MATHEMATICS 300 — SPRING 2015

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S NOTES

LECTURE ON THE FUNDAMENTAL THEOREM OF ARITHMETIC

Contents

1 The fundamental theorem of arithmetic

The fundamental theorem of arithmetic (FTA), also called

- the unique factorization theorem,

or

- the unique prime factorization theorem,

is supposed to say the following, roughly:

(FTA, tentative version) Every natural number greater than or equal to* 2 *has a unique prime factorization.

1.1 Is a prime factorization a set of primes?

The above statement is not completely precise, and some clarification is required.

First of all, what do we mean by "prime factorization"?

The first possible definition that may come to our mind is that a "factorization" of a natural number n is a set S of natural numbers such that the product of all the members of S is n. And a "prime factorization" of a natural number n is a factorization of n whose members are prime numbers.

So, for example, since $6 = 2 \times 3$, and 2 and 3 are prime numbers, we could say that the set $\{2, 3\}$ is a prime factorization of 6.

This, however, is not a good idea. To see why, look for example at the number 12. Clearly, $12 = 2 \times 2 \times 3$. So, what is the "prime factorization" of 12. You may be tempted to say that "it is the set $\{2, 2, 3\}$", right? But *"the set* $\{2, 2, 3\}$*" is none other than the set* $\{2, 3\}$. ***Sets do not have repeated members!*** For a set S, there are objects x that are members of S and objects that are not members, and there is nothing else. (For example, there is no such thing as "being a member of a set twice". If S is a set, then an object x either is a member of S or is not a member.) And two sets that have the same members are the same set. For "the set $\{2, 2, 3\}$", 2 is a member, 3 is a member, and no other object is a member. And for the set $\{2, 3\}$" it is also true that 2 is a member, 3 is a member, and no other object is a member. So the members of the set $\{2, 2, 3\}$ are exactly the same as the members of the set $\{2, 3\}$. Hence the set $\{2, 2, 3\}$ is the same as the set $\{2, 3\}$. And the product of the members of this set is 6, not 12. So it would appear that 12 does not have a prime factorization, because the only possible prime factorization of 12—if we define "prime factorization" as a set— is in fact a prime factorization of 6, not of 12.

This means that we have to change the definition of "prime factorization": instead of being a *set*, a "prime factorization" is going to be a *finite list*.

To make this precise, we need to say a few words about finite lists.

1.2 Finite lists

First, let us introduce some notation: for a natural number n, we are going to use $\mathbb{N}_n$ to denote the set of all natural numbers j such that $j \leq n$. That is

$$\mathbb{N}_n = \{j \in \mathbb{N} : j \leq n\} .$$

A finite list has a *length*, which is a natural number, and, for each natural number j such that $j \in \mathbb{N}_n$, where n is the length of the list, an *entry*.

There are finite lists and infinite lists. In this section, we will only be talking about finite lists, so we am going to use "list" throughout to mean "finite list". Later we will want to consider lists that may be infinite, so we will have to say "finite list" when we want to talk about a finite list.

We will use various symbols, such as capital letters or boldface lower-case letters, for lists. And, if $\mathbf{a}$ is a list, we will write

$$\mathbf{a} = (a_j)_{j=1}^n$$

or

$$\mathbf{a} = (a_j)_{j\in\mathbb{N}_n}$$

to indicate that $\mathbf{a}$ is a list of length n whose j-entry, for each $j \in \mathbb{N}_n$, is a_j.

Example 1. If we want to introduce the list of all U.S. presidents from George Washington to Barack Obama, in chronological order, and call it $\mathbf{p}$, we can say

> Let
>
> $$\mathbf{p} = (p_j)_{j=1}^{44}$$
>
> where, for $j \in \mathbb{N}_{44}$, p_j is the j-th president of the U.S.

And, if we then want to introduce the list of U.S presidents in backward chronological order, and call it $\mathbf{q}$, we can say

> Let $\mathbf{q} = (q_j)_{j=1}^{44}$ where, for $j \in \mathbb{N}_{44}$, $q_j = p_{45-j}$.

(This is what we can do if we have already introduced $\mathbf{p}$, so the reader knows who $\mathbf{p}$ and the p_j are.) □

When the length of a list is a small number, we can just write the entries from left to right, separated by commas, and with a left parenthesis at the beginning and right parenthesis at the end.

Example 2. If we want to introduce the list of the first five prime numbers, and call it $\mathbf{p}$, we can write

> Let $\mathbf{p} = (p_j)_{j=1}^{5}$ where, for $j \in \mathbb{N}_5$, p_j is the j-th prime number.

Or we can write

> Let $\mathbf{p} = (p_j)_{j=1}^{5}$ where $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, and $p_5 = 11$.

Or we can just write

> Let $\mathbf{p} = (2, 3, , 5, 7, 11)$.

But, if we want to introduce the list of the first 200 primes, and call it $\mathbf{p}$, then of course the only reasonable choice is to write

> Let $\mathbf{p} = (p_j)_{j=1}^{200}$ where, for $j \in \mathbb{N}_{200}$, p_j is the j-th prime number.

Remark 1. Often, one writes

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

or

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

instead of $\mathbf{p} = (p_j)_{j=1}^{n}$. I strongly prefer the $(p_j)_{j=1}^{n}$ notation, but I will accept the other one. □

Remark 2. Pay attention to the following:

1. Sets have ***members***, not entries.
2. Lists have ***entries***, not members.

3. In the set notation, we use ***braces***, as in "the set $\{1,2,3,4\}''$, or "the set $\{x \in \mathbb{R} : x > 0\}$".

4. In the list notation, we use ***parentheses***[1], as in "the list $(2,2,3,4)$", or "the list $\mathbf{p} = (p_j)_{j=1}^n$". □

1.3 Equality of lists

Two lists $\mathbf{p} = (p_j)_{j=1}^n$, $\mathbf{q} = (q_j)_{j=1}^m$, are ***equal*** if

1. $n = m$,

and

2. $p_j = q_j$ for every $j \in \mathbb{N}_n$. (That is, $(\forall j \in \mathbb{N}_n) p_j = q_j$.)

Example 3. The lists $(2,2,3)$ and $(3,2,2)$ are *not* equal because, for example, the first entry of the first list is not equal to the fist entry of the second list.

But, of course, the sets $\{2,2,3\}$ and $\{3,2,2\}$ are equal. □

Problem 1.What would be wrong if, in Example 3, I had written

> *The lists $(2,2,3)$ and $(3,2,2)$ are not equal because, for example, $p_1 \neq q_1$.*

Answer: What is wrong is that we haven't the faintest idea of who p_1 and q_1 are, because we haven't been told. □

1.4 Prime factorizations

Definition 1. A prime factorization of a natural number n is a finite list $\mathbf{p} = (p_j)_{j=1}^m$ such that

(1) p_j is a prime number for every $j \in \mathbb{N}_m$. (That is, all the entries in the list are prime numbers.)

[1] Not all books usse the same notation, so if you are reading a mathematics book you have to make sure to check which notations it is using. For example, some books use braces for lists, so they would write "the list $\{p_j\}_{j=1}^n$". I strongly prefer the parenthesis notation, and in this course this is the official notation.

(2) $\prod_{j=1}^{m} p_j = n$. □

Example 4. The list $(2, 2, 3)$ is a prime factorization of the number 12, because each of the three entries (2, 2, and 3) is a prime number, and the product $2 \times 2 \times 3$ is equal to 12. □

Example 5. The list $(3, 2, 2)$ is also a prime factorization of 12, and is different from the prime factorization $(2, 2, 3)$ of Example 4. □

So the number 12 has at least two different prime factorizations. And yet we want the prime factorization of a natural number to be unique!

To solve this problem we have to introduce the concept of an "ordered prime factorization".

Definition 2. A list $\mathbf{p} = (p_j)_{j=1}^{m}$ whose entries are real numbers is <u>ordered</u> if

(ORD) $p_j \leq p_{j+1}$ for every $j \in \mathbb{N}_m$ such that $j < m$. □

Definition 3. An <u>ordered prime factorization</u> of a natural number n is a prime factorization $\mathbf{p} = (p_j)_{j=1}^{m}$ of n which is an ordered list. □

Example 6. The list $(2, 2, 3)$ is an ordered prime factorization of 12, but the list $(3, 2, 2)$ is not. □

1.5 A correct statement of the FTA

From now on, if $\mathbf{p} = (p_j)_{j=1}^{k}$ *is a list of real numbers, we write "*$\prod \mathbf{p}$*" for "*$\prod_{j=1}^{k} p_j$*". So, for example, if* $\mathbf{p} = (p_j)_{j=1}^{5}$*, where* p_j *is the* j*-th prime for each* $j \in \mathbb{N}_5$*, then* $\prod \mathbf{p} = 2,310$.

And here is a correct, almost perfect[2] statement of the FTA:

Theorem 1. *(An almost perfect version of the fundamental theorem of arithmetic.) Every natural number* n *such that* $n > 1$ *has a unique ordered prime factorization.*

[2] I say "almost perfect" because the statement can be made even nicer and more elegant, thus obtaining a truly "perfect" statement. We will do this later.

1.6 The proof

We have to prove existence and uniqueness of the ordered prime factorization.

The *existence* of a prime factorization of any natural number n such that $n > 1$ has been proved before, in Theorem 2 on page 4 of the lecture notes on well-ordering.

But here we need to prove the existence of an *ordered* prime factorization. Intuitively, this is obvious. Let $n \in \mathbb{N}$ be arbitrary. Asssume that $n > 1$. Take a prime factorization $\mathbf{p} = (p_j)_{j=1}^m$ of n. (Such a factorization exists by Theorem 2 on page 4 of the lecture notes on well-ordering. And then Rule $\exists_{use}$ enables us to pick one and call it $\mathbf{p}$.) Then reorder $\mathbf{p}$, by forming a new list $\mathbf{q} = (q_j)^m$ that has the same entries as $\mathbf{p}$, but in increasing order. This gives us an ordered prime factorization of n, proving that such a factorization exists. ***If you are satisfied with this proof of existence, you may skip the following lemma, and move on directly to the beginning of the proof of uniqueness.***

How can we do prove the existence of the ordered list $\mathbf{q}$ in a completely precise, rigorous way? Here is one way. We can prove, by induction on k, the following lemma:

Lemma 1. *If $k \in \mathbb{N}$, and $\mathbf{p} = (p_j)_{j=1}^k$ is a list of primes, then there exists an ordered list $\mathbf{q}$ of primes such that $\prod \mathbf{q} = \prod \mathbf{p}$.*

Proof of the lemma. **I AM WORKING ON THIS PROOF. IT WILL BE INCLUDED IN THE FINAL VERSION OF THESE NOTES.**

Using Lemma 1, the existence part of the FTA follows easily: let n be an arbitrary natural number such that $n \geq 2$. By Theorem 2 on page 4 of the lecture notes on well-ordering, there exists a list of primes whose product is n, so we may pick one such list and call it $\mathbf{p}$. Then, by Lemma 1, there exists an ordered list of primes whose product is equal to $\prod \mathbf{p}$. So we may pick such a list and call it $\mathbf{q}$. But then $\mathbf{q}$ is an ordered prime factorization of n. So an ordered prime factorization of n exists. This concludes the proof of existence.

The uniqueness proof. This is the most delicate part. We have to prove that if we have two ordered prime factorizations $\mathbf{p}$, $\mathbf{q}$, of a natural number n, it follows that $\mathbf{p} = \mathbf{q}$. In other words: we have to assume that

() We have two lists

$$\mathbf{p} = (p_j)_{j=1}^{k}\,, \qquad \mathbf{q} = (q_j)_{j=1}^{\ell}\,,$$

such that

(1) all the p_j and all the q_j are prime numbers,

(2) $\mathbf{p}$ and $\mathbf{q}$ are ordered lists (that is, $p_j \le p_{j+1}$ whenever $j \in \mathbb{N}$, $j < k$, and $q_j \le q_{j+1}$ whenever $j \in \mathbb{N}$, $j < \ell$),

(3) $\prod_{j=1}^{k} p_j = \prod_{j=1}^{\ell} q_j$,

and we want to conclude that $\mathbf{p} = \mathbf{q}$.

To prove that $\mathbf{p} = \mathbf{q}$, we have to show that

$$(\forall k \in \mathbb{N})(\forall \ell \in \mathbb{N})(\forall \mathbf{p})(\forall \mathbf{q})A(k, \ell, \mathbf{p}, \mathbf{q})\,, \tag{1.1}$$

where

$A(k, \ell, \mathbf{p}, \mathbf{q})$ is the statement:

If $\mathbf{p}$ and $\mathbf{q}$ are ordered lists of primes of lengths k, ℓ, and $\prod \mathbf{p} = \prod \mathbf{q}$, then $\mathbf{p} = \mathbf{q}$.

We would like to do a proof by induction. But one can do induction with respect to one natural number variable, not with respect to two natural number variables, or with respect to variables of other kinds such as lists.

So we have to express what we want to prove as a satatement of the form $(\forall k \in \mathbb{N})P(k)$. But this is easy to do:

Statetemnt (1.1) says

$$(\forall k \in)P(k)\,, \tag{1.2}$$

where

$P(k)$ is the statement:

$$(\forall \ell \in \mathbb{N})(\forall \mathbf{p})(\forall \mathbf{q})A(k, \ell, \mathbf{p}, \mathbf{q})\,.$$

To prove (1.1) we will prove (1.2). And, since (1.2) is of the form that lends itself to a proof by induction, we will prove (1.2) by induction.

The base case. We have to prove $P(1)$. But P(1) says that "if $\mathbf{p}$ is an ordered list of just one prime, $\mathbf{q}$ is an ordered list of primes, and $\prod \mathbf{p} = \prod \mathbf{q}$, then $\mathbf{p} = \mathbf{q}$".

Equivalently, P(1) says that "if p is a prime number, $\mathbf{q}$ is an ordered list of primes, and $p = \prod \mathbf{q}$, then $\mathbf{q}$ has length one, so it consists of a single prime q, and $q = p$".

But this is obviously true, because, if $\mathbf{q} = (q_j)_{j=1}^{\ell}$, and $p = \prod_{j=1}^{\ell} q_j$, then ℓ must be equal to 1, because p is prime, and a prime number cannot be written as a product of two or more primes.

So $P(1)$ is true, and the proof of the base case is complete.

The inductive step. We have to prove that

$$(\forall k \in \mathbb{N})(P(k) \Longrightarrow P(k+1))\,. \tag{1.3}$$

Let $k \in \mathbb{N}$ be arbitrary.

Assume $P(k)$ is true.

We want to prove $P(k)+1$.

That is, we want to prove that

(*) If

(1) $\mathbf{p}$ is an ordered list of primes of length $k+1$,

(2) $\mathbf{q}$ is an ordered list of primes of length ℓ,

(3) $\prod \mathbf{p} = \prod \mathbf{q}$.

then $\mathbf{p} = \mathbf{q}$.

To prove (*), assume that (1), (2), (3) hold.

We want to prove that $\mathbf{p} = \mathbf{q}$.

Let $\mathbf{p} = (p_j)_{j=1}^{k+1}$, $\mathbf{q} = (q_j)_{j=1}^{\ell}$.

Then

$$\prod \mathbf{p} = \prod_{j=1}^{k+1} p_j = \Big(\prod_{j=1}^{k} p_j\Big) p_{k+1}\,.$$

It follows that

$$p_{k+1} | \prod \mathbf{p}\,.$$

Since $\prod \mathbf{p} = \prod \mathbf{q}$, we can conclude that

$$p_{k+1} | \prod \mathbf{q}\,.$$

So

$$p_{k+1}|\prod_{j=1}^{\ell} q_j\,.$$

By the generalized Euclid lemma, p_{k+1} must divide one of the numbers q_j. So we may pick an index $j_* \in \mathbb{N}_\ell$ such that

$$p_{k+1}|q_{j_*}\,.$$

Then, since p_{k+1} and q_{j_*} are natural numbers, it follows that

$$p_{k+1} \leq q_{j_*}\,.$$

Since the list $\mathbf{q}$ is ordered, $q_{j_*} \leq q_\ell$. Hence

$$p_{k+1} \leq q_\ell\,. \tag{1.4}$$

So we have proved that "the last of the p's is less than or equal to the last of the q's". Clearly, we can use exactly the same argument to prove that "the last of the q's is less than or equal to the last of the p's", that is, that

$$q_\ell \leq p_{k+1}\,. \tag{1.5}$$

It then follows from (1.4) and (1.5) that

$$p_{k+1} = q_\ell\,. \tag{1.6}$$

Then

$$\prod \mathbf{q} = \prod_{j=1}^{\ell} q_j = \Big(\prod_{j=1}^{\ell-1} q_j\Big) q_\ell$$

and

$$\prod \mathbf{p} = \prod_{j=1}^{k+1} p_j = \Big(\prod_{j=1}^{k} p_j\Big) p_{k+1} = \Big(\prod_{j=1}^{k} p_j\Big) q_\ell\,.$$

Since $\prod \mathbf{q} = \prod \mathbf{p}$, we can conclude that

$$\Big(\prod_{j=1}^{k} p_j\Big) q_\ell = \Big(\prod_{j=1}^{\ell-1} q_j\Big) q_\ell\,.$$

Hence

$$\prod_{j=1}^{k} p_j = \prod_{j=1}^{\ell-1} q_j\,.$$

So, if we define lists $\mathbf{p}'$, $\mathbf{q}'$, by letting

$$\mathbf{p}' = (p_j)_{j=1}^{k}\,,\quad \mathbf{q}' = (q_j)_{j=1}^{\ell-1}k\,,$$

we have:

(1') $\mathbf{p}'$ is an ordered list of primes of length k,

(2') $\mathbf{q}'$ is an ordered list of primes of length $\ell - 1$,

(3') $\prod \mathbf{p}' = \prod \mathbf{q}$.

Our inductive hypothesis says that $P(k)$ is true, and this tells us that

$$\mathbf{p}' = \mathbf{q}'\,.$$

In particular, the lists $\mathbf{p}'$, $\mathbf{q}'$ have the same length, that is,

$$k = \ell - 1\,.$$

But then

$$k + 1 = \ell\,, \tag{1.7}$$

so the lists $\mathbf{p}$, $\mathbf{q}$ have the same length.

Furthermore, since $\mathbf{p}' = \mathbf{q}'$, we have

$$(\forall j \in \mathbb{N}_k) p_j = q_j\,.$$

But we have proved that $p_{k+1} = q_\ell$, i.e., that $p_{k+1} = q_{k+1}$ (because $\ell = k + 1$). Hence the equality "$p_j = q_j$, that we know holds for all $j \in \mathbb{N}_k$, also holds for $j = k + 1$. So

$$(\forall j \in \mathbb{N}_{k+1}) p_j = q_j\,. \tag{1.8}$$

Equations (1.7) and (1.8) say, precisely, that $\boxed{\mathbf{p} = \mathbf{q}}$

So we have proved that $\mathbf{p} = \mathbf{q}$ assuming (1), (2), and (3).

Hence we have proved (*).

That is, we have proved $P(k + 1)$.

Since we proved $P(k+1)$ assuming $P(k)$, we have proved that $P(k) \Longrightarrow P(k + 1)$.

Since this was proved for an arbitrary $k \in \mathbb{N}$, we have proved that $(\forall k \in \mathbb{N})(P(k) \Longrightarrow P(k + 1))$. This completes the inductive step.

By the Principle of Mathematical induction, we can conclude that $(\forall k \in \mathbb{N})P(k)$. This completes our proof. **Q.E.D.**

1.7 The perfect statement of the FTA

Mathematicians like to have their theorems as simple and general as possible. The FTA, as we have stated it, has a condition that makes it inelegant, namely, the requirement that $n > 1$.

Wouldn't it be nicer if we could just say:

Theorem 2. *(The fundamental theorem of arithmetic.) Every natural number has a unique ordered prime factorization.*

This is clearly more elegant, isn't it? It's much simpler than our previous version, and it is also more general, because it applies to all natural numbers, even to the number 1.

But, of course, just because a statement is nice, it doesn't mean that it is true[3].

Is our new statement of the FTA true? The answer is "yes", but we have to be careful about what this means.

Notice that the only difference between the previous statement of the FTA and our new statement is that the new statement says that the number 1 also has a unique ordered prime factorization. And we have to ask the obvious question: *what is that factorization?*

The answer is: *the ordered prime factorization of* 1 *is the empty list.* Let me explain.

First of all, until now we said that every list has a length, and that this length is a natural number. We now change that, and add a new list: the empty list.

The empty list is a list of length zero, that has no entries whatsoever. We use the symbol $\emptyset$ to denote this list[4].

[3] For example, the statement "every natural number is a product of even primes" is very nice, but it just happens to be completely false.

[4] You may worry that "$\emptyset$" already stands for the empty set. You need not worry. If one does things carefully, it turns out that the empty set and the empty list true are the same

Then ***the empty list is a list of primes.*** This can be rigoruously proved as follows: we want to prove that every entry of the empty list is a prime number. That is, we want to prove that

$$(\forall x)(x \text{ is an entry of } \emptyset \Longrightarrow x \text{ is a prime number})\,.$$

To prove this, we do what we usually do to prove a universal sentence: we let x be arbitrary, and set out to prove that

$$x \text{ is an entry of } \emptyset \Longrightarrow x \text{ is a prime number}\,.$$

Now, "x is an entry of $\emptyset \Longrightarrow x$ is a prime number" is an implication, and the premiss of this implication is false. So the implication is true, and we have proved what we wanted to prove.

Finally, it turns out that $\boxed{\prod \emptyset = 1}$. If you have trouble believing this, I will give you two reasons:

Reason No.1: $\prod \emptyset = 1$ because mathematicians have agreed that this is so. In other words, the statement "$\prod \emptyset = 1$" is true by convention, because mathematicians have agreed that the product of the empty list is equal to one[5].

Reason No.2: Mathematicians are reasonable people, so if they decided that $\prod \emptyset = 1$ they must have had a good reason.

Here is the reason. The inductive definition of "$\prod$" tells us that

$$\prod_{i=1}^{n+1} a_i = \Big(\prod_{i=1}^{n} a_i\Big) a_{n+1} \tag{1.9}$$

if n is a natural number. This means that

$$\prod_{i=1}^{n} a_i = \frac{\prod_{i=1}^{n+1} a_i}{a_{n+1}} \tag{1.10}$$

thing, so it is perfectly all right to use "$\emptyset$" both to denote the empty set and to denote the empty list. But it takes some work to establish this, so for the moment just accept that the empty list is called "$\emptyset$".

[5] This is like many other conventions. Why is Pluto not a planet? Because astronomers have decided that it is isn't. Why is 1 not a prime number? Because mathematicians have decided that it isn't. Why do we drive on the right side of the street? Because at some point it was decided (in the U.S and many other countries, but not in all countries) that the right side of the street is the side on which people should drive. Why are cows called "cows" rather than, say, "zebras"? Because people have agreed that that is the name of those animals.

for $n \in \mathbb{N}$. Now suppose we want to make Formula (1.10) also true for $n = 0$. Then we must have

$$\prod_{i=1}^{0} a_i = \frac{\prod_{i=1}^{1} a_i}{a_1}\,. \tag{1.11}$$

But the list $(a_i)_{i=1}^{0}$ is the empty list, because there are no indices i such that $1 \le i \le 0$. And

$$\prod_{i=1}^{1} a_i = a_1\,.$$

So

$$\prod \emptyset = \frac{a_1}{a_1}\,, \tag{1.12}$$

and then

$$\prod \emptyset = 1\,. \tag{1.13}$$

This is not a rigorous proof. (Why should Formula (1.10) be valid for $n = 0$? We have not given a reason. And what if $a_1 = 0$?) But it is an argument showing that the convention that $\prod \emptyset = 1$ is a reasonable one.

In any case, once you agree that $\prod \emptyset = 1$, it follows[6] that our nicer version of the FTA is true.

[6] We should also prove that the empty list is ordered. But that's easy to do. You should try to do it.