MATHEMATICS 300 — FALL 2017

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S NOTES

PART I

Contents

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

Our first examples of proofs are going to be very simple. We are going to prove things that you already know, and that you believe are completely obvious. Do not worry about that:

- When you learn to swim, you first learn to do very simple things. You practice putting your face in the water while standing in the shallow end of the pool; then you practice floating while holding onto the side of the pool; then you practice floating without holding onto the side of the pool; then maybe you practice moving in the water using a flotation device, and so on.
- When you learned to read, you did not start by reading a Shakespeare play or a Jane Austen novel. You learned to read very simple words, like "dog", "cat", "dad". Then you moved on to more difficult words, to sentences, paragraphs, and longer and more complicated texts. And it took you quite a while to get to read really serious stuff.
- The same is true with proofwriting : we will start by doing some very simple proofs, such as for example a proof that $2 + 2 = 4$. You will complain by saying that "everybody knows that", but the point of doing such a proof is not to discover that $2 + 2 = 4$, but to practice proof-writing.
- Later in the course we will do really nontrivial things, including the proof of facts that will actually be new to you. So, ***if it bothers you that we are proving simple things that you already know are true, just wait a few weeks.***

A proof is a story about mathematical objects, such as numbers, lines, curves, sets, functions, or geometrical figures. So we have to start by introducing the "cast of characters" of our stories, that is, the mathematical objects that we will be talking about.

It turns out that the objects that we will need at this point are rather simple ones:

- The natural numbers.
- The integers.
- Sets.

2 Getting started: Some very simple proofs about the natural numbers and the integers

In our proofs, we will talk about mathematical objects and give them names, so we need to say a few words first about how to give names to things.

2.1 Naming things

2.1.1 Things

In these notes, we will be talking mostly about ***mathematical objects***, that is, numbers of various kinds (natural numbers, integers, rational numbers, real numbers, complex numbers, integers modulo n, etc.), sets, functions, relations, graphs, geometric objects (points, lines, segments, circles, planes, curves of various kinds, surfaces of various kinds, higher dimensional flat and curved spaces, etc.), and many other kinds of objects.

And in order to talk about these mathematical objects we will use ***mathematical language***. But mathematical language is a special language, in many ways similar to other languages such as English, and in many ways different. So, in order to talk about mathematical language we will want to say a few words about language in general, so that we can explain what makes mathematical language special.

THINGS

In these notes, the word ***thing*** refers to an object of any kind, concrete inanimate material objects such a table or a molecule or a planet, as well as plants, animals and people ("living things"), and abstract objects such as mathematical objects.

So, in these notes, Mount Everest is a thing, and the chair in which you are sitting is a thing, and a book is a thing, but so are a giraffe, a spider, and you, and I, and my uncle Jim.

Some students don't like using the word "thing" to refer to people, perhaps because they are thinking that "people are not things". My answers to that are:

1. We can use words in any way we like, as long as we do it consistently. So in this course we can decide how to use the word "thing", and there should be no problem as long as what we mean is clear to everybody.

2. We often do talk about "living things", and that includes people.

3. If you don't like using the word "thing" in this way, there is a word that's perfect for you: you can talk about "entities" instead. An entity is anything that exists. It can be a table, a river, a planet, an atom, a cell, a plant, a giraffe, a person, a number, a triangle, a matrix, a set, or a function. So just substitute the word "entity" for "thing" throughout these notes, and you will be fine.

2.1.2 Using variables to name things in English

In every language, the speakers want to be able to talk about things by giving them ***names***. The simplest way to do that is to give each thing an individual name, as when you call people with names such as "Mary", "John", or "George Washington". But this way of naming things is not very convenient, because in our daily life we have to talk about an enormous number of things, and it would be truly impossible to give an individual name to each one. (Just imagine if every time you want to ask a waiter for a spoon you had to find out first the name of that particular spoon!) So languages have developed devices for naming things without having to give each individual thing its own name.

Without getting into details about how this is done, the main point is that languages use ***variables***, that is, words or phrases that can be used as the name of some thing in one situation, and then can be reused later as the name of a different thing. For example, the phrases "this spoon", "the table", "his brother", and the words "he", "she", "it", "you", can be used and reused to serve as names of different things as the need arises. What is important is that there always has to be a way for the speakers to ***declare a value*** for a variable each time they want to use it to name a specific thing, to specify for how long this value declaration holds, when the declaration of value expires so that the variable is available to be used to name some other object.

Example 1. In a criminal court of law, the phrase "the defendant" is used as a variable. When a trial begins, someone announces in some way that, for the duration of this trial, the words "the defendant" will refer to a certain specific person. Then, during the trial, everybody refers to that person as "the defendant". When the trial is over, the variable "the defendant" becomes ***free***, that is, not attached to any particular person, and free to be used to refer to a new defendant when a new trial begins. □

Example 2. Consider the following paragraph:

> George Washington was the first president of the United States, and he served as president for two terms. He was succeeded by John Adams, who served only one term. When Adams ran for reelection to a second term, he was the object of malicious attacks by his opponents, and eventually lost the election to Thomas Jefferson.

In this text, the pronoun "he" appears three times. The first two times, it refers to George Washington, but the third time it refers to John Adams. So "he" is a variable. The mention of John Adams undoes the declaration that "he" stands for George Washington, and assigns the new value "John Adams" to the pronoun. □

Example 3. When you buy a house, the contract will probably contain a clause at the beginning declaring the words "the buyer" to stand for you for that particular contract. This means that the phrase "the buyer" is a variable, whose value is you for this contract. Once your attorney goes to the signing for the next house sale, where the buyer is a different person, then he will present this person with a different contract, in which "the buyer" has a totally different value. So the value of the phrase "the buyer" is fixed only within a specific contract, and changes when yo go another contract. □

2.1.3 Using variables to name things in mathematical language

In mathematical language, it is customary to use ***letters*** as variables, although it is perfectly possible to use as variables longer strings such as "*abb*" or "the number I have been talking about".

A free variable is a letter (or string of symbols) that is "unattached", in the sense that it has no particular value, and is free to be assigned any value we want.

A temporary constant is a variable that has been assigned a specific value, by means of a ***value declaration***.

We can turn a free variable into a temporary constant by ***declaring its value.*** For example, we can say:

(*) Let $x = \frac{1+\sqrt{5}}{2}$. Then $x^2 = 1 + x$.

Here, the phrase "let $x = \frac{1+\sqrt{5}}{2}$" effectively declare the variable x to be a constant, that stands for the number $\frac{1+\sqrt{5}}{2}$. And, clearly, statement (*) is just a roundabout way to say that

$$\Big(\frac{1+\sqrt{5}}{2}\Big)^2 = 1 + \frac{1+\sqrt{5}}{2}\,.$$

Once this particular use of the variable x is over, you could, if you want to, use the same letter to represent some other number or object of any kind. But in that case it would have to be very clear that the old declaration that $x = \frac{1+\sqrt{5}}{2}$ no longer applies.

You could do this, for example, by saying something like

> Let $x = \frac{1+\sqrt{5}}{2}$. Then $x^2 = 1 + x$.
> Now suppose, instead, that $x = \frac{1-\sqrt{5}}{2}$. Then it is also true that $x^2 = 1 + x$.

The word "now" serves the purpose of telling the reader that "we are starting all over again, and the old declared value of x no longer applies." (And the word "instead", which is unnecessary, strictly speaking, reinforces that.)

The declared value of a constant can be ***unknown*** to us, even if it is fixed in some way.

For example, we could write

Let a be the number such that $3a + 5 = 17$.
Then $3a = 17 - 5 = 12$. Therefore $a = 4$.

In this case, when we declare a to be have a specific value, we are not explicitly stating what that value is. We are just declaring that the value of a must satisfy a certain condition, namely, the equation $3a + 5 = 17$. Then we go on and solve the equation, so we end up with $a = 4$, but our knowledge of the value of a is a *consequence* of our original declaration together with some reasoning.

2.1.4 Arbitrary things

Another way in which a constant can be assigned a value is by declaring it to be an ***arbitrary*** object of a certain kind, and stipulating certain conditions that it must satisfy. (See the box on page 7 for a detailed explanation of how this works.)

ARBITRARY THINGS

An ***arbitrary thing*** of a certain kind is a fixed thing about which we know nothing, except that it is of that kind. For example, an “arbitrary integer” is an integer about which you know nothing other than that it is an integer.

The way you should think about “arbitrary things ” is as follows: imagine that there is somebody (a friend, or a computer, or an alien from the planet Metaluna) whose job is, every time you write “let a be an arbitrary thing,” to pick one such thing, write down what it is on a piece of paper, and then put the paper in an envelope and seal the envelope.

We will call such a person (or computer, or alien) the **CAT** (“creator of arbitrary things”). So, for example, if you say “let a be an arbitrary natural number” then the **CAT** will pick a natural number and write down what it is on a piece of paper that will go inside the envelope. And later. after you have finished talking, you or the CAT will open the envelope, and you will know who a really was. And at that point, if what you said was not true, you lose.

The key fact is this: ***If you are going to be talking about this arbitrary thing, and want to be sure that what you say is true, you have to be sure that what you say is true of all the things of the given kind,*** because if there is just one thing for which what you said is not true, then a could turn out to be that thing, and then you will have been proved wrong.

Example 4. Suppose you say:

Let n be an arbitrary integer.

What can you say after that, being sure that it is true?

Certainly, you cannot say that $n = 2$, because n could be 1, or -7, or 25.

And you cannot say that n is even, because n could be odd.

But here are a few things you *can* say:

- n is either a natural number, or the negative of a natural number, or zero.

- $n + n^2$ is even. (Reason: n is either even or odd. If n is even, then n^2 is also even, so the sum $n + n^2$ is even. If n is odd, then n^2 is also odd, and the sum of two odd integers is even, so $n + n^2$ is even. So, no matter who n is, whether it is even, or odd, positive or negative, yuuo can be sure that $n + n^2$ is even.)
- $n^2 \geq 0$. (Reason: the square of every real number, and in particular of every integer, is ≥ 0.)

On the other hand, you cannot say that $n^2 > 0$, because n could be 0, in which case "$n^2 > 0$" would no be true. □

Example 5. Suppose you say:

Let m, n be arbitrary natural numbers.

What can you say after that, being sure that it is true?

Certainly, you cannot say that $m = n$, because m and n could be different.

And you cannot say that $m \neq n$, because m and n could be equal.

And you cannot say that $m > n$, because m could be smaller than n.

But here are a few things you *can* say:

- $m + n \geq 2$. (Reason: $m \geq 1$ and $n \geq 1$, so $m + n \geq 2$.)
- $m.n$ is a natural number.
- $n + n^2$ and $m + m^2$ are even.
- Either $m > n$ or $m = n$ or $m < n$. □

2.1.5 Universal statements

A universal statement is a statement that asserts that something is true for all the things of a certain kind.

Example 6. Here are some examples of universal statements:

1. Every Rutgers student is required to take[1] Math 300.

[1] I am not saying that this is true. I am only saying that this is a universal statement

2. All Rutgers professors are very nice people and very smart.
3. Every U.S. Senator is either a Democrat or a Republican[2]
4. Every natural number is an integer.
5. Every real number has a square root[3].
6. Every real number has a cube root[4].
7. If n is any natural number then n is even or odd. □

Universal statements can always be rewritten using the word "arbitrary". For example, here are the six universal statements in the list above, rewritten in terms of arbitrary things.

1. If s is an arbitrary Rutgers student then s is required to take Math 300.
2. If p is an arbitrary Rutgers professor, then p is a very nice person and very smart.
3. If s is an arbitrary U.S. Senator then s is either a Democrat or a Republican.
4. If n is an arbitrary natural number then n is an integer.
5. If r is an arbitrary real number then r has a square root.
6. If r is an arbitrary real number then r has a cube root.
7. If n is an arbitrary natural number then n is even or odd.

[2] This is definitely false. At this moment, there are two independent U.S. Senators.

[3] False!

[4] True!

2.1.6 How to prove universal statements

In order to prove a universal statement, what we do is ***prove that the statement is true for an arbitrary thing of the given kind. We give a name—say*** x***, or*** y***, or*** z***, or*** a***, or*** b***, or*** m***, or*** n***, or "Jimmy"—to that arbitrary thing, and prove the statement for that thing.*** The reason that this works is that, if we prove that the statement is true for an arbitrary thing, then this means that it has to be true for ***all the things***.

Example 7. If we want to prove that "if n is any natural number then $n(n+1)$ is even", we begin by writing

- Let n be an arbitrary natural number.

and then we work with that arbitrary thing that we have called n, and prove that $n(n+1)$is even. □

2.2 The natural numbers and the integers

The natural numbers, also called whole numbers, are the "counting numbers", that is, the numbers you use to count. In other words, the natural numbers are 1, 2, 3, 4, and so on.

Remark 1. ***For us, zero is not a natural number.*** Some authors define the natural numbers by starting to count at zero rather than one, so for those authors zero is a natural number.

When you read a mathematics article or book, you should always make sure that you know whether the author is using natural numbers starting at 1 or starting at 0. □

The integers are the natural numbers together with

- The number zero ("0″).
- The negatives of the natural numbers, that is, -1, -2, -3, -4, and so on.

2.2.1 The sets $\mathbb{N}$ and $\mathbb{Z}$.

We are going to be talking about ***sets*** later, but at this point all you need to know is that

1. Sets have ***members***.
2. To say that a thing a is a member of a set S, we can also say "a belongs to S".
3. If S is a set and a is any thing, 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.
4. The expression "$a \in S$" is read as "a belongs to S", or "a is a member of S", or "a is in S". The expression "$a \notin S$" is read as "a does not belong to S", or "a is not a member of S", "or a is not in S.".

WARNING: *Never* read "$a \in S$" as "a is contained in S". The word "contained" has a different meaning.

$\mathbb{N}$ and $\mathbb{Z}$

- The set whose members are all the natural numbers is called $\mathbb{N}$.
- The set whose members are all the integers is called $\mathbb{Z}$.

So, if you want to say that a certain thing a is a natural number, you can just write
$$a \in \mathbb{N}\,,$$
instead of writing the longer sentence "a is a natural number".

Similarly, if you want to say that a certain thing a is an integer, you can just write
$$a \in \mathbb{Z}\,,$$
instead of writing the longer sentence "a is an integer".

EXAMPLES: The following statements are true:

$$\begin{array}{rrrr}
3 \in \mathbb{N} & 3 \in \mathbb{Z} & 3.5 \notin \mathbb{N} & 3.5 \notin \mathbb{Z} \\
0 \notin \mathbb{N} & 0 \in \mathbb{Z} & 27 \in \mathbb{N} & 27 \in \mathbb{Z} \\
\frac{27}{3} \in \mathbb{N} & \frac{27}{3} \in \mathbb{Z} & \pi \notin \mathbb{N} & \pi \notin \mathbb{Z} \\
-1 \notin \mathbb{N} & -1 \in \mathbb{N}\mathbb{Z} & (-3)+5 \in \mathbb{N} & (-3)+5 \in \mathbb{Z} \\
3+(-5) \notin \mathbb{N} & 3+(-5) \in \mathbb{Z} & 3+(-3) \in \mathbb{Z} & 3+(-3) \notin \mathbb{N}\,.
\end{array}$$

Reading sentences with “$\in \mathbb{N}$” and “$\in \mathbb{Z}$”

The sentence

$$3 \in \mathbb{N}$$

can be read as “3 belongs to the set of natural numbers”, or “3 is a member of the set of natural numbers”. But it is much simpler, and nicer, to say “3 is a natural number”. So you should always read it this way.

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.)

2.2.2 A first list of basic facts about the natural numbers and the integers

We are going to start by giving a first list of “Basic Facts” about the natural numbers and the integers. These are the facts that we will take as known in order to start deriving other facts about $\mathbb{N}$ and $\mathbb{Z}$.

In addition, as we develop the theory, we will introduce new concepts, such as the numbers 2, 3, 4, the notions of "factor", divisibility, "prime number", and so on. This will be done by giving ***definitions***, that is, explanations of what the new concept means. (For example, we will define 2 to be $1 + 1$, and once we have defined what "2" standsfor we will be able to talk about it.)

The main rule of the game here is that

> ***at each point in our development of the theory, the only mathematical facts that we are allowed to use all the facts known to be true up to that point, that is***
>
> - ***the basic facts,***
> - ***the definitions given up to that point,***
> - ***the theorems proved before,***
>
> ***and we are not allowed to use anything other mathematical fact until we have proved it.***

So, for the first theorem we will prove, we will only be allowed to use the basic facts, plus whatever definitions will have been given up to that point[5]. and nothing else.

Then, for the second theorem, we are will be allowed to use the basic facts, the definitions of 1, 2 and 3, and the first theorem.

Furthermore: when you are writing a proof of a theorem, in order to write a new step we can use what we know at that point, that is:

- the basic facts,
- the definitions given up to that point,
- the theorems proved before,

[5] After stating the basic facts, the first thing we are going to do is give three definitions, by defining 2 to be $1 + 1$, 3 to be $2 + 1$, and 4 to be $3 + 1$, Then we will prove our first theorem, that $2 + 2 = 4$, and in the proof we will be allowed to use the basic facts, the definitions of 1, 2 and 3, and nothing else.

- the results of the previous steps of the proof.

Question 1. *What is wrong with the following proof of the statement "2+2 = 4"?*
Proof.

> $2 \times 2 = 4.$
>
> *But* $2 = 1 + 1.$
>
> *So* $2 \times (1 + 1) = 4.$
>
> *And* $2 \times (1 + 1) = 2 \times 1 + 2 \times 1 = 2 + 2.$
>
> *So* $2 + 2 = 4$*, and we have proved that* $2 + 2 = 4$*, as desired.*

Answer. What is wrong with this alleged proof is that it is a ***circular proof***[6]*. because the proof that* $2 \times 2 = 4$ *comes* ***after*** *the proof that* $2 + 2 = 4$*, and uses the fact that* $2 + 2 = 4$*. So when you are proving that* $2 + 2 = 4$*' we are* ***not*** *allowed to use the fact that* $2 \times 2 = 4$ □.

2.2.3 Circularity must be avoided at all costs

If you prove A using B, but you prove B using A, then you have given a ***circular proof***. ***Circular proofs are invalid***[7], because such a proof proves nothing, because:

- If you prove A using B first, and then you prove B using A, then the first proof is wrong, because when you proved A using B you had not yet proved B.
- If you prove B using A first, and then you prove A using B, then the first proof is wrong, because when you proved B using A you had not yet proved A.

[6] See Subsection 2.2.3 for an explanation of what 'circular" means.

[7] You probably know what it means for an argument to be "invalid". If you don't, then wait and I will tell you later.

2.2.4 An example of circularity from Calculus

In Calculus[8] courses, when students are asked to prove that $\lim_{x\to 0}\frac{\sin x}{x}=1$, they often do it using L'Hôpital's Rule.

This is circular, because in order to apply L'Hôpital's Rule you need to use the fact that the derivative of $\sin x$ is $\cos x$, and if you look at the proof of this fact in any reasonably serious Calculus book, you will see that this proof uses the fact that $\lim_{x\to 0}\frac{\sin x}{x}=1$.

So this is a circular argument.

In order to avoid the circularity, you have to do one of two things:

either

a. Prove that

$$\lim_{x\to 0}\frac{\sin x}{x}=1 \tag{2.1}$$

without using L'Hôpital's Rule, and then use (2.1) to prove that

$$\frac{d}{dx}\Big(\sin x\Big)=\cos x\,, \tag{2.2}$$

or

b. Prove (2.2) without using (2.1), and then use (2.2) to prove (2.1), for example using L'Hôpital's Rule.

RECOMMENDED EXERCISE. Figure out (or read in a good book) how to prove (2.1) and (2.2) correctly. □

2.2.5 Dealing with equality

Throughout these notes, the symbols "$=$" and "$\neq$" will be used.

The symbol "$=$" is read as "is equal to", and "$\neq$" is read as "is not equal to".

The symbol "$\neq$" is read as "is not equal to".

The meaning of "$=$" in mathematics is quite simple: if a and b are any two things, then "$a=b$" (read as "a is equal to b", or "a equals b") means that a and b are the same thing.

[8] I do not mean our Freshman calculus course. I mean, a Calculus course where you really prove the theorems.

Example 8.

- The sentence "$3 = 2 + 1$" is read as "three is equal to two plus one".
- The sentence "$3 = 2 + 2$" is read as "three is equal to two plus two".
- The sentence "$3 \neq 2 + 1$" is read as "three is not equal to two plus one".
- The sentence "$3 \neq 2 + 2$" is read as "three is not equal to two plus two".
- The sentences "$3 = 2 + 1$" and "$3 \neq 2 + 2$" are true."$3 = 2 + 1$" is read as "three is equal to two plus one".
- The sentences "$3 = 2 + 2$" and "$3 \neq 2 + 1$" are false. □

There are two basic facts you need to know about equality.

THE TWO BASIC FACTS ABOUT EQUALITY

First, there is the ***substitution rule***, which tells you that in a proof you can always "substitute equals for equals":

RULE SEE (substitution of equals for equals): If in a step of a proof you have an equality $s = t$ or $t = s$, and in another step you have a sentence P, then you can write as a step any statement obtained by substituting t for s in one or several of the occurrences of s in P.
The second thing you need to know is the following axiom:

EQUALITY AXIOM (*The "everything is equal to itself" axiom*):

$$x = x \qquad \text{if } x \text{ is any thing}\,.$$

NOTE: A "thing" can be a concrete object like a table or a chair or an atom or New York City or Mount Everest, or a living thing like a cow or a spider or a person.

Example 9. In the sentence "$2 + 2 = 4$", the symbol "2" occurs twice. Suppose you have "$2 + 2 = 4$" as one of the steps in a proof. And suppose that in another step you have "$1+1=2$". Then you can substitute "$1+1$" for "2" in the first occurrence of "2" in the sentence "$2+2=4$", thus getting "$(1+1)+2=4$". Or you can substitute "$1+1$" for "2" in the second occurrence of "2" in "$2+2=4$", thus getting "$2+(1+1)=4$". Or you can substitute "$1+1$" for "2" in both occurrences of "2" in "$2+2=4$", thus getting "$(1+1)+(1+1)=4$". Or you can substitute "$1+1$" for "2" in none of occurrences, in which case you get back "$2+2=4$". □

Example 10. The following are true thanks to the equality axiom:

1. $3=3$,
2. $(345+1,031)\times 27=(345+1,031)\times 27$,
3. Jupiter=Jupiter[9]
4. $\pi=\pi$.
5. My uncle Billy=My uncle Billy. □

2.2.6 Equality is reflexive, symmetric, and transitive

Most textbooks will tell you that equality has the following three properties:

I. Equality is a ***reflexive*** relation. That is:

$$\text{for every } x\,,\ \ x=x\,. \tag{2.3}$$

II. Equality is a ***symmetric*** relation. That is:

$$\text{for every } x\,,\,y\,,\ \text{ if } x=y \text{ then } y=x\,. \tag{2.4}$$

III. Equality is a ***transitive*** relation. That is:

$$\text{for every } x\,,\,y\,,z\,,\ \text{ if } x=y \text{ and } y=z \text{ then } x=z \tag{2.5}$$

[9] But you have to be ***very*** careful here! There are at least three things named "Jupiter": a planet, a Roman god, and a Mozart symphony. When you write "Jupiter=Jupiter", you have to make sure that the two "Jupiter" in the equation have the same meaning. It would be false if you said that the planet Jupiter si the same as the Roman god Jupiter!

And, in addition, they will also tell you that the following important property holds:

IV. ***If two things are equal to a third thing then they are equal to each other.*** That is,

$$\text{for every } x\,,\,y\,,z\,,\ \text{ if } x=z \text{ and } y=z \text{ then } x=y\,. \tag{2.6}$$

We could have put these properties as axioms, but we are not doing that because all these facts can easily be proved from our two basic facts about equality.

Problem 1. ***Prove*** *that Facts I, II, III, and IV above follow from our two basic facts about equality.*

Actually, Fact I is exactly our Equality Axiom, so you don't need to prove it. And I am doing to do the proof of Fact II for you. So ***what you have to do is prove III and IV****.*

Proof of II.

Suppose that $x=y$.

We want to prove that $y=x$.

By the Equality Axiom, $x=x$.

Since we have "$x=y$", Rule SEE tells us that, in the sentence "$x=x$", we can substitute "y" for any of the two occurrences of x in "$x=$". So we choose to substitute "y" for the first of the two xs that occur in "$x=x$".

This yields $\boxed{y=x}$, which is what we wanted to prove. **Q.E.D.**

2.3 The basic facts about $\mathbb{N}$ and $\mathbb{Z}$

BASIC FACTS ABOUT THE INTEGERS I

BFZ1: 0 (“zero”) and 1 (“one”) are integers, and $0 \neq 1$.
BFZ2: Integers can be ***added*** and ***multiplied***. If $m \in \mathbb{Z}$ and $n \in \mathbb{Z}$ then then there are integers $m+n$ (we read this as “m plus n”), called the sum of m and n. and $m.n$ (we read this as “m times n”), called the product of m and n.
BFZ3: The operations of addition and multiplication satisfy

1. the ***commutative laws***:

$$m+n=n+m \qquad \text{whenever } m \in \mathbb{Z}\,,\ n \in \mathbb{Z}\,, \tag{2.7}$$

$$m.n=n.m \qquad \text{whenever } m \in \mathbb{Z}\,,\ n \in \mathbb{Z}\,, \tag{2.8}$$

2. the ***associative laws***:

$$m+(n+p)=(m+n)+p \qquad \text{whenever } m \in \mathbb{Z}\,,\ n \in \mathbb{Z}\,,\ p \in \mathbb{Z}\,, \tag{2.9}$$

$$m.(n.p)=(m.n).p \qquad \text{whenever } m \in \mathbb{Z}\,,\ n \in \mathbb{Z}\,,\ p \in \mathbb{Z}\,, \tag{2.10}$$

3. the ***distributive law of multiplication with respect to addition***:

$$m.(n+p)=m.n+m.p \qquad \text{whenever } m \in \mathbb{Z}\,,\ n \in \mathbb{Z}\,,\ p \in \mathbb{Z}\,, \tag{2.11}$$

BFZ4: the ***properties characterizing*** 0 ***and*** 1:

$$n+0=n \qquad \text{whenever } n \in \mathbb{Z} \tag{2.12}$$

(that is, 0 is an ***additive identity***,

$$n.1=n \qquad \text{whenever } n \in \mathbb{Z} \tag{2.13}$$

(that is, 0 is a ***multiplicative identity***,
BFZ5: if $n \in \mathbb{Z}$ then there is an integer $-n$ such that

$$n+(-n)=0\,. \tag{2.14}$$

(The integer $-n$ is called the ***additive inverse*** of n).

HOW TO READ THE "-" (MINUS) SIGN

I strongly recommend that you read "$-n$" as "minus n", rather that as "negative n".

Here is why: when you say "negative n", you are giving the strong impression that $-n$ is a negative number.

However, $-n$ ***need not be negative.*** For example, if $n = -5$, then $-n$ is 5, which is positive.

When you say "minus n", the danger that you will mistakenly think that $-n$ is negative is much smaller.

THE THREE NOTATIONS FOR MULTIPLICATION: $m.n$, mn, $m \times n$

Usually, we write "$m.n$" to denote the product of m and n (and we read this as "m times n".

But sometimes we write "'mn" rather than "$m.n$". (This is called juxtaposition: we write the name of one number and then the name of the other number, with nothing in between.)

The juxtaposition notation "mn" is more convenient when the numbers you are multiplying are being referred to by letter names, such as m, or n, or a, or b, or x, or y.

But when we are using numerals[a].), it would be disastrous if we used juxtaposition. For example, suppose wanted to talk about "two times three", and we wrote "23". Everybody would read this as "twenty-three"! So we do not want that. And it would not be any better if we wrote "2.3"? No! If we did thos, everybody would read "2.3" as "two point three", i.e., as the number whici is equal to $\frac{23}{10}$, or $2 + \frac{3}{10}$.

So, in order to avoid having these problems, we allow an alternative notation for the product of m times n, namely, "$m \times n$'.

And we use this notation for multiplication of numerals. So, for example, "two times three" is written as "2×3".

[a] A numeral is an expression that is the name of a natural number. For example, "1", "2", "35", "307", "$2,530,983$" are numerals. We do not write "2.3" if we want to say "two times three", because the expression "2.3" usually stands for something else, namely, the number "two point three", that is, $\frac{21}{10}$. So, if we want to say "two times three" we write "2×3".

2.4 A few very simple proofs

Now that we know a few things about the integers, we are ready to actually ***prove*** some theorems about them.

And, as I promised before, ***these are going to be very stupid proofs***.

First of all, let us observe that so far the only integer that we know anything about is 1. To make things a little bit more interesting, we need to have some more numbers. For example, we would like to talk about the numbers 2, 3, etc. So we give a few definitions:

Definition 1. $2 = 1 + 1.$ □

Definition 2. $3 = 2 + 1.$ □

Definition 3. $4 = 3 + 1.$ □

And, now that we know what 1, 2, 3, and 4 are, we are ready to prove our first theorem[10]:

Theorem 1. $2 + 2 = 4.$

Proof. First, we observe that

$$2 + 2 = 2 + 2\,, \tag{2.15}$$

by the Equality Axiom.

On the other hand,

$$2 = 1 + 1$$

by Definition 1.

Hence Rule SEE enables us to conclude that

$$2 + 2 = 2 + (1 + 1)\,. \tag{2.16}$$

On the other hand,

$$2 + (1 + 1) = (2 + 1) + 1\,, \tag{2.17}$$

by the associative law of addition (Basic Fact BFN2.2, i.e., Equation (2.9)).

Hence

$$2 + 2 = (2 + 1) + 1\,. \tag{2.18}$$

[10] I told you this was going to be very stupid!

But

$$2+1=3\,, \tag{2.19}$$

by Definition 2.

Hence

$$2+2=3+1\,. \tag{2.20}$$

Finally, Definition 2 tells us that

$$3+1=4\,. \tag{2.21}$$

Hence

$$\boxed{2{+}2{=}4}\,. \tag{2.22}$$

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.

Theorem 2. $2 \times 2 = 4$.

Proof. The Equality Axiom implies that

$$2 \times 2 = 2 \times 2\,. \tag{2.23}$$

And Definition (1) tells us that $2 = 1 + 1$. So, using Rule SEE, we get

$$2 \times 2 = 2 \times (1+1)\,. \tag{2.24}$$

By the distributive law (Basic Fact BFN3.3, i.e., Equation (2.11))

$$2 \times (1+1) = 2 \times 1 + 2 \times 1\,. \tag{2.25}$$

Hence

$$2 \times 2 = 2 \times 1 + 2 \times 1\,. \tag{2.26}$$

By Basic Fact BFN4A, $2 \times 1 = 2$. Hence

$$2 \times 2 = 2 + 2\,. \tag{2.27}$$

Finally, Theorem 1 tells us that $2+2=4$. it follows that

$$\boxed{2\times 2=4}\,. \tag{2.28}$$

Q.E.D.

So far, we have introduced and given names to four integers, namely, 1, 2, 3, and 4. We can then go on and introduce a few more.

Definition 4. $5=4+1$. □

Definition 5. $6=5+1$. □

Definition 6. $7=6+1$. □

Definition 7. $8=7+1$. □

Definition 8. $9=8+1$. □

And we can prove things about these numbers, such as, for example:

Theorem 3. $3+3=6$.

Proof. YOU DO THIS ONE.

Theorem 4. $3\times 2=6$.

Proof. YOU DO THIS ONE.

Theorem 5. $4+3=7$.

Proof. YOU DO THIS ONE.

Problem 2. *Prove Theorems 3, 4, and 5. In each proof, you are allowed to use the basic facts known so far, the definitions given so far, and the theorems proved so far. So, for example: in your proof of Theorem 3 you are allowed to use the basic facts, definitions 1, 2, 3, 4, 5, 6, 7, 8, and Theorems 1 and 2; in your proof of Theorem 4 you are allowed to use the basic facts, definitions 1, 2, 3, 4, 5, 6, 7, 7, and Theorems 1, 2, and 3; and in your proof of Theorem 5 you are allowed to use the basic facts, definitions 1, 2, 3, 4, 5, 6, 7, 7, Theorems 1, 2, 3; and 4.*

Theorems 1, 2, 3, and 4. □

2.4.1 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[11].

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 9. Let a, b be integers.

1. We say that b is a <u>factor</u> of 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.
3. We say that b <u>divides</u> a if b is a factor of 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 2. 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 s divisible by m,
- $m|n$. □

[11] 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.

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 statementsd.

Let us prove some theorems about divisibilty.

Theorem 6. *If a, b, c are integers such that a divides b and a divides c, then a divides $b+c$.*

Proof. Since $a|b$, Definition 9 tells us that we may pick j such that $j \in \mathbb{Z}$ and

$$b = aj\,. \tag{2.29}$$

Since $a|c$, Definition 9 tells us that we may pick k such that $k \in \mathbb{Z}$ and

$$c = ak\,. \tag{2.30}$$

Then

$$b + c = aj + ak\,. \tag{2.31}$$

The distributive law (Basic Fact BFZ.3) tells us that

$$aj + ak = a(j+k)\,. \tag{2.32}$$

Therefore

$$b + c = a(j+k)\,. \tag{2.33}$$

Since $j \in \mathbb{Z}$ and $k \in \mathbb{Z}$, Basic Fact BFZ1 tells us that $j + k$ is an integer.

Hence Equation (2.33) implies that the exists an integer ℓ such that $b+c = a\ell$. (It suffices to take $\ell = j + k$.)

So $\boxed{a \text{ divides } b + c}$. **Q.E.D.**

Theorem 7. *If a, b, c are integers such that a divides b and b divides c, then a divides c.*

Proof. **YOU DO THIS ONE.**

Problem 3. *Prove Theorem 7*

Corollary 1. *If a, b, c are integers such that a divides b, then a divides bc.*

Proof.

It follows from the definition of "divides" (Definition 9) that b divides bc.

So a divides b and b divides bc.

Therefore Theorem 7 tells us that $\boxed{a \text{ divides } bc}$.

Q.E.D.

2.4.2 *Getting serious: Some more interesting theorems about divisibility

*In this section we "run wild": we prove lots of things using everything we know, including facts that we have not proved yet. So the proofs we will give now are, strictly speaking, invalid. But they wiil become valid once we have proved all the results that we are going to use here**provided there is no circularity**[12]**.***

So far we have only proved some very simple things, and the proofs were easy. Now I want to discuss some more serious and nontrivial questions.

Specifically, I want to investigate the following:

Question 2.*: Is the following statement true?*

[12] That is: If we prove all the things used in this section without using any of the results proved in this section, then we can think of the proofs of this section as coming ***after*** the proofs of the other results, and then they become valid.

(*) *If a and b are integers, then every integer n that is divisible by a and by b must be divisible by the product ab.*

Another way to state this question is

Question 3.*: Is the following statement about a and b true for all integers a, b??*

(**) *Every integer n that is divisible by a and by b must be divisible by the product ab.*

Clearly, Question 2 says "*Is the answer to Question 3 'yes' for every choice of the integers a, b?*"

And the answer to Question 3 cannot be "yes" for all choices if a and b, as shown by the following examples.

Example 11.

- 12 is divisible by 3 and by 6, but is not divisible by the product 3×6, because $3 \times 6 = 18$, and it's not true that $19|12$.
- $6|30$ and $15|30$, but it's not true that $6 \times 15|30$, because $6 \times 15 = 90$, and 90 certainly does not divide 30.
- $6|24$ and $8|24$, but it's not true that $6 \times 8|24$, because $6 \times 8 = 48$, and 48 certainly does not divide 24.

So (**) is not true for $a = 3$ and $b = 6$, or for $a = 6$ and $b = 15$. □

Is (**) true for, say, $a = 3$ and $b = 5$? It turns out that the answer is "yes", because we can prove the following theorem.

Theorem 8. *If n is an integer such that $3|n$ and $5|n$, then $15|n$.*

Proof. First, we observe that

$$10 - 9 = 1\,. \tag{2.34}$$

At this point you must be wondering "what does Equation (2.34 have to do with proving what we want to prove?" Just wait and you will see.

Suppose $n \in \mathbb{Z}$, and n is divisible by 3 and by 5.
Since $3|n$, we may pick a j such that $j \in \mathbb{Z}$ and

$$n = 3j\,. \tag{2.35}$$

Since $5|n$, we may pick a k such that $k \in \mathbb{Z}$ and

$$n = 5k\,. \tag{2.36}$$

Since $10 - 9 = 1$, we can write

$$\begin{aligned} n &= (10-9)n \\ &= 10n - 9n \\ &= 10 \times 3j - 9 \times 5k \\ &= 30j - 45k \\ &= 15 \times 2j - 15 \times 3k \\ &= 15 \times (2j - 3k) \\ &= 15m\,, \end{aligned}$$

where $m = 2j - 3k$.
The number m is clearly an integer.
Since $m \in \mathbb{Z}$ and $n = 15m$, it follows that $\boxed{15|n}$. **Q.E.D.**

The trick in the preceding proof was writing 1 as the difference of a multiple of 5 and a multiple of 3. (It does not matter that we used 10 and 9. We could have used, for example, $21 - 20 = 1$, or $25 - 24 = 1$.)

Problem 4. *Write a different proof of Theorem 8 using the equality* $21-20 = 1$ *instead of 2.34.* □

Let us try our hand at a different choice of a and b. For example, let us take $a = 23$ and $b = 51$. We need to find a multiple of 23 and a multiple of 52 that are so close to each other that they differ by 1. And, in order to do that, we will use the following approach:

1. We start by finding multiples of 23 and 51 that are not too far from one another, without insisting that the difference be exactly 1.

2. We then try to modify these multiples and make them closer to one another, and we keep doing that until we end up with two multiples that differ by 1.

One thing we can do is observe that 2×23 is 46, which is somewhat close to 51. So we write

$$51 - 2 \times 23 = 5\,. \tag{2.37}$$

Let us try to improve upon this, and look for an even smaller difference. For example, we can observe that $4 \times 5 = 20$, which is close[13] to 23.

So let us multiply both sides of (2.37) by 4:

$$\begin{aligned} 4 \times 51 - 4 \times 2 \times 23 &= 4 \times 5 \\ &= 20 \\ &= 23 - 3 \end{aligned}$$

and then

$$4 \times 51 - 4 \times 2 \times 23 - 23 = -3$$

so

$$4 \times 51 - (4 \times 2 + 1) \times 23 = -3\,,$$

that is,

$$4 \times 51 - 9 \times 23 = -3\,,$$

and then

$$9 \times 23 - 4 \times 51 = 3\,, \tag{2.38}$$

(Let us check that this works: $9 \times 23 = 207$, and $4 \times 51 = 204$, so (2.38) is true.)

So now we have a multiple of 23 and a multiple of 51 whose difference is 3. This is not 1 yet, but ***we are definitely getting closer***.

Now let us take one more step: 7×3 is 21, which differs from 1 by 1. So this should get us there. So let us multiply both sides of (2.38) by 7. We get

$$7 \times 9 \times 23 - 7 \times 4 \times 51 = 7 \times 3 = 21 = 23 - 2\,.$$

Hence

$$7 \times 9 \times 23 - 7 \times 4 \times 51 - 23 = -2\,,$$

[13] If you ask "what do you mean by 'close'?", my frank answer is "I don't know". But 20 is certainly closer to 23 than 46 was to 51. So we have improved the situation.

so

$$\begin{aligned} -2 &= 7\times 9\times 23 - 7\times 4\times 51 - 23 \\ &= 63\times 23 - 28\times 51 - 23 \\ &= 62\times 23 - 28\times 51\,, \end{aligned}$$

so

$$28\times 51 - 62\times 23 = 2\,. \tag{2.39}$$

(Verification: $28\times 51 = 142$, and $62x23 = 1426$, so it works.)

We are not there yet, but we are certainly much closer than before And one more should take us there. Let us multiply both sides of (2.39) by 11. We get

$$11\times 28\times 51 - 11\times 62\times 23 = 11\times 2 = 22 = 23 - 1\,.$$

So

$$11\times 28\times 51 - 11\times 62\times 23 - 23 = -1$$

and then

$$11\times 28\times 51 - (11\times 62 + 1)\times 23 = -1$$

from which it follows that

$$\begin{aligned} 1 &= (11\times 62 + 1)\times 23 - 11\times 28\times 51 \\ &= 683\times 23 - 308\times 51\,, \end{aligned}$$

that is,

$$683\times 23 - 308\times 51 = 1\,. \tag{2.40}$$

(Verification: $683\times 20 = 15709$ and $308\times 51 = 15708$, so it works.)

Now that we have expressed 1 as the difference of a multiple of 23 and a multiple of 51, we can use 2.40) and then repeat almost word by word the proof of Theorem 8 and prove

Theorem 9. *If n is an integer such that $23|n$ and $51|n$, then $23\times 52|n$, that is. $1173|n$.*

Proof. First, we observe that

$$23a - 51b = 1\,, \tag{2.41}$$

where $a = 683$ and $b = 508$.
Suppose n is an integer such that n is divisible by 23 and by 51.
Since $23|n$, we may pick an integer j such that

$$n = 23j\,. \tag{2.42}$$

Since $52|n$, we may pick an integer k such that

$$n = 51k\,. \tag{2.43}$$

Since $23a - 51b = 1$, we can write

$$\begin{aligned} n &= 1 \times n \\ &= (23a - 51b) \times n \\ &= 23an - 51bn \\ &= 23a \times 51k - 51b \times 23j \\ &= (23 \times 51)(ak - bj) \\ &= 1173m\,, \end{aligned}$$

where $m = ak - bj$.
The number m is clearly an integer. So $\boxed{1173|n}$. **Q.E.D.** The previous examples suggests that for some choices of a and b statement (**) iss true, and for some other choices it is false.

In our examples,

- For $a = 2$ and $b = 5$, (**) is true.
- For $a = 23$ and $b = 51$, (**) is true.
- For $a = 3$ and $b = 6$, (**) is false.
- For $a = 6$ and $b = 15$, (**) is false.
- For $a = 6$ and $b = 8$, (**) is false.

Is there a pattern here? Can we tell, if we are given a and b, whether (**) is true or false?

If you look at our examples, you see that the one thing that the “false” cases have in common is that a and b have a common factor:

- if $a = 3$ and $b = 6$, then both a and b are divisible by 3,
- if $a = 6$ and $b = 15$, then both a and b are divisible by 3,
- if $a = 6$ and $b = 8$, then both a and b are divisible by 2.

Could this be the answer? Could it be that the reason that (**) is true for certain choices of a and b is that a and b have a common factor?

We would like to formulate this as a conjecture. But first we need to have a precise definition of "common factor".

Definition 10. If a, b are integers, then a

1. a common factor of a and b is an integer f such that $f|a$ and $f|b$. □
2. a nontrivial common factor of a and b is a common factor f such that $f \neq 1$ and $f \neq -1$. □

Remark 3. The concept of a "nontrivial" common factor is important because every integer is divisible by 1 and by -1, so what is really interesting is whether our integers a, b have factors other than those two. □

And now here is our conjecture:

CONJECTURE X: If a, b are nonzero[14] integers, then

1. If a and b have a nontrivial common factor, then (**) is not true.
2. If a and b do not have a nontrivial common factor, then (**) is true.

Remark 4. In the statement of Conjecture X, why do we insist that a and b should be nonzero? The reason is that when $a = 0$ or $b = 0$ some special things can happen. To begin with, 0 *is divisible by every integer*. (Reason: if $n \in \mathbb{Z}$ then[15] $n \times 0 = 0$, so $n|0$.) Furthermore, *the only integer that is divisible by* 0 *is* 0. (Reason: if $0|n$ then we may pick an integer k such that $k \times 0 = n$. But $k \times 0 = 0$, so $n = 0$.)

It follows from this that if $a = 0$ (or $b = 0$) then

1. If an integer n is divisible by a and b, then n must be zero.

[14] That is, $a \neq 0$ and $b \neq 0$.

[15] This fact will be proved in the next section

2. Since $n = 0$, n is divisble by 0.

3. But $ab = 0$. So n is divisible by ab.

So statement (**) is always true when $a = 0$ or $b = 0$. And yet it can happen that a and b have a nontrivial common factor. (For example, if $a = 0$ and $b = 2$ then both a and b are divisible by 2, so they have a nontrivial common factor.)

This means that if we had not included in Conjecture X the requirement that a and b be nonzero, the conjecture would be false. This explains why we put in the condition that $a \neq 0$ and $b]neq0$. □

What is a conjecture?

A conjecture is a statement that somebody puts forth claiming that it is probably true but not knowing for sure that it is true.
Here are two famous examples of conjectures that nobody so far has been able to prove or disprove[a]:

Goldbach's conjecture: *Every even natural number other than* 2 *is the sum of two prime numbers.*

The twin primes conjecture: *There exist infinitely many natural numbers p such that p and $p + 2$ are prime.*

[a] To "disprove" a statement means "to prove that it is false".

Problem 5.

I. For each of the following choices of a and b, prove that (**) is true, or prove that it is false. (NOTE: To prove that (**) is false, it suffices to give an example of an n such that $a|n$, $b|n$ but it's not true that $ab|n$. To prove that (**) is true, you need an argument, like the one we gave in our proofs of Theorems 8 and 9.)

1. $a = 35$ *and* $b = 49$.
2. $a = 22$ *and* $b = 41$.
3. $a = 210$ *and* $b = 65$.
4. $a = 68$ *and* $b = 89$. □

II. Verify that the answers you got in Part I are consistent with the conjecture. □

Problem 6. ***Prove*** *statement 1 of Conjecture X. (That is, prove that if the integers a, b have a nontrivial common factor, then (**) is not true.) (HINT: If $a = jf$ and $b = kf$, try $n = jkf$.)* □

After you do Problem 6, you will have proved half of Conjecture X. We will be able to prove Part 2 as well, but we are no ready to do that yet, because we are going to need more sophisticated technical tools that are not available to us at this moment.