Speaking Mathematically and Introduction to Proofs

Slide Credit: Prof. Aaron Tan (CS1231S)

1.1 Variables and Important Sets

- Variables; writing sentences using variables
- Important Sets and their Notations

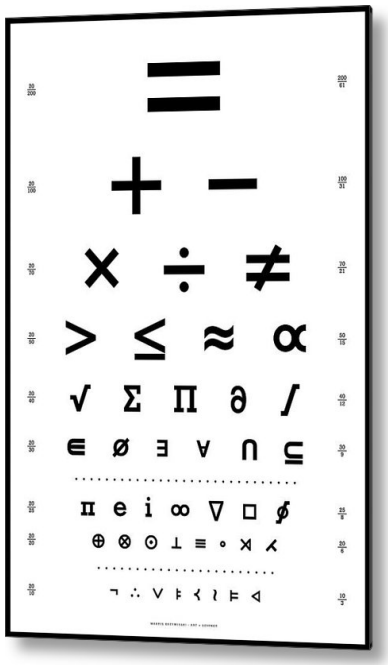
1.2 Some Important Kinds of Mathematical Statements

- Universal statement, conditional statement, existential statement
- Combination of universal, conditional and existential statements

1.3 Proofs

- What is a proof?
- Terminology: Definition, Axiom, Theorem, Lemma, Corollary, Conjecture
- Proof methods: Direct Proof, Proof by Construction, Disproof by counterexample, Proof by Exhaustion, Proof by Contradiction

Reference: Epp's Chapter 1 Speaking Mathematically



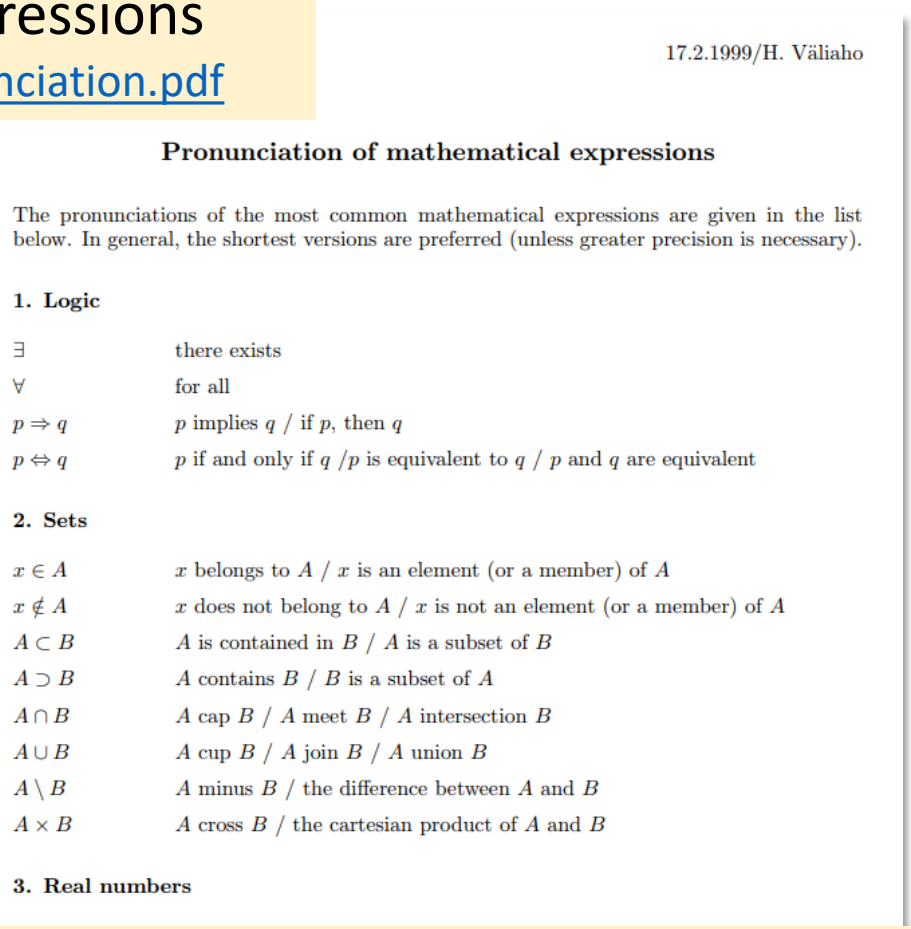
The language of mathematics is the systems used by mathematicians to communicate mathematical ideas among themselves.

Symbols, vocabulary, grammatical structures, conventions, abbreviations.

Pronunciation of mathematical expressions

https://par.cse.nsysu.edu.tw/link/math-pronunciation.pdf

Note some differences in symbols
$p \to q$ for p implies q,
$A \subseteq B$ for A is a subset of B,
$A - B$ for difference between set A and set B.



17.2.1999/H. Väliaho

Pronunciation of mathematical expressions

The pronunciations of the most common mathematical expressions are given in the list below. In general, the shortest versions are preferred (unless greater precision is necessary).

1. Logic

$\exists$	there exists
$\forall$	for all
$p \Rightarrow q$	p implies q / if p, then q
$p \Leftrightarrow q$	p if and only if q /p is equivalent to q / p and q are equivalent

2. Sets

$x \in A$	x belongs to A / x is an element (or a member) of A
$x \notin A$	x does not belong to A / x is not an element (or a member) of A
$A \subset B$	A is contained in B / A is a subset of B
$A \supset B$	A contains B / B is a subset of A
$A \cap B$	A cap B / A meet B / A intersection B
$A \cup B$	A cup B / A join B / A union B
$A \setminus B$	A minus B / the difference between A and B
$A \times B$	A cross B / the cartesian product of A and B

3. Real numbers

A more comprehensive resource:

Handbook for Spoken Mathematics

https://librivox.org/uploads/xx-nonproject/Handbook%20for%20Spoken%20Mathematics.pdf

1.1 Variables and Important Sets

1.1.1 Variables

To give names to what you are seeking, and to maintain generality.

Is there a number with the following property:
doubling it and adding 3 gives the same result as squaring it?

Is there a number x such that $2x + 3 = x^2$?

No matter what number might be chosen, if it is greater than 2, then its square is greater than 4.

Variables

No matter what number n might be chosen, if $n > 2$, then $n^2 > 4$.

1.1.2 Writing Sentences Using Variables

Rewrite the following sentences using variables:

a. Are there two numbers such that the sum of their square equals the square of their sum?

↳ Are there numbers a and b such that $a^2 + b^2 = (a + b)^2$?

b. Given any real number, its square is non-negative.

↳ Given any real number r, r^2 is non-negative.

1.1.3 Important Sets

The following are important sets often encountered:

- $\mathbb{N}$: the set of all natural numbers { 0, 1, 2, 3, …} *
- $\mathbb{Z}$: the set of all integers
  - Eg: 315, -9047, 3^5, $\sqrt{49}$
- $\mathbb{Q}$: the set of all rational numbers
  - Eg: ½, -23, 8.6, $\frac{-37}{5}$
- $\mathbb{R}$: the set of all real numbers
  - Eg: -1, π, $\sqrt{2}$, 4.5
- $\mathbb{C}$: the set of all complex numbers (note: we will not cover this)
  - Eg: $7.8, i, 3.2 - 9.1i, \sqrt{5} + \sqrt{2}i$

It is well-known that all integers are rational numbers, and all rational numbers are real numbers.

Sometimes, superscripts and subscripts are used:

- $\mathbb{Z}^+$: the set of all positive integers
- $\mathbb{R}^-$: the set of all negative real numbers
- $\mathbb{Z}_{\geq 12}$: the set of all integers greater than or equal to 12
- Note that 0 is neither negative nor positive

The symbol $\in$ means "is an element/member of"

- Example: $x \in \mathbb{Z}$ (x is a member of the set of integers; in other words, x is an integer)

1.2 Some Important Kinds of Mathematical Statements

2.1.1 Some Important Kinds of Mathematical Statements

Three of the most important kinds of statements in mathematics:

Universal statement

says that a certain property is true for ALL elements in a set. Symbol: $\forall$

Eg: All positive integers are greater than zero.

$\forall x \in \mathbb{Z}^+, x > 0$

Conditional statement

says that if one thing is true then some other thing also has to be true.

Symbol: $\rightarrow$

Eg: If 378 is divisible by 18, then 378 is divisible by 6.

Existential statement

says that there is at least one thing for which the property is true.

Symbol: $\exists$

Eg: $\exists m \in \mathbb{Z}^+$ such that $m^2 = m$.

Others:

Universal conditional statement

is a statement that is both universal and conditional.

Eg: $\forall x \in \mathbb{R}\ (x > 2 \rightarrow x^2 > 4)$.

Universal existential statement

is a statement that is universal because its first part says that a certain property is true for all objects of a given type, and it is existential because its second part asserts the existence of something.

Eg: $\forall$ nonzero real numbers u, $\exists$ a real number v such that uv = 1.

Others:

Existential universal statement

is a statement that is existential because its first part asserts that a certain object exists and is universal because its second part says that the object satisfies a certain property for all things of a certain kind.

Eg: $\exists$ c $\in \mathbb{R}$ such that $\forall$ d $\in \mathbb{R}$, cd $\neq$ 1.

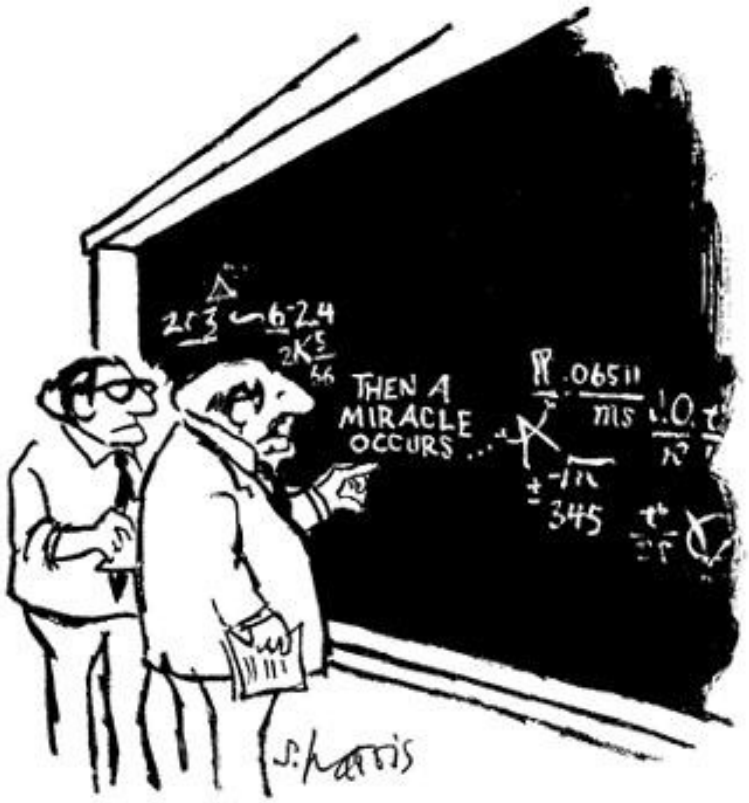
Combination

Some of the most important mathematical concepts can only be defined using universal, existential and conditional all combined.

Eg: If $a_1, a_2, a_3, \cdots$ is a sequence of real numbers, saying that "the limit of a_n as n approaches infinity is L" means that "For all positive real numbers ε, there is an integer B such that for all integers n, if $n > B$ then $-\varepsilon < a_n - L < \varepsilon$."

1.3 Proofs

1.3.1 Introduction



"I think you should be more explicit here in step two."

A **mathematical proof** is an inferential argument for a mathematical statement. In the argument, other previously established statements, such as theorems, can be used.

In principle, a proof can be traced back to self-evident or assumed statements, known as axioms, along with accepted rules of inference.

Proof methods

- Direct proof
- Proof by construction
- Disproof by counterexample
- Proof by exhaustion
- Proof by contradiction
- Proof by contraposition
- Proof by mathematical induction
- Combinatorial proof
- etc…

Not these!

Common proof techniques

Proof by intimidation Trivial!

Proof by cumbersome notation The theorem follows immediately from the fact that $\left|\bigoplus_{k\in S}\left(\mathfrak{K}^{\mathbb{F}^{\alpha}(i)}\right)_{i\in\mathcal{U}_k}\right| \preccurlyeq \aleph_1$ when $[\mathfrak{H}]_{\mathcal{W}} \cap \mathbb{F}^{\alpha}(\mathbb{N}) \neq \emptyset$.

Proof by inaccessible literature The theorem is an easy corollary of a result proven in a hand-written note handed out during a lecture by the Yugoslavian Mathematical Society in 1973.

Proof by ghost reference The proof my be found on page 478 in a textbook which turns out to have 396 pages.

Circular argument Proposition 5.18 in [BL] is an easy corollary of Theorem 7.18 in [C], which is again based on Corollary 2.14 in [K]. This, on the other hand, is derived with reference to Proposition 5.18 in [BL].

Proof by authority My good colleague Andrew said he thought he might have come up with a proof of this a few years ago...

Internet reference For those interested, the result is shown on the web page of this book. Which unfortunately doesn't exist any more.

Proof by avoidance *Chapter 3:* The proof of this is delayed until Chapter 7 when we have developed the theory even further. *Chapter 7:* To make things easy, we only prove it for the case $z = 0$, but the general case in handled in Appendix C. *Appendix C:* The formal proof is beyond the scope of this book, but of course, our intuition knows this to be true.

facebook.com/Mathematicx

Nor these!

Useful Methods of Mathematical Proof

Proof by intimidation:

Clearly ...

Proof by obscurity:

... (see de Melziac's unpublished paper, 1863) ...

Proof by flattery:

The intelligent reader will see at once that ...

Proof by attrition:

... and eleventhly ...

Proof by delegation:

I leave the proof as an exercise for the reader.

Proof by procrastination:

Omit the proof on first reading

Study this "proof" of 2 = 1:

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

$$a = b$$
$$\Rightarrow a^2 = ab$$
$$\Rightarrow a^2 - b^2 = ab - b^2$$
$$\Rightarrow (a - b)(a + b) = (a - b)b$$
$$\Rightarrow (a - b)2b = (a - b)b$$
$$\Rightarrow 2(a - b)\, b = (a - b)b$$
$$\Rightarrow 2 = 1$$

"The essential quality of a proof is to compel belief."

Pierre de Fermat,
1601 – 1665

A good proof is a concise, polished argument explaining the validity of a statement to a skeptic (usually, you).

- Concise means there are no irrelevant details. It also means to use few words. (Don't be long-winded!)
- Polished means it should be the final draft, i.e. you should have revised it (possibly several times) to make it understandable, like writing an essay.
- Argument means every step should follow logically from all previous steps.

1.3.2 Terminology

Credit: Prof Dave Richeson

Definition

A precise and unambiguous description of the meaning of a mathematical term. It characterizes the meaning of a word by giving all the properties and only those properties that must be true.

Examples:

- For any $x \in \mathbb{R}$, the absolute value of x, denoted $|x|$, is defined as follows:

$$|x| = \begin{cases} x, & \text{if } x \geq 0 \\ -x, & \text{if } x < 0 \end{cases}$$

Axiom/Postulate

A statement that is assumed to be true without proof. These are the basic building blocks from which all theorems are proved.

Examples: Euclid's five postulates, Peano axioms.

Theorem

A mathematical statement that is proved using rigorous mathematical reasoning. A theorem is usually a major or important result.

Lemma

A small theorem; a minor result whose purpose is to help in proving a theorem. (Occasionally, lemmas can take on a life of their own, eg: Bézout's lemma.)

Corollary

A result that is a simple deduction from a theorem.

Example:

- (Chapter 4)
  Theorem 4.2.2 (5^{th}: 4.3.2) The sum of any two rational numbers is rational
  Corollary 4.2.3 (5^{th}: 4.3.3) The double of a rational number is rational.

Conjecture

A statement believed to be true, but for which there is no proof (yet).

Example:

- Goldbach's conjecture: Every even integer greater than 2 can be expressed as the sum of two primes.

1.3.3 Basic Properties of Integers

In this section, we will assume the usual properties of integers.

For example, $\forall x, y, z \in \mathbb{Z}$:

- Closure: Integers are closed under addition and multiplication, i.e. $x + y \in \mathbb{Z}$ and $xy \in \mathbb{Z}$.
- Commutativity: Addition and multiplication are commutative, i.e. $x + y = y + x$ and $xy = yx$.
- Associativity: Addition and multiplication are associative, i.e. $x + y + z = (x + y) + z = x + (y + z)$ and $xyz = (xy)z = x(yz)$.
- Distributivity: Multiplication is distributive over addition (but not the other way round), i.e. $x(y + z) = xy + xz$ and $(y + z)x = yx + zx$.
- Trichotomy: Exactly one of the following is true: $x = y$, or $x < y$, or $x > y$.

(See Appendix A of Epp's book for properties of real numbers. You may quote them in your work.)

1.3.4 Examples

Definitions: Even and Odd integers

An integer n is even if, and only if, n equals twice some integer.

An integer n is odd if, and only if, n equals twice some integer plus 1.

Symbolically, if n is an integer, then

$$n \text{ is even} \iff \exists \text{ an integer } k \text{ such that } n = 2k.$$
$$n \text{ is odd} \iff \exists \text{ an integer } k \text{ such that } n = 2k + 1.$$

"if, and only if" may be abbreviated to "iff".
Similarly, "such that" is often abbreviated to "s.t.".

You may assume that every integer is even or odd, but not both.

Example of Direct Proof

Example #1: Prove that the product of two consecutive odd numbers is always odd.

Justification. (Important!)

Numbering and indentation.

1. Let a and b be the two consecutive odd numbers.
   - 1.1 Without loss of generality*, assume that $a < b$, hence $b = a + 2$.
   - 1.2 Now, $a = 2k + 1$ (by definition of odd numbers)
   - 1.3 Similarly, $b = a + 2 = 2k + 3$.
   - 1.4 Therefore, $ab = (2k + 1)(2k + 3) = (4k^2 + 6k) + (2k + 3) = 4k^2 + 8k + 3 = 2(2k^2 + 4k + 1) + 1$ (by basic algebra)
   - 1.5 Let $m = (2k^2 + 4k + 1)$ which is an integer (by closure of integers under $\times$ and $+$).
   - 1.6 Then $ab = 2m + 1$, which is odd (by definition of odd numbers).
2. Therefore, the product of two consecutive odd numbers is always odd.

"Without loss of generality" may be abbreviated to WLOG. This is used before an assumption in a proof which narrows the premise to some special case, and implies that the proof for that case can be easily applied to all other cases.

Example of Direct Proof

Previous slide: Prove that the product of two consecutive odd numbers is always odd.

1. Would the proof be very different if we change the task to the following?

   Prove that the product of any two odd numbers is always odd.

2. If we have proven the above as a theorem, what can we say about the original task "Prove that the product of two consecutive odd numbers is always odd"?

   Corollary

Example #2: Prove the following

$$\exists x \in \mathbb{Z} \text{ s.t. } x > 2 \text{ and } x^2 - 5x + 6 > 0.$$

1. Let $x = 17$.
2. Note that $17 \in \mathbb{Z}$ and $17 > 2$.
3. Also, $x^2 - 5x + 6 = 17^2 - 5(17) + 6 = 210 > 0$. ■

- In the proof above, there is no need to explain how 17 is obtained. You just need to show that 17 has the required properties. Of course, many integers satisfy the same properties and any of these will suffice for the proof.
- This style of proof – where you explicitly find the value with the correct properties – is called a proof by construction. It is a form of direct proof and it is the most direct way to prove that something exists.

A counter-example is an example that shows that a statement is not always true.

Prove that the following statement is not true:
The product of two irrational numbers is always irrational.

1. Let the two irrational numbers be $\sqrt{2}$ and $\sqrt{8}$.

   1.1 Then $\sqrt{2} \times \sqrt{8} = \sqrt{2 \times 8}$ (by basic algebra)

   $= \sqrt{16} = 4$ which is a rational number.

2. Therefore, that statement "the product of two irrational numbers is always irrational" is not true. ■

Note that <u>one</u> counter-example is sufficient.

Definition: Divisibility

If n and d are integers and $d \neq 0$, then

n is divisible by d iff n equals d times some integer.

We may also say that "n is a multiple of d", or "d is a factor of n", or "d is a divisor of n" or "d divides n".

We use the notation $d \mid n$ to mean "d divides n". Symbolically, if $n, d \in \mathbb{Z}$ and $d \neq 0$:

$$d \mid n \iff \exists k \in \mathbb{Z} \text{ such that } n = dk.$$

- Note that division is not used in this particular definition of divisibility. Here, the notation $a|b$ simply means a is a factor of b; no actual division is performed.
- $a|b$ is a statement, which is evaluated to true or false. It is not a numerical value. That is, you say $3|12$ is true; $3|10$ is false; you don't say $3|10$ is 1 or $3\frac{1}{3}$.

Example #3: Prove that $6a$ is not divisible by 5 for an integer a between 1 and 4 inclusive.

1. Let a be an integer between 1 and 4 inclusive.
   - 1.1 If a = 1, then $6a = 6$ but $5 \nmid 6$.
   - 1.2 If a = 2, then $6a = 12$ but $5 \nmid 12$.
   - 1.3 If a = 3, then $6a = 18$ but $5 \nmid 18$.
   - 1.4 If a = 4, then $6a = 24$ but $5 \nmid 24$.
2. Therefore, $6a$ is not divisible by 5 for an integer a between 1 and 4 inclusive. ■

Example #4: Prove that the difference of two consecutive squares between 30 and 100 is odd.

1. The squares between 30 and 100 are 36, 49, 64 and 81.
   - 1.1 Case 1: 49 – 36 = 13 which is odd.
   - 1.2 Case 2: 64 – 49 = 15 which is odd.
   - 1.3 Case 3: 81 – 64 = 17 which is odd.
2. Therefore, the difference of two consecutive squares between 30 and 100 is odd. ■

Proof by exhaustion, also called proof by cases, or proof by brute force, is suitable when the number of cases is finite.

What if we need to prove a general problem where the number of cases is infinite?
We may then use proof by deduction, a type of direct proof.

Example #5: Prove that the difference of two consecutive squares is always odd.

1. Suppose s and t are two consecutive squares and $s < t$. Then $s = n^2$ and $t = (n+1)^2$.
   1.1 $(n+1)^2 - n^2 = n^2 + 2n + 1 - n^2 = 2n + 1$ (by basic algebra)
   1.2 $2n + 1$ is odd (by definition of odd numbers)
2. Therefore, the difference of two consecutive squares is odd. ■

1.3.5 More Examples

The preceding examples are straight-forward. Let's try something more interesting.

Sometimes a direct proof is difficult. For example, to prove theorems below:

Theorem 4.6.1 (5th: 4.7.1)

There is no greatest integer.

Proposition 4.6.4 (5th: 4.7.4)

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

In this case, we use indirect proof. Proof by contradiction and proof by contraposition are indirect proof methods.

Theorem 4.6.1 (5th: 4.7.1)

There is no greatest integer.

Proof (by contradiction):

1. Suppose not, i.e. there is a greatest integer.
   - 1.1 Let call this greatest integer g, and $g \geq n$ for all integers n.
   - 1.2 Let $G = g + 1$.
   - 1.3 Now, G is an integer (closure of integers under $+$) and $G > g$.
   - 1.4 Hence, g is not the greatest integer → contradicting 1.1.
2. Hence, the supposition that there is a greatest integer is false.
3. Therefore, there is no greatest integer.

Recall: Contrapositive of $p \to q$ is $\sim q \to \sim p$.

Proof by Contraposition

1. Statement to be proved: $\forall x \in D \left(P(x) \to Q(x)\right)$.
2. Rewrite the statement into its contrapositive form:
   $\forall x \in D \left(\sim Q(x) \to \sim P(x)\right)$.
3. Prove the contrapositive statement by a direct proof.
   - 3.1 Suppose x is an (particular but arbitrarily chosen) element of D s.t. $Q(x)$ is false.
   - 3.2 Show that $P(x)$ is false.
4. Therefore, the original statement $\forall x \in D \left(P(x) \to Q(x)\right)$ is true.

Proposition 4.6.4 (5th: 4.7.4)

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

Proof (by contraposition):

1. Contrapositive statement:
   For all integers n, if n is odd then n^2 is odd.
2. Let n be an arbitrarily chosen odd number.
   - 2.1 Then $n = 2k + 1$ for some integer k (by definition of odd integer).
   - 2.2 Then $n^2 = (2k + 1)(2k + 1) = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$
   - 2.3 Let $m = 2k^2 + 2k$. Now, m is an integer (by closure property) and $n^2 = 2m + 1$.
   - 2.4 So n^2 is odd.
3. Therefore, for all integers n, if n^2 is even then n is even.

1.3.6 How to Write Proofs

We introduced the format which includes numbering and indentation to help organize your proof. But how do you fill in the content of the proof? Which proof method should you use?

In this section we show a general approach. However, writing proofs require insight and ingenuity at times, so the more you practice on your own and study others' proofs, the more skillful you will get.

As you examine more examples, and solve more problems, you will gain the experience you need.

- Doing a proof is like solving a jigsaw puzzle*. No two jigsaws are alike: no two proofs are alike.

- Sometimes you solve large chunks quickly, other times you get stuck. You don't have to solve from top to bottom.

- Some strategies are used, eg. fixing the border of the puzzle first. Likewise, there are useful strategies for proofs.

*: Adapted from D. Velleman, *How to Prove It*, 2nd Edition, 2006.

END OF FILE