MATHEMATICS 300 — SPRING 2019

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S NOTES

Date of this version: September 13, 2019

Contents

Part I

1 Introduction

These notes are about ***mathematical proofs***. We are going to get started by presenting some examples of proofs. Later, after we have seen several proofs, we will discuss in general, in great detail,

- What proofs are.
- How to read proofs.
- How to write and how not to write proofs.
- What proofs are for.
- Why proofs they are important.

But first, in Sections 2 and 3, I am going to show you several examples of ***proofs***.

In each of these examples, we are going to prove a ***theorem***. Theorems have ***statements***. Each statement expresses a ***proposition***, and the fact that the statement has been proved implies that the proposition is ***true***, in which case we say that the statement is true.

So maybe it is a good idea to start by clarifying the meanings of the words "theorem", "statement", "proof", and of other related words such as "proposition", "fact", and "conclusion".

1.1 Sentences, propositions, terms, variables, theorems and proofs

THIS SECTION IS STILL BEING WRITTEN. WHEN IT IS FINISHED IT WILL BE INCLUDED IN THESE NOTES.

2 An example of a proof: Euclid's proof of the infinitude of the set of prime numbers

Our first example of a proof will be Euclid's proof that there are infinitely many prime numbers. This proof is found in Euclid's *Elements* (Book IX, Proposition 20). Euclid (who was probably born in 325 BCE and died in 270 BCE) was the first mathematician to write a large treatise where mathematics is presented as a collection of definitions, postulates, propositions (i.e., theorems and constructions) and mathematical proofs of the propositions.

2.1 What Euclid's proof is about

You probably know what a "prime number" is. (If you do not know, do not worry; I will explain it to you pretty soon.) Here are the first few prime numbers:

$$2, 3, 5, 7, 11, 13, 17, 19 \ldots$$

Does the list of primes stop there? Of course not. It goes on:

$$23, 29, 31, 37, 41, 43, 47, 53, 59, 61 \ldots$$

And it doesn't stop there either. It goes on:

$$67, 71, 73, 79, 83, 89, 97, 101, 103 \ldots .$$

Does the list go on forever? If you go on computing primes, you would find more and more of them. And mathematicians have actually done this, and found an incredibly large number of primes.

The largest known prime

As of January, 2019, the largest known prime was

$$2^{82,589,933} - 1\,.$$

(That is, 2 multiplied by itself $82,589,933$ times, minus one.) This is a huge number! It has $24,862,048$ decimal digits.

Is it possible that the list of primes stops here, that is, that there are no primes larger than $2^{82,589,933} - 1$?

Before we answer this, just ask yourself: suppose it was indeed true that the list stops with this prime number. How would you know that? If you think about it for a minute, you will see that *there is no way to know.* You could go on looking at natural numbers larger than $2^{82,589,933} - 1$, and see if among these numbers you find one that is prime. But if you don't find any it doesn't mean there aren't any. It could just be that you haven't gone far enough in your computation, and if you went farther you would find one.

In fact, no matter how many primes you may compute, you will never know whether the largest prime you have found is indeed the largest prime there is, or there is a larger one.

Can we know in some way, other than by computing lots of primes, whether the list of primes goes on forever or there is a prime number which is the largest one?

It turns out that this question can be answered by means of **reasoning**. And, amazingly, the answer is "yes, the list of primes goes on forever"! This was discovered, in the year 300 B.C., approximately, by the great Greek mathematician Euclid. Euclid's 3,000-year old proof is a truly remarkable achievement, the first result of what we would now call "number theory", one of the most important areas of Mathematics.

Euclid's theorem says the following:

Theorem. *The set of prime numbers is infinite.*

In order to prove the theorem, we need to understand the precise meaning of the terms that occur in the statement. So I will begin by explaining the meaning of "prime number" and "infinite set".

And, in order to explain what a prime number is, we will have to explain first what we mean by "divisibility",

and "factors".

2.2 Divisibility of integers; factors

If you have two integers a and b, you would like to "divide a by b", and obtain a "quotient" q, i.e., an integer q that multiplied by b gives you back a. For example, we can divide 6 by 2, and get the quotient 3. And we can divide 6 by 3, and get the quotient 2.

But it is not always possible to divide a by b. For example, if $a = 4$ and $b = 3$, then an integer q such that $3q = 4$ does not exist[1].

Since dividing a by b is sometimes possible and sometimes not, we will introduce some new words to describe those situations when division is possible.

Definition 1. Let a, b be integers.

1. We say that b <u>divides</u> a if there exists an integer k such that
$$a = bk\,.$$

2. We say that a is a <u>multiple</u> of b if b is a factor of a.

[1] You may say that "the result of dividing 4 by 3 is the fraction $\frac{4}{3}$". That is indeed true, but $\frac{4}{3}$ ***is not an integer***, and so far we are working in a world in which there are integers and nothing else. If we want $\frac{4}{3}$ to exist, we have to invent new numbers—the fractions, or "rational numbers". We are going to do that pretty soon, but for the moment, since we are working with integers only, it is ***not*** possible to divide 4 by 3 and get a quotient which is an integer.

3. We say that b is a <u>factor</u> of a if b divides a.
4. We say that a is <u>divisible</u> by b if b divides a.
5. We write

$$b|a$$

to indicate that b divides a. □

Remark 1. As the previous definition indicates,

The following are five different ways of saying exactly the same thing:

- m divides n,
- m is a factor of n,
- n is a multiple of m,
- n is divisible by m,
- $m|n$.

□

Reading statements with the "divides" symbol "|"

The symbol "|" is read as "divides", or "is a factor of".
For example, the statement "3|6" is read as "3 divides 6", or "3 is a factor of 6". And the statement "3|5" is read as "3 divides 5", or "3 is a factor of 5". (Naturally, "3|6" is true, but "3|5" is false.)
The vertical bar of "divides" has nothing to do with the bar used to write fractions. For example, " $3|6$ ***" is the statement*** [a] ***"*** 3 ***divides*** 6 ***', which is true. And "*** $\frac{3}{6}$ ***" is a noun phrase: it is one of the names of the number also known as "*** $\frac{1}{2}$ ***", or "*** 0.5 ***".***

[a] A statement is something we can say that is true or false. A noun phrase is something we can say that stands for a thing or person. For example, "Mount Everest", "New York City", "My friend Alice", "The movie I saw on Sunday", are noun phrases. "Mount Everest is very tall", "I live in New York City", "My friend Alice studied mathematics at Rutgers", and "The movie I saw on Sunday was very boring", are statements.

Example 1. Here are some examples illustrating the use of the word "divides" and the symbol "|":

- The following statements are true:
  1. 6 divides 6,

2. $6|6$,
3. 6 divides 12,
4. $6|12$,
5. 1 divides 5,
6. $1|5$,
7. 13 divides 91,
8. $13|91$,
9. 6 divides 0,
10. $6|0$,
11. 6 divides -6,
12. $6|-6$,
13. -6 divides 6,
14. $-6|6$,
15. 6 divides -12,
16. $-6|12$,
17. 6 divides 0,
18. $6|0$,
19. 0 divides 0,
20. $0|0$,

- and the following statements are false:

1. 6 divides 7,

2. $6|7$,
3. 0 divides 1,
4. $0|1$,
5. 12 divides 6,
6. $12|6$,
7. -5 divides 6,
8. $-5|6$,
9. $0|6$.

2.3 What is a "prime number"

Definition 2. A prime number is a natural number p such that

I. $p > 1$,

II. p is not divisible by any natural numbers other than 1 and p. □

And here is another way of saying the same thing, in case you do not want to talk about "divisibility".

Definition 3. A prime number is a natural number p such that

I. $p > 1$,

II. There do not exist natural numbers j, k such that $j > 1$, $k > 1$, and $p = jk$. □

2.3.1 Why isn't 1 prime?

If you look at the definition of "prime number", you will notice that, ***for a natural number*** p ***to qualify as a prime number, it has to satisfy*** $p > 1$. In other words, ***the number*** 1 ***is not prime.*** Isn't that weird? After all, the only natural number factor of 1 is 1, so the only factors of 1 are 1 and itself, and this seems to suggest that 1 *is* prime.

Well, if we had defined a number p to be prime if p has no natural number factors other than 1 and itself, then 1 *would* be prime. But we were *very* careful not to do that. Why?

The reason is, simply, that there is a very nice theorem called the "unique factorization theorem", that says that every natural number greater than 1 either is prime or can be written as a product of primes *in a unique way*. (For example: $6 = 2 \cdot 3$, $84 = 2 \cdot 2 \cdot 3 \cdot 7$, etc.)

If 1 was a prime, then the result would not be true as stated. (For example, here are two different ways to write 6 as a product of primes: $6 = 2 \cdot 3$ and $6 = 1 \cdot 2 \cdot 3$.) And mathematicians like the theorem to be true as stated, so we have decided not to call 1 a prime[2].

[2]This is exactly the same kind of reason why Pluto is not a planet. Pluto is not a planet because astronomers have decided not to call Pluto a planet. Similarly, mathematicians have decided not to call 1 prime, and that's why 1 is not prime.

If you do not like this, just keep in mind that we can use words any way we like, as long as we all agree on what they are going to mean. If we decide that 1 is not prime, then 1 is not prime, and that's it. If you think that for you 1 is really prime, just ask yourself why and you will see that you do not have a proof that 1 is prime.

2.3.2 The prime factorization theorem

In our proof of Euclid's theorem, we are going to use the fact that every natural number (except 1) can be written as a product of prime numbers. This is a very important result in arithmetic[3], and we are going to prove it later.

The precise statement is as follows:

Theorem. (The prime factorization theorem.) *Every natural number n such that $n \geq 2$ is a product of primes.* □

2.3.3 Clarification: What is a "product of primes"?

Like all mathematical ideas, even something as simple as "product of primes" requires a precise definition. Without a precise definition, it would not be clear, for example, whether a single prime such as 2 or 3 or 5 is a "product of primes".

[3]Actually, many mathematicians call "The Fundamental Theorem of Arithmetic".

Definition 4. A natural number n is a product of primes if there exist

1. a natural number k,

and

2. a finite list[4]
$$\mathbf{p} = (p_1, \ldots, p_k)$$
of prime numbers,

such that
$$n = p_1 \cdot p_2 \cdot \cdots \cdot p_k \,. \tag{2.1}$$
(If you are familiar with the product "$\prod$" notation, formula (2.1) says that $n = \prod_{i=1}^{k} p_i$.)

Notice that k *can be equal to one.* That is, ***a single prime, such as*** 2***, or*** 3***, or*** 23***, is a product of primes in the sense of our definition.*** □

Definition 5. If n is a natural number, then a list $\mathbf{p} = (p_1, \ldots, p_k)$ of prime numbers such that (2.1) holds is called a prime factorization of n. □

Example 2. The following natural numbers are products of primes:

- 7 (because 7 is prime); the list (7) is a prime factorization of 7,

[4]Finite lists will be defined and discussed in great detail later in these notes.

- 24; (the list $(2, 2, 2, 3)$ is a prime factorization of 24, because $24 = 2 \times 2 \times 2 \times 3$),
- 309; (the list $(3, 103)$ is a prime factorization of 309);
- $3,895,207,331,689$. Here it would really take a lot of work to find the natural number k and the prime numbers $p_1, p_2, \ldots, p_k$ such that

$$3,895,207,331,689 = p_1 \cdot p_2 \cdot \cdots \cdot p_k .$$

But the prime factorization theorem guarantees to us that $3,895,207,331,689$ is a product of primes.□

2.4 Proofs by contradiction

Our proof if Euclid's theorem is going to be a ***proof by contradiction***

Proof by contradiction is probably the most important and most widely used of all proof strategies. So you should not only learn what proofs by contradiction are, but ***acquire the habit of always[a] seriously considering the possibility of using the proof by contradiction strategy when you are trying to figure out how to do a proof.***

[a]Sure, I am exaggerating a little bit. There are quite a few direct proofs (that is, proofs that are not by contradiction). But the number of proofs by contradiction is huge.

Let me first explain what proofs by contradiction are, and then I will tell you why they are so important.

And the first thing I need to explain is what a ***contradiction*** is.

And, ir order to explain that, I have to discuss how to *negate* a sentence.

2.4.1 Negation

To ***negate*** (or ***deny***) a statement A is to assert that A is false. (Any such statement is called a *denial* of A)

So, for example, a denial of "7 is a prime number" is "7 is not a prime number". (But there are many other ways to write a denial of "7 is a prime number." For example, we could write "it is not true that 7 is a prime number", or "it is not the case that 7 is a prime number".)

The symbol "$\sim$" ("it's not true that")

The symbol "$\sim$", put in front of a statement, is used to assert that the statement is false.

So "$\sim$" stands for "it is not the case that", or "it is not true that".

Example 3. The following sentences are true:

- $\sim$ 6 is a prime number (that is, "6 is not a prime number"),
- $\sim$ 2 is an odd integer (that is, "2 is not an odd integer"),
- $\sim$(6 is even and 7 is even) (that is, "it's not true that 6 and 7 are both even").

The following sentences are false:

- $\sim$ 7 is a prime number (that is, "7 is not a prime number"),
- $\sim$ 3 is an odd integer (that is, "3 is not an odd integer"),
- $\sim$(6 is even or 7 is even) (that is, "it's not true that 6 is even or 7 is even"),
- $\sim$ 6 is even and 7 is even (that is, "6 is not even and 7 is even").

2.4.2 When is a negation true?

If A is a sentence, then

- $\sim A$ is true if A is false;
- $\sim A$ is false if A is true.

2.4.3 What is a contradiction?

The precise definition of "contradiction" is complicated, and requires some knowledge of logic. So let me give you a simplified definition that is easy to understand and is good enough for our purposes.

Temporary, simplified definition of "contradiction": A contradiction is a statement of the form "A and $\sim A$", that is, "A is true and A is not true". □

Example 4

- The sentence "$2 + 2 = 7$" is ***not*** a contradiction. It is a false statement, of course, but not every false statement is a contradiction.
- The sentence "$2 + 2 = 7$ and $2 + 2 = 4$" is ***not*** a contradiction either. It is a false statement (because it is the conjunction of two sentences one of which is false), but that does not make it a contradiction.
- The sentence "$2 + 2 = 7$ and $2 + 2 \neq 7$" ***is*** a contradiction. because it is of the form "A and no A", with the sentence "$2 + 2 = 7$" in the role of A.
- The sentence "$n = 1$ and $n \neq 1$" is a contradiction.
- The sentence "John Adams was the first U.S. president" is false, but it ***not*** a contradiction.

- The sentence "John Adams was the first U.S. president and was the second U.S. president" is false, but it ***not*** a contradiction.
- The sentence "John Adams was the first U.S. president and was not the first U.S. president" ***is*** a contradiction. □

2.4.4 What is a proof by contradiction?

A ***proof by contradiction*** is a proof in which you start by assuming that the statement you want to prove is false, and you prove a contradiction. Once you have done that, you are allowed to conclude that the statement you are trying to prove is true.

To do a proof by contradiction, you would write something like this:

> We want to prove A.
>
> > Assume that A is false.
> > ⋮
> > $2 = 1$ and $2 \neq 1$.
> > And "$2 = 1$ and $2 \neq 1$" is a contradiction.
>
> So assuming that A is false has led us to a contradiction.
> Therefore A is true. **Q.E.D.**

WARNING

Having explained very precisely what a contradiction is, I have to warn you that mathematicians will often say things like " '$2 + 2 = 7$' is a contradiction".
This is not quite true, but when a mathematician says that every mathematician will understand what is really intended.
What the person who said " '$2 + 2 = 7$' is a contradiction" really meant is something like this:

> Now that I have proved that $2 + 2 = 7$, I can easily get a contradiction from that, because we all know how to prove that $2 + 2 \neq 7$, and then we can deduce from these two formulas the sentence "$2 + 2 = 7$ and $2 + 2 \neq 7$", which is truly a contradiction.
> In other words, once I get to "$2 + 2 = 7$", it is clear to me, and to every mathematician, how to get to a contradiction from there, so there is no need to go ahead and do it, so I can stop here.

This is something mathematicians do very often[a]: ***once we get to a point where it is clear how to go on and finish the proof, we just stop there.***

For a beginning student I would recommend that you actually write your proof until you get a real contradiction, because this is the only way to make it clear to the person reading (and grading) your work that you do understand what a contradiction is.

[a] And not only mathematicians! In chess, once you get to a position from which it is clear that you can take your rival's King and win, you say "checkmate" and the game stops there.

WHAT DOES "ASSUME" MEAN?

"Assume" means "imagine". In order to prove that some statement S is true, we imagine that it is not true, that is, we explore an imaginary world W in which S is not true, and we prove that in this imaginary world something impossible (such as a contradiction, "A is true and A is not true") would have to happen. And from this we draw the conclusion that a world in which S is not true is impossible, so in the real world S must be true.

2.5 What is a finite set? What is an infinite set?

We now explain what a "finite set" is.

Definition 6. Let S be a set,

1. We say that S is finite if there exist a natural number n and a finite list[5]

$$\mathbf{a} = (a_1, a_2, \ldots, a_n)$$

with n entries which is a list of all the members of S. (This means: *every member of S occurs in the*

[5]If you are wondering "what is a finite list?", then I can tell you two things: (1) you are asking a good question, (2) I will give you more information about "finite lists" later, on page 25.

list; that is, *for every member x of S there exists a natural number j such that $j \leq n$ and $x = p_j$.*)

2. We say that S is infinite if it is not finite.

□

2.5.1 A simple lemma

A lemma is a statement that one proves in order to use it in the proof of a theorem. In our proof of Euclid's Theorem we are going to need the following lemma:

Lemma 1. *If a, b, c are integers, and c divides both a and b, then c divides $a + b$ and $a - b$.*

Proof. Since $c|a$ and $c|b$, we may write

$$a = cj \text{ and } b = ck\,, \tag{2.2}$$

where j and k are integers.

But then

$$a + b = c(j + k) \text{ and } a - b = c(j - k)\,, \tag{2.3}$$

and $j + k$ and $j - k$ are integers. So $c|a + b$ and $c|a - b$. **Q.E.D.**

2.6 The proof of Euclid's Theorem

The proof I am going to present here is not exactly Euclid's, but is based essentially on the same idea.

First, here is Euclid's result, again:

Theorem 1. *The set of prime numbers is infinite.*

And here is the proof.

Let S be the set of all prime numbers.
We want to prove that S is an infinite set.
We will prove this by contradiction.

Suppose S is not infinite.

Then S is a finite set.

Since S is finite, we may write a finite list

$$\mathbf{p} = (p_1, p_2, \ldots, p_n)$$

of all the members of S, i.e., of all the prime numbers.

Let $N = p_1.p_2.\cdots.p_n$. (That is, N is the product of all the entries of the list $\mathbf{p}$.)

Let $M = N + 1$.

Then $M \geq 2$, so by the prime factorization theorem (in section 2.3.2) M is a product $q_1.q_2.\cdots.q_k$ of prime numbers.

Then q_1 is a prime number[6], and $\boxed{q_1 \text{ divides } M}$ (because $M = q_1 u$, if $u = q_2.q_3.\cdots.q_k$).

[6]All we need here is to have a prime number that divides M. We choose q_1, but we could equally well have chosen q_2, or any of the other q_j.

On the other hand, since **p** is a list of all the prime numbers, and q_1 is a prime number, we can conclude that q_1 is one of the entries $p_1, p_2, \ldots, p_n$ of the list **p**.

So we may write

$$q_1 = p_j \,,$$

where j is one of the nmbers $1, 2, \ldots, n$.

It follows that $\boxed{q_1 \text{ divides } N}$ (because p_j divides N and $q_1 = p_j$).

Since q_1 divides M and q_1 divides N, it follows that q_1 divides $M - N$, by Lemma 1.

But $M - N = 1$. So $\boxed{q_1 \text{ divides } 1}$.

On the other hand, q_1 is prime. It then follows from the definition of "prime number" (Definition 2, on page 11) that $q_1 > 1$.

Hence $q_1 \neq 1$.

But then $\boxed{q_1 \text{ does not divide } 1}$, because the only natural number that divides 1 is 1.

So $\boxed{q_1 \text{ divides } 1 \text{ and } q_1 \text{ does not divide } 1}$, which is a contradiction.

Hence the assumption that S is not an infinite set has led us to a contradiction.

Therefore $\boxed{S \text{ is an infinite set}}$. **Q.E.D.**

2.6.1 What is "Q.E.D."?

What does "Q.E.D." mean?

"Q.E.D." stands for the Latin phrase *quod erat demonstrandum*, meaning "which is what was to be proved". It is used to indicate the end of a proof.

Appendix: Finite lists

Finite lists have ***entries***. Sets have ***members***.

We can write[7] finite lists as follows:

1. First we write a left parenthesis, i.e., the symbol "(".
2. Then we write the names of the entries of the list, in order, beginning with entry number 1, then entry number 2, and so on. The entries must be separated by commas.
3. Then, finally, write a right parenthesis, i.e., the symbol ")".

And we can write finite sets as follows:

1. First we write a left brace, i.e., the symbol "{".
2. Then we write the names of the members of the set, in some order, separated by commas.

[7] I am saying "we can write" rather than "we write" because there are other ways to write lists and sets. We will discuss those ways later.

3. Then, finally, we write a right brace, i.e., the symbol "}".

WARNING
Be careful with the distinction between ***sets***, written with braces ("{" and "}") and ***lists***, written with parentheses ("(" and ")"). For example, the sentence $$(1, 2, 3) = (3, 1, 2)$$ is false, but the sentence $$\{1, 2, 3\} = \{3, 1, 2\}$$ is true.

Example 5.

- Here is the list **a** of the first ten natural numbers, in increasing order:

$$\mathbf{a} = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10)\,. \tag{2.4}$$

- Here is the list **b** of the first ten natural numbers, in decreasing order:

$$\mathbf{b} = (10, 0, 8, 7, 6, 5, 4, 3, 2, 1)\,. \tag{2.5}$$

And here is a list $\mathbf{c}$ of the first ten natural numbers, in a different order:

$$\mathbf{c} = (10, 1, 5, 8, 3, 2, 4, 9, 6, 7)\,. \tag{2.6}$$

These three lists are different. For example, the second entry of $\mathbf{a}$ is 2, whereas the second entry of $\mathbf{b}$ is 9 and that of $\mathbf{c}$ is 1.

Now let S be the set whose members are the first ten natural numbers. Then we can write

$$S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}\,, \tag{2.7}$$

or

$$S = \{10, 9, 8, 7, 6, 5, 4, 3, 2, 1\}\,, \tag{2.8}$$

or, for example,

$$S = \{1, 3, 5, 7, 9, 2, 4, 6, 8, 10\}\,, \tag{2.9}$$

or

$$S = \{4, 2, 7, 8, 10, 1, 9, 3, 5, 6\}\,, \tag{2.10}$$

or even

$$S = \{4, 4, 2, 7, 7, 7, 5, 5, 5, 8, 10, 1, 9, 4, 3, 5, 6\}\,. \tag{2.11}$$

The sets S given by equations (2.7), (2.8), (2.9), (2.10), (2.11), are all the same set, even though the formulas describing them are different. What

the formulas do is tell us who the members of the set are. So, for example, according to formula (2.7), 1 is a member of S, and 23 is not. And the other formulas also say that 1 is a member of S, and 23 is not.

The key facts are these:

- Two sets S, T are the same set if they have the same members, that is, if every member of S is a member of T and every member of T is member of S.
- Two lists $\mathbf{a}$, $\mathbf{b}$ are the same if the first entry of $\mathbf{a}$ is the same as the first entry of $\mathbf{b}$, the second entry of $\mathbf{a}$ is the same as the second entry of $\mathbf{b}$, and so on. That is, $\mathbf{a} = \mathbf{b}$ if the j-th entry of $\mathbf{a}$ is the same as the j-th entry of $\mathbf{b}$ for every j.

Example 6. Let S be the set whose members are all the presidents of the United States, from George Washington to Donald Trump.

Let $\mathbf{a}$ be the list of all the presidents of the United States, from George Washington to Donald Trump, in chronological order, so

$$\mathbf{a} = (a_1, a_2, \ldots, a_{45}),$$

where, for $j = 1, 2, \ldots, 45$, a_j is the j-th U.S. president.

Then $\mathbf{a}$ has 45 entries. How many members does S have?

If you think that the answer is 45, think again!

It turns out that Grover Cleveland served two non-consecutive terms as president, from 1885 to 1889 and from 1893 to 1897, and Congress decided that Cleveland would count as both the 22nd and the 24th president of the United States. So in the list $\mathbf{a}$, the 22nd entry a_{22} and the 24th entry a_{24} are equal. So the set S has in fact 44 members, even though the list $\mathbf{a}$ has 5 entries. □

2.7 An analogy: twin primes

Let me tell you about another problem, very similar to the one we have just discussed, for which the situation is completely different.

Definition 7. A twin prime is a prime number p such that $p + 2$ is also prime. □

Example 7. Here are the first few twin primes:

$$3,\ 5,\ 11,\ 17,\ 29,\ 41,\ 59,\ 71,\ 101,\ 107\ .$$ □

Now we can ask the same question that we asked for primes: does the list go on forever, or does it stop at some largest pair of twin primes?

In other words,

Are there infinitely many twin primes?

This looks very similar to the question whether there are infinitely many primes. And yet, the situation in this case is completely different:

> Nobody knows whether there are infinitely twin primes. Mathematicians have been trying for more than 2,000 years to solve this problem, by proving that there are infinitely many twin primes, or that that there aren't, and so far they haven't been successful.

The twin prime conjecture is the statement that there are infinitely many pairs of twin primes. It was formulated by Euclid, about 2,300 years ago, and it is still an open problem.

THE LARGEST KNOWN TWIN PRIME

According to *Wikipedia*, as of September 2018, the current largest twin prime known was $2996863034895 \times 2^{1290000} - 1$, with $388,342$ decimal digits. It was discovered in September 2016. (The fact that the number $2996863034895 \times 2^{1290000} - 1$ is a twin prime means that it is prime, and the number $2996863034895 \times 2^{1290000} + 1$ is also prime.)

2.8 A surprising fact: non-twin primes

How about primes that are *not* twin?

Definition 8. A non-twin prime is a prime number p such that $p + 2$ is not prime. □

Example 8. Here are the first few non-twin primes:

2, 7, 13, 19, 23, 31, 37, 43, 47, 53,
61, 67, 73, 79, 83, 89, 97, 103 . □

And now we can ask, again, the same question that we asked for primes and for twin primes: does the list go on forever, or does it stop at some largest pair of twin primes?

In other words,

Are there infinitely many non-twin primes?

This looks very similar to the question whether there are infinitely many twin primes. And yet, the situation in this case is completely different: it is very easy to prove the following:

Theorem 2. *The set of non-twin primes is infinite.*

(I am asking you to do this proof. See Problem 8 below.)

2.9 Problems

Problem 1. Using the definition of "divides" (Definition 1), explain precisely why the statements "1 divides 5", "6 divides -6", "6 divides 0", and "0 divides 0" are true, and the statements "$5|6$" and "$0|6$" are false. □

Problem 2. Indicate which of the statements in the following list are true and which ones are false, and explain why. (That is, prove that the true statements are true and the false ones are false.)

1. Every integer is divisible by 1.
2. Every integer is divisible by 2.
3. Every integer is divisible by 0.
4. Every integer divides 1.
5. Every integer divides 2.
6. Every integer divides 0.

Problem 3. Express each of the following numbers

- 37,
- 28,
- 236,
- 2247,

as a product of prime numbers. □

Problem 4. Give a precise mathematical definition of "prime number". □

Problem 5. Give a precise mathematical definition of "twin prime". □

Problem 6. Give a precise mathematical definition of "finite set" and "infinite set". □

Problem 7. Give precise mathematical definitions of each of the following concepts:

- divides,
- is divisible by,
- factor (as in "is a factor of"),
- multiple (as in "is a multiple of"). □

Problem 8. ***Prove*** Theorem 2 (on page 31). □

Problem 9. ***Prove*** that if a, b, c are integers, $a|b$ and $b|c$, then $a|c$. □

Problem 10. ***Prove*** that if a, b are integers, $a|b$ and $b|a$, then $a = b$ or $a = -b$. □

Problem 11. The proof that was given in Section 2.6 of Euclid's Theorem uses the definition of "prime number" given on page 11. In this problem, we change the definition of "prime number" and use the following definition:

A prime number is a natural number p such that p is not divisible by any natural numbers other than 1 *and* p*.* That is, we do not require p to be > 1. So according to this new definition 1 is now prime

Rewrite the proof of Euclid's Theorem given in Section 2.6 using the new definition of "prime number". (What you have to do is basically copy the proof, but making a few changes. For example, one of the steps of the proof given in Section 2.6 says "It follows from the definition of 'prime number' that $q_1 > 1$". This step is not valid now, because 1 is prime, so q_1 could be 1. You have to make some slight changes in the proof to adapt it to this new situation.) □

Problem 12. ***Prove*** that if p is a prime number and $p \neq 2$ then p is odd.

In the following problems, you may want to use the division theorem: ***If*** a, b ***are integers and*** $b \neq 0$***, then it is possible to write*** $a = bq + r$***, where*** q, r ***are integers such that*** $0 \leq r < |b|$***.*** (For example: if a is an integer then we can write $a = 3q + r$ where $r = 0$ or $r = 1$ or $r = 2$.)

Problem 13. ***Prove*** that if p is a prime number such that $p + 2$ and $p + 4$ are also prime, then $p = 3$.

Problem 14.

1. ***Find*** at least ten different prime numbers p such that $p + 4$ is also prime.
2. ***Prove*** that the only prime number p such that $p+4$ and $p + 8$ are also prime is $p = 3$.
3. ***Prove*** that there does not exist a prime number p such that $p + 4$, $p + 8$ and $p + 12$ are also prime.

Problem 15.

1. ***Find*** at least ten different prime numbers p such that $p + 6$ is also prime.
2. ***Find*** at least ten different prime numbers p such that $p + 6$ and $p + 12$ are also prime.
3. ***Find*** at least four[8] different prime numbers p such that $p + 6$, $p + 12$ and $p + 18$ are also prime.
4. ***Prove*** that there exists a unique prime number p such that $p + 6$, $p + 12$, $p + 18$ and $p + 24$ are also prime.
5. ***Prove*** that there does not exist a prime number p such that $p+6$, $p+12$, $p+18$, $p+24$ and $p+30$ are also prime.

[8]There are many more. I am just asking you to find four because I don't want to make you work too hard.

Problem 16.

1. ***Express*** the integer 28 as a difference of two squares of integers. (That is, ***find*** two integers m, n such that $m^2 - n^2 = 28$.)
2. ***Express*** the integer 29 as a difference of two squares of integers. (That is, ***find*** two integers m, n such that $m^2 - n^2 = 29$.)
3. ***Prove*** that it is not possible to express the integer 30 as a difference of two squares of integers. (That is, ***prove*** that there do not exist two integers m, n such that $m^2 - n^2 = 30$.) $\square$

3 More examples of proofs: irrationality of $\sqrt{2}$ and of other numbers

3.1 Numbers and number systems

There are several different kinds of numbers, i.e., several different number systems. It is convenient to give the number systems *names*, and to introduce mathematical symbols to represent them.

3.1.1 The most common types of numbers

Here are some examples of number systems:

- the symbol $\mathbb{N}$ stands for the set of *natural numbers*,
- the symbol $\mathbb{Z}$ stands for the set of *integers*,
- the symbol $\mathbb{Q}$ stands for the set of *rational numbers*,
- the symbol $\mathbb{R}$ stands for the set of *real numbers*,
- the symbol $\mathbb{C}$ stands for the set of *complex numbers*,
- there are sets $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_6$, and, more generally, $\mathbb{Z}_n$—the set of *integers modulo* n—for every natural number n such that $n \geq 2$. (So, for example, there are the systems $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_{10}$, $\mathbb{Z}_{11}$, $\mathbb{Z}_{5403}$.)

Some of the above kinds of numbers should be familiar to you, and others may be less so or not at all. Do not worry if you find on our list things that you have never

heard of before: we will be coming back to the list later, and discussing all the items in much greater detail.

A number can belong to different number systems, in the same way as, say, a person can belong to different associations. (For example, somebody could be a member, say, of the American Association of University Professors, the Rutgers Alumni Association, and the Sierra Club. Similarly, the number 3 belongs to lots of different number systems, such as, for example, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$.)

At this point, we will just discuss $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$, and we will do so very briefly. We will talk much more about these systems later, and we will also discuss later other number systems such as $\mathbb{C}$, and the $\mathbb{Z}_n$.

The symbols $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, are *special mathematical symbols*. They are *not* the capital letters N, Z, Q, R, C.

(Why do we use these special symbols? It's because mathematicians need to use lots of letters in their proofs, so they do not want to take the letters C, R, for example, and declare once and for all that they stand for "the set of all complex numbers" and "the set of all real numbers". For example, if they are working with a circle, they want to have the freedom to call the circle "C", and to say "let R be the radius of C", and this would not be allowed if

the symbols "C", "R" already stood for something else. So they invented the special symbols $\mathbb{C}$, $\mathbb{R}$ to stand for the set of complex numbers and the set of real numbers, so that the ordinary letters C, R, will be available to be used as variables.)

Please do not say "$\mathbb{N}$ is the natural numbers", or "$\mathbb{Z}$ is the integers". When we group things together to create a set, that set is one thing, not many things. So $\mathbb{N}$ cannot be "the natural numbers". What you can, and should, say is: "$\mathbb{N}$ is the set of all natural numbers."

3.1.2 The symbol "$\in$"

If S is a set and a is an object, we write

$$a \in S$$

to indicate that a is a member of S.

And we write

$$a \notin S$$

to indicate that a is not a member of S.

How to read the "$\in$" symbol

The expression "$a \in S$" is read in any of the following ways:

- a belongs to S,
- a is a member of S,
- a is in S.

The expression "$a \notin S$" is read in any of the following ways:

- a does not belong to S,
- a is not a member of S,
- a is not in S.

Remark 2 Sometimes, "$a \in S$" is read as "a belonging to S", or "a in S", rather than "a belongs to S", or "a is in S." For example, if we write

$$\text{Pick an } a \in S,$$

then it would be bad English grammar to say "pick an a belongs to S". But "pick an a belonging to S", "pick an a in S", or "pick an a that belongs to S", are fine. $\square$

Never read "$\in$" as "is contained in", or "is included in". The words "contained" and "included" have different meanings, that will be discussed later.

3.1.3 The natural numbers

The symbol $\mathbb{N}$ stands for the set of all *natural numbers*. (Natural numbers are also called "positive integers", or—sometimes—"whole numbers", or "counting numbers".) The members of this set are the numbers $1, 2, 3 \ldots$.

More precisely:

The **natural numbers** are the numbers obtained from the number 1 by adding 1 any number of times. So, for example, the numbers 1, $1 + 1$ (i.e., 2), $1+1+1$ (i.e., 3), $1+1+1+1$ (i.e., 4), are natural numbers. And so are the numbers $4,503$, $46,902,444,531,322$ and $10^{10^{10^{10}}}$.
The symbol $\mathbb{N}$ stands for **the set of all natural numbers**.

3.1.4 The integers

The symbol $\mathbb{Z}$ stands for the set of all *integers*.

The members of $\mathbb{Z}$ (i.e., the integers) are the natural numbers as well as 0 and the negatives of natural numbers, i.e., the numbers -1, -2, -3, etc. So, to say that a number n is an integer, we can write "$n \in \mathbb{Z}$", which we read as "n belongs to the set of integers" or, even better, as "n is an integer".

So, for example, the following statements are true:

$$\begin{aligned} 35 &\in \mathbb{N} \\ 35 &\in \mathbb{Z} \\ \sim -35 &\in \mathbb{N} \\ -35 &\in \mathbb{Z} \\ 35 &\notin \mathbb{Z} \\ 0 &\in \mathbb{Z} \\ \sim 0 &\in \mathbb{N} \\ 0 &\notin \mathbb{N} \\ 0.37 &\notin \mathbb{Z} \\ \pi &\notin \mathbb{Z} \quad . \end{aligned}$$

3.1.5 The real numbers

The symbol $\mathbb{R}$ stands for the set of all *real numbers*.

The real numbers are those numbers that you have used in Calculus. They can be positive, negative, or zero.

The positive real numbers have an "integer part", and

then a "decimal expansion" that may terminate after a finite number of steps or may continue forever. (So, for example, the number 4.23 is a real number, and so is the number π. The decimal expansion of the number 4.23 terminates after two decimal figures, but the decimal expansion of π goes on forever. Here, for example, is the decimal expansion of π with 30 decimal digits:

$$3.14159265358979323846264338327\,9\,.$$

Using Google you can find π with one million digits. As of 2011, 10 trillion digits of π had been computed, and nobody has found any pattern! Even simple questions, such as whether every one of the digits $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ appears infinitely many times, are unresolved.)

And the negative real numbers are the negatives of the positive real numbers. So, for example, -4.23 and $-\pi$ are negative real numbers.

3.1.6 Positive, negative, nonnegative, and nonpositive numbers

In this course, "positive" means "> 0" (i.e., "greater than zero"), and "nonnegative" means "≥ 0" ("greater than or equal to zero"). So, for example, 3 and 0.7 are positive (and nonnegative), and 0 is nonnegative but not positive.

Similarly, "negative" means "< 0", and "nonpositive" means "≤ 0". So, for example, -3 and -0.7 are negative

(and nonpositive), 0 is nonpositive but not negative.

3.1.7 Subsets

A set A is a **subset** of a set B if every member of A is a member of B. We write $A \subseteq B$ to indicate that A is a subset of B.

For example,

a. If S is the set of all people in the world. and T is the set of all people who live in the United States, then T is a subset of S. So the sentence "$T \subseteq S$" is true.

b. If A is the set of all animals, and G is the set of all giraffes, then G is a subset of A, so the sentence "$G \subseteq A$" is true.

c. Let S be the set of all people who live in the United States, and let C be the set of all U.S. citizens. Is C a subset of S? The answer is "no", because there are U.S. citizens who do not live in the U.S., so these people are members of C but not of S, so it's not true that every member of C belongs to S.

And here are some mathematical examples:

I. The following sentences are true:

$$\mathbb{N} \subseteq \mathbb{Z}\,,$$
$$\mathbb{N} \subseteq \mathbb{R}\,,$$
$$\mathbb{Z} \subseteq \mathbb{R}\,,$$

because every natural number is an integer, every natural number is a real number, and every integer is a real number.

II. And the following sentences are false:

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

(For example, it is not true that $\mathbb{Z} \subseteq \mathbb{N}$, because not every integer is a natural number since, for example, $0 \in \mathbb{Z}$ but $0 \notin \mathbb{N}$.)

3.1.8 The word "number", in isolation, is too vague

As we have seen, there are different kinds of numbers. So, if you just say that something is a "number", without specifying what kind of number it is, then this is too vague. In other words,

Never say that something is a "number", unless you have made it clear in some way what kind of "number" you are talking about.

For example, suppose you are asked to define "divisible", and you write:

> A number a is divisible by a number b if we can write $a = bc$ for some number c.

This is too vague! What kind of "numbers" are we talking about? Could they be real numbers?. If this was the case, then 3 would be divisible by 5, because $3 = 5.z$, if we take $z = 3/5$. But we do not want 3 to be divisible by 5. And we want the "numbers: we are talking about to be integers.

So here is a correct definition of "divisible":

Divisibility of integers: We say that an integer a is divisible by an integer b (or that a is a multiple of b, or that b is a factor of a, or that b divides a), if we can write

$$a = bc$$

for some integer c. □

For example, the following sentences are true:

$$3 \text{ divides } 6\,,$$
$$-3 \text{ divides } 6\,,$$

$$6 \text{ is divisible by } 3\,,$$
$$6 \text{ is a multiple of } 3\,,$$
$$3 \text{ is a factor of } 6\,.$$

3.2 Existential statements

In the definition of divisibility given above, we have used the words "we can write". This language makes it sound as though, in order to decide whether, say, 3 divides 6, we need to have somebody there who "can write" things. This should not be necessary: "3 divides 6" would be a true sentence even if there was nobody around to do any writing. So it is much better to use a more impersonal language:

Divisibility of integers

DEFINITION. An integer a is divisible by an integer b (or a is a multiple of b, or b is a factor of a, or b divides a), if there exists an integer c such that

$$a = bc\,.$$

The sentence "there exists an integer c such that $a = bc$" is an example of nn **existential sentence**, i.e., a sentence that asserts that an object of a certain kind

exists. Later, when we learn to write mathematics in formal language (that is, using only formulas), we will see that this sentence can be written as follows:

$$(\exists c \in \mathbb{Z})a = bc\,. \tag{3.12}$$

The symbol "$\exists$" is the **existential quantifier symbol**, and the expression "$(\exists c \in \mathbb{Z})$" is an **existential quantifier**, and is read as "there exists an integer c such that".

So Sentence (3.12) is read as "there exists an integer c such that $a = bc$". And it can also be read as "$a = bc$ for some integer c", or "it is possible to pick an integer c such that $a = bc$". (I recommend the "it is possible to pick ..." reading.)

3.2.1 The rule for using existential statements (Rule $\exists_{use}$)

Suppose you know that cows exist, that is that

$$(\exists x)x \text{ is a cow}\,. \tag{3.13}$$

Then the rule for using existential statements says that we can introduce into our conversation a cow, and give her name, by saying something like "pick a cow and call her Suzy".

In general,

- For a sentence $(\exists x)P(x)$, a witness is an object a such that $P(a)$. (For example: for the sentence (3.13), a witness is any a such that a is a cow, that is, any cow.)

- For a sentence $(\exists x \in S)P(x)$, a witness is an object a which belongs to S and is suchthat $P(a)$. (For example, if C is the set of all cows, then a witness for the sentence $(\exists x \in C)x$ is brown is any brown cow.)

The ***rule for using existential statements*** (Rule $\exists_{use}$) says that, ***if you know that an existential statement is true, then you can "pick a witness and give it a name".***

For example: suppose you know that a natural number n is not prime and is > 1. Then you know that the following is true: $(\exists m \in \mathbb{N})(m|n$ and $m \neq 1$ and $m \neq n)$. (That is, n has a factor which is a natural number and is not equal to 1 or n.) Then Rule $\exists_{use}$ says that we can pick a witness and call it a, that is, we can pick a natural number a such that $a|n$, $a \neq 1$ and $a \neq n$.

Rule $\exists_{use}$

- From
$$(\exists x)P(x)$$
you can go to "Let w be a witness for $(\exists x)P(x)$, so $P(w)$," or "Pick a witness for $(\exists x)P(x)$ and call it w", or "Pick a w such that $P(w)$."

- From
$$(\exists x \in S)P(x)$$
you can go to "Let w be a witness for $(\exists x \in S)P(x)$, so $w \in S$ and $P(w)$," or "Pick a witness for $(\exists x \in S)P(x)$ and call it w", or "Pick a w such that $w \in S$ and $P(w)$."

For example:

i. If you know that Polonius has been killed, but you do not know who did it, then you can talk about the person who killed Polonius and give a name to that person, for example, call him (or her) "the killer".

ii. if you know that an equation (say, the equation $3x^2 + 5x = 8$) has a solution (that is, you know that the existential statement "there exists a real number x

such that $3x^2+5x = 8$" is true) then you are allowed to pick a solution and call it, for example[9], "a".

3.3 Pythagoras' Theorem and two of its proofs

Pythagoras' Theorem is one of the oldest and most important theorems in Mathematics. It is named after the Greek mathematician and philosopher Pythagoras, who lived approximately from 570 to 495 BCE, although there is a lot of evidence that the theorem (but probably not the proof) was known before, by the ancient Babylonians.

The statement of the theorem is as follows:

Theorem 3. (Pythagoras' Theorem) *If T is a right triangle*[10]*, c is the length of the hypothenuse*[11] *of T, and a, b are the lengths of the other two sides, then*

$$a^2 + b^2 = c^2 \,. \tag{3.14}$$

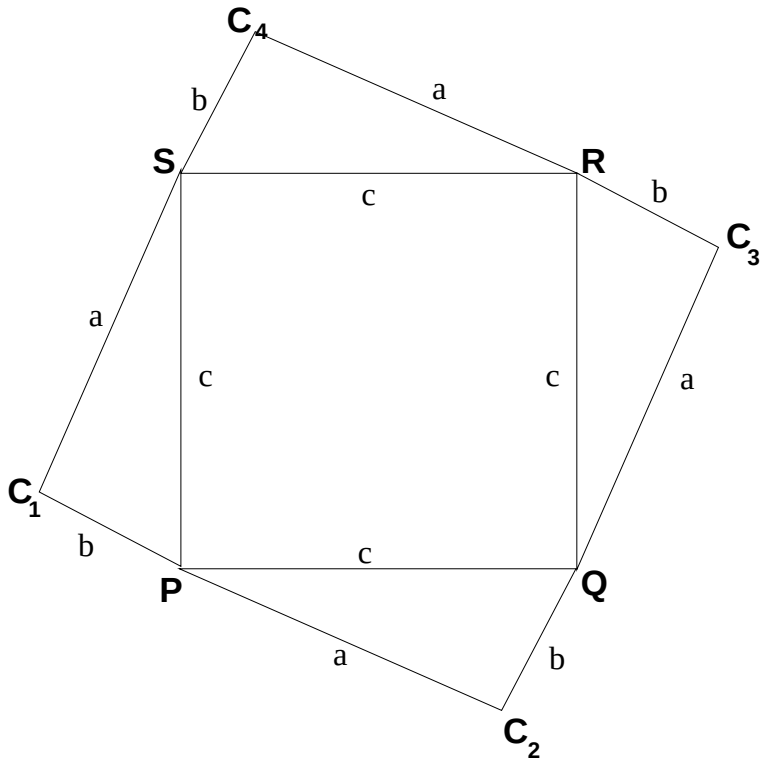
There are many different proofs of Pythagoras' Theorem. I am going to give you two proofs.

[9] Can you call this solution x? This is a complicated issue. Think of this as follows: the letter x is really a slot where you can put in a number. A number that can be put in the slot so as to make the formula true is called a "solution". The solution and the slot are two different things. So it is not a good idea to use the same name for both. If you do things *very* carefully, it turns out that it is O.K. to call both the slot and a solution with the same name, but I strongly recommend that you do not do it. For example the equation $3x^2 + 5x = 8$ has are two solutions, namely, 1 and $-\frac{8}{3}$. Which one is "x"? You cannot call both of them "x", because they are different. So I think it is better to call one of the solutions a (or A, or u, or U, or p, or P, or α, or $\heartsuit$) and then call the other one a different name (say b, or B, or v, or V, or q, or Q, or β, or $\clubsuit$).

[10] A right triangle is a triangle having one right angle

[11] The hypothenuse of a right triangle T is the side opposite to the right angle of T.

Pythagoras' proof. We draw a $c \times c$ square $PQRS$, and then attach at each side a copy[12] of T as shown in the picture.



The point P lies on the straight line segment from C_1 to C_2, because

1. If α_1 is the angle at S of the triangle SC_1P, and α_2 is the angle at P of the triangle PC_2Q, then $\alpha_1 = \alpha_2$,

[12]For those who have studied Euclidean Geometry in high school: a copy of a figure F is a figure F' congruent to F. "Congruent to F" means: "obtainable from F by combining displacements and rotations. For example, the triangles QC_3R, RC_4S, and SC_1P are all congruent to PC_2Q.

because the triangles SC_1P and PC_2Q re congruent.

2. Similarly, if β_1 is the angle at P of the triangle SC_1P, and β_2 is the angle at Q of the triangle PC_2Q, then $\beta_1 = \beta_2$, because the triangles SC_1P and PC_2Q are congruent.

3. Since SC_1P and PC_2Q are both right triangles, and the sum of the angles of every triangle is 180^o, we have

$$\alpha_1 + \beta_1 + 90^o = 180^o \text{ and } \alpha_2 + \beta_2 + 90^o = 180^o\,,$$

so

$$\alpha_1 + \beta_1 = 90^o \text{ and } \alpha_2 + \beta_2 = 90^o\,.$$

4. Since $\alpha_1 = \alpha_2$, it follows that $\alpha_2 + \beta_1 = 90^o$,

5. Hence the angle θ between the segments PC_1 and PC_2 is equal to $\alpha_2 + 90^o + \beta_1$, i.e., to 180^o. This proves that the segments PC_1 and PC_2 lie on the same straight line, so P lies on the segment C_1C_2.

A similar argument shows that Q lies on the segment C_2C_3, R lies on the segment C_3C_4, and S lies on the segment C_4C_1.

So the polygonal $C_1PC_2QC_3RC_4SC_1$ is a square.

Let $d = a+b$. Then the sides of the square $C_1C_2C_3C_4$ have length d.

Therefore the area of the square $C_1C_2C_3C_4$ is d^2.

On the other hand, the smaller square $PQRS$ has side of length c, so its area is c^2. Each of the four triangles has area $\frac{ab}{2}$. So the area of $C_1C_2C_3C_4$ is equal to $c^2 + 4 \times \frac{ab}{2}$, i.e., to $c^2 + 2ab$.

It follows that

$$\begin{aligned} (a+b)^2 &= d^2 \\ &= c^2 + 4 \times \frac{ab}{2} \\ &= c^2 + 2ab\,. \end{aligned}$$

On the other hand, $(a+b)^2 = a^2 + b^2 + 2ab$. It follows that

$$a^2 + b^2 + 2ab = c^2 + 2ab\,.$$

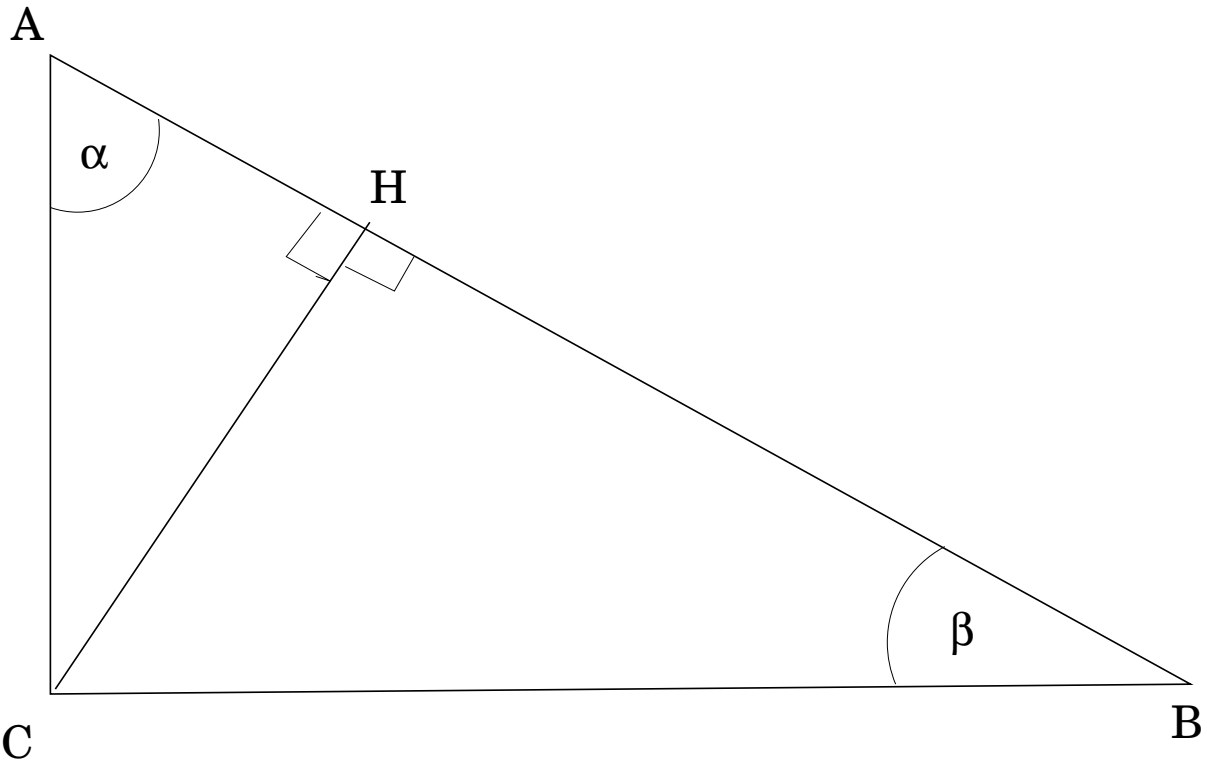
Subtracting $2ab$ from both sides, we get

$$a^2 + b^2 = c^2\,,$$

which is the desired result. **Q.E.D.**

Proof using similar triangles. Let C be the vertex of T where the right angle is located, and let A, B be the other two vertices.

Draw a line through C perpendicular to the line AB, and let H be the point where this line intersects the line AB.



Let α, β be the angles of T at A, B, so $\alpha + \beta = 90^o$. The angle of ACH at H is also 90^o, and the angle at A is α. Hence the angle of ACH at C is β. So the triangles ABC and ACH are similar. Hence the sides opposites to equal angles are proportional. That is:

$$\frac{|AC|}{|AH|} = \frac{|AB|}{|AC|}\,,$$

from which it follows that

$$|AC|^2 = |AH| \cdot |AB|\,.$$

A similar argument shows that

$$|BC|^2 = |BH| \cdot |AB| \,.$$

Adding both equalities we get

$$\begin{aligned} a^2 + b^2 &= |AH| \cdot |AB| + |HB| \cdot |AB| \\ &= \Big(|AH| + |HB|) \cdot |AB| \\ &= |AB| \cdot |AB| \\ &= |AB|^2 \\ &= c^2 \,. \end{aligned}$$

So $a^2 + b^2 = c^2$, as desired. **Q.E.D.**

3.4 Irrational numbers

In this section we will prove a very important fact, namely, that "the number $\sqrt{2}$ is irrational". This means, roughly, the same thing as "there does not exist a rational number r such that $r^2 = 2$." (The two statements do not say exactly the same thing. I will discuss how they differ later.)

But first I want to explain what this means and why this result is so important. And to do this we need a small philosophical digression into the question: ***what is a "number"?***. (If you are not interested in philosophical questions, you may skip this discussion and move on to subsection 3.4.4.)

3.4.1 What are "numbers"?

We have already been talking quite a bot about "numbers", but I never told you what a "number" is. The question "what is a number?" is not an easy one to answer, and I will not even try. But there are some tings that can be said.

1. ***Numbers*** are, basically, tags (or labels) that we use to specify the amount or quantity of something, i.e., to answer the questions "how much ...?" or "how many ...?"

2. Since ancient times, it was understood that there are at least two kinds of "numbers":

   (a) The ***counting numbers***, that we use to specify amounts of discrete quantities, such as coins, people, animals, stones, books, etc.

   - counting numbers are used to ***count***: 1, 2, 3, 4, 5, and so on,
   - they are the ones that ***answer questions of the form "how many ... are there?"***;
   - they ***vary in discrete steps***: they start with the number 1, then they "jump" from 1 to 2, and there is no other counting number between 1 and 2, then they "jump" from 2

to 3, and there is no other counting number between 2 and 3, and so on.

(b) The ***measuring numbers***, that we use to specify amounts that can vary continuously, such as lengths, areas, volumes, weights.

- measuring numbers are used to ***measure*** continuously varying quantities;
- they are the ones that ***answer questions of the form "how much ... is there?"***;
- they ***vary continuously***, so that, for example, when you pour water into a cup, if at some time point there are 10 ounces in the cup, and later there are 12 ounces, it does not occur to us that the amount of water in the cup may have jumped directly from 10 to 12 ounces: we understand that at some intermediate time there must have been 11 ounces, and at some time before that there must have been 10.5 ounces, and at some time before that there must have been 10.25 ounces, and at some time before the amount of water in the cup was 10.153098341832189504[82] ounces; and so on[13]. At no time did the amount of water

[13]WARNING: The words "and so on" here are very imprecixse. It's not at all what they mean. When I talk about the counting numbers and I write "1, 2, 4, 5, and so

"jump"[14] from some value u to some larger value v.

- they ***can be subdivided indefinitely***: for example
  - You can take a segment of length 1 (assuming we have fixed a unit of length), and divide it into seven equal segments, each one of which has length $\frac{1}{7}$. And then you can draw segments whose lengths are $\frac{3}{7}$, or $\frac{4}{7}$, or $\frac{9}{7}$, or $\frac{23}{7}$, thus getting fractional lengths.
  - And, instead of 7, you can use any denominator you want, and get lengths such as $\frac{5}{2}$, $\frac{12}{5}$, $\frac{29}{17}$, $\frac{236{,}907}{189{,}276}$, and so on.
  - Hence, if n and m are any natural numbers, then we can (at least in principle) construct segments of length $\frac{m}{n}$. That is, we can construct segments of length f, for any fraction f.

---

on", you know exacrtly what comes next: it's 6. But when I write "11, 10.5, 10.25, 10.153098341832189504 82, and so on", I haven't the faintest idea what comes next! So the "and so on" for counting numbers is acceptable, but the "and so on" for measuring numbers is not, and when we do things rigorusly and precisely we must get rid of it.

[14] To make this precise, one needs to use tha language of Calculus: if $w(t)$ is the amount of water at time t, then w is a ***continuous function*** of t. The trouble with this is: at this point you only have a nonrigorous, not very precise idea of what a "continuous function" is. You will learn to define the notion of "continuous function", and work with it, and prove things about it, in your next "Advanced Calculus" or "Real Analysis" course.

The measuring numbers such as $\frac{5}{2}$, $\frac{12}{5}$, $\frac{29}{17}$, or $\frac{236{,}907}{189{,}276}$, that can obtained by dividing a counting number m into n equal parts, where n is another counting number, are called ***fractions***.

And this suggests an idea:

Idea 1: *Perhaps the measuring numbers are exactly the same as the fractions.*

In other words: suppose we use the length u of some straight-line segment U as the unit for measuring length. (That is, we call the lenght of this segment "meter", or "yard", or "foot", or "mile", and then we try to express every length in meters, or yards, or feet, or miles.) When we do that, we will of course need fractions to expres some lenghts because, for example, if we measure distances in miles, not every distance will be 1 mile, or 2 miles, or n miles for some counting number n. Some distances will be, say, half a mile, or three quarters of a mile, on thirteen hundredths of a mile, or forty-seven thousandths of a mile[15].

[15]Here is another important difference between counting and measuring numbers: to count things using counting numbers you do not need units, but to measure amounts using measuring numbers you do. If you are asked how many pills there are in a bottle, then you answer "six", or "twenty-five', or whatever, and nobody is going to ask "six what?". But if you are asked how much water there are in the bottle, and you answer "six", then somebody is going to ask "six what?", expecting that you will say something like "six ounces", or "six liters", because if you do not specify the units of your measurement the number you gave is meaningless.

Then Idea 1 suggests that the length of every segment V should be equal to a fraction $\frac{m}{n}$ times u (wnere m, n are natural numbers, i.e., counting numbers). That means that if we divide the segment U into n equal segments of length $w = \frac{u}{n}$, then the length of U is n times w, and the length of V is m times w. So U and V are commensurable. Since we can take U and V to be any two segments we want, we find that ***If Idea 1 i true, then any two segments are commensurable.***

COMMENSURABLE LENGTHS

"Commensurable" means "measurable together". Precisely:

Definition 9.

- Two segments U, V, are commensurable if you can use a ruler of the same length w to "measure u and v together", that is, to express both lengths u and v as integer multiples mw, nw of the unit of length w.
- Two segments U, V, are incommensurable if they are not commensurable.

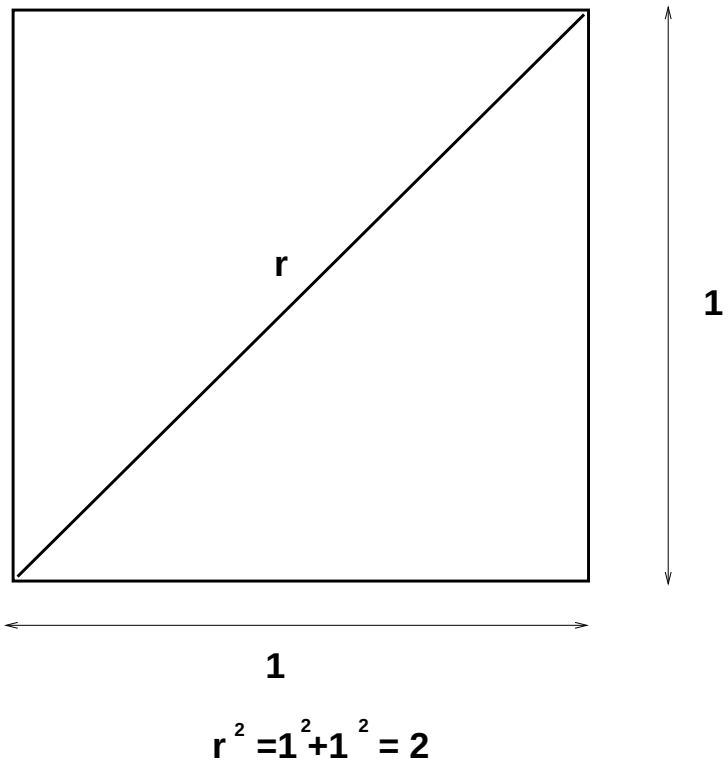
But then a momentous discovery of far-reaching consequences was made:

There are incommensurable lenghts.

That is, ***it is not true that any two lengths are commensurable***.

Precisely: it is possible to construct geometricallly[16] a segment whose length r satisfies $r^2 = 2$. For example, if we draw a square whose sides have length 1, then the length r of the diagonal of the square will satisfy $r^2 = 2$, by Pythagoras' theorem.

[16]What does "constructing geometrically" mean? This is tricky. For Euclid (who lived about 23 centuries ago), "constructing geometrically" meant "constructing with a ruler and compass". (See the Wikipedia article "Compass and straightedge consrtuctions".) Using ruler and compass, one can construct lines and circles, but there are lots of other curves—for example, ellipses—that cannot be constructed that way. On the other hand, there are other equally "geometric" methods that can be used to construct some of those curves. For example, ellipses can be constructed using pins and strings. (See the Wikipedia article "Ellipses".)



And it was discovered that ***there is no fraction*** r ***such that*** $r^2 = 2$. This means that

I. If you believe that "number" means "fraction", then there is no number that measures the length of the diagonal of a square whose sides have lengt 1.

II. If you are willing to accept that there could be "numbers" that are not fractions, then maybe there is a number r that measures the length of the diagonal of a square whose sides have lengt 1, but that number r, that we could call "$\sqrt{2}$", is not a fraction.

Today we would say that

- Those numbers that are not fractions, such as $\sqrt{2}$, do indeed exist, and we call them "real numbers".
- The fractions, called "rational[17] numbers", are real numbers, but many real numbers are "irrational" numbers, that is, numbers that are not rational.
- Actually, most[18] real numbers are not rational.
- It took mathematicians more than 2,000 years after the discovery of the irrationaly of $\sqrt{2}$ to come up with a truly rigorous definition of the concept of "real number". (The name "real number" was introduced by Descartes in the 17th century. The first rigorous definition was given by George Cantor in 1871, and the most widely used definitions were proposed by Karl Weierstrass and Richard Dedekind.

[17]The word "rational" here has nothing to do with "rationality" in the sense of "in accordance withb reason or logic". It comes from the word "ratio", which means "quotient". An "irrational number" is a number that is not the quotient ("'ratio") of two integers. If you hear somebody say something like "scientists have shown that nature is irrational: mathematicians have shown that irrationality is everywhere present, because most numbers are irrational", then you shoud realize that thit is an ignorant statement by somebody who does not understand what "irratioanl numbers" are. The "irrationality" of irrational numbers has nothing to do with their being unreasonable, absurd, or illogical; it just means that they are not quotients of two integers.

[18]If this statement does not strike you as incomprehensible because you don't know what it means, you should think again, and ask yourself "what could it possibly mean to say that most real numbers are irrational"? It turns out that this can be made precise, but making it precise is hard.

3.4.2 Why was the irrationality of $\sqrt{2}$ so important?

The discovery of the inconmensurability of $\sqrt{2}$ was made, according to legend, by ***Hippasus of Metapontum***, who lived in the 5th century B.C.E and was a member of the religious sect of the Pythagoreans, i.e., the followers of the philosopher and mathematician Pythagoras[19]. And the legend also says that the discovery was so shocking to the Pythagoreans that Hippasus was drowned at sea, as punishment for having divulged the secret. (But this is a legend, and there is no evidence that it is true.)

Why was the existence of inconmensurable magnitudes so upsetting to the Pythagoreans? The reason is this: the Pythagoreans were a mystical-religious cult.

[19] Yes, that's the same Pythagoras of Pythagoras's theorem.

> The Pythagoreans honored the effort put into mathematics, and coordinated it with the observation of the cosmos in various ways, for example: by including number in their reasoning from the revolutions and their difference between them, by theorizing what is possible and impossible in the organization of the cosmos from what is mathematically possible and impossible, by conceiving the heavenly cycles according to commensurate numbers with a cause, and by determining measures of the heaven according to certain mathematical ratios, as well as putting together the natural science which is predictive on the basis of mathematics, and putting the mathematical objects before the other observable objects in the cosmos, as their principles.
>
> From the *Wikipedia* article on *Pythagoreanism*, which quotes the *Protrepticus*, by D. S. Hutchinson and M. R. Johnson, a 2015 reconstruction of a lost dialogue of Aristotle.

In other words, for the Pythagoreans everything in the world was determined by ratios (i.e. quotients) of "numbers", and for them "number" meant "natural number"

(i.e., counting number). The discovery that some lengths were not ratios of "numbers" undermined the Pythagorean system to such an extent that the members of the sect felt it necessary to conceal this fact from the general public.

But it is important to put all this in proper perspective: there is no real proof that Hippasus truly was the discoverer of the irrationality of $\sqrt{2}$, or that he was drowned at sea for that discovery.

3.4.3 What is a "real number", really?

The discovery that there are lengths that are inconmensurable with one another naturally forced mathematicians to ask a fundamental question: ***what is a "number", really?***

And, as we have explained, it took more than 2,000 years until mathematicians found a satisfactory answer.

3.4.4 The most important number systems: real numbers vs. integers and natural numbers; definition of "rational number"

Now let us look at the main number systems[20] that mathematicians use today.

1. The measuring numbers, together with their negatives, and zero, are called ***real numbers***.

[20] There are many number systems. What we will do here is barely scratch the surface of a very rich theory.

2. The set of all real numbers is called $\mathbb{R}$. (It is also called "the set of all real numbers", or "the real line".)

3. The counting numbers are called ***natural numbers***. (They are also called "positive integers".)

4. The set of all natural numbers is called $\mathbb{N}$.

5. The natural numbers, together with their negatives and zero, are called ***integers***.

6. The set of all integers called $\mathbb{Z}$.

7. The real numbers that are quotients of two integers are called ***rational numbers***. That is, we have the following key definition:

Definition 10.

- A rational number is a real number r such that there exist integers m, n for which:
  (a) $n \neq 0$
  (b) $r = \frac{m}{n}$.
- The set of all rational numbers is called $\mathbb{Q}$. (So "$x \in \mathbb{Q}$" is a way of saying "x is a rational number".)
- In formal language: If $r \in \mathbb{R}$, then $r \in \mathbb{Q}$ if[a]

$$(\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})\left(n \neq 0 \text{ and } r = \frac{m}{n}\right). \tag{3.15}$$

- An irrational number is a real number r which is not rational.

[a] Formula (3.15) is not yet completely formal, because it contains the word "and". Soon we are going to leanr the symbol "$\wedge$" for "and", and then we will be able to rewrite (3.15) as $(\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})\left(n \neq 0 \wedge r = \frac{m}{n}\right)$.

3.4.5 A remark about sets

We will spend a lot of time in this course studying ***sets***. At this point, all you need to know is that

- ***sets have members***.

- If S is a set and x is an object (for example, a number or a person or a giraffe or a set) then "$x \in S$" is a way of saying that x is a member of S.
- "$x \in S$" is read as "x belongs to S", or "x is in S", or "x is a member of S".
- We write "$x \notin S$" to indicate that x is not a member of S.
- So, for example,
  - If C is the set of all cows, then to say that Suzy is a cow we can equally well say "Suzy$\in C$".
  - You can read "Suzy$\in C$ in any of the following ways:
    1. Suzy belongs to C,
    2. Suzy is in C,
    3. Suzy belongs to the set of all cows,
    4. Suzy is a cow.

    But the third reading, although correct, is very stupid, because there is no reason to say "Suzy is a member of the set of all cows" when you can say the same thing in a much shorter and simpler way by saying "Suzy is a cow".
  - Similarly, you can read "Suzy$\notin C$ in any of the following ways:

1. Suzy does not belong to C,
2. Suzy is not in C,
3. Suzy does not belong to the set of all cows,
4. Suzy is not a cow.

And the third reading, though correct, sounds silly, so you would never say it that way.

- Here is another example.
  - "$\mathbb{N}$", as we know, is the set of all natural numbers. So, to say that 3 is a natural number we can equally well say "$3 \in \mathbb{N}$".
  - You can read "$3 \in \mathbb{N}$ in any of the following ways:
    1. 3 belongs to $\mathbb{N}$,
    2. 3 is in $\mathbb{N}$,
    3. 3 belongs to the set of all natural numbers,
    4. 3 is a natural number.

    But the third reading, althogh correct, is very stupid, because there is no reason to say "3 is a member of the set of all natural number" when you can say the same thing in a much shorter and simpler way by saying "3 is a natural number".

Problem 17. For each of the following formulas,

(a) translate the formula into English,
(b) indicate whether it is true or false.

Give the best, most natural English translation. For example, the formula "$1 \in \mathbb{N}$*" could be translated as "*1 *belongs to the set of natural numbers", but this sounds very awkward. A much better way to say the same thing in English is "*1 *is a natural number", so this translation is to be preferred.*

1. $-3 \in \mathbb{N}$,
2. $0 \in \mathbb{N}$,
3. $0 \notin \mathbb{Z}$,
4. $0 \in \mathbb{Z}$,
5. $-3 \in \mathbb{R}$,
6. $0 \in \mathbb{R}$,
7. $0 \notin \mathbb{R}$,
8. $0 \in \mathbb{R}$,
9. $0 \in \mathbb{Q}$,
10. $3 \in \mathbb{Q}$,
11. $-3 \in \mathbb{Q}$,
12. $\frac{237}{42} \in \mathbb{Q}$,
13. $\sqrt{2} \in \mathbb{Q}$,
14. $\sqrt{2} \notin \mathbb{Q}$,
15. $\pi \in \mathbb{Q}$.

3.4.6 Proof of the irrationality of $\sqrt{2}$

As explained before, we could state the theorem on the irrationality of $\sqrt{2}$ by saying that "$\sqrt{2}$ is irrational". This, however, would mean that there is a "number $\sqrt{2}$", i.e., a number whose square is 2. But the issue whether such a number exists is different from the one that concerns us here, namely, whether there exists a rational number r such that $r^2 = 2$. So I prefer to state the theorem in a way that does not imply any *a priori* commitment to the existence of a "number" r such that $r^2 = 2$.

And, before we give the proof, we introduce a few concepts and state some facts that will be used in the proof, (These facts will be proved later in the course.)

THE DEFINITION OF "EVEN" AND "ODD" INTEGERS

Definition 11. Let a be an integer. We say that a is even if it is divisible by 2. And we say that a is odd if it is not even.

The integers 1 are -1 are factors of every integer, because if $n \in \mathbb{Z}$ then $n = n \times 1$ and $n = (-n) \times (-1)$, so n is divisible by 1 and by -1. So 1 and -1 are not very interesting factors, because they are always there. So we refer to 1 and -1 as the ***trivial factors*** of an integer.

THE DEFINITION OF "COPRIME" INTEGERS

Definition 12.

- Let a, b be integers. We say that a and b are coprime if they do no have any nontrivial common factors.
- We write "$a \perp b$" to indicate that a and b are coprime.
- In formal language, if $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$, then $a \perp b$ if

$$\sim (\exists k \in \mathbb{Z})(k|a \text{ and } k|b \text{ and } k \neq 1 \text{ and } k \neq -1).$$

Example 9. The integers 12 and 35 are coprime. Indeed:

- The factors of 12 are 1, -1, 2, -2, 3, -3, 4, -4, 6, -6, 12 and -12.
- The factors of 35 are 1, -1, 5, -5, 7, -7, 35 and -35.

So the only common factors are 1 and -1, i.e., the trivial factors. Hence 12 and 35 are coprime. □

3.5 The proof of the irrationality of $\sqrt{2}$

Now, finally, we are ready to prove that $\sqrt{2}$ is irrational.

We are going to use two facts:

Fact 1. *Every rational number is equal to a quotient $\frac{m}{n}$ of two coprime integers.*

Fact 2. *The product of two odd integers is odd.*

Theorem 4. *There does not exist a rational number r such that $r^2 = 2$.*

Proof. We give a proof by contradiction .

Assume that there exists a rational number r such that $r^2 = 2$.

Pick one such number and call it r. (Here we are using Rule $\exists_{use}$.)

Using the fact that $r \in \mathbb{Q}$, we may pick integers m, n such that

(1) $n \neq 0$,

(2) $r = \frac{m}{n}$,

(Here we are using again Rule $\exists_{use}$.)

Using Fact 1, we may actually choose m, n such that

(3) m and n are coprime.

Since $r^2 = 2$, we have $\frac{m^2}{n^2} = 2$.

Therefore $m^2 = 2n^2$.

So m^2 is even.

But then m is even. (Reason: Assume[21] that m is not even. Then m is odd. So by Fact 2, m^2 is odd. But we have proved that m^2 is even. So m^2 is not odd. Therefore m^2 is odd and m^2 is not odd, which is a contradiction.)

Since m is even, m is divisible by 2, that is, $(\exists k \in \mathbb{Z})m = 2k$.

So we may pick an integer k such that $m = 2k$.

Then $m^2 = 4k^2$.

But $m^2 = 2n^2$.

Hence $2n^2 = m^2 = (2k)^2 = 4k^2$.

Therefore $n^2 = 2k^2$.

So n^2 is even.

[21] Notice that we have a proof by contradiction within our main proof by contradiction.

But then n is even. (Reason: Assume[22] that n is not even. Then n is odd. So n^2 is odd by Fact 2. But we have proved that n^2 is even. So n^2 is not odd. Therefore n^2 is odd and n^2 is not odd, which is a contradiction.)

So m is even and n is even.

Therefore m and n are divisible by 2.

So m and n have a nontrivial common factor.

Hence $\boxed{m \text{ and } n \text{ are not coprime}}$.

But $\boxed{m \text{ and } n \text{ are coprime}}$

So $\boxed{m \text{ and } n \text{ are coprime and } m \text{ and } n \text{ are not coprime}}$, which is a contradiction.

So the assumption that there exists a rational number r such that $r^2 = 2$ has led us to a contradiction,

Therefore $\boxed{\text{there does not exist a rational number } r \text{ such that } r^2 = 2}$.
Q.E.D.

3.6 More irrationality proofs

We now use the same technique to prove that $\sqrt{3}$ is irrational. The key point here is to realize that "even vs.

[22] Another proof by contradiction !

odd" now has to be replaced by "divisible by 3 vs. not divisible by 3". And, in order to do the crucial step (the analogue of "if m^2 is divisible by 2 then m is divisible by 2") we need a generalization of Fact 2:

Fact 3. *If p is a prime number, then the product of two integers that are not divisible by p is not divisible by p either.*

(We will prove Fact 3 later.)

Theorem 5. *There does not exist a rational number r such that $r^2 = 3$.*

Proof. We want to prove that $\sim (\exists r \in \mathbb{Q}) r^2 = 2$. We will do a proof by contradiction .

Assume that $(\exists r \in \mathbb{Q}) r^2 = 2$, i.e., there exists a rational number r such that $r^2 = 3$.

Pick one such number and call it r.

Using the fact that $r \in \mathbb{Q}$, we may pick integers m, n such that

(1) $n \neq 0$,
(2) $r = \frac{m}{n}$,

Then, using Fact 1, we can actually choose m, n so that

(3) m and n are coprime.

Since $r^2 = 3$, we have $\frac{m^2}{n^2} = 3$.

Therefore $m^2 = 3n^2$.

So m^2 is divisible by 3.

But then m is divisible by 3. (Reason: By Fact 3, if m was not divisible by 3, it would follow that m^2 is not divisible by 3 either. But m^2 is divisible by 3, and we got a contradicition.)

Since m is divisible by 3, we may pick an integer k such that $m = 3k$.

Then $m^2 = 9k^2$.

But $m^2 = 3n^2$.

Hence $3n^2 = 9k^2$, so

$$n^2 = 3k^2 \,. \tag{3.16}$$

So n^2 is divisible by 3.

But then n is divisible by 3. (Reason: By Fact 3, if n was not divisible by 3, it would follow that n^2 is not divisible by 3 either. But n^2 is divisible by 3, and we got a contradicition.)

So 3 is a factor of m and 3 is a factor of n.

Hence m and n have a nontrivial common factor.

So m and n are not coprime.

But m and n are coprime.

Therefore $\boxed{m \text{ and } n \text{ are coprime and } m \text{ and } n \text{ are not coprime}}$, which is a contradiction,

So the assumption that there exists a rational number r such that $r^2 = 3$ has led us to a contradiction,

Therefore $\boxed{\text{there does not exist a rational number } r \text{ such that } r^2 = 3}$.
Q.E.D.

3.6.1 What happens when you make a mistake in a proof

Can we do the same that we did before to prove the following theorem?

THEOREM: There does not exist a rational number r such that $r^2 = 4$.

Proof. We will do a proof by contradiction .

Assume that there exists a rational number r such that $r^2 = 4$.

Pick one such number and call it r.

Using Fact 1, we may pick integers m, n such that

(1) $n \neq 0$,

(2) $r = \frac{m}{n}$,

(3) m and n have no nontrivial common factors.

Since $r^2 = 4$, we have $\frac{m^2}{n^2} = 4$.

Therefore $m^2 = 4n^2$.

So m^2 is divisible by 4.

But then m is divisible by 4. (Reason: By Fact 3, if m was not divisible by 4, it would follow that m^2 is not divisible by 4 either. But m^2 is divisible by 4, and we got a contradicition.)

Since m is divisible by 4, we may pick an integer k such that $m = 4k$.

Then $m^2 = 16k^2$.

But $m^2 = 4n^2$.

Hence $n^2 = 4k^2$, so

$$n^2 = 3k^2 \,. \tag{3.17}$$

So n^2 is divisible by 4.

But then n is divisible by 4. (Reason: By Fact 3, if n was not divisible by 4, it would follow that n^2 is not divisible by 3 either. But n^2 is divisible by 4, and we got a contradicition.)

So 3 is a factor of m and 4 is a factor of n.

Hence m and n have a nontrivial common factor.

So m and n are not coprime.

But m and n are coprime.

Therefore $\boxed{m \text{ and } n \text{ are coprime and } m \text{ and } n \text{ are not coprime}}$, which is a contradiction,

So the assumption that there exists a rational number r such that $r^2 = 4$ has led us to a contradiction,

Therefore $\boxed{\text{there does not exist a rational number } r \text{ such that } r^2 = 4}$.
Q.E.D.

Same proof, right?

WRONG!!!!!

What is wrong here?

1. The result is ***false***. It is not true that there does not exist a rational number r such that $r^2 = 4$. Indeed, if we take $r = 2$ then r is ratinal and $r^2 = 4$.

2. Since the conclusion of the proof is false, the proof itself must be wrong. That is, whoever wrote this proof must have cheated[23] in some step.

[23]Nothing personal here. "Cheat" means "violate the rules." Of course, I haven't told you yet what the rules are, but let me anticipate one of them. ***You are allowed to use a result that has been proved, but you are now allowed to make up a statement that has not been proved and use it as if it was true.***

In our case, Fact 3 explicitly says that "if p is prime then if a is not divisible by p it follows that a^2 is not divisible by p". So we are allowed to apply Fact 3 if p is prime, but we are not allowed to apply it if p is not prime.

So the two steps where we applied Fact 3 are wrong. In those steps, we cheated, by violating the rules.

The general principle is this: ***If a proof is correct then you can be sure that the conclusion is true.***

And another way to say that is this: ***if the conclusion of a proof is false, then the proof must be wrong. There has to be a mistake in the proof itself.***

So, if I give you a proof of a conclusion that is false, you have to be able to find where in the proof the author cheated. I will not be satisfied with a statement such as "the proof is wrong because the conclusion is false." I will want to know where in the proof a mistake was made.

Consider the following analogy: If I am trying to drive to Boston and end up in New York, then of course I can conclude thta I did something worng. But I will want to know what I did wrong, where I made a wrong turn. The same happens with proofs.

3.6.2 More complicated irrationality proofs

I hope it is clear to you that the same method, exactly, will apply to prove that $\sqrt{5}$, $\sqrt{7}$, $\sqrt{11}$, and, more generally, $\sqrt{p}$ for any prime number, is irrational.

Now let us try a more complicated case. Let us prove that

Theorem 6. *There does not exist a rational number r such that $r^2 = 12$.*

Remark 3. The number 12 is not prime. (Actually, $12 = 4 \times 3$.) So we cannot apply Fact 3 with 12 in the role of p.

Proof. We will do a proof by contradiction .

> Assume that there exists a rational number r such that $r^2 = 12$.
>
> Pick one such number and call it r, so $r^2 = 12$..
>
> Using the fact that $r \in \mathbb{Q}$, we may pick integers m, n such that
>
> (1) $n \neq 0$,
>
> (2) $r = \frac{m}{n}$,
>
> Then, using Fact 1, we may pick m, n such that

(3) m and n are coprime.

Since $r^2 = 12$, we have $\frac{m^2}{n^2} = 12$.

Therefore $m^2 = 12n^2$.

Hence $m^2 = 3 \times 4n^2$.

So m^2 is divisible by 3.

But then m is divisible by 3. (Reason: By Fact 3, if m was not divisible by 3, it would follow that m^2 is not divisible by 3 either. But m^2 is divisible by 3, and we got a contradicition.)

Since m is divisible by 3, we may pick an integer k such that $m = 3k$.

Then $m^2 = 9k^2$.

But $m^2 = 12n^2$.

Hence $12n^2 = 9k^2$, so

$$4n^2 = 3k^2 \,. \tag{3.18}$$

So $4n^2$ is divisible by 3.

But then n is divisible by 3. (Reason: By Fact 3, assume n is not divisible by 3; then by Fact 3 n^2 is not divisible by 3; since 4 is not divisible by 3,

another application of Fact 3 tells us that $4n^2$ is not divisible by 3. But $4n^2$ is divisible by 3, so we got a contradiction.)

So 3 is a factor of m and 3 is a factor of n.

Hence m and n have a nontrivial common factor.

So m and n are not coprime.

But m and n are coprime.

Therefore $\boxed{m \text{ and } n \text{ are coprime and } m \text{ and } n \text{ are not coprime}}$, which is a contradiction,

So the assumption that there exists a rational number r such that $r^2 = 12$ has led us to a contradiction,

Therefore $\boxed{\text{there does not exist a rational number } r \text{ such that } r^2 = 12}$.
Q.E.D.

Problem 18. ***Prove*** that each of the following numbers is irrational:

1. $\sqrt{5}$,
2. $\sqrt[3]{5}$,
3. $\sqrt[3]{9}$,
4. $\sqrt{28}$,

5. $\sqrt{2+\sqrt{2}}$,
6. $\sqrt{\frac{2}{3}}$,
7. $\sqrt{\frac{27}{31}}$. □

Problem 19. ***Prove or disprove***[24] each of the following statements:

1. The sum of two rational numbers is a rational number.
2. The product of two rational numbers is a rational number.
3. The sum of two irrational numbers is an irrational number.
4. The product of two irrational numbers is an irrational number.
5. The sum of two irrational numbers is a rational number.
6. The product of two irrational numbers is a rational number.
7. The sum of a rational number and an irrational number is an irrational number.
8. The product of a rational number and an irrational number is an irrational number. □

[24]To ***disprove*** a stetement means "to prove that the statement is false". For example, when we proved that $\sqrt{2}$ is irrational we disproved the statement '$\sqrt{2}$ is rational.

Problem 20.

I. ***Explain*** why the following "proofs" that $\sqrt{2}+\sqrt{3}$ and $\sqrt{6}$ are irrational (in which we are allowed to use the facts that $\sqrt{2}$ and $\sqrt{3}$ are irrational) are wrong:

1. *Proof that $\sqrt{2}+\sqrt{3}$ is irrational:*

   We know that $\sqrt{2}$ is irrational.
   We know that $\sqrt{3}$ is irrational.
   Hence the sum $\sqrt{2}+\sqrt{3}$ is irrational. **Q.E.D.**

2. *Proof that $\sqrt{6}$ is irrational:*

   We know that $\sqrt{2}$ is irrational.
   We know that $\sqrt{3}$ is irrational.
   Hence the product $\sqrt{2}.\sqrt{3}$ is irrational.
   So $\sqrt{6}$ is irrational. **Q.E.D.**

II. ***Give correct proofs*** that $\sqrt{2}+\sqrt{3}$ and $\sqrt{6}$ are irrational. □

Problem 21. ***Prove*** that $\sqrt{2}+\sqrt[3]{2}$ is irrational. □

Problem 22. ***Prove*** that $\sqrt{2}+\sqrt{3}+\sqrt{5}$ is irrational. (NOTE: This requires some hard thinking on your part.) □

Problem 23. ***Prove*** that $\sqrt{2}+\sqrt{3}+\sqrt{5}+\sqrt{7}$ is irrational. (NOTE: This requires ***quite a lot*** of thinking on your part.) □

Problem 24 ***Prove*** that, if $n \in \mathbb{N}$, and $p_1, p_2, \ldots, p_n$ are n distinct primes, then $\sqrt{p_1} + \sqrt{p_2} + \cdots + \sqrt{p_n}$ is irrational. (NOTE: This is very difficult.) $\square$

3.7 A general theorem on irrationality of square roots

After having proved that various numbers such as $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt{28}$, $\sqrt{\frac{2}{3}}$, $\sqrt{\frac{27}{31}}$ are irrational, can we prove once and for all a general theorem that will include all these cases? The answer is "yes", and here is the theorem. Notice that all the irrationality results about square roots that we have proved before follow easily from this theorem. (For example: if $r = 2$, then $r = \frac{2}{1}$ and $2 \perp 1$, so Theorem 7 tells us that $\sqrt{r}$ is irrational, because 2 is not the square of an integer; similarly, if $r = \frac{2}{3}$, then Theorem 7 tells us that $\sqrt{r}$ is irrational, because $2 \perp 3$ and 2 and 3 are not squarea of integers.)

Theorem 7. *Let r be a rational number written as a quotient $\frac{m}{n}$, where m and n are coprime integers and $n > 0$. Then either $\sqrt{r}$ is irrational or both m, n are squares of integers.*

The key fact that will be used in this proof is the following

Fact 4 *If a, b, c are integers such that $c|ab$ and $c \perp b$,*

then $c|a$. (That is, if c divides ab and is coprime with b, then c divides a.

Rough idea of the proof of Fact 4. We can write a, b, c as products of primes: $a = p_1.p_2.\cdots.p_n$, $b = q_1.q_2.\cdots.q_m$, $c = r_1.r_2.\cdots.r_k$. Then the expression of ab as a product of primes is

$$ab = p_1.p_2.\cdots.p_n.q_1.q_2.\cdots.q_m\,. \tag{3.19}$$

Since $c|ab$, all the primes r_j occur in the right-hand side of (3.19). But $c \perp b$, so none of the r_j is a q_j. It follows that all the r_j are p's i.e., factors of a, so $c|a$.

This argument is not completely rigorous. I will give you a rigorous—and much more elegant—proof later.

Proof of Theorem 7:

We will prove that if $\sqrt{r}$ is rational then both m, n are squares of integers.

Assume $\sqrt{r} \in \mathbb{Q}$.

Then we can write $\sqrt{r} = \frac{p}{q}$, where p, q are integers, and $q \neq 0$.

Furthermore, in view of Fact 1, we can actually choose p and q to be coprime.

We then have

$$\frac{p^2}{q^2} = \frac{m}{n}\,,$$

so

$$p^2 n = mq^2 \, .$$

So $n|mq^2$. But $n \perp m$, so by Fact 7 $n|q^2$.

Also, $q^2|p^2 n$.

But $q^2 \perp p^2$. (Reason: Suppose q^2 and p^2 were not coprime. Then they would have a common factor k such that $k > 1$. And k would have a prime factor u. Then u is prime and divides both q^2 and p^2. By Fact 3, u divides q and u divides p, so p and q are not coprime. But p and q are coprime, so we get a contradiction.)

Since $q^2|p^2 n$ and $q^2 \perp p^2$, it follows that $q^2|n$.

So q^2 divides n, n divides n are natural numbers.

Therefore $n = q^2$.

Since $n = q^2$ and $p^2 n = mq^2$, it follows that $p^2 n = mn$.

So $p^2 = m$.

We have shown that $m = p^2$ and $n = q^2$. Hence both m and n are squares of integers.

We have shown that if $\sqrt{r}$ is rational then m and n must be squares of integers. So either m and n are squares of integers or r is irrational. **Q.E.D.**