MATHEMATICS 300 — FALL 2018

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S NOTES

Contents

Part V **2**

1 The ordering of the integers **2**
- 1.1 Review of the basic facts about $\mathbb{N}$ and $\mathbb{Z}$ . . . 2
- 1.2 The definition of "$<$", "$>$", "$\leq$", and "$\geq$" . . . 3
- 1.3 Elementary facts about $<$, $>$, $\leq$, and $\geq$ . . . 3
  - 1.3.1 Unary and binary relations . . . 4
  - 1.3.2 Properties of relations . . . 7
  - 1.3.3 Properties of the relations $<$, $>$, $\leq$, and $\geq$ . . . 9
  - 1.3.4 Positive, nonnegative, negative, and nonpositive integers . . 12
- 1.4 When is the product of two integers equal to zero? . . . 13
- 1.5 The cancellation law for multiplication . . . 14
- 1.6 Two obvious but very important theorems . . . 15

2 The Well-ordering Principle **17**
- 2.1 Statement of the Well-ordering Principle . . . 17
- 2.2 Proof of the Well-Ordering Principle . . . 19
- 2.3 A simple example of a proof using well-ordering: existence of prime factors . . . 22
- 2.4 More examples of simple proofs using well-ordering . . . 23
- 2.5 An example of a proof using well-ordering; the existence part of the fundamental theorem of arithmetic . . . 25
  - 2.5.1 Clarification: What is a "product of primes"? . . . 26
  - 2.5.2 Outline of the strategy for proving the theorem . . . 27
  - 2.5.3 The proof . . . 27

3 The main theorems of elementary integer arithmetic I: the division theorem **31**
- 3.1 What is the division theorem about? . . . 31
  - 3.1.1 An example: even and odd integers . . . 33
- 3.2 Precise statement of the division theorem . . . 35

3.3 Proof of the division theorem 36
3.3.1 The existence proof 36
3.3.2 The uniqueness proof 38

4 The main theorems of elementary integer arithmetic II: the greatest common divisor and Bézout's lemma 40
4.1 The greatest common divisor of two integers 41
4.1.1 When do we use "a" and when do we use "the"? 43
4.1.2 Uniqueness of the greatest common divisor 44
4.1.3 Bézout's lemma: an example 46
4.1.4 Bézout's lemma: the statement 46
4.1.5 Bézout's lemma: the proof 47
4.2 The Euclidean Algorithm 51
4.2.1 Description of the algorithm for the computation of the greatest common divisor 52
4.2.2 Proof that the algorithm works to compute the greatest common divisor of a and b 54
4.2.3 How the algorithm can be used to express the greatest common divisor as an integer linear combination of a and b . . 54

5 The main theorems of elementary integer arithmetic III: Prime numbers and Euclid's lemma 58
5.1 The definition of "prime number" 58
5.1.1 Why isn't 1 prime? 58
5.2 Euclid's lemma: an important application of Bézout's lemma . . . 59
5.2.1 An important notational convention: the sets $\mathbb{N}_k$ 60
5.2.2 The generalized Euclid lemma 62
5.2.3 Coprime integers 65
5.2.4 Divisibility of an integer by the product of two integers . . 66
5.2.5 Coprime integers and divisibility: an extension of Euclid's lemma 67
5.2.6 Another extension of Euclid's lemma 69
5.2.7 Another extension of Euclid's lemma 70
5.2.8 Another proof of the generalized Euclid lemma 73
5.2.9 Divisibility of an integer by the product of several integers . 74

6 The main theorems of elementary integer arithmetic IV: The fundamental theorem of arithmetic 78
6.1 Introduction to the fundamental theorem of arithmetic 78
6.1.1 Precise statetement of the fundamental theorem of arithmetic 81
6.1.2 Is a prime factorization a set of primes? 81

6.2 Finite lists 83
6.2.1 How to introduce, specify, and name lists 83
6.2.2 Equality of lists 87
6.2.3 The sum, the product and the maximum and minimum of a finite list of real numbers 89
6.3 Prime factorizations 93
6.4 A correct (and nearly perfect) statement of the FTA 94
6.5 The proof 94
6.5.1 The perfect statement of the FTA 99

7 The main theorems of elementary integer arithmetic V: Euclid's proof that there are infinitely many primes 103
7.0.1 Statement of Euclid's theorem 103
7.0.2 What is a finite set? What is an infinite set? 103
7.0.3 The proof of Euclid's Theorem 103

Appendix: a lemma on rearranging lists of numbers 105

Part V

1 The ordering of the integers

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

1.1 Review of the basic facts about $\mathbb{N}$ and $\mathbb{Z}$

In section 1.6.1 of Part IV of these notes, we talked about the ***natural numbers***, and discussed how they are related to the integers.

Specifically, we listed four basic facts about $\mathbb{N}$ and how it is related to $\mathbb{Z}$. Here is the list:

BASIC FACTS ABOUT THE NATURAL NUMBERS AND THE INTEGERS

BFZ1: $\mathbb{N} \subseteq \mathbb{Z}$. (That is, every natural number is an integer.)

BFZ2: $1 \in \mathbb{N} \wedge 0 \notin \mathbb{N}$. (That is: 1 is a natural number, and 0 is not a natural number.)

BFZ3: The sum and the product of two natural numbers is a natural number. number.) That is

$$(\forall m \in \mathbb{Z})(\forall n \in \mathbb{Z})(m + n \in \mathbb{N} \wedge m.n \in \mathbb{N})\,. \tag{1.1}$$

BFZ4: Every integer is either a natural number, or minus a natural number, or zero. That is:

$$(\forall n \in \mathbb{Z})(n \in \mathbb{N} \vee n = 0 \vee -n \in \mathbb{N}) \tag{1.2}$$

1.2 The definition of "<", ">", "≤", and "≥"

It turns out that, using the natural numbers, it is very easy to define the relations "less than", "grater than", "less than or equal to" and "greater than or equal to":

Definition 1. Let m, n be integers. We say that

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

1.3 Elementary facts about <, >, ≤, and ≥

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

1.3.1 Unary and binary relations

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

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

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

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

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

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

Example 1.

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

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

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

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

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

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

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

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

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

[2] Or predicate, or property.

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

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

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

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

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

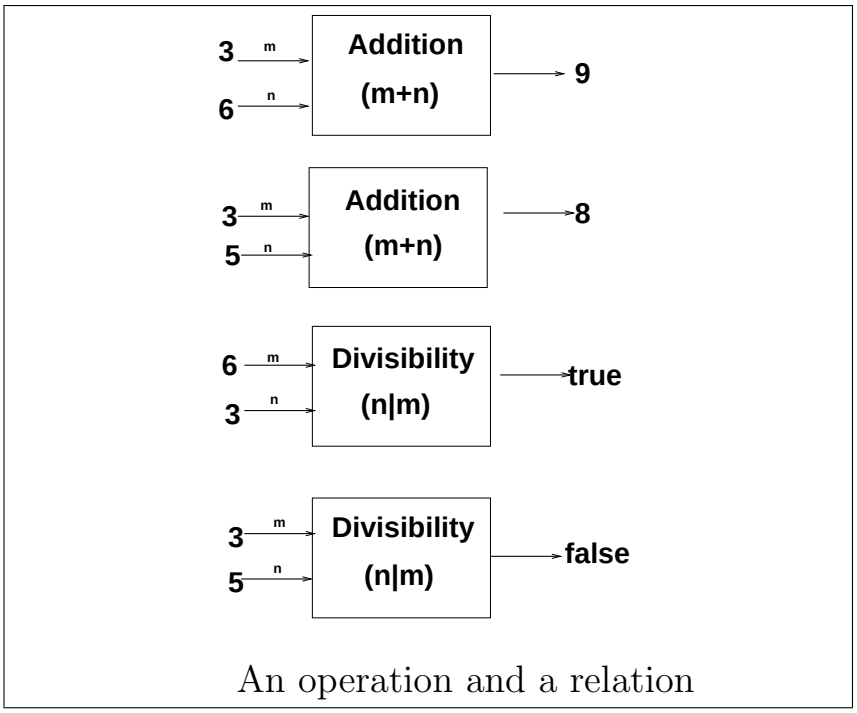
- And there are also relations "greater than" and "greater than or equal to", between integers and between real numbers.

Remark 1. You may have noticed that relations are very similar to operations. Both have arguments, and produce a value for each value of the arguments. The difference between them is that an operation produces a thing (number, set, function, giraffe, whatever) as output, and a relation or predicate produces a truth value (true or false). □

For example:

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

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



An operation and a relation

1.3.2 Properties of relations

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

In order to describe thse properties, we will use the following notation: if R is a binary relation, then the expression "xRy" will stand for the statement that x is R-related to y". For example,

- if R is the relation "$<$", i.e., "is less than", then "$x < y$" is the statement "x is less than y";
- if R is the relation "$|$", i.e., "divides", or "is a factor of", then "$x|y$" is the statement "x divides y";

- if R is the relation "=", i.e., "is equal to", then "$x = y$" is the statement "x is equal to y".

Definition 2. A binary relation R on a set S is

- reflexive if xRx for all members x of S; that is, R is reflexive if

$$(\forall x \in S)xRx\,,$$

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

$$(\forall x \in S) \sim xRx\,,$$

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

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

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

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

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

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

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

$$(\forall x \in S)(\forall y \in S)\Bigg((xRy \vee x = y \vee yRx)$$

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

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

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

Question 1. *In the explanation of what it means for a binary relation to be trichotomous, whwre I wrote the condition in formal language,* ***explain*** *why it was not necessary to include a third clause stating that*

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

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

Theorem 1. *The relations "$<$", and "$>$", on the set of integers, are irreflexive, transitive, and trichotomous.*

Translated into English, the above statement says that:

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

Proof.
We first prove that "$<$" is irreflexive. We have to show that if $n \in \mathbb{Z}$ then it cannot be tha case that $n < n$. But this is clear because "$n < n$" means "$n - n \in \mathbb{N}$", that is, "$0 \in \mathbb{N}$", but Basic Fact BFZ2 tells us that $0 \notin \mathbb{N}$.

Next, we prove that "$<$" is transitive.

Let m, n, p be arbitrary integers.

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

We want to prove that $m < p$.

It follows from Definition 1 that $n - m \in \mathbb{N}$ and $p - n \in \mathbb{N}$.

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

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

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

Therefore $m < p$.

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

We now prove the trichotomy law.

Let m, n be arbitrary integers.

Let $p = m - n$.

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

So Basic Fact BFZ4 tells us that either $p \in \mathbb{N}$, or $-p \in \mathbb{N}$, or $p = 0$.

We analyze separately the three cases, and show that

$$n < m \vee m = n \vee m < n \tag{1.3}$$

in each of the cases.

If $p \in \mathbb{N}$, then $m - n \in \mathbb{N}$, so $n < m$, and then (1.3) holds.

If $-p \in \mathbb{N}$, then $-(m - n) \in \mathbb{N}$, so $n - m \in \mathbb{N}$, so $m < n$, and (1.3) holds.

If $p = 0$, then $m - n = 0$, so $m = n$, and then (1.3) holds.

So in each of the three cases, we have proved that (1.3) is

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

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

Suppose first that $m = n \wedge m < n$ or $m = n \wedge n < m$. Then it follows that $m < m$, which we know is not true.

Now suppose that $m < n$ and $n < m$. Then $n - m \in \mathbb{N}$ and $m - n \in \mathbb{N}$, so $(m - n) + (n - m) \in \mathbb{N}$, because of Fact BFZ3. Hence $0 \in \mathbb{N}$, which we know is not true by Fact BFZ2.

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

This proves that "<" is irreflexive, transitive, and trichotomous.

A similar proof works for ">". **Q.E.D.**

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

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

Prove that

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

Problem 2. For each of the following binary relations on the given set, ***indicate*** whether the relation is reflexive, irreflexive, symmetric, antisymmetric, transitive, or trichotomous:

1. Equality (on any set S).
2. Divisibility (that is, the relation "$m|n$"), on the set $\mathbb{N}$.
3. Divisibility (that is, the relation "$m|n$"), on the set $\mathbb{Z}$.
4. "Less than or equal to", on the set $\mathbb{Z}$.
5. "<" on the set $\mathcal{F}$ of all continuous real-valued functions on the interval $[0, 1]$. (If f, g are two functions defined on $[0, 1]$, we say that $f < g$ if $f(x) < g(x)$ for every x belonging to the interval $[0, 1]$. For example, if f is the function defined by $f(x) = x^2$ for $0 \leq x \leq 1$. and g is the function defined by $g(x) = 1 + x$ for $0 \leq x \leq 1$. then $f < g$, because, if x is an arbitrary member of $[0, 1]$, then $x^2 < 1 + x$, fer the following reason: if $0 < x < 1$, then $x^2 < x$, so $x^2 < 1 + x$; if $x = 0$, then $x^2 = 0$ and $1 + x = 1$, so $x^2 < 1 + x$; if $x = 1$ then $x^2 = 1$ and $1 + x = 2$, so $x^2 < 1 + x$.) □

1.3.4 Positive, nonnegative, negative, and nonpositive integers

Definition 3. Let n be an integer. We say that n is

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

The precise meaning of "positive"

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

Theorem 2.

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

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

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

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

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

We now state the standard rules that you know for manipulating inequalities. The proofs are all very easy, and I am leaving them up to you.

Theorem 3. *Let a, b, c, d be arbitrary integers. Then **Prove** the following laws for manipulating inequalities:*

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

Proof. **YOU DO IT.**

Problem 3. ***Prove*** Theorem 3.

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

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

Theorem 4. *If a, b are integers such that $ab = 0$, then $a = 0$ or $b = 0$.*

Proof.
Let a, b be arbitrary integers.

Assume that $ab = 0$.

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

We will do a proof by contradiction .

> Assume that it is not true that $a = 0 \vee b = 0$.
>
> Then $a \neq 0$ and $b \neq 0$.
>
> Since $a \neq 0$, either $a > 0$ or $a < 0$.
>
> Similarly, either $b > 0$ or $b < 0$, because $b \neq 0$.
>
> So there are four possibilities:
>
> 1. $a > 0$ and $b > 0$.
> 2. $a > 0$ and $b < 0$.
> 3. $a < 0$ and $b > 0$.
> 4. $a < 0$ and $b < 0$.
>
> In cases 1 and 4, Theorem 2 tells us that $ab > 0$. So $ab \neq 0$.
>
> In cases 2 and 3, Theorem 2 tells us that $ab < 0$. So $ab \neq 0$.
>
> So we have proved that $ab \neq 0$ in all four cases.
>
> Hence $ab \neq 0$.
>
> But we know that $ab = 0$.
>
> So $ab \neq 0 \wedge ab = 0$, which is clearly a contradiction.

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

1.5 The cancellation law for multiplication

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

Theorem 5. *If a, b, c are arbitrary integers such that $c \neq 0$ and $ac = bc$, then it follows that $a = b$. That is,*

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})((c \neq 0 \wedge ac = bc) \Longrightarrow a = b)\,. \tag{1.4}$$

Proof.

Let a, b, c be arbitrary integers.

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

Then $ac - bc = 0$.

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

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

Then Theorem 4 tells us that $a - b = 0$ or $c = 0$.

But $c \neq 0$.

Hence $a - b = 0$.

So $a = b$.

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

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

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

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

Q.E.D.

1.6 Two obvious but very important theorems

We now state and prove two completely obvious but very important facts about the integers.

We now state and prove two completely obvious but very important facts facts about the integers. The first one is essentially a restatement of the "successor theorem', i.e., Theorem 28 in Part IV of these notes (page 56).

Theorem 6. *Every natural number is greater than or equal to* 1. *(That is:* $(\forall n \in \mathbb{N})n \geq 1$.*)*

Proof.

Let n be an arbitrary natural number.

Then either $n = 1$ or $n \neq 1$.

If $\boxed{n = 1}$ then of course $\boxed{n \geq 1}$.

If $\boxed{n \neq 1}$ then by the successor theorem $n-1$ is a natural number, and then Definition 1, $n > 1$, so $\boxed{n \geq 1}$.

So $n \geq 1$ in both cases. **Q.E.D.**

Theorem 7. *If $n \in \mathbb{Z}$ then there is no integer m such that $n < m < n + 1$.*

Proof.

Let n be an arbitrary integer.

Assume[5] that there exists an integer m such that $n < m < n + 1$.

Pick one such integer and call it m_*, so that $m_* \in \mathbb{Z}$, and $n < m_* < n + 1$.

Since $n < m_*$, $m_* - n$ is a natural number.

Hence $m_* - n \geq 1$, by Theorem 6.

Hence $\boxed{m_* \geq n + 1}$.

Since $m_* < n + 1$, and then the trichotomy law implies that $\boxed{\sim m_* \geq n + 1}$.

So we have arrived at a contradiction.

So we have proved that there does not exist an integer m such that $n < m < n + 1$. **Q.E.D.**

[5] A proof by contradiction !

2 The Well-ordering Principle

The well-ordering principle is a very simple consequence of the PMI, and is a very powerful tool for proving properties of the integers.

2.1 Statement of the Well-ordering Principle

The standard version of the well-ordering principle, the one that you will find in most textbooks, says that *every nonempty set of natural numbers has a smallest member:*

THE WELL-ORDERING PRINCIPLE (WOP) STANDARD VERSION

Theorem 8. *Every nonempty set of natural numbers has a smallest member.*

In formal language, Theorem 8 says that

$$(\forall S)\Big(\big(S \subseteq \mathbb{N} \wedge S \neq \emptyset\big) \Longrightarrow (\exists s \in S)(\forall t \in S) s \leq t\Big)\,, \tag{2.5}$$

or

$$(\forall S \in \mathcal{P}(\mathbb{N}))\Big(S \neq \emptyset \Longrightarrow (\exists s \in S)(\forall t \in S) s \leq t\Big)\,. \tag{2.6}$$

But there is a sligthly more general version that is often more useful than the standard one: instead of subsets of $\mathbb{N}$, we can consider equally well sets that are subsets of $\mathbb{Z}_{s_*}$ for some $s_* \in \mathbb{Z}$. (Recall that, if $s_* \in \mathbb{Z}$, then $\mathbb{Z}_{s_*}$ is the set of all integers n such that $n \geq s_*$. That is,

$$\mathbb{Z}_{s_*} = \{n \in \mathbb{Z} : n \geq s_*\}\,. \tag{2.7}$$

as explained earlier in these notes.) I will use the name "the well-ordering principle" (WOP) for this more general version.

In order to state the WOP, we need a couple of definitions.

Definition 4. A subset S of $\mathbb{Z}$ is bounded below if there exists an integer s_* such that $S \subseteq \mathbb{Z}_{s_*}$. □

So a set S of integers is bounded below if there is an integer s_* such that all the members of S are to the right[6] of s_*.

We also recall the definition of "smallest member" of a set:

Definition 5. A smallest member of a subset S of[7] $\mathbb{Z}$ is a member s of S such that

$$(\forall t \in S) s \leq t\,. \tag{2.8}$$

The following theorem states the obvious fact that if a set has a smallest member, then that smallest member is unique.

Trivial theorem. *If a subset S of $\mathbb{Z}$ (or of $\mathbb{R}$) has a smallest member, then it has only one smallest member.*

Proof. Let s_1, s_2 be smallest members of S. Since s_1 is a smallest member of S, $s_1 \leq t$ for every $t \in S$. In particular, since $s_2 \in S$, $s_1 \leq s_2$.

Similarly, $s_2 \leq s_1$. So $s_1 = s_2$. **Q.E.D.**

[6]Let us be precise: "to the right of" means "$\geq$"; "to the left of" means "$\leq$"; "strictly to the right of" means "$>$"; and "strictly to the left of" means "$<$".

[7]or of $\mathbb{R}$, or of any set equipped with an onder relation $\leq$

And now we are ready to state the WOP:

THE WELL-ORDERING PRINCIPLE (WOP) GENERAL VERSION

Theorem 9. *Every nonempty set of integers which is bounded below has a smallest member.*

In formal language, Theorem 9 says that

$$(\forall s_* \in \mathbb{Z})(\forall S)\Big(\big(S \subseteq \mathbb{Z}_{s_*} \wedge S \neq \emptyset\big) \Longrightarrow (\exists s \in S)(\forall t \in S) s \leq t\Big), \tag{2.9}$$

or

$$(\forall s_* \in \mathbb{Z})(\forall S \in \mathcal{P}(\mathbb{Z}_{s_*}))\Big(S \neq \emptyset \Longrightarrow (\exists s \in S)(\forall t \in S) s \leq t\Big). \tag{2.10}$$

2.2 Proof of the Well-Ordering Principle

We want to prove (2.10). So we fix an arbitrary integer s_*, and try to prove that

$$(\forall S \in \mathcal{P}(\mathbb{Z}_{s_*}))\Big(S \neq \emptyset \Longrightarrow (\exists s \in S)(\forall t \in S) s \leq t\Big). \tag{2.11}$$

We will first prove a lemma.

Lemma. *If $n \in \mathbb{Z}$, $S \subseteq \mathbb{Z}_{s_*}$ and $n \in S$, then S ha a smallest member.*

In formal language, the lemma says:

$$(\forall n \in \mathbb{Z}_{s_*})(\forall S)\left(\Big(S \subseteq \mathbb{Z}_{s_*} \wedge n \in S\Big) \Longrightarrow (\exists s \in S)(\forall t \in S) s \leq t\right). \tag{2.12}$$

Before we prove the lemma, let us show how Theorem 9 —i.e., formula (2.11— follows immediately from it.

Proof of formula (2.11) using the lemma:
Let S be a nonempty subset of $\mathbb{Z}_{s_*}$. Since $S \neq \emptyset$, we may pick a member n of S. Then $S \subseteq \mathbb{Z}_{s_*}$ and $n \in S$. So by the lemma, S has a smallest member, This proves Theorem 9.

Proof of the lemma.
We will do a proof by induction starting at s_*.

In the proof, we will write $H(S)$ for "S has a smallest member".
Let $P(n)$ be the predicate "for every subset S of $\mathbb{Z}_{s_*}$ such that $n \in S$ has a smallest member". That is, $P(n)$ stands for

$$(\forall S)\left(\Big(S \subseteq \mathbb{Z}_{s_*} \wedge n \in S\Big) \Longrightarrow H(S)\right). \tag{2.13}$$

We will prove $(\forall n \in \mathbb{Z}_{s_*})P(n)$, which is exactly formula (2.12), by induction starting with $n = s_*$.

Basis step. We have to prove $P(s_*)$. But $P(s_*)$ says "if $S \subseteq \mathbb{Z}_{s*}$ and $s_* \in S$, then $H(S)$". And this is obvious because if $s_* \in S$ and $S \subseteq \mathbb{Z}_{s_*}$, then all the members of S are $\geq s_*$, so s_* is the smallest member of S, and then $H(S)$ is true. Hence $\boxed{P(s_*)}$ holds.

Inductive srep. We have to prove

$$(\forall n \in \mathbb{Z}_{s)*}\big(P(n) \Longrightarrow P(n+1)\big). \tag{2.14}$$

Let $n \in \mathbb{Z}_{s_*}$ be arbitrary.

We want to prove the implication $P(n) \Longrightarrow P(n+1)$.

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

But $P(n+1)$ says "if S is an arbitrary subset of $\mathbb{Z}_{s*}$ such that $n+1 \in S$, then $H(S)$".

Let S be an arbitrary subset of $\mathbb{Z}_{s_*}$ such that $n+1 \in S$. We want to prove that $H(S)$.

There are two possibilities, namely, $\boxed{n \in S \text{ or } n \notin S}$.
We first consider the case when $n \in S$.

Assume $\boxed{n \in S}$.

Then, since we are assuming that $P(n)$ holds, $\boxed{H(S)}$.

So $\boxed{n \in S \Longrightarrow H(S)}$. [Rule $\forall_{prove}$]

We next consider the case when $n \notin S$.

Assume $\boxed{n \notin S}$.

Let [8] $T = S \cup \{n\}$.

[8] That is, T is the set obtained from S by adding n as a new member to S.

Then $T \subseteq \mathbb{Z}_{s_*}$, because $S \subseteq \mathbb{Z}_{s_*}$ and $n \in \mathbb{Z}_{s_*}$.
Furthermore, $n \in T$. Since we are assuming that $P(n)$ holds, and $P(n)$ says "if a subset of $\mathbb{Z}_{s_*}$ contains n, then the subset has a smallest member", it follows that $H(T)$.
Let $\bar{t}$ be the smallest member of T. Then

$$\bar{t} \in T \wedge (\forall t \in T)\bar{t} \leq t\,. \tag{2.15}$$

In particular, since $S \subseteq T$, (2.15) implies

$$(\forall t \in S)\bar{t} \leq t\,, \tag{2.16}$$

So $\bar{t}$ is less than or equal to every member of S.
If $\boxed{\bar{t} \in S}$, then $\bar{t}$ is the smallest member of S, so $\boxed{H(S)}$.
If $\boxed{\bar{t} \notin S}$, then $\bar{t} = n$, because $T = S \cup \{n\}$ and $\bar{t} \in T$.
Furthermore, every member t of S satisfies $t \geq \bar{t}$, by (2.15).
So, if $t \in S$ then $t \geq \bar{t}$, i.e., $t \geq n$, but t cannot be equal to n, because $t \in S$ and $n \notin S$ (since $n = \bar{t}$ and $\bar{t} \notin S$). Hence $t > n$, and then $t \geq n + 1$.
So we have proved that every member t of S satisfies $t \geq n+1$. Since $n + 1 \in S$, it follows that $n + 1$ is the smallest member of S, so $\boxed{H(S)}$.
Since we have shown that $H(S)$ both when $\bar{t} \in S$ and when $\bar{t} \notin S$, we have proved $\boxed{\boxed{H(S)}}$.

Since we have proved $H(S)$ assuming $n \notin S$, we can conclude that $\boxed{n \notin S \Longrightarrow H(S)}$.

Since we have proved $\boxed{n \in S \Longrightarrow H(S)}$ and $\boxed{n \notin S \Longrightarrow H(S)}$, it follows that $\boxed{H(S)}$.

So we have proved $H(S)$ for an arbitrary subset S of $\mathbb{Z}_{s_*}$ such that $n + 1 \in S$. And this proves that $\boxed{P(n + 1)}$ holds.

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

And, since we proved that $P(n) \Longrightarrow P(n+1)$ for arbitrary $n \in \mathbb{Z}_{s_*}$, it follows that

$$(\forall n \in \mathbb{Z}_{s)*}\big(P(n) \Longrightarrow P(n + 1)\big)\,. \tag{2.17}$$

which is exactly (2.14).

This completes the inductive step. Since we have also carried out the basic step, the PMI enables us to conclude that

$$(\forall n \in \mathbb{Z}_{s)*} P(n)\,, \tag{2.18}$$

which is exactly the statement of the lemma.

So we have proved the lemma and, as explained above, Theorem 9 is proved.

2.3 A simple example of a proof using well-ordering: existence of prime factors

As an illustration of the power of the well-ordering pincple, let us use it to prove the following

Theorem 10. *If n is any natural number such that $n > 1$, then n has a prime factor. (That is, there exists a prime number p such that p is a factor of n, i.e., equivalently, $p|n$.)*

Idea of the proof. Let $n \in \mathbb{N}$ be arbitrary. Assume that $n > 1$. Then n has at least one nontrivial[9] natural number factor m. (Reason: n itself is one such factor.)

Let p be smallest of all the nontrivial natural number factors of n. Then p must be prime, because if p was not prime then p would have a smaller nontrivial factor q, and then q would be a nonrivlal natural number factor of n smaller than p.

And now we write this down in a more detailed fashion.

Proof.
Let n be a natural number such that $n > 1$.
Let F be the set of all natural numbers m such that $m > 1$ and m is a factor of n.
Then F is nonempty. (Proof: The number n is obviously a factor of n. And $n > 1$. So $n \in F$.)
Also, F is a subset of $\mathbb{Z}$, and F is bounded below (because $F \subseteq \mathbb{N}$).
By the well-ordering principle, F has a smallest member.
Let q be the smallest member of F.
Then q is a factor of n, and $q > 1$.
Furthermore, we claim that q is prime.

[9] "Nontrivial" means "not equal to 1".

Proof that q is prime.

Suppose q was not prime.
Then either $q=1$ or q has a natural number factor other than 1 and q.
Pick one such factor and call it r.
Then r is a factor of q, so $q=rk$ for some natural number k.
And q is a factor of n, so $n=qj$ for some natural number j.
So $n = qj = (rk)j = r(jk)$.
So r is a factor of n.
But $r < q$, because r is a factor of q and r is not q.
And $r > 1$, because r is a factor of q and r is not 1.
Since r is factor of n and $r > 1$, it follows that $r \in F$.
Since $r < q$ and $r \in F$, q is not the smallest member of F.
But q is the smallest member of F.
So we have reached a contradiction.
So q is prime.

Hence q is a prime number which is a factor of n. So n has a prime factor. Q.E.D.

2.4 More examples of simple proofs using well-ordering

Every proof that can be done by induction can also be done using well ordering. Indeed, suppose $P(n)$ is a one-variable predicate, and you can prove $P(1)$ and $(\forall n \in \mathbb{N})\big(P(n) \implies P(n+1)\big)$.

Then, instead of invoking the PMI, you could argue by well-ordering as follows. Call a natural number "bad" if $P(n)$ is not true. We want to prove that there are no bad numbers. Let B be the set of all bad natural numbers. We want to prove that B is empty. Suppose B is not empty. Then by the WOP B has a smallest member b. So b is bad but every natural number c such that $c < b$ is good (i.e., not bad). Then b cannot be 1, because $P(1)$ is true, so 1 is good. Since $b \in \mathbb{N}$ and $b \neq 1$, $b-1$ is a natural number. And $b-1$ is not bad, because b is the smallest bad natural number. So $b-1$ is good, that is, $P(b-1)$ is true. But then, since the implication $P(n) \implies P(n+1)$ is true for every $n \in \mathbb{N}$, it is true for $n = b-1$, which means that $P(b-1) \implies P(b)$ is true. Since $P(b-1)$ is true, t follows that $P(b)$ is true. So b is good, and we have derived a contradiction. Hence $B = \emptyset$.

Example 2. Let us prove using well-ordering that *if n is natural number, then $8^n - 5^n$ is divisible by* 3.

(We have already proved this by induction. I want to show that it can be done using well-ordering, and it's almost the same proof.)

Proof. We want to prove that

$$(\forall n \in \mathbb{N}) 3 | 8^n - 5^n \,. \tag{2.19}$$

Call a natural number n "bad" if 3 does not divide $8^n - 5^n$.

Ler B be the set of all bad natural numbers. We want to prove that $B = \emptyset$.

Assume that $B \neq \emptyset$.
Then, by the WOP, B has a smallest member b.
Then b is bad, so $8^b - 5^b$ is not divisible by 3.
In paericular, this means that $b \neq 1$, because $8^1 - 5^1$ is divisible by 3.
So $b - 1$ is a natural number, and $8^{b-1} - 5^{b-1}$ is divisible by 3.
So we can write

$$8^{b-1} - 5^{b-1} = 3k \,, \;\; k \in \mathbb{Z} \,.. \tag{2.20}$$

Then

$$8 \times (8^{b-1} - 5^{b-1}) = 3 \times 8k \,. \tag{2.21}$$

So

$$8^b - 8 \times 5^{b-1} = 3 \times 8k \,, \tag{2.22}$$

and then

$$8^b = 8 \times 5^{b-1} + 3 \times 8k \,, \tag{2.23}$$

But $8 = 5 + 3$, so

$$8 \times 5^{b-1} = 5 \times 5^{b-1} + 3 \times 5^{b-1} = 5^b + 3 \times 5^{b-1} \,, \tag{2.24}$$

so

$$8^b = 5^b + 3 \times 5^{b-1} + 3 \times 8k \,, \tag{2.25}$$

and then

$$8^b = 5^b + 3(5^{b-1} + 8k)\,, \tag{2.26}$$

so that

$$8^b - 5^b = 3(5^{b-1} + 8k)\,, \tag{2.27}$$

Let $j = 5^{b-1} + 8k$. Then $j \in \mathbb{Z}$ and

$$8^b - 5^b = 3j\,. \tag{2.28}$$

Hence $3|8^b - 5^b$. That is, $\boxed{b \text{ is good}}$.
But b is bad. So we have arrived at a contradiction.

The contradiction arose from assuming that B was nonemoty.

Hence B is empty, and our theorem is proved. **Q.E.D.**

2.5 An example of a proof using well-ordering; the existence part of the fundamental theorem of arithmetic

In this section we prove the existence part of the ***fundamental theorem of arithmetic (FTA).*** This theorem is one of the most important results in integer arithmetic. It says that every natural number n such that $n \geq 2$ can be written as a product of primes in a unique way. (That is, not only is the number equal to a product of primes, but there is only one way to write it as a product of primes.) We will prove a part of the FTA, namely, the assertion that if $n \in \mathbb{N}$ and $n \geq 2$ then n can be written as a product of primes.

The proof of uniqueness requires more sophisticated tools, and will be done later.

Theorem 11. *Every natural number n such that $n \geq 2$ is a product of primes.*

Before we prove the theorem, let us explain what it says.

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

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

Definition 6. A natural number n is a product of primes if there exist

1. a natural number k,

and

2. a finite list[10]

   $\mathbf{p} = (p_1, \ldots, p_k)$ of prime numbers,

such that

$$n = \prod_{i=1}^{k} p_i \,. \tag{2.29}$$

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

Definition 7. If n is a natural number, then a list $\mathbf{p} = (p_1, \ldots, p_k)$ of prime numbers such that (2.29) holds is called a prime factorization of n. □

Example 3. The following natural numbers are products of primes:

- 7 (because 7 is prime),
- 24 (because $24 = 2 \times 2 \times 2 \times 3$),
- 309 (because $309 = 3 \times 103$ and both 3 and 103 are prime).
- $3,895,207,331,689$. Here it would really take a lot of work to find the primes $p_1, p_2, \ldots, p_k$ such that $3,895,207,331,689 = \prod_{i=1}^{k} p_i$. But the theorem that we are going to prove tell us that $3,895,207,331,689$ is a product of primes. □

[10] Finite lists are defined and discussed in great detail in section 6.2 below, on page 83.

2.5.2 Outline of the strategy for proving the theorem

Call a natural number n "bad" if $n > 1$ and n is not a product of primes.

What we want is to prove is that there are no bad natural numbers.

The strategy is going to be this: we let B be the set of all bad numbers, so our goal is to prove that B is empty. For this purpose, we assume it is nonempty, and use the well-ordering Principle to conclude that it has a smallest member b. Then b is bad, and in addition b is the smallest bad natural number. But then b cannot be prime, because if it is prime then it is a product of primes, so b would not be bad. Since $b > 1$, and b is not prime, b must be a product cd of two smaller natural numbers. But then c and d cannot be bad. So c is a product $p_1 \times p_2 \times \cdots \times p_k$ of primes, and d is a product $q_1 \times q_2 \times \cdots \times q_j$ of primes. So

$$b = cd = p_1 \times p_2 \times \cdots \times p_k \times q_1 \times q_2 \times \cdots \times q_j \,.$$

But then b is a product of primes, so b is not bad. But b is bad, and we got a contradiction. Hence B is empty, and that means that there are no bad numbers.

2.5.3 The proof

Let B be the set of all natural numbers n such that $n \geq 2$ and n is not a product of primes.

We want to prove that the set B is empty. For this purpose, we assume that B is not empty and try to get a contradiction.

So assume that $B \neq \emptyset$. By the well-ordering principle, B has a smallest member b. Then $b \in B$, so

a. b is a natural number,

b. $b \geq 2$,

c. $\boxed{b \text{ is not a product of primes}}$.

And, in addition,

d. b is the smallest member of B, that is,

$$(\forall m)(m \in B \Longrightarrow m \geq b) \,.$$

Since b is not a product of primes, it follows in particular that b is not prime. (Reason: if b was prime, then b would be a product of primes according to our definition.)

Since b is not prime, there are two possibilities: either $b = 1$ or b has a factor k which is a natural number such that $k \neq 1$ and $k \neq b$.

But the fist possibility ($b = 1$) cannot arise, because $b \geq 2$.

Hence the second possibility occurs. That is, we can pick a natural number k such that k divides b, $k \neq 1$, and $k \neq b$.

Since $k|b$, we can pick an integer j such that

$$b = jk\,.$$

And then j has to be a natural number. (Reason: we know that $k \in \mathbb{N}$, so $k > 0$. If j was ≤ 0, it would follow that $kj \leq 0$. But $kj - b$ and $b > 0$.)

Then $j \neq 1$ and $j \neq b$. (Reason: j cannot be 1 because if $j = 1$ then it would folows from $b = jk$ that $k = b$, and we know that $k \neq b$. And j cannot be b because if $j = b$ then it would folows from $b = jk$ that $k = 1$, and we know that $k \neq 1$.)

Then $j < b$ and $k < b$. (Reason: $k \geq 1$, because $k \in \mathbb{N}$; so $k > 1$, because $k \neq 1$; so[11] $k \geq 2$; and then if j was $\geq b$ it would follow that $jk \geq 2j > j > b$, but $jk = b$. The proof that $k < b$ is exactly the same.)

Hence $j \notin B$ (because b is the smallest member of B, and $j < b$). And $j \geq 2$ (because $j > 1$). This means that j is a product of primes (because if j wasn't a product of primes it would be in B).

Similarly, k is a product of primes. So we can write

$$j = \prod_{i=1}^{m} p_i \qquad \text{and} \qquad k = \prod_{\ell=1}^{\mu} q_\ell\,,$$

where $m \in \mathbb{N}$, $\mu \in \mathbb{N}$, and the p_i and the q_ℓ are primes. But then

$$b = \Big(\prod_{i=1}^{m} p_i\Big) \times \Big(\prod_{\ell=1}^{\mu} q_\ell\Big)\,,$$

[11] Notice that here we are using again Theorem 47: "there is no integer between 1 and 2", so the fact that $k > 1$ implies $k \geq 2$ because if $k < 2$ then we would have $1 < k < 2$, contradicting Theorm 47.

so $\boxed{b \text{ is a product of primes}}$. (Precisely: define u_j, for $j \in \mathbb{N}$, $1 \leq j \leq m+\mu$, by the formula

$$u_j = \begin{cases} p_j & \text{if} \quad 1 \leq j \leq m \\ q_{j-m} & \text{if} \quad m+1 \leq j \leq m+\mu \end{cases} .$$

Then

$$b = \prod_{i=1}^{m+\mu} u_j \, .$$

And the u_j are prime, because each u_j is either one of the p_is or one of the q_ℓs.)

So $\boxed{b \text{ is a product of primes}}$.

But we know that $\boxed{b \text{ is not a product of primes}}$. So we got two contradictory statements.

This contradiction was derived by assuming that $B \neq \emptyset$. So $B = \emptyset$, and this proves that every natural number n such that $n \geq 2$ is a product of primes, which is our desired conclusion. **Q.E.D.**

Remark 2. The ***fundamental theorem of arithmetic (FTA)*** says that every natural number greater than 2 can be written as a product of primes in a unique way. (That is, not only is the number equal to a product of primes, but there is only one way to write it as a product of primes.) Theorem 11 is a part of the FTA, namely, the assertion that if $n \in \mathbb{N}$ and $n \geq 2$ then n can be written as a product of primes.

What we have not proved is the uniqueness of the factorization. This is much more delicate, and we will prove it later.

At this point, just notice that even
bf*defining* what "uniqueness" of the factorization of a natural number n into primes means is not a trivial question. For example, we can write the number 6 as a product of primes in this way:

$$6 = 2 \times 3 \, ,$$

but we can also write it as

$$6 = 3 \times 2 \, .$$

Are these two expressions different ways of factoring 6 as a product of primes, or are they "the same"? Obviously, they must be "the same". because if

they were different then the factorization of 6 as a product of primes would not be unique, and the FTA would not be true.

This means that we will have to be very precise, and define very carefully what "writing a number as a product of primes in a unique way" means. And this will be done later. □

3 The main theorems of elementary integer arithmetic I: the division theorem

We now study the phenomena that make the natural numbers and the integers different in crucial ways from the real numbers. The root of this difference is that the division operation on $\mathbb{N}$ and $\mathbb{Z}$ is very different from division on $\mathbb{R}$.

3.1 What is the division theorem about?

The first important fact about the integers is the ***division theorem***. It deals with an issue that you know very well, namely, what happens if you have an integer a and an integer b and you want to "divide" a by b:

1. First of all: dividing by zero is never a good idea, so we have to work with integers a and b such that $b \neq 0$.

2. Dividing a by b should amount, roughly, to finding a number q, called the "quotient of a by b", such that

$$a = bq\,. \tag{3.30}$$

3. If we were dealing with real numbers rather than integers, then it is always possible[12] to find q. The real number q that satisfies (3.30) is denoted by the expression $\frac{a}{b}$, that we read as "a over b", or "a divided by b".

4. The situation is different when we are dealing with integers rather than real numbers. In this case, it is not always possible to find an integer q for which (3.30) is satisfied *exactly*. But we can come close: we can find an integer q for which (3.30) is satisfied *approximately*.

5. Precisely, let us rewrite (3.30) as follows:

$$a = bq + r \qquad \text{and} \quad r = 0\,. \tag{3.31}$$

   Then what happens is this: we cannot satisfy (3.31), but we can satisfy

$$a = bq + r \qquad \text{and} \quad r \text{ is small}\,. \tag{3.32}$$

[12] Assuming, of course, that $b \neq 0$.

6. And the precise meaning of "small", if $b > 0$, is "$0 \leq r < b$". So what you will be satisfying (if $b > 0$) is

$$a = bq + r \qquad \text{and} \quad 0 \leq r < b\,. \tag{3.33}$$

7. The number q is called the ***quotient of the division of*** a ***by*** b, and the number r is called the ***remainder of the division of*** a ***by*** b.

8. The reason that r is called the "remainder" is very straightforward: suppose you have, say, 27 dollar bills, and you want to divide them equally among 5 people. Then the best you can do is give 5 dollars to each of the five people, and when you do that 2 dollars will "remain".

9. Notice that, if instead of 27 dollar bills you were dealing with, say, 27 gallons of water, then you would be able to divide the water equally, by giving 5.4 gallons to each of the five people. But with dollar bills you cannot do that. That's because ***dollar bills are countable***, whereas ***water is uncountable***. In other words,

   - You can talk about the ***amount*** of water in a tank, and ***amounts of water are measured in terms of real numbers***.
   - And you cannot talk about the ***number*** of water in a tank.
   - You can talk about the ***number*** of dollar bills in your wallet, and ***numbers of dollar bills are measured in terms of natural numbers***. (And if you want to consider negative amounts as well, e.g. to talk about debts, you would use ***integers***.)
   - And you cannot [13] talk about the ***amount*** of dollar bills in your wallet.
   - If you have a units of a countable quantity such as dollar bills or coins, and b persons among whom you want to divide your a units equally, then the best you can do is give q units to each of the b persons, where q is the quotient of the division of a by b, and

[13] I really mean "you shouldn't, because it's wrong". Strictly speaking, you can say anything you want, in this free counrty of ours. But there are rules of grammar, and according to those rules it is wrong to say things like "a large amount of people were at the rally", or "she has a large amount of dollar bills". But it's O.K. to ta;lk about "a large amount of money". "People", like "dollar bills", or "coins", is countable. "Water", like "money", is uncountable.

when you do that there will be a remainder of r undistributed dollar bills, where r is the remainder of the division of a by b.

- What happens if b is negative? Well, in this case you certainly cannot have $0 \leq r < b$, because if $b < 0$ this is impossible. But you can ask for a remainder r such that $0 \leq r < |b|$, where $|b|$ is the ***absolute value*** of b, that is, the number defined by

$$|x| = \begin{cases} x & \text{if} \quad x \geq 0 \\ -x & \text{if} \quad x < 0 \end{cases} . \tag{3.34}$$

- So the final condition is

$$a = bq + r \qquad \text{and} \quad 0 \leq r < |b| . \tag{3.35}$$

The division theorem says precisely that given integers a, b, there exist integers q, r such that (3.35) holds, provided, of course, that b is not equal to zero. And in addition it makes the very important and very useful assertion that q and r are ***unique***, that is, there is only one possible choice of q and r.

3.1.1 An example: even and odd integers

Example 4. Let us apply the division theorem to the case when $b = 2$. Suppose a is an integer.

What does the division theorem tell us about a?

The theorem makes two assertions, namely,

1. that the quotient and remainder exist (that's the ***existence part***),
2. that the quotient and remainder are unique (that's the ***uniqueness part***).

So let us look at each of these two parts, and see what it tells us about a.

The existence part of the theorem tells us that we can find integers q and r such that

$$a = 2q + r \text{ and } 0 \leq r < 2 .$$

Since $0 \leq r < 2$ and r is an integer, it follows that $r = 0$ or $r = 1$.

If $r = 0$ then $a = 2q$, so a is divisible by 2, that is, a is even.

If $r = 1$ then $a = 2q + 1$, so $a - 1 = 2q$, and then $a - 1$ is divisible by 2, that is, $a - 1$ is even, and, according to our definition of "odd", this implies that a is odd.

So we have shown that: either $r = 0$, in which case a is even, or $r = 1$, in which case a is odd. So ***the existence part of the division theorem tells us that*** a ***must be even or odd.***

The uniqueness part of the theorem tells us that we cannot find integers q, r such that

$$a = 2q + r \text{ and } 0 \leq r < 2\,,$$

and also find different integers q', r' such that

$$a = 2q' + r' \text{ and } 0 \leq r' < 2\,.$$

In particular, it is not possible to find integers q, q' such that

$$a = 2q \text{ and } a = 2q' + 1 \text{ (i.e., } a = 1 = 2q')\,.$$

In other words, a cannot be both even and odd. So ***the uniqueness part of the division theorem tells us that*** a ***cannot be both even and odd.***

Summarizing: ***the division theorem, for*** $b = 2$***, tells us that an integer*** a ***has to be even or odd and cannot be both even and odd.*** And this is exactly Theorem 26, that we had to work so hard to prove!

In other words: ***The division theorem (that is, Theorem 12 below) is a generalization of the theorem that says that every integer is even or odd and not both.*** □

Now that we understand what the division theorem says for $b = 2$, let us look at what it says for other values of b.

- Theorem 12 says that, when you try to divide an integer a by 2, then one and only one of two things will happen:
  1. you will be able to divide a by 2 exactly, with a remainder equal to zero, and conclude that a is even,
  2. you will not be able to divide a by 2 exactly, but you will be able to do it with a remainder equal to 1, and conclude that $a - 1$ is divisible by 2, so a is odd.
- The division theorem, applied with $b = 2$, says exactly that that evry integers is even or odd and not both.

- The division theorem, applied with $b = 3$, says that, when you try to divide an integer a by 3, then one and only one of three things will happen:

  1. you will be able to divide a by 3 exactly, with a remainder equal to zero, and conclude that a is divisible by 3,
  2. you will not be able to divide a by 3 exactly, but you will be able to do it with a remainder equal to 1, and conclude that $a = 3q+1$ for some integer q, so $a - 1$ is divisible by 3.
  3. you will not be able to divide a by 3 exactly, but you will be able to do it with a remainder equal to 2, and conclude that $a = 3q+2$ for some integer q, so $a - 2$ is divisible by 3.

- The division theorem, applied with $b = 4$, says that, when you try to divide an integer a by 4, then one and only one of four things will happen: $4|a$, $4|a-1$, $4|a-2$, $4|a-3$.

- The division theorem, applied with $b = 5$, says that, when you try to divide an integer a by 5, then one and only one of five things will happen: $5|a$, $5|a-1$, $5|a-2$, $5|a-3$, $5|a-4$.

- $\cdots$

- The division theorem, applied with $b = 29$, says that, when you try to divide an integer a by 29, then one and only one of 29 things will happen: $29|a-j$ for $j \in \mathbb{Z}$, $0 \leq j < 29$.

- $\cdots$

- The division theorem, applied with $b = 372,508$, says that, when you try to divide an integer a by $372,508$, then one and only one of $372,508$ things will happen: $372,508|a-j$ for $j \in \mathbb{Z}$, $0 \leq j < 372,508$.

3.2 Precise statement of the division theorem

And here is, finally, the division theorem:

The division theorem for integers

Theorem 12. *If a, b are integers, and $b \neq 0$, then there exist unique integers q, r such that*

$$a = bq + r \text{ and } 0 \leq r < |b| .$$

3.3 Proof of the division theorem

3.3.1 The existence proof

Let a, b be arbitrary integers such that $b \neq 0$.

We want to prove

(E) *There exist integers q, r such that*

$$a = bq + r \text{ and } 0 \leq r < |b| . \tag{3.36}$$

Let S be the set of all integers r such that $r \geq 0$ and $s = a - bq$ for some integer q. In other words,

$$S = \{s \in \mathbb{Z} : (\exists q \in \mathbb{Z}) s = a - bq\{ . \tag{3.37}$$

We prove that

(I) S has a smallest member,

(II) if r is the smallest member of S, then $0 \leq r < |b|$ and $r = a - bq$ for some $q \in \mathbb{Z}$.

Proof of (I). The well ordering principle tells us that S has a smallest member, provided we prove that

1. S is a set of integers,
2. S is bounded below,
3. S is nonempty.

The fact that S is a set of integers is obvious from the definition of S, i.e., formula (3.37).

It also follows from formula (3.37) that S is bounded below, since every member of S is ≥ 0.

Finally, S is nonempty for the following reason: take $q = -b|a|$, and let $s = a - bq$, then

$$s = a - bq = a - b(-b|a|) = a + b^2|a| \geq a + |a| \geq 0\,;$$

then $s \in S$ (because $s \in \mathbb{Z}$, $s \geq 0$, $s = a - bq$, and $q \in \mathbb{Z}$).

Since we have proved that the three conditions needed to be able to apply the WOP hold, we can apply the WOP and conclude that S has a smallest member.

Proof of (II). Let r be the smallest member of S. Then r is nonnegative, because all the members of S are nonnegative. And, since $r \in S$, we may pick $q \in \mathbb{Z}$ such that $r = a - bq$. Then $a = bq + r$ and $r \geq 0$.

Only one thing is missing, namely, proving that $r < |b|$. We prove this by contradiction.

Assume that $r \geq |b|$.

Let

$$m = \begin{cases} 1 & \text{if} \quad b > 0 \\ -1 & \text{if} \quad b < 0 \end{cases}\,.$$

Then $m \in \mathbb{Z}$ and $mb = |b|$.

Let $q' = q + m$, and let $r' = r - |b|$. Then $r' \in \mathbb{Z}$, and the assumption that $r \geq |b|$ implies that $r' \geq 0$.

Furthermore, if we let $q' = q + m$, then $q' \in \mathbb{Z}$, and

$$r' = r - |b| = r - mb = a - bq - mb = a - b(q + m) = a - bq'\,.$$

Since $r' \geq 0$, $r' = a - bq'$, and $q' \in \mathbb{Z}$, it follows that $r' \in S$.

But $r' = r - |b|$, and $b \neq 0$, so $r' < r$. Hence r is not the smallest member of S, because $r' \in S$ and $r' < r$.

So the assumption that $r \geq |b$ has led us to a contradction. Hence $r < |b|$.

So we have proved that S has a smallest member r, that $0 \leq r < |b|$, and that $a = bq + r$ for some integer q. This completes the proof of the existence of q and r.

3.3.2 The uniqueness proof

To prove thet the pair (q, r) is unique, we have to prove

(U) *If q_1, q_2, r_1, r_2 are integers such that*

$$\begin{aligned} a &= bq_1 + r_1\,, && (3.38)\\ 0 &\le r_1 < b\,, && (3.39)\\ a &= bq_2 + r_2\,, && (3.40)\\ 0 &\le r_2 < b\,,\,, && (3.41) \end{aligned}$$

then $q_1 = q_2$ and $r_1 = r_2$.

Proof of (U).

Let q_1, q_2, r_1, r_2 be integers such that (3.38), (3.39), (3.40), and (3.41) hold.

We will prove that $q_1 = q_2$ and $r_1 = r_2$.

Since $a = bq_1 + r_1$ and $a = bq_2 + r_2$, we have

$$bq_1 + r_1 = bq_2 + r_2\,,$$

so

$$b(q_2 - q_1) = r_1 - r_2\,, \tag{3.42}$$

and then

$$|b| \cdot |q_2 - q_1| = |r_1 - r_2|\,, \tag{3.43}$$

because $|xy| = |x| \cdot |y|$ for arbitrary real numbers x, y.

Since q_1 and q_2 are integers, the number $|q_1 - q_2|$ is a nonnegative integer.

We now prove[14] that $q_1 = q_2$.

> Assume that $q_1 \neq q_2$.
>
> Then the nonnegative integer $|q_1 - q_2|$ is not zero, so it is a natural number.

[14] by contradiction , naturally.

And then $|q_1 - q_2| \geq 1$, because of Theorem 6.

COMMENT: This is the only step in the proof where we use the fact the we are working with the integers. All the other would be equally valid if we were working in $\mathbb{R}$ *rather than* $\mathbb{Z}$*.*

Therefore (3.43) implies that $\boxed{|r_1 - r_2| \geq |b|}$.

So $\boxed{\text{it's not true that } |r_1 - r_2| < |b|}$.

On the other hand, $\boxed{|r_1 - r_2| < |b|}$. (Reason: Since $r_1 < |b|$ and $0 \leq r_2$, we have $-r_2 \leq 0$, so $r_1 - r_2 < |b|$. Similarly, $r_2 - r_1 < |b|$. Since one of the two numbers is $r_1 - r_2$, it follows that $|r_1 - r_2| < |b|$.)

So wee have arrived at a contradiction.

This proves that $\boxed{q_1 = q_2}$.

And then (3.43) implies that $\boxed{r_1 = r_2}$.

So we have proved (U), for arbitrary integers a, b such that $b \neq 0$.

This completes the proof of the uniqueness part of the division theorem. So our proof is complete. **Q.E.D.**

4 The main theorems of elementary integer arithmetic II: the greatest common divisor and Bézout's lemma

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.

4.1 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 3. 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[15]:

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:

[15]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 8. 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,

$$c \text{ is a common divisor of } a \text{ and } b \iff (c|a \wedge c|b)\,. \tag{4.44}$$

Definition 9. 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

$$g \text{ is a GCD of } a \text{ and } b \iff \left(g|a \wedge g|b \wedge (\forall c \in \mathbb{Z})\Big((c|a \wedge c|b) \Longrightarrow c \leq g\Big)\right). \tag{4.45}$$

4.1.1 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[16]; we say "c is *a* common divisor of a and b".
- "the", if there is only one gcd. For example:

[16] 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.

4.1.2 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 9, 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 1. *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 5.

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 2. *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.**

4.1.3 Bézout's lemma: an example

Problem 4. Suppose you have two bottles. One of the bottles has a volume of exactly 500 milliliter and the other one has a volume of 700 milliliter. In addition, you have a large container and you can pour water from the bottles to the container or from the container to the bottles.

Show how, using these two bottles, you can end up with exactly 100 milliliter of water in the container.

Solution. The greatest common divisor of 500 and 700 is 100. By Bézout's Lemma, there exist integers u, v such that

$$100 = 500u + 700v\,. \tag{4.46}$$

Integers u, v for which (4.46) holds can be oomputed, for example, using the Euclidean algorithm. We find that $u = 3$, $v = -2$ are possible values[17] of u and v. So

$$100 = (-2) \times 700 + 3 \times 500\,.$$

So we can measure exactly 100 milliliters if water as follows:

- Fill the bottle whose volume is 500 milliliters with water, and then empty the bottle by pouring its contents into the large container. Do this three times.
- You will end up with 1500 milliliters in the container.
- Now pour water from the container into the bottle whose volume is 700 milliliters, until you fill it, and then empty the bottle. Do this twice. This will remove 1400 milliliters from the large container.
- So you will end up with 100 milliliters in the container, as desired

4.1.4 Bézout's lemma: the statement

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

[17] But they are *not* the only possible values. Other values are, for example, $u = -4$, $v = 3$.

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

$$GCD(a, b) = ua + vb\,. \tag{4.47}$$

4.1.5 Bézout's lemma: the proof

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 10. 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:

$$\text{ILC}(a, b) = \{\, c \in \mathbb{Z} : (\exists u \in \mathbb{Z})(\exists v \in \mathbb{Z}) c = ua + bv \,\}\,. \tag{4.48}$$

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 13. *Let a, b be integers. Then:*

1. *If $a = 0$ and $b = 0$, then a greatest common divisor in the sense of Definition 9 does not exist.*

2. *If $a \neq 0$ or $b \neq 0$, then*

   (a) *The greatest common divisor $GCD(a, b)$ of a and b exists,*

   (b) *$GCD(a, b)$ is the smallest of all positive integers 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,

$$g|a \wedge g|b\,. \tag{4.49}$$

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

$$(\forall c \in \mathbb{Z})\Big((c|a \wedge c|b) \Longrightarrow c \leq g\Big)\,. \tag{4.50}$$

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

$$g = ua + vb\,. \tag{4.51}$$

*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

$$a = gq + r \text{ and } 0 \leq r < g\,. \tag{4.52}$$

(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

$$r \in \mathrm{ILC}(a,b)\,. \tag{4.53}$$

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, (4.52) 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 (4.50).

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.**

4.2 The Euclidean Algorithm

Bézout's Lemma says that, if a, b are integers and are not both sero, then

(a) the gratest common divisor g of a and b can be written as an integer linear combination

$$g = ua + vb \tag{4.54}$$

of a and b,

(b) g is actually the smallest positive integer linear combination of a and b.

The ***Euclidean algorithm*** is a method for computing g and finding the coefficients u, v of the expression (4.54) of g as an integer linear combination of a and b.

4.2.1 Description of the algorithm for the computation of the greatest common divisor

We are given two integers a, b, and we want to find their greatest common divisor g. And, in addition, we may also want to find an expression of g as an integer linear combination of a and b.

We first observe that the greatest common divisor of a and b is the same as the greatest common divisor of $|a|$ and $|b|$. So we might as well asume that a and b aare nonnegative.

Second, if $a = b =$, the greatest common divisor does not exist. Sp we will assume that $\neq 0$ or $b \neq 0$.

Third, if $a > 0$ and $b = 0$, then $g = a$, and an expression of g as an integer linear combination of a and b is

$$g = a \times 1 + b \times 0\,.$$

So we have the results we want and there is no need to do any computations.

Similarly, if $a = 0$ and $b > 0$, then $g = b$, and an expression of g as an integer linear combination of a and b is

$$g = a \times 0 + b \times 1\,,$$

so again there is no need to do any computations.

Finally, if a and b are equal, then $g = a$ (or $g = b$), and an expression of g as an integer linear combination of a and b is

$$g = a \times 1 + b \times 0\,,$$

so again there is no need to do any computations.

So we are going to assume from now on that the integers a, b are positive and not equal. After relabeling them, if necessary, we assume that $a > b > 0$.

Here is how the alogorithm proceeds to find the greatest common divisor of a and b:

- We compute a sequence r_0, r_1, r_2, …, r_k of positive integers as follows:
  - $r_0 = a$, $r_1 = b$, and then
  - if $r_1 \neq 0$, then we write[18]

$$r_0 = r_1 q_2 + r_2\,, \quad \text{where } \; q_2 \in \mathbb{Z}\,,\; r_2 \in \mathbb{Z}\,,\; 0 \leq r_2 < r_1$$

[18] Naturally, this is possible because of the division theorem, which not only tells us that q_2 and r_2 exist, but also guarantess that they are unique.

(that is, we divide r_0 by r_1, and let q_2 be the quotient and r_2 be the remainde of the division);

- if $r_2 \neq 0$, then we write

$$r_1 = r_2 q_3 + r_3\,, \text{ where } q_3 \in \mathbb{Z}\,,\ r_3 \in \mathbb{Z}\,,\ 0 \leq r_3 < r_2$$

(that is, we divide r_1 by r_2, and let q_3 be the quotient and r_3 be the remainder of the division);

- if $r_3 \neq 0$, then we write

$$r_2 = r_3 q_4 + r_4\,, \text{ where } q_4 \in \mathbb{Z}\,,\ r_4 \in \mathbb{Z}\,,\ 0 \leq r_4 < r_3$$

(that is, we divide r_2 by r_3, and let q_4 be the quotient and r_4 be the remained of the division);

- as so on .....
- once we have computed $r_0, r_1, \ldots, r_k$ and $q_2, \ldots, q_k$, if $r_k \neq 0$, then we write

$$r_{k-1} = r_k q_{k+1} + r_{k+1}\,, \text{ where } q_{k+1} \in \mathbb{Z}\,,\ r_{k+1} \in \mathbb{Z}\,,\ 0 \leq r_{k+1} < r_3$$

(that is, we divide r_{k-1} by r_k, and let q_{k+1} be the quotient and r_{k+1} be the remainder of the division);

- as so on .....

- the first time we get to $r_{k+1} = 0$, the process stops.

- The reason that we necessarily have to get to $r_{k+1} = 0$ at some point is this: if the process went on for ever, we would be generating numbers r_0, r_1, r_2, r_3 that are always positive and in addition are decreasing (that is, $r_0 > r_1 > r_2 > r_3 > \cdots$, and $r_j > 0$ for every j). But this is not possible because of the well-ordering principle: let S be the set whose members are all the r_j that are > 0. Then S is a nonempty set of natural numbers. By the WOP, S has a smallest member s. But then $s = r_k$ for some k. And then r_{k+1} must be zero, because if r_{k+1} was $\neq 0$ then it would be > 0, so it would be a member of S smaller than r_k, contradicting the fact that r_k is the smallest member of S.

- Then r_k is the greatest common divisor of a and b.

4.2.2 Proof that the algorithm works to compute the greatest common divisor of a and b

Since $r_{k-1} = r_k q_{k+1} + r_{k+1}$, and $r_{k+1} = 0$, we have

$$r_{k-1} = r_k q_{k+1} \,,$$

so r_k divides r_{k-1}.

Since $r_{k-2} = r_{k-1} q_k + r_k$, and r_k divides r_{k-1}, it follows that r_k divides r_{k-2} as well.

Since $r_{k-3} = r_{k-2} q_{k-1} + r_{k-1}$, and r_k divides r_{k-1}, and r_{k-2}, it follows that r_k divides r_{k-3} as well.

Continuing in this way, we show that r_k divides r_{k-1}, r_{k-2}, ..., until eventually we find that r_k divides r_0 and r_1, that is, r_k divides a and b.

So r_k is a common divisor of a and b.

Now we need to prove that r_k is the greatest common divisor of a and b. For this purpose, we have to prove that if c is any common divisor of a and b then $c \leq r_k$.

So let $c \in \mathbb{Z}$ be a common divisor of a and b. Then c divides r_0 and c divides r_1.

Since $r_0 = r_1 q_2 + r_2$, we have $r_2 = r_0 - r_1 q_1$ and, since c divides r_0 and r_1, it follows that c divides r_2.

Since $r_1 = r_2 q_3 + r_3$, we have $r_3 = r_1 - r_2 q_3$ and, since c divides r_1 and r_2, it follows that c divides r_3.

Continuing in this way, we prove that c divides r_0, r_1, r_2, r_3, r_4, and so on, until we end up proving that c divides r_k.

Since c divides r_k, it follows that $c \leq r_k$. (Proof: if $c \leq 0$ then $c \leq r_k$, because $r_k > 0$. If $c > 0$, then c and r_k are both positive integers. Since $c | r_k$, we may write $r_k = cm$, $m \in \mathbb{Z}$. But then $m > 0$, so $m \in \mathbb{N}$, and then $m \geq 1$. It follows that $r_k = mc \geq c$. So $c \leq r_k$.)

So we have proved that r_k satisfies the two conditions in the definition of "greatest common divisor of a and b": it divides both a and b, and it is $\geq c$ for every common divisor c of a and b.

Therefore r_k is the greatest common divisor of a and b. **Q.E.D.**

4.2.3 How the algorithm can be used to express the greatest common divisor as an integer linear combination of a and b

Having computed the greatest common divisor r_k of a and b, it turns out that, if we are interested, we can also use our computation to express r_k as

an integer linear combination of a and b.

The key point is this: *whenever two integers u, v are integer linear combinations of a and b, it follows that every integer w which is an integer linear combination of u and v can be expressed as an integer linear combination of a and b.*

(This how this can be done: write

$$u = ma + nb\,,\ v = pa + qb\,,\ w = ru + sv\,,\ \ m, n, p, q, r, s \in \mathbb{Z}\,.$$

Then

$$\begin{aligned} w &= ru + sv \\ &= r(ma + nb) + s(pa + qb) \\ &= rma + rnb + spa + sqb \\ &= (rm + sp)a + (rn + sq)b\,, \end{aligned}$$

so $w = (rm + sp)a + (rn + sq)b$ is the desired expression of w as an integer linear combination of a and b.)

Using this, we can successively express r_0, r_1, r_2, r_3, ..., as integer linear combinations of a and b as follows:

- r_0 and r_1 are integer linear combinations of a and b, because $r_0 = a$ and $r_1 = b$;
- r_2 is an integer linear combination of r_0 and r_1, because $r_2 = r_0 - r_1 q_1$, so r_2 is an integer linear combination of a and b,
- r_3 is an integer linear combination of r_1 and r_2, because $r_3 = r_1 - r_2 q_2$; since r_1 and r_2 are integer linear combinations of a and b, it follows that r_3 is an integer linear combination of a and b,
- r_4 is an integer linear combination of r_2 and r_3, because $r_4 = r_2 - r_3 q_4$; since r_2 and r_3 are integer linear combinations of a and b, it follows that r_4 is an integer linear combination of a and b,
- continuing in this way, we end up finding an expression for r_k as an integer linear combination of a and b.

Example 6. Let us find the greatest common divisor of a and b, if $a = 700$, $b = 500$, using the Euclidean algorithm.

We let $r_0 = 700$, $r_1 = 500$. We then divide r_0 by r_1, and find q_2, r_2 such that $r_0 = r_1 q_2 + r_2$. We get

$$700 = 500 \times 1 + 200\,,$$

so $q_2 = 1$, $r_2 = 200$.

We then divide r_1 by r_2, and find q_3, r_3 such that $r_1 = r_2 q_3 + r_3$. We get

$$500 = 200 \times 2 + 100\,,$$

so $q_3 = 2$, $r_3 = 100$.

Next, we r_2 by r_3, and find q_4, r_4 such that $r_2 = r_3 q_4 + r_4$. We get

$$200 = 100 \times 2 + 0\,,$$

so $q_4 = 2$, $r_4 = -0$.

Since $r_4 = 0$, the process stops here, and the greatest common divisor is r_3, that is, 100.

To express the greatest common divisor as an integer linear combination of 700 and 500, we successively express r_0, r_1, r_2, r_3 as integer linear combinations of 700 and 500:

$$\begin{aligned} r_0 &= 700\,, \\ r_1 &= 500\,, \\ r_2 &= r_0 - r_1 q_2 \\ &= 700 - 500\,, \\ r_3 &= r_1 - r_2 q_3 \\ &= 500 - (700 - 500) \times 2 \\ &= 3 \times 500 + (-2) \times 700\,, \end{aligned}$$

so we end up with $\boxed{100 = 3 \times 500 + (-2) \times 700}$, which is the expression of the greatest common divisor 100 as an integer lienar combination of 500 and 700 that we used in our solution of problem 4. □

Problem 5. ***Prove*** that if a, b are nonzero integers, g is the greatest common divisor of a and b, and $|a| + |b| > 2$, then g can be expressed as an integer linear combination

$$g = ua + vb\,,\ \ u \in \mathbb{Z}\,,\ v \in \mathbb{Z}\,,$$

in such a way that $|u| < |b|$ and $|v| < |a|$.

NOTE: The reason for the asumption that $|a| + |b| > 2$ is as follows. First of all, we are assuming that a and b are nonzero, and this means that $|a| \geq 1$ and $|b| \geq 1$, so $|a| + |b| \geq 2$. So all our hypothesis that $|a| + |b| > 2$ does in exclude the possibility that $|a| + |b| = 2$. If $|a| + |b| = 2$, then $|a| = 1$ and $|b| = 1$. Now, when $|a| = 1$ and $|b| = 1$, then $g = 1$, and no matter how we exprsss g as a linear combination $ua + vb$ is with integer coefficients u, v, either u or v will have to be nonzero. If $u \neq 0$, then $|u| \geq 1$, because u is an integer, so the condition "$|u| < |b|$ and $|v| < |a|$" is not satisfied, because $|b| = 1$ and $|u| \geq 1$. If $v \neq 0$, then $|v| \geq 1$, because v is an integer, so the condition "$|u| < |b|$ and $|v| < |a|$" is not satisfied in this case either, because $|a| = 1$ and $|v| \geq 1$. So in the exceptional case the conclusion that we can take u, v such that $|u| < |b|$ and $|v| < |a|$ is not true. Therefore, if we want this concusion to be true, we have to exclude the special case. $\square$

5 The main theorems of elementary integer arithmetic III: Prime numbers and Euclid's lemma

5.1 The definition of "prime number"

Definition 11. 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 12. 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 $p = jk$. □

5.1.1 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.

5.2 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 2. *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 7. 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 14. ***(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[19] that $(\sim p|a) \Longrightarrow p|b$. i.e., that if p does not divide a then p divides b.

[19]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

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

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

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

5.2.1 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.

---

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.

THE SETS $\mathbb{N}_k$ (A.K.A. $\{1, 2, \ldots, k\}$)

The expression "$\mathbb{N}_k$" stands for the set of all natural numbers that are less than or equal to k. That is,

$$\mathbb{N}_k = \{n \in \mathbb{N} : n \leq k\}\,. \tag{5.55}$$

Another notation often used for this set is "$\{1, \ldots, k\}$", or "$\{1, 2, \ldots, k\}$".
We will use "$\mathbb{N}_k$" when k is a natural number, and also when $k = 0$. (So $\mathbb{N}_k$ makes sense when $k \in \mathbb{N} \cup \{0\}$.) Naturally, for $n = 0$ the set defined by (5.55) has no members, because there are no natural numbers k such that $k \leq 0$. So

$$\mathbb{N}_0 = \emptyset\,. \tag{5.56}$$

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 $j \leq k$".

5.2.2 The generalized Euclid lemma

Theorem 14 (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 3. *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 15. *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

$$(\forall k \in \mathbb{N})(\forall p, a_1, a_2, \ldots, a_k \in \mathbb{Z}) \left(\left(p \text{ is a prime number} \wedge p \Big| \prod_{j=1}^{k} a_j \right) \Longrightarrow (\exists j \in \mathbb{N}_k) p|a_j \right). \quad (5.57)$$

Sentence (5.57) 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 (5.57) as "$(\forall k \in \mathbb{N}) P(k)$", where $P(k)$ be the sentence

$$(\forall p, a_1, a_2, \ldots, a_k \in \mathbb{Z}) \left(\left(p \text{ is a prime number} \wedge p \Big| \prod_{j=1}^{k} a_j \right) \Longrightarrow (\exists j \in \mathbb{N}_k) p|a_j \right). \quad (5.58)$$

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

$$(\forall p, a_1 \in \mathbb{Z})\left(\left(p \text{ is a prime number} \wedge p\Big|\prod_{j=1}^{1} a_j\right) \Longrightarrow (\exists j \in \mathbb{N}_1)p|a_j\right). \quad (5.59)$$

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

$$(\forall p, a_1 \in \mathbb{Z})\left(\left(p \text{ is a prime number} \wedge p|a_1\right) \Longrightarrow p|a_1\right). \quad (5.60)$$

And this is clearly true. So (5.60) is true.

Hence $P(1)$ is true.

Inductive step. We want to prove that

$$(\forall k \in \mathbb{N})(P(k) \Longrightarrow P(k+1)). \quad (5.61)$$

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

Assume that $P(k)$ is true.

Then

$$(\forall p, a_1, a_2, \ldots, a_k \in \mathbb{Z})$$
$$\left(\left(p \text{ is a prime number} \wedge p\Big|\prod_{j=1}^{k} a_j\right) \Longrightarrow (\exists j \in \mathbb{N}_k)p|a_j\right). \quad (5.62)$$

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

$$(\forall p, a_1, a_2, \ldots, a_k, a_{k+1} \in \mathbb{Z})$$
$$\left(\left(p \text{ is a prime number} \wedge p\Big|\prod_{j=1}^{k+1} a_j\right) \Longrightarrow (\exists j \in \mathbb{N}_{k+1})p|a_j\right). \quad (5.63)$$

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

This completes the inductiove step.

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

5.2.3 Coprime integers

Definition 13. 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 3. *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:

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

5.2.4 Divisibility of an integer by the product of two integers

In this section we look at the following question:

Question 4. *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 8. 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 4 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 16. *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.**

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

In this section we look at the following question:

Question 5. *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 7.

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 17. *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

$$ua + vp = 1\,. \tag{5.64}$$

Then, if we multiply both sides of (5.64) 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 17 is an extension of Euclid's lemma. To see this, let me show how, once you have Theorem 17, Euclid's lemma follows easily:

An easy derivation of Euclid's lemma from Theorem 17: 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 17 tells us that p divides b, which is exactly what we want to prove in order to prove Euclid's Lemma. **Q.E.D.**

5.2.6 Another extension of Euclid's lemma

In addition to providing an easy way to prove Euclid's lemma, Theorem 17 has another important consequence:

Theorem 18. *If a, b, p, are integers, and p is coprime with a and with b, then p is coprime with the product ab.*

Theorem 17 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 18.

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 17, 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 18 "an extension of Euclid's lemma"? The reason is, once again, that from Theorem 18 one can easily derive Euclid's lemma.

An easy derivation of Euclid's lemma from Theorem 18: 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 18 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.**

5.2.7 Another extension of Euclid's lemma

Theorem 18 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 6. *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 19. *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

$$(\forall p, a_1, a_2, \ldots, a_k \in \mathbb{Z})\Big((\forall j \in \mathbb{N}_k) p \perp a_j \Longrightarrow p \perp \prod_{j=1}^{k} a_j \Big) . \tag{5.65}$$

Remark 4. Formula (5.65) 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 *(5.65) is a one-variable predicate, and the open variable is k.* That's why we can call the predicate (5.65) $P(k)$, 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

$$(\forall p \in \mathbb{Z})(\forall a_1 \in \mathbb{Z})\Big(p \perp a_1 \Longrightarrow p \perp \prod_{j=1}^{1} a_j \Big) , \tag{5.66}$$

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

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

Therefore $P(1)$ says

$$(\forall p \in \mathbb{Z})(\forall a_1 \in \mathbb{Z})\Big(p \perp a_1 \Longrightarrow p \perp a_1 \Big) . \tag{5.67}$$

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

$$p \perp \prod_{j=1}^{k+1} a_j\,. \tag{5.68}$$

We have proved (5.68) assuming ($\Diamond$).

Hence ($\Diamond$) implies (5.68).

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.**

5.2.8 Another proof of the generalized Euclid lemma

Theorem 14 (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 15). Here I am giving you another proof of Theorem 15, based on Theorem 15).

Proof of Theorem 15 using Theorem 15.

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 19, 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.**

5.2.9 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 7. *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 14. 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 20. *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,

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

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

$$(\forall n, a_1, a_2, \ldots, a_k \in \mathbb{Z})$$
$$\left(\Big((\forall j \in \mathbb{N}_k) a_j | n \wedge (\forall i, j \in \mathbb{N}_k)(i \neq j \implies a_i \perp a_j) \Big) \implies \prod_{j=1}^{k} a_j | n \right). \quad (5.69)$$

Remark 5. Formula (5.69) 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 *(5.69) is a one-variable predicate, and the open variable is k.* That's why we can call the predicate (5.69) $P(k)$, 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

$$(\forall n, a_1 \in \mathbb{Z})\Big(a_1|n \Longrightarrow \prod_{j=1}^{1} a_j|n\Big)\,, \tag{5.70}$$

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

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

so $P(1)$ says

$$(\forall n, a_1 \in \mathbb{Z})\Big(a_1|n \Longrightarrow a_1|n\Big)\,. \tag{5.71}$$

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 (19), 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 16 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**.

6 The main theorems of elementary integer arithmetic IV: The fundamental theorem of arithmetic

6.1 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

$$n = \prod_{j=}^{k} p_j \,. \tag{6.72}$$

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 (6.72) 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

$$n = \prod_{j=1}^{k} p_j \quad \text{and} \quad n = \prod_{i=1}^{m} q_i \,, \tag{6.73}$$

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 9. 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

$$n = \prod_{j=1}^{k} p_j \quad \text{and} \quad n = \prod_{j=1}^{m} q_j\,, \tag{6.74}$$

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

$$P = \{p \in \mathbb{N} : (\exists j \in \mathbb{N}_k) p = p_j\}\,, \tag{6.75}$$

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

$$Q = \{q \in \mathbb{N} : (\exists j \in \mathbb{N}_m) q = q_j\}\,. \tag{6.76}$$

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

Example 10. Let

$$n = 72\,, \text{ that is } n = 2 \times 2 \times 2 \times 3 \times 3\,. \tag{6.77}$$

Then Formula (6.77) 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 (6.75) 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 11. 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 12. 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 $q_1 \leq q_2 \leq q_3 \leq \cdots \leq q_m$. 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 11 and 12 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 $n \geq 2$ has a unique ordered factorization as a product of prime numbers.*

6.1.1 Precise statetement of the fundamental theorem of arithmetic

6.1.2 Is a prime factorization a set of primes?

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

Question 8. *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[20], like water, or politics. We can say things like

   Water is a transparent and nearly colorless chemical substance

[20] 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.

6.2 Finite lists

In this section we will use the sets $\mathbb{N}_k$. The meaning of "$\mathbb{N}_k$" is explained in section 5.2.1, on page 60.

Definition 15. 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 $\mathbf{a}$ could be numbers of any kind (integers, real numbers, complex numbers, integers modulo 37), or matrices, or aets, orpoints, or lines, or planes, or functions, or lists, 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 "pf the same kind" means). So for or example, you can perfectly well have a finite list $\mathbf{a} = (a_1, a_2, a_3, a_4, a_5)$ 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 6. *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.* □

6.2.1 How to introduce, specify, and name lists

- In principle, any symbol or string of symbols can be used as the name of a list, so we could name a list "a", or "q", or "Alice", or "list-of-primes".

- But in these notes we will use **boldface lower-case letters** for lists.
- And often, when we use a boldface letter such as **a** or **b** or **p** or **x** for a list, we will use the same letter in *italic*, with a subscript, as the name of an entry of a list.
- So, for example, if **p** is a list, then we may write "p_1" for the first entry of **p**, "p_2" for the second entry, and, in general, "p_j" for the j-th entry.
- So, if **p** is a list of length n, then p_j will make sense for every $j \in \mathbb{N}_n$.
- We will write
$$\mathbf{a} = (a_j)_{j=1}^n \text{ or } \mathbf{a} = (a_j)_{k\in\mathbf{N}_n} \tag{6.78}$$
to indicate that **a** *is a finite list or length* n *and, for each* $j \in \mathbb{N}_n$*, the* j*-th entry of* **a** *is called* a_j*.*
- For short lists weill write (a_1), or (a_1, a_2), or (a_1, a_2, a_3), or (a_1, a_2, a_3, a_4), rather than $(a_j)_{j=1}^1$, or $(a_j)_{j=1}^2$, or $(a_j)_{j=1}^3$, or $(a_j)_{j=1}^4$.

And here are some examples of list specification:

Example 13. 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 **a**. We could write any of the following things to specify such a list:

$$\text{Let } \mathbf{a} = (2, 3, 5)\,, \tag{6.79}$$
$$\text{Let } \mathbf{a} = (a_1, a_2, a_3)\,, \text{ where } a_1 = 2,\ a_2 = 3,\ a_3 = 5\,, \tag{6.80}$$
$$\text{Let } \mathbf{a} = (a_j)_{j=1}^3\,, \text{ where } a_1 = 2,\ a_2 = 3,\ a_3 = 5\,, \tag{6.81}$$
$$\text{Let } \mathbf{a} = (a_j)_{j=1}^3\,, \text{ where } a_j \text{ is the } j\text{–th prime for } j = 1, 2, 3\,, \tag{6.82}$$
$$\text{Let } \mathbf{a} = (a_j)_{j=1}^3\,, \text{ where } a_j \text{ is the } j\text{–th prime for } j \in \mathbb{N}_3\,, \tag{6.83}$$
$$\text{Let } \mathbf{a} = (a_j)_{j=1}^3\,, \text{ where } (\forall j \in \mathbb{N}_3) a_j \text{ is the } j\text{–th prime}\,. \tag{6.84}$$

Example 14. Suppose we want to introduce the list of the first 500 prime numbers and give it a name. In this case, if we try to write something like (6.79) or (6.80) or (6.81) or (6.82) the formulas would get too long. But we can write

$$\text{Let } \mathbf{a} = (a_j)_{j=1}^{500}\,, \text{ where } a_j \text{ is the } j\text{–th prime for } j \in \mathbb{N}_{500}\,, \tag{6.85}$$
$$\text{Let } \mathbf{a} = (a_j)_{j=1}^{500}\,, \text{ where } (\forall j \in \mathbb{N}_{500}) a_j \text{ is the } j\text{–th prime}\,. \tag{6.86}$$

Example 15. Suppose we want to introduce the list of the first 500 squares of natural numbers and give it a name. In this case we can write one of the following:

$$\text{Let} \quad \mathbf{a} \;=\; (a_j)_{j=1}^{500}\,, \;\; \text{where} \;\; a_j \;\; \text{is the} \;\; j\text{–th square for} \;\; j \in \mathbb{N}_{500}\,, \tag{6.87}$$

$$\text{Let} \quad \mathbf{a} \;=\; (a_j)_{j=1}^{500}\,, \;\; \text{where} \;\; (\forall j \in \mathbb{N}_{500}) a_j \;\; \text{is the} \;\; j\text{–th square}\,, \tag{6.88}$$

but, since we have the *formula* $a_j = j^2$ for a_j, we have the additional options of writing one of the following:

$$\text{Let} \quad \mathbf{a} \;=\; (a_j)_{j=1}^{500}\,, \;\; \text{where} \;\; a_j = j^2 \;\; \text{for} \;\; j \in \mathbb{N}_{500}\,, \tag{6.89}$$

$$\text{Let} \quad \mathbf{a} \;=\; (j^2)_{j=1}^{500}\,. \tag{6.90}$$

Example 16. Suppose we want to introduce the list of all the U.S. presidents from George Washington to Donald Trump, in *chronological order*, that is, starting with George Washington and ending with Donald J. Trump.

We could do this by writing

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

Now suppose we don't know how many presidents there have been from Washington to Trump, and we don't know that Trump is the 45-th president. We could write:

$$\text{Let } \mathbf{a} = (a_j)_{j=1}^{N}\,, \;\; \text{where :}$$

(a) N is the number of U.S. presidents from G. Washington to D. Trump and

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

Example 17. Suppose we want to introduce the list of all the U.S. presidents from George Washington to Donald Trump, in *reverse chronological order*, that is, starting with George Washington and ending with Donald J. Trump.

We could do this by writing

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

Remark 7. 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 8. Pay attention to the following:

SETS VS. LISTS

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 $\mathbf{a} = (a_j)_{j=1}^n$ it is possible for an object a to be the first entry of $\mathbf{a}$ (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 $\mathbf{a}$ is a finite list, then we can associate to $\mathbf{a}$ a set $\mathrm{Set}(\mathbf{a})$, called the ***set of entries*** of the list $\mathbf{a}$

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

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

This set is a totally different object from the list $\mathbf{a}$.

Remark 9. 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 $\{p : (\exists j \in \mathbb{N}_n) p = p_j\}$". (For example: the list $(2, 2, 3, 4)$ has four entries, but the set $\{2, 2, 3, 4\}$ has three members.) □

6.2.2 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 18. 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 19. 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. $\square$

6.2.3 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:

$$\max(x, y) = \begin{cases} x & \text{if} \quad x \geq y \\ y & \text{if} \quad y \geq x \end{cases} . \tag{6.91}$$

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:

$$\min(x, y) = \begin{cases} y & \text{if} \quad x \geq y \\ x & \text{if} \quad y \geq x \end{cases} . \tag{6.92}$$

Problem 6. 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

$$|x| = \begin{cases} x & \text{if} \quad x \geq 0 \\ -x & \text{if} \quad x \leq 0 \end{cases} . \tag{6.93}$$

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 16. 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:

$$\sum_{j=1}^{0} a_j = 0 , \tag{6.94}$$

$$\sum_{j=1}^{1} a_j = a_1 , \tag{6.95}$$

$$\sum_{j=1}^{n+1} a_j = \Big(\sum_{j=1}^{n} a_j \Big) + a_{n+1} \qquad \text{if } \ n \in \mathbb{N} . \tag{6.96}$$

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

$$\prod_{j=1}^{0} a_j = 1 , \tag{6.97}$$

$$\prod_{j=1}^{1} a_j = a_1 , \tag{6.98}$$

$$\prod_{j=1}^{n+1} a_j = \Big(\prod_{j=1}^{n} a_j \Big) \times a_{n+1} \qquad \text{if } \ n \in \mathbb{N} , \tag{6.99}$$

$$\tag{6.100}$$

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

$$\operatorname{Max}_{j=1}^{1} a_j = a_1 \,, \tag{6.101}$$

$$\operatorname{Max}_{j=1}^{n+1} a_j = \max\left(\operatorname{Max}_{j=1}^{n} a_j, a_{n+1}\right) \qquad \text{if } n \in \mathbb{N} \,. \tag{6.102}$$

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

$$\operatorname{Min}_{j=1}^{1} a_j = a_1 \,, \tag{6.103}$$

$$\operatorname{Min}_{j=1}^{n+1} a_j = \max\left(\operatorname{Min}_{j=1}^{n} a_j, a_{n+1}\right) \qquad \text{if } n \in \mathbb{N} \,. \tag{6.104}$$

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 20.

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

$$\sum(\mathbf{a}\#\mathbf{b}) = (\sum \mathbf{a}) + (\sum \mathbf{b}), \tag{6.105}$$

$$\prod(\mathbf{a}\#\mathbf{b}) = (\prod \mathbf{a}) \times (\prod \mathbf{b}), \tag{6.106}$$

$$\operatorname{Max}(\mathbf{a}\#\mathbf{b}) = \max\Big(\operatorname{Max}\mathbf{a}, \operatorname{Max}\mathbf{b}\Big), \tag{6.107}$$

$$\operatorname{Min}(\mathbf{a}\#\mathbf{b}) = \min\Big(\operatorname{Min}\mathbf{a}, \operatorname{Min}\mathbf{b}\Big). \tag{6.108}$$

Proof. **YOU PROVE THIS.**

Problem 7. ***Prove*** Theorem 21. □

Theorem 22. *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 8. ***Prove*** Theorem 22. □

Theorem 23. *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 9. ***Prove*** Theorem 22. □

6.3 Prime factorizations

Definition 18. 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 21. 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 22. The list $(3, 2, 2)$ is also a prime factorization of 12, and is different from the prime factorization $(2, 2, 3)$ of Example 21. □

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 19. 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 20. 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 23. The list $(2, 2, 3)$ is an ordered prime factorization of 12, but the list $(3, 2, 2)$ is not. □

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

Here, finally, is a correct, nearly perfect[21] statement of the FTA:

Theorem 24 *(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.*

6.5 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 Theorem 11 on page 25,

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[22], you can find the proof in the Appendix, on page 105***.

So the existence part of the FTA has been proved.

[21] 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.

[22] If you take this issue seriously, and want to see a real proof, then I congratulate you: you are thinking like a true mathematician! A true matematician understands that nothing can be justified by saying "it is obvious". If it seems obvious, then either (a) it can be proved easily, or (b) maybe it is not so obvious; maybe it is not even true! Every time something seems obvious to you, you should ask yourself "how can I prove it?". And if you do not know how to prove it, then you should not say it is obvious.

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

($\Diamond$) *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

($\Diamond\Diamond$) $\mathbf{p} = \mathbf{q}$.

That is, we want to prove, assuming ($\Diamond$), that

$$k = \ell \wedge (p_j = q_j \text{ for } j = 1, 2, \dots, k)\,. \tag{6.109}$$

So from now one we assume ($\Diamond$).

First, let prove that $p_1 = q_1$. To prove this, we observe that, since

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell\,,$$

the prime number p_1 divides the product $q_1 q_2 \cdots q_\ell$. Hence, by the generalized Euclid lemma, p_1 divides one of the factors of this product, so we may pick j such that $p_1 | q_j$. Then p_1 is a factor of q_j, so $p_1 = 1$ or $p_1 = q_j$. But p_1 is prime, so[23] $p_1 \neq 1$, So $p_1 = q_j$. But $q_1 \le q_j$, so $q_1 \le p_1$.

[23] ***Notice how important it is that in the definition of "prime number" (definition 11, on page 58) we included the requirement that, for p to be prime, p has to be > 1.*** This is the step where that condition is used. As explained in section 5.1.1, or page 58, if we had decided to count 1 as a prime number, then the Fundamental Theorem of Arithmetic would not be true. What would fail is the uniqueness part. For example, we could take $k = 2$, $\ell = 3$, $p_1 = 2$, $p_2 = 3$, $q_1 = 1$, $q_2 = 2$, and $q_3 = 3$, and we would get $p_1 p_2 = q_1 q_2 q_3$, with p_1, p_2, q_1, q_2, q_3 prime, $p_1 \le p_2$, and $q_1 \le q_2 \le q_3$, but it is not true that $\ell = k$ and $p_1 = q_1$ and $p_2 = q_2$. So it is not surprising that, since the condition "$p \neq 1$" is needed for the uniqueness part of the FTA to be valid, it is precisely in the proof of the uniqueness part of the FTA that this condition is used. And the step where it is used is preciely here.

Similarly, q_1 must equal one of the p_j, and this p_j is $\geq p_1$, so $q_1 \geq p_1$.
Since $q_1 \leq p_1$ and $q_1 \geq p_1$, it folows that $\boxed{p_1 = q_1}$.
We then have, since $p_1 = q_1$,

$$\begin{aligned} p_1 p_2 \cdots p_k &= q_1 q_2 \cdots q_\ell \\ &= p_1 q_2 \cdots q_\ell \,, \end{aligned}$$

so $p_1 p_2 \cdots p_k = p_1 q_2 \cdots q_\ell$, from which it follows that

$$p_2 \cdots p_k = q_2 \cdots q_\ell \,.$$

So we find ourselves in the same situation we started with, except that now we have p_2, q_2 in the role previously played by p_1, q_1. So, repeating the same argument, we get $p_2 = q_2$ and then we can go on and repeat the argument once more and prove that $p_3 = q_3$, and so on.

However, we know that "and so on" is problematic, and the rigorous way to do an "and so on"' argument is with a proof by induction. So let us do a proof by induction.

What we have done so far is show that we can prove that $p_1 = q_1$, and then go from that to $p_2 = q_2$, then go from that to $p_3 = q_3$. So this suggests that, for our induction, we could use the predicate $P(n)$, where $P(n)$ stands for "$p_1 = q_1 \wedge p_2 = q_2 \wedge \cdots \wedge p_n = q_n$".

There is, however, a minor problem with this idea:

- $P(n)$ only makes sense for n if $p_1, p_2, \ldots, p_n$ and $q_1, q_2, \ldots, q_n$ are defined, that is, if $n \leq k$ and $n \leq \ell$.
- But to do induction we need a predicate that makes sense for every $n \in \mathbb{N}$.

So we modify the previous $P(n)$ a little bit and use instead the following choice for $P(n)$:

(*) We let $P(n)$ be the predicate

$$\text{if } \; n \leq k \; \text{ and } \; n \leq \ell \; \text{ then } \; p_j = q_j \; \text{ for } \; j = 1, 2, \ldots, n \,. \tag{6.110}$$

That is,

$$P(n) \;\; \text{stands for:} \quad (n \leq k \wedge n \leq \ell) \Longrightarrow (\forall j \in \mathbb{N}_n) p_j = q_j \,. \tag{6.111}$$

(The virtue of this precdicate is that when $n > k$ or $n > \ell$, the premise "$n \leq k \wedge n \leq \ell$)" is false, so $P(n)$ is true. and we don't need to worry about the issue whether p_n or q_n is well defined.)

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

Basis step. We want to prove $P(1)$, that is,

$$(1 \leq k \wedge 1 \leq \ell) \Longrightarrow p_1 = q_1\,. \tag{6.112}$$

But we have already proved that $p_1 = q_1$. So (6.112) is true, and we have proved $\boxed{P(1)}$.

Inductive step. We want to prove that

$$(\forall n \in \mathbb{N})\Big(P(n) \Longrightarrow P(n+1)\Big)\,. \tag{6.113}$$

Let $n \in \mathbb{N}$ be arbitrary. Assume $P(n)$.

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

$$(n+1 \leq k \wedge n+1 \leq \ell) \Longrightarrow \big(p_1 = q_1 \wedge \cdots \wedge p_{n+1} = q_{n+1}\big)\,. \tag{6.114}$$

To prove the implication (6.114) we assume the premise and try to prove the conclusion.

Assume that $\boxed{n+1 \leq k \wedge n+1 \leq \ell}$.

Then $n < k$ and $n < \ell$, so in particular $n \leq k \wedge n \leq \ell$.

Since we are assuming $P(n)$, we know that

$$(n \leq k \wedge n \leq \ell) \Longrightarrow \big(p_1 = q_1 \wedge \cdots \wedge p_n = q_n\big)\,. \tag{6.115}$$

But we know that $n \leq k \wedge n \leq \ell$, which is the premise of the implication (6.115).

Then Rule $\Longrightarrow_{use}$ (the Modus Ponens rule) allows us to go to the conclusion of (6.115), i.e.,

$$p_1 = q_1 \wedge \cdots \wedge p_n = q_n\,. \tag{6.116}$$

Since $n < k$ and $n < \ell$, the equality $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$ can be rewritten as

$$p_1 p_2 \cdots p_n p_{n+1} \cdots p_k = q_1 q_2 \cdots q_n q_{n+1} \cdots q_k q_{k+1} \cdots q_\ell\,,$$

and, since $p_j = 1$ for $j = 1, \ldots, n$, this says

$$p_1 p_2 \cdots p_n p_{n+1} \cdots p_k = p_1 p_2 \cdots p_n q_{n+1} \cdots q_k q_{k+1} \cdots q_\ell\,,$$

from which it follows that

$$p_{n+1} \cdots p_k = q_{n+1} \cdots q_k q_{k+1} \cdots q_\ell\,. \tag{6.117}$$

We then repeat the same argument used earlier to prove that $p_1 = q_1$ and conclude that $p_{n+1} = q_{n+1}$. (The prime p_{n+1} divides the product $q_{n+1} \cdots q_k q_{k+1} \cdots q_\ell$, so it is equal to one of the factors; but this factor is $\geq q_{n+1}$, so $p_{n+1} \geq q_{n+1}$; similarly, $q_{n+1} \geq p_{n+1}$; and then $p_{n+1} = q_{n+1}$.)

Since we already know that $p_j = q_j$ for $j = 1, \ldots, n$, we have proved that

$$p_1 = q_1 \wedge \cdots \wedge p_{n+1} = q_{n+1}\,, \tag{6.118}$$

Since we have proved (6.118) assuming that $n+1 \leq k \wedge n+1 \leq \ell$, we have proved that

$$(n+1 \leq k \wedge n+1 \leq \ell) \Longrightarrow \big(p_1 = q_1 \wedge \cdots \wedge p_{n+1} = q_{n+1}\big)\,. \tag{6.119}$$

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

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

Since we have proved $P(n) \Longrightarrow P(n+1)$ for arbitrary $n \in \mathbb{N}$, it follows that $\boxed{(\forall n \in \mathbb{N})\Big(P(n) \Longrightarrow P(n+1)\Big)}$.

This completes the inductive step. Since we have also proved $P(1)$, we can conclude, thanks to the PMI, that $(\forall n \in \mathbb{N})P(n)$.

End of the uniqueness proof. Now that we have proved that $P(n)$ is true for every $n \in \mathbb{N}$, we can conclude our uniqueness proof.

Let $\nu = \min(k, \ell)$, so ν is the smallest of k and ℓ.

Then $\nu \in \mathbb{N}$, so $P(\nu)$ is true.

But $P(\nu)$ says

$$\text{if } \ \nu \leq k \ \text{ and } \ \nu \leq \ell \ \text{ then } \ p_j = q_j \ \text{ for } \ j = 1, 2, \ldots, \nu\,. \tag{6.120}$$

But $\nu \leq k$ and $\nu \leq \ell$, so we can conclude that

$$p_j = q_j \ \text{ for } \ j = 1, 2, \ldots, \nu\,. \tag{6.121}$$

We are now going to prove that $\ell = k$. Suppose $\ell > k$. Then $\nu = k$, and the formula $p_1 p_2 \cdots p_k = q_q q_2 \cdots q_\ell$ can be rewritten as

$$\begin{aligned} p_1 p_2 \cdots p_k &= q_1 q_2 \cdots q_k q_{k+1} q_{k+2} \cdots q_\ell \\ &= p_1 p_2 \cdots p_k q_{k+1} q_{k+2} \cdots q_\ell\,. \end{aligned}$$

Hence

$$q_{k+1}q_{k+2}\cdots q_\ell = 1\,.$$

but this is impossible, because the product $q_{k+1}\cdots q_\ell$ is a product of at least one prime[24], so the product is > 1.

Hence it is not true that $\ell > k$. A similar argument shows that it cannot happen that $\ell < k$. So $\boxed{\ell = k}$.

Since $\ell = k$, ν equals k as well, and then formula (6.121) tells us that $\boxed{p_j = q_j \text{ for } j = 1, 2, \ldots, k}$.

Ths completes the proof. **Q.E.D.**

6.5.1 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 25.** *(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.

[24] There is at least one prime in this product because $\ell > k$.

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[25].

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 4. *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

$$(\forall j)(j \in \mathbb{N}_0 \Longrightarrow p_j \text{ is a prime number}) \tag{6.122}$$

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

So let j be arbitrary. We want to prove that

$$j \in \mathbb{N}_0 \Longrightarrow p_j \text{ is a prime number}\,. \tag{6.123}$$

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 (6.123) is true.

So we have proved (6.123), for arbitrary j, And then we have proved (6.122).

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 $p_j \leq p_{j+1}$". 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:

[25]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 "$\emptyset$".

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[26].

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

$$\prod_{j=1}^{n+1} p_j = \Big(\prod_{j=1}^{n} p_j\Big) p_{n+1} \tag{6.124}$$

if n is a natural number. This means that

$$\prod_{j=1}^{n} p_j = \frac{\prod_{j=1}^{n+1} p_j}{p_{n+1}} \tag{6.125}$$

for $n \in \mathbb{N}$. Now suppose we want to make Formula (6.125) also true for $n = 0$. Then we must have

$$\prod_{j=1}^{0} p_j = \frac{\prod_{j=1}^{1} p_j}{p_1}\,. \tag{6.126}$$

But

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

So we must have

$$\prod_{j=1}^{0} p_j = \frac{p_1}{p_1} = 1\,. \tag{6.127}$$

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.

[26]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.

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

7 The main theorems of elementary integer arithmetic V: 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.

7.0.1 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".

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

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

Definition 21. 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. □

7.0.3 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 $\mathbf{p} = (p_1, p_2, \ldots, p_n)$ be a list[27] such that S is the set $\mathrm{Set}(\mathbf{p})$ of all entries of $\mathbf{p}$. (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 $\mathbf{p}$).
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 $\mathbf{p}$.

Suppose q was one of the entries of the list $\mathbf{p}$.
Then we may pick $j \in \mathbb{N}_n$ such that $q = p_j$.
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 $N - M$. That is, $\boxed{q \text{ is a factor of } 1}$ (because $N - M = 1$).
But q is a prime number, so $\boxed{q \text{ is not be a factor of } 1}$.
So we have derived a contradiction from the assumption that q is one of the entries of the list $\mathbf{p}$.

Hence $\boxed{q \text{ is not one of the entries of the list } \mathbf{p}}$.

But $\mathbf{p}$ is supposed to be a list of all the prime neumebrs, and q is a prime number, so $\boxed{q \text{ is one of the entries of the list } \mathbf{p}}$.

So we have derived a contradiction from the assumption that S is a finite set.

So S is an infinite set. **Q.E.D.**

[27] 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.

Appendix: a lemma on rearranging lists of numbers

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

Definition 22. 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 1**. *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 having just one entry, 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

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

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[28], $j_* \in \mathbb{N}_{n+1}$ 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 $j_* \le j \le n$.)

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

[28]The existence of such a j_* is a consequence of Theorem 23. 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.

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 $q''_1 \le q''_2 \le \cdots \le q''_n$. In addition, for some $j \in \mathbb{N}_{n+1}$, $q''_n = p_j \le p_{j_*} = q''_{n+1}$.)

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 have 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.**