Math 507 class notes

Randall Holmes

September 29, 2020

Contents

1 Wednesday August 26th: some of which is mysterious

In the first lecture, I made a perhaps misguided attempt to give a minimal specification of what the natural numbers are, and an explanation of how the natural numbers might be implemented in terms of set theory, and then how the integers might be implemented given the natural numbers. Nothing really hinges on this, except that it does give an illustraton of the very great power of the proof method of mathematical induction.

1.1 A little about sets

I didn't say this in the lecture, but it might be useful.

We assume in this discussion some basics about sets, none of which should be too unfamiliar.

Membership is a basic notion.

Sets A and B are equal if and only if for all x, $x \in A \leftrightarrow x \in B$.

It is common to view all mathematical objects as sets, but we are leaving open the possibility that there are objects which are not sets. We require that anything which has an element is a set; we note below that there is only one set with no elements.

For any set A and property P of elements of A, there is a set

$$\{x \in A : P(x)\}.$$

Its defining axiom is that for all a, $a \in \{x \in A : P(x)\}$ iff $a \in A$ and $P(a)$.

We say $A \subseteq B$ iff A and B are sets and for any x, if $x \in A$ then $x \in B$: we read this "A is a subset of B". For any set A, there is a set $\mathcal{P}(A)$, the power set of A, whose defining axiom is $B \in \mathcal{P}(A) \leftrightarrow B \subseteq A$: this is called the power set of A, the set of all subsets of A.

For any x there is a set $\{x\}$ such that for all y, $y \in \{x\} \leftrightarrow y = x$.

For any sets A, B there is a set $A \cup B$ such that $x \in A \cup B$ iff $x \in A$ or $x \in B$ or both.

The notation $\{x_1, x_2, \ldots, x_n\}$ for a set given by listing its elements can be understood to abbreviate $\{x_1\} \cup \{x_2\} \cup \ldots \cup \{x_n\}$.

The notation $\emptyset$ refers to the empty set which can be computed as

$$\{x \in A : x \neq x\}$$

for any set A: notice that there can be only one empty set.

1.2 Basic axioms for the natural numbers

We give a minimal set of axioms for the natural numbers. We will *not* require that proofs based on this minimal set be written; we may discuss later what the book's official basic assumptions about the integers must be. We give these to demonstrate that a basic description *can* be given in limited space.

The basic assumptions are as follows

(1) 0 is a natural number

(2) If n is a natural number, $\sigma(n)$ is a natural number (this is simply the successor of n, what we usually write $n+1$, and we will not use this notation outside this introduction to basic axiomatics of the natural numbers).

(3) For any natural number n, $\sigma(n) \neq 0$. 0 is the first natural number.(3)

(4) For any natural numbers m, n, $\sigma(m) = \sigma(n) \rightarrow m = n$. Successor is one-to-one.

(5) The principle of mathematical induction: for any property $P(n)$ of natural numbers n, if we have $P(0)$ and $(\forall k \in \mathbb{N} : P(k) \rightarrow P(\sigma(k)))$, it follows that $(\forall n \in \mathbb{N} : P(n))$. The symbol $\mathbb{N}$ is used here for the set of all natural numbers.

The five basic assumptions we have just given, along with some manipulations of sets, due to Peano (and thus called the Peano axioms can be used to derive all properties of the natural numbers.

But the manipulations of sets required to define the usual operations of addition and multiplication using the very limited information we have are very sophisticated: if we add addition and multiplication as primitive notions with some axioms, the need to appeal to set constructions can be avoided in elementary arithmetic.

Our further axioms follow.

(6) If m, n are natural numbers, $m + n$ and $m \cdot n$ are natural numbers.

(7) For any natural number m, $m + 0 = m$.

(8) For any natural numbers m, n, $m + \sigma(n) = \sigma(m + n)$.

(9) For any natural number m, $m \cdot 0$.

(10) For any natural numbers m, n, $m \cdot \sigma(n) = (m \cdot n) + m$.

The reader will notice that instead of the full list of familiar rules of arithmetic, we have given recursive definitions of addition and multiplication based on the notions of zero and successor. It turns out that in combination with mathematical induction, this is enough to define all familiar notions of arithmetic and prove all familiar theorems.

We note that Peano actually had 1 as the first natural number. The

reader might want to think about what formal changes would be needed in the axioms: they are straightforward.

The familiar natural numbers are of course defined as $1 = \sigma(0); 2 = \sigma(1)$, etc. You might notice (in the interest of familiar notation) that it is very direct to prove that for any natural number n, $n+1 = n+\sigma(0) = \sigma(n+0) = \sigma(n)$.

1.3 Proving the commutative law of addition

We demonstrate the familiar commutative law "for all natural numbers m, n,

$$m + n = n + m".$$

Fix m. We prove "for all natural numbers n, $m + n = n + m$" by mathematical induction.

There are two things to prove: the basis step is $m + 0 = 0 + m$. The induction step is "If for a fixed natural number k, $m + k = k + m$, it follows that $m + \sigma(k) = \sigma(k) + m$.

We prove the basis step $m + 0 = 0 + m$ by induction (how else?) on m. The new basis is $0 + 0 = 0 + 0$, which is obvious. The new induction step is "Assuming that $k+0 = 0+k$, show that $\sigma(k)+0 = 0+\sigma(k)$". We write out the proof of the new induction step: Assume $k + 0 = 0 + k$ (the inductive hypothesis). Now $\sigma(k) + 0 =_{(7)} \sigma(k) =_{(7)} \sigma(k + 0) =_{(\texttt{ind hyp})} \sigma(0 + k) =_{(8)} 0 + \sigma(k)$. We annotated each equation with the reason for its validity (an axiom or the inductive hypothesis).

Now we have to prove the main induction step, "If for a fixed natural number k, $m + k = k + m$, it follows that $m + \sigma(k) = \sigma(k) + m$. Assume $m+k = k+m$ (inductive hypothesis). Now $m+\sigma(k) =_{(8)} \sigma(m+k) =_{(\texttt{ind hyp})} \sigma(k + m) =_{(???)} \sigma(k) + m$. Of course, this isn't a proof yet because we have a step labelled `???` which hasn't been justified. If we can prove $\sigma(k + m) = \sigma(k) + m$, which looks like axiom 8 but applied on the left instead of the right, we would complete our proof. So, we prove this lemma.

We prove $\sigma(k + m) = \sigma(k) + m$ by induction on m. The basis step is $\sigma(k + 0) = \sigma(k) + 0$. This is direct: $\sigma(k + 0) =_{(7)} \sigma(k) =_{(7)} \sigma(k) + 0$. The induction step is "Given $\sigma(k + p) = \sigma(k) + p$, we can deduce $\sigma(k + \sigma(p)) = \sigma(k) + \sigma(p)$". Notice that we have to introduce a new variable p for the induction step as the variable k is already used by the induction step this proof is embedded in! Assume $\sigma(k + p) = \sigma(k) + p$ (inductive hypothesis).

Now $\sigma(k+\sigma(p)) =_{(8)} \sigma(\sigma(k+p)) =_{(\texttt{ind hyp})} \sigma(\sigma(k)+p) =_{(8)} \sigma(k)+\sigma(p)$, which completes the verification of the missing step labelled with `???` above, and so completes the entire proof. Whew.

We are going to assume the commutative law of addition in our development of number theory, and similarly assume the validity of other basic laws of algebra, without appealing to proofs from the minimalist Peano axioms. There are two reasons to provide this kind of information: one is to remind us that we do have basic assumptions, and we need to be able to back up and work from an explicit formulation of our basic assumptions when we need to. We need to whenever the concern is raised that we might be assuming what we are trying to prove, for example. The second reason why this digression is useful is that it gives an extended example of mathematical induction, which *will* be very important in our work in this class.

1.4 Defining the natural numbers as sets

It is possible to define the natural numbers as sets and give a definition of the set $\mathbb{N}$ (whose existence will have to be assumed as an axiom in addition to our system of set theoretic assumptions above; we do not make heavy weather of this, but set theory is always in the background of advanced work in mathematics).

The usual implementation of natural numbers may look a bit weird. But any implementation will look weird. We implement 0 as $\emptyset$, the empty set. For each set x, we define $\sigma(x)$ as $x \cup \{x\}$. The effect of this is that $1 = \sigma(0) = 0 \cup \{0\} = \emptyset \cup \{0\} = \{0\}; 2 = \sigma(1) = 1 \cup \{1\} = \{0\} \bigcup \{1\} = \{0,1\}$, and generally we implement each natural number n as the set $\{0,\ldots,n-1\}$ of all smaller natural numbers. Any such definition is rather artificial (there are alternatives!): this one has the nice feature that n is a set with n elements.

We look at the axioms. Axiom 3 certainly holds: $\sigma(x) = x \cup \{x\}$ is not 0, the empty set, because it has at least x as an element. Axiom 4 requires an additional comment about our set theory: suppose $x \cup \{x\} = y \cup \{y\}$ but $x \neq y$. Then we would have to have $x \in y$ and $y \in x$. We simply rule this out as an axiom of set theory: for any sets x, y, either $x = y$ or $x \notin y$ or $y \notin x$. One way of understanding this is that we assert that sets are constructed in some order, and the elements of a set must be sets constructed before it in that order.

We arrange for axiom 5 to be true by the way we define the set $\mathbb{N}$ of

natural numbers. We say that a set I is inductive if $0 \in I$ and

$$(\forall x : x \in I \to \sigma(x) \in I).$$

We abbreviate this as $\texttt{inductive}(I)$. Note that all natural numbers should belong to an inductive set if our definitions work. Now we assert as an axiom that there is an inductive set I. We then define

$$\mathbb{N} = \{n \in I : (\forall J : \texttt{inductive}(J) \to n \in J)\}.$$

In other words, we define the set of natural numbers as the set of things which satisfy every property which can be proved by mathematical induction: we make axiom 5 true by force!

I'll spare you the formal development of addition and multiplication, unless you are curious! It can be done, and it doesn't even take up that much space, but it requires some further abstract work.

1.5 Defining the integers as sets

The book takes the integers as the basic data of number theory. It is also quite possible to take the natural numbers, or the positive natural numbers, as the basic data. But we certainly want to be able to talk about the integers. We actually assume basic familiarity with the integers and their properties, but we do briefly indicate here how we would implement them in set theory.

The basic idea is that the integers are obtained by closing up the natural numbers under subtraction.

We define a relation $\sim$ on pairs of natural numbers. $(m, n) = (r, s)$ is defined as holding if $m + s = n + r$. If we allow ourselves to peek at the back of the book, we know that this implies that $m - n = r - s$ (where $m - n$ and $r - s$ are general integers). We turn this on its head: for any natural numbers m, n, we define the integer $m - n$ as $\{(r, s) \in \mathbb{N} \times \mathbb{N} : (m, n) \sim (r, s)\}$, the equivalence class of (m, n) under the relation $\sim$. We further define $(m-n)+(m'-n')$ as $(m+m')-(n+n')$ and $(m-n)\cdot(r-s)$ as $(mr+ns)-(ms+nr)$.

There are things to prove to show that this works. One needs to prove, using properties of the natural numbers alone, that $\sim$ is an equivalence relation. One further needs to prove that the operations of addition and multiplication defined above actually have the properties expected of addition and multiplication of integers. There is a further technical irritation that the

natural number 1 (for example) and the integer 1 are not the same object. Problems with this can generally be avoided by always being careful what kind of object we are talking about. Generally, if we are not really looking at implementations of numbers as sets, we can harmlessly identify the natural numbers with the corresponding non-negative integers, and we will always do so.

1.6 The division algorithm theorem

We now take the standpoint we will usually take, that we are aware of basic properties of the natural numbers and the integers, and prove a very basic theorem. We note that this theorem itself might be regarded as one of those basic properties, so we have a little work to do to isolate what the book's basic assumptions really are (which we may or may not completely do).

Theorem: For each integer a and each integer $b > 0$, there are uniquely determined integers q, r (for quotient, remainder such that $a = bq + r$ and $0 \leq r < b$.

Proof: We first prove (*) "for each integer $a \geq 0$ and each integer $b > 0$, there are integers q, r (for quotient, remainder such that $a = bq + r$ and $0 \leq b < r$: we restrict ourselves to natural numbers a and we do not for the moment try to prove that q, r are unique.

We prove this (of course!) by induction on a. We first fix $b > 0$.

The basis step: if $a = 0$ we let $q = 0$, $r = 0$ and we do have $a = 0 = b \cdot 0 + 0 = bq + r$ and $0 \leq r < b$ because $r = 0$.

The induction step: Fix $k > 0$. We assume as the induction hypothesis that $k = bq_0 + r_0$ and $0 \leq r_0 < b$. Our goal is to show that there are q, r such that $k+1 = bq+r$ and $0 \leq r < b$. You should recognize that when we complete the proof of this induction step we will have proved (*). Note the care I take naming the witnesses to the induction hypothesis and the induction goal, which cannot harmlessly be supposed to be the same.

There are two cases: either $r_0 < b - 1$ or $r_0 = b - 1$.

If $r_0 < b - 1$ then $r_0 + 1 < b$ and we can let $q = q_0$ and $r = r_0 + 1$, and we have $k + 1 = (bq_0 + r_0) + 1 = bq_0 + (r_0 + 1) = bq + r$ and $0 \leq r = r_0 + 1 < b$.

If $r_0 = b - 1$ then let $q = q_0 + 1$ and $r = 0$ and we have $k + 1 = (bq_0 + r_0) + 1 = bq_0 + (b - 1) + 1 = b(q_0 + 1) + 0 = bq + r$, and certainly $0 \leq 0 = r < b$.

Since we get q and r with desired properties in both cases, we can always find such q, r, and the proof of (*) by induction is complete.

Now we need to generalize to all integers a, and we need to verify uniqueness of q and r.

Suppose $a < 0$. It follows that $-a \geq 0$, so we can find q_0, r_0 such that $-a = bq_0 + r_0$ and $0 \leq r_0 < b$.

There are two cases. If $r_0 = 0$, let $q = -q_0$ and let $r = 0 = r_0$. We then have $-a = -(bq_0 + r_0) = -bq_0 = bq = bq + r$ and of course $0 \leq 0 = r < b$.

If $r_0 \neq 0$, then let $q = -(q_0 + 1)$ and let $r = b - r_0$. We then have $-a = -(bq_0 + r_0) = -(b(q_0 + 1) - b + r_0) = b(-(q_0 + 1)) + (b - r_0) = bq + r$ and $0 \leq r = b - r_0 < b$ holds because $r_0 < b$ and $r_0 > 0$.

A concrete example serves to remind us of the need for caution with negative a. $100 = (3)(33) + 1$ ($a = 100, b = 3, q = 33, r = 1$). But while it is true that $-100 = (3)(-33) + (-1)$, -1 cannot be r. The correct result is $-100 = (3)(-34) + 2$.

Now we need to prove uniqueness. Suppose that $a = bq + r = bq' + r'$ and $0 \leq r' \leq r < b$ (we can choose $r \leq r'$ without loss of generality. Now observe that $0 = b(q - q') + (r - r')$. Suppose $r \neq r'$. We then have $0 < r - r' < b$. This puts $b(q - q')$ strictly between 0 and b, and so puts $q - q'$ strictly between 0 and 1, which is impossible.

Thus $r = r'$, whence we have $bq + r = bq' + r$, from which we readily get $q = q'$, so we have established that the witnesses q, r found in the proof of the division algorithm theorem are unique.

So, I have a question about this proof in the spirit of the earlier material. Can you get an idea of what basic properties of the integers we are allowing ourselves to use in this proof? I shall try at some point to make a convincing list.

2 Friday, August 28th: section 1.1 continued

2.1 The Minimality Principle

The author states and uses a different principle equivalent to Mathematical Induction. This is the Minimality Principle: any nonempty set of integers which is bounded below has a least element.

We state all these concepts precisely.

A number b is a *lower bound* for a set A iff $(\forall a \in A : a \geq b)$. Notice that a lower bound of a set can be an element of the set, if it is the smallest element.

A set A is *bounded below* if there is a number b which is a lower bound for A.

A number m is the least element of A iff $m \in A$ and m is a lower bound for A.

2.2 Re-proving the Divisibility Theorem

Any theorem which can be proved by induction can be proved using the minimality theorem and vice versa; this is a homework exercise. You should look at how he states the principle of mathematical induction as a principle about integers (basically, the starting point of the induction does not have to be 0).

We re-prove the Divisibility Theorem using the Minimality Principle (this will look more like his proof in the book.

Theorem: For every integer a and integer $b > 0$, there are uniquely determined q and r such that $a = bq + r$ and $0 \leq r < b$.

Proof: A proof using the minimality principle is of course going to use some more or less cleverly designed set which will need to be shown to be nonempty and bounded below. Here we fix an integer a and an integer $b > 0$ and consider the set $S = \{r : r \geq 0 \wedge (\exists q \in \mathbb{Z} : r = a - bq)\}$.

The set S is obviously bounded below, since all of its elements are nonnegative, so 0 is a lower bound for S.

It is slightly trickier to see that S is nonempty.

If $a \geq 0$, then $a - b0 = a \geq 0$, so $a \in S$.

If $a < 0$, then $a - b(-a) = (b-1)(-a) \geq 0$, so $(b-1)(-a) \in S$, so again S is nonempty.

Since S is nonempty it has a smallest element r_0. We know that $r_0 \geq 0$ and we know that for some integer q_0, $r_0 = a - bq_0$, so we have $a = bq_0 + r_0$.

We can also establish that $r_0 < b$. Suppose for the sake of a contradiction that $r_0 \geq b$. Then $r_0 - b \geq 0$, and further $r_0 - b = a - b(q_0 + 1)$, from which it would follow that $r_0 - b \in S$. But $r_0 - b < r_0$, and r_0 is the smallest element of S. So this is impossible and we have $r_0 < b$.

Thus we have $a = bq_0 + r_0$ with $0 \leq r_0 < b$. All that remains is to show that q_0 and r_0 are uniquely determined.

Suppose that $a = bq_0 + r_0 = bq_1 + r_1$ and that $0 \leq r_0 \leq r_1 < b$ (if we have distinct r_0 and r_1 we can assume without loss of generality that r_1 is larger).

We then have $b(q_0 - q_1) = r_1 - r_0$, and $0 \leq r_1 - r_0 < b$. Now if $q_1 - q_0 \geq 1$, we have $b(q_0 - q_1) \geq b$, and if $q_1 - q_0 < 0$, we have $b(q_0 - q_1) < 0$, so the only possibility is $q_0 - q_1 = 0$, so $q_0 = q_1$, so $a = bq_0 + r_0 = bq_0 + r_1$, so $r_0 = r_1$. This completes the proof of uniqueness.

2.3 Uniqueness of base b representations

Now I need to try to redeem myself for the very awkward production of this proof in class.

The result to be proved is that for a fixed $b > 0$ and any positive integer n, there is a unique representation of n as a sum $\Sigma_{0 \leq i \leq k} d_i b^i$, where $0 \leq d_i < b$ for each i and in addition $d_k > 0$.

We define the sentence $S(k)$ as the assertion "for each positive integer n such that $b^{k'} \leq n < b^{k'+1}$, where $k' \leq k$, there is a unique representation of n as a sum $\Sigma_{0 \leq i \leq p} d_i b^i$, where $0 \leq d_i < b$ for each i and in addition $d_p > 0$, and moreover for this unique representation we have $p = k'$".

We will show that $S(k)$ is true for each n by mathematical induction.

$S(0)$ asserts that each n with $1 \leq n < b$ can be expressed in exactly one way in the form $d_0 b^0$ with $0 \leq d_0 < b$. This is obviously true, since $d_0 = n$ works and $d_0 b^0 = n$ implies $d^0 = n$.

Now suppose that $S(k)$ is true and deduce $S(k+1)$. We need to show that n with $b^{k+1} \leq n < b^{k+2}$ has a unique representation in the form $\Sigma_{0 \leq i \leq k+1} d_i b^i$

with $0 \leq d_i < b$ for each i and in addition $d_{k+1} > 0$ (the inductive hypothesis handles all values of $k' < k+1$ already).

By the division algorithm theorem there are unique q, r such that $n = qb^{k+1} + r$ and $0 \leq r < b^{k+1}$. Note that q is not zero, because $r < b^{k+1}$ and $n = qb^{k+1} + r \geq b^{k+1}$, and $q < b$, because if $q \geq b$ we would have $qb^{k+1} \geq b^{k+2} > n$. If $r = 0$, we have $n = \Sigma_{0 \leq i \leq k+1} d_i b^i$ with $d_{k+1} = q$ and all other d_i's zero. If $r > 0$, then we have $b^{k'} \leq r < b^{k'+1}$ for some $k' \leq k$, and by inductive hypothesis we have a unique representation of r in the form $\Sigma_{0 \leq i \leq k'} d_i b^i$ with $0 \leq d_i < b$ and $d_{k'} > 0$. We can then represent n as $\Sigma_{0 \leq i \leq k+1} D_i b^i$, where $D_i = d_i$ for $i \leq k'$, $D_{k+1} = q$, and $D_i = 0$ if $k' < i \leq k$, simply because $n = qb^{k+1} + r$.

Now we have to argue that this is the only representation of n. Suppose $n = \Sigma_{0 \leq i \leq p} d_i b^i$, with $0 \leq d_i < b$ for each i and $d_p > 0$. We note first that $p < k+2$ must hold because if $p \geq k+2$ then $n = \Sigma_{0 \leq i \leq p} d_i b^i \geq d_p b^p \geq b^p \geq b^{k+2} > n$, which is absurd. We note that $p > k$, because if $p \leq k$ we have $n = \Sigma_{0 \leq i \leq p} d_i b^i \leq \Sigma_{0 \leq i \leq p} (b-1) b^p = b^{p+1} - 1 < b^{k+1} \leq n$, which is absurd. Thus $p = k+1$.

So if we have two distinct representations $n = \Sigma_{0 \leq i \leq k+1} d_i b^i$ and $n = \Sigma_{0 \leq i \leq k+1} D_i b^i$, we have $n = d_{k+1} b^{k+1} + \Sigma_{0 \leq i \leq k} d_i b^i$ and $n = D_{k+1} b^{k+1} + \Sigma_{0 \leq i \leq k} D_i b^i$, where both $\Sigma_{0 \leq i \leq k} d_i b^i$ and $\Sigma_{0 \leq i \leq k} D_i b^i$ are nonnegative and less than b^{k+1}. By the division algorithm theorem, $d_{k+1} = D_{k+1}$ and $\Sigma_{0 \leq i \leq k} d_i b^i = \Sigma_{0 \leq i \leq k} D_i b^i$. By the inductive hypothesis $S(k)$, the representations $\Sigma_{0 \leq i \leq k} d_i b^i$ and $\Sigma_{0 \leq i \leq k} D_i b^i$ are the same. So there is only one representation of n.

3 Continued Fractions

This was unfamiliar material to me. I have seen it before, but never really come to grips with it (I've read about it, but never taught it or been taught it).

Let $[r]$ represent the greatest integer $\leq r$ for a real number r.

The book uses the notation $\{r\}$ for $r - [r]$, the fractional part of r.

Now we define a finite or infinite sequence C_i^r such that $C_0^r = [r]$. If $r = [r]$, there is no C_1^r. If $r \neq [r]$ then $0 < r < 1$, so $1 < \{r\}$ and we can define C_n^r for each $n > 1$ as $C_{n-1}^{\frac{1}{\{r\}}}$. Please note that the notation C_i^r is mine: it is not in the book.

$$r = C_0^r + \cfrac{1}{C_1^r + \cfrac{1}{C_2^r + \cfrac{1}{C_3^r + \cfrac{1}{\cdots}}}}$$

should give the idea of what is happening.

It should be clear that if a number has a finite continued fraction, it is rational.

It should be clear that irrational numbers have infinite continued fractions (logically equivalent!)

It should also be obvious that if r is irrational, the sequence of convergents for r (the rational numbers r_i for which $C_j^{r_i} = C_j^r$ for each $j \leq i$ and $C_{i+1}^{r_i}$ is undefined) converges to r.

It is not perhaps entirely obvious that every rational number has a finite continued fraction, but we already have the machinery for this.

We show that computation of $C^{\frac{a}{b}}$ is basically the same thing as the Euclidean algorithm.

Let a be an integer and $b \geq 1$. We set $r_0 = a$ and $r_1 = b$.

In the Euclidean algorithm, once we have computed r_i and r_{i+1}, we stop if $r_{i+1} = 0$ and otherwise we compute q_i and r_{i+2} as the unique numbers such that $r_i = q_i r_{i+1} + r_{i+2}$ and $0 \leq r_{i+2} < 1$.

Notice that $q_0 = [\frac{a}{b}] = C_0^{\frac{a}{b}}$.

Now observe that $\frac{a}{b} = q_0 + \frac{r_2}{b}$, so we will define each $C_{k+1}^{\frac{a}{b}}$ as $C_k^{\frac{b}{r_2}}$ (because $\{\frac{a}{b}\} = \frac{r_2}{b}$, so $\frac{1}{\{\frac{a}{b}\}} = \frac{b}{r_2}$). (if $r_2 \neq 0$; if $r_2 = 0$ we are simply done).

But this is exactly how the Euclidean algorithm works: to compute stage $k+1$ of the Euclidean algorithm for a and b as the starting values is the same thing as to compute stage k of the Euclidean algorithm for b and r_2 as the starting values (if $r_2 \neq 0$; if $r_2 = 0$ we are simply done).

So the computation of the Euclidean algorithm shows that

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\cdots}}}}$$

The book gives notation for a finite continued fraction $q = \langle C_0^q, \ldots, C_N^q \rangle$, where C_{N+1}^q is undefined (i.e, we have the entire continued fraction). It relates to exercise 13 in section 1.3 to explain why C_N^q in this case will not be 1 unless $N = 0$ (and the finite continued fraction $q = \langle C_1^q, \ldots, C_N^q - 1, 1 \rangle$ will have the same value). As a hint for that last point, notice that $\langle 1, 1 \rangle = \langle 2 \rangle = 2$.

4 The Fundamental Theorem of Arithmetic

I'll give my own self-contained account of this which you can compare with the account in the book. The main difference is that I really view prime factorizations as unique, because I impose the additional condition that the primes in the factorization are presented in nondecreasing order.

A prime number is a positive integer p with exactly two positive divisors (that is, a positive integer $p > 1$ such that the positive divisors of p are exactly 1 and p).

The lemma of Euclid says that if $a|bc$ and $\texttt{gcd}(a, b) = 1$, then $a|c$.

We prove the lemma of Euclid. Because $\texttt{gcd}(a, b) = 1$ there are integers x, y such that $ax + by = 1$. So $c = 1c = (ax + by)c = acx + bcx$. $a|acx$ is obvious. $a|bcx$ follows from $a|bc$. So $a|c = acx + bcx$.

A prime factorization for us is of the form $\prod_{i=1}^{n} p_i$ where each p_i is a prime.

We argue using the minimality principle that each positive integer n has a prime factorization. We argue this using the minimality principle. If there is a positive integer with no prime factorization, then there is a smallest one N.

N cannot be a prime p because any prime p has the prime factorization $\prod_{i=1}^{1} p_i$ where $p_1 = p$.

So there are positive integers A, B with $1 < A, B < N$ such that $AB = N$ (if there were not, N would be prime). A and B have prime factorizations because N is minimal, so $A = \prod_{i=1}^{m} p_i$ and $B = \prod_{i=1}^{m} q_i$. But then $AB = \prod_{i=1}^{m+n} r_i$ where $r_i = p_i$ for $i \leq m$ and $r_i = q_{i-m}$ for $m < i \leq m + n$.

Now we make a further condition on prime factorizations: we require in $\prod_{i=1}^{n} p_i$ that the sequence of $p_i's$ be nonincreasing, that is, that for $i < j$ we have $p_i \leq p_j$. It should be clear that each prime factorization can be reordered to be nondecreasing in exactly one way. Stating and proving this fact is exceedingly annoying: defining what is meant is hard, and proving it is a nasty induction. I tried to put it here but thought better of it!

We prove that each positive integer N has exactly one nondecreasing prime factorization.

Again, we prove this by the minimality principle. Suppose that N is the smallest positive integer expressible with two different nondecreasing prime factorizations $\prod_{i=1}^{m} p_i$ and $\prod_{i=1}^{n} q_i$.

We argue that $p_1 = q_j$ for some j. Suppose otherwise for the sake of a contradiction.

We argue using this assumption that $p_1 | \prod_{i=z}^{n} q_i$ for each $z \leq n$. The basis step is direct: $p_1 | \prod_{i=1}^{m} p_i = \prod_{i=1}^{n} q_i$.

Now suppose that $p_1 | \prod_{i=k}^{n} q_i$: our goal is to show (if $k < n$) that $p_1 | \prod_{i=k+1}^{n} q_i$. $\prod_{i=k+1}^{n} q_i = q_k \cdot \prod_{i=k+1}^{n} q_i$. $\texttt{gcd}(p_1, q_k) = 1$ because p_1 and q_k are distinct primes. So by Euclid's lemma $p_1 | \prod_{i=k+1}^{n} q_i$.

So by induction $p_1 | \prod_{i=z}^{n} q_i$ for each $z \leq n$. But this is absurd, because then $p_1 | \prod_{i=n}^{n} q_i = q_n$, and so $p_1 = q_n$ contrary to hypothesis.

So in fact $p_1 = q_j$ for some j.

Now $\frac{N}{p_1}$ has the nondecreasing factorization $\prod_{i=1}^{m-1} p_{i+1}$, which is unique by minimality of N. But it also has the nondecreasing factorization $\prod_{i=1}^{n-1} q_i^*$ where $q_i^* = q_i$ for $i < j$ and $q_i^* = q_{i+1}$ for $j \leq i \leq n+1$ (the result of dropping q_j)). It is immediately clear that $m = n$. If $j = 1$, it is clear that our original factorizations were the same, because $p_1 = q_1$ and each $p_{i+1} = q_i^* = q_{i+1}$. If $j > 1$, observe that each q_i for $1 \leq i < j$ is $\leq p_1 = q_j$ because q is nondecreasing, but also $q_i = q_i^* = p_{i+1} \geq p_1$ for all such j, so in fact $q_i = p_{i+1} = p_1$ for each $i < j$. So we have $p_1 = q_1$, and we have $p_{i+1} = q_i^* = q_{i+1}$ if $i \geq j$, and if $i < j$ we have $p_{i+1} = q_{i+1} = p_1$, so the original factorizations were the same.

5 Tuesday Sept 29: in which the instructor addresses a backlog of interesting questions.

I'm planning to organize this into subsections addressing problems in past homework for which I promised to give writeups, followed by an account of the Friday lecture, which was rather creative.

5.1 problem 22, page 9 (yes, a blast from the past)

Let $\{m_i\}$ be a strictly increasing sequence of numbers such that $m_0 = 1$ and $m_i | m_{i+1}$ for all $i \geq 0$. Prove that every positive integer n can be represented uniquely in the form

$$n = \sum_{i=0}^{\infty} a_i m_i,$$

where $0 \leq a_i < \frac{m_i+1}{m_i}$ for each i.

We show by (strong) induction that for every n with $m_i \leq n < m_{i+1}$ we have a unique representation

$$n = \sum_{j=0}^{\infty} a_j m_j,$$

in which $a_i > 0$ and each a_j for $j > i$ is 0.

Certainly this is true for $i = 0$: If $m_0 = 1 \leq n < m_1$ we can set $a_0 = n > 0$ and all $a_{j+1} = 0$, and we do get a representation of n. Any sum of the form above in which some a_{j+1} is not zero will have value at least $a_{j+1}m_{j+1}$ (because all terms of the sum are nonnegative), which is greater than or equal to $m_{j+1} \geq m_1 > n$.

Now suppose that this is true for all $k \leq i$. We aim to show that it is true for $i + 1$. Let $m_{i+1} \leq n < m_{i+2}$. By the division algorithm, $n = qm_{i+1} + r$ for unique q and $0 \leq r < m_{i+1}$, and clearly $1 \leq q < \frac{m_{i+2}}{m_{i+1}}$. We must have $n < i + 1$ such that $m_n \leq r < m_{n+1}$ and so by inductive hypothesis there is a unique representation of r as

$$r = \sum_{j=0}^{\infty} b_j m_j,$$

in which $b_n > 0$ and each b_j for $j > n$ is 0. We then define a_j as b_j for $j \neq i$ and q for $j = i + 1$ to obtain a representation

$$n = \sum_{j=0}^{\infty} a_j m_j,$$

in which $a_{i+1} > 0$ and each a_j for $j > i + 1$ is 0, clearly satisfying all other conditions for such a representation. So we have shown uniqueness.

Now suppose that we have another representation

$$n = \sum_{j=0}^{\infty} a'_j m_j.$$

We observe that the remainder on division by m_{i+1} of this sum must be the same as the remainder on division by m_{i+1} of

$$r' = \sum_{j=0}^{i} a'_j m_j.$$

It is straightforward to prove by induction that for each i,

$$\sum_{j=0}^{i}(\frac{m_{j+1}}{m_j} - 1)m_j < m_{i+1},$$

whence $r' < m_{i+1}$, whence $r' = r$ by the division algorithm and each $a'_j = a_j$ for $j < i + 1$ by the inductive hypothesis with respect to uniqueness. No a_j for $j \geq i + 2$ can be greater than 0, because then $n \geq m_{i+2}$ would follow. So, again by division properties, $a'_{i+1} = q = a_{i+1}$.

I cheated by leaving you one little induction proof to do on your own, but it should not be difficult.

5.2 problem 8, p. 22

Let $\frac{a}{b}$ be a rational number which is not an integer. Prove that there exist unique integers $a_0, \ldots, a_1, \ldots, a_{N-1}, a_N$ such that $a_i \geq 1$ for $0 \leq i \leq N$ and $a_N \geq 2$ and $\frac{a}{b} = \langle a_0, \ldots, a_N \rangle$.

We know by Theorem 1.6 that every rational number $\frac{a}{b}$ has a representation as a continued fraction $\langle x_0, \ldots, x_N \rangle$ for some N. We know by the minimality principle that for each fraction $\frac{a}{b}$ there is a smallest N such that $\frac{a}{b} = \langle x_0, \ldots, x_N \rangle$ for some sequence of x_i's. Notice that N must be at least 1 if $\frac{a}{b}$ is not an integer: if we have a representation $\langle x_0 \rangle$ of $\frac{a}{b}$ then $\frac{a}{b} = x_0$, an integer.

We prove the result by induction on N: in fact, we prove the stronger result that $\frac{a}{b}$ has exactly one shortest representation as a continued fraction, which has the indicated properties. If $N = 1$, then $\frac{a}{b}$ has a representation $\langle x_0, x_1 \rangle$. If $x_1 = 1$ then $\frac{a}{b} = x_0 + \frac{1}{1}$ is an integer contrary to hypothesis. So in this case $a_N \geq 2$. Further, the representation is clearly unique. This handles the basis $N = 1$.

Now suppose the result is true for $N = k$ and we have a shortest representation of $\frac{a}{b}$ as $\langle x_0, x_1, \ldots, x_k, x_{k+1} \rangle$. $\frac{a}{b}$ then can be written as $x_0 + \frac{1}{\langle x_1, \ldots, x_{k+1} \rangle}$, in which $\langle x_1, \ldots, x_{k+1} \rangle$ is clearly uniquely determined by $\frac{a}{b}$ (it is the reciprocal of $\frac{a}{b} - [\frac{a}{b}]$) and by induction has only one shortest representation as a continued fraction, which must be of length exactly k (we are given one of length k, and if there were a shorter one we would have a shorter representaton of $\frac{a}{b}$), and which must have its last term x_{k+1} greater than equal to 2 by the inductive hypothesis.

5.3 problem 23, page 25

I leave myself a note that I might want to write my own proof of this theorem, but the one student who wrote one appears to have written it correctly, so I can defer this.

5.4 Computer experiments on Homework 3 problems

. . .will be produced, elsewhere.

5.5 Notes on the lecture of Sept 28

I used Theorem 2.6 rather differently than the author does.

Theorem 2.6 says that if m and n are relatively prime integers ($\texttt{gcd}(m,n) = 1$) then for every integer c there are unique a, b such that a is a remainder mod n and b is a remainder mod m and $am + bn = c \bmod mn$.

This tells you that there is a complete set of residues mod mn which is not quite the one you expect: the largest one is $(n-1)m + (m-1)n$, which is considerably larger than mn itself.

Suppose that a, a' are residues mod n and b, b' are residues mod m and $am + bn \equiv a'm + b'n \,\texttt{mod}\, mn$. So we have $am + bn = a'm + b'n + kmn$ so $am - a'm = b'n - bn + kmn$, so $am \equiv a'n \,\texttt{mod}\, n$ from which it follows that $a = a'$, since both are remainders mod n and m has a multiplicative inverse mod n, since they are relatively prime. Similarly $b = b'$. Thus there are mn distinct congruence classes of the form $am + bn + k\mathbb{Z}$, and these must be all of the congruence classes mod mn since there are only mn of them Thus each number has a unique congruence class mod mn which has a unique element of the form $am + bn$ with a a remainder mod n and b a remainder mod m.

I then use this to prove a special case of the Chinese Remainder Theorem.

Let m and n be relatively prime integers ($\texttt{gcd}(m,n) = 1$). Then each set of simultaneous equations

$$x \equiv a \,\texttt{mod}\, n$$

$$x \equiv b \,\texttt{mod}\, n$$

has a unique solution in mod mn arithmetic.

We determine what such an x must be using theorem 2.6. By theorem 2.6, x is equivalent mod mn to a unique number $Am + Bn$ where A is a remainder mod n and B is a remainder mod m. We then have

$$Am + Bn \equiv a \bmod m$$

$$Am + Bn \equiv b \bmod n$$

and from this it follows that $Bn \equiv a \bmod m$ and $Am \equiv b \bmod n$ must hold, so A must be $b(m^{-1} \bmod n) \bmod n$ and B must be $a(n^{-1} \bmod m) \bmod m$. Further, explicit calculation shows that these values actuall work, so the unique solution to the system of equations mod mn is explicitly

$$x = (b(m^{-1} \bmod n) \bmod n)m + (a(n^{-1} \bmod m) \bmod m)n.$$

Isn't that fun?

Then we prove that the Euler ϕ function is multiplicative, that is, that if m and n are relatively prime we have $\phi(mn) = \phi(m)\phi(n)$. We need to show that the cardinality $\phi(mn)$ of the set of remainders mod mn which are relatively prime to mn is in one to one correspondence with the set of pairs (a, b) where a is a remainder mod m which is relatively prime to m and n is a remainder mod n which is relatively prime to n: this set of pairs has $\phi(m)$ possible first elements and $\phi(n)$ possible second elements so it has size $\phi(m)\phi(n)$.

The one to one correspondence sends each c which is a residue mod mn to $(c \bmod m, c \bmod n)$. That this map is one to one is a consequence of the form of the Chinese Remainder Theorem given above: there is only one solution mod mn to $x \equiv (c \bmod m) \bmod m; x \equiv (c \bmod n) \bmod n$. We need to show that if c is mapped to (a, b) in this way, c is relatively prime to mn iff a is relatively prime to m and b is relatively prime to n. Suppose c has a nontrivial prime factor p in common with mn. Then it must have this common factor with one of m, n (Euclid's Lemma). Without loss of generality suppose c has a common factor p with m; then $(c \bmod m$ has the same common factor p with m. Thus remainders mod mn which are relatively prime to mn are mapped to pairs (a, b) where a is relatively prime to m and b is relatively prime to n. Suppose $c \bmod m$ has a nontrivial common factor with m: it immediately follows that $c = c \bmod m + km$ for some $k \in \mathbb{Z}$ has the same common factor with m and so with mn. Similarly if $c \bmod n$ has a common factor with n, it

follows that c has a common factor with mn. So the bijection is verified and $\phi(mn) = \phi(m)\phi(n)$ if m and n are relatively prime.