MATHEMATICS 300 — FALL 2017

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S NOTES

PART VIII

Contents

19 The great theorems of elementary integer arithmetic

Elementary integer arithmetic

Integer arithmetic is the study of the integers.
Elementary integer arithmetic is the study of the most basic facts about the integers. It is a body of theory that

- involves a number of important concepts, such as

  (**) divisibility,

  (**) prime numbers,

  (! !) greatest common divisor,

- contains interesting and sometimes surprising results, such as

  (* !) the fundamental theorem of arithmetic,

  (! !) Bézout's lemma,

  (! !) Euclid's lemma,

  (! !) Euclid's theorem on the existence of infinitely many prime numbers,

  and uses several powerful tools, such as

  (**) the principle of mathematical induction (PMI),

  (**) the well-ordering principle (WOP),

  (**) the division theorem.

(The items marked "(**)" have already been discussed in these notes. The items marked "(! !)" will be discussed in this section. One item is marked "(!)", because we have already proved one half of it, whereas the other half has not yet been proved, but will be proved in this section.*

We now explain the concepts and results from the above list that have not been discussed yet, and prove the theorems.

19.1 The greatest common divisor of two integers

The first item in the list that is new to us is the concept of "greatest common divisor", so we begin by explainimg what this means.

Remark 24. We are about to define "greatest common divisor". If in an exam you are asked to define "greatest common divisor", then the first two questions that you have to ask yourself are ***is "greatest common divisor" a term or a predicate?***, and ***what are the arguments?***. There are two equally correct possible answers[1]:

FIRST ANSWER:

1. "the greatest common divisor of" is a ***term***: we talk about "the greatest common divisor of two integers a, b", which is an integer; so "the greatest common divisor of a and b" is a term, because it is the name of a thing (specifically, an integer),

2. "the greatest common divisor of" has ***two arguments***: we talk about *the greatest common divisor of two integers a and b.*

SECOND ANSWER:

1. "is the greatest common divisor of " is a ***predicate***: we say things such as "g is the greatest common divisor of the integers a, b", and this is a statement that can be true or false, depending on who a, b, and g are; so "is the greatest common divisor of" is a predicate, because it has a true-false truth value,

2. "is the greatest common divisor of" has ***three arguments***: we write sentences such as *g is the greatest common divisor of a and b.*

So, even before you specify exactly what "greatest common divisor" means, you already know how the definition should start:

[1]There is not contradiction between those two answers. The words "greatest common divisor" are part of both the two-argument term "the greatest common divisor of a and b", and the three-argument predicate "g is the greatest common divisor of a and b".

1. If you choose Answer No. 1, then your definition should start with the words

   > Let a, b be integers. The greatest common divisor of a and b is . . . .

2. If you choose Answer No. 2, your definition should start with the words

   > Let a, b, g be integers. We say that g is a greatest common divisor of a and b if . . . . □

We are going to choose Answer No. 2. That is, we are going to define the three-argument predicate "g is a greatest common divisor of a and b". And then we will prove that if a greatest common divisor of a and b exists, then it is unique. And this will allow us to talk about ***the*** greatest common divisor of a and b.

In order to define "geatest common divisor",

1. We will first define "common divisor". This is going to be a *three-argument predicate* (because "c is a common divisor of a and b" is a statement about a, b and c that can be true or false depending on who a, b, c are).

2. Having defined "common divisor", the definition of "greatest common divisor" will just say the most obvious thing: a greatest common divisor of a and b is a common divisor that is the largest of all commmon divisors.

And here, finally, are the definitions:

Definition 42. Let a, b, g be integers. We say that c is a common divisor (or common factor) of a and b if c divides a and c divides b. □

In other words,

$$c \text{ is a common divisor of } a \text{ and } b \iff (c|a \wedge c|b)\,. \tag{19.1}$$

Definition 43. Let a, b, g be integers. We say that g is a greatest common divisor of a and b if

1. g is a common divisor of a and b.

2. If c is any common divisor of a and b, then $c \leq g$. $\square$

In other words: ***a greatest common divisor of the integers*** a***,*** b***, is a common divisor that is greater that or equal to every common divisor of*** a ***and*** b.

We are going to use "GCD" as an abbreviation for "greatest common divisor. Then

$$g \text{ is a GCD of } a \text{ and } b \iff \left(g|a \wedge g|b \wedge (\forall c \in \mathbb{Z})\Big((c|a \wedge c|b) \Longrightarrow c \leq g\Big)\right). \tag{19.2}$$

19.1.1 When do we use "a" and when do we use "the"?

Can we talk about "the" greatest common divisor of a and b? The answer would be

- "no", if there is more than one gcd. For example:
  - We do not say "Piscataway is *the* town in New Jersey", because there are lots of towns in New Jersey; we say "Piscataway is *a* town in New Jersey",
  - We do not say "B is *the* subset of A", because a set typically has lots of subsets; we say "B is *a* subset of A",
  - We do not say "John McCain is ***the*** U.S. Senator", because there are many U.S. Senators; we say "John McCain is ***a*** U.S. Senator".
  - We do not say "2 is ***the*** factor of 6", because 6 has several factors (eight of them, to be precise: 1, -1, 2, -2, 3, -3, 6, and -6). We say "2 is ***a*** factor of 6", .
  - We do not say "c is *the* common divisor of a and b", because two integers typically have lots of common divisors[2]; we say "c is *a* common divisor of a and b".
- "the", if there is only one gcd. For example:

[2]They always have at least two comoon divisors, namely, 1 and -1. And in most cases they have many more: for example, 12 and 18 have eight common divisors: 1, -1, 2, -2, 3, -3, 6, and -6.

- We do not say "Paris is *a* capital of France", because France has only one capital; we say "Paris is *the* capital of France".
- We do not say "$\mathcal{P}(A)$ is *a* power set of A", because a set only has one power set; we say "$\mathcal{P}(A)$ is *the* power set of A".
- We do not say "p is *a* product of a and b", because two integers have only one product; we say "p is *the* product of a and b".
- We do not say "$A \times B$ is *a* Cartesian product of A and B", because two sets have only one Cartesian product; we say "$A \times B$ is *the* Cartesian product of A and B".

In general: whatever a "shmoo" might be, we talk about "***the*** shmoo" if there is only one shmoo, and we talk about "***a*** shmoo" if there is more that one shmoo.

19.1.2 Uniqueness of the greatest common divisor

So which one is it? Shall we talk about "the" greatest common divisor of two integers, or about "a" greatest common divisor?

So far, in Definition 43, I talked about ***a*** greatest common divisor, because we didn't know yet if there is only one or more than one greatest common divisor of two given integers.

But now we are going to ***prove*** that the greatest common divisor, if it exists, is unique. And once we know that, we will be able to talk about ***the*** greatest common divisor of two integers.

Proposition 3. *Let a, b be integers. Then, if a greatest common divisor of a and b exists, it follows that a and b have only one greatest common divisor.*

Proof. To prove that there is only one GCD of a and b, we assume that g_1 and g_2 are GCDs of a and b, and prove that $g_1 = g_2$.

Since g_1 is a GCD of a and b, the definition of "GCD" tells us that $g_1|a$ and $g_1|b$.

Since g_2 is a GCD of a and b, the definition of "GCD" tells us that if c is any integer such that $c|a$ and $c|b$, then $c \leq g_2$. And we can apply this with g_1 in the role of c. Since $g_1|a$ and $g_1|b$, it follows that $g_1 \leq g_2$.

Exactly the same argument works to prove that $g_2 \leq g_1$.

Since $g_1 \leq g_2$ and $g_2 \leq g_1$, it follows that $g_1 = g_2$. **Q.E.D.**

So from now on we can talk about "***the*** GDC of a and b". And we can give it a name. So we shall call it "$GCD(a, b)$".

> If a, b are integers, and the greatest common divisor of a and b exists, then "$GDC(a, b)$" is the name of the GCD of a and b.

Example 29.

1. $GCD(5, 7) = 1$. *Reason:* The only common divisors of 5 and 7 are 1 and -1. And 1 is the largest of the two, so $1 = GCD(5, 7)$.

2. $GCD(5, 15) = 5$. *Reason:* The common divisors of 5 and 15 are 1, -1, 5 and -5. And 5 is the largest of these four integers, so $5 = GCD(5, 15)$.

3. $GCD(18, 30) = 6$. *Reason:* The common divisors of 18 and 30 are 1, -1, 2, -2, 3, -3, 6, and -6. And 6 is the largest of these integers, so $6 = GCD(18, 30)$.

4. $GCD(28, 73) = 1$. *Reason:* 73 is prime. So the only factors of 73 are 1, -1, 73 and -73. But 73 and -73 are not factors of 28. So the only common divisors of 28 and 73 are 1 and -1. And 1 is the largest one. So $1 = GCD(28, 73)$.

5. $GCD(28, 0) = 28$. *Reason:* Every integer k is a factor of 0, because $0 = 0 \times k$, so $(\exists u \in \mathbb{Z})0 = uk$, so $k|0$. So the common factors of 28 and 0 are the factors of 28. And the largest of those factors is 28. So $28 = GCD(28, 0)$.

6. $GCD(-28, 0) = 28$. *Reason:* Every integer k is a factor of 0, as explained before. So the common factors of -28 and 0 are the factors of -28. And the largest of those factors is 28. So $28 = GCD(-28, 0)$.

In all the examples in the previous list, the GDC turned out to be positive. We can prove easily that this is a general fact:

Proposition 4. *Let a, b be integers such that the greatest common divisor $GCD(a, b)$ exists. Then*

$$GCD(a, b) \geq 1\,.$$

Proof. $GCD(a, b)$ is greater than or equal to every common factor of a and b. And 1 is a common factor of a and b. So $GCD(a, b) \geq 1$. **Q.E.D.**

19.1.3 Bézout's lemma; the statement

An extremely important, and rather surprining, fact about geratest common divisors is ***Bézout's lemma:***

Bézout's lemma

If a and b are two integers that are not both equal to zero, then $GCD(a, b)$ is equal to the sum of a multiple of a and a multiple of b. That is, there exist integers u, v such that

$$GCD(a, b) = ua + vb\,. \tag{19.3}$$

19.1.4 The proof of Bézout's lemma

In order to prove Bézout's lemma we will have to work all the time with numbers that are sums $ua + vb$ of a multiple of a and a multiple of b. So it will be convenient to give those numbers a name.

Definition 44. Assume that a, b, and c are integers. Then we say that c is an integer linear combination of a and b if c is the sum of a multiple of a and a multiple of b.

In other words: c is an integer linear combination of a and b if

$$(\exists u \in \mathbb{Z})(\exists v \in \mathbb{Z})\, c = ua + vb\,.$$

In order to avoid having to write the words "c is an integer linear combination of a and b" all the time, we give a name to the set of all numbers c such that c is an integer linear combination of a and b. We call this set "ILC(a, b)".

So the set ILC(a, b) is defined as follows:

$$\text{ILC}(a, b) = \{\, c \in \mathbb{Z} : (\exists u \in \mathbb{Z})(\exists v \in \mathbb{Z}) c = ua + bv \,\}\,. \tag{19.4}$$

And now that we have defined the set ILC(a, b), we can say "$c \in$ ILC(a, b)" instead of "c is an integer linear combination of a and b".

And now we are ready to state the main theorem of this section, which is a result that contains Bézout's lemma as a special case.

Theorem 60. *Let a, b be integers. Then:*

1. *If $a = 0$ and $b = 0$, then a greatest common divisor in the sense of Definition 43 does not exist.*
2. *If $a \neq 0$ or $b \neq 0$, then*
   (a) *The greatst common divisor $GCD(a, b)$ of a and b exists,*
   (b) *$GCD(a, b)$ is the smallest of all positive integrs that are integer linear combinations of a and b. (In other words, $GCD(a, b)$ is the smallest member of the set $\mathrm{ILC}(a, b) \cap \mathbb{N}$.)*

Proof. First let us look at the case when $a = 0$ and $b = 0$. In this case, every integer is a common factor of a and b, because every integer divides 0. So there is no largest integer that is a common factor of a and b. That is, the GDC of a and b does not exist.

Now let us look at the case when $a \neq 0$ or $b \neq 0$. In this case, one of the four numbers $a, -a, b, -b$ must be positive. (If $a \neq 0$ then either $a > 0$ or $-a > 0$. If $b \neq 0$ then either $b > 0$ or $-b > 0$.) And all four numbers belong to $\mathrm{ILC}(a, b)$. So one of the four numbers belongs to $\mathrm{ILC}(a, b) \cap \mathbb{N}$. Hence

$$\mathrm{ILC}(a, b) \cap \mathbb{N} \neq \emptyset\,.$$

So $\mathrm{ILC}(a, b) \cap \mathbb{N}$ is a nonempty set of natural numbers. By the well-ordering principle, $\mathrm{ILC}(a, b) \cap \mathbb{N}$ has a smallest member. And, in addition, we know that the smallest member of a subset of $\mathbb{R}$, if it exists, is unique. So we can talk about ***the*** smallest member of $\mathrm{ILC}(a, b) \cap \mathbb{N}$.

Let us give a name to this smallest member; let us call it g. So

$$\begin{aligned} & g \in \mathrm{ILC}(a, b) \cap \mathbb{N} \\ \text{and} \qquad & (\forall n \in \mathbb{Z})(n \in \mathrm{ILC}(a, b) \cap \mathbb{N} \Longrightarrow g \leq n)\,. \end{aligned}$$

We want to prove that

(*) g is the greatest common divisor of a and b.

In order to prove (*), the definition of "greatest common divisor" tells us that we have to prove the following two things:

(*1) g is a common divisor of a and b; that is,

$$g|a \wedge g|b\,. \tag{19.5}$$

(*2) g is the largest of all common divisors of a and b; that is,

$$(\forall c \in \mathbb{Z})\Big((c|a \wedge c|b) \Longrightarrow c \leq g\Big)\,. \tag{19.6}$$

Since $g \in \mathrm{ILC}(a,b)$, we can pick integers u, v such that

$$g = ua + vb\,. \tag{19.7}$$

*Proof of (*1).* Using the division theorem, we can divide a by g with a remainder r. That is, we can pick integers q, r such that

$$a = gq + r \text{ and } 0 \leq r < g\,. \tag{19.8}$$

(The division theorem says "$0 \leq r < |g|$". But in our case we know that $g \in \mathbb{N}$, so $|g| = g$.)

Then

$$\begin{aligned} r &= a - gq \\ &= a - (ua + vb)q \\ &= a - uqa - vqb \\ &= (1 - uq)a + (-vq)b\,. \end{aligned}$$

So

$$r \in \mathrm{ILC}(a,b)\,. \tag{19.9}$$

We know that $r \geq 0$. Let us prove that $r = 0$, by contradition.

Assume that $r \neq 0$.

Since $r \geq 0$, it follows that $r > 0$.

So r is an integer and $r > 0$.

Hence $r \in \mathbb{N}$.

Since $r \in \mathrm{ILC}(a,b)$, it follows that $r \in \mathrm{ILC}(a,b) \cap \mathbb{N}$.

In addition, (19.8) tells us that $r < g$.

So g is not the smallest member of $\mathrm{ILC}(a,b) \cap \mathbb{N}$, because r is a member of $\mathrm{ILC}(a,b) \cap \mathbb{N}$ and $r < g$.

But g is the smallest member of $\mathrm{ILC}(a,b) \cap \mathbb{N}$.

Hence

g is the smallest member of $\mathrm{ILC}(a,b) \cap \mathbb{N}$ and g is not the smallest member of $\mathrm{ILC}(a,b) \cap \mathbb{N}$,

which is a contradiction.

So we have derived a contradiction from the assumption that $r \neq 0$.

Hence $r = 0$.

Since $r = 0$ and $a = gq + r$, we can conclude that $a = gq$.

Therefore $g|a$.

The proof that $g|b$ is identical, and we omit it.

So $\boxed{g|a \wedge g|b}$, and this completes the proof of (*1).

*Proof of (*2).* We want to prove the universal sentence (19.6).

Let $c \in \mathbb{Z}$ be arbitrary.

Assume that $c|a \wedge c|b$.

Then we can pick integers j, k such that

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

Since $g = ua + vb$, we get

$$\begin{aligned} g &= ua + vb \\ &= ucj + vck \\ &= c(uj + vk)\,. \end{aligned}$$

Furthermore, $uj + vk$ is an integer, because u, v, j and k are integers.

Hence c divides g.

Our goal is to prove that $c \leq g$. And for that purpose we distinguish two cases: either $c \leq 0$ or $c > 0$.

Case 1: $c \leq 0$. In this case, the conclusion that $\boxed{c \leq g}$ is obvious, because $c \leq 0$ and $g > 0$, since $g \in \mathbb{N}$.

Case 2: $c > 0$. In this case, we have

$$g = \ell c\,,$$

where $\ell = uj + vk$. Then ℓ is an integer.

Then ℓ must be > 0. (Reason: if ℓ was ≤ 0 then ℓc would be ≤ 0, since $c > 0$. But $\ell c = g$, and $g > 0$. So ℓ cannot be ≤ 0. So $\ell > 0$.)

Since ℓ is an integer, and $\ell > 0$, it follows that ℓ is a natural number. Hence $\ell \geq 1$.

Since $\ell \geq 1$ and $\ell c = g$, it must be the case that $\boxed{c \leq g}$. (Reason: if $c > g$, then it would follow that $\ell c > g$, because $\ell c \geq c$—since $\ell \geq 1$—and $c > g$. But $\ell c = g$.)

So we have shown that $c \leq g$. And this completes our proof. **Q**.**E**.**D**.

19.2 Prime numbers

Definition 45. A prime number is a natural number p such that

I. $p > 1$,

II. p does not have any natural number factors other than 1 and p. □

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

Definition 46. A prime number is a natural number p such that

I. $p > 1$,

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

19.2.1 Why isn't 1 prime?

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

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

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

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

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

19.2.2 Euclid's lemma: an important application of Bézout's lemma

Euclid's lemma is one of the most important technical results in elementary integer arithmetic. For example, ***Euclid's lemma is the key fact needed to prove the missing half of the Fundamental Theorem of Arithmetic (FTA), that is, the uniqueness of the prime factorization.***

And, as you will see, the key fact that makes the proof of Euclid's lemma work is Bézout's lemma.

Euclid's lemma is about the following question:

Question 5. *Suppose an integer p divides the product ab of two integers a, b. Does it follow that p must divide a or p must divide b?* □

The answer is "no" if a, b and p are arbitrary integers.

Example 30. 6 divides 2×3 (because $6 = 2 \times 3$) but 6 doesn't divide 2 and 6 does not divide 3. □

But it turns out that the answer s "yes" if p is prime, and this is what Euclid's lemma says:

Theorem 61. ***(Euclid's lemma)*** *If a, b, p are integers, such that p is prime and p divides the product ab, then p divides a or p divides b.*

Proof. To prove that $p|a \vee p|b$, we prove[3] that $(\sim p|a) \Longrightarrow p|b$. i.e., that if p does not divide a then p divides b.

Assume that p does not divide a. Since p is prime, the only natural numbers that are factors of p are 1 and p. And p is not a factor of a, because we are assuming that p does not divide a.

Therefore the greatest common divisor of p and a is equal to 1.

It then follows from Bézout's lemma that 1 is equal to the sum of a multiple of p and a multiple of a. That is, we can pick integers u, v such that

$$1 = up + va\,.$$

On the other hand, since p divides ab, we may pick an integer k such that

$$ab = pk\,.$$

Then

$$\begin{aligned} b &= b \times 1 \\ &= b \times (up + va) \\ &= ubp + vab \\ &= ubp + vpk \\ &= (ub + vk)p\,, \end{aligned}$$

[3]Why do we do that? This is so because of Rule $\vee_{prove}$, the rule for proving "$\vee$" sentences: if, assuming $\sim A$, you prove B, then you can go to $A \vee B$. And the reason for Rule $\vee_{prove}$ is this: suppose we want to prove $A \vee B$. There are two possibilities: either A is true or A is not true. If A is true then $A \vee B$ is true, and we are done. If A is false then, since we know how to prove B assuming $\sim A$, B follows, so "$A \vee B$" is true in this case as well. Here is another way to see this: "$A \vee B$" is false if and only if both A and B are false. And the implication "$(\sim A) \Longrightarrow B$" is false only if and only if the premise is true and the conclusion is false, that is, if and only if A is false and B is false. So "$A \vee B$" is false if and only if "$(\sim A) \Longrightarrow B$" is false. So "$A \vee B$" is true if and only if "$(\sim A) \Longrightarrow B$" is true. So proving "$A \vee B$" amounts to the same thing as proving "$(\sim A) \Longrightarrow B$". And to prove "$(\sim A) \Longrightarrow B$" we assume $\sim A$ and prove B.

so p divides b. **Q.E.D.**

19.2.3 An important notational convention: the sets $\mathbb{N}_k$

In what follows we will be making lots of statements about "the natural numbers $1, 2, \ldots, k$", that is "all the natural numbers j such that $j \leq k$". So it will be convenient to give a name to the set of all such js.

If $k \in \mathbb{N} \cup \{0\}$ (that is, k is a nonnegative integer, i.e., k is a natural number or zero), we let

$$\mathbb{N}_k = \{j \in \mathbb{N} : j \leq k\}.$$

Then $\mathbb{N}_k$ is ***the set of the first k natural numbers.***
For example:

$$\mathbb{N}_0 = \emptyset, \quad \mathbb{N}_1 = \{1\}, \quad \mathbb{N}_2 = \{1, 2\},$$
$$\mathbb{N}_3 = \{1, 2, 3\}, \quad \mathbb{N}_4 = \{1, 2, 3, 4\}, \quad \mathbb{N}_5 = \{1, 2, 3, 4, 5\}.$$

Then

$$j \in \mathbb{N}_k$$

is just another way of saying "$j \in \mathbb{N}$ and $j \leq k$".

19.2.4 The generalized Euclid lemma

Theorem 61 (that is, Euclid's lemma) tells us that If p is a prime and a, b, are integers such that p is prime and p divides the product ab, then p divides a or p divides b.

The ***generalized Euclid lemma*** answers the following more general question:

Question 6. *What happens if instead of two integers a, b we have three integers a, b, c? Is it still true that if $p|abc$ then $p|a$ or $p|b$ or $p|c$?*

What if we have four integers a, b, c, d. Is it still true that if $p|abcd$ then $p|a$ or $p|b$ or $p|c$ or $p|d$? □

The answer is "yes", for three, four, or any number of integers, as we now prove.

Theorem 62. *Let k be a natural number, and let $p, a_1, a_2, \ldots, a_k$ be integers such that*

1. *p is a prime number,*
2. *p divides the product $\prod_{j=1}^{k} a_j$.*

Then p divides one of the factors. That is, $(\exists j \in \mathbb{N}_k) p|a_j$,

Proof. We will prove this by induction.

We want to prove

$$(\forall k \in \mathbb{N})(\forall p, a_1, a_2, \ldots, a_k \in \mathbb{Z})$$
$$\left(\left(p \text{ is a prime number} \wedge p \Big| \prod_{j=1}^{k} a_j \right) \Longrightarrow (\exists j \in \mathbb{N}_k) p|a_j \right). \quad (19.10)$$

Sentence (19.10) is a closed sentence. i.e., a sentence with no open variables, because the sentence contains the variables $k, p, a_1, a_2, \ldots, a_k$ and j, but they are all quantified, so no variables are open.

We can express sentence (19.10) as "$(\forall k \in \mathbb{N}) P(k)$", where $P(k)$ be the sentence

$$(\forall p, a_1, a_2, \ldots, a_k \in \mathbb{Z})$$
$$\left(\left(p \text{ is a prime number} \wedge p \Big| \prod_{j=1}^{k} a_j \right) \Longrightarrow (\exists j \in \mathbb{N}_k) p|a_j \right). \quad (19.11)$$

Then $P(k)$ is a sentence with one open variable, and the open variable is k. So $P(k)$ is exactly the kind of sentence for which we can expect to be able to prove "$(\forall k \in \mathbb{N}) P(k)$" by induction.

Now let us prove "$(\forall k \in \mathbb{N}) P(k)$" by induction.

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

$$(\forall p, a_1 \in \mathbb{Z})\left(\left(p \text{ is a prime number} \wedge p \Big| \prod_{j=1}^{1} a_j\right) \Longrightarrow (\exists j \in \mathbb{N}_1) p|a_j\right). \quad (19.12)$$

But $\mathbb{N}_1$ is just the set $\{1\}$, so "$(\exists j \in \mathbb{N}_1)p|a_j$" just amounts to saying "$p|a_1$".

Furthermore. $\prod_{j=1}^{1} a_j = a_1$. So $P(1)$ actually says

$$(\forall p, a_1 \in \mathbb{Z})\left(\left(p \text{ is a prime number} \wedge p|a_1\right) \Longrightarrow p|a_1\right). \quad (19.13)$$

And this is clearly true. So (19.13) is true.

Hence $P(1)$ is true.

Inductive step. We want to prove that

$$(\forall k \in \mathbb{N})(P(k) \Longrightarrow P(k+1)). \quad (19.14)$$

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

Assume that $P(k)$ is true.

Then

$$(\forall p, a_1, a_2, \ldots, a_k \in \mathbb{Z})$$
$$\left(\left(p \text{ is a prime number} \wedge p \Big| \prod_{j=1}^{k} a_j\right) \Longrightarrow (\exists j \in \mathbb{N}_k) p|a_j\right). \quad (19.15)$$

We want to prove $P(k+1)$, that is,

$$(\forall p, a_1, a_2, \ldots, a_k, a_{k+1} \in \mathbb{Z})$$
$$\left(\left(p \text{ is a prime number} \wedge p \Big| \prod_{j=1}^{k+1} a_j\right) \Longrightarrow (\exists j \in \mathbb{N}_{k+1}) p|a_j\right). \quad (19.16)$$

So let $p, a_1, a_2, \ldots, a_k, a_{k+1}$ be arbitrary integers such that

1. p is a prime number.
2. p divides $\prod_{j=1}^{k+1} a_j$.

We want to prove that $(\exists j \in \mathbb{N}_{k+1})p|a_j$. i.e., that $p|a_j$ for some $j \in \mathbb{N}_{k+1}$.

The inductive definition of "$\prod$" tells us that

$$\prod_{j=1}^{k+1} a_j = \Big(\prod_{j=1}^{k} a_j\Big) a_{k+1}\,.$$

So

$$p\Big|\Big(\prod_{j=1}^{k} a_j\Big) a_{k+1}\,.$$

Euclid's lemma tells us, since p is prime, that if p divides a product uv of two integers then $p|u$ or $p|v$. In our case, if we take $u = \prod_{j=1}^{k} a_j$ and $v = a_{k+1}$, the lemma tells us that either

(i) p divides $\prod_{j=1}^{k} a_j$

or

(ii) p divides a_{k+1}..

We now see what happens in each of these two cases.

Case (i): Assume that p divides $\prod_{j=1}^{k} a_j$. Then we can use $P(k)$ and conclude that p divides one of the factors, that is, we can conlude that $(\exists j \in \mathbb{N}_k)p|a_j$. So we may pick j in $\mathbb{N}_k$ such that $p|a_j$. Then obviously $j \in \mathbb{N}_{k+1}$, so $\boxed{(\exists j \in \mathbb{N}_{k+1})p|a_j}$.

Case (ii): Assume that p divides a_{k+1}. Then it is is also true that $\boxed{(\exists j \in \mathbb{N}_{k+1})p|a_j}$.

So in both cases $(\exists j \in \mathbb{N}_{k+1})p|a_j$, so we have established the conclusion that $\boxed{\boxed{(\exists j \in \mathbb{N}_{k+1})p|a_j}}$.

We have proved this for arbitrary integers $p, a_1, a_2, \ldots, a_k, a_{k+1}$ such that p is a prime number and p divides $\prod_{j=1}^{k+1} a_j$.

Hence we have proved $P(k+1)$.

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

Since we have proved $P(k) \Longrightarrow P(k+1)$ for arbitray $k \in \mathbb{N}$, we have proved $(\forall k \in \mathbb{N})(P(k) \Longrightarrow P(k+1))$.

This completes the inductiove step.

So we have proved $(\forall k \in \mathbb{N})P(k)$. **Q.E.D.**

19.2.5 Coprime integers

Definition 47. If a, b are integers, we say that a and b are coprime (or that "a is coprime with b", or that "b is coprime with a") if a and b have no nontrivial common factors (that is, if the only integers f such that $f|a$ and $f|b$ are 1 and -1). □

If a and b are coprime, then they cannot both be zero, because if $a = 0$ and $b = 0$ then every integer is a common factor of a and b (because every integer n is a factor of 0, since $0 = 0 \times n$), so a and b have lots of nontrivial common factors.

And if a and b are not both 0, then the greatest common divisor $GCD(a, b)$ exists. If a and b are coprime, then $GCD(a, b)$ must be equal to 1, because $GCD(a, b)$ is a common factor of a and b.

On the other hand, if $GCD(a, b) = 1$ then a and b must be coprime. (Reason: if a and b were not coprime, then they would have a common factor f such that $f > 1$, and since $f \leq GCD(a, b)$, we would conclude that $GCD(a, b) > 1$.)

So we have proved:

Proposition 5. *Let a and b are integers, then a and b are coprime if and only if they are not both equal to zero and $GCD(a, b) = 1$.* □

We now introduce a symbol for coprimeness:

If a and b are integers, we write

$$a \perp b$$

for "a and b are coprime".
For example:

$$\begin{array}{ccc} 3 \perp 7 & -12 \perp 55 & 1 \perp 0 \\ \sim 22 \perp 14 & \sim 78 \perp -15 & \sim 49 \perp 77 \end{array}.$$

19.2.6 Divisibility of an integer by the product of two integers

In this section we look at the following question:

Question 7. *If an integer n is divisible by two integers a, b, when can we conclude that n is divisible by the product ab?* □

It is clear that the answer is "not always".

Example 31. If $a = 6$ and $b = 4$, then it is ***not*** true that every integer that is divisible by a and by b is divisible by ab. For example, 12 is divisible by a and by b, but it is clearly not divisible by ab, since $ab = 24$. □

The answer to Question 7 is: ***if*** $a|n$ ***and*** $b|n$***, then we can conclude that*** n ***is divisible by the product*** ab ***if*** a ***and*** b ***are coprime***.

Indeed, we can prove:

Theorem 63. *If*

1. *a, b, n are integers,*
2. *a divides n,*
3. *b divides n,*
4. *a and b are coprime,*

then ab divides n.

Proof. Since a and b are coprime, we may pick integers u, v such that

$$1 = ua + vb\,.$$

Since n is divisible by a and by b, we can pick integers j, k such that

$$n = aj \qquad \text{and} \qquad n = bk\,.$$

Then

$$\begin{aligned} n &= n \times 1 \\ &= n \times (ua + vb) \\ &= nua + nvb \\ &= (bk)ua + (aj)vb \\ &= ab(ku + jv)\,. \end{aligned}$$

So ab divides n. **Q.E.D.**

19.2.7 Coprime integers and divisibility: an extension of Euclid's lemma

In this section we look at the following question:

Question 8. *If*

1. *p, a, b are integers,*
2. *p divides ab,*
3. *p does not divide a,*

can we conclude that p must divide b?

Euclid's lemma tells us that the answer is "yes" if p is prime.

But if p is not prime the answer could be "no", as we showed in Example 30.

It turns out that, using exactly the same strategy—nased on Bézout's lemma—that we used to prove Euclid's lemma, we can extend Euclid's lemma by proving that the answer is "yes" not only when p is prime but also in some cases when p is not prime.

What is needed is that p ***and*** a ***should be coprime***. This will always be the case when p is prime, because when p is prime and p does not divide a it follows that p and a are coprime.

Theorem 64. *If*

- a, b, p, *are integers,*
- p *is coprime with* a,
- p *divides the product* ab,

then p *divides* b.

Proof. Since $p \perp a$, the greatest common divisor $GCD(p, a)$ is equal to 1.

Using Bézout's lemma, we can pick integers u, v such that

$$ua + vp = 1\,. \tag{19.17}$$

Then, if we multiply both sides of (19.17) by b, we get

$$uab + vpb = b\,.$$

Since p divides ab, we can pick an integer k such that

$$ab = kp\,.$$

Then

$$\begin{aligned} b &= uab + vpb \\ &= ukp + vpb \\ &= (uk + vb)p\,, \end{aligned}$$

so p divides b. **Q.E.D.**

We said before that Theorem 64 is an extension of Euclid's lemma. To see this, let me show how, once you have Theorem 64, Euclid's lemma follows easily:

An easy derivation of Euclid's lemma from Theorem 64: Suppose p is prime and p divides the product ab of two integers a, b. We want to prove that $p|a$ or $p|b$. For this purpose, we assume that p does not divide a and prove that p divides b.

Since p is prime and p does not divide a, p is coprime with a. Then Theorem 64 tells us that p divides b, which is exactly what we want to prove in order to prove Euclid's Lemma. **Q.E.D.**

19.2.8 Another extension of Euclid's lemma

In addition to providing an easy way to prove Euclid's lemma, Theorem 64 has another important consequence:

Theorem 65. *If a, b, p, are integers, and p is coprime with a and with b, then p is coprime with the product ab.*

Theorem 64 is easy to remember: it says that

$$\text{If } p \perp a \text{ and } p \perp b \text{ then } p \perp ab\,.$$

Proof of Theorem 65.

Assume that p is not coprime with ab. Then p and ab have a common factor m such that $m > 1$.

Since $m|p$, and $p \perp a$, m must be coprime with a as well. (Reason: any common factor of m and a would be a common factor of p and a, since $m|p$. Since p and a do not have nontrivial common factors, m and a cannot have nontrivial common factors either.)

On the other hand, m divides ab, because $m|p$ and $p|ab$.

So m divides ab and m is coprime with a. By Theorem 64, m divides b.

Hence $m|b$, $m|p$, and $m > 1$. Therefore p and b have a nontrivial common factor.

It follows that $\boxed{p \text{ and } b \text{ are not coprime}}$.

But $\boxed{p \text{ and } b \text{ are coprime}}$.

So we have reached a contradiction, and this was the result of assuming that p is not coprime with ab.

Hence p is coprime with ab. **Q.E.D.**

Why is Theorem 65 "an extension of Euclid's lemma"? The reason is, once again, that from Theorem 65 one can easily derive Euclid's lemma.

An easy derivation of Euclid's lemma from Theorem 65: Suppose p is prime and p divides the product ab of two integers a, b. We want to prove that $p|a$ or $p|b$. For this purpose, we assume that it is not true that $p|a \vee p|b$. Then p does not divide a and p does not divide b. Since p is prime and p does not divide a, p is coprime with a. Since p is prime and p does not divide b, p is coprime with b. Then Theorem 65 tells us that $\boxed{p \text{ is coprime with } ab}$.

On the other hand, we are assuming that $p|ab$, so p and ab have a non-trivial common factor, namely, p. So $\boxed{p \text{ is not coprime with } ab}$.

So we have reached a contradiction, and this happened because we assumed that it is not true that $p|a \vee p|b$. Hence $\boxed{\boxed{p|a \vee p|b}}$. **Q.E.D.**

19.2.9 Another extension of Euclid's lemma

Theorem 65 tells us that if an integer p is coprime with two integers a, b, then it is coprime with the product ab.

We now consider the following question:

Question 9. *What happens if instead of two integers a, b we have three integers a, b, c? Is it still true that if $p \perp a$, $p \perp b$, and $p \perp c$, then $p \perp abc$?*

What if we have four integers a, b, c, d. Is it still true that if $p \perp a$, $p \perp b$, $p \perp c$, and $p \perp d$, then $p \perp abcd$? □

The answer is "yes", for three, four, or any number of integers, as we now prove.

Theorem 66. *Let k be a natural number, and let $p, a_1, a_2, \ldots, a_k$ be integers such that p is coprime with a_j for every $j \in \mathbb{N}_k$. Then p is coprime with the product $\prod_{j=1}^{k} a_j$.*

Proof. We will do a proof by induction.

Let $P(k)$ be the sentence

(%) If $p, a_1, a_2, \ldots, a_k$ are integers such that $p \perp a_j$ for every $j \in \mathbb{N}_k$, then $p \perp \prod_{j=1}^{k} a_j$.

In formal language, $P(k)$ is the sentence

$$(\forall p, a_1, a_2, \ldots, a_k \in \mathbb{Z})\Big((\forall j \in \mathbb{N}_k) p \perp a_j \Longrightarrow p \perp \prod_{j=1}^{k} a_j \Big) . \tag{19.18}$$

Remark 25. Formula (19.18) contains the variables $p, j, k, a_1, a_2, \ldots, a_k$. But all these variables, except k, are quantified. So k is the only open variable. Hence *(19.18) is a one-variable predicate, and the open variable is k.* That's why we can call the predicate (19.18) $P(k)$, and try to prove by induction on k that $(\forall k \in \mathbb{N})P(k)$. □

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

Base step. We have to prove that $P(1)$ is true. But $P(1)$ says

$$(\forall p \in \mathbb{Z})(\forall a_1 \in \mathbb{Z})\Big(p \perp a_1 \Longrightarrow p \perp \prod_{j=1}^{1} a_j \Big) , \tag{19.19}$$

and the inductive definition of "$\prod$" says that

$$\prod_{j=1}^{1} a_j = a_1 .$$

Therefore $P(1)$ says

$$(\forall p \in \mathbb{Z})(\forall a_1 \in \mathbb{Z})\Big(p \perp a_1 \Longrightarrow p \perp a_1 \Big) . \tag{19.20}$$

Since "$p \perp a_1 \Longrightarrow p \perp a_1$" is clearly true for every p and every a_1, $P(1)$ is true.

Inductive step. We have to prove $(\forall k \in \mathbb{N})(P(k) \Longrightarrow P(k+1))$.

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

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

Assume that $P(k)$ holds.

We want to prove $P(k+1)$. That is, we want to prove

(*) if $p, a_1, a_2, \ldots, a_{k+1}$ are integers such that $p \perp a_j$ for every $j \in \mathbb{N}_{k+1}$, then $p \perp \prod_{j=1}^{k+1} a_j$.

Let $p, a_1, a_2, \ldots, a_{k+1}$ be arbitrary integers.

Assume

($\Diamond$) $p \perp a_j$ for every $j \in \mathbb{N}_{k+1}$.

Then

(&) $a_1, a_2, \ldots, a_k$ are integers such that $p \perp a_j$ for every $j \in \mathbb{N}_k$.

Since we are assuming that $P(k)$ is true, we can conclude that $p \perp \prod_{j=1}^{k} a_j$.

Let $b = \prod_{j=1}^{k} a_j$.

It then follows that

$$\prod_{j=1}^{k+1} a_j = b a_{k+1}\,,$$

$$p \perp b\,,$$

and (since we are assuming ($\Diamond$)),

$$p \perp a_{k+1}\,.$$

So Theorem 65 implies that $p \perp b a_{k+1}$, i.e., that

$$p \perp \prod_{j=1}^{k+1} a_j\,. \tag{19.21}$$

We have proved (19.21) assuming ($\Diamond$).

Hence ($\Diamond$) implies (19.21).

And this has been proved for arbitrary integers $p, a_1, a_2, \ldots, a_{k+1}$.

So (*) holds. That is, $P(k+1)$ is true.

We have proved $P(k+1)$ assuming $P(k)$, so we have proved the implication $P(k) \Longrightarrow P(k+1)$.

And "$P(k) \implies P(k+1)$" has been proved for arbitrary $k \in \mathbb{N}$.

So we have proved $(\forall k \in \mathbb{N})(P(k) \implies P(k+1))$. This completes the inductive step.

It then follows from the PMI that $P(k)$ is true for all $k \in \mathbb{N}$, which is what we wanted to prove. **Q.E.D.**

19.2.10 Another proof of the generalized Euclid lemma

Theorem 61 (that is, Euclid's lemma) tells us that If p is a prime and a, b, are integers such that p is prime and p divides the product ab, then p divides a or p divides b.

The ***generalized Euclid lemma*** answers the more general question "what happens if instead of two integers a, b we have three integers a, b, c? Or four integers a, b, c, d" Or, more generally, any number n of integers.

We answered this question by proving the generalized Euclid lemma (Theorem 62). Here I am giving you another proof of Theorem 62, based on Theorem 62).

Proof of Theorem 62 using Theorem 62.

Let $p, a_1, a_2, \ldots, a_k$ be integers such that p is prime and p divides $\prod_{j=1}^{k} a_j$.

We want to prove that p divides one of the a_j.

Assume that $\boxed{p \text{ does not divide any of the } a_j}$.

Then, for each j, p is coprime with a_j. (Reason: since p is prime the only natural numbers that divide p are 1 and p. Since p does not divide a_j, the only natural number that divides both p and a_j is 1. So the greatest common divisor of p and a_j is 1. Then p is coprime with a_j.)

According to Theorem 66, it follows that p is coprime with the product $\prod_{j=1}^{k} a_j$.

But then $\boxed{p \text{ does not divide the product } \prod_{j=1}^{k} a_j}$.

But $\boxed{p \text{ divides the product } \prod_{j=1}^{k} a_j}$.

So we have reached a contradiction. And this happened because we assumed that p does not divide any of the a_j.

So p must divide one of the a_j. **Q.E.D.**

19.2.11 Divisibility of an integer by the product of several integers

Supose an integer n is divisible by three integers a, b, c. Can we conclude that n is divisible by the product abc?

What if n is divisible by four integers a, b, c, d? Can we conclude that n is divisible by the product $abcd$?

In general, let us look at the following question:

Question 10. *Suppose that*

1. *n is an integer,*
2. *k is a natural number,*
3. *$a_1, a_2, \ldots, a_k$ are integers,*
4. *n is divisible by all the a_j; that is,*

$$a_j | n \qquad \text{for each } j \in \mathbb{N}_k \,,$$

or, in more formal language,

$$(\forall j \in \mathbb{N}_k) a_j | n \,.$$

Can we conclude that the product $\prod_{j=1}^{k}$ divides n? □

For the case of two integers a_1, a_2, we know that the answer is "yes" if a_1 and a_2 are coprime. The answer for several integers $a_1, a_2, \ldots, a_k$ is similar: we have to require that $a_1, a_2, \ldots, a_k$ be ***pairwise coprime***. This means that $a_1 \perp a_2$, $a_1 \perp a_3$, $a_2 \perp a_3$, $a_1 \perp a_4$, $a_2 \perp a_4$, and so on. *Every pair a_i, a_j has to be coprime* (except of course when $i = j$; we do not want to demand, for example, that a_1 be coprime with a_1, because that would amount to requiring that a_1 be equal to 1). .

Definition 48. Let $k \in \mathbb{N}$, and let $a_1, a_2, \ldots, a_k$ be integers. We say that $a_1, a_2, \ldots, a_k$ are pairwise coprime if for every $i \in \mathbb{N}_k$ and every $j \in \mathbb{N}_k$, if $i \neq j$ then a_i and a_j are coprime. □

Theorem 67. *Assume that $n, a_1, a_2, \ldots, a_k$ are integers, k is a natural number, and*

1. *n is divisible by all the a_j; that is,*

$$a_j | n \qquad \text{for each } j \in \mathbb{N}_k \,,$$

or, in more formal language,

$$(\forall j \in \mathbb{N}_k) a_j | n \,.$$

2. *$a_1, a_2, \ldots, a_k$ are pairwise coprime, that is,*

$$a_i \perp a_j \qquad \text{whenever } i, j \in \mathbb{N}_k \,,\ i \neq j \,,$$

or, in more formal language,

$$(\forall i, j \in \mathbb{N}_k)(i \neq j \Longrightarrow a_i \perp a_j) \,.$$

Then the product $\prod_{j=1}^{k} a_j$ divides n.

Proof. We prove this by induction on k. Let $P(k)$ be the statement

($\langle\diamond\rangle$) If $n, a_1, a_2, \ldots, a_k$ are integers such that each a_j divides n, and the a_j are pairwise coprime, then the product $\prod_{j=1}^{k} a_j$ divides n,

or, in formal language

$$(\forall n, a_1, a_2, \ldots, a_k \in \mathbb{Z})$$
$$\left(\Big((\forall j \in \mathbb{N}_k) a_j | n \wedge (\forall i, j \in \mathbb{N}_k)(i \neq j \Longrightarrow a_i \perp a_j) \Big) \Longrightarrow \prod_{j=1}^{k} a_j | n \right) . \quad (19.22)$$

Remark 26. Formula (19.22) contains the variables $n, i, j, k, a_1, a_2, \ldots, a_k$. But all these variables, except k, are quantified. So k is the only open variable. Hence *(19.22) is a one-variable predicate, and the open variable is k.* That's why we can call the predicate (19.22) $P(k)$, and try to prove by induction on k that $(\forall k \in \mathbb{N}) P(k)$. □

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

Base step. We have to prove that $P(1)$ is true. But $P(1)$ says

$$(\forall n, a_1 \in \mathbb{Z})\Big(a_1|n \Longrightarrow \prod_{j=1}^{1} a_j|n\Big)\,, \tag{19.23}$$

and the inductive definition of "$\prod$" tells us that

$$\prod_{j=1}^{1} a_j = a_1\,,$$

so $P(1)$ says

$$(\forall n, a_1 \in \mathbb{Z})\Big(a_1|n \Longrightarrow a_1|n\Big)\,. \tag{19.24}$$

Since "$a_1|n \Longrightarrow a_1|n$" is clearly true for all n and all a_1, $P(1)$ us true.

Inductive step. We have to prove that $(\forall k \in \mathbb{N})(P(k) \Longrightarrow P(k+1))$.

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

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

Assume $P(k)$. That is, assume that

(*) if $a_1, a_2, \ldots, a_k$ are integers that are pairwise coprime, n is an integer, and every a_j, for $j \in \mathbb{N}_k$, divides n, then $\prod_{j=1}^{k} a_j$ divides n.

We want to prove

(**) if $a_1, a_2, \ldots, a_{k+1}$ are integers that are pairwise coprime, and every a_j, for $j \in \mathbb{N}_{k+1}$, divides an integer n, then $\prod_{j=1}^{k+1} a_j$ divides n.

In order to prove (**), let $n, a_1, a_2, \ldots, a_{k+1}$ be integers such that $a_1, a_2, \ldots, a_{k+1}$ are pairwise coprime, and $a_j|n$ for every $j \in \mathbb{N}_{k+1}$.

It then follows that

(&) $a_1, a_2, \ldots, a_k$ are integers that are pairwise coprime, and every a_j, for $j \in \mathbb{N}_k$, divides n.

Since we are assuming that $P(k)$ is true, i.e., that (*) holds, we can conclude that the product $b = \prod_{j=1}^{k} a_j$ divides n.

Then

$$\prod_{j=1}^{k+1} a_j = ba_{k+1}\,.$$

We are assuming that the a_j, for $j \in \mathbb{N}_{k+1}$, are pairwise coprime.

Hence $a_{k+1} \perp a_j$ for every $i \in \mathbb{N}_k$.

And this implies, thanks to Theorem (66), that a_{k+1} is coprime with b.

So now we know that $a_{k+1} \perp b$, $b|n$, and $a_{k+1}|n$.

Then Theorem 63 tells us that ba_{k+1} divides n, that is, that

$$\prod_{j=1}^{k+1} a_j \Big| n\,.$$

So we have proved (**), that is, $P(k+1)$, assuming $P(k)$,

Hence $\forall k \in \mathbb{N})(P(k) \Longrightarrow P(k+1))$. And this completes the inductive step. **Q**.**E**.**D**.

19.3 The fundamental theorem of arithmetic

19.3.1 Introduction to the fundamental theorem of arithmetic

The *fundamental theorem of arithmetic* (FTA) says, roughly, that

(I) Every natural number n such that $n \geq 2$ is a product of prime numbers.

(II) The expression of n as a product of prime numbers is unique.

Statement (I) is an *existence* result: it says that

(E) For every $n \in \mathbb{N}$ such that $n \geq 2$ there exists a list

$$L = (p_1, p_2, \ldots, p_k)$$

such that $p_1, p_2, \ldots, p_k$ are prime numbers, and

$$n = \prod_{j=}^{k} p_j \,. \tag{19.25}$$

And we have already proved this, in Theorem 59.

The second half of the FTA is Statement (II), the *uniqueness* assertion: the list L such that (19.25) holds is unique.

We now have to prove (II). But before we do that, we have to make it precise. One possible meaning of (II) would be this:

(II_1) If $n \in \mathbb{N}$ and $n \geq 2$, then, if

$$L = (p_1, p_2, \ldots, p_k)$$

and

$$M = (q_1, q_2, \ldots, q_m)$$

are two lists of prime numbers such that

$$n = \prod_{j=1}^{k} p_j \quad \text{and} \quad n = \prod_{i=1}^{m} q_i \,, \tag{19.26}$$

then $L = M$. (That means "$m = k$, and $q_j = p_j$ for every $j \in \mathbb{N}_k$" , that is, $q_1 = p_1$, $q_2 = p_2$, …, $q_k = p_k$.)

But it is easy to see that statement (II_1) cannot be true.

Example 32. Let $n = 6$, $p_1 = 2$, $p_2 = 3$, $q_1 = 3$, $q_2 = 2$. Then

$$6 = 2 \times 3 \text{ and } 6 = 3 \times 2\,,$$

so that

$$6 = p_1 p_2 \text{ and } 6 = q_1 q_2\,,$$

but it is not true that $p_1 = q_1$ and $p_2 = q_2$. □

In this example, it is clear what is really going on: ***it is not necessarily true that*** $p_1 = q_1$ ***and*** $p_2 = q_2$***. It could be the case that*** $p_1 = q_2$ ***and*** $p_2 = q_1$**.** In other words, "the p_js have to be the same as the q_js, but not necessarily in the same order".

How can we say this precisely? Let us try a second option:

(II_2) If $n \in \mathbb{N}$ and $n \geq 2$, then, if

$$L = (p_1, p_2, \ldots, p_k)$$

and

$$M = (q_1, q_2, \ldots, q_m)$$

are two lists of prime numbers such that

$$n = \prod_{j=1}^{k} p_j \quad \text{and} \quad n = \prod_{j=1}^{m} q_j\,, \tag{19.27}$$

then $m = k$ and the set P whose members are the p_j; that is, the set

$$P = \{p \in \mathbb{N} : (\exists j \in \mathbb{N}_k) p = p_j\}\,, \tag{19.28}$$

is the same as the set Q whose members are the q_j, that is, the set

$$Q = \{q \in \mathbb{N} : (\exists j \in \mathbb{N}_m) q = q_j\}\,. \tag{19.29}$$

But it is easy to see that this cannot be the right formulation either.

Example 33. Let

$$n = 72\,, \text{ that is } n = 2 \times 2 \times 2 \times 3 \times 3\,. \tag{19.30}$$

Then Formula (19.30) gives us a factorization of n as product of primes, namely,

$$n = p_1 p_2 p_3 p_4 p_5\,, \quad \text{where } p_1 = 2\,,\ p_2 = 2\,,\ p_3 = 2\,,\ p_4 = 3\,,\ p_5 = 3\,.$$

We would like to say that, if we have any other factorization

$$n = q_1 q_2 \cdots q_m\,,$$

then the q_js must be "the same" as the p_js, meaning first of all, that $m = 5$, and second, that three of the q_js must be equal to 2, and two of the q_js must be equal to 3.

And just saying that the set of the p_j is the same as the set of the q_j is not enough. The set P defined by Equation (19.28) is just the set $\{2, 3\}$, i.e., the set whose members are 2 and 3. (Remember that, for a set P, an object p is a member of P or is not a member of P; there is no such thing as "being a member of P twice", or "being a member of P three times".)

We want the q_js to be "the same" as the p_js not just in the set sense (that is, the set Q is also the set $\{2, 3\}$), but in the much stronger sense that "there are five q_js; three of them are 2s and two of them are 3s". And Formulation (II_2) does not capture that. □

So, how shall we say what we want to say? Let us go back to our examples.

Example 34. For the factorization

$$6 = p_1 p_2 \text{ where } p_1 = 2 \text{ and } p_2 = 3\,,$$

we want to say that if $q_1, q_2, \cdots, q_m$ are primes and $6 = q_1 q_2 \cdots q_m$, then

- m must be 2, so the equation "$6 = q_1 q_2 \cdots q_m$"becomes "$6 = q_1 q_2$".
- q_1 must be 2 and q_2 must be 3.

We can achieve this if we limit ourselves to ***ordered factorizations*** of 6, i.e., factorizations of 6 in which 6 is expressed as a product $q_1 q_2 \cdots q_m$ of primes, but the q_j are required to be in ***increasing order***, that is, to be such that $q_1 \le q_2 \le q_3 \le \cdots \le q_m$. This excludes the factorization $6 = 3 \times 2$, and leaves $6 = 2 \times 3$ as the only possible prime factorization of 6. □

Example 35. For the factorization

$$72 = p_1p_2p_3p_4p_5 \text{ where } p_1 = 2\,,\ p_2 = 2\,,\ p_3 = 2\,,\ p_4 = 3\,,\ p_5 = 3\,,$$

we want to say that if $q_1, q_2, \cdots, q_m$ are primes and $72 = q_1q_2\cdots q_m$, then m must be 5, three of the q_j must be 2, and two of the q_j must be 3. Again, we can achieve that if we limit ourselves to ***ordered factorizations*** of 72, i.e., factorizations of 72 in which 72 is expressed as a product $q_1q_2\cdots q_m$ of primes, but the q_j are required to be in increasing order, that is, to be such that $q_1 \le q_2 \le q_3 \le \cdots \le q_m$. This excludes other factorizations such as $72 = 3\times3\times2\times2\times2$, or $72 = 3\times2\times2\times3\times2$, and leaves $72 = 2\times2\times2\times3\times3$ as the only possible prime factorization of 72. □

Examples 34 and 35 show us the path: we have to define "ordered factorization" precisely, and then the statement of the FTA will be: *every natural number n such that $n \ge 2$ has a unique ordered factorization as a product of prime numbers.*

19.3.2 Precise statetement of the fundamental theorem of arithmetic

19.3.3 Is a prime factorization a set of primes?

If we are going to say that "every natural number n such that $n \ge 2$ has a unique prime factorization", then, to begin with, we have to answer the following question:

Question 11. *What do we mean, exactly, by a **prime factorization** of an integer n?* □

A prime factorization is, of course, something like "several primes that multiplied together result in n".

But such vague language will not do. We have to give a precise definition.

1. First of all, "prime factorization" is not an entity[4], like water, or politics. We can say things like

   Water is a transparent and nearly colorless chemical substance

[4]According to the Merriam-Webster dictionary, an entity is "something that has separate and distinct existence and objective or conceptual reality".

or

> Politics is the process of achieving and exercising positions of governance or organized control over a human community, particularly a state.

But we cannot say "prime factorization is ...".

2. "Prime factorization" is like "subset", or "factor", or "divisible", or "absolute value": it is a ***relational concept***, it has arguments:
   (a) You cannot say "factor is ...", because "factor", by itself, is not something that can be or not be anything.
   (b) But you can say things like "a is a factor of b".
   (c) You cannot say "divisible is ..." (or, even worse, "divisible is when ..."), because "divisible", by itself, is not something that can be or not be anything.
   (d) But you can say things like "a is divisible by b".
   (e) You cannot say "absolute value is ...", because "absolute value", by itself, is not something that can be or not be anything.
   (f) But you can talk about "the absolute value of x".
3. More precisely, "prime factorization" is a ***two-argument predicate***: we say things like "$\mathbf{P}$ is a prime factorization of n". The arguments are n and $\mathbf{P}$. And, clearly, n must be a number.
4. And we haven't yet answered the question ***what kind of a thing shall*** $\mathbf{P}$ ***be?***
5. A prime factorization $\mathbf{P}$ should be a single object, not "several things".
6. And we have seen that it is not a good idea to think of a prime factorization as a ***set*** of primes, because, for example, the factorization of 72 given by $72 = 2 \times 2 \times 2 \times 3 \times 3$ contains more information than the set $\{2, 3\}$. It contains the fact that 2 "occurs three times", and 3 "occurs twice".

The conclusion of all this is that *a "prime factorization" should not be a* ***set****: it should be a* ***finite list****.*

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

19.3.4 Finite lists

Definition 49. Let n be a natural number.

1. A finite list of length n consists of the specification, for each natural number j in the set $\mathbb{N}_n$, of an object a_j.

2. The a_j are called the entries of the list:

   (a) a_1 is the first entry,

   (b) a_2 is the second entry,

   (c) a_3 is the third entry,

   and so on, so that, for example, a_{283} is the 283rd entry.

3. The entries a_j of a finite list L could be numbers of any kind (integers, real numbers, complex numbers), or points, or lines, or planes, or sets, or functions, or lists, or matrices, or planets, or animals, or people, or books, or viruses, or mice, or atoms, or ghosts, or unicorns, or angels, objects of any kind whatsoever, concrete or abstract, real or imaginary.

4. Actually, the entries of a list do not all have to be objects of the same kind (whatever "kind" means). So for or example, you can perfectly well have a finite list $L = (a_1, a_2, a_3, a_4, a_5)$ in which a_1 is the number 5, a_2 is Mickey Mouse, a_3 is Abraham Lincoln, a_4 is the word "cow", and a_5 is the Pacific Ocean.

Remark 27. *There are finite lists and infinite lists. In this section, we will only be talking about finite lists. But infinite lists are very important, and we will come back to them later.* □

We will use various symbols, such as capital letters or boldface lower-case letters, for lists.

And here are some examples of list creation.

Example 36. Suppose, for example, that we want to create a list of length 3, whose entries are the first three prime numbers, and we want to call it $\mathbf{a}$. We could write

$$\text{Let} \quad \mathbf{a} = (2, 3, 5)\,, \tag{19.31}$$

or we could write

$$\text{Let} \quad \mathbf{a} = (a_1, a_2, a_3)\,, \ \text{ where } \ a_1 = 2,\ a_2 = 3,\ a_3 = 5\,. \tag{19.32}$$

Example 37. Now suppose we want to write the list of all the presidents of the U.S., in chronological order, from George Washington to Donald Trump. and we want to call it **a**.

We could write something like (19.31) or (19.32). But there are several problems with this:

1. It is going to be a very long list.
2. We may not remember, for example, the name of the 13th president, so we cannot write the definition of **a** using the same style as in (19.31) or (19.32).

But we can write

$$\text{Let } \mathbf{a}=(a_j)_{j=1}^{45}, \text{ where, for } j\in\mathbb{N}_{45}, \ a_j \text{ is the } j-\text{th U.S. president.} \quad (19.33)$$

And, even if we do not know that there have been exactly 45 U.S. presidents from George Washington to Donald Trump, we can still write

Let

$$\mathbf{a} = (a_j)_{j=1}^{N}\,, \qquad (19.34)$$

where

(1) N is the number of U.S. presidents from G. Washington to D.J.Trump,

(2) for $j \in \mathbb{N}_N$, a_j is the j-th U.S. president.

Example 38. Suppose we want to introduce the list of the first 500 prime numbers and give it a name. We could write

Let

$$\mathbf{p} = (p_j)_{j=1}^{500}$$

where, for $j \in \mathbb{N}_{500}$, p_j is the j-th prime number.

Example 39. Suppose we want to introduce the list of all the U.S. presidents from George Washington to Donald Trump, in *backward chronological order*, that is, starting from D. J. Trump and going backwards all the way to G. Washington.

We could do this by writing

$$\text{Let } \mathbf{a} = (a_{46-j})_{j=1}^{45}\,, \text{ where, for } j \in \mathbb{N}_{45}\,, \ a_j \text{ is the } j-\text{th president}\,. \quad \square$$

Remark 28. Often, one writes

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

or

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

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

Remark 29. Pay attention to the following:

1. Sets have ***members***, not entries.
2. Finite lists have ***entries***, not members.
3. In the set notation, we use ***braces***, as in "the set $\{x \in \mathbb{R} : x > 0\}$", or "the set $\{1, 2, 3, 4\}$".
4. In the finite list notation, we use ***parentheses***, as in "the list $(p_j)_{j=1}^n$", or "the list $(2, 3, 5)$".
5. In a set S, an object a either is a member or is not a member. There is no such thing as "being a member of the set S twice".
6. In a finite list $L = (a_j)_{j=1}^n$ it is possible for an object a to be the first entry of L (that is $a = a_1$) and also the second entry (that is, $a = a_2$) and the 25th entry (that is, $a = a_{25}$).
7. So ***a finite list can have repeated entries***, but ***a set cannot have repeated members***.

and to the following:

8. If L is a finite list, then we can associate to L a set $\mathrm{Set}(L)$, called the ***set of entries*** of the list.

9. The set of entries of the list $L = (a_j)_{j=1}^n$ is the set $\mathrm{Set}(L)$ given by

$$\boxed{\mathrm{Set}(L) = \{x : (\exists j \in \mathbb{N}_n) x = a_j\}\,.}$$

This set is a totally different object from the list L.

Remark 30. Not all books and journals use the same notation. So if you are reading a mathematics book or article you have to make sure to check which notations are being used. 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, so we write "the list $(2, 2, 3, 4)$", or "the list $\mathbf{p} = (p_j)_{j=1}^n$", which are very different from "the set $\{2, 2, 3, 4\}$", or "the set $\{p : (\exists j \in \mathbb{N}_n) p = p_j\}$". □

19.3.5 Equality of lists

We know that two sets A, B are equal if they have the same members. That is

$$A = B \iff (\forall x)(x \in A \iff x \in B)\,.$$

When are two finite lists equal?

Here is the asnwer:

Two lists

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

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 40. The lists $\mathbf{p} = (2, 2, 3)$ and $\mathbf{q} = (3, 2, 2)$ are *not* equal because, for example, the first entry of the first list is not equal to the first entry of the second list.

But, of course, the sets $\{2, 2, 3\}$ and $\{3, 2, 2\}$ are equal, because they are both equal to the set $\{2, 3\}$. □

Example 41. Let $\mathbf{P} = (p_j)_{j=1}^{45}$ be the list of all U.S. presidents from George Washington to Donald Trump. Then, for each $j \in \mathbb{N}_{45}$, p_j stands for "the j-th president of the United States".

Then $\mathbf{P}$ has 45 entries. Let S be the associated set $\mathrm{Set}(\mathbf{P})$. Then S is the set of all U.S. presidents from George Washington to Donald Trump. That is,

$$S = \{x : (\exists j \in \mathbb{N}_{45}) x = p_j\}\,.$$

How many members does S have?

If you guessed "45", you are wrong!

The correct answer is 44.

The reason for this is that Grover Cleveland was U.S. president from 1885 to 1889, and then again from 1893 to 1897. During his first presidency, he was the 22nd president. Then Benjamin Harrison served as the 23rd president, from 1889 to 1893, and after that Grover Cleveland was elected president again, and Congress decided that he would be counted at the 24th president, in addition to being counted as the 22nd president.

So the list $\mathbf{P}$ has a repeated entry: p_{22} is the same as p_{24}. The set $\operatorname{Set}(\mathbf{P})$ does not know this, because all a set knows is whether something (or somebody) is a member or not. So the set $\operatorname{Set}(\mathbf{P})$ has only 44 members. $\square$

19.3.6 The sum, the product and the maximum and minimum of a finite list of real numbers

If $\mathbf{a}$ is a finite list of real numbers, then we can define several numbers associated to $\mathbf{a}$, using inductive definitions:.

Specifically, we will define

1. the ***sum*** $\sum \mathbf{a}$ of the entries of $\mathbf{a}$,
2. the ***product*** $\prod \mathbf{a}$ of the entries of $\mathbf{a}$,
3. the ***maximum*** $\operatorname{Max} \mathbf{a}$ of the entries of $\mathbf{a}$.
4. the ***minimum*** $\operatorname{Min} \mathbf{a}$ of the entries of $\mathbf{a}$.

In each of the cases, we start from a ***binary operation*** on $\mathbb{R}$, that is, an operation that can be performed on ***two*** real numbers, and extend it to finite lists.

The sum $\sum \mathbf{a}$ will be defined starting with the ***addition*** operation, i.e., the operation that for two real numbers x, y produces the number $x + y$.

The product $\prod \mathbf{a}$ will be defined starting with the ***multiplication*** operation, i.e., the operation that for two real numbers x, y produces the number $x \cdot y$.

The maximum $\operatorname{Max} \mathbf{a}$ will be defined starting with the ***maximum*** operation, i.e., the operation that for two real numbers x, y produces the number $\max(x, y)$ (the "maximum of a and b") defined as follows:

$$\max(x, y) = \begin{cases} x & \text{if} \quad x \geq y \\ y & \text{if} \quad y \geq x \end{cases} . \tag{19.35}$$

The minimum $\operatorname{Min} \mathbf{a}$ will be defined starting with the ***minimum*** operation, i.e., the operation that for two real numbers x, y produces the number $\min(x, y)$ (the "minimum of a and b") defined as follows:

$$\min(x, y) = \begin{cases} y & \text{if} \quad x \geq y \\ x & \text{if} \quad y \geq x \end{cases} . \tag{19.36}$$

Problem 46. *The absolute value of a real number is defined as follows: if* $x \in \mathbb{R}$*, then the* absolute value *of* x *is the number* $|x|$ *given by*

$$|x| = \begin{cases} x & \text{if} \quad x \geq 0 \\ -x & \text{if} \quad x \leq 0 \end{cases} . \tag{19.37}$$

Prove *that*

$$(\forall x \in \mathbb{R})(\forall y \in \mathbb{R}) \max(x, y) = \frac{x + y + |x - y|}{2}$$

and

$$(\forall x \in \mathbb{R})(\forall y \in \mathbb{R}) \min(x, y) = \frac{x + y - |x - y|}{2} .$$

The four operations $\sum$, $\prod$, Max, Min are defined as follows:

Definition 50. Let $\mathbf{a} = (a_j)_{j=1}^n$ be a finite list of real numbers.

1. The sum $\sum \mathbf{a}$, or $\sum_{j=1}^n a_j$, is defined inductively as follows:

$$\sum_{j=1}^{0} a_j = 0 , \tag{19.38}$$

$$\sum_{j=1}^{1} a_j = a_1 , \tag{19.39}$$

$$\sum_{j=1}^{n+1} a_j = \Big(\sum_{j=1}^{n} a_j \Big) + a_{n+1} \qquad \text{if } \ n \in \mathbb{N} . \tag{19.40}$$

2. The product $\prod \mathbf{a}$, or $\prod_{j=1}^n a_j$, is defined inductively as follows:

$$\prod_{j=1}^{0} a_j = 1 , \tag{19.41}$$

$$\prod_{j=1}^{1} a_j = a_1 , \tag{19.42}$$

$$\prod_{j=1}^{n+1} a_j = \Big(\prod_{j=1}^{n} a_j \Big) \times a_{n+1} \qquad \text{if } \ n \in \mathbb{N} , \tag{19.43}$$

$$\tag{19.44}$$

3. The <u>maximum</u> $\operatorname{Max}\mathbf{a}$, or $\operatorname{Max}_{j=1}^{n} a_j$, is defined inductively as follows:

$$\operatorname{Max}_{j=1}^{1} a_j = a_1 \,, \tag{19.45}$$

$$\operatorname{Max}_{j=1}^{n+1} a_j = \max\left(\operatorname{Max}_{j=1}^{n} a_j, a_{n+1}\right) \quad \text{if } n \in \mathbb{N} \,. \tag{19.46}$$

4. The <u>minimum</u> $\operatorname{Min}\mathbf{a}$, or $\operatorname{Min}_{j=1}^{n} a_j$, is defined inductively as follows:

$$\operatorname{Min}_{j=1}^{1} a_j = a_1 \,, \tag{19.47}$$

$$\operatorname{Min}_{j=1}^{n+1} a_j = \max\left(\operatorname{Min}_{j=1}^{n} a_j, a_{n+1}\right) \quad \text{if } n \in \mathbb{N} \,. \tag{19.48}$$

There are several facts about these operations that are fairly obvious, and whose proofs are very easy but very boring. I would urge you to practice by doing a few of these proofs, just to make sure that you can do them if you are asked to. Naturally, since the operations are defined inductively, the proofs will have to be by induction.

Before I tell you what these obvious facts are, let me define the ***concatenation*** of two lists: Roughly, the concatenation $\mathbf{a}\#\mathbf{b}$ is the list obtained by listing the entries of $\mathbf{a}$ first, and then the entries of $\mathbf{b}$.

Example 42.

1. Let

$$\mathbf{a} = (3, 6, 1, 3, 5) \,,$$
$$\mathbf{b} = (1, 0, 1, 3, 7) \,.$$

   Then

$$\mathbf{a}\#\mathbf{b} = (3, 6, 1, 3, 5, 1, 0, 1, 3, 7) \,.$$

2. Let $\mathbf{p} = (p_j)_{j=1}^{16}$ be the list of the first 16 U.S. presidents, in chronological order. Let $\mathbf{q} = (q_j)_{j=1}^{10}$ be the list in chronological order of the first 10 presidents after the 16th one, that is, the list defined by

$$q_j = \text{the } (16+j)\text{−th U.S. president for } j \in \mathbb{N}_{10} \,.$$

   (So, for example, q_1 =Andrew Johnson, q_2 =Ulysses Grant, and so on.)

   Then $\mathbf{p}\#\mathbf{q}$ is the list of the first 26 U.S. presidents, in chronological order. □

And here is the precise definition:

Definition 51. Let $\mathbf{a} = (a_j)_{j=1}^m$ and $\mathbf{b} = (b_j)_{j=1}^n$ be two finite lists. The concatenation of $\mathbf{a} = (a_j)_{j=1}^m$ and $\mathbf{b} = (b_j)_{j=1}^n$ is the finite list $\mathbf{a}\#\mathbf{b}$ given by

$$\mathbf{a}\#\mathbf{b} = (c_j)_{j=1}^{m+n}, \text{ where } c_j = \begin{cases} a_j & \text{if} \quad j \in \mathbb{N}_m \\ b_{j-m} & \text{if} \quad j \in \mathbb{N} \wedge m+1 \leq j \leq m+n \end{cases}.$$

And here are some of the obvious theorems I announced.

Theorem 68. *If* $\mathbf{a}$ *and* $\mathbf{b}$ *are finite lists of real numbers. Then:*

$$\sum(\mathbf{a}\#\mathbf{b}) = (\sum \mathbf{a}) + (\sum \mathbf{b}), \tag{19.49}$$

$$\prod(\mathbf{a}\#\mathbf{b}) = (\prod \mathbf{a}) \times (\prod \mathbf{b}), \tag{19.50}$$

$$\operatorname{Max}(\mathbf{a}\#\mathbf{b}) = \max\Big(\operatorname{Max}\mathbf{a}, \operatorname{Max}\mathbf{b}\Big), \tag{19.51}$$

$$\operatorname{Min}(\mathbf{a}\#\mathbf{b}) = \min\Big(\operatorname{Min}\mathbf{a}, \operatorname{Min}\mathbf{b}\Big). \tag{19.52}$$

Proof. **YOU PROVE THIS.**

Problem 47. ***Prove*** *Theorem 68.* □

Theorem 69. *Let* $\mathbf{a} = (a_j)_{j=1}^n$, $\mathbf{b} = (b_j)_{j=1}^n$, *be finite lists of real numbers of the same length. Then,*

1. *If*

$$(\forall j \in \mathbb{N}_n) a_j \leq b_j$$

then

$$\begin{aligned} \sum \mathbf{a} &\leq \sum \mathbf{b} \\ \operatorname{Max}\mathbf{a} &\leq \operatorname{Max}\mathbf{b} \\ \operatorname{Min}\mathbf{a} &\leq \operatorname{Min}\mathbf{b}. \end{aligned}$$

2. *If all the* a_j *and all the* b_j *are integers, and*

$$(\forall j \in \mathbb{N}_n) a_j | b_j$$

then

$$\prod \mathbf{a} \Big| \prod \mathbf{b}.$$

Proof. **YOU PROVE THIS.**

Problem 48. ***Prove*** *Theorem 69.* □

Theorem 70. *Let* $\mathbf{a} = (a_j)_{j=1}^n$ *be a finite list of real numbers. Then*

1. $\operatorname{Min} \mathbf{a} \leq a_j \leq \operatorname{Max} \mathbf{a}$ *for every* $j \in \mathbb{N}_n$.
2. *There exist indices* j_-, j_+ *in* $\mathbb{N}_n$, *such that* $\operatorname{Min} \mathbf{a} = a_{j_-}$ *and* $\operatorname{Max} \mathbf{a} = a_{j_+}$.

Proof. **YOU PROVE THIS.**

Problem 49. ***Prove*** *Theorem 69.* □

19.3.7 Prime factorizations

Definition 52. 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.)

(2) $\prod_{j=1}^m p_j = n$. □

Example 43. 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 44. The list $(3, 2, 2)$ is also a prime factorization of 12, and is different from the prime factorization $(2, 2, 3)$ of Example 43. □

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 53. A finite list $\mathbf{p} = (p_j)_{j=1}^m$ whose entries are real numbers is ordered if

(ORD) $p_j \leq p_{j+1}$ for every $j \in \mathbb{N}_{m-1}$. □

Definition 54. An ordered prime factorization of a natural number n is a prime factorization $\mathbf{p} = (p_j)_{j=1}^m$ of n which is an ordered list. □

Example 45. The list $(2, 2, 3)$ is an ordered prime factorization of 12, but the list $(3, 2, 2)$ is not. □

19.3.8 A correct (and nearly perfect) statement of the FTA

Here, finally, is a correct, nearly perfect[5] statement of the FTA:

Theorem 71. *(A nearly perfect version of the fundamental theorem of arithmetic.) Every natural number n such that $n \geq 2$ has a unique ordered prime factorization.*

19.3.9 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 $n \geq 2$ has been proved before, in the lecture notes on well-ordering (Theorem 59, on page 260).

But here we need to prove the existence of an *ordered* prime factorization. Intuitively, this is obvious, because we can take any prime factorization and rearrange the entries putting them in increasing order. More precisely: Let $n \in \mathbb{N}$ be such that $n \geq 2$. Take a prime factorization $\mathbf{p} = (p_j)_{j=1}^m$ of n. (We know that such a factorization exists. Then Rule $\exists_{use}$ enables us to pick one such factorization and call it $\mathbf{p}$.) Then reorder $\mathbf{p}$, by forming a new list $\mathbf{q} = (q_j)_{j=1}^m$ 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. ***This is not a completely rigorous proof, but the conclusion is fairly obvious, so I will omit the proof at this point. But if you really care about this, and are not satisfied with a nonrigorous proof[6], you can find the proof in subsection 19.3.11, on page 318.***

So the existence part of the FTA has been proved.

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

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

[6] If you take this issue seriously, and want to see a real proof, then I congratulate you: you are thinking like a true mathematician!

($\Diamond$) We have two finite 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 $j \in \mathbb{N}_{k-1}$, and $q_j \le q_{j+1}$ whenever $j \in \mathbb{N}_{\ell-1}$),

(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

$$(\forall k \in \mathbb{N})(\forall \ell \in \mathbb{N})(\forall \mathbf{p})(\forall \mathbf{q}) A(k, \ell, \mathbf{p}, \mathbf{q})\,, \tag{19.53}$$

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

We would like to do a proof by induction. But ***one can only do induction with respect to one natural number variable***. One cannot do induction with respect to two or more variables, or to variables that are not natural numbers, such as integers or real numbers or sets or finite lists.

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

Statement (19.53) says

$$(\forall k \in \mathbb{N})P(k)\,, \tag{19.54}$$

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 (19.53) we will prove (19.54). And, since (19.54) is of the form that lends itself to a proof by induction, we will prove (19.54) 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, $\mathbf{p} = (p_j)_{j=1}^{1}$, $\mathbf{q} = (q_j)_{j=1}^{\ell}$, and $\prod_{j=1}^{1} p_j = \prod_{j=1}^{\ell} q_j$, then $\mathbf{p} = \mathbf{q}$".

Equivalently, $P(1)$ says that "if p_1 is a prime number, $\mathbf{q} = (q_j)_{j=1}^{\ell}$ is an ordered list of primes, and $p_1 = \prod_{j=1}^{\ell} q_j$, then $\mathbf{q}$ has length one, so it consists of a single prime q_1, and $q_1 = p_1$".

But this is obviously true, because, if $\mathbf{q} = (q_j)_{j=1}^{\ell}$, and $p_1 = \prod_{j=1}^{\ell} q_j$, then ℓ must be equal to 1, because p_1 is prime, and a prime number cannot be written as a product of two or more primes[7]. And then $\prod_{j=1}^{\ell} q_j = \prod_{j=1}^{1} q_j = q_1$, so $q_1 = p_1$, and then $\mathbf{p} = \mathbf{q}$.

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

The inductive step. We have to prove that

$$(\forall k \in \mathbb{N})\Big(P(k) \Longrightarrow P(k+1)\Big)\,. \tag{19.55}$$

Let $k \in \mathbb{N}$ be arbitrary. We want to prove that $P(k) \Longrightarrow P(k+1)$.

Assume $P(k)$ is true.

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

That is, we want to prove that

(*) If

(1) $\mathbf{p} = \prod_{j=1}^{k+1} p_j$ is an ordered list of primes of length $k+1$,

(2) $\mathbf{q} = \prod_{j=1}^{\ell} q_j$ is an ordered list of primes of length ℓ,

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

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

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

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

The inductive definition of $\prod$ tells us that

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

[7]Notice that ***in this step we are using in a very crucial way the fact that*** 1 ***is not a prime number!***. If 1 was a prime number, then it would be possible to write a prime number as a product of several prime numbers. For example, we could write $3 = 3 \times 1$, or $3 = 1 \times 1 \times 1 \times 3$.

It follows that

$$p_{k+1} \Big| \prod_{j=1}^{k+1} p_j \, .$$

Since $\prod_{j=1}^{k+1} p_1 = \prod_{j=1}^{\ell} q_j$, we can conclude that

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

By the generalized Euclid lemma (i.e., Theorem 62, on page 279), 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

$$p_{k+1} \leq q_\ell \, . \tag{19.56}$$

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

$$q_\ell \leq p_{k+1} \, . \tag{19.57}$$

It then follows from (19.56) and (19.57) that

$$p_{k+1} = q_\ell \, . \tag{19.58}$$

Then

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

so

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

and then

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

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

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

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

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

$$k + 1 = \ell \,, \tag{19.59}$$

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 we now know that $\ell = k + 1$). 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

$$(\forall j \in \mathbb{N}_{k+1}) p_j = q_j \,. \tag{19.60}$$

Equations (19.59) and (19.60) 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 the implication $P(k) \Longrightarrow P(k+1)$.

Since this was proved for an arbitrary $k \in \mathbb{N}$, we have proved the universal sentence

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

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.**

19.3.10 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 $n \geq$.

Wouldn't it be nicer if we could just say

> **Theorem 72** *(The fundamental theorem of arithmetic.) Every natural number has a unique ordered prime factorization.*

?

This would clearly be more elegant, wouldn'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.

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[8].

And we can also think of the empty list as the list $(a_j)_{j=1}^{0}$, because there are no values of j such that $1 \leq j$ and $j \leq 0$, so the list $(a_j)_{j=1}^{0}$ has no entries.

Then the following is true:

Proposition 6. *The empty list is an ordered list of primes.*

This can be rigoruously proved as follows.

Proof. First, we want to prove that $\emptyset$ is a list of primes.

Write the empty liist $\emptyset$ as $(p_j)_{j=1}^{0}$.

We have to prove that

$$(\forall j)(j \in \mathbb{N}_0 \Longrightarrow p_j \text{ is a prime number}) \tag{19.61}$$

where "p_j" stands for "the j-entry of the empty list".

So let j be arbitrary. We want to prove that

$$j \in \mathbb{N}_0 \Longrightarrow p_j \text{ is a prime number}\,. \tag{19.62}$$

But $\mathbb{N}_0$ is the empty set, so $\mathbb{N}_0$ has no members, and then "$j \in \mathbb{N}_0$" is false, no matter who j might be.

Since "$j \in \mathbb{N}_0$" is false, the implication (19.62) is true.

So we have proved (19.62), for arbitrary j, And then we have proved (19.61).

We can use a similar argument to prove that $\emptyset$ is an ordered list. (Sketch of the argument: we have to prove that "if $j \in \mathbb{N}_0$ and $j + 1 \in \mathbb{N}_0$ then

[8]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 truly are the same 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 "$\emptyset$".

$p_j \le p_{j+1}$". And this is true because it is an implication with a false premise.) **Q**.**E**.**D**.

Finally, it turns out that $\boxed{\prod_{j=1}^{0} p_j = 1}$. If you have trouble believing this, I will give you three reasons:

Reason No.1: $\prod_{j=1}^{0} p_j = 1$ because in these notes we defined $\prod_{j=1}^{0} p_j$ to be equal to 1, when we gace the inductive definition of "$\prod$".

Reason No.2: $\prod_{j=1}^{0} p_j = 1$ because mathematicians have agreed that this is so. In other words, the statement "$\prod_{j=1}^{0} p_j = 1$" is ***true by convention***, because mathematicians have agreed that the product of the empty list is equal to one[9].

Reason No.3: Mathematicians are reasonable people, so if we decided that $\prod_{j=1}^{0} p_j = 1$ we must have had a good reason.

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

$$\prod_{j=1}^{n+1} p_j = \Big(\prod_{j=1}^{n} p_j\Big) p_{n+1} \tag{19.63}$$

if n is a natural number. This means that

$$\prod_{j=1}^{n} p_j = \frac{\prod_{j=1}^{n+1} p_j}{p_{n+1}} \tag{19.64}$$

for $n \in \mathbb{N}$. Now suppose we want to make Formula (19.64) also true for $n = 0$. Then we must have

$$\prod_{j=1}^{0} p_j = \frac{\prod_{j=1}^{1} p_j}{p_1}\,. \tag{19.65}$$

But

$$\prod_{j=1}^{1} p_j = p_1\,.$$

[9]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", or "tables"? Because English-speaking people have agreed that that is the name of those animals.

So we must have

$$\prod_{j=1}^{0} p_j = \frac{p_1}{p_1} = 1\,. \tag{19.66}$$

This is not a rigorous proof. But it is an argument showing that the convention that $\prod_{j=1}^{0} p_j = 1$ is a reasonable one.

In any case, ***once you agree that*** $\prod_{j=1}^{0} p_j = 1$ ***follows that our nicer version of the FTA is true.***

19.3.11 A lemma on rearranging lists of numbers.

First of all, let us introduce the notion of "equivalent lists".

Definition 55. Let $\mathbf{p} = (p_j)_{j=1}^{n}$ and $\mathbf{q} = (q_j)_{j=1}^{m}$ be finite lists. We say that $\mathbf{p}$ and $\mathbf{q}$ are equivalent (or that $\mathbf{p}$ is a rearrangement of $\mathbf{q}$, or that $\mathbf{q}$ is a rearrangement of $\mathbf{p}$) if

1. $m = n$,
2. the sets

$$\begin{aligned} \mathrm{Set}(\mathbf{p}) &= \{x : (\exists j \in \mathbb{N}_m) p_j = x\}\,, \\ \mathrm{Set}(\mathbf{q}) &= \{x : (\exists j \in \mathbb{N}_m) q_j = x\}\,, \end{aligned}$$

   are equal,
3. every member of $\mathrm{Set}(\mathbf{p})$ (i.e., of $\mathrm{Set}(\mathbf{q})$) occurs the same number of times as an entry of $\mathbf{p}$ as it does as an entry of $\mathbf{q}$. □

We will write

$$\mathbf{p} \equiv \mathbf{q}$$

to indicate that $\mathbf{p}$ is a rearrangement of $\mathbf{q}$.

(II) **Lemma 6**. *Let* $\mathbf{p} = (p_j)_{j=1}^{n}$ *be a finite list of real numbers. Then there exists a list* $\mathbf{q} = (q_j)_{j=1}^{n}$ *such that*

1. $\mathbf{q} \equiv \mathbf{p}$,
2. $\mathbf{q}$ *is ordered,*

3. $\sum_{j=1}^{n} p_j = \sum_{j=1}^{n} q_j$,

4. $\prod_{j=1}^{n} p_j = \prod_{j=1}^{n} q_j$.

Proof. We do a proof by induction.

Let $P(n)$ be the statement

> For every list $\mathbf{p} = (p_j)_{j=1}^{n}$ of length n consisting of real numbers there exists an ordered list $\mathbf{q} = (q_j)_{j=1}^{n}$ that is equivalent to $\mathbf{p}$ and satisfies $\sum_{j=1}^{n} p_j = \sum_{j=1}^{n} q_j$ and $\prod_{j=1}^{n} p_j = \prod_{j=1}^{n} q_j$.

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

The base case. $P(1)$ is obviously true, because if $\mathbf{p} = (p_j)_{j=1}^{1}$ is a list consisting of just one prime, then of course $\mathbf{p}$ is ordered, so we can take $\mathbf{q}$ to be $\mathbf{p}$, and then $\mathbf{q}$ is an ordered list and is equivalent to $\mathbf{p}$.

The inductive step. We want to prove $(\forall n \in \mathbb{N})(P(n) \implies P(n+1))$.

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

Assume that $P(n)$ is true.

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

Statement $P(n+1)$ says

$$(\forall \mathbf{p})\Bigg(\mathbf{p} = (p_j)_{j=1}^{n+1} \text{ is a list of real numbers} \implies$$
$$(\exists \mathbf{q})\Big(\mathbf{q} = (q_j)_{j=1}^{n+1} \text{ is a list of length } k+1 \wedge \mathbf{q} \text{ is ordered} \wedge$$
$$\mathbf{q} \equiv \mathbf{p} \wedge \sum_{j=1}^{n+1} p_j = \sum_{j=1}^{n+1} q_j \wedge \prod_{j=1}^{n+1} p_j = \prod_{j=1}^{n+1} q_j\Big)\Bigg).$$

To prove $P(n+1)$ we must take an arbitrary $\mathbf{p}$, assume that $\mathbf{p}$ is a list of real numbers of lenght $n+1$, and prove that there exists an ordered list $\mathbf{q}$ that is equivalent to $\mathbf{p}$ and satisfies the conditions on the sum and the product.

Let $\mathbf{p}$ be an arbitrary list of real numbers of length $n+1$.

Let $\mathbf{p} = (p_j)_{j=1}^{n+1}$.

Let j_* be an index belonging to $\mathbb{N}_{n+1}$ such that p_{j_*} has the maximum possible value of all the p_j. (That is, precisely[10], $j_* \in \mathbb{N}_{n+1}$ and $p_{j_*} = \operatorname{Max} \mathbf{p}$.)

Let $\mathbf{p}'$ be the list of length n obtained from $\mathbf{p}$ by removing the j_*-th entry. (Precisely, let $\mathbf{p}' = (p'_j)_{j=1}^{n}$ be the list defined by $p'_j = p_j$ for $j < j_*$, and $p'_j = p_{j+1}$ for $j_* \leq j \leq n$.)

Then $\mathbf{p}'$ is a list of primes of length n.

Since we are assuming that $P(n)$ holds, there exists an ordered list $\mathbf{q}' = (q'_j)_{j=1}^{n}$ such that $\mathbf{q}' \equiv \mathbf{p}'$, $\sum_{j=1}^{n} q'_j = \sum_{j=1}^{n} p'_j$, and $\prod_{j=1}^{n} q'_j = \prod_{j=1}^{n} p'_j$.

Let $\mathbf{p}''$ be the list of length $n+1$ obtained from $\mathbf{p}'$ by adding p_{j_*} as the $n+1$-th entry. (Precisely, $\mathbf{p}'' = (p''_j)_{j=1}^{n+1}$, where $p''_j = p'_j$ for $j \in \mathbb{N}$, and $p''_{n+1} = p_{j_*}$.)

Let $\mathbf{q}''$ be the list of length $n+1$ obtained from $\mathbf{q}'$ by adding p_{j_*} as the $n+1$-th entry. (Precisely, $\mathbf{q}'' = (q''_j)_{j=1}^{n+1}$, where $q''_j = q'_j$ for $j \in \mathbb{N}$, and $q''_{n+1} = p_{j_*}$.)

Since $\mathbf{q}' \equiv \mathbf{p}'$ and the lists $\mathbf{q}''$, $\mathbf{p}''$ are obtained from $\mathbf{q}'$ and $\mathbf{p}'$ by adding the same entry p_{j_*} at the end, it is clear that $\mathbf{q}'' \equiv \mathbf{p}''$.

Since $\mathbf{p}''$ is obtained from $\mathbf{p}$ by interchanging two entries (by moving p_{j_*} from the j_*-th position to the $n+1$-th position), it is clear that $\mathbf{p}'' \equiv \mathbf{p}$.

So $\mathbf{q}'' \equiv \mathbf{p}$.

Furthermore, $\mathbf{q}''$ is ordered. (Reason: $\mathbf{q}'$ is ordered, so the first n entries of $\mathbf{q}''$ satisfy $q''_1 \leq q''_2 \leq \cdots \leq q''_n$. In addition, for some $j \in \mathbb{N}_{n+1}$, $q''_n = p_j \leq p_{j_*} = q''_{n+1}$.)

[10]The existence of such a j_* is a consequence of Theorem 70. This theorem says that every finite list of real numbers has a lagest entry, which is completely obvious, but can also be proved rigorously if anyone so desires.

Finally,

$$\begin{aligned}
\sum_{j=1}^{n+1} q''_j &= (\sum_{j=1}^{n} q''_j) + q''_{n+1} \\
&= (\sum_{j=1}^{n} q'_j) + p_{j_*} \\
&= (\sum_{j=1}^{n} p'_j) + p_{j_*} \\
&= (\sum_{j=1}^{j_*-1} p'_j + \sum_{j=j_*}^{n} p'_j) + p_{j_*} \\
&= (\sum_{j=1}^{j_*-1} p_j + \sum_{j=j_*}^{n} p_{j+1}) + p_{j_*} \\
&= (\sum_{j=1}^{j_*-1} p_j + \sum_{j=j_*+1}^{n+1} p_j) + p_{j_*} \\
&= (\sum_{j=1}^{j_*-1} p_j) + p_{j_*} + (\sum_{j=j_*+1}^{n+1} p_j) \\
&= \sum_{j=1}^{n+1} p_j \,,
\end{aligned}$$

so

$$\sum_{j=1}^{n+1} q''_j = \sum_{j=1}^{n+1} p_j \,.$$

$*$ A similar argument shows that

$$\prod_{j=1}^{n+1} q''_j = \prod_{j=1}^{n+1} p_j \,.$$

So, if we take $\mathbf{q}$ to be $\mathbf{q}''$, we hvae shown that $\mathbf{q}$ satisfies all the conditions that appear in statement $P(n+1)$.

This completes the proof of $P(n+1)$, assuming $P(n)$.

Hence $P(n) \Longrightarrow P(n+1)$.

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

This completes the inductive step, and the proof of our lemma. **Q.E.D.**

19.4 Euclid's proof that there are infinitely many primes

About 2,300 years ago, the great mathematician Euclid, in his book the *Elements* (ca. 300 BCE), proved that there are infinitely many prime numbers.

19.4.1 Statement of Euclid's theorem

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

First, here is Euclid's result:

THEOREM. The set of prime numbers is infinite.

And now we discuss the proof. And, before that, we have to clarify what the statement means, by giving a precise definition of "finite set".

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

We now explain what a "finite set" is. t

Definition 56. Let S be a set,

1. We say that S is <u>finite</u> if $S = \emptyset$ or there exists a finite list $\mathbf{a} = (a_j)_{j=1}^n$ such that $S = \text{Set}(\mathbf{a})$, that is
$$S = \{x : (\exists j \in \mathbb{N}_n) x = a_j\}.$$
2. We say that S is <u>infinite</u> if it is not finite.

□

19.4.3 The proof of Euclid's Theorem

Let S be the set of all prime numbers.

We want to prove that S is an infinite set.

Suppose S is not infinite, so S is a finite set.

Let $L = (p_1, p_2, \ldots, p_n)$ be a list[11] such that S is the set $\mathrm{Set}(L)$ of entries of L. (This means that S is the set $\{x : (\exists j \in \mathbb{N}_n) x = p_j\}$.)

Let $M = \prod_{j=1}^{n} p_j$ (so M is the product of all the entries of the list L.)

Let $N = M + 1$.

Then N is a product of primes, by the Fundamental Theorem of Arithmetic, so N has a prime factor.

Pick a prime number which is a factor of N, and call it q.

We will show that the prime number q is not on the list L.

Suppose q was one of the entries of the list L.

Then we may pick j such that $j \in \mathbb{N}$, $1 \leq j \leq n$, and $q = p_j$.

Then q is a factor of the number M, because p_j is a factor of the product $p_1.p_2.\cdots.p_n$.

But q is also a factor of N.

So q is a factor of $N-M$, i.e. q is a factor of 1 (because $N-M = 1$).

But q is a prime number, so q cannot be a factor of 1.

The two previous statements contradict each other. So we have derived a contradiction.

Hence the assumption that q is one of the entries of the list L is impossible. So q is not an entry of L.

But q is a prime number.

Hence L is not a list of all the primes.

But we have assumed that L is a list of all the primes.

So we have established a contradiction. This contradiction arose from assuming that S is a finite set.

So S is an infinite set.

Q.E.D.

[11] I say "*a* list" rather than "*the* list", because you could list the primes in different ways, for example: in increasing order, or in decreasing order.