Math250

Lecture Notes

on

Discrete Mathematics

M. Andrew Moshier

January 2015

Version: 0.0.0 (January 13, 2015) Format: print

Contents ii

1 The Natural Numbers 1
1.1 The Basic Picture . . . 2
1.2 Narrowing the possibilities . . . 4

2 Arithmetic 7
2.1 Basic Arithmetic Operations . . . 7

3 Laws of Arithmetic 12
3.1 Basic Laws . . . 13
3.2 Inductive Proofs . . . 13

4 Lists 24
4.1 List Basics . . . 24
4.2 List Itemization . . . 32
4.3 Lists of a Particular Type . . . 33
4.4 Other Inductively Defined Collections . . . 37
4.5 Binary Trees . . . 38

5 Ordering the Natural Numbers by Addition 44
5.1 Less or Equal . . . 45
5.2 Other Forms of Induction . . . 48
5.3 Minimum and Maximum . . . 52

6 Divisibility 55
6.1 Quotients and Remainders . . . 59

7 Prime Numbers 62
7.1 Greatest Common Divisor and Least Common Multiple . . . 68

Goals

Lecture

- Present the natural numbers as comprising a structure suited to counting.
- Identify similar structures that can not properly represent counting.
- Rule out "bad" structures via postulates.

Study

- Gain facility in the course's *successor* notation, including translating between successor notation and base 10 notation.
- Commit to memory the postulates of natural numbers.
- Demonstrate ability to recognize failures of the postulates.

The *natural numbers* have to do with counting: 0, 1, 2, 3, ... They do not include negatives or fractions or irrationals. In this lecture, the structure of natural numbers is the topic. To hone in on that structure, we look at structures similar to the natural numbers, but that fail to capture some basic aspects of counting. Bogus structures are ruled out by *postulates* (also known as *axioms*) that distinguish the structure of natural numbers from others.

1.1 The Basic Picture

Our first task is to look back to one of the very first mathematical concepts we all learned, namely, *counting*. Some numbers obviously are meant for conuting. 1, 2, 3, and so on are counting numbers, whereas -1, $\frac{1}{2}$ and $\sqrt{2}$ are not. So let's start with a basic intuitive definition: a *counting* or *natural* number is a number that can be used to answer a qeustion of the form "How many x are there?" This is distinct, somehow, from "How *much* x?" The latter sort of question could be answered with $\frac{1}{2}$ (as long as we know how we are measuring). On the other hand, the answer to a "how many" question could be 0 ("how many professors own unicorns?"). So 0 shoud be included in our thinking.

Natural numbers are pictured like stepping stones in Figure 1.1.

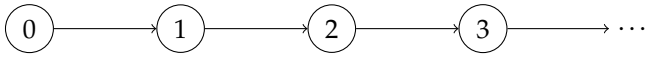


Figure 1.1: A picture of the natural numbers

Not all "stepping stone" pictures are acceptable. Figures 1.2, 1.3 and 1.4 illustrate three ways *not* to picture the natural numbers.

Figure 1.2: Nowhere to start

Figure 1.3: Nowhere to go

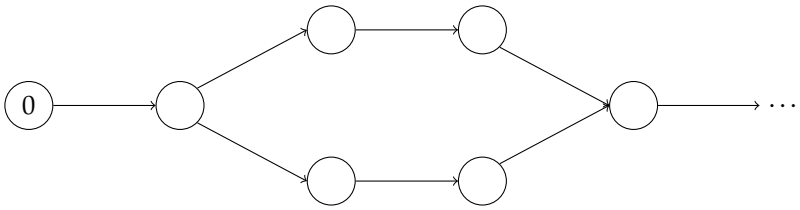


Figure 1.4: Forks in the path

These incorrect pictures can be ruled out by explaining the basic structure of counting. We will "explain the obvious" by stating things like this as *postulates*.

Postulate 1: Basic Structure of Natural Numbers

The **natural numbers** have the following basic structure.

- There is a special natural number. We denote this by 0.
- For any natural number n, there is a unique *next* natural number. We call this the **successor of** n. In these lectures, we denote the successor of n by $n^{\curvearrowright}$.

According to Postulate 1, 0, $0^{\curvearrowright}$, $0^{\curvearrowright\curvearrowright}$, $0^{\curvearrowright\curvearrowright\curvearrowright}$ each denote a natural number. Of course, we usually abbreviate them by writing 0, 1, 2, 3. But the *characters* 1, 2, 3, etc., are not related to each other in any way. The notation we are using here makes it completely clear that $0^{\curvearrowright}$ is the number after 0, and so on. We will want to be able to switch between the familiar "decimal' notation and "successor" notation whenever it is convenient.

Exercises for Lecture 1

Convert the following from decimal notation to successor notation.

1. 9
2. 10
3. $4 + 3$
4. $n + 4$

Convert the following to from successor notation to decimal notation.

1. $0\overset{\frown}{\frown}\overset{\frown}{\frown}\overset{\frown}{\frown}$
2. $n\overset{\frown}{\frown}\overset{\frown}{\frown}\overset{\frown}{\frown}\overset{\frown}{\frown}$
3. $5\overset{\frown}{\frown}\overset{\frown}{\frown}$
4. $0\overset{\frown}{} + 0\overset{\frown}{\frown}$

1.2 Narrowing the possibilities

Figures 1.5 and 1.6 illustrate problems that Postulate 1 does not avoid.

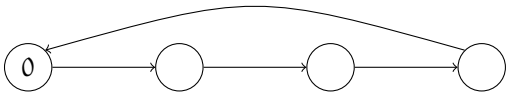


Figure 1.5: A strange way to count

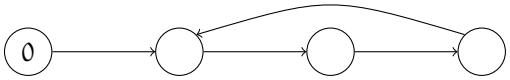


Figure 1.6: Another strange way to count

Exercises for Lecture 1

1. Explain, in one or two sentences each, why Figures 1.5 and 1.6 depict systems that agree with Postulate 1.

Figure 1.5 is flawed because 0 has a *predecessor*: a value n satisfying $0^{\curvearrowright\curvearrowright\curvearrowright\curvearrowright} = 0$. Figure 1.6 is flawed because an element has two distinct predecessors: $0^{\curvearrowright} = 0^{\curvearrowright\curvearrowright\curvearrowright\curvearrowright}$. We can insist that these flaws do not happen in the natural numbers. That is, we rule them out with axioms.

Postulate 2

[Nothing Precedes 0] For every natural number n, $n^{\curvearrowright} \neq 0$.

Postulate 3

[Predecessors are Unique] For any natural numbers m and n, if $m^{\curvearrowright} = n^{\curvearrowright}$ then $m = n$.

These postulates eliminate Figures 1.5, 1.6 and similar pictures. But there is still a subtle problem. Consider Figure 1.7.

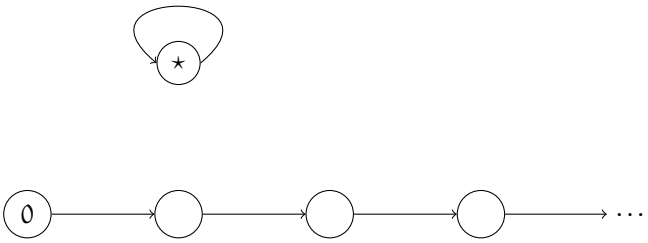


Figure 1.7: A model of the natural numbers?

This picture satisfies the first three postulates. Yet, it is not a picture of natural numbers because it has "extra stuff" in it ($\star$).

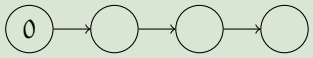
To rule out "extra stuff", we formulate our final postulate for natural numbers. We diagnose the problem as follows. Were we to erase the circle labelled $\star$ and any the arrows leading to and from it, the remaining part of Figure 1.7 would still live up to Postulate 1. This is exactly what we mean by "extra stuff": elements that can be removed without violating the Postulate 1 (the essential structure). This leads to our last axiom.

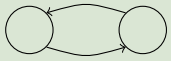
Postulate 4

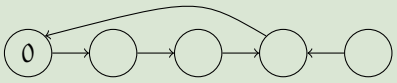
[The Axiom of Induction] No natural numbers can be removed without violating 1.

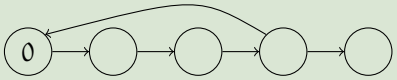
Exercises for Lecture 1

1. Each of the following pictures fails to satisfy either the one or more of our axioms. For each, explain which axioms are violated.

1. 

2. 

3. 

4. 

2. I have in mind a picture for the Basic Vocabulary 1 and that satisfies Axioms 2 and 3. Furthermore, in that picture, I have in mind and element n for which (a) $n \neq 0$ and (b) n has no predecessor (that is, $n \neq m^{\frown}$ for every m). Convince me that the picture fails to satisfy Axiom 4.

The latest exercise shows that in the natural numbers, if $n \neq 0$, then $n = m^{\frown}$ for some m. In other words, every non-zero natural number has a predecessor.

Goals

Lecture
- Present addition and multiplication via defining equations.
- Practice using the defining equations to calculate sums and products.

Study
- Understand addition and multiplication as characterized by defining equations.
- Be able to explain how addition and multiplication relate to counting.
- Exhibit competence in calculating sums and products from the defining equations.

Adding and multiplying arise from counting. In this section, we explore how to define them purely in terms of counting.

2.1 Basic Arithmetic Operations

We know that addition "works" by counting ahead. For example, to *add* $4 + 5$, we can start with 4 and then count up five more. Likewise, multiplication "works" by counting a number of additions. For example, to multiply $2 \cdot 3$ we can add 2 three times: $2 + 2 + 2$. The following definitions capture the idea.

Definition 1: Arithmetic Operations

The **sum** of two natural numbers, m and n, is a natural number (denoted by $m + n$). For every natural number m, the following are true:

$$m + 0 = m$$
$$m + k^{\curvearrowright} = (m + k)^{\curvearrowright} \qquad \text{for any natural number } k$$

The **product** of two natural numbers, m and n, is a natural number (denoted by $m \cdot n$). For

Definition 1 (cont.)

every natural number m, the following are true:

$$m \cdot 0 = 0$$
$$m \cdot k^{\frown} = m + (m \cdot k) \qquad \text{for any natural number } k$$

A moment's thought about arithmetic should convince you that these equations are reasonable. Certainly $m + 0 = m$ and $m \cdot 0 = 0$ should be true for any m. The second equation for $+$ can be read as saying "to add m to the successor of k, simply add m to k, then take the successor." The second equation for $\cdot$ can be read as saying "to multiply m by the successor of k, simply multiply m by k, and add m to the result."

The Axiom of Induction ensures that there are indeed unique operations $+$ and $\cdot$ that satisfy the equations. A proof of this fact is not particularly illuminating right now, so let us agree to take it for granted.

Example 2

Do the defining equations for addition really explain how to add? Let's use them to calculate $4 + 3$:

$$\begin{aligned}
4 + 3 &= 4 + 0^{\frown\frown\frown} && [3 \text{ abbreviates } 0^{\frown\frown\frown}] \\
&= 4^{\frown} + 0^{\frown\frown} && [m + k^{\frown} = m^{\frown} + k] \\
&= 4^{\frown\frown} + 0^{\frown} && [\text{Same reason}] \\
&= 4^{\frown\frown\frown} + 0 && [\text{Same reason}] \\
&= 4^{\frown\frown\frown} && [m + 0 = m] \\
&= (0^{\frown\frown\frown\frown})^{\frown\frown\frown} && [4 \text{ abbreviates } 0^{\frown\frown\frown\frown}] \\
&= 0^{\frown\frown\frown\frown\frown\frown\frown} && [\text{Remove unneeded parentheses}] \\
&= 7 && [7 \text{ abbreviates } 0^{\frown\frown\frown\frown\frown\frown\frown}]
\end{aligned}$$

Example 3

A product can be calculated similarly. Consider $2 \cdot 2$.

$$
\begin{aligned}
2 \cdot 2 &= 2 \cdot 0^{\frown\frown} && \text{[2 abbreviates } 0^{\frown\frown}\text{]} \\
&= 2 + (2 \cdot 0^{\frown}) && [m \cdot k^{\frown} = m + (m \cdot k)] \\
&= 2 + (2 + (2 \cdot 0)) && \text{[Same reason]} \\
&= 2 + (2 + 0) && [m \cdot 0 = 0] \\
&= 2 + 2 && [m + 0 = m] \\
&= 2 + 0^{\frown\frown} && \text{[2 abbreviates } 0^{\frown\frown}\text{]} \\
&= 2^{\frown} + 0^{\frown} && [m + k^{\frown} = m^{\frown} + k] \\
&= 2^{\frown\frown} + 0 && \text{[Same reason]} \\
&= 2^{\frown\frown} && [m + 0 = m] \\
&= (0^{\frown\frown})^{\frown\frown} && \text{[2 abbreviates } 0^{\frown\frown}\text{]} \\
&= 0^{\frown\frown\frown\frown} && \text{[Remove unnecessary parentheses]} \\
&= 4 && \text{[4 abbreviates } 0^{\frown\frown\frown\frown}\text{]}
\end{aligned}
$$

We certainly will not want to calculate this way in real life. After all, it took twelve steps just to figure $2 \cdot 2 = 4$. But these examples and the following exercises show how addition and multiplication are closely tied to simple counting.

Exercises for Lecture 2

1. Calculate these sums, following the previous example to write each step of your calculation explicitly. Include the reason for each step (as in the previous example).Take care to lay out the chain of equalities correctly, and do not skip any steps.
    1. $2 + 4$
    2. $4 + 2$
    3. $3 + (3 + 1)$
    4. $(3 + 3) + 1$
    5. $0 + 3$
2. Notice that it takes more steps to calculate $2 + 4$ than $4 + 2$, even though we know they will produce the same answer. Explain why.
3. Calculate the following values, writing each step explicity.
    1. $2 \cdot 3$

Exercises for Lecture 2 (cont.)

2. $0 \cdot 2$
3. $2 \cdot (2 \cdot 2)$
4. $3 \cdot (2 + 1)$
5. $(3 \cdot 2) + (3 \cdot 1)$

4. Write a definition of exponentiation via defining equations. Follow the pattern of definition I have written for addition and multiplication.

Goals

Lecture

- Present the most common Laws of Arithmetic for natural numbers.
- Explain the method of *proof by simple induction*
- Prove a representative sample of the laws by simple induction.

Study

- Become familiar with the common names for the Laws of Arithmetic.
- Pay particular attention to the Laws of Positivity and Cancellativity (they may be the least familiar to you).
- Demonstrate the ability to identify the main parts of a proof by simple induction.
- Demonstrate the ability to construct the parts of a proof by simple induction.
- Prove the remaining laws for yourself.

Before working the last exercises, you knew that $3 \cdot (2 + 1)$ and $3 \cdot 2 + 3 \cdot 1$ would come out the same because of a law of arithmetic known as *distributivity*. Addition and multiplication satisfy several other laws.

3.1 Basic Laws

The following list summarizes several useful laws of arithmetic on the natural numbers. They are organized to emphasize similarities between addition and multiplication.

Laws 1

For any natural numbers, m, n and p:

Laws 1 (cont.)

	$m + (n + p) = (m + n) + p$ $m \cdot (n \cdot p) = (m \cdot n) \cdot p$	**Commutativity**	$m + n = n + m$ $m \cdot n = n \cdot m$
Identity	$m + 0 = m$ $m \cdot 1 = m$	**Positivity**	if $m + n = 0$ then $m = 0$ if $m \cdot n = 1$ then $m = 1$
Cancellativity	if $m + p = n + p$ then $m = n$ if $m \cdot p^\frown = n \cdot p^\frown$ then $m = n$		
Distributivity	$m \cdot (n + p) = (m \cdot n) + (m \cdot p)$		
Case Distinction	if $m \neq 0$ then $m = k^\frown$ for some k		

Most of these laws are familiar and are listed with their common names. The Law of Case Distinction was the subject of Lecture **??** Exercise 2.. *Go back and look at that exercise again*. The Law of Positivity for multiplication is not a common name, but I have used it to emphasize the analogies between addition and multiplication. Also Case Distinction does not really have a common name. I made that up.

3.2 Inductive Proofs

Suppose we wish to prove that every natural number has some property. For example, let us suppose we wish to prove that every natural number is *mimsy*. I have no idea what a mimsy number is, but let us try to prove this anyway. We could try proving that 0 is mimsy, 1 is mimsy, 2 is mimsy, and so on. But this won't work because our proof will never end. In fact, it is not so obvious that we, humans with finite minds, can ever prove that some property is true for *all* natural numbers, since it seems to involve checking infinitely many individual cases.

The Axiom of Induction provides a way forward in spite of our limitations. Suppose we were to show that the mimsy natural numbers all by themselves constitute a picture of Signature 1. Then there could not be any natural numbers left out, for otherwise, we could erase all the non-mimsy natural numbers and still have a picture of 1. This is exactly what the Axiom of Induction forbids: we can not erase *anything* without breaking the signature.

So to prove that all natural numbers are mimsy, we simply need to prove that

- 0 is mimsy, and
- for all natural numbers k, if k is mimsy so is $k^\frown$.

From these, we conclude that the mimsy natural numbers by themselves form a picture of 1. So the Axiom of Induction ensures that all natural numbers are mimsy.

To make inductive proofs easier to understand, we often write them using a three step outline, as illustrated here.

- [Basis] Prove that 0 is mimsy.

- [Inductive Hypothesis] Assume that k is mimsy.
- [Inductive Step] Prove that $k^{\curvearrowright}$ is mimsy. [You may use the assumption that k is mimsy in this part of the proof.]

More practical examples are next.

Proposition 2

Addition is associative.

Proof: We need to show that $m + (n + p) = (m + n) + p$ for all m, n and p. Let us suppose that m and n are fixed values (not known to us). We now prove that the values p for which $m + (n + p) = (m + n) + p$ holds form a picture of 1.

- [Basis] $m + (n + 0) = m + n = (m + n) + 0$. Both steps are due to the defining equations of $+$.
- [Inductive Hypothesis] Assume $m + (n + k) = (m + n) + k$.
- [Inductive Step] We must show that $m + (n + k^{\curvearrowright}) = (m + n) + k^{\curvearrowright}$.

$$\begin{aligned} m + (n + k^{\curvearrowright}) &= m + (n + k)^{\curvearrowright} && \text{[Def. of +]} \\ &= (m + (n + k))^{\curvearrowright} && \text{[Same]} \\ &= ((m + n) + k)^{\curvearrowright} && \text{[Inductive Hypothesis]} \\ &= (m + n) + k^{\curvearrowright} && \text{[Def. of +]} \end{aligned}$$

Therefore (by the Axiom of Induction), $m + (n + p) = (m + n) + p$ holds for all p. Since the argument does not depend on any extra assumptions about m and n, it holds for all m and n. □

In the remainder of this section, we further illustrate the technique of simple arithmetic induction via proofs of other laws of arithmetic.

Proposition 3

0 is the identity for addition.

Proof: We must prove that $m + 0 = m = 0 + m$ for all m. The first equality is true by the definition of $+$. But the second equality, $m = 0 + m$, is not explicitly one of the defining facts about $+$. So we proceed by induction on m.

- [Basis] $0 + 0 = 0$ is true by definition of $+$.
- [Inductive Hypothesis] Assume $0 + k = k$.
- [Inductive Step] We must show that $0 + k^{\curvearrowright} = k^{\curvearrowright}$.

$$\begin{aligned} 0 + k^{\curvearrowright} &= (0 + k)^{\curvearrowright} && \text{[Def. of } +\text{]} \\ &= k^{\curvearrowright} && \text{[Inductive hypothesis]} \end{aligned}$$

Therefore, $0 + m = m$ holds for all m. □

To prove that addition is commutative, we need an additional fact about how successor and addition interact. Mathematicians use the word *lemma* to indicate that a certain fact is only needed to make others proofs easier and is not necessarily valuable in its own right.

Lemma 4

For any m and n, $(m + n)^{\curvearrowright} = m^{\curvearrowright} + n$.

Proof: By induction on n:

- [Basis]

$$\begin{aligned} (m + 0)^{\curvearrowright} &= m^{\curvearrowright} && \text{[Def. of } +\text{]} \\ &= m^{\curvearrowright} + 0 && \text{[Def. of } +\text{]} \end{aligned}$$

- [Inductive Hypothesis] Assume $(m + k)^{\curvearrowright} = m^{\curvearrowright} + k$ for some k.
- [Inductive Step] We must show that $(m + k^{\curvearrowright})^{\curvearrowright} = m^{\curvearrowright} + k^{\curvearrowright}$.

$$\begin{aligned} (m + k^{\curvearrowright})^{\curvearrowright} &= ((m + k)^{\curvearrowright})^{\curvearrowright} && \text{[Def. of } +\text{]} \\ &= (m^{\curvearrowright} + k)^{\curvearrowright} && \text{[Inductive Hypothesis]} \\ &= m^{\curvearrowright} + k^{\curvearrowright} && \text{[Def. of } +\text{]} \end{aligned}$$

So $(m + n)^{\curvearrowright} = m^{\curvearrowright} + n$. Because the proof does not depend on any assumption about m, it is valid for all m. □

Roughly speaking this lemma permits us to move $\curvearrowright$ anywhere within an addition: $m^{\curvearrowright} + n = (m + n)^{\curvearrowright} = m + n^{\curvearrowright}$. So we are free to move a successor "out of the way" whenever we need to. The next proof illustrates the point.

Proposition 5

Addition is commutative.

Proof: We need to show that $m + n = n + m$ for all m and n. This time, the proof is by induction on m. Fix a value for n.

- [Basis] $0 + n = n = n + 0$ holds because of Proposition 3 and the definition of $+$.
- [Inductive Hypothesis] Assume that $k + n = n + k$ for some k.
- [Inductive Step] We must show that $k^\curvearrowright + n = n + k^\curvearrowright$.

$$\begin{aligned} k^\curvearrowright + n &= (k + n)^\curvearrowright && \text{[Lemma 4]} \\ &= (n + k)^\curvearrowright && \text{[Inductive Hypothesis]} \\ &= n + k^\curvearrowright && \text{[Def. of } +\text{]} \end{aligned}$$

Therefore, $m + n = n + m$ for all m. Since this argument does not depend on any assumptions about n, it is valid for all n. □

The next law may be less familiar to you. Roughly, it says that we can "subtract" equals and get equals. But note that actual subtraction does not always make sense for natural numbers. We can not, for example, say what $5 - 7$ means without introducing negative numbers.

Proposition 6

Addition is cancellative.

Proof: We need to prove that if $m + p = n + p$, then $m = n$. This proof is a little subtler than the previous ones. But notice that is still follows the same form.

The proof is by induction on p. Assume that m and n are some fixed natural numbers.

- [Basis] Suppose $m + 0 = n + 0$. Then immediately by definition of $+$, $m = n$.
- [Inductive Hypothesis] Assume that the following statement is true for some k: if $m + k = n + k$ then $m = n$.
- [Inductive Step] We must show that if $m + k^\curvearrowright = n + k^\curvearrowright$ then $m = n$. Suppose $m + k^\curvearrowright = n + k^\curvearrowright$ [call this (*) for reference]. Then

$$\begin{aligned} (m + k)^\curvearrowright &= m + k^\curvearrowright && \text{[Def. of } +\text{]} \\ &= n + k^\curvearrowright && \text{[By the supposition (*)]} \\ &= (n + k)^\curvearrowright && \text{[Definition of } +\text{]} \end{aligned}$$

  Hence, by Axiom 3 $m + k = n + k$. So by the Inductive Hypothesis, $m = n$.

Therefore, $m + p = n + p$ implies $m = n$ for all p. Since this argument does not depend on any assumptions regarding m and n, it is valid for all m and n. □

To prove that multiplication is commutative and cancellative, we will need the following technical facts (analogous to Proposition 3 and Lemma 4).

Lemma 7

For any n, $0 \cdot n = 0$

Proof: The proof is by induction on n.

- [Basis] $0 \cdot 0 = 0$ by definition of $\cdot$.
- [Inductive Hypothesis] Assume that $0 \cdot k = 0$ for some k.

Lemma 7 (cont.)

- [Inductive Step] We must show that $0 \cdot k^{\curvearrowright} = 0$.

$$\begin{aligned} 0 \cdot k^{\curvearrowright} &= 0 + 0 \cdot k && \text{[Definition of } \cdot\text{]} \\ &= 0 + 0 && \text{[Inductive Hypothesis]} \\ &= 0 && \text{[Definition of } +\text{]} \end{aligned}$$

□

Lemma 8

For any m and n, $m^{\curvearrowright} \cdot n = m \cdot n + n$

Proof: The proof is by induction on n.

- [Basis] $m^{\curvearrowright} \cdot 0 = 0 = 0 + 0 = m \cdot 0 + 0$ all follow from the definitions of $+$ and $\cdot$.
- [Inductive Hypothesis] Assume that $m^{\curvearrowright} \cdot k = m \cdot k + k$ for some k.
- [Inductive Step] We must show that $m^{\curvearrowright} \cdot k^{\curvearrowright} = m \cdot k^{\curvearrowright} + k^{\curvearrowright}$.

$$\begin{aligned} m^{\curvearrowright} \cdot k^{\curvearrowright} &= m^{\curvearrowright} + m^{\curvearrowright} \cdot k && \text{[Exercise]} \\ &= (m + m^{\curvearrowright} \cdot k)^{\curvearrowright} && \text{[Exercise]} \\ &= (m + (m \cdot k + k))^{\curvearrowright} && \text{[Exercise]} \\ &= ((m + m \cdot k) + k)^{\curvearrowright} && \text{[Exercise]} \\ &= (m \cdot k^{\curvearrowright} + k)^{\curvearrowright} && \text{[Exercise]} \\ &= m \cdot k^{\curvearrowright} + k^{\curvearrowright} && \text{[Exercise]} \end{aligned}$$

□

Some of the other laws are left as exercises.

Exercises for Lecture 3

1. Prove that 1 is the identity for multiplication. That is $1 \cdot m = m = m \cdot 1$.
2. Write out the entire proof of Lemma 8 providing the justifications for each line of the equational calculation in the Inductive Step.
3. Prove that multiplication distributes over addition $[m \cdot (n + p) = m \cdot n + m \cdot p]$ by induction on p. You can use the any of the lemmas and propositions we have already proved.
    1. Prove the basis: $m \cdot (n + 0) = m \cdot n + m \cdot 0$.
    2. Write the inductive hypothesis.
    3. Prove the inductive step: $m \cdot (n + k^{\curvearrowright}) = m \cdot n + m \cdot k^{\curvearrowright}$
4. Prove that multiplication is associative $[m \cdot (n \cdot p) = (m \cdot n) \cdot p]$ by induction on p.
    1. Prove the basis: $m \cdot (n \cdot 0) = (m \cdot n) \cdot 0$.
    2. Write the inductive hypothesis.
    3. Prove the Inductive Step: $m \cdot (n \cdot k^{\curvearrowright}) = (m \cdot n) \cdot k^{\curvearrowright}$. Hint: Use the Law of Distribution, which you just proved.
5. Prove that multiplication is commutative. Hint: Use the two Lemmas we proved right before these exercises.

Lists

Natural numbers constitute an important example of something more general, where objects are built up from simpler ones. The Axiom of Induction captures the idea of building "up" and provides an important method for proving facts about natural numbers.

In this lecture, we develop an analogous way to think about *lists*.

Goals

Lecture Goals

- Introduce a formal counterpart to the informal concept of a list
- Emphasize the close analogy between lists and natural numbers
- Introduce basic operations on lists.

Study Goals

- Demonstrate facility with basic list manipulation including calculating length and concatenation of lists.

4.1 List Basics

In this section, we concentrate on the fundamental concept of *lists*. The idea is really meant to be the familiar one, so a list of "to do" items is a list. The alphabetized names on a class roster is a list. We will write lists using square brackets. So for example, $[2, 3, 5, 7]$ is the list of the prime numbers less than 10 in ascending order. For lists, we expect the order to matter. So $[7, 5, 3, 2]$ is a different list.

Something that occurs on a list is called an *item* of the list. We can even specify where it is. So we can talk about the "first", "second" item, and so on, assuming the list has enough items.

Because we have already agreed that natural numbers begin with 0, it turns out to make many things easier if we change the way we talk about items on a list to gibe with the natural numbers. So instead of refering to the "first" item, we might call it the "initial" item. Furthermore, we will number them to start with 0. What I mean is that if $L = [2, 3, 5, 7]$, we will write L_0, L_1, L_2, L_3 for

the elements 2, 3, 5, 7, respectively. In short, the "initial" item is indexed by the "initial" natural number 0. The next item after that is indexed by next natural number, $0^\frown$, and so on.

Like natural numbers, lists can be built up by starting with an empty list and incrementally adding items. We have choices for how we might formalize the idea. We will follow a standard that has developed in computer science. Clearly, since we use square brackets to punctuate lists, the empty list should be written as $[]$. To add an item to a list, we will conventionally put it on the front.

Given the list $[x, y, z]$, we may build a new list with initial item w and the given list as the rest, resulting in $[w, x, y, z]$. The operation of *prepending* an item to a list is denoted by a colon (:). So $w : [x, y, z]$ *is* the list $[w, x, y, z]$.

The empty list, together with prepending items, gives us a way to construct any list we want.

Example 1

Here are some examples.

- $5 : 6 : [4, 5]$ is the same as $5 : [6, 4, 5]$, which is the same as $[5, 6, 4, 5]$.
- $[]$ is the empty list
- $1 : []$ is the same as $[1]$
- $1 : 2 : 3 : 4 : []$ is the same as $[1, 2, 3, 4]$.

Notice that every list is either empty ($[]$) or not. If not, it has the form $x : L$ where x is the initial item and L is the rest of the list. This suggests a signature for lists, not so different from the signature for natural numbers.

Postulate 2: Basic Structure of Lists

Lists have the following basic structure.

- There is a special list, which we call *the empty list* and denote by $[]$.
- For any thing x and any list L, there is another list, obtained by *prepending* x to L. We denote the result by $x : L$.

As with the natural numbers, we need to think about axioms that prevent strange behavior. These are exactly analogous to the axioms of natural numbers. First, $[]$ can not be obtained by adding a new initial item to another list. So

Postulate 3

For any list L and any thing x, $[] \neq x : L$.

Likewise, a list that is not empty can only be built one way.

Postulate 4

For any things x and y and lists L and M, if $x : L = y : M$, then $x = y$ and $L = M$.

For example, if I tell you that $[2, 3, 4, 5] = x : L$, then you know immediately that $x = 2$ and $L = [3, 4, 5]$.

Finally, lists need an induction axiom that ensures that all lists are built up from $[]$.

Postulate 5: The Axiom of List Induction

No lists can be removed without violating Postulate **??**.

This axiom justifies conducting proofs about all lists by a scheme almost identical to simple arithmetic induction. That is, to prove some property is true about all lists, it is enough to show

- [Basis] The property is true about $[]$.
- [Inductive Hypothesis] Assume that the property is true for from list K.
- [Inductive Step] Prove that for any thing x, the property is true about $x : K$. [You may use the assumption about K in this part of the proof.]

Operations on lists can now also be defined by schemes similar to how we defined addition and multiplication on natural numbers. For example, every list has a length. Writing $\mathsf{len}(L)$ for the length of a list, $\mathsf{len}([2, 3, 4]) = 3$. A precise definition is now easy to formulate.

Definition 6

For a list L. the *length* of L, denoted by $\mathsf{len}(L)$, is the natural number. This satisfies the following equalities.

$$\mathsf{len}([]) = 0$$
$$\mathsf{len}(x : L) = \mathsf{len}(L)^{\curvearrowright}$$

Example 7

$$\begin{aligned}
\mathsf{len}([2,3,4]) &= \mathsf{len}(2:[3,4]) \\
&= \mathsf{len}([3,4])^\frown \\
&= \mathsf{len}(3:[4])^\frown \\
&= \mathsf{len}([4])^\frown{}^\frown \\
&= \mathsf{len}(4:[])^\frown{}^\frown \\
&= \mathsf{len}(,])^\frown{}^\frown{}^\frown \\
&= 0^\frown{}^\frown{}^\frown \\
&= 3
\end{aligned}$$

Another common operation on lists is *concatenation*: $[2,3,4] \otimes [4,1,3] = [2,3,4,4,1,3]$, whereby the two lists are simply glued together in their original orders. This is defined precisely by the following.

Definition 8

For lists L and M, their *concatenation*, denoted by $L \otimes M$, is a list. For all lists M, the following are true.

$$\begin{aligned}
[] \otimes M &= M \\
(x : K) \otimes M &= x : (K \otimes M) \qquad \text{for any thing } x \text{ and any list } K
\end{aligned}$$

Example 9

To calculate $[4,5,2,1] \otimes [3,4,1]$, we can follow a method similar to arithmetic:

$$\begin{aligned}
[4,5,2,1] \otimes [3,4,1] &= (4:5:2:1:[]) \otimes [3,4,1] && [[4,5,2,1] \text{ abbreviates } 4:5:2:1:[]] \\
&= 4 : ((5:2:1:[]) \otimes [3,4,1]) && [\text{Def. of } \otimes] \\
&= 4:5:((2:1:[]) \otimes [3,4,1]) && [\text{Same}] \\
&= 4:5:2:((1:[]) \otimes [3,4,1]) && [\text{Same}] \\
&= 4:5:2:1:([] \otimes [3,4,1]) && [\text{Same}] \\
&= 4:5:2:1:[3,4,1] && [\text{Same}] \\
&= [4,5,2,1,3,4,1] && [\text{Abbreviation}]
\end{aligned}$$

Now we can prove some useful facts about lists.

Lemma 10

On lists, $[]$ is the identity for $\otimes$,

Proof: By definition $[] \otimes L = L$ always true. But $[]$ must also satisfy $L \otimes [] = L$ always. We can proceed by induction on L. The proof should look familiar (see the proof of Lemma **??**).

- [Basis] $[] \otimes [] = []$ is true by definition of $\otimes$.
- [Inductive Hypothesis] Assume $K \otimes [] = K$ for some list K.
- [Inductive Step] Suppose x is some thing. We need to show that $(x : K) \otimes [] = x : K$.

$$\begin{aligned} (x : K) \otimes [] &= x : (K \otimes []) && \text{[by definition of } \otimes] \\ &= x : K && \text{[by the Inductive Hypothesis]} \end{aligned}$$

Thus (by the Axiom of List Induction), the lists for which $L \otimes [] = L$ constitute all lists. □

Lemma 11

On lists, $\otimes$ is associative.

Proof: We prove $L \otimes (M \otimes N) = (L \otimes M) \otimes N$ using induction on L. This should look familiar. It is almost identicial to the proofs that addition and multiplication are associative.

- [Basis] $[] \otimes (M \otimes N) = M \otimes N = ([] \otimes M) \otimes N$. Both steps are by the definition of $\otimes$.
- [Inductive hypothesis] Suppose $K \otimes (M \otimes N) = (K \otimes M) \otimes N$ for some particular list K.
- [Inductive step]

$$\begin{aligned} (x : K) \otimes (M \otimes N) &= x : (K \otimes (M \otimes N)) && \text{Def. of } \otimes \\ &= x : ((K \otimes M) \otimes N) && \text{Inductive Hypothesis} \\ &= (x : (K \otimes M)) \otimes N && \text{Def. of } \otimes \\ &= ((x : K) \otimes M) \otimes N && \text{Def. of } \otimes \end{aligned}$$

Lemma 11 (cont.)

So $L \otimes (M \otimes N) = (L \otimes M) \otimes N$ is true for all L. Since the proof does not depend on any special propertis of M and N (except that they are both lists), the result is true for all lists M and N. □

Here is another nice fact that we can prove by induction relating length to concatenation.

Lemma 12

For any lists L and M, $\mathsf{len}(L \otimes M) = \mathsf{len}(L) + \mathsf{len}(M)$.

Proof: [This claim is probably fairly obvious to you. Nevertheless, to illustrate the technique of list induction again, we prove it explicitly.]

- [Basis] $\mathsf{len}([\,]) + \mathsf{len}(M) = 0 + \mathsf{len}(M) = \mathsf{len}(M) = \mathsf{len}([\,] \otimes M)$. These are by definition of $\otimes$ and $+$.
- [Inductive Hypothesis] Suppose $\mathsf{len}(K \otimes M) = \mathsf{len}(K) + \mathsf{len}(M)$ holds for some particular list K.
- [Inductive Step]

$$\begin{aligned}
\mathsf{len}((x : K) \otimes M) &= \mathsf{len}(x : (K \otimes M)) && \text{Def. of } \otimes \\
&= \mathsf{len}(K \otimes M)^{\curvearrowright} && \text{Def. of len} \\
&= (\mathsf{len}(K) + \mathsf{len}(M))^{\curvearrowright} && \text{Inductive Hypothesis} \\
&= \mathsf{len}(K)^{\curvearrowright} + \mathsf{len}(M) && \text{Lemma 4} \\
&= \mathsf{len}(x : K) + \mathsf{len}(M) && \text{Def. of len}
\end{aligned}$$

□

Often we will use a list somewhat informally without all the punctuation. For example, we might say "Consider a list $a_0, a_1, \ldots, a_{n-1}$ of real numbers." If we do not intend to use the list itself for anything special, but only want to think about the numbers a_0 through a_n, then there is no need to be formal about it. Also, there is no harm in writing something like this: a_5, a_6, a_7, a_8, where the indices start at 5. The default is to start at 0, but that is merely a convention.

Lemma 13

$\otimes$ is cancellative on the left and on the right. That is,

Lemma 13 (cont.)

- $L \otimes M = L \otimes N$ implies $M = N$; and
- $L \otimes N = M \otimes N$ implies $L = M$.

Proof: Exercise. □

4.2 List Itemization

In a list L, the items are in order. So we can refer to items by their position in the list. There are two standards in mathematics for doing this. Either we start counting from 1 or from 0. Although it may seem unintuitive at first to start from 0 (meaning that the "initial" item of a list is item number 0), this actually makes many calculations simpler. For that reason, most programming languages use this convention for a lists and arrays. So I will consistently start with 0.

The idea can be made precise as follows.

Definition 14

Suppose L is a list and $i < \mathsf{len}(L)$. Then L_i is an item on the list defined as follows.

$$
\begin{aligned}
[\,]_i &\text{ is never defined because } 0 \not< \mathsf{len}([\,]) \\
(x : L)_0 &= x \\
(x : L)_{k\frown} &= L_k \qquad \text{provided that } L_k \text{ is defined}
\end{aligned}
$$

This is a precise way of explaining that in a list, for example $L = [a, b, c, d, e]$, we can refer to an item by its *index*, so that $L_0 = a$, $L_1 = b$ and so on, up to $L_4 = e$. Notice that L_k is undefined if $k \geq \mathsf{len}(L)$.

Example 15

Suppose $L = [a, b, c, d, e]$. We can calculate L_3 explicitly step by step.

$$\begin{aligned} L_3 &= [a, b, c, d, e]_3 \\ &= (a : b : c : d : e : [])_{0\frown\frown\frown} \\ &= (b : c : d : e : [])_{0\frown\frown} \\ &= (c : d : e : [])_{0\frown} \\ &= (d : e : [])_0 \\ &= d \end{aligned}$$

Of course, this is just a very careful (you might even say fussy) way to find item number 3 in the list. In every day use, we humans would not do this. We would simply count forward from the beginning of the list.

Exercises for Lecture 4

1. Suppose $L = [3, 2, 3, 3, 5]$ and $M = [0, 1, 2, 3, 4, 5]$. Calculate the following explicitly step by step.
    1. $\mathsf{len}(L)$
    2. L_4
    3. $(L \otimes M)_9$

4.3 Lists of a Particular Type

We will commonly need to consider lists in which all elements are similar, such as a list consisting of natural numbers. For example, because we know how arithmetic operations work on natural numbers, we can also define operations on lists of natural numbers using arithmetic. Similar extensions are possible for other operations defined on other types of elements.

To illustrate, suppose L is a list of natural numbers. We can define the *sum* of items on the list in the obvious way, so that the sum of the list $[2, 3, 4]$ is $2 + 3 + 4 = 9$. We make this precise with the following.

Definition 16

For a list L of natural numbers, the *sum of* L, denoted by $\sum L$, is a natural number, satisfying

$$\sum [] = 0$$
$$\sum m : L = m + \sum L \qquad \text{for any natural number } m \text{ and any list of natural numbers } L$$

We will introduce variations and extensions of this notation this later. For now, we look only at lists.

Exercises for Lecture 4

1. Prove using list induction that for any lists of natural numbers,
$$\sum L + \sum M = \sum (L \otimes M)$$
2. Define the product of lists of natural numbers, following the pattern of our definition for $\sum L$. The standard notation for a product is $\prod L$. The result should be that $\prod [2,3,4]$ equals 24. Pay close attention the base case $\prod []$.
3. Using your definition of products, prove by list induction that for any lists of natural numbers,
$$\prod L \cdot \prod M = \prod (L \otimes M)$$
.

We can also consider lists of integers, lists of real numbers, and so on. We can even think about lists of lists. For example, $[[2,3,4],[4,3,2],[5]]$ is a list consisting of two items: $[2,3,4]$, $[4,3,2]$ and $[5]$. Written this using :, this is list is $[2,3,4] : [4,3,2] : [5] : []$. Suppose we have a list of lists like this we can define the concatenation of all the items. For this example, the result should be $[2,3,4,4,3,2,5]$. The definition of this is exactly analogous to sums and products.

Definition 17

For a list $\mathcal{L}$ of lists, the *fold of* $\mathcal{L}$, denoted by $\bigotimes \mathcal{L}$, is a list, satisfying

$$\bigotimes [] = []$$
$$\sum M : \mathcal{L} = M \otimes \bigotimes \mathcal{L} \qquad \text{for any list } M \text{ and any list of lists } \mathcal{L}$$

Compare the definitions of $\sum$, $\prod$ and $\otimes$. They differ only in terms of (i) what is the result for an empty list and (ii) what binary operation is used in the second equation.

Suppose we are given a list $\mathcal{L}$ of lists of natural numbers (like the example just above the latest definition). Then its fold is a list of natural numbers. So this can be summed. That is, $\bigotimes\mathcal{L}$ is a list of natural numbers, and $\sum(\bigotimes\mathcal{L})$ is a natural number. But we might also apply the summation operation to each list on $\mathcal{L}$ separately, resulting in another list of natural numbers. The idea of applying an operation to each element of a list is called "mapping". In this case, we intend to "map" the operation $\sum$ across lists of lists of natural numbers. Here is a suitable definition.

Definition 18

For a list $\mathcal{L}$ of lists of natural numbers, the *mapping of* $\sum$ *on* $\mathcal{L}$, denoted by $\mathsf{map}_{\sum}(\mathcal{L})$ is a list of natural numbers, satisfying

$$\bigotimes[] = []$$

$$\sum M : \mathcal{L} = (\,)\sum M) : \mathcal{L} \quad \text{for any list of natural numbers } M \text{ and any list of lists of natural numbers } \mathcal{L}$$

Exercises for Lecture 4

1. Calculate $\sum(\bigotimes[[3,4,5],[6,3]])$.
2. Calculate $\mathsf{map}_{\sum}([[3,4,5],[6,3]])$.
3. Calculate $\sum(\mathsf{map}_{\sum}([[3,4,5],[6,3]]))$.
4. Prove that $\sum(\bigotimes\mathcal{L}) = \sum(\mathsf{map}_{\sum}(\mathcal{L}))$ for any list of lists of natural numbers $\mathcal{L}$.

4.4 Other Inductively Defined Collections

The structure of natural numbers and the structure of lists are very similar. This similarity can be exploited to develop a simple way of summarizing their properties.

For natural numbers, 0 and $n^\frown$ are the only ways to construct them. Operations like addition and multiplication are defined in terms of 0 and $^\frown$, so they do not contribute directly to the *construction* of natural numbers. So we refer to 0 and $\frown$ as *constructors*.

Axioms 2 and 3 spell out how these constructors behave. Namely, Axiom 2 captures the idea that the two constructors are entirely different from the other: $0 \neq n^\frown$. Axiom 3 captures the idea that $^\frown$ constructs distinct natural numbers from distinct natural numbers: $m^\frown = n^\frown$ implies $m = n$ (or equivalently, $m \neq n$ implies $m^\frown \neq n^\frown$).

So the basic ingredients of natural numbers are the constructors 0 and $\curvearrowright$ with the understanding that (a) each produces different results and (b) from different ingredients, $\curvearrowright$ produces different results. In fact, point (b) also applies to 0 trivially, because 0 does not use any ingredients.

We can summarize everything we want to say about natural numbers concisely in the following way.

Definition 19

The *natural numbers* are defined *inductively* by

$$n \coloneqq 0 \mid n\curvearrowright$$

In this notation, the vertical bar separates the different constructors for natural numbers. The first constructor (0) does not depend on anything else. The second constructor depends on a natural number n and produces a new one $n\curvearrowright$. So this gives a very concise description of the signature of natural numbers. Implicitly, this notation is meant to indicate that the two alternatives are completely distinct. This is Axiom 2. Also implicitly, the notation is meant indicate that $n\curvearrowright$ produces distinct results from distinct n's. This is Axiom 3. By declaring saying that this defines natural numbers *inductively*, we also mean that no natural numbers can be removed without violating the signature.

Now let's consider lists. Again, there are two ways to construct lists. $[]$ and $x : L$ for any thing x and any list L. Likewise, the constructrs are distinct, and $x : L = y : M$ is true if and only if both $x = y$ and $L = M$. So we can encapsulate the definition of lists similarly.

Definition 20

The *lists* are defined *inductively* by

$$L \coloneqq [] \mid x : L \qquad \text{for any thing } x$$

Notice that x can also be a list.

Later in the course, we will make these definitions, and many others like them, rigorous. For now, we just draw attention to the similarity between natural numbers and lists, and point out that proofs by induction work thanks to the structure of these definitions.

4.5 Binary Trees

Simple binary trees are structures that play a role in many parts of computer science and mathematics. Figure 4.1 illustrates an example. There are many variations on the basic idea, but we concentrate on the simplest version (where there is no extra structure).

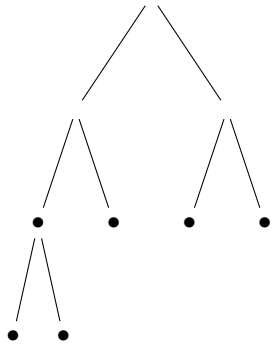


Figure 4.1: A simple binary tree

Such structures are built from *leaves* (denoted here by •) by "grafting" two smaller trees to form a larger one as pictured in Figure 4.2. Trees are usually depicted "upside down", so the *root* is at the top and the leaves are at the bottom. What can you do? It's tradition.

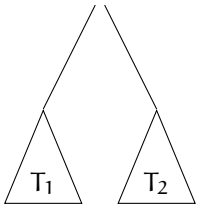


Figure 4.2: Constructing a tree from subtrees

In addition to drawing pictures of binary trees, we can use a linear notation (something that can we written in the midst of prose). If T_1 and T_2 are simple binary trees, we may denote the tree constructed by grafting T_1 on the left and T_2 on the right as $(T_1 \curlywedge T_2)$ (as in Figure 4.2. Thus we define simple binary trees, and two operations on them, as follows.

Definition 21

Simple binary trees are defined inductively by

$$T ::= \bullet \mid (T_1 \curlywedge T_2)$$

The *size* of a simple binary tree is a natural number defined by the equations

$$\begin{aligned} \mathsf{sz}(\bullet) &:= 0 \\ \mathsf{sz}(T_1 \curlywedge T_2) &:= 1 + \mathsf{sz}(T_1) + \mathsf{sz}(T_2) \end{aligned}$$

The *height* of a simply binary tree a natural number is defined by the equations

$$\begin{aligned} \mathsf{ht}(\bullet) &\coloneqq 0 \\ \mathsf{ht}(T_1 \curlywedge T_2) &\coloneqq 1 + \max(\mathsf{ht}(T_1), \mathsf{ht}(T_2)) \end{aligned}$$

where $\max(m, n)$ is the larger of the two numbers.

These definitions suggest a relation between the size and height of a tree.

Lemma 22

For any simple binary tree T,

$$\mathsf{ht}(T) \leq \mathsf{sz}(T) < 2^{\mathsf{ht}(T)}.$$

Proof: To prove this by *structural induction*, we must prove it for the basis ($\bullet$) and that if it is true for some T_1 and T_2, then it is true for $(T_1 \curlywedge T_2)$.

- [Basis] $\mathsf{ht}(\bullet) = 0$, $\mathsf{sz}(\bullet) = 0$ and $2^{\mathsf{ht}(\bullet)} = 1$. So the claim is true for $\bullet$.
- [Inductive Hypothesis] Suppose the inequalities holds for some T_1 and T_2.
- [Inductive Step] We must prove the two inequalities for $T = (T_1 \curlywedge T_2)$. Without loss of generality, assume that $\mathsf{ht}(T_1) \leq \mathsf{ht}(T_2)$. That is, if this is not so, then we may swap T_1 for T_2 in the following.

$$\begin{aligned} \mathsf{ht}(T) &= 1 + \max(\mathsf{ht}(T_1), \mathsf{ht}(T_2)) && \text{[Definition of ht]} \\ &\leq 1 + \mathsf{ht}(T_1) + \mathsf{ht}(T_2) && \text{[Arithmetic]} \\ &\leq 1 + \mathsf{sz}(T_1) + \mathsf{sz}(T_2) && \text{[Inductive Hypothesis]} \\ &= \mathsf{sz}(T) && \text{[Definition of sz]} \end{aligned}$$

And

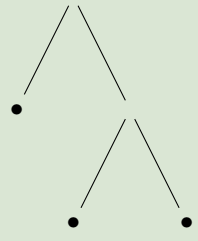
$$\begin{aligned} \mathsf{sz}(T) &= 1 + \mathsf{sz}(T_1) + \mathsf{sz}(T_2) && \text{[Definition of sz]} \\ &\leq 1 + 2^{\mathsf{ht}(T_1)} - 1) + (2^{\mathsf{ht}(T_2)} - 1) && \text{[Inductive Hypothesis]} \\ &\leq 2 \cdot 2^{\mathsf{ht}(T_2)} - 1 && \text{[Assumption that } \mathsf{ht}(T_1) \leq \mathsf{ht}(T_2)\text{]} \\ &= 2^{\mathsf{ht}(T_2)+1} - 1 && \text{[Arithmetic]} \\ &= 2^{\mathsf{ht}(T)} - 1 && \text{[Definition of ht]} \end{aligned}$$

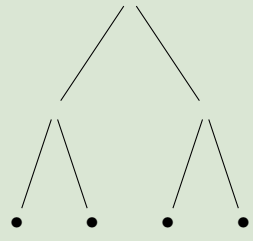
So $\mathsf{sz}(T) < 2^{\mathsf{ht}(T)}$

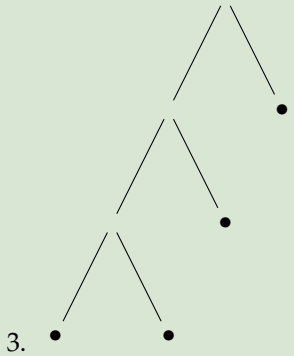
□

Exercises for Lecture 4

1. Calculate the height and size of the following simple binary trees.
   1. $(\bullet \curlywedge \bullet)$
   2. $(\bullet \curlywedge (\bullet \curlywedge \bullet))$
   3. $((\bullet \curlywedge \bullet) \curlywedge (\bullet \curlywedge (\bullet \curlywedge \bullet)))$
   4. $((\bullet \curlywedge (\bullet \curlywedge \bullet)) \curlywedge ((\bullet \curlywedge \bullet) \curlywedge (\bullet \curlywedge (\bullet \curlywedge \bullet))))$
2. Draw diagrams (similar to those in Figure 4.1) for the following simple binary trees.
   1. $((\bullet \curlywedge \bullet) \curlywedge (\bullet \curlywedge \bullet))$
   2. $(((\bullet \curlywedge \bullet) \curlywedge \bullet) \curlywedge ((\bullet \curlywedge \bullet) \curlywedge (\bullet \curlywedge (\bullet \curlywedge \bullet))))$
3. For each of the following diagrams, write the expression using $\bullet$ and $\curlywedge$ defining the same tree.

1.


2.


3.


We will study binary trees in more depth later in the course.

Ordering the Natural Numbers by Addition

We have used the ordering of numbers informally without much comment because $\leq$ has its obvious meaning. In this lecture we exploit the fact that $\leq$ on the natural numbers is defined by addition, setting the stage for an analogous concept defined by multiplication. The multiplicative analogue of "m is less than or equal n" is "m divides n".

Goals

Lecture

- Introduce a formal definition of $\leq$ on natural numbers, and discuss simple facts about order
- Review basic laws involving min and max.
- Introduce Strong Induction and the Principle of Well-foundedness as alternatives to Simple Induction.

Study

- Prove basic facts about $\leq$, min and max.
- Commit to memory the concepts of reflexivity, transitivity, anti-symmetry and linearity.
- Practice using Strong Induction.

5.1 Less or Equal

For the natural numbers, $\leq$ has a particularly simple definition.

Definition 1

For natural numbers n and m, say that m *is less than or equal to* n (written $m \leq n$) if and only if there is a natural number d so that $m + d = n$. [I've used the letter d because d is the

Definition 1 (cont.)

difference of m from n.]

Also, say that m **is (strictly) less than** n if and only if there is a natural number d so that $m + d^{\frown} = n$.

All of the usual properties of $\leq$ for natural numbers follow easily from this definition using only the laws of addition. The important properties have names.

Laws 2

Reflexivity $\leq$ is *reflexive*: $m \leq m$ is true for any m. This is simply because because $m+0 = m$.

Transitivity $\leq$ is *transitive*: if $m \leq n$ and $n \leq p$, then $m \leq p$. Transitivity follows from the law of associativity for addition (you will prove this as an exercise).

Anti-symmetry $\leq$ is *anti-symmetric*: if $m \leq n$ and $n \leq m$, then $m = n$. This follows from cancellativity and positivity (another exercise).

Linearity $\leq$ is *linear*: for any m and n, either $m \leq n$ or $n \leq m$. This requires a separate proof using induction, dealt with below.

Clearly, $\leq$ is also meaningful for integers, rational numbers and real numbers, and is still reflexive, transitive and anti-symmetric and linear for them. For our purposes, though, the interesting features are already present in the natural numbers. For one thing, if $m + d = n$ and $m + e = n$ then $d = e$ (why?). This tells us that $m \leq n$ can only be true for one reason.

Exercises for Lecture 5

In the following you will use the Laws of Arithmetic from Lecture 3 to prove the basic facts about $\leq$.

1. Show that $\leq$ is transitive by the following steps.
    1. Assume that $m \leq n$. By definition, there is some d_0 so that $m + d_0 = n$
    2. Assume that $n \leq p$. Write out what this means. "By definition, there is some ..."
    3. Now find an e so that $m + e = p$.
    4. Write out the conclusion.
2. Show that $\leq$ is anti-symmetric by the following steps.
    1. Assume $m \leq n$. Write out what this means: "There is some d_0 so that ...."

Exercises for Lecture 5 (cont.)

2. Assume $n \leq m$. Write out what this means. "There is some d_1 so that ...."
3. Show that $d_0 + d_1 = 0$. [Think about using cancellativity.]
4. Conclude that $d_0 = 0$. [Which law justifies this?]
5. Conclude that $m = n$.

As we mentioned, $\leq$ is *linear*, meaning that for any m and n, either $m \leq n$ or $n \leq m$. A proof of this is not terribly difficult, but is more subtle than transitivity and anti-symmetry.

Lemma 3

$\leq$ is linear.

Proof: Note that we defined linearity in terms of $\leq$, but it is equivalent to saying that for any m and n, either $m < n$)or $n \leq m$. After all, if $m < n$ then $m \leq n$. And if $m \leq n$, then either $m = n$ and hence $n \leq n$, or $m < n$. A proof is by induction on m.

- [Basis] $0 + n = n$ is always true. So $0 \leq n$.
- [Inductive Hypothesis] Suppose that for some k, it is the case that either $k \leq n$ or $n \leq k$ (but we do not know which comparison is true).
- [Inductive Step] We must show that either $k^{\curvearrowright} \leq n$ or $n \leq k^{\curvearrowright}$. According to the Inductive Hypothesis, there are two cases to consider. Either $k \leq n$ or $n \leq k$. We take them in reverse.
  1. Suppose $n \leq k$. Then obviously $n \leq k^{\curvearrowright}$ (meaning, it is so obvious that we do not bother to fill in the details).
  2. Suppose $k < n$. So for some d, $k + d^{\curvearrowright} = n$. Hence $k^{\curvearrowright} + d = n$. if $d = 0$, then $k^{n}xt = n$, so $n \leq k^{\curvearrowright}$. Otherwise, $k^{\curvearrowright} < n$.

□

Exercises for Lecture 5

The following proofs should require you only to refer to the definition of $\leq$ and to the basic Laws of Arithmetic.

1. Prove that addition is **monotonic** with respect to $\leq$. This means that $m \leq n$ implies $m + p \leq n + p$ for all natural numbers m, n and p.

Exercises for Lecture 5 (cont.)

2. Prove that addition is **order reflectiing** with respect to $\leq$. This means that if $m + p \leq n + p$, then $m \leq n$.

5.2 Other Forms of Induction

Using $\leq$, we can formulate a more flexible method of proof by induction.

Suppose we wish to prove that all natural numbers are *outgrabe*. Again this is nonsense, but let's try anyway. We prove the basis with no trouble; formulate the Inductive Hypothesis; get stuck on the Inductive Step. Here is a simple idea that can help. Define a *hypergrabe* number to be a natural number k so that for every $j < k$, j is outgrabe. In other words, k does not necessarily have the property we really care about, but all the numbers below it do. Now suppose every natural number is outgrabe. Then clearly, every natural number is also hypergrabe. Likewise, if every natural number is hypergrabe, then every natural number is outgrabe. So proving either property by induction will suffice to prove the other. A proof by simple induction that all natural numbers are hypergrabe amounts to this:

- [Basis] Show that every natural number $j < 0$ is outgrabe. But since there are no such numbers, this is trivially true no matter what outgrabe happens to mean.
- [Inductive Hypothesis] Suppose that k is hypergrabe for some k. That is, suppose that for all $j < k$, j is outgrabe.
- [Inductive Step] Prove that $k^\frown$ is hypergrabe. By the Inductive Hypothesis, all $j < k$ are outgrabe. So to prove that every $j < k^\frown$ is outgrabe just amounts to proving it for k. So the Inductive Step (for proving that $k^\frown$ is hypergrabe) amounts to proving that k is outgrabe.

This can now be reformulated without mentioning *hypergrabe* at all. The Basis is not needed, because it is true automatically. The Inductive Hypothesis can be reformulated as supposing that for all $j < k$, j is outgrabe. The proof of the Inductive Step amounts to proving that k is outgrabe.

This leads to a formulation of induction that is typically called *Strong Induction*, even though it is not really any stronger (i.e., it is not able to prove more facts). A proof of property P by Strong Induction has the outline:

- [Strong Inductive Hypothesis] Suppose that $P(j)$ is true for all $j < k$.
- [Strong Inductive Step] Prove that $P(k)$ is true.

Exercises involving strong inductive proofs are not easy to come by right now. We will see a very important example when we prove that every positive natural number can be factored into primes.

Example 4

Here is an example that uses strong induction to prove something. Define Fibonnacci number f_n by the equations

$$\begin{aligned} f_0 &= 0 \\ f_1 &= 1 \\ f_{n+2} &= f_{n+1} + f_n \qquad \text{for any } n \end{aligned}$$

We claim that for all n, $2f_n \leq f_{n+2}$.

- [Strong Inductive Hypothesis] Suppose that for all $j < k$, $2f_j \leq f_{j+2}$.
- [Strong Inductive Step]. We need to show that the claim also holds for k. In case $k = 0$, this is obviously true because $2f_0 = 0$. In case $k = 1$, it is also obviously true because $2f_1 = 2 = f_3$. In all other cases $k = i + 2$ for some i. So

$$\begin{aligned} 2f_k &= 2f_i + 2f_{i+1} && \text{[By definition of } f \text{ and distributivity]} \\ &\leq f_{i+2} + f_{i+3} && \text{[By Inductive Hypothesis]} \\ &= f_k + f_{k+1} && [i + 2 = k] \\ &= f_{k+2} && \text{[By definition of } f] \end{aligned}$$

We close this section with another method for using induction that is sometimes useful.

Lemma 5

Suppose $P(-)$ is a property that makes sense for natural numbers. Suppose, furthermore, that $P(m)$ is true for some m. Then there is a smallest m for which $P(m)$ is true. That is, there is a natural number m_0 so that $P(m_0)$ and so that $P(n)$ implies $m_0 \leq n$.

Proof: Suppose $P(-)$ is a property that makes sense for natural numbers and that there is no minimal m for which $P(m)$ is true. We will show that $P(m)$ is false for all m by strong induction.

- [Strong Inductive Hypothesis] Assume that $P(j)$ is false for all $j < k$.
- [Inductive Step] We must show that $P(k)$ is also false. Suppose $P(k)$ were true. By the strong inductive hypothesis, $P(j)$ is false for all $j < k$. So k would be the smallest natural number for which $P(k)$ is true. This contradicts the assumption that there is no minimal value for which $P(m)$ is true. So $P(k)$ must not be true.

□

Exercises for Lecture 5

1. Define the "tribonacci" numbers as follows:

$$\begin{aligned} t_0 &= 0 \\ t_1 &= 1 \\ t_2 &= 2 \\ t_{n+3} &= t_{n+2} + t_{n+1} + t_n \qquad \text{for each } n \end{aligned}$$

   Prove by strong induction that $t_n < 2^{n-1}$ is true for all natural numbers n. [Recall that $2^{-1} = \frac{1}{2}$.]

2. Prove that $n^3 < 3^n$ for all natural numbers n.

5.3 Minimum and Maximum

The minimum of two numbers m and n is, of course, the smaller of the two. We write $\min(m, n)$ for this. The maximum is written as $\max(m, n)$. To make this precise, we can write a formal definition.

Definition 6

For natural numbers m and n, $\min(m, n)$ is a natural number satisfying:

- $\min(m, n) \leq m$ and $\min(m, n) \leq n$;
- for any natural number p, if $p \leq m$ and $p \leq n$, then $p \leq \min(m, n)$.

Also, $\max(m, n)$ is defined *dually*. For natural numbers m and n, $\max(m, n)$ is a natural number satisfying:

- $m \leq \max(m, n)$ and $n \leq \max(m, n)$;
- for any natural number p, if $m \leq p$ and $n \leq p$, then $\max(m, n) \leq p$.

Both min and max are characterized by what we may call an "adjoint situation".

$$p \leq \min(m, n) \iff p \leq m \text{ and } p \leq n$$
$$\max(m, n) \leq p \iff m \leq p \text{ and } n \leq p$$

This shows that comparing p to two numbers on the right is the same as comparing p to their minimum on the right; and similarly for comparison on the left and maximum. We say that $\min(m, n)$ is the *greatest lower bound* of m and n and that $\max(m, n)$ is the *least upper bound* of m and n.

Some simple facts about min and max derive directly from this characterization by adjointness. The two operations, min and max, have many useful properties, all of which can be proved using the above characterizations plus some facts about addition.

In particular, together with addition, min and max make the natural numbers into something called a *distributive lattice ordered monoid*. Basically, this means that addition together with min and max cooperate in specific ways that are akin to the basic laws of arithmetic. The most useful laws having to do with min and max are:

Laws 7

For all natural numbers m, n and p:

Commutativity

$$\min(m, n) = \min(n, m) \qquad \max(m, n) = \max(n, m)$$

Associativity

$$\min(\min(m, n), p) = \min(m, \min(n, p)) \quad \max(\max(m, n), p) = \max(m, \max(n, p))$$

Laws 7 (cont.)

Idempotency

$$\min(m, m) = m \qquad \max(m, m) = m$$

Absorption

$$\min(m, \max(n, m)) = m \qquad \max(m, \min(n, m)) = m$$

Distributivity

$$m + \min(n, p) = \min(m + n, m + p) \qquad m + \max(n, p) = \max(m + n, m + p)$$
$$\max(m, \min(n, p)) = \min(\max(m, n), \max(m, p)) \qquad \min(m, \max(n, p) = \max(\min(m, n), \min(m, p))$$

Modularity

$$m + n = \min(m, n) + \max(m, n)$$

We will not prove most of these as they follow easily from arithmetic laws. But the most subtle is worth looking at.

Lemma 8

$m + \min(n, p) = \min(m + n, m + p)$ for all $m, n, p \in \mathbb{N}$.

Proof: By definition, $\min(n, p) \leq n$. Because addition is monotonic, $m + \min(n, p) \leq m + n$. Likewise $m + \min(n, p) \leq m + p$. So $m + \min(n, p) \leq \min(m + n, m + p)$.

So to complete the proof, we must show that $\min(m+n, m+p) \leq m+\min(n, p)$. Suppose $k \leq \min(m + n, m + p)$. Then if $k \leq m$, then $k \leq m + \min(n, p)$ obviously. Otherwise, $m \leq k$ by Linearity. So $m + d = k$ for some d. Hence $m + d \leq m + n$ and $m + d \leq m + p$. Since $\leq$ is order reflecting, $d \leq \min(n, p)$. Consequently, $k = m + d \leq m + \min(n, p)$. We have thus shown that $k \leq \min(m + n, m + p)$ implies $k \leq m + \min(n, p)$. In particular, this applies to $\min(m + n, m + p)$. □

Exercises for Lecture 5

1. Calculate the following values. Show work.

Exercises for Lecture 5 (cont.)

1. $\min(5, \min(4, 6))$
2. $\min(5, \max(4, 6))$
3. $\min(340, \max(234, 340))$
4. $\min(5, \max(3, \min(\max(1, 2), 7)))$
5. $\min(5 + \max(4 + \min(3 + \max(7, 8), 3 + \min(7, 8)), 6), 7)$

2. Prove that min distributes over max.

Divisibility

Goals

Lecture

- Develop the analogue of $\leq$ defined by multiplication instead of by addition.
- Illustrate the value of the analogy to prove useful properties of divisibility.
- Introduce general division for natural numbers.

Study

- Demonstrate competence in determining divisibility and division facts.

Study

For natural numbers, $m \leq n$ *means* that $m + d = n$ for some d. Since multiplication satisfies many of the same laws (it is commutative, associative, etc.), a similar definition is possible in terms of multiplication.

Definition 1

For natural numbers m and n, say that m **divides** n, if and only if $m \cdot q = n$ for some natural number q. We write $m \mid n$ when m divides n.

We have an analogy between "m is less than or equal to n" and "m divides n." The difference is precisely that the former is defined by addition and the latter by multiplication. This is useful because we can sometimes transfer a fact about $\leq$ to a fact about $\mid$ simply by noticing that they both depend on analogous laws of arithmetic.

For example, the relation $\leq$ is reflexive *because* 0 is the identity for addition. The relation $\mid$ is reflexive because 1 is the identity for multiplication. Likewise, $\leq$ is transitive *because* addition is associative; so $\mid$ is transitive because multiplication is associative.

Anti-symmtry is also true, but a proof hints at why our analogy is not perfect. Recall that we proved that $m \leq n$ and $n \leq m$ implies $m = n$. using cancellativity of addition. But multiplication is only cancellative for non-zeros. That is, $m \cdot p = n \cdot p$ implies $m = n$ only when $p \neq 0$. This means that we need to treat 0 as a special case. Suppose $m \cdot q = n$ and $n \cdot r = m$. If $m = 0$, then obviously $n = 0$. So $m = n$. If $m \neq 0$, then $m \cdot q \cdot r = m$ and $m \neq 0$. So by cancellativity $q \cdot r = 1$, and so $q = 1$. Hence $m = m \cdot 1 = n$.

The divisibility relation begins to be more interesting when we realize that it is *not* linear. For example, 4 does not divide 13 and 13 does not divide 4. Apparently, the structure of the natural numbers with respect to $|$ is much more complicated that with respect to $\leq$.

Note that $1 \mid m$ is true for any m, simply because $1 \cdot m = m$. And $m \mid 0$ is true for any m because $m \cdot 0 = 0$. So 1 is "at the bottom" of the divisibility relation and 0 is "at the top". This may seem strange. Some people find it so irritating that they simply rule 0 out of consideration, and declare that $0 \mid 0$ is undefined. This is fine, but I prefer to understand $0 \mid 0$ to mean $0 \cdot q = 0$ for *some* q.

Figure 6 shows a fragment of the natural numbers with respect to divisibility.

Exercises for Lecture 6

For each of the following pairs (m, n) of natural numbers, determine whether or not $m \mid n$.

1. $(4, 202)$
2. $(7, 49)$
3. $(11, 1232)$
4. $(9, 19384394)$
5. $(n, 6n)$
6. $(26, 65)$

Divisibility also makes sense for integers, but it is no longer anti-symmetric for a somewhat trivial reason. For example, $5 \mid -5$ and $-5 \mid 5$, but obviously $5 \neq -5$. In short, divisibility ignores the sign of an integer. This is a good reason to concentrate our attention on natural numbers, but bear in mind that most of what we can say about divisibility is true for integers as well.

Before closing this section, we note additional facts about how $|$ interacts with arithmetic.

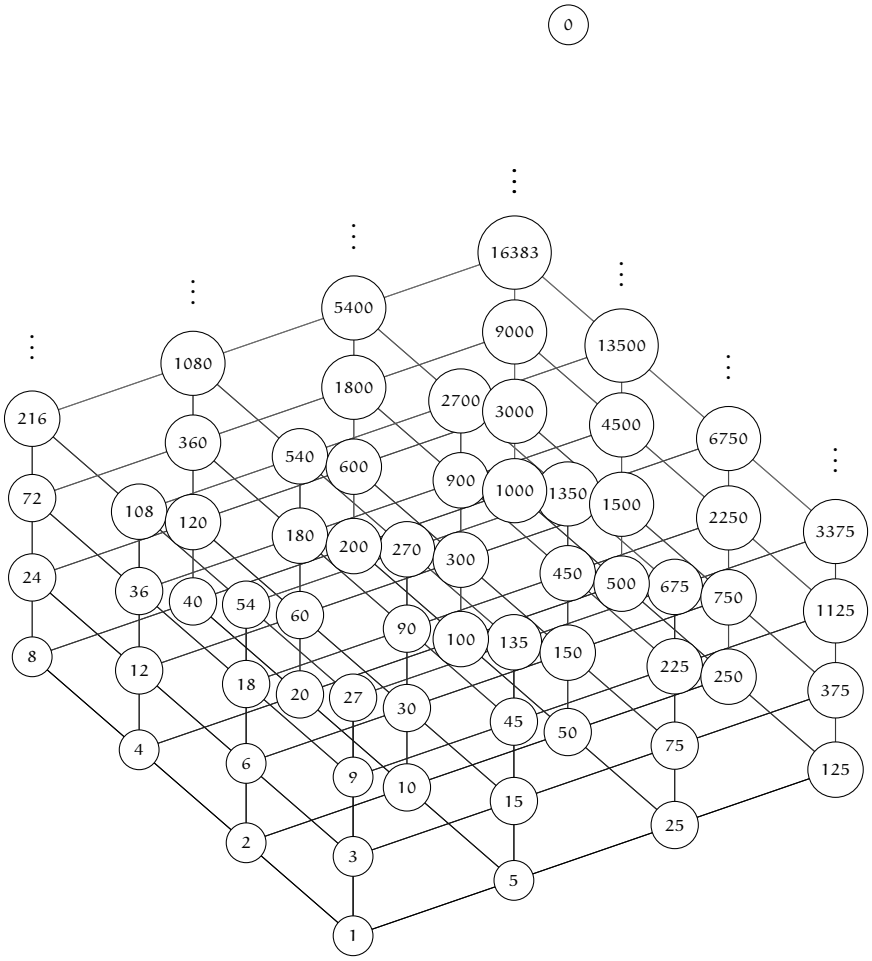


Figure 6.1: Part of the divisibility relation

Proposition 2

1. $m \mid n$ implies $m \mid np$
2. $m \mid n$ and $m \mid p$ implies $m \mid (n + p)$
3. $0 < n < m$ implies $m \nmid pm + n$

Proposition 2 (cont.)

4. $m \mid n$ and $n > 0$ implies $0 < m \leq n$.

Proof:

1. is true by associativity.
2. is due to distributivity.
3. can be proved by showing that $mq \neq pm + n$ for all q. We leave this as a voluntary exercise.
4. uses (3). That is, suppose $m \mid n$ and $n > 0$. Then we can write this as $m \mid 0 \cdot m + n$. Thus $0 < m$. And according to (3), $0 < n < m$ has to fail. Since $0 < n$ holds by assumption, $m \leq n$.

□

6.1 Quotients and Remainders

Without rational numbers, division still makes sense. We only need to account for the fact that sometimes numbers don't divide evenly. To make this work properly, we can speak of a *quotient* and *remainder*. For example, dividing 23 by 7 results in a quotient of 3 and a remainder of 2. That is, $3 \cdot 7 + 2 = 23$. Let us make this precise.

Theorem 3: Natural Number Division

For any natural number m and any positive natural number n, there is a unique pair of natural numbers q and r satisfying

$$m = qn + r$$

and

$$r < n$$

Proof: First, we prove that if q and r satisfy the stated conditions, and so do q' and r', then $q = q'$ and $r = r'$. This will prove that there can be at most one pair of natural numbers satisfying the stated conditions. Suppose $qn + r = q'n + r'$ and $r < n$ and $r' < n$. If $r < r$, then there is some positive e so that $r + e = r'$. Hence $qn = q'n + e$. But this means that $n \mid q'n + e$. Clearly, $e < n$, so is impossible. Thus it can not be the case that $r < r'$. For the same reason, it can not be the case that $r' < r$. So $r = r'$.

Theorem 3 (cont.)

Now we prove that there actually is a pair of numbers q and r satisfying the condtions. For this, we proceed by induction on m.

- [Basis] $0 = 0 \cdot n = 0$. So $q = 0$ and $r = 0$ do the job.
- [Inductive hypothesis] Assume that for some k, natural numbers p and s exist for which $k = p \cdot n + s$ and $s < n$.
- [Inductive Step] We must find q and r so that $m^\frown = q \cdot n + r$ and $r < n$. There are two cases: either $s^\frown = n$ or $s^\frown < n$. Suppose $s^\frown < n$. Then $m^\frown = p \cdot n + s^\frown$. So let $q = p$ and let $r = s^\frown$. Suppose $s^\frown = n$. Then $p \cdot n + s^\frown = p^n x \cdot n + 0$. So let $q = p^\frown$ and $r = 0$.

□

This theorem indicates that division of natural numbers works, as long as we account for both the quotient and the remainder. It is useful to have notation for both of these. So we will sometimes use the same notation for an integer divided by a positive natural number.

Definition 4

For any integer a and positive natural number n, let $a \mathbin{//} n$ denote the *quotient* and $a \bmod n$ the *remainder* of dividing a by n. That is, $a \mathbin{//} n$ and $a \bmod n$ are the unique two integers so that

$$a = (a \mathbin{//} n) \cdot n + (a \bmod n)$$

and

$$0 \leq a \bmod n < n$$

The notation // is borrowed from the programming langauge Python. It is intended to avoid confusion with real number division x/y. Python, Java, C and many other languages use a percent sign for remainder, but unfortunately, its precise meaning differs from langauge to language. The notation mod avoids this ambiguity.

Exercises for Lecture 6

1. Calculate the following:
    1. $24 // 7$
    2. $10000000 \bmod 10000001$
    3. $13 \bmod 8$

Exercises for Lecture 6 (cont.)

4. $8 \bmod 5$
5. $5 \bmod 3$
6. $3 \bmod 2$
7. $2 \bmod 1$

2. Show that for any natural number m, any positive natural number n and any positive natural number p, it is the case that $pm \mathbin{//} pn = m \mathbin{//} n$ and that $pm \bmod pn = p(m \bmod n)$.

Prime Numbers

Goals

Lecture

- Prove the Fundamental Theorem of Arithmetic
- Prove that the prime numbers are unbounded in the natural numbers.

Study

- Demonstrate competence in prime factorization.

We all know what a prime number is. It is a number that is not 1 and has no non-trivial factors. One might ask why 1 does not count as a prime number since it seems like an arbitrary thing to exclude. We settle that question here. The key insight (from an earlier lecture) is that an *empty product* is 1.

Recall that the product of a list of natural numbers is defined inductively by

- $\prod [] = 1$
- $\prod n : L = n \cdot \prod L$

Definition 1

A **prime number** is a positive natural number p so that for any list L of natural numbers, if $p \mid \prod L$ holds, then $p \mid L_i$ holds for some $i < \mathsf{len}(L)$. In other words, if p divides a product of natural numbers, it divides one of them.

With this definition, 1 is not prime for exactly the same reason that 6 is not prime. That is, 6 is not prime because, for example, $6 \mid \prod [2, 3]$ but 6 does not divide any item on the list $[2, 3]$. Likewise, $1 \mid \prod []$ but 1 does not divide any item on the list $[]$ because there are no items on the empty list. In contrast, 2 is prime because if $2 \mid \prod L$ with L being a list of natural numbers, at least one of the

items on the list must be even. It is not hard to check that this definition of primality agrees with the more familiar one.

Our first task involving primes is to remind ourselves of the *Fundamental Theorem of Arithmetic*, that every positive natural number factors uniquely into primes. We split the proof of this into two separate parts.

Lemma 2

For any positive natural number m, there is a list P consisting only of primes so that $m = \prod P$.

Proof: Here we use strong induction.

- [Strong Inductive Hypothesis] Assume that for some k, it is the case that for every $0 < j < k$, there is a list of primes P so that $j = \prod P$.
- [Strong Inductive Step] There are three cases to consider. Either $k = 1$, or $k = i \cdot j$ for some positive i and j strictly less than k, or neither of these holds.

  Suppose $k = 1$. Then we let $P = []$. This is a (trivial) list of primes whose product is k.

  Suppose $k = i \cdot j$ where i and j are both positive and strictly less than k. By the inductive hypothesis, there are lists of primes Q and R so that $i = \prod Q$ and $j = \prod R$. Hence $k = \prod Q \cdot \prod R = \prod(Q \otimes R)$.

  Suppose k is neither equal to 1, nor equal to $i \cdot j$ for any two natural numbers strictly less than k. Then k itself is prime. So $k = \prod[k]$.

  These are the only possible cases.

□

The list of primes we constructed in the Lemma 2 is called a **prime factorization of** m. Generally, a composite has more than one prime factorization for trivial reasons. For example, $[2, 3]$ and $[3, 2]$ both are prime factorizations of 6. But the *only* way two prime factorizations of the same number can differ is by the order in which the factors are listed. If we insist that our lists are sorted in increasing order, this ambiguity is avoided. That is, say P is a *sorted* list of natural numbers if $P_i \leq P_j$ whenever $i \leq j < \mathsf{len}(P)$.

Lemma 3

For every positive natural number m, there is at most one sorted prime factorization of m.

Proof: Suppose P and Q are sorted prime factorizations of m. We need to show that they are equal. We do this by structural induction on P. That is, we show that for all sorted lists of

Lemma 3 (cont.)

primes Q, if $\prod P = \prod Q$, then $P = Q$.

- [Basis] If $\prod[] = \prod Q$, then Q must also be the empty list because no non-empty list of primes has a product of 1.
- [Inductive hypothesis] Assume that, for some fixed sorted list of primes K, it is the case that for all sorted lists of primes R, if $\prod K = \prod R$, then $K = R$.
- [Inductive Step] Suppose $\prod p : K = \prod Q$ where $p : K$ and Q are sorted lists of primes. Then $p \mid \prod Q$. But p is prime, so p must appear somewhere in the list Q. There are two cases: either p is the initial item of Q, or not.

  If p is the initial element of Q, then we can write $Q = p : R$ for some list R. By cancellativity, $\prod K = \prod R$. So by the inductive hypothesis, $K = R$. So $p : K = Q$.

  On the other hand, suppose p is not the initial item on the list Q. We show that this leads to a contradiction, so the previous case is the only possibility. Since p is prime, it is somewhere on the list Q. So Q is not empty. That is, Q can be written as $q : Q'$ where q is a prime strictly less than p. But q is also prime, so it must appear somewhere on the list P. But that violates the assumption that $p : P$ is sorted, for it means that the smaller value q appears later in the list that p.

□

The two preceeding lemmas show that every positive m has a unique sorted prime factorization, typically called *the* prime factorization.

Theorem 4: Fundamental Theorem of Arithmetic

Every positive natural number has a unique sorted prime factorization.

Proof: All that remains is to the remark that if P is a prime factorization of m, then P can be sorted into increasing order. The result has the same product P because of commutativity. □

For example, 24 is factored as $[2, 2, 2, 3]$. Likewise, 800 is factored as $[2, 2, 2, 2, 2, 5, 5]$. We can get a simpler representation by listing the number of times each prime is repeated. So we can represent 800 by $[5, 0, 2]$, signifying that $800 = 2^5 3^0 5^2$. Notice that in this notation, we need the middle 0 as a "place holder" to indicate that our number does not have any 3 factors. Also notice that "trailing zeros" in this notation do not make a difference. $[5, 0, 3, 0]$ also represents 800. The extra 0 at the end simply tells us that 800 is not divisible by the next prime (7). We will investigate this notation after establishing that we have a plentiful supply of primes.

Theorem 5

There are infinitely many primes.

Proof: We prove this by showing that no finite list of primes exhausts all the possible primes.

Suppose L is a non-empty list consisting of primes. To show that L is missing a prime, consider the number $m = 1 + \prod L$. Since $\prod L \geq 1$, $m > 1$. So m has a non-empty prime factorization, say M. Clearly M does not have any item in common with L (this could be proved explicitly by induction on L). So we have found a prime number (namely, any item of M) that is missing from L. Thus L can not be an exhaustive list of all primes. □

Definition 6

We can enumerate the primes: $2, 3, 5, 7, \ldots$ in increasing order. For every natural number k, let p_k be the k^{th} prime. That is, the numbers p_k satisfy

$$p_0 = 2$$
$$p_{k\frown} = \text{the smallest prime } q \text{ so that } p_k < q$$

Notice that this is well-defined because for any m there is a prime greater than m. We would not know this if we did not know there are infinitely many primes.

Exercises for Lecture 7

1. What is p_{10}?
2. What is the prime factorization of 1440?

Using p_k, we can succinctly represent any positive natural number by a list of exponents of primes. Namely, for a list R of natural numbers, define R_{pr} (for "prime representation") to be

$$R_{pr} := \prod_{i<\mathsf{len}R} p_i^{R_i}.$$

For example, $[1, 2, 0, 2]_{pr} = 2^1 3^2 5^0 7^2 = 882$.

For a positive natural number n, let $\mathsf{PR}(n)$ denote the unique list so that $\mathsf{PR}(n)_{pr} = n$.

Recall that we defined $P \overline{+} Q$ for two lists of natural numbers by adding the items of the two lists itemwise.

$$P \overline{+} [] = P$$
$$[] \overline{+} Q = Q$$
$$m : P \overline{+} n : Q = (m + n) : (P \overline{+} Q)$$

Then it is clear (we will not give a proof) that $P_{pr} \cdot Q_{pr} = (P \overline{+} Q)_{pr}$. Also define a relation $P \preceq Q$ on lists of natural numbers by $[] \preceq Q$ always, $m : P \preceq []$ never, and $m : P \preceq n : Q$ if $m \leq n$ and $P \preceq Q$. Then $P_{pr} \mid Q_{pr}$ if and only if $P \preceq Q$.

7.1 Greatest Common Divisor and Least Common Multiple

Recall that min and max are defined in terms of $\leq$ (which is defined in terms of addition). They have analogues defined in terms of $\mid$ (which is defined in terms of multiplication).

Definition 7

For natural numbers m and n, a *common divisor of* m *and* n is a natural number c satisfying $c \mid m$ and $c \mid n$; a *greatest common divisor of* m *and* n is a natural number g so that

- g is a common divisor of m and n, and
- if p is a common divisor of m and n then $p \mid g$.

For natural numbers m and n, a *common multiple of* m *and* n is a natural number c satisfying $m \mid c$ and $n \mid c$; a *least common multiple of* m *and* n is a natural number ℓ so that

- ℓ is a common mulitple of m and n; and
- if p is a common multiple of m and n, then $\ell \mid p$.

For now, let us at least see that *if* a greatest common divisor or a least common multiple exists, then it is unique. The pattern of the proof is important because it sows up in many other places in mathematics. So it is worth noting here.

Lemma 8

For any natural numbers m and n, there is at most one greatest common divisor and at most one least common multiple.

Proof: Suppose g and g' are both greatest common divisors of m and n. Then $g \mid m$ and $g \mid n$. Since g' is a greatest common divisor, $g \mid g'$ according to the second requirement in

Lemma 8 (cont.)

the definition. Similarly, g' is a common divisor of m and n, so $g' \mid g$. But divisibility is anti-symmetric, so $g = g'$. The proof for least common multiples is *dually similar* meaning the role of "divides" is replaced by the opposite, "is divided by". □

This justifies writing $\gcd(m, n)$ for *the* greast common divisor and $\mathrm{lcm}(m, n)$ for *the* least common multiple, because if some gretest common divisor exists, it is unique and likewise for a least common multiple. So when does a greatest common divisor exist? The following proof that the answer is "always" is of practical value because it actually provides an algorithm for calculating $\gcd(m, n)$ for any m and n.

Lemma 9

For any two natural numbers m and n, $\gcd(m, n)$ exists.

Proof: Without loss of generality, we may assume that $m \leq n$ because the requirements for $\gcd(m, n)$ to exist are the same as for $\gcd(n, m)$.

To simplify the notation, we write $P(i)$ to mean that for all $j \geq i$, the greatest common divisor $\gcd(i, j)$ exists. We proceed by strong induction on to show that for all m, $P(m)$ holds.

- [Strong Inductive Hypothesis] Assume that for some natural number a it the case that for all natural numbers $k < a$, $P(k)$ holds.
- [Strong Inductive step] We must show that for every $P(a)$ holds. That is, for every $b \geq a$, the a greatest common divisor of a and b exists. Consider any $b \geq a$. We consider two cases: $a = 0$ or not. In case $a = 0$, then b can be any natural number. Evidently b divides both 0 and b. And since any natural number is a divisor of 0, b is the greatest common divisor of 0 and b.

  In case $a > 0$, the division algorithm provides a remainder $b \bmod a$. Since $b \bmod a < a$, the Strong Inductive Hypothesis ensures $P(b \bmod a)$ is true. In particular, $\gcd(b \bmod a, a)$ exists. Let $g = \gcd(b \bmod a, b)$. We claim that g is also a greatest common divisor of a and b.

  Clearly, $g \mid a$. And since $b = a \cdot (b \mathbin{/\!/} a) + (b \bmod a)$, and g divides both summands separately, $g \mid b$. So g is a common divisor of a and b. Now, suppose c divides both a and b, then c also divides $b \bmod a$. Hence $c \mid g$, because g is the greatest common divisor of $b \bmod a$ and a.

□

The proof of this lemma gives us an algorithm (a method) for calculating $\gcd(a, b)$. Namely,

$$\begin{aligned} &\gcd(0, b) \coloneqq b \\ &\gcd(a, b) \coloneqq \gcd(b \bmod a, a) && \text{for } a > 0 \end{aligned}$$

If you are interested, this translates to Python.

Algorithm 10

```
def gcd(a,b):
    if a == 0:
        return b
    else:
        return gcd(b%a, a)
```

As with gcd, we are obliged to show that $\operatorname{lcm}(m, n)$ actually exists and is unique. There are a number of ways to do this. We prove it using a direct inductive proof. It happens that, at the same time, we can prove a useful law involving gcd and lcm. Recall that min and max are related by a law we called *Modularity*: $m + n = \min(m, n) + \max(m, n)$. The analogous fact is true for gcd and lcm: $\gcd(m, n) \cdot \operatorname{lcm}(m, n) = m \cdot n$.

A lemma regarding interaction of gcd with multiplication will be helpful.

Lemma 11

For any natural numbers m and n and prime number p, $\gcd(pm, pn) = p \gcd(m, n)$.

Proof: Evidently, $p \gcd(m, n)$ divides both pm and pn. So $p \gcd(m, n)$ divides $\gcd(pm, pn)$. Assume that $m \leq n$. For a prime p, $pn \bmod pm = p(n \bmod m)$ because $pn = (pn \mathbin{//} pm)pn + pn \bmod pm$

□

Theorem 12

Any two natural numbers m and n have a unique least common multiple (denoted $\text{lcm}(m, n)$).

Proof: Uniqueness of $\text{lcm}(m, n)$ follows from the definition and the fact that divisibility is anti-symmetrtic.

So we must show that some least common multiple exists and satisfies $\gcd(m, n)\,\text{lcm}(m, n) =$

Theorem 12 (cont.)

mn.

If $mn = 0$, then the only common multiple is 0 because 0 is the only multiple of 0.

Suppose $mn > 0$. Then mn is a common multiple. So there is a smallest one (by $\leq$ ordering). Call this s. There are natural numbers s_m and s_n for which $ms_m = s$ and $ns_n = s$. We now claim that s is actually the least common multiple, not just the smallest. That is, if $m \mid p$ and $n \mid p$, then $s \mid p$.

Suppose $m \mid p$ and $n \mid p$. If $p = 0$, then $s \mid p$ in any case. Otherwise, there are natural numbers p_m and p_n so that $mp_m = np_n = p$. Also p is positive. So there are natural numbers q and r so that $p = qs + r$ and $r < s$. But this means that $p = mp_m = qms_m + r$. So $r = m(p_m - qs_m)$ is a multiple of m. Likewise, it is a multiple of n. But we chose s to be the smallest non-zero common multiple. So $r = 0$. Hence $p = qs$. This proves that $s \mid p$. $\square$