 2(2) + 1$ (simplify)

  $\implies$ $n^2 - 6n + 5 = 2(2a^2 - 6a + 2) + 1$ (take 2 common)

  $\implies$ $n^2 - 6n + 5$ is odd (defn. of odd)
- Hence, the proposition is true.

$xy > 9 \implies x > 3$ **or** $y > 3$

Proposition

- For reals x and y, if $xy > 9$, then either $x > 3$ or $y > 3$.

$xy > 9 \implies x > 3$ **or** $y > 3$

Proposition

- For reals x and y, if $xy > 9$, then either $x > 3$ or $y > 3$.

Proof

- Contrapositive. If $x \leq 3$ and $y \leq 3$, then $xy \leq 9$.
- Suppose $x \leq 3$ and $y \leq 3$.
  $\implies xy \leq 9$ (multiply the two inequalities)
- Hence, the proposition is true.

$xy > 9 \implies x > 3$ **or** $y > 3$

Proposition

- For reals x and y, if $xy > 9$, then either $x > 3$ or $y > 3$.

Proof

- Contrapositive. If $x \leq 3$ and $y \leq 3$, then $xy \leq 9$.
- Suppose $x \leq 3$ and $y \leq 3$.
  $\implies xy \leq 9$ (multiply the two inequalities)
- Hence, the proposition is true.

- Incorrect! Why?

Nonconstructive Proof

$\text{Irrational}^{\text{irrational}}$ can be rational

Proposition

- An irrational raised to an irrational power may be rational.

Irrational$^{\text{irrational}}$ can be rational

Proposition

- An irrational raised to an irrational power may be rational.

Proof

- We make use of the fact that $\sqrt{2}$ is irrational.

  Let $x = \sqrt{2}^{\sqrt{2}}$. Number x is either rational or irrational.

  Case 1. If x is rational, then the proposition is true.

Irrational	Irrational	Rational
$\sqrt{2}$	$\sqrt{2}$	$\sqrt{2}^{\sqrt{2}} = x =$ rational

  Case 2. If x is irrational, then the proposition is true.

Irrational	Irrational	Rational
x	$\sqrt{2}$	$x^{\sqrt{2}} = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^{2} = 2$

Proof by Contradiction

n^2 is even $\implies$ n is even

Proposition

- For all integers n, if n^2 is even, then n is even.

n^2 is even $\implies$ n is even

Proposition

- For all integers n, if n^2 is even, then n is even.

Proof

- Negation. Suppose there is an integer n such that n^2 is even but n is odd.
- $n = 2k + 1$ (definition of odd number)

  $\implies n^2 = (2k+1)^2$ (squaring both sides)

  $\implies n^2 = 4k^2 + 4k + 1$ (expand)

  $\implies n^2 = 2(2k^2 + 2k) + 1$ (taking 2 out from two terms)

  $\implies n^2 = 2m + 1$ (set $m = 2k^2 + 2k$)

  (m is an integer as multiplication is closed on integers)

  $\implies n^2 =$ odd (definition of odd number)
- Contradiction! Hence, the proposition is true.

Greatest integer

Proposition

- There is no greatest integer.

Greatest integer

Proposition

- There is no greatest integer.

Proof

- Negation. Suppose there is a greatest integer N.
  Then $N \geq n$ for every integer n.
  Let $M = N + 1$.
  M is an integer since addition is closed on integers.
  $M > N$ since $M = N + 1$.
  M is an integer that is greater than N.
  So, N is not the greatest integer.
  Contradiction! Hence, the proposition is true.

$\sqrt{2}$ is irrational

Proposition

- $\sqrt{2}$ is irrational.

$\sqrt{2}$ is irrational

Proposition

- $\sqrt{2}$ is irrational.

Proof

- Suppose $\sqrt{2}$ is the simplest rational.

$\implies \sqrt{2} = m/n$ (m, n have no common factors, $n \neq 0$)

$\implies m^2 = 2n^2$ (squaring and simplifying)

$\implies m^2 =$ even (definition of even)

$\implies m =$ even (why?)

$\implies m = 2k$ for some integer k (definition of even)

$\implies (2k)^2 = 2n^2$ (substitute m)

$\implies n^2 = 2k^2$ (simplify)

$\implies n^2 =$ even (definition of even)

$\implies n =$ even (why?)

$\implies m, n$ are even (previous results)

$\implies m, n$ have a common factor of 2 (definition of even)

- Contradiction! Hence, the proposition is true.

If $p|n$, then $p \nmid (n+1)$.

Proposition

- For any integer n and any prime p, if $p|n$, then $p \nmid (n+1)$.

If $p|n$, then $p \nmid (n+1)$.

Proposition

- For any integer n and any prime p, if $p|n$, then $p \nmid (n+1)$.

Proof

- Negation. Suppose there exists integer n and prime p such that $p|n$ and $p|(n+1)$.
  $p|n$ implies $pr = n$ for some integer r
  $p|(n+1)$ implies $ps = n+1$ for some integer s
  Eliminate n to get:
  $1 = (n+1) - n = ps - pr = p(s-r)$
  Hence, $p|1$, from the definition of divisibility.
  As $p|1$, we have $p \leq 1$. (why?)
  As p is prime, $p > 1$.
  Contradiction! Hence, the proposition is true.

#Primes is infinite

Proposition

- The set of prime numbers is infinite.

#Primes is infinite

Proposition

- The set of prime numbers is infinite.

Proof

- Negation. Assume that there are only finite number of primes.
  Let the set of primes be $\{p_1, p_2, \ldots, p_n\}$
  such that $(p_1 = 2) < (p_2 = 3) < \cdots < p_n$.
  Consider the number $N = p_1 p_2 p_3 \ldots p_n + 1$. Clearly, $N > 1$.

#Primes is infinite

Proposition

- The set of prime numbers is infinite.

Proof

- Negation. Assume that there are only finite number of primes.
  Let the set of primes be $\{p_1, p_2, \ldots, p_n\}$
  such that $(p_1 = 2) < (p_2 = 3) < \cdots < p_n$.
  Consider the number $N = p_1 p_2 p_3 \ldots p_n + 1$. Clearly, $N > 1$.
  (i) There is a prime that divides N.
  Use unique prime factorization theorem.

#Primes is infinite

Proposition

- The set of prime numbers is infinite.

Proof

- Negation. Assume that there are only finite number of primes.
  Let the set of primes be $\{p_1, p_2, \ldots, p_n\}$
  such that $(p_1 = 2) < (p_2 = 3) < \cdots < p_n$.
  Consider the number $N = p_1 p_2 p_3 \ldots p_n + 1$. Clearly, $N > 1$.
  (i) There is a prime that divides N.
  Use unique prime factorization theorem.
  (ii) No prime divides N.
  For all $i \in [1, n]$, p_i does not divide N as it leaves a remainder of 1 when it divides N.
  So, $p_1 \not| N$, $p_2 \not| N$, $\ldots$, $p_n \not| N$.
  Contradiction! Hence, the proposition is true.

Average

Proposition

- If $a_1, a_2, \ldots, a_n$ are n real numbers for natural number n, then at least one of these n numbers is greater than or equal to the average of those n numbers.

Average

Proposition

- If $a_1, a_2, \ldots, a_n$ are n real numbers for natural number n, then at least one of these n numbers is greater than or equal to the average of those n numbers.

Proof

- Average $A = (a_1 + a_2 + \cdots + a_n)/n$
- Negation. $\forall i \in \{1, 2, \ldots, n\}\ a_i < A$. That is
- We have $a_1 < A$, $a_2 < A$, …, $a_n < A$

Average

Proposition

- If $a_1, a_2, \ldots, a_n$ are n real numbers for natural number n, then at least one of these n numbers is greater than or equal to the average of those n numbers.

Proof

- Average $A = (a_1 + a_2 + \cdots + a_n)/n$
- Negation. $\forall i \in \{1, 2, \ldots, n\}\ a_i < A$. That is
- We have $a_1 < A$, $a_2 < A$, ..., $a_n < A$
  Now add all these inequalities to get
  $(a_1 + a_2 + \cdots + a_n) < n \times A$
  $\implies A > (a_1 + a_2 + \cdots + a_n)/n$ on simplification
  How is it possible that A is both equal to and greater than $(a_1 + a_2 + \cdots + a_n)/n$
- Contradiction! Hence, the proposition is true.

Average

Proposition

- If $a_1, a_2, \ldots, a_n$ are n real numbers for natural number n, then at least one of these n numbers is greater than or equal to the average of those n numbers.

Average

Proposition

- If $a_1, a_2, \ldots, a_n$ are n real numbers for natural number n, then at least one of these n numbers is greater than or equal to the average of those n numbers.

Proof

- Let $a_{\textsf{max}}$ represent the maximum among the n real numbers.
- Let average $A = (a_1 + a_2 + \cdots + a_n)/n$. Then

Average

Proposition

- If $a_1, a_2, \ldots, a_n$ are n real numbers for natural number n, then at least one of these n numbers is greater than or equal to the average of those n numbers.

Proof

- Let $a_{\textsf{max}}$ represent the maximum among the n real numbers.
- Let average $A = (a_1 + a_2 + \cdots + a_n)/n$. Then
- $a_1 = a_{\textsf{max}} - b_1$ such that $b_1 \geq 0$
  $a_2 = a_{\textsf{max}} - b_2$ such that $b_2 \geq 0$
  $\ldots$
  $a_n = a_{\textsf{max}} - b_n$ such that $b_n \geq 0$

Average

Proposition

- If $a_1, a_2, \ldots, a_n$ are n real numbers for natural number n, then at least one of these n numbers is greater than or equal to the average of those n numbers.

Proof

- Let a_{max} represent the maximum among the n real numbers.
- Let average $A = (a_1 + a_2 + \cdots + a_n)/n$. Then
- $a_1 = a_{\text{max}} - b_1$ such that $b_1 \geq 0$

  $a_2 = a_{\text{max}} - b_2$ such that $b_2 \geq 0$

  $\ldots$

  $a_n = a_{\text{max}} - b_n$ such that $b_n \geq 0$

  Adding the above equations, we get

  $(a_1 + a_2 + \cdots + a_n) = n \times a_{\text{max}} - (b_1 + b_2 + \cdots + b_n)$

  $\implies a_{\text{max}} = [(a_1 + a_2 + \cdots + a_n) + (b_1 + b_2 + \cdots + b_n)]/n$

  $= ((a_1 + a_2 + \cdots + a_n)/n) + ((b_1 + b_2 + \cdots + b_n)/n)$

  $= A + ((b_1 + b_2 + \cdots + b_n)/n)$

  $\geq A \qquad (\forall i, b_i \geq 0)$

$2^p - 1$ is prime $\implies$ p is prime

Proposition

- Suppose $p \in \mathbb{N}$ and $p \geq 2$. If $2^p - 1$ is prime, then p is prime.

$2^p - 1$ is prime $\implies$ p is prime

Proposition

- Suppose $p \in \mathbb{N}$ and $p \geq 2$. If $2^p - 1$ is prime, then p is prime.

Proof

- Negation. Suppose p is an integer at least 2 such that $2^p - 1$ is prime and p is composite.

$2^p - 1$ is prime $\implies$ p is prime

Proposition

- Suppose $p \in \mathbb{N}$ and $p \geq 2$. If $2^p - 1$ is prime, then p is prime.

Proof

- Negation. Suppose p is an integer at least 2 such that $2^p - 1$ is prime and p is composite.
- p is composite

  $\implies$ $p = rs$ such that both r, s are in the range $[2, p-1]$

  Then, $2^p - 1$

  $= 2^{rs} - 1$ (substitute for p)

  $= (2^r)^s - 1$ $(a^{bc} = (a^b)^c)$

  $= (2^r - 1)\left(\frac{(2^r)^s - 1}{2^r - 1}\right)$ (multiply and divide by $(2^r - 1) > 0$)

  $= (2^r - 1)\left(1 + (2^r)^1 + (2^r)^2 + \cdots + (2^r)^{s-1}\right)$

  $= m \times n$ $(m \geq 2$ and $n \geq 2)$
- Contradiction! Hence, the proposition is true.

Pythagorean triplets

Proposition

- For integers a, b, c, if $a^2 + b^2 = c^2$, then a is even or b is even.

Pythagorean triplets

Proposition

- For integers a, b, c, if $a^2 + b^2 = c^2$, then a is even or b is even.

Proof

- Negation. a and b are odd and $a^2 + b^2 = c^2$.

Pythagorean triplets

Proposition

- For integers a, b, c, if $a^2 + b^2 = c^2$, then a is even or b is even.

Proof

- Negation. a and b are odd and $a^2 + b^2 = c^2$.
- $a = 2m + 1$; $b = 2n + 1$ (definition of odd)

  Consider $a^2 + b^2$

  $= (2m+1)^2 + (2n+1)^2$

  $= 4m^2 + 4n^2 + 4m + 4n + 2$ (expand)

  $= 4 \times (m^2 + n^2 + m + n) + 2$ (take common factor)

  $\equiv 2 \bmod 4$ (remainder is 2 when divided by 4)

Pythagorean triplets

Proposition

- For integers a, b, c, if $a^2 + b^2 = c^2$, then a is even or b is even.

Proof

- Negation. a and b are odd and $a^2 + b^2 = c^2$.
- $a = 2m + 1$; $b = 2n + 1$ (definition of odd)

  Consider $a^2 + b^2$

  $= (2m + 1)^2 + (2n + 1)^2$

  $= 4m^2 + 4n^2 + 4m + 4n + 2$ (expand)

  $= 4 \times (m^2 + n^2 + m + n) + 2$ (take common factor)

  $\equiv 2 \bmod 4$ (remainder is 2 when divided by 4)
- $c = 2k$ or $c = 2k + 1$ (quotient-remainder theorem)

  Consider c^2

  $= 4k^2$ or $4(k^2 + k) + 1$ (squaring)

  $\not\equiv 2 \bmod 4$ (remainder is never 2 when divided by 4)
- Contradiction! Hence, the proposition is true.

Proof by Division into Cases

$n^2 + 3n + 2$

Proposition

- There is a natural number n such that $n^2 + 3n + 2$ is prime.

Proof 2

- False!
- Negation. $\forall$ natural number n, $n^2 + 3n + 2$ is composite.
  We prove the negation in two cases:
  1. n is even
  2. n is odd

$n^2 + 3n + 2$

Proof 2 (continued)

1. Prove that n is even $\implies n^2 + 3n + 2$ is composite.

   n is even

   $\implies n^2$ is even and $3n$ is even (even × integer = even)

   $\implies n^2 + 3n + 2$ is even (even + even = even)

   $\implies n^2 + 3n + 2$ is composite (2 is a factor)

2. Prove that n is odd $\implies n^2 + 3n + 2$ is composite.

   n is odd

   $\implies n^2$ is odd and $3n$ is odd (odd × odd = odd)

   $\implies n^2 + 3n$ is even (odd + odd = even)

   $\implies n^2 + 3n + 2$ is even (even + even = even)

   $\implies n^2 + 3n + 2$ is composite (2 is a factor)

$n^2 + 3n + 2$

Proof 2 (continued)

1. Prove that n is even $\implies$ $n^2 + 3n + 2$ is composite.

   n is even

   $\implies$ n^2 is even and $3n$ is even (even × integer = even)

   $\implies$ $n^2 + 3n + 2$ is even (even + even = even)

   $\implies$ $n^2 + 3n + 2$ is composite (2 is a factor)

2. Prove that n is odd $\implies$ $n^2 + 3n + 2$ is composite.

   n is odd

   $\implies$ n^2 is odd and $3n$ is odd (odd × odd = odd)

   $\implies$ $n^2 + 3n$ is even (odd + odd = even)

   $\implies$ $n^2 + 3n + 2$ is even (even + even = even)

   $\implies$ $n^2 + 3n + 2$ is composite (2 is a factor)

Proposition

- Use this approach to prove that for all natural number n, $9n^4 - 7n^3 + 5n^2 - 3n + 10$ is composite.

Odd$^2 = 8m + 1$

Proposition

- The square of any odd integer has the form $8m + 1$ for some integer m.

Odd$^2 = 8m + 1$

Proposition

- The square of any odd integer has the form $8m + 1$ for some integer m.

Proof

- n is odd
  $\Longrightarrow\ n = 4q$ or $n = 4q + 1$ or $n = 4q + 2$ or $n = 4q + 3$
  (n can be written in one of the four forms using the quotient-remainder theorem)
  But, $n \neq 4q$ and $n \neq 4q + 2$ (as $4q$ and $4q + 2$ are even)
  Hence, $n = 4q + 1$ or $n = 4q + 3$.
- Case 1. $n = 4q + 1$.
  $\Longrightarrow\ n^2 = (4q + 1)^2 = 8(2q^2 + q) + 1 = 8m + 1,$
  where $m = 2q^2 + q =$ integer.
- Case 2. $n = 4q + 3$.
  $\Longrightarrow\ n^2 = (4q + 3)^2 = 8(2q^2 + 3q + 1) + 1 = 8m + 1,$
  where $m = 2q^2 + 3q + 1 =$ integer.

$(x^2 - y^2) \bmod 4 \neq 2$

Proposition

- There is no solution in integers to: $(x^2 - y^2) \bmod 4 = 2$.

$(x^2 - y^2) \bmod 4 \neq 2$

Proposition

- There is no solution in integers to: $(x^2 - y^2) \bmod 4 = 2$.

Proof

- Case 1. x is even and y is even.
  $\implies x^2 = 4m$ and $y^2 = 4n$
  $\implies x^2 - y^2 = 4(m - n)$.
- Case 2. x is even and y is odd.
  $\implies x^2 = 4m$ and $y^2 = 4n + 1$
  $\implies x^2 - y^2 = 4(m - n) - 1$.
- Case 3. x is odd and y is even.
  $\implies x^2 = 4m + 1$ and $y^2 = 4n$
  $\implies x^2 - y^2 = 4(m - n) + 1$.
- Case 4. x is odd and y is odd.
  $\implies x^2 = 4m + 1$ and $y^2 = 4n + 1$
  $\implies x^2 - y^2 = 4(m - n)$.
- In all these four cases, $(x^2 - y^2) \bmod 4 \neq 2$.

Problems for practice

Prove or disprove the following propositions:

- If more than n pigeons fly into n pigeon holes for natural number n, then at least one pigeon hole will contain at least two pigeons. [Hint: Contradiction.]
- $1/\sqrt{2}$ is irrational. [Hint: Contradiction.]
- $\sqrt{3}$ is irrational. [Hint: Contradiction.]
- $\sqrt{6}$ is irrational. [Hint: Contradiction.]
- $\log_2 3$ is irrational. [Hint: Contradiction.]
- $\log_2 7$ is irrational. [Hint: Contradiction.]
- For all integers a and b, if ab is a multiple of 6, then a is even and b is a multiple of 3. [Hint: Counterexample.]
- There are no integers a and b such that $752b = 4183 - 326a$. [Hint: Contradiction.]
- $a^n + b^n = c^n$ has no integral solutions for all natural numbers $n \geq 1$. [Hint: Counterexample.]
- Suppose $p \in \mathbb{N}$ and $p \geq 2$. If $2^p - 1$ is prime, then p is prime. [Hint: Contraposition.]

Problems for practice

Prove or disprove the following propositions:

- For integers a, b, c, if $a^2 + b^2 = c^2$, then a is even or b is even. [Hint: Contraposition + division into cases.]
- There are 1000 consecutive natural numbers that are not perfect squares. [Hint: Direct proof.]
- Consider any ten prime numbers that are greater than or equal to 15. Then the sum of these prime numbers can never be (1 trillion + 1). [Hint: Direct proof, contradiction.]
- Let n be a positive integer. Prove that the closed interval $[n, 2n]$ contains a power of 2. [Hint: Division into cases (power of 2 and not a power of 2).]

Problems for practice

Prove or disprove the following propositions:

- Rational + rational = rational. [Hint: Direct proof.]
- Rational + irrational = irrational. [Hint: Contradiction.]
- Irrational + irrational = rational or irrational. [Hint: Examples. $\sqrt{2} + (-\sqrt{2}) = 0$ and $\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} = \sqrt{2}$.]
- Rational × rational = rational. [Hint: Direct proof.]
- Rational × irrational = rational or irrational. [Hint: Examples $0 \times \sqrt{2} = 0$ and $1 \times \sqrt{2} = \sqrt{2}$.]
- Nonzero rational × irrational = irrational. [Hint: Contradiction.]
- Irrational × irrational = rational or irrational. [Hint: Examples $\sqrt{2} \times \sqrt{2} = 2$ and $\sqrt{2} \times \sqrt{2} = \sqrt{6}$.]
- $\text{Rational}^{\text{rational}}$ = rational or irrational. [Hint: Examples $1^1 = 1$ and $2^{1/2} = \sqrt{2}$.]

Bogus Proofs

Prove 1 = 2 using basic algebra

Proof

- $a > 0, b > 0$ ▷ Given
- $a = b$ ▷ Given
- $ab = b^2$ ▷ Multiply both sides by b
- $ab - a^2 = b^2 - a^2$ ▷ Subtract a^2 from both sides
- $a(b - a) = (b + a)(b - a)$ ▷ Factoring
- $a = b + a$ ▷ Divide both sides by $(b - a)$
- $0 = b$ ▷ Subtract a from both sides
- $b = 2b$ ▷ Add b to both sides
- $1 = 2$ ▷ Divide both sides by b
- What is the problem with this proof?

Prove 1 = 2 using basic algebra

Proof

- $a > 0, b > 0$ $\triangleright$ Given
- $a = b$ $\triangleright$ Given
- $ab = b^2$ $\triangleright$ Multiply both sides by b
- $ab - a^2 = b^2 - a^2$ $\triangleright$ Subtract a^2 from both sides
- $a(b - a) = (b + a)(b - a)$ $\triangleright$ Factoring
- $a = b + a$ $\triangleright$ Divide both sides by $(b - a)$
- $0 = b$ $\triangleright$ Subtract a from both sides
- $b = 2b$ $\triangleright$ Add b to both sides
- $1 = 2$ $\triangleright$ Divide both sides by b
- What is the problem with this proof?

Error

- Cannot divide by 0 in mathematics
- Cannot divide by $(b - a)$ as $a = b$

Prove 1 = 2 using basic algebra

Proof

- $n^2 + 2n + 1 = (n+1)^2$ ▷ Expand
- $n^2 = (n+1)^2 - (2n+1)$ ▷ Subtract
- $n^2 - n(2n+1) = (n+1)^2 - (2n+1) - n(2n+1)$ ▷ Subtract
- $n^2 - n(2n+1) = (n+1)^2 - (n+1)(2n+1)$ ▷ Factoring
- $n^2 - n(2n+1) + (2n+1)^2/4 =$
  $(n+1)^2 - (n+1)(2n+1) + (2n+1)^2/4$ ▷ Add
- $(n - (2n+1)/2)^2 = ((n+1) - (2n+1)/2)^2$ ▷ Simplify
- $n - (2n+1)/2 = (n+1) - (2n+1)/2$ ▷ Square roots
- $n = n + 1$ ▷ Add
- $1 = 2$ ▷ Subtract
- What is the problem with this proof?

Prove $1 = 2$ using basic algebra

Proof

- $n^2 + 2n + 1 = (n+1)^2$ ▷ Expand
- $n^2 = (n+1)^2 - (2n+1)$ ▷ Subtract
- $n^2 - n(2n+1) = (n+1)^2 - (2n+1) - n(2n+1)$ ▷ Subtract
- $n^2 - n(2n+1) = (n+1)^2 - (n+1)(2n+1)$ ▷ Factoring
- $n^2 - n(2n+1) + (2n+1)^2/4 =$
  $(n+1)^2 - (n+1)(2n+1) + (2n+1)^2/4$ ▷ Add
- $(n - (2n+1)/2)^2 = ((n+1) - (2n+1)/2)^2$ ▷ Simplify
- $n - (2n+1)/2 = (n+1) - (2n+1)/2$ ▷ Square roots
- $n = n + 1$ ▷ Add
- $1 = 2$ ▷ Subtract
- What is the problem with this proof?

Error

- Cannot take square roots directly
- $a^2 = b^2$ does not imply $a = b$
  E.g.: $1^2 = (-1)^2$ does not imply $1 = -1$

Prove 1 = 2 using calculus

Proof

- $\int u \mathrm{d}v = uv - \int v \mathrm{d}u$ ▷ Product rule
- Set $u = \frac{1}{x}$ and $v = x$; We get $\mathrm{d}u = -\frac{1}{x^2}\mathrm{d}x$ and $\mathrm{d}v = \mathrm{d}x$
- $\int \frac{1}{x}\mathrm{d}x = x \cdot \frac{1}{x} - \int x \cdot \left(-\frac{1}{x^2}\right) \mathrm{d}x$ ▷ Substitute
- $\int \frac{1}{x}\mathrm{d}x = 1 + \int \frac{1}{x}\mathrm{d}x$ ▷ Simplify
- $0 = 1$ ▷ Subtract
- $1 = 2$ ▷ Add
- What is the problem with this proof?

Prove 1 = 2 using calculus

Proof

- $\int u \mathrm{d}v = uv - \int v \mathrm{d}u$ ▷ Product rule
- Set $u = \frac{1}{x}$ and $v = x$; We get $\mathrm{d}u = -\frac{1}{x^2}\mathrm{d}x$ and $\mathrm{d}v = \mathrm{d}x$
- $\int \frac{1}{x}\mathrm{d}x = x \cdot \frac{1}{x} - \int x \cdot \left(-\frac{1}{x^2}\right)\mathrm{d}x$ ▷ Substitute
- $\int \frac{1}{x}\mathrm{d}x = 1 + \int \frac{1}{x}\mathrm{d}x$ ▷ Simplify
- $0 = 1$ ▷ Subtract
- $1 = 2$ ▷ Add
- What is the problem with this proof?

Error

- Cannot subtract integrals from both sides
- $\int \mathrm{d}x = x +$ const. ▷ const. depends on conditions

  E.g.: $\frac{\mathrm{d}}{\mathrm{d}x}(x+1) = \frac{\mathrm{d}}{\mathrm{d}x}(x+2)$ does not imply

  $\int \frac{\mathrm{d}}{\mathrm{d}x}(x+1) = \int \frac{\mathrm{d}}{\mathrm{d}x}(x+2)$

Prove $1 = 2$ using algebra and calculus

Proof

- $x \neq 0$ ▷ Given
- $x = x$ ▷ Given
- $x + x = 2x$ ▷ Add
- $\underbrace{x + x + \cdots + x}_{x \text{ times}} = x^2$ ▷ Repeatedly add x times
- $\underbrace{1 + 1 + \cdots + 1}_{x \text{ times}} = 2x$ ▷ Differentiate
- $x = 2x$ ▷ Simplify
- $1 = 2$ ▷ Divide
- What is the problem with this proof?

Prove 1 = 2 using algebra and calculus

Proof

- $x \neq 0$ ▷ Given
- $x = x$ ▷ Given
- $x + x = 2x$ ▷ Add
- $\underbrace{x + x + \cdots + x}_{x \text{ times}} = x^2$ ▷ Repeatedly add x times
- $\underbrace{1 + 1 + \cdots + 1}_{x \text{ times}} = 2x$ ▷ Differentiate
- $x = 2x$ ▷ Simplify
- $1 = 2$ ▷ Divide
- What is the problem with this proof?

Error

- Cannot write $\underbrace{x + x + \cdots + x}_{x \text{ times}} = x^2$ for non-integers
- E.g.: Cannot write $\underbrace{1.5 + 1.5 + \cdots + 1.5}_{1.5 \text{ times}} = 1.5^2$

Prove $1 = 2$ using continued fractions

Proof

- $1 = \frac{2}{3-1} = \frac{2}{3-\frac{2}{3-1}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-1}}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-1}}}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-\cdots}}}}$
- $2 = \frac{2}{3-2} = \frac{2}{3-\frac{2}{3-2}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-2}}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-2}}}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-\cdots}}}}$
- $1 = 2$ ▷ Continued fractions are the same
- What is the problem with this proof?

Prove 1 = 2 using continued fractions

Proof

- $1 = \frac{2}{3-1} = \frac{2}{3-\frac{2}{3-1}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-1}}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-1}}}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-\cdots}}}}$
- $2 = \frac{2}{3-2} = \frac{2}{3-\frac{2}{3-2}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-2}}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-2}}}} = \frac{2}{3-\frac{2}{3-\frac{2}{3-\frac{2}{3-\cdots}}}}$
- $1 = 2$ ▷ Continued fractions are the same
- What is the problem with this proof?

Error

- Cannot equate the values of the continued fractions
- The given continued fraction is $x = \frac{2}{3-x}$
  Solving for x, we have $x = 1$ or $x = 2$
- Beware of infinity!

Prove $1 = 2$ using infinite series

Proof

- Consider Grandi's series $S = 1 - 1 + 1 - 1 + \cdots$
- $S = (1 - 1) + (1 - 1) + \cdots = 0 + 0 + \cdots = 0$
- $S = 1 + (-1 + 1) + (-1 + 1) + \cdots = 1 + 0 + 0 + \cdots = 1$
- $0 = 1$ $\qquad\triangleright$ $S = 0$ and $S = 1$
- $1 = 2$ $\qquad\triangleright$ Add
- What is the problem with this proof?

Prove $1 = 2$ using infinite series

Proof

- Consider Grandi's series $S = 1 - 1 + 1 - 1 + \cdots$
- $S = (1 - 1) + (1 - 1) + \cdots = 0 + 0 + \cdots = 0$
- $S = 1 + (-1 + 1) + (-1 + 1) + \cdots = 1 + 0 + 0 + \cdots = 1$
- $0 = 1$ ▷ $S = 0$ and $S = 1$
- $1 = 2$ ▷ Add
- What is the problem with this proof?

Error

- Cannot use several algebraic methods on a divergent series
- Grandi's series is divergent
- Beware of infinity!

Prove $1 = 2$ using set theory

Proof

- Using Georg Cantor's set theory and his idea of one-to-one correspondence, we can show that the number of points on the number line segment $[0, 1]$ is same as the number of points on the number line segment $[0, 2]$
- $1 = 2$
- What is the problem with this proof?

Prove $1 = 2$ using set theory

Proof

- Using Georg Cantor's set theory and his idea of one-to-one correspondence, we can show that the number of points on the number line segment $[0, 1]$ is same as the number of points on the number line segment $[0, 2]$
- $1 = 2$
- What is the problem with this proof?

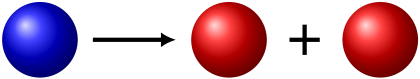
Error

- Solution is out of scope
- The problem is because the principles that apply in the world of finite quantities do not apply in the world of infinite quantities
- Beware of infinity!

Prove $1 = 2$ using geometry

Proof

- Banach-Tarski paradox states that a solid ball can be split into a finite number of disjoint subsets, which can then be assembled to create two identical copies of the original solid ball

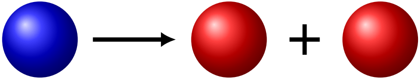


- $1 = 2$
- What is the problem with this proof?

Prove $1 = 2$ using geometry

Proof

- Banach-Tarski paradox states that a solid ball can be split into a finite number of disjoint subsets, which can then be assembled to create two identical copies of the original solid ball



- $1 = 2$
- What is the problem with this proof?

Error

- Solution is out of scope
- The problem is because the principles that apply in the world of finite quantities do not apply in the world of infinite quantities
- Beware of infinity!

The Pythagorean theorem

- History. The theorem first appeared in a Babylonian tablet dated 1900-1600 B.C.
- Incorrect proofs. Alexander Bogomolny's website Cut-The-Knot `https://www.cut-the-knot.org/pythagoras/FalseProofs.shtml` presents 9 incorrect proofs of the theorem
- Correct proofs. Elisha Scott Loomis' book "The Pythagorean Proposition" presents 367 correct proofs of the theorem (algebraic proofs + geometric proofs + trigonometric proofs)
- More Proofs. An infinite number of algebraic and geometric proofs exist for the theorem (Proof?)