MATHEMATICS 300 — FALL 2017

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S NOTES

PART III

Contents

6 The ordering of the integers

We have not yet discussed how we can ***order*** the integers, i.e., talk about an integer m being "less than", or "greater than", an integer n, and prove, for example, that if m and n are integers then one and only one of the three possibilties $m < n$, $m = n$, $m > n$ occurs.

The easiest way to do that, given what we know so far, is to give the following definition:

Definition 14. Let m, n be integers. We say that

- m is smaller than n (or m is less than n), and write
$$m < n\,,$$
if $n - m$ is a natural number.
- m is smaller than or equal to n (or m is less than or equal to n), and write
$$m \leq n\,,$$
if $m < n$ or $m = n$.
- m is larger than n (or m is greater than n), and write
$$m > n\,,$$
if $m - n$ is a natural number.
- m is larger than or equal to n (or m is greater than or equal to n), and write
$$m \geq n\,,$$
if $m > n$ or $m = n$. □

6.1 Elementary facts about $<$, $>$, $\leq$, and $\geq$

The symbols $<$, $>$, $\leq$, and $\geq$ represent ***binary relations***. So before we discuss them we must talk about relations in general.

6.1.1 Unary and binary relations

Unary and binary relations, a.k.a. predicates, a.k.a. properties

A relation, or predicate, or property, is something that can be asserted about one or several variable objects, called the inputs, or arguments, of the relation (or predicate, or property), in such a way that, for each choice of a value for each of the inputs, the assertion has a definite truth value, i.e., is true or false.

A relation (predicate, property) with one argument is called a unary relation (predicate, property).

A relation (predicate, property) with two arguments is called a binary relation (predicate, property).

Usually, each of the arguments of a relation has a domain, i.e. a set D such that the argument takes values in D. (And, for a binary relation with two arguments x, y, it can happen sometimes that the domain of the x variable is different from the domain of the y variable. But usually both domains are the same set D, and in that case we say that the relation is a ***binary relation on*** D.)

For unary relations (predicates, properties) it is customary to use the words ***predicate***, or ***property***, rather than relation.

Example 27.

- ***Positivity of integers*** is a unary predicate, whose domain is the set $\mathbb{Z}$ of all integers: it takes an integer n as input and results in the truth value "true" if $n > 0$, and in the truth value "false" if it is not true that $n > 0$ (that is, if $n \leq 0$). We can name this predicate by the formula describing it, and talk about "the predicate '$n > 0$' ", or we can call it "positivity", or, if you want to make it clear that we are talking about integer inputs, "positivity of integers".

- ***Nonnegativity of integers*** is also a unary predicate whose domain is $\mathbb{Z}$: it takes an integer n as input and results in the truth value "true" if $n \geq 0$, and in the truth value "false" if it is not true that $n \geq 0$ (that is, if $n < 0$). We can name this predicate by the formula describing it, and

talk about "the predicate '$n \geq 0$'", or we can call it "nonnegativity", or, if you want to make it clear that we are talking about integer inputs, "nonnegativitiy of integers".

- There are also unary predicates ***positivity of real numbers*** and ***nonnegativity of real numbers***. They are defined in the same way as positivity of integers and nonnegativity of integers, except for the fact that now the arguments take values in the set $\mathbb{R}$ of all real numnbers.

- ***Evenness of integers*** is a unary predicate whose domain is $\mathbb{Z}$: it takes an integer n as input and results in the truth value "true" if n is even (i.e., if $2|n$), and in the truth value "false" if n is not even (and we know now that "n is ot even" is equiva;ent to "n is odd"). We can name this predicate by the formula describing it, and talk about "the predicate 'n is even'", or "the predicate '$2|n$'", or we can call it "evenness", or, if you want to make it clear that we are talking about integer inputs, "evenness of integers".

- ***Primality***, that is, the property of being a prime number, is a unary predicate whose domain[1]: it takes an integer n as input and results in the truth value "true" if n is a prime number, and in the truth value "false" if n is not a prime number. We can name this predicate by the formula describing it, and talk about "the predicate 'p is prime'", or we can call this predicate "the 'is prime' predicate", or "primality".

- You may ask whether there is such a thing as "evenness of real numbers". You could of course define such a thing, by saying that "a real number x is even if there exists a real number y such that $x = 2y$". But this would be a very stupid predicate, because every real number is even according to this definition, so saying that a real number x is even would just amount to saying that x is a real number, which says nothing new about x.

- ***Equality*** (on any set you want) is a binary relation [2]: it takes two objects x, y (of any kind, integers, real numbers, cows, giraffes, cities,

[1] You could also take the domain to be $\mathbb{N}$. It does not matter, because the integers that are not natural numbers are never prime.

[2] Or predicate, or property.

molecules, sets, functions), as inputs, and results in the truth value "true" if $x = y$ (that is, if x and y are one and the same thing) and the truth value "false" if $x \neq y$. We can name this relation by the formula describing it, and talk about "the relation '$x = y$'" but a nicer, better way is to call it "equality".

- ***Divisibility*** is a binary relation on the set $\mathbb{Z}$ of all integers: it takes two integers m, n as inputs, and results in the truth value "true" if m is divisible by n, that is, if $n|m$, and in the truth value "false" if m is not divisible by n. We can name this relation by the formula describing it, and talk about "the relation "$n|m$'" but a nicer, better way is to call it "divisibility".

- ***Less than*** is a binary relation on $\mathbb{Z}$: it takes two integers m, n as inputs, and results in the truth value "true" if $m < n$, and in the truth value "false" if it is not true that $m < n$. We can name this relation by the formula describing it, and talk about "the relation '$m < n$'" or we can call it "the 'less than' relation".

- ***Less than or equal to*** is a binary relation on $\mathbb{Z}$: it takes two integers m, n as inputs, and results in the truth value "true" if $m \leq n$, and in the truth value "false" if it is not true that $m \leq n$, We can name this relation by the formula describing it, and talk about "the relation '$m \leq n$'" or we can call it "the 'less than or equal to' relation".

- Naturally, there are also relations "less than" and "less than or equal to between real numbers.

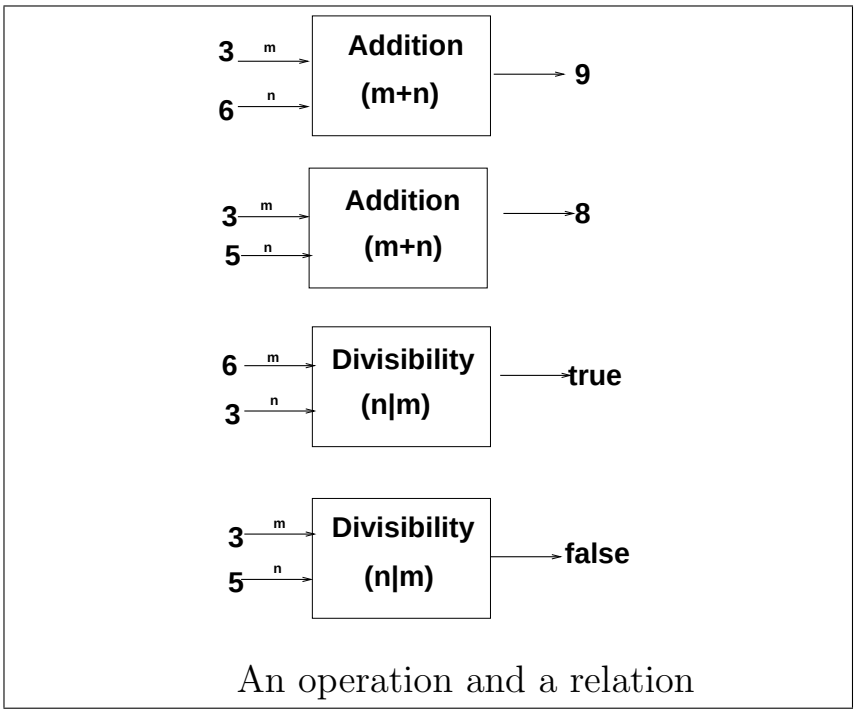
- And there are also relations "greater than" and "greater than or equal to", between integers and between real numbers.

Remark 11. You may have noticed that relations are very similar to operations. Both have arguments, and produce a value for each value of the arguments. The difference between them is that an operation produces a thing (number, set, function, giraffe, whatever) as output, and a relation or predicate produces a truth value (true or false). □

For example:

- ***Addition of integers*** is a binary operation: given two integers m, n it produces as output an integer $m + n$.

- ***Divisibility of integers*** is a binary relation: given two integers m, n it produces a true-false output according to the following rule:
  - If m is divisible by n then the output is "true".
  - If m is not divisible by n then the output is "false".



An operation and a relation

6.1.2 Properties of the relations $<$, $>$, $\leq$, and $\geq$

There are several interesting properties that a binary relation may or may not have.

Definition 15. A binary relation xRy on a set S is

- reflexive if xRx for all members x of S; that is, R is reflexive if
$$(\forall x \in S) xRx\,,$$
- irreflexive if[3] $\sim xRx$ for all members x of S; that is, R is irreflexive if
$$(\forall x \in S) \sim xRx\,,$$

[3]Recall that "$\sim$" stands for "it is not true that", so "$\sim xRx$" means "x is not R-related to x".

- symmetric if, whenever $x \in S$, $y \in S$ are such that xRy, then it follows that yRx; that is, R is symmetric if

$$(\forall x \in S)(\forall y \in S)(xRy \Longrightarrow yRx)\,,$$

- antisymmetric if, whenever $x \in S$, $y \in S$ are such that xRy and yRx, then it follows that $x = y$. (That is, R is antisymmetric if

$$(\forall x \in S)(\forall y \in S)((xRy \wedge yRx) \Longrightarrow x = y)\,,$$

- transitive if, whenever $x \in S$, $y \in S$, $z \in S$ are such that xRy and yRz, then it follows that xRz. That is, R is transitive if

$$(\forall x \in S)(\forall y \in S)(\forall z \in S)\Big((xRy \wedge yRz) \Longrightarrow xRz\Big)\,.$$

- trichotomous if it satisfies the ***trichotomy*** [4] ***law***: whenever $x \in S$ and $y \in S$ it follows that one and only one of the following three assertions is true: xRy, $x = y$, yRx. That is, R is trichotomous if

$$(\forall x \in S)(\forall y \in S)\Bigg((xRy \vee x = y \vee yRx)$$
$$\wedge\Big(x = y \Longrightarrow \big((\sim xRy) \wedge (\sim yRx)\big)\Big) \wedge \Big(xRy \Longrightarrow \big((\sim x = y) \wedge (\sim yRx)\big)\Big)\Bigg)\,.$$

Question 4. *In the explanation of what it means for a binary relation to be trichotomous, whwre I wrote the condition in formal language,* ***explain*** *why it was not necessary to include a third clause stating that*

$$yRx \Longrightarrow \Big((\sim x = y) \wedge (\sim xRy)\Big)\,.$$

Theorem 27. *The relation "<", on the set of integers, is irreflexive, transitive, and trichotomous.*

Translated into English, the above statement says that:

[4] A ***dichotomy*** is a situation in which one and only one of two possibilities occurs. Similarly, a ***trichotomy*** is a situation in which one and only one of three possibilities occurs.

1. If m is an integer, then it is not the case that $m < m$ or $m > m$.
2. If m, n, p are integers such that $m < n$ and $n < p$, then $m < p$.
3. If m, n are integers, then one and only one of the following three possibilities occurs: $m < n$, $m = n$, $n < m$.

Proof.
We first prove that "$<$" is transitive.

Let m, n, p be arbitrary integers.

Assume that $m < n$ and $n < p$.

We want to prove that $m < p$.

It follows from Definition 14 that $n - m \in \mathbb{N}$ and $p - n \in \mathbb{N}$.

Therefore $(p - n) + (n - m) \in \mathbb{N}$, because the sum of two natural numbers is a natural number.

But $(p - n) + (n - m) = p - m$.

So $p - m \in \mathbb{N}$.

Therefore $m < p$.

This completes the proof that "$<$" is transitive.

We now prove the trichotomy law.

Let m, n be arbitrary integers.

Let $p = m - n$.

Then $p \in \mathbb{Z}$.

So Basic Fact BFZ9 tells us that either $p \in \mathbb{N}$, or $-p \in \mathbb{N}$, or $p = 0$.

We analyze separately the three cases, and show that

$$n < m \vee m = n \vee m < n \tag{6.1}$$

in each of the cases.

If $p \in \mathbb{N}$, then $m - n \in \mathbb{N}$, so $n < m$, and then (6.1) holds.

If $-p \in \mathbb{N}$, then $-(m - n) \in \mathbb{N}$, so (6.1) holds.

If $p = 0$, then $m - n = 0$, so $m = n$, and then (6.1) holds.

So in each of the three cases, we have proved that (6.1) is

Therefore $\boxed{n < m \vee m = n \vee m < n}$.

We now show that it is not possible for two of the three possibilities to occur.

Suppose first that $m = n$. Then $m - n = 0$ and $n - m = 0$. So it is not possible to have $m < n$, because "$m < n$" means "$n - m \in \mathbb{N}$", which is not possible since $n - m = 0$ and $0 \notin \mathbb{N}$. And it is not possible to have $n < m$, because "$n < m$" means "$m - n \in \mathbb{N}$", which cannot happen since $m - n = 0$ and $0 \notin \mathbb{N}$.

Now suppose that $n < m$. Then we already know that $m \neq n$.

Furthermore, it is not the case that $m < n$. (Reason: Suppose[5] that $m < n$. Then $m - n \in \mathbb{N}$ and $n - m \in \mathbb{N}$. It follows that $(m - n) + (n - m) \in \mathbb{N}$, so $0 \in \mathbb{N}$, because $0 = (m - n) + (n - m)$. But we know that $0 \notin \mathbb{N}$. So $o \in \mathbb{N} \wedge 0 \notin \mathbb{N}$, which is a contradiction. Hence it is not true that $m < n$.)

Finally, let us assume that $m < n$. Then the posibilities $n = m$ and $n < m$ do not occur. (There is no need to give a separate proof of this fact. We proved in the previous paragraph that "if $n < m$ then $m \neq n$ and $\sim m < n$". This means[6] that "if $a < b$ then $b \neq a$ and $\sim b < a$". Now apply this with "n" in the role of "b" and "m" in the role of "a". You get "if $m < n$ then $n \neq m$ and $\sim n < m$".)

So we have proved that "one and only one of the possibilities '$m < n$', '$m = n$', '$n < m$', occurs" for arbitrary integers m, n.

Therefore we can conclude that

[5] Another proof by contradiction here.

[6] Remember that in order to say something about arbitrary objects you can use any letters you want as names for those objects. So, for example, once you know that "if $a|b$ and $a|c$ then $a|b + c$", you can rewrite this as "if $m|n$ and $m|p$ then $m|n + p$". And then you can rewrite this as "if $b|a$ and $b|c$ then $b|a + c$. These are all different ways of saying exactly the same thing.

If m and n are arbitrary integers, then one and only one of the possibilities "$m < n$", "$m = n$", "$n < m$", occurs.

Q.E.D.

Remark 12. Clearly, the relation "¿" is also irreflexive, transitive, and trichotomous. This can be proved exactly as we proved Theorem 27, or using the result of Problem 15 below. □

Problem 15. *The* ***inverse*** *of a binary relation R on a set S is the binary relation R^{-1} on S defined by*

$$xR^{-1}y \iff yRx \qquad \text{if} \quad x \in S, y \in S\,.$$

Prove *that*

1. *The inverse of "$<$" is "$>$".*
2. *If a relation R on a set S is reflexive, then R^{-1} is reflexive.*
3. *If a relation R on a set S is irreflexive, then R^{-1} is irreflexive.*
4. *If a relation R on a set S is symmetric, then R^{-1} is symmetric.*
5. *If a relation R on a set S is antisymmetric, then R^{-1} is antisymmetric.*
6. *If a relation R on a set S is transitive, then R^{-1} is transitive.*
7. *If a relation R on a set S is trichotomous, then R^{-1} is trichotomous.*□

Problem 16. For each of the following binary relations on the given set, ***indicate*** whether the relation is reflexive, irreflexive, symmetric, antisymmetric, transitive, or trichotomous:

1. Equality (on any set S).
2. Divisibility (that is, the relation "$m|n$"), on the set $\mathbb{N}$.
3. Divisibility (that is, the relation "$m|n$"), on the set $\mathbb{Z}$.
4. "Less than or equal to", on the set $\mathbb{Z}$.

5. "$<$" on the set $\mathcal{F}$ of all continuous real-valued functions on the interval $[0,1]$. (If f, g are two functions defined on $[0,1]$, we say that $f < g$ if $f(x) < g(x)$ for every x belonging to the interval $[0,1]$. For example, if f is the function defined by $f(x) = x^2$ for $0 \leq x \leq 1$. and g is the function defined by $g(x) = 1 + x$ for $0 \leq x \leq 1$. then $f < g$, because, if x is an arbitrary member of $[0,1]$, then $x^2 < 1 + x$, fer the following reason: if $0 < x < 1$, then $x^2 < x$, so $x^2 < 1 + x$; if $x = 0$, then $x^2 = 0$ and $1 + x = 1$, so $x^2 < 1 + x$; if $x = 1$ then $x^2 = 1$ and $1 + x = 2$, so $x^2 < 1 + x$.) □

Definition 16. Let n be an integer. We say that n is

- positive if $n > 0$,
- negative if $n < 0$,
- nonnegative if $n \geq 0$,
- nonpositive if $n \leq 0$. □

The precise meaning of "positive"

The distinction between "positive" and "nonnegative" is important. "Positive" means "> 0", whereas "nonnegative" means "≥ 0". So the ***positive integers*** are exactly the same as the natural numbers, and the ***nonnegative integers*** are the natural numbers together with 0.

Theorem 28.

1. *The sum of two positive integers is a positive integer.*
2. *The product of two positive integers is a positive integer.*
3. *The sum of two negative integers is a negative integer.*
4. *The product of two negative integers is a positive integer.*
5. *The product of a positive integers and a negatiue integer is a negative integer.*

Proof. These statements are so trivial that they do not need really a proof. But we will give one all the same.

The first and second statement are true because we already know that the sum and the product of two natural numbers is a natural number, and "positive integer" means exactly the same as "natural number". The third and fourth statements are true because, if a and b are negative integers, then $-a \in \mathbb{N}$ and $-b \in \mathbb{N}$, so

- $(-a) + (-b) \in \mathbb{N}$ and $(-a) \times (-b) \in \mathbb{N}$. But $(-a) + (-b) = -(a + b)$, so $-(a + b) \in \mathbb{N}$, and then $a + b$ is negative.
- $(-a) \times (-b) = ab$, so $ab \in \mathbb{N}$, i.e., ab is positive.

The fifth statement is true because, if a is a positive integer and b is a negative integer, then $a \in \mathbb{N}$ and $-b \in \mathbb{N}$, so $a \times (-b) \in \mathbb{N}$. But $a \times (-b) = -ab$, so $-ab \in \mathbb{N}$, and then ab is negative. □

Problem 17. ***Prove*** *the following laws for manipulating inequalities:*

1. *If a, b, c, d are integers, $a \leq b$ and $c < d$, then $a + c < b + d$.*
2. *If a, b, c, d are integers, $a \leq b$ and $c \leq d$, then $a + c \leq b + d$.*
3. *If a, b, c, d are integers, $a < b$, $c < d$, $a \geq 0$, and $c \geq 0$ then $ac < bd$.*
4. *If a, b are integers, $a < b$, and $a \geq 0$ then $a^2 < b^2$.*

NOTE: The square of an integer a is defined by

$$a^2 = a \times a\,.$$

Naturally, this definition makes sense on any system of objects in which an operation of multiplication is defined, such as, for example, the rational numbers, the real numbers, the complex numbers, square matrices, or functions. □

6.2 When is the product of two integers equal to zero?

Is it possible for the product of two nonzero integers to be equal to zero? The answer is "no", and the proof of this fact is very easy, now that we know about the ordering of the integers, so we give it now.

Theorem 29. *If a, b are integers such that $ab = 0$, then $a = 0$ or $b = 0$.*

Proof.
Let a, b be arbitrary integers.

Assume that $ab = 0$.

We want to prove that $a = 0$ or $b = 0$.

We will do a proof by contradiction .

Assume that it is not true that $a = 0 \vee b = 0$.

Then $a \neq 0$ and $b \neq 0$.

Since $a \neq 0$, either $a > 0$ or $a < 0$.

Similarly, either $b > 0$ or $b < 0$, because $b \neq 0$.

So there are four possibilities:

1. $a > 0$ and $b > 0$.
2. $a > 0$ and $b < 0$.
3. $a < 0$ and $b > 0$.
4. $a < 0$ and $b < 0$.

In cases 1 and 4, Theorem 28 tells us that $ab > 0$. So $ab \neq 0$.

In cases 2 and 3, Theorem 28 tells us that $ab < 0$. So $ab \neq 0$.

So we have proved that $ab \neq 0$ in all four cases.

Hence $ab \neq 0$.

But we know that $ab = 0$.

So $ab \neq 0 \wedge ab = 0$, which is clearly a contradiction.

We have derived a contradiction from the assumption that the sentence "$a = 0 \vee b = 0$" is not true. So the sentence is true, that is, $\boxed{a = 0 \vee b = 0}$. **Q.E.D.**

6.3 The cancellation law for multiplication

Now that we know how to order the integers, we can use this to prove the ***cancellation law for multiplication***:

Theorem 30. *If a, b, c are arbitrary integers such that $c \neq 0$ and $ac = bc$, then it follows that $a = b$. That is,*

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})((c \neq 0 \wedge ac = bc) \Longrightarrow a = b)\,. \tag{6.2}$$

Proof.

Let a, b, c be arbitrary integers.

Assume that $c \neq 0$ and $ac = bc$.

Then $ac - bc = 0$.

But $ac - bc = (a - b)c$.

So $(a - b)c = 0$.

Then Theorem 29 tells us that $a - b = 0$ or $c = 0$.

But $c \neq 0$.

Hence $a - b = 0$.

So $a = b$.

We have proved "$a = b$" assuming that $c \neq 0 \wedge ac = bc$.

So we have proved "if $c \neq 0 \wedge ac = bc$ then $a = b$.", that is, "$(c \neq 0 \wedge ac = bc) \Longrightarrow a = b$."

We have proved "$(c \neq 0 \wedge ac = bc) \Longrightarrow a = b$" for arbitrary integers a, b, c. So we can conclude, thanks to the rule for proving universal sentences, that

$$\boxed{(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})((c \neq 0 \wedge ac = bc) \Longrightarrow a = b).}$$

Q.E.D.

7 *Examples of proofs by contradiction and by induction

7.1 Solutions of some Diophantine equations

A Diophantine equation is an equation in one or several variables for which we are only seeking solutions that are integers.

7.1.1 Pythagorean triples

A famous example of a Diophantine equation, motivated by Pythagoras's theorem, is the equation

$$x^2 + y^2 = z^2 \,. \tag{7.3}$$

An integer solution of (7.3) is a triple (a, b, c) of integers such that $a^2+b^2 = c^2$. An integer solution of (7.3) is called a Pythagorean triple.

A well known example of a Pythagorean triple is $(3, 4, 5)$. This is an integer solution of (7.3) because $3^2 + 4^2 = 9 + 16 = 25 = 5^2$.

Beginning with the Babylonians some 3,000 years ago, mathematicians have asked the following questions:

1. Are there infinitely many Pythagorean triples?

2. Is there a simple way to generate all the Pythagorean triples?

The asnwer to the first question as stated, is "yes", but for a very stupid reason: just take the triple $(3, 4, 5)$ and multiply all three numbers by a natural number n. Then you get the triple $(3n, 4n, 5n)$, and this is also a Pythagorean triples because $(3n)^2 + (4n)^2 = 9n^2 + 16n^2 = 25n^2 = (5n)^2$.

So in this way we can generate an infinite number of Pythagorean triples: $(6, 8, 10)$, $(9, 12, 15)$, $(12, 16, 20)$, and so on. But notice that all these triples have a common factor larger than 1. For example, $(6, 8, 10)$ has the common factor 2, $(9, 12, 15)$ has the common factor 3, and so on.

A much more interesting questions is whether there are infinitely many Pythagorean triples without a common factor.

Definition 17. An irreducible Pythagorean triple is a Pythagorean triple (a, b, c) such that a, b and c do not have a nontrivial common factor. (That is, there does not exist an integer k, different from 1 and -1, such that $k|a$, $k|b$, and $k|c$.) □

The triple $(3, 4, 5)$ is irreducible, Another famous example of an irreducible Pythagorean triple is $(5, 12, 13)$. (This is a Pythagorean triple because $5^2 = 25$, $12^2 = 144$, $13^2 = 169$, and $25 + 144 = 169$.)

Problem 18. ***Prove*** *that there exist infinitely many irreducible Pythagorean triples. (HINT:* $(n + 1)^2 = n^2 + 2n + 1$*.)* □

7.1.2 Expressing an integer as the difference of two squares

Let us look at the Diophantine equations

$$x^2 - y^2 = 27\,, \tag{7.4}$$
$$x^2 - y^2 = 28\,, \tag{7.5}$$
$$x^2 - y^2 = 29\,, \tag{7.6}$$
$$x^2 - y^2 = 30\,, \tag{7.7}$$
$$\tag{7.8}$$

and let us not forget that we are interested in ***integer solutions***.

For Equation (7.4) here are two solutions:

- First solution: $x = 6$ and $y = 3$. (This works because $6^2 - 3^2 = 36 - 9 = 27$.)
- Second solution: $x = 14$ and $y = 13$. (This works because $14^2 = 196$ and $13^2 = 169$, so $14^2 - 3^3 = 196 - 169 = 27$.)

(And, of course, there are also six other solutions, namely, $x = -8$ and $y = 6$, $x = 8$ and $y = -6$, $x = -8$ and $y = -6$, $x = -14$ and $y = 13$, $x = 14$ and $y = -13$, $x = -14$ and $y = -13$. But these solutions are not very interesting, so we will from now on look for solutions x, y that are ***nonnegatve integers***.)

And we could ask

Q1: *Does Equation (7.4) have other solutions besides the two we have shown?*

For Equation (7.5) here is a solution:

- Let $x = 8$, $y = 6$. (This works because $8^3 - 6^2 = 64 - 36 = 28$.)

And we could ask

Q2: *Does Equation (7.5) have other solutions besides the one we have shown?*

For Equation (7.6) here is a solution:

- Let $x = 8$, $y = 6$. (This works because $8^3 - 6^2 = 64 - 36 = 28$.)

And, once again, we could ask

Q3: *Does Equation (7.6) have other solutions besides the one we have shown?*

Finally, let us look at Equation (7.7). Try as hard as you can, you will ***not*** find a solution.

So it would be natural to ask

Q4: *Does Equation (7.7) have any solutions at all?*

Just because you have spent a lot of time trying to find a solution and failed, this does not prove that the equation does not have a solution. To prove that, we need ***reasoning***. We have to give a ***proof*** that the solution does not exist. And here is the proof.

Theorem 31. *Equation (7.7) does not have any integer solutions. That is, there do not exist integers x, y such that $x^2 - y^2 = 30$.*

Proof. We prove our result by contradiction .

Assume there exist integers x, y such that $x^2 - y^2 = 30$.

Pick a pair of such integers and call them a, b.

So $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, and $a^2 - b^2 = 30$.

It is well known that $a^2 - b^2 = (a - b)(a + b)$.

So $(a - b)(a + b) = 30$.

On the other hand, the numbers a, b are both odd or both even. (Reason: Suppose[7] a was even and b odd. Then a^2 would be even and b^2 would be odd, so $a^2 - b^2$ would be odd. But $a^2 - b^2 = 30$, and 30 is even. A similar argument[8] proves that it cannot be the case that a is odd and b is even.)

[7]Here we have a proof by contradiction .

[8]And another proof by contradiction ,

Since a and b are both odd or both even, the numbers $a-b$ and $a+b$ are even.

So we may pick integers j, k such that $a-b=2j$ and $a+b=2k$.

Then $30=(a-b)(a+b)=(2j)\times(2k)=4jk$.

So 30 is divisible by 4.

But 30 is not divisible by 4.

Therefore $\boxed{\text{30 is divisible by 4 and 30 is not divisible by 4}}$, which is a contradiction..

So the assumption that there exist integers x, y such that $x^2-y^2=30$ has led us to a contradiction.

Therefore $\boxed{\text{there do not exist integers } x, y \text{ such that } x^2-y^2=30}$. **Q.E.D.**

The method used in the proof of Theorem 31 can be generalized, and one can prove the following:

Theorem 32. *Let n be an integer. Then there exist integers x, y such that $x^2-y^2=n$ if and only if n is either odd or divisible by 4.*

Proof.

YOU DO IT.

Problem 19. ***Prove*** *Theorem 32.*

HINTS:

1. *Study carefully the proof of Theorem 31, and use a similar method.*
2. *Read Subsection 7.2 to find out how to prove "if and only if" statements.*

□

7.2 Biconditionals (i.e., "if and only if")

The ***biconditional*** symbol $\iff$ is read as "if and only if".

A sentence of the form "$A \iff B$" is a ***biconditional sentence***. We read it as "A if and only if B". For example, if A is the sentence "$x \geq 0$", and B is the statement "x has a square root", then we can read $A \iff B$ as "$x \geq 0$ if and only if x has a square root".

The meaning of the biconditional symbol. "A if and only if B" means "if A then B and if B then A".

That is, "$A \iff B$" means "$(A \implies B) \wedge (B \implies A)$".

The truth value of a biconditional. *If A and B are both true or both false then $A \Leftrightarrow B$ is true. If one of A, B is true and the other one is false, then $A \Leftrightarrow B$ is false.* So the truth value of $A \Leftrightarrow B$ is given in terms of the truth values of A and B by the following ***truth table***:

A	B	$A \Leftrightarrow B$
T	T	T
T	F	F
F	T	F
F	F	T

7.2.1 How to prove a biconditional sentence

The rule for proving biconditionals. In order to prove "$A \iff B$", you prove "$A \implies B$" and "$B \implies A$".

As an example, let us prove:

Proposition 1. *If n is an integer, then n is divisible by 6 if and only if n is divisible by 2 and by 3.*

Proof.
We want to prove that

$$(\forall n \in \mathbb{Z})\Big(6|n \iff (2|n \wedge 3|2)\Big). \tag{7.9}$$

Let n be an arbitrary integer.

We want to prove that

$$6|n \Longrightarrow (2|n \wedge 3|n) \tag{7.10}$$

and that

$$(2|n \wedge 3|n) \Longrightarrow 6|n\,. \tag{7.11}$$

Proof of (7.10):

Assume that $6|n$.

Then we can pick an integer k such that $n = 6k$.

Therefore, $n = 3 \times (2k)$ and, since $2k \in \mathbb{Z}$, it follows that $3|n$.

Also, $n = 2 \times (3k)$ and, since $3k \in \mathbb{Z}$, it follows that $2|n$.

So $\boxed{2|n \text{ and } 3|n}$.

So we have proved (7.10).

Proof of (7.11):

Assume that $2|n$ and $3|n$.

Then we can pick integers j, k such that $n = 2j$ and $n = 3k$.

Then

$$\begin{aligned} n &= n \times 1 \\ &= n \times (3 - 2) \\ &= 3n - 2n \\ &= 3 \times (2j) - 2 \times (3k) \\ &= 6j - 6k \\ &= 6(j - k)\,. \end{aligned}$$

So $\boxed{6|n}$.

So we have proved (7.11).

Since we have proved (7.10) and (7.11), the rule for proving biconditionals tells us that we can conclude that

$$6|n \iff (2|n \wedge 3|n)\,. \tag{7.12}$$

Since we have proved (7.12) for an arbitrary integer n, we can conclude that

$$(\forall n \in \mathbb{Z})\Big(6|n \iff (2|n \wedge 3|n)\Big)\,. \tag{7.13}$$

Q.E.D.

7.3 An inequality

Let us use induction to prove an inequality:

Theorem 33. *If x is a positive real number, and n is a natural number, then*

$$(1+x)^n \geq 1 + nx\,. \tag{7.14}$$

Proof. We want to prove that

$$(\forall x \in \mathbb{R})\left(x > 0 \Longrightarrow \Big((\forall n \in \mathbb{N})(1+x)^n \geq 1 + nx\Big)\right). \tag{7.15}$$

Let x be an arbitrary real number.

We want to prove that

$$x > 0 \Longrightarrow \Big((\forall n \in \mathbb{N})(1+x)^n \geq 1 + nx\Big)\,. \tag{7.16}$$

Assume that $x > 0$.

We want to prove that

$$(\forall n \in \mathbb{N})(1+x)^n \geq 1 + nx\,. \tag{7.17}$$

We prove this by induction.

Let $P(n)$ be the statement "$(1+x)^n \geq 1 + nx$".

Base step. We have to prove $P(1)$.

But $P(1)$ says "$1 + x \geq 1 + x$", and this is obviously true.

So $P(1)$ is true, and we are done with the base case.

Inductive step. We have to prove

$$(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))\,. \tag{7.18}$$

Let n be an arbitrary natural number.

Assume $P(n)$.

Then

$$(1+x)^n \geq 1 + nx\,. \tag{7.19}$$

Multiplying both sides of (7.19) by $1 + x$ (which is possible because $1 + x > 0$), we get

$$(1+x)^{n+1} \geq (1+x)(1+nx)\,. \tag{7.20}$$

But

$$\begin{aligned}(1+x)(1+nx) &= 1 + x + nx + nx^2 \\ &= 1 + (n+1)x + nx^2 \\ &\geq 1 + (n+1)x\,.\end{aligned}$$

(The fact that $1+(n+1)x+nx^2 \geq 1+(n+1)x$ follows because $nx^2 \geq 0$ and then, adding $1 + (n+1)x$ to both sides, we get $1 + (n+1)x + nx^2 \geq 1 + (n+1)x$.)

So

$$(1+x)^{n+1} \geq 1 + (n+1)x\,. \tag{7.21}$$

That is, $P(n+1)$ holds.

So we have proved (7.18). Since we have also proved $P(1)$, we can use the PMI to conclude that (7.16) holds, i.e., that

$$(\forall n \in \mathbb{N})(1+x)^n \geq 1 + nx\,. \tag{7.22}$$

Since we have proved (7.22) assuming that $x > 0$, we can cnnclude that

$$x > 0 \Longrightarrow \Big((\forall n \in \mathbb{N})(1+x)^n \geq 1 + nx\Big)\,. \tag{7.23}$$

Since we have proved (7.23) for an arbitrary real number x, we can conclude that

$$(\forall x \in \mathbb{R})\left(x > 0 \Longrightarrow \Big((\forall n \in \mathbb{N})(1+x)^n \geq 1 + nx \Big) \right), \tag{7.24}$$

which is exactly what we wanted to prove. **Q.E.D.**

With a little bit more work, it is possible to prove a stronger theorem:

Theorem 34. *If x is a positive real number, and n is a natural number, then*

$$(1+x)^n \geq 1 + nx + \frac{n(n-1)}{2}x^2 \,. \tag{7.25}$$

Proof.

YOU DO THIS ONE. □

Problem 20. ***Prove*** *Theorem 34.* □

7.3.1 An application of Theorem 34

Let us prove that

$$\lim_{n\to\infty} \sqrt[n]{n} = 1 \,. \tag{7.26}$$

Define

$$\alpha_n = \sqrt[n]{n} - 1 \,.$$

To prove (7.26), we have to prove that

$$\lim_{n\to\infty} \alpha_n = 0 \,. \tag{7.27}$$

It is clear that $\alpha_n \geq 0$. (Reason: $\sqrt[n]{n} \geq 1$, because if $\sqrt[n]{n}$ was < 1, it would follow that $\left(\sqrt[n]{n}\right)^n < 1$, but $\left(\sqrt[n]{n}\right)^n = n$, and $n \geq 1$.)

Also, $1 + \alpha_n = \sqrt[n]{n}$, so

$$(1+\alpha_n)^n = n \,. \tag{7.28}$$

Using the inequality of Theorem 34, we get

$$(1+\alpha_n)^n \geq 1 + n\alpha_n + \frac{n(n-1)}{2}\alpha_n^2 \,. \tag{7.29}$$

So

$$\begin{aligned} n &= (1+\alpha_n)^n \\ &\geq 1 + n\alpha_n + \frac{n(n-1)}{2}\alpha_n^2 \\ &\geq \frac{n(n-1)}{2}\alpha_n^2 \,. \end{aligned}$$

Hence

$$n \geq \frac{n(n-1)}{2}\alpha_n^2 \,,$$

so

$$1 \geq \frac{n-1}{2}\alpha_n^2 \,,$$

and then

$$\alpha_n^2 \leq \frac{2}{n-1} \,,$$

so

$$\alpha_n \leq \sqrt{\frac{2}{n-1}} \,.$$

Hence the numbers α_n satisfy

$$0 \leq \alpha_n \leq \sqrt{\frac{2}{n-1}} \,.$$

So the α_n are 'sandwiched" between two sequences that converge to 0. Hence $\lim_{n\to\infty} \alpha_n = 0$ by the sandwiching theorem.

7.4 Some formulas for sums

In this section we use the notation "$\sum_{k=1}^n a_k$" for "$a_1 + a_2 + \cdots + a_n$".

Theorem 35. *If n is an arbitrary natural number, then*

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2} \,. \tag{7.30}$$

(That is, $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.)

Proof. Let $P(n)$ be the statement "$\sum_{k=1}^n = \frac{n(n+1)}{2}$".

We prove $(\forall n \in \mathbb{N})P(n)$ by induction.

Base step. $P(1)$ says "$1 = \frac{1(1+1)}{2}$", which is obviously true. So $P(1)$ is true.

Inductive step.

We prove $(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))$.

Let n be an arbitrary natural number.

Assume that $P(n)$ is true.

Then $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Therefore

$$\begin{aligned}
\sum_{k=1}^{n+1} k &= (\sum_{k=1}^{n} k) + (n+1) \\
&= \frac{n(n+1)}{2} + (n+1) \\
&= (n+1)\left[\frac{n}{2} + 1\right] \\
&= (n+1) \times \frac{n+2}{2} \\
&= \frac{(n+1)(n+2)}{2}\,.
\end{aligned}$$

So

$$\sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2}\,.$$

That is, $P(n+1)$ holds.

We have proved $P(n+1)$ assuming $P(n)$. Hence $\boxed{P(n) \Longrightarrow P(n+1)}$.

We have preved $P(n) \Longrightarrow P(n+1)$ for an arbitrary natural number n. Therefore $(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))$, which completes the inductive step.

Hence, by the PMI, $(\forall n \in \mathbb{N})P(n)$, that is,

$$(\forall n \in \mathbb{N}) \sum_{k=1}^{n} k = \frac{n(n+1)}{2}\,.$$

Q.E.D.

Using the same method, many other formulas for sums can be proved. Here is an exmaple of a rather remarkable one:

Theorem 36. *If n is a natural number, then*

$$\sum_{k=1}^{n} k^3 = \Big[\frac{n(n+1)}{2}\Big]^2, \tag{7.31}$$

that is:

$$1^3 + 2^3 + 3^3 + 4^3 + \cdots + n^3 = \Big[\frac{n(n+1)}{2}\Big]^2.$$

Proof. **YOU DO THIS ONE.**

Problem 21.

1. ***Compute*** *the sum $\sum_{k=1}^{n} k^3$ for $n = 1, 2, 3, 4, 5$ and 6.*
2. ***Verify*** *that in each case the sum you got is a perfect square (i.e., the square of an integer).*
3. ***Prove*** *Theorem 36.* □

Problem 22.

1. ***Compute*** *the sum $\sum_{k=1}^{n} k^2$ for $n = 1, 2, 3, 4, 5$ and 6.*
2. ***Verify*** *that in each case the sum you got agrees with the formula*

$$\sum_{k=1}^{n} k^2 = \frac{n + 3n^2 + 2n^3}{6}. \tag{7.32}$$

3. ***Prove*** *that Formula (7.32) holds for every natural number n.* □

7.5 Irrational numbers

In this section we use the definition of "rational number", plus two facts that have not been proved yet, but will be proved later.

Definition 18. A rational number is a real number r such that there exist integers m, n for which:

1. $n \neq 0$
2. $r = \frac{m}{n}$. □

Fact 1. *Every rational number is equal to a quotient $\frac{m}{n}$ of two integers that have no nontrivial common factor.*

Fact 2. *(Euclid's Lemma.) If a, b, p are integers, p is a prime number, and $p|ab$, then $p|a$ or $p|b$.*

7.5.1 Real numbers vs. natural numbers

Since ancient times, it was understood that there were two kinds of "numbers":

1. The "counting numbers", that we now call "natural numbers". These are the numbers that we use to count: 1, 2, 3, 4, 5, ...
2. "Geometric magnitudes", that we use to measure amounts that can vary continuously, such as lengths, areas, volumes, weights.

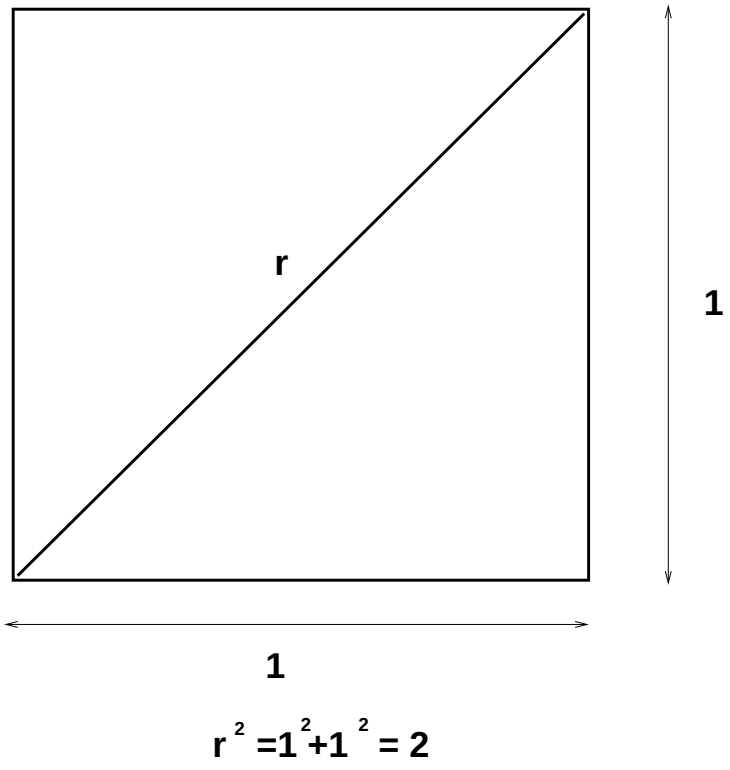
Geometric magnitudes can be subdivided indefinitely: for example,

- You can take a segment of length 1 (assuming we have fixed a unit of lenght), and divide it into seven equal segments, each one of which has length $\frac{1}{7}$. And then you can draw segments whose lenghts 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.

At first, it was believed that fractions were sufficient to measure all possible lenghts. This meant that ***any two lenghts were commensurable***[9]***: given and two lengths*** a ***and*** b***, you can take a sufficiently small lenght*** u ***(the unit of lenght) and find natural numbers*** m***,*** n ***such that*** $a = mu$ ***and*** $b = mu$***. That is, if*** a***,*** b ***are any two lenghts, then*** $b = \frac{m}{n} \times a$***, or, equivalently,*** $b = fa$ ***for some fraction*** f***.***

But then a momentous discovery of far-reaching consequences was made: ***it is not true that any two lenghts are commensurable***.

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



[9] "Conmensurable" means "measurable together", that is, you can use a ruler of the same lenght u to "measure a and b together", that is, to express both lengths a and b as integer multiples mu, nu of the unit of lenght u.

But 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 L, that we could call "$\sqrt{2}$", is not a fraction.

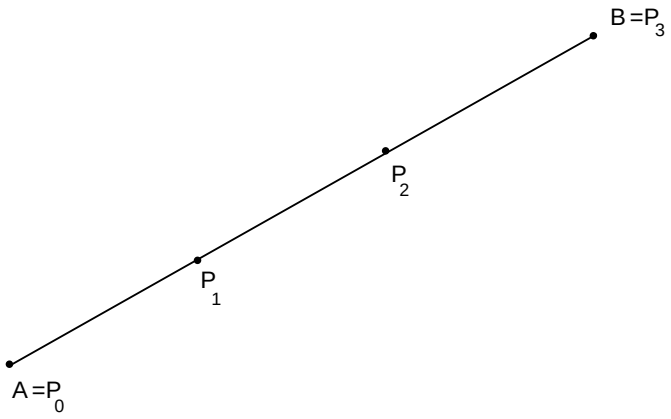
Today we would say that

- Those numbers that are not fractions, such as $\sqrt{2}$, do indeed exist, and we call them "real numbers".
- The fractions, called "rational[10] numbers", are real numbers, but many real numbers are "irrational" numbers, that is, numbers that are not rational.
- Actually, most[11] 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.

[10]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 irrrationality 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.

[11]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.

Problem 23. ***Explain*** how, if you are given two distinct points A, B, and the segment from A to B is declared to be the unit of length (i.e. to have length 1), you could subdivide the segment $\overline{AB}$ into three equal parts ***using a ruler and a compass and nothing else.*** (By "subdividing $\overline{AB}$ into three equal parts" I mean "finding four points $P_0, P_1.P_2, P_3$ lying on the segment $\overline{AB}$ such that $P_0 = A$, $P_3 = B$, and the segments $\overline{P_0P_1}$, $\overline{P_1P_2}$, $\overline{P_2P_3}$, have length $\frac{1}{3}$."



Dividing a segment into three equal parts

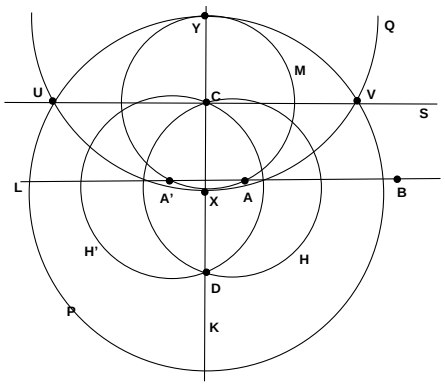
The following are allowed:

- *Given two points A, B, you can draw the straight line segment joining them, and you can prolong this line and draw the entire line going through A and B.*
- *Given two points A, B, you can draw the circle with center A going through B.*
- *Once you have two lines S and T, or a line S and a circle T, or two circles S, T, you can find (i.e., mark on the paper) the point or points of intersection, of S and T, if S and T intersect.*

For example, suppose I give you two distinct points A, B, and a third point C not lying on the line that joins A to B, and I ask you to construct the line through C that is parallel to the line from A to B. Here is how you would do that:

1. *You draw the line L that goes through A and B.*
2. *You draw the circle centered at C that goes through*[12] *A and call it M.*
3. *You mark the point of intersection of M and L other than A, an call it A'.*
4. *You draw the circle centered at A that goes through C and call it H.*
5. *You draw the circle centered at A' that goes through C, and call it H'*
6. *You mark the point of intersection of H and H' other than C, and call it D.*
7. *You draw the line through C and D, and call it K. Then K is a line perpendicular to L and going through C.*
8. *You mark the two points of intersection of the line K and the circle M, and call them X and Y.*
9. *You draw the circle centered at X that goes through Y and call it P.*
10. *You draw the circle centered at Y that goes through X and call it Q.*
11. *You mark the two points of intersection of the circles P and Q, and call them U and V.*
12. *You draw the line joining U and V and call it S.*
13. *Then S is the solution. That is, S is a line through C parallel to L.* □

[12]Or you could draw the circle centered at C that goes through B.



Construction of a line parallel to a given line through a given point

Problem 24. ***Prove*** *that for every natural number n it is possible to subdivide a given segment into n equal segments. (Precisely: for every $n \in \mathbb{N}$, if we are given two distinct points A, B, then it is possible to cinstruct, using a ruler and a compass and nothing else, points A_0, A_1, ..., A_n, lying on the segment $\overline{AB}$, such that $A_0 = A$, $A_n = B$, and all the segments $\overline{A_{j-1}A_j}$, for $j = 1. \ldots, n$, have the same length (which will, of course, be equal to $\frac{1}{n}$ times the lenght of the segment $\overline{AB}$).* □

Problem 25. ***Prove*** *by induction that for every natural number n, if we are given two distinct points A, B, then it is possible to construct, using a ruler and a compass and nothing else, a point C, lying on the line from A to B, such that the length of the segment $\overline{AC}$ is $\sqrt{n}$ times the length of $\overline{AB}$.* □

7.5.2 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[13]. 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.)

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

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

> 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". 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.

7.5.3 What is a "real number", really?

The discovery that there are lenghts 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.

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

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 commitment to the existence of a "number" r such that $r^2 = 2$.

Theorem 37. *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.
> 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 $r^2 = 2$, 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[14] that m is not even. We know that every integer is even or odd; so, since m is not even, m must be odd. And we know that the product of two odd integers is odd. So, since m is odd, it follows that m^2 is odd as well. But we have proved that m^2 is even. And we know that an integer cannot be both even and odd. 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.
> So we may pick an integer k such that $m = 2k$.
> Then $m^2 = 4k^2$.
> But $m^2 = 2n^2$.

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

Hence $2n^2 = 4k^2 = 2 \times (2k^2)$, so

$$2n^2 = 2 \times 2k^2 \,. \tag{7.33}$$

Using the cancellation law for multiplication (i.e., Theorem 30), we can cancel the factor "2" in (7.33), and conclude that $n^2 = 2k^2$.
So n^2 is even.
But then n is even. (Reason: Assume[15] that n is not even. We know that every integer is even or odd; so, since n is not even, n must be odd. And we know that the product of two odd integers is odd. So, since n is odd, it follows that n^2 is odd as well. But we have proved that n^2 is even. And we know that an integer cannot be both even and odd. 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 $2|m$ and $2|n$.
But m and n do not have a nontrivial common factor.
So 2 cannot be a common factor of m and n.
In other words, it is not true that "$2|m$ and $2|n$".
So the sentence "$2|m$ and $2|n$" is true and is not true, which is a contradcition.

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

Therefore $\boxed{\text{there does exist a rational number } r \text{ such that } r^2 = 2}$. **Q.E.D.**

7.6 More irrationality proofs

We now use the same tecbnique to prove that $\sqrt{3}$ is irrational. The key point here is to realize that "even vs. odd" now has to be replaced by "divisible by 3 vs. not divisible by 3".

Theorem 38. *There does not exist a rational number r such that $r^2 = 3$.*

Proof. We will do a proof by contradiction .

[15] Another proof by contradiction !

Assume that there exists a rational number r such that $r^2 = 3$.

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

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

So $3|m^2$.

But then $3|m$. (Reason: By Euclid's Lemma (i.e. Fact 2) since 3 divides the product $m.m$, it follows that 3 must divide one of the factors. So $3|m$.)

Since $3|m$, we may pick an integer k such that $m = 3k$.

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

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

Hence $3n^2 = 9k^2 = 3 \times (3k^2)$, so

$$3n^2 = 3 \times 3k^2 \,. \tag{7.34}$$

Using the cancellation law for multiplication, we can cancel the factor "3" in (7.34), and conclude that $n^2 = 3k^2$.

So $3|n^2$.

But then $3|n$. (Reason: By Euclid's Lemma (i.e. Fact 2) since 3 divides the product $n.n$, it follows that 3 must divide one of the factors. So $3|n$.)

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

Hence m and n have a nontrivial common factor.

But m and n do not have a nontrivial common factor.

Therefore

$$\boxed{\begin{array}{l}m \text{ and } n \text{ have a nontrivial common factor, and } m \text{ and } n \text{ do} \\ \text{not have a nontrivial common factor,}\end{array}}$$

which is a contradiction,

So the assumeption 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**.

Problem 26. ***Prove*** *that each of the following numbers is irrational:*

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

Problem 27. ***Prove or disprove***[16] *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 a rational number.*
4. *The product of two irrational numbers is a rational number.*
5. *The sum of two irrational numbers is an irrational number.*
6. *The product of two irrational numbers is an irrational number.*
7. *The sum of a rational number and an irrational number is an irrational number.*

[16]To ***disprove*** a stetement means "to prove that the statement is false". For example, when we proced that 1 is not even we disproved the statement '1 is even".

8. *The product of a rational number and an irrational number is an irrational number.* □

Problem 28.

1. ***Explain*** *why the following "proof" that* $\sqrt{2}+\sqrt{3}$ *is irrational is wrong:*

   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. ***Explain*** *why the following "proof" that* $\sqrt{6}$ *is irrational is wrong:*

   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.**

3. ***Give a correct proof*** *that* $\sqrt{2}+\sqrt{3}$ *is irrational.*

4. ***Give a correct proof*** *that* $\sqrt{6}$ *is irrational.*

5. ***Prove*** *that* $\sqrt[3]{2}$ *is irrational.*

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

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

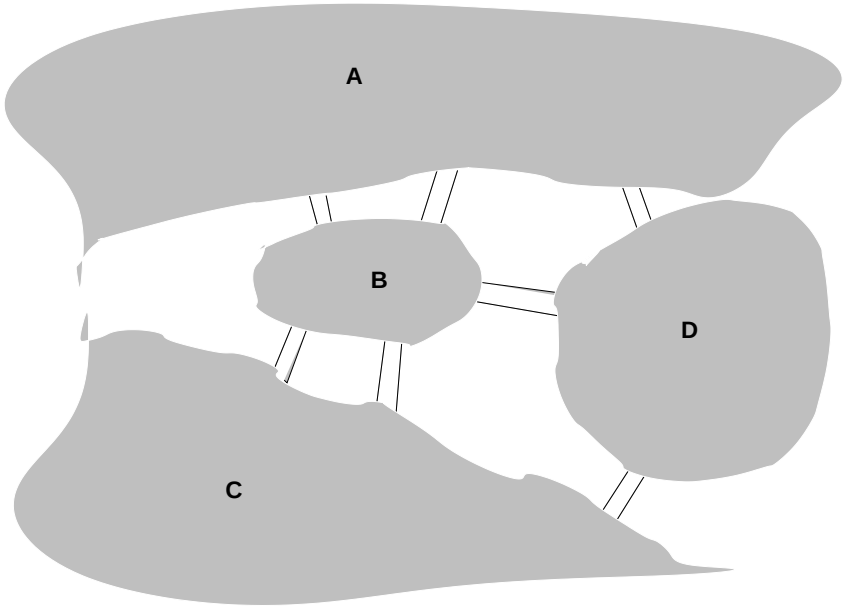
Problem 29. ***Prove*** *that, if* $n \in \mathbb{N}$*, and* $p_1, p_2, \ldots, p_n$ *are* n *distinct primes, then* $\sqrt{p_1}+\sqrt{p_2}+\cdots+\sqrt{p_n}$ *is irrational.* □

7.7 The seven bridges of Königsberg

In 1736, the great mathematician Leonhard Euler (1707-1783) wrote a paper on the ***Königsberg bridge problem***: *Is it possible to walk through the city of Königsberg crossing each of the town's seven bridges once and only once?* The city was divided into two parts by a river crossing it, and in addition

there were two islands, so the city truly had four parts, joined by seven bridges, as shown in the picture.

Euler's solution of the bridges of Königsberg problem marhed the birth of a new field of mathematics, now known as ***graph theory***, which has evolved into a major area of research, with an enormous variety of applications.



The seven bridges of Königsberg

Euler's answer was that *it is impossible to walk as proposed in the problem*: there is no way to walk through all seven bridges, crossing each bridge once and only once. Furthermore, Euler's proof is by contradiction, so it is most appropriate to include it here, to show you an example of how a proof by contradiction works.

Theorem 39. *There is no way to walk through all the seven bridges of Königsberg crossing each of the bridges once and only once.*

Proof.
We give a proof by contradiction.

> Assume there is a way to walk through all the seven bridges, crossing each bridge once and only once.

This walk starts in one of the four parts A, B, C, D into which the city is divided by the river.

Call this starting part S, so S is either A or B or C or D.

Furthermore, the walk ends in one of the four parts A, B, C, D.

Call this part E, so E is either A or B or C or D, and E could be the same as S, or not.

Let P be one of the four parts which is not S or E. (Such a part must exist, because there are four parts, and at most two of them can be S or E.)

Then our walk does not start or end at P, so it must enter P at some point through one of the bridges connecting P to the other parts, and then it must leave P through a different bridge. And, if it ever enters P again, it must be through a third bridge. And then it must leave P through a fourth bridge. And so on. So the total number of bridges connecting P to other parts that are crossed by our walk has to be even, because for every bridge used to enter P there must ne a different bridge used to leave P.

But our walk crosses all the bridges. And this implies that

$\boxed{\text{the number of bridges connecting } P \text{ to one of the other parts is even}}$.

On the other hand, for each the four parts the number of bridges connecting that part to the others is odd. (For part A the number is 3, for part B it is 5, for part C it is 3, and for part D it is also 3.)

Let n be the number of bridges connecting P to one of the other parts.

Then n is odd.

But we have proved that n is even.

So $\boxed{n \text{ is odd and } n \text{ is not odd}}$, which is clearly a contradiction.

Hence the assumption that it is possible to walk through Königsberg crossing each bridge once and only once has led us to a contradiction.

Therefore $\boxed{\text{such a walk is impossible}}$. **Q.E.D.**