

# Lecture 1: Speaking Mathematically

Aaron Tan

## 1. Speaking Mathematically

## 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

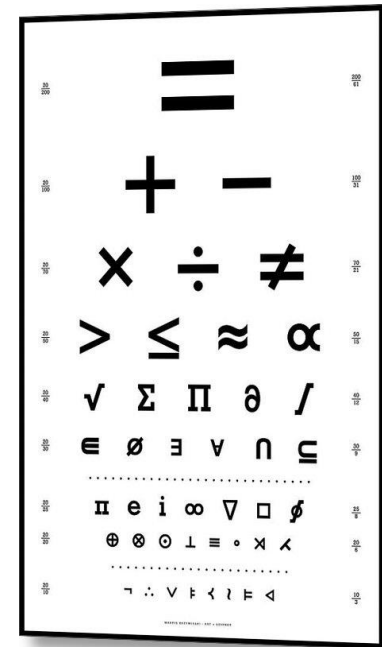
- What is a proof?
- Terminology: Definition, Axiom, Theorem, Lemma, Corollary, Conjecture
- Proof methods: Direct Proof, Proof by Construction, Disproof by counterexample, Proof by Exhaustion, Proof by Contradiction

Reference: Epp's Chapter 1 Speaking Mathematically

## 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.

## 1. Speaking Mathematically

## Pronunciation of mathematical expressions

<http://par.cse.nsysu.edu.tw/link/math-pronunciation.pdf>

17.2.1999/H. Väliaho

Note some differences in symbols we use in CS1231S, such as:

$p \rightarrow q$  for  $p$  implies  $q$ ,

$A \subseteq B$  for  $A$  is a subset of  $B$ ,

$A - B$  for difference between set  $A$  and set  $B$ .

## 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

plus one
minus one
plus or minus one
$y$ / $x$ multiplied by $y$

A more comprehensive resource:

Handbook for Spoken Mathematics

<http://www.tsbvi.edu/mathproject/appB-sec1.asp>

## 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.



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

Variables

## 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?

$$x^2 + y^2 = (x+y)^2$$

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

given any real number  $r$ ,  $r^2$  is  $\geq 0$

## 1.1.3 Important Sets

The following are important sets often encountered:

- $\mathbb{N}$ : the set of all natural numbers  $\{0, 1, 2, 3, \dots\}$  \*  
includes 0  
take note of trick
- $\mathbb{Z}$ : the set of all integers
  - Eg: 315, -9047,  $3^5$ ,  $\sqrt{49}$  )
- $\mathbb{Q}$ : the set of all rational numbers
  - Eg:  $\frac{1}{2}$ , -23, 8.6,  $\frac{-37}{5}$  )
- $\mathbb{R}$ : the set of all real numbers
  - Eg: -1,  $\pi$ ,  $\sqrt{2}$ , 4.5

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

\*: Some define  $\mathbb{N}$  to exclude 0, some include 0. Here, we include 0.



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

## Some Important Kinds of Mathematical Statements

## 2.1.1 Some Important Kinds of Mathematical Statements

Three of the most important kinds of sentences in mathematics:

watch out for trick questions

### Universal statement

says that a certain property is true for ALL elements in a set. (Eg: **All positive integers are greater than zero.**) Keywords: 'all', 'every', 'any'. Symbol:  $\forall$

### Conditional statement

says that if one thing is true then some other thing also has to be true. (Eg: **If 378 is divisible by 18, then 378 is divisible by 6.**)

Keyword: 'if ... then'. Symbol:  $\rightarrow$  same as implies statement

### Existential statement

says that there is at least one thing for which the property is true. (Eg: **There is a prime number that is even.**) Keywords: 'there exists', 'there is', 'some'. Symbol:  $\exists$

Others:

## Universal conditional statement

is a statement that is both universal and conditional.

Eg: For all animals  $a$ , if  $a$  is a dog, then  $a$  is a mammal.

Universal conditional statements can be re-written to make them appear to be purely universal or purely conditional.

Eg: All dogs are mammals. Every dog is a mammal. Every integer is a real number.

hidden implicit statement

## 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: Every real number has an additive inverse.

(The additive inverse of  $n$  is the number that, when added to  $n$ , yields zero.)

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.

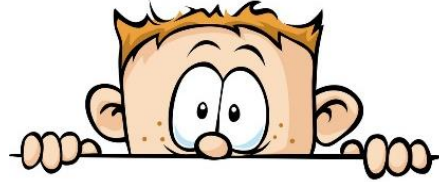
Eg: There is a positive integer that is less than or equal to every positive integer.

## Combination

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

Eg: If  $a_1, a_2, a_3, \dots$  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  $\varepsilon$ , there is an integer  $N$  such that for all integers  $n$ , if  $n > N$  then  $-\varepsilon < a_n - L < \varepsilon$ .”

# Peeking ahead

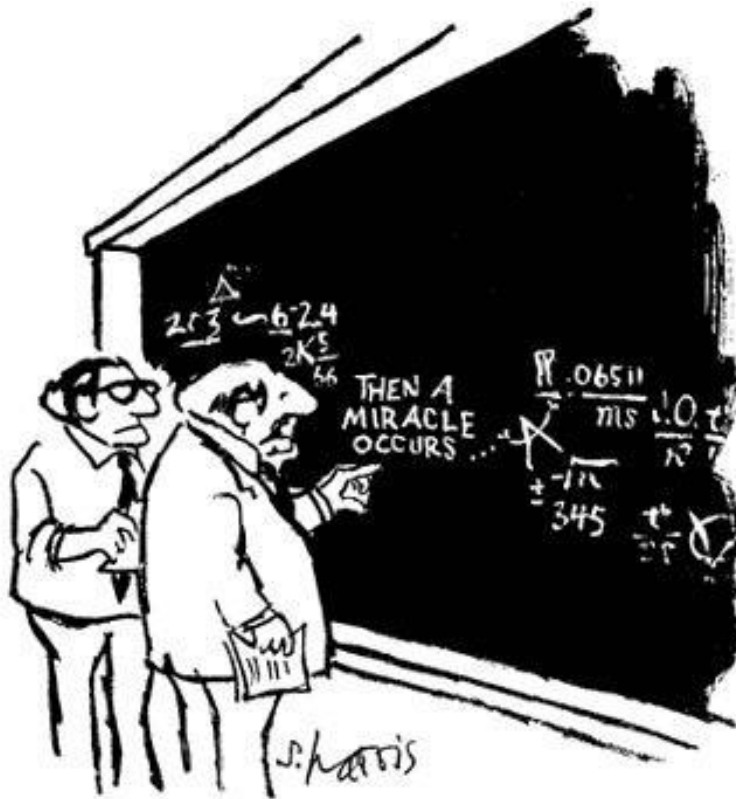


## Universal, Existential and Conditional Statements

- Chapter 2 The Logic of Compound Statements
- Chapter 3 The Logic of Quantified Statements

## 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...

This section shows only a few examples. More to come in subsequent lectures.

# Common proof techniques

**Proof by intimidation** Trivial!

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

**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 may 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 is 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.

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

polished assignment

A 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. (We will study logical argument next week.)

## 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:

- (Chapter 2) A **statement** is either true or false but not both.
- (Chapter 4) 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**.

Example:

- (Chapter 4) Theorem 4.4.6 (5<sup>th</sup>: 4.5.6) **The Triangle Inequality**  
For any  $x, y \in \mathbb{R}$ ,  $|x + y| \leq |x| + |y|$ .

## 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.)

Example:

- (Chapter 4) Lemma 4.4.4 (5<sup>th</sup>: 4.5.4) For any  $r \in \mathbb{R}$ ,  $-|r| \leq r \leq |r|$ .



## Corollary

A result that is a **simple deduction** from a theorem.

Example:

- (Chapter 4)  
Theorem 4.2.2 (5<sup>th</sup>: 4.3.2) The sum of any two rational numbers is rational  
Corollary 4.2.3 (5<sup>th</sup>: 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.

### 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

$n$  is even  $\iff \exists$  an integer  $k$  such that  $n = 2k$ .

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

We will learn the meaning of “if, and only if”,  $\iff$ ,  $\exists$ , etc. in the next lecture. “if, and only if” may be abbreviated to “iff”. Similarly, “such that” is often abbreviated to “s.t.”.

## Example of Direct Proof

is a huge umbrella term, a lot of other proofs are direct proofs

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

if someone questions this assumption, rewrite proof but switch  $a$  &  $b$  so will look very similar

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  $m = (2k^2 + 4k + 1)$ 

multiplication of integers is an integer (by closure property)  
everything add together is an integer (by closure property)
  - 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.

therefore use this to show that no need to show complete proof since similar

“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. a proof that is more general than the previous one

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”?

this is now a special case and a subset of the above proof will be repetition

example of corollary

## Example of Proof by Construction

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 was 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.

## Example of Disproof by Counter Example

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 one counter-example is sufficient.

enough because the prove is trying to be universal "always"

## Example of Proof

## 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  $a \mid b$  simply means  $a$  is a **factor of  $b$** ; no actual division is performed.
- $a \mid b$  is a statement, which is evaluated to **true or false**. It is not a numerical value. That is, you say  $3 \mid 12$  is true;  $3 \mid 10$  is false; you don't say  $3 \mid 10$  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 of Proof by Exhaustion

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.

## Example of Proof by Deduction

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. Let the numbers be  $n$  and  $n + 1$ .

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 Theorem 4.7.1 (5<sup>th</sup>: 4.8.1) below:

**Theorem 4.7.1 (5<sup>th</sup>: 4.8.1) Irrationality of  $\sqrt{2}$**

$\sqrt{2}$  is irrational.

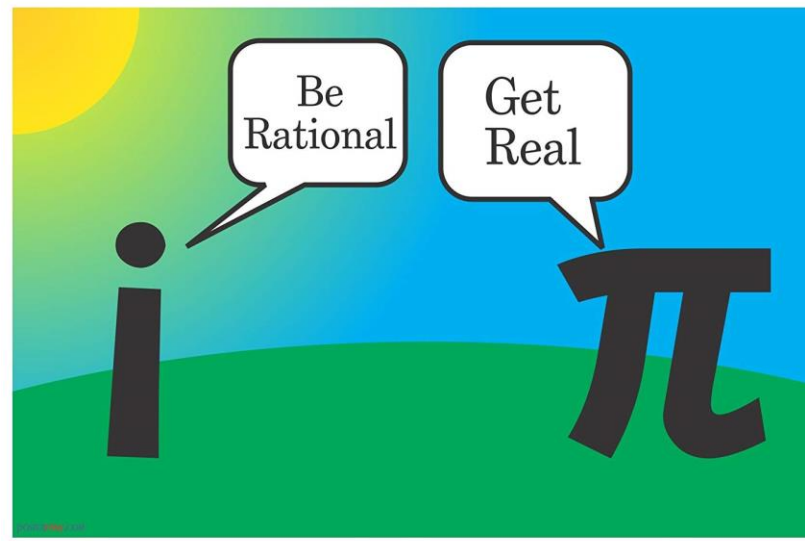
Direct proof in this case is difficult because irrationality has an absence of a form. We know how a rational number “looks like”, but we can't say the same for irrationals.

## Definition: Rational and irrational numbers

A real number  $r$  is **rational** iff it can be expressed as a quotient of two integers with a nonzero denominator. That is,

$$r \text{ is rational} \Leftrightarrow \exists a, b \in \mathbb{Z} \text{ s.t. } r = \frac{a}{b} \text{ and } b \neq 0.$$

A real number that is not rational is **irrational**.



Example of **Proof by Contradiction**

In this case we need to do an indirect proof. One type of indirect proof is **proof by contradiction**.

To prove a statement  $S$  by contradiction, you first assume that  $\sim S$  (not  $S$ ) is true. Based on this, you use **known facts and theorems** to arrive at a logical contradiction. using any theorem proved during lecture/tutorial/textbook

Since every step of your argument thus far is logically correct, the problem must lie in your assumption (that  $\sim S$  is true).

Thus, you conclude that  $\sim S$  is false, that is,  $S$  is true.

So now we can proceed to prove the irrationality of  $\sqrt{2}$ . We also need this proposition, which we will defer the proof for now.

**Proposition 4.6.4 (5<sup>th</sup>: 4.7.4)**

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

## Example of Proof by Contradiction

Example #6: Prove Theorem 4.7.1 (5<sup>th</sup>: 4.8.1)  $\sqrt{2}$  is irrational.

1. Suppose not, that is,  $\sqrt{2}$  is rational.
  - 1.1 Then  $\exists m, n \in \mathbb{Z}$  s.t.  $\sqrt{2} = \frac{m}{n}$  \* (by definition of rational numbers)
  - 1.2  $m^2 = 2n^2$  (by basic algebra)
  - 1.3 Hence  $m^2$  is even (by definition of even number, as  $n^2$  is an integer by closure)
  - 1.4 Hence  $m$  is even (by Proposition 4.6.4)
  - 1.5 Let  $m = 2k$ ; substituting into 1.2:  $4k^2 = 2n^2$ , or  $n^2 = 2k^2$
  - 1.6 Hence  $n^2$  is even (by definition of even number)
  - 1.7 Hence  $n$  is even (by Proposition 4.6.4)
  - 1.8 So both  $m$  and  $n$  are even, but this contradicts that  $\frac{m}{n}$  is in its lowest term.
2. Therefore the assumption that  $\sqrt{2}$  is rational is false.  
Hence  $\sqrt{2}$  is irrational. ■

\*: Here, we require that  $\frac{m}{n}$  be in its lowest terms, i.e. the only common factor of  $m$  and  $n$  is 1. It is always possible to reduce a rational to its lowest terms. We defer proving this claim.

Example of Proof by **Contradiction**

In example #2, for proof by construction, the proof is rather straight-forward as the right value (eg: 17) can be found easily.

Example #2: Prove the following

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

However, sometimes finding the right thing takes some **cleverness**, as the next example illustrates.



## Example of Proof by Contradiction

**Example #7:** Prove that there exist irrational numbers  $p$  and  $q$  such that  $p^q$  is rational.



1. From Theorem 4.7.1,  $\sqrt{2}$  is irrational
2. Consider  $\sqrt{2}^{\sqrt{2}}$ . It is either rational or irrational.
3. Case 1:  $\sqrt{2}^{\sqrt{2}}$  is rational.
  - 3.1 Let  $p = q = \sqrt{2}$  and we are done.
4. Case 2:  $\sqrt{2}^{\sqrt{2}}$  is irrational.
  - 4.1 Let  $p = \sqrt{2}^{\sqrt{2}}$ , and  $q = \sqrt{2}$
  - 4.2 Now  $p$  is irrational (by assumption), so is  $q$  (by Theorem 4.7.1).
  - 4.3 Consider  $p^q = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2} \times \sqrt{2}} = (\sqrt{2})^2 = 2$  (by basic algebra)
  - 4.4 Clearly 2 is rational
5. In either case, we have found the required  $p$  and  $q$ !

## 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 will 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 in class and the book, and solve more problems in tutorials, you will gain the experience you need.

## How to Write Proofs

- 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*, 2<sup>nd</sup> Edition, 2006.

We introduce the definition of **colorful** for this section. Note that this terminology is non-standard and is used only in this class.

### Definition of Colorful (only for CS1231/CS1231S)

An integer  $n$  is said to be **colorful** if there exists some integer  $k$  such that  $n = 3k$ .



Are the following colorful?

■ **-1353** colourful because  $3(-451) = -1353$

■ **7**  
not colourful because there is not integer  $k$  where  $7 = 3k$

■ **0**  
colourful because  $3(0) = 0$

Example #8: Prove that

if  $x, y$  are colorful integers, then so is  $x + 2y$ .

Identify  $P$  and  $Q$  to be:

$P$ :  $x, y$  are colorful integers

$Q$ :  $x + 2y$  is colorful

We can immediately write down the **start** and **end** of the proof, as follows:

Draft proof:

1. Let  $x, y$  be colorful integers.
2. ...
3. And thus  $x + 2y$  is colorful. ■

Example #8: Prove that

if  $x, y$  are colorful integers, then so is  $x + 2y$ .

The next logical thing is to use the definition of colorful.

Draft proof:

1. Let  $x, y$  be colorful integers.

1.1 Then  $\exists a, b \in \mathbb{Z}$  s.t.  $x = 3a$  and  $y = 3b$  (by definition of colorful).

2. ...

3. So  $\exists c \in \mathbb{Z}$  s.t.  $x + 2y = 3c$ .

4. And thus  $x + 2y$  is colorful (by definition of colorful). ■

Example #8: Prove that

if  $x, y$  are colorful integers, then so is  $x + 2y$ .

This means we need to **connect  $c$  to  $a$  and  $b$** . Obviously, we should try writing  $(x + 2y)$  in terms of  $a, b$ :

Draft proof:

1. Let  $x, y$  be colorful integers.

1.1 Then  $\exists a, b \in \mathbb{Z}$  s.t.  $x = 3a$  and  $y = 3b$  (by definition of colorful).

2. ...

$$x + 2y = 3a + 2(3b) = 3(a + 2b)$$

3. So  $\exists c \in \mathbb{Z}$  s.t.  $x + 2y = 3c$ .

4. And thus  $x + 2y$  is colorful (by definition of colorful). ■

Example #8: Prove that

if  $x, y$  are colorful integers, then so is  $x + 2y$ .

So our final proof:

Proof:

1. Let  $x, y$  be colorful integers.
  - 1.1 Then  $\exists a, b \in \mathbb{Z}$  s.t.  $x = 3a$  and  $y = 3b$  (by definition of colorful).
  - 1.2 Now,  $x + 2y = 3a + 2(3b) = 3(a + 2b)$  (by basic algebra)
2. Let  $c = a + 2b$ . Note that  $c \in \mathbb{Z}$  (by closure)
3. So  $\exists c \in \mathbb{Z}$  s.t.  $x + 2y = 3c$ .
4. And thus  $x + 2y$  is colorful (by definition of colorful). ■



## Extra: Thinking Mathematically

# Reasoning

## Observing structures

## Working systematically

## Visualising

# Modelling

No rote learning!



## Extra: Thinking Mathematically

Back to the basic: **Understanding definitions.**

Definition: Rational number

$r$  is rational  $\Leftrightarrow \exists a, b \in \mathbb{Z}$  s.t.  $r = \frac{a}{b}$  and  $b \neq 0$ .



Is every integer a rational number?

1. Let  $n$  be an integer.
  - 1.1 Let  $a = n$  and  $b = 1$
  - 1.2 then  $n = \frac{a}{b}$
2. Therefore, every integer is a rational number

## Extra: Thinking Mathematically

No rote learning!

In AY2017/18 Semester 1 exam paper, the following new definitions are given and 7 questions are based on them!

The next 7 questions (Q9 to Q15) refer to the following definitions.

**Definition 1.** A **Group**, denoted  $(G, *)$ , is a set  $G$  along with a binary operator  $*$  that satisfies these four axioms:

- (A1) Closure:  $\forall a, b \in G, a * b \in G.$
- (A2) Associativity:  $\forall a, b, c \in G, (a * b) * c = a * (b * c).$
- (A3) Identity:  $\exists e \in G$  such that  $\forall a \in G, a * e = e * a = a.$
- (A4) Inverse:  $\forall a \in G, \exists b \in G$  (called the *inverse* of  $a$ ) such that  $a * b = b * a = e.$

**Definition 2.** If  $G$  is finite with  $m \in \mathbb{Z}^+$  elements, then the **group order** of  $G$  is said to be  $m$ . For small  $m$ , it is often helpful to see the group as a **Cayley table**. Let  $a_1, a_2, \dots, a_m$  be the elements of  $G$ , then each entry,  $c_{ij}$  in the  $m \times m$  Cayley table is defined as  $c_{ij} = a_i a_j$ , for  $i, j = 1, 2, \dots, m$  (see Table 1(a) on page 6.)

**Definition 3.** Given a group  $(G, *)$ , and any  $x \in G$ , define **powers** of  $x$  recursively as follows:

$$x^n = \begin{cases} e \text{ (identity)}, & \text{if } n = 0, \\ x * x^{n-1}, & \text{if integer } n > 0, \\ x^{-1} * x^{n+1}, & \text{if integer } n < 0. \end{cases}$$

This means the usual power law holds:  $x^{m+n} = x^m * x^n$  and  $(x^m)^n = x^{mn}$ ,  $\forall m, n \in \mathbb{Z}$ .

**Definition 4.** For any  $x \in G$ , let  $k$  be the smallest positive integer, if such a  $k$  exists, such that  $x^k = e$ , then the **element order** of  $x$  is said to be  $k$ .

# Next lecture

## 2. The Logic of Compound Statements

$\sim$        $\wedge$        $\vee$        $\rightarrow$

END OF FILE