Class notes for Math 287 Spring 2022

Dr Holmes

March 21, 2022

I'm pulling together the files of class notes that exist. I note that I perhaps should add more discussion of logic.

Contents

The book so far has avoided talking about logic too much directly, preferring to emphasize the development of mathematics from primitive notions and axioms, with the essentials of correct reasoning being understood. Unchecked, one can spend an entire semester talking about correct reasoning in formal detail and not end up doing any correct reasoning about mathematical content...other than the logic itself, which is also mathematical content.

In these notes I will talk just a little about formal notions of mathematical logic.

1 Propositional Logic

To begin with, we view mathematical propositions as either true or false in every case, though we may not always know what the truth value is. The basic operations of propositional logic depend only on the truth values of the sentences they connect (which is not always true of the English words and phrases we use to express them) which makes truth tables appropriate for their definitions.

In this section on propositional logic, we can represent sentences as single letters $P, Q, R \ldots$: this is an unusual use of variables but you have probably seen it before.

I present a series of basic operations. For each one, I give a definition, discuss its relation to the corresponding English words or phrases, talk about how to approach proving a proposition of that form, and how to approach using a proposition of that form which you are assuming or have proved in an argument.

1.1 Not (negation) – very brief introduction

We use $\neg P$ to say that P is false, or equivalently, "It is not the case that P".

P	$\neg P$
T	F
F	T

We mention negation briefly because we use it in the discussion of methods of reasoning with other operations before we really want to discuss its own special rules.

1.2 And (conjunction)

We use $P \wedge Q$ to translate "P and Q", and it is a pretty good translation of a particular use of English "and", namely, when this word is used to connect sentences.

We succinctly define it using a truth table:

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

The uses in "John and Mary love ice cream" and "John plays tennis and badminton" can be expressed in terms of $\wedge$ but are not literally uses of $\wedge$, since this operation (which we call "conjunction") connects sentences, not noun or verb phrases. These sentences expand into "John loves ice cream and Mary loves ice cream" and "John plays tennis and John plays badminton". This sort of use of the propositional operations to connect noun or verb phrases certainly does occur in mathematical English, but traditionally we do not discuss this usage in formal logic (though we could): we suppose that such sentences are expanded as indicated.

The uses in "John and Mary carried the half ton safe" and "14 and 37 are relatively prime" are not uses of $\wedge$ at all.

To prove a conjunction proceed as follows:

Goal: Prove $P \wedge Q$.

subgoal 1: Prove P

$\vdots$

14: P

subgoal 2: Prove Q

$\vdots$

37: Q

38: $P \wedge Q$ rule of conjunction, 14,37

The line numbers are quite arbitrary. This proof strategy is supported by having the rule of conjunction,

$$\frac{\begin{array}{c} P \\ Q \end{array}}{P \wedge Q}$$

Suppose you have proved or allowed yourself to assume $P \wedge Q$. Then you can at any time pull out P or Q as further things you are entitled to assume. This is the rule of simplification, which comes in two flavors,

$$\frac{P \wedge Q}{P}$$

and

$$\frac{P \wedge Q}{Q}$$

I'm not really teaching formal line by line proofs here; what you should notice is that these formal line-by-line style rules correspond to how we would reason about an "and" sentence in English, quite precisely.

1.3 If, then (implication or conditional):

The mathematical definition of "if..., then ..." may not look like your informal understanding of this phrase. It supports reasoning rules very much like those of the English phrase, but its definition is definitely surprising.

We write "If P, then Q" as $P \to Q$, and we define it thus:

P	Q	$P \to Q$
T	T	T
T	F	F
F	T	T
F	F	T

We stipulate that whenever we state an implication in mathematics, this is what we mean.

Notice that a false statement implies any other statement, and any statement implies a true statement. To see how this disagrees with English usage: we are not entirely comfortable with the statement "If Napoleon conquered China, then 2+2=5". Under the definition given, this sentence is simply true. A brief way of expressing the discomfort we feel is that the folk notion of implication probably assumes some relation of causality or at least relevance between the two statements connected.

There are a lot of equivalent ways to state $P \to Q$. If P, then Q, Q if P, P only if Q, P is sufficient for Q, and Q is necessary for P are all fairly common expressions.

To prove $P \to Q$, the direct strategy is

Goal: Prove $P \to Q$

> **Assume:** P
>
> **Goal:** Q
>
> $\vdots$
>
> Q

Thus: $P \to Q$

Notice that the indented block where we prove Q should be ignored after we have finished the proof of $P \to Q$, because whatever is proved in it may have used the assumption P which we made only for the sake of argument.

That this method is valid we can see from the truth table. P is either true or false. If it is false, $P \to Q$ is true. So it is enough to show that if we assume P is true, it must follow that Q is true (which makes $P \to Q$ true). It is also simply a natural method of proof of an implication.

There is an alternative indirect method, proof of the contrapositive.

Goal: Prove $P \to Q$

> **Assume:** $\neg Q$
>
> **Goal:** $\neg P$
>
> $\vdots$
>
> $\neg P$

Thus: $P \to Q$

To use an implication there are two formal rules, each of which has a fancy Latin name, and each of which is pure common sense even on the folk reading of implication.

The rule of *modus ponens* says that if you have P, and you have "if P, then Q", then you have Q:

$$\frac{\begin{array}{c} P \\ P \to Q \end{array}}{Q}$$

The rule of *modus tollens* says that if you have $\neg Q$, and you have "if P, then Q", then you have $\neg P$:

$$\frac{\begin{array}{c} \neg Q \\ P \to Q \end{array}}{\neg P}$$

1.4 Or (disjunction)

The mathematical definition of "or" exactly captures one sense of English "or". $P \vee Q$ means "P or Q or both", the inclusive sense of or, and we further stipulate that in mathematical English the word "or" (not just the symbol) *always* has this meaning. Lawyers use and/or when they want to be clear that this is what they mean.

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

is the precise truth table definition.

The exclusive sense of or has its own truth table.

P	Q	$P \oplus Q$
T	T	F
T	F	T
F	T	T
F	F	F

It doesn't always have the same symbol, and we will not often if ever mention it. Computer scientists call it XOR.

We reiterate: when we say or, we always mean $\vee$, just as, when we say if/then, we always mean $\rightarrow$.

Our favorite strategy for proving an or statement looks rather like the strategy for proving an implication.

Goal: Prove $P \vee Q$

> **Assume:** $\neg P$
>
> **Goal:** Q
>
> $\vdots$
>
> Q

Thus: $P \vee Q$

If P is true, then of course $P \vee Q$ is true. If we can show that in the other case where P is false, we must have Q, then we have $P \vee Q$ iin both cases.

This proof strategy

Goal: Prove $P \vee Q$

> **Assume:** $\neg Q$
>
> **Goal:** P
>
> $\vdots$
>
> P

Thus: $P \vee Q$

also works, because disjunction is commutative. This is not a second part of the proof of $P \vee Q$: it is another way to give a complete proof.

We give an actual example of a proof of this form, from your homework

Theorem: For any integers a, b, if $ab = 0$ then $a = 0$ or $b = 0$.

Proof: Let a, b be arbitrarily chosen integers.

> **Assume:** $ab = 0$ (using the implication proof strategy)
>
> **Goal:** $a = 0$ or $b = 0$
>
> > **Assume:** $\neg a = 0$, that is, $a \neq 0$ (using the disjunction strategy)
> >
> > **Goal:** $b = 0$
> >
> > **the main argument:** Because $ab = 0$, we have $ab = a0$ (Prop 1.14) so we have $b = 0$ (multiplicative cancellation, using the assumption that $a \neq 0$)

To reassure you about what is expected, you should know that you can write this much more briefly. I am being very explicit because I am carefully explaining the logical strategy.

Here is a perfectly acceptable proof:

Theorem: For any integers a, b, if $ab = 0$ then $a = 0$ or $b = 0$.

Proof: Let a, b be arbitrarily chosen integers. Suppose that $ab = 0$. Our goal is to show $a = 0$ or $b = 0$. If $a = 0$ we are done, so suppose $a \neq 0$ and show that $b = 0$ must be true. We have $ab = 0$, so we have $ab = a0$ by prop 1.14, so we have $b = 0$ by multiplicative cancellation (using the assumption $a \neq 0$). And we are done.

There is a nice set of strategies for using not and or together. The rule of *disjunctive syllogism* in one of its forms says that if we have $P \vee Q$ and we have $\neg Q$, we get P. Commutativity of disjunction and double negation give us four different forms:

1.
$$\frac{\begin{array}{c} P \vee Q \\ \neg Q \end{array}}{P}$$

2.
$$\frac{\begin{array}{c} P \vee Q \\ \neg P \end{array}}{Q}$$

3.
$$\frac{\begin{array}{c} P \vee \neg Q \\ Q \end{array}}{P}$$

4.
$$\frac{\begin{array}{c} \neg P \vee Q \\ P \end{array}}{Q}$$

An important way to use an or statement which you have proved or assumed is *proof by cases*

Given: $P \vee Q$ (already proved or assumed)

Goal: C

Case 1: Assume P

$\vdots$

C

Case 2: Assume Q

$\vdots$

C

Thus: C

This can be presented as a rule:

$$\frac{\begin{array}{c} P \vee Q \\ P \to C \\ Q \to C \end{array}}{C}$$

To see this, notice that the proof of Case 1 above is a proof of $P \to C$ and the proof of case 2 is a proof of $Q \to C$.

We will show in the next section that we can prove the validity of this rule from rules we have already given, just for fun.

1.5 Negation:

We have given the definition already, and we have already stated many rules involving negation. But it has its own special strategies and rules.

It is convenient to introduce a special symbol $\perp$ which simply represents a false statement.

We have two basic ways to use a negative statement, apart from the ones given above.

Double negation:

$$\frac{\neg\neg P}{P}$$

and contradiction:

$$\frac{\begin{array}{c} P \\ \neg P \end{array}}{\bot}$$

These should both be common sense. The rule deducing $\neg\neg P$ from P is also valid and useful, but it can be proved from the other rules we give.

We present two proof strategies, both of which may suggest "proof by contradiction" or *reductio ad absurdum*, though I think only the second one is really that. I won't object if you call the first one proof by contradiction too.

Negation introduction (direct proof of a negative statement):

Goal: Prove $\neg P$

> **Assume:** P
>
> $\vdots$
>
> $\bot$

Thus: $\neg P$

Notice that this is simply a proof of $P \to \bot$.

Proof by contradiction (*reductio ad absurdum*. Note that this is a general proof method for statements of any form at all (the last resort):

Goal: Prove P

> **Assume:** $\neg P$
>
> $\vdots$
>
> $\bot$

Thus: P

Notice that what you are actually doing is proving $\neg\neg P$ by negation introduction and hiding an application of double negation.

There is an important thing to remember when thinking about negation in ordinary or mathematical English. We write $\neg P$, but the closest thing to this in English is "It is not the case that P" or "It is false that P", which is formal and awkward.

If P is a simple sentence, we usually negate the verb: we say "Roses aren't red", not "It is not the case that roses are red". We do the same thing in math: $a \neq b$ and $a \notin b$ instead of $\neg a = b$ and $\neg a \in b$.

If P is a complex sentence we usually apply logical transformations to move the negation to individual sentences. Instead of saying "It is not the case that roses are red and violets are blue", we say "Roses are not red **or** violets are not blue".

In symbols, here are the transformations:

$\neg(A \wedge B)$ is equivalent to $\neg A \vee \neg B$; $\neg(A \vee B)$ is equivalent to $\neg A \wedge \neg B$; $\neg(P \to Q)$ is equivalent to $P \wedge \neg Q$ (this last may be surprising because of the unusual meaning of implication in logic). The first two transformations have a name: they are called de Morgan's laws.

We prove the validity of proof by cases in rule form, just for fun, as promised.

Given: 1. $P \vee Q$

2. $P \to C$

3. $Q \to C$

Goal: C

> **Assume (4):** $\neg C$ for the sake of a contradiction
>
> **Goal:** $\bot$
>
> **(5)** $\neg P$ 2,4, modus tollens
>
> **(6)** Q 5,1 disjunctive syllogism
>
> **(7)** C modus ponens 3,6
>
> **(8)** $\bot$ 4,7 contradict each other

Thus: C by reductio ad absurdum, 4-8

2 Quantifiers

This section isn't finished. In fact, there is some stuff which belongs in the first section which I will revisit in the next lecture, and which I list here:

1. converse, inverse, contrapositive
2. the biconditional operation $\leftrightarrow$, if and only if (iff)

Let $P(x), Q(x), R(x) \ldots$ represent sentences which probably have the variable x in them.

The symbol $(\forall x \in S : P(x))$ means "For all/any/each x in the set S, $P(x)$". The symbol $\forall$ is called the universal quantifier.

The symbol $(\exists x \in S : P(x))$ means "For some x in the set S, $P(x)$" or "There exists x in the set S such that $P(x)$". The symbol $\exists$ is called the existential quantifier.

The authors like to write $(\exists x \in S$ `such that` $P(x))$ for this. I'm interested in why they want to do this, but I think the reasons are deep and I'll try not to share my thoughts about it with you too much. I will sometimes write the such that (or s.t.) but I may just write a colon in both a lot of the time.

In principle we do not need to bound our quantifiers in a set, but there is a historical reason why we are inclined to do this. I'll demonstrate with a little reasoning about the related construction of sets. $\{x : P(x)\}$ is a name for the set of all x with property P, we might say.

We would expect naively that for any a, $a \in \{x : P(x)\}$ if and only if $P(a)$.

But this statement is false. Define R as $\{x : x \notin x\}$. Then by the principle in the previous paragraph, $a \in R$ iff $a \notin a$. So $R \in R$ iff $R \notin R$. Ooooops.

In the usual systems of set theory, we fix this by restriction of the set builder notation. We allow construction of sets $\{x \in S : P(x)\}$ and assert that for any a, $a \in \{x \in S : P(x)\}$ iff $a \in S \wedge P(a)$. We allow properties to defined sets, only if these sets are carved out of previously given sets, as it were.

Now this doesn't really apply directly to quantification. We *can* for instance say $(\forall x : x = x)$, the statement that all objects without exception are equal to themselves. The usual system of set theory does in fact allow unrestricted quantifiers. But it seems safer to restrict our quantifiers to a particular kind of object collected in a (possibly infinite) set S, and we will

generally do this: when we really have to make a universal statement about absolutely everything, we will call special attention to it.

Then I spent some time talking about order of quantifiers. For purposes of these notes, I'll give just one math example.

1. $(\forall x \in \mathbb{Z} : (\exists y \in \mathbb{Z} : x + y = 0))$

2. $(\exists y \in \mathbb{Z} : (\forall x \in \mathbb{Z} : x + y = 0))$

These are two statements which differ only in the order of the leading quantifiers.

The first one is familiar. It says that for each x, there is a y such that $x + y = 0$. The choice of the y depends on x: of course the y that works is the additive inverse $-x$.

The second one is a shocking false assertion. It says that there is an integer y such that for any integer x at all, $x + y = 0$.

I gave a similar analysis of the English sentences

1. Everyone loves someone

2. Someone is loved by everyone

The usual convention (it isn't invariable in English, but we **mandate** it in mathematical English) is that the order in which we supply quantifiers in sentences like these is dictated by the order in which the relevant noun phrases appear in the sentence.

Use xLy for x loves y. Notice that it also means y is loved by x (but this rule only applies when x and y are really names for particular objects).

Everyone loves someone becomes Every human x loves some human y becomes $(\forall x \in H : (\exists y \in H : xLy))$.

Someone is loved by everyone becomes Some human y is loved by every human x becomes $(\exists y \in H : (\forall x \in H : xLy))$.

The second statement here says something much stronger than the first.

More discussion of quantifiers to come.

3 Feb 22 lecture

I don't usually put up class notes, but there is a student out of class who requested them, and the second part of today's lecture addresses things which

are not in the book. I still owe you an extension to the previous set of notes on logic, and working with sets may induce me to get on it and produce them.

The lecture had two parts, one extending the lecture before the test about strong induction and the kind of extension to recursion which gives the Fibonacci numbers, and one an introduction to basic concepts about sets.

4 Stuff about Strong Induction, Recursion, and Fibonacci-Like sequences, Feb 22 2022

I'm just going to present the examples and theorems I did rather than try to say more about general principles.

Definition: Define a sequence A by $A_1 = 2$, $A_2 = 5$, $A_{k+2} = 5A_{k+1} - 6A_k$.

Calculations: $A_3 = 5A_2 - 6A_1 = (5)(5) - (6)(2) = 13$

$A_4 = 5A_3 - 6A_2 = (5)(13) - (6)(5) = 35$

and so forth

Theorem: For each natural number n, $A_n = 2^n + 3^n$ (as is typical with induction proofs, we aren't told where this statements comes from)

Proof: We prove this by strong induction.

$A_1 = 2 = 1 + 1 = 2^0 + 3^0$, true for $n = 1$.

$A_2 = 5 = 1 + 1 = 2^1 + 3^1$, true for $n = 2$. (we use two pieces of information at the basis).

Let $k \geq 2$ be chosen arbitarily and assume for all m with $1 \leq m \leq k$ that $A_m = 2^m + 3^m$. We already know this for $k = 2$, the basis of our induction.

Our goal is to show that $A_{k+1} = 2^{k+1} + 3^{k+1}$.

We know by definition of the sequence A that $A_{k+1} = 5A_k - 6A_{k-1}$. Notice that this uses our assumption that $k \geq 2$.

Now by inductive hypothesis $5A_k - 6A_{k-1} = 5(2^k + 3^k) - 6(2^{k-1} + 3^{k-1})$.

$5(2^k + 3^k) - 6(2^{k-1} + 3^{k-1}) = (10)2^{k-1} + (15)3^{k-1} - 6(2^{k-1}) - 6(3^{k-1})$ $= 4(2^{k-1}) + 9(3^{k-1}) = 2^{k+1} + 3^{k+1}$

And this completes the proof.

Observation: You might ask...where does this come from? We give a hint...suppose we had a sequence B with $B_{k+2} = 5B_{k+1} - 6B_k$...and make a further guess, $B_k = r^k$ for some r.

$r^{k+2} = 5r^{k+1} - 6r^k$ is true (if $r \neq 0$) if and only if $r^2 = 5r - 6$, that is $r^2 - 5r + 6$, which has roots 2 and 3 which you can find by standard techniques. So the sequence of powers of 2 and the sequence of powers of 3 satisfy this recurrence relation, and it is straightforward to show that adding two sequences which have this property will give a sequence with this property.

Definition: Define $G_k = \sum_{i=1}^{k} F_k$.

Experiment: Compute the first eight terms of this sequence and look for patterns. Two were noticed by students: $G_{k+2} = G_k + G_{k+1} + 1$, and $G_k = F_{k+2} - 1$. I admit freely that I was expecting you all to notice the second one; the first one was a bonus.

It is surprising, perhaps that neither of these proofs needs strong induction. In the coming homework problems involving proofs about Fibonacci numbers, be ready to use strong induction, but also be ready to find that you need nothing more than ordinary induction.

Theorem: For all natural numbers n, $G_{n+2} = G_n + G_{n+1} + 1$

Proof: For $n = 1$, observe that $G_1 = 1, G_2 = 1 + 1 = 2, G_3 = 1 + 1 + 2 = 4$, and $G_3 = 4 = 1 + 2 + 1 = G_1 + G_2 + 1$.

Now fix a natural number k and assume $G_{k+2} = G_k + G_{k+1} + 1$ (ind hyp). The induction goal is to show that $G_{k+3} = G_{k+1} + G_{k+2} + 1$.

$G_{k+3} = \sum_{i=1}^{k+3} F_i = \sum_{i=1}^{k+2} F_i + F_{k+3}$ by the definition of summation
$= G_{k+2} + F_{k+3}$ by definition of G

$= G_k + G_{k+1} + 1 + F_{k+3}$ by ind hyp

$= G_k + G_{k+1} + 1 + F_{k+1} + F_{k+2}$ by definition of F

$= G_k + F_{k+1} + G_{k+1} + F_{k+2} + 1$ regrouping

$= \sum_{i=1}^{k} F_i + F_{k+1} + \sum_{i=1}^{k+1} F_i + F_{k+2} + 1$ definition of G

$= \sum_{i=1}^{k+1} F_i + \sum_{i=1}^{k+2} F_i + 1$ definition of summation

$= G_{k+1} + G_{k+2} + 1$ definition of G; which is what we needed.

Theorem: For all natural numbers n, $G_n = F_{n+2} - 1$

Proof: By induction. $G_1 = 2 - 1 = F_3 - 1$, so the statement is true for $n = 1$.

Fix an arbitrary natural number k. Assume that $G_k = F_{k+2} - 1$. Our goal is to show $G_{k+1} = F_{k+3} - 1$.

$G_{k+1} = \sum_{i=1}^{k+1} F_i$ definition of G

$= \sum_{i=1}^{k} F_i + F_{k+1}$ definition of summation

$= G_k + F_{k+1}$ definition of G

$= F_{k+2} - 1 + F_{k+1}$ ind hyp

$= F_{k+3} - 1$ regrouping and definition of F.

5 Introducing Sets, Feb 22, 2022

The book introduces basic concepts of sets at a level needed for success in more advanced mathematics. You may notice that they have already been using these concepts earlier.

I will take an approach which is a bit more explicit. Without too much logic (I hope) I am going to emulate the book's treatment of natural numbers by giving some primitive notions and axioms governing the notion of set.

Some objects in the mathematical world are sets. This is a primitive notion.

Sets have objects as elements. We write $a \in S$ for a is an element of S. The membership relation is a primitive notion.

Axiom of Members: If a membership relation $a \in S$ holds, we can deduce that S is a set. (It is equivalent to say that any object which is not a set has no elements).

It is common in foundations of mathematics to assume that everything is a set. We will not make this assumption, but neither will we explicitly assume that there are non-sets.

We introduce a familiar piece of notation $\{x, y\}$: this is the set whose only elements are x and y, an unordered pair (if x and y are distinct). We call a set $\{x, x\}$ a singleton and feel free to write $\{x\} = \{x, x\}$.

Axiom of Pairs: For any objects x, y (not necessarily distinct) there is a set $\{x, y\}$. For any z, $z \in \{x, y\}$ if and only if $z = x \vee z = y$.

This notation (which should be familiar to you) can be used to make an important point. Whatever elements are, they are not parts of the sets they belong to. Let a, b be distinct objects and consider the set $\{\{a, b\}\}$. This set has only one element $\{a, b\}$, so at least one of a, b does not belong to it: suppose wlog that $a \notin \{\{a, b\}\}$. So we have $a \in \{a, b\}$ and $\{a, b\} \in \{\{a, b\}\}$ but $a \notin \{\{a, b\}\}$: the membership relation is not transitive. So members of sets are not in general parts of sets: the relationship of part to whole is transitive.

There is another important relation between sets which is a much better candidate for the relation of part to whole between sets.

Definition: The relation $A \subseteq B$ is defined as holding if and only if $(\forall x \in A : x \in B)$: that is, if every element of A is an element of B.

Theorem: For any set A, $A \subseteq A$.

Theorem: If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.

Proof: Suppose that $A \subseteq B$ and $B \subseteq C$

Let x be chosen arbitrarily. Suppose $x \in A$. Our goal is to show $x \in C$.

(can you see that this is a plan to prove the Theorem?)

Since $x \in A$ and $A \subseteq B$, it follows that $x \in B$.

Since $x \in B$ and $B \subseteq C$, it follows that $x \in C$.

So we have shown that any element of A must belong to C, which is what it means for $A \subseteq C$ to be true.

The subset relation, being transitive, is a much more reasonable implementation of the idea of a *part* of a set.

This relation can be used to state the criterion for identity of sets.

Axiom of Extensionality: If A and B are sets, $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$. Equivalently, sets A and B are equal exactly if they have the same elements (every element of A is an element of B and every element of B is an element of A).

Example: We can now prove that $\{a, b\} = \{b, a\}$.

We introduce another interesting object.

Axiom of the Empty Set: There is a set $\emptyset$ such that $x \in \emptyset$ is false for any object x.

Theorem: For any set X with no elements and any set A, $X \subseteq A$ holds. In particular, $\emptyset \subseteq A$.

Proof: Suppose that X is a set with no elements. Then for any object x, if $x \in X$, $x \in A$, because a false statement implies anything. So all elements of X (none of them) are in A, so $X \subseteq A$. $\emptyset$ has no elements, so $\emptyset \subseteq A$ by the same argument.

Observation: This does **NOT** say that the empty set belongs to every set as an element.

Theorem: Suppose that X is a set with no elements. Then $X = \emptyset$. There is only one empty set.

Proof: By the previous Theorem, $X \subseteq \emptyset$ and $\emptyset \subseteq X$, so $X = \emptyset$ by the Axiom of Extensionality.

We have used sets already in this book, usually correlated with properties. The principle we are using can be expressed formally:

Axiom of Separation: Let S be a set and let $P(x)$ be a sentence expressing a property of x. There is a set $\{x \in S : P(x)\}$ such that for every a, $a \in \{x \in S : P(x)\}$ if and only if $a \in S$ and $P(a)$.

When we use the well-ordering principle to show that all numbers have some property, we are usually applying the axiom of separation. Suppose we are trying to prove that all numbers x have some property $P(x)$. Suppose not. Then there is some natural number n such that $\neg P(n)$, so the set $\{x \in \mathbb{N} : \neg P(x)\}$ is nonempty, so it has a smallest element (the least counterexample)...and then we reason to a contradiction.

Notice that the axiom of separation lets us define sets only if we are already given sets to carve them out of. We give some additional axioms which provide us with grist for our mill.

Axiom of Power Set: For any set A, there is a set $\mathcal{P}(A)$, called the power set of A, such that $B \in \mathcal{P}(A)$ exactly if $B \subseteq A$, for any B. $\mathcal{P}(A)$ can be called...the set of all subsets of A.

We look at familiar Venn diagram operations. $A \cap B$ can be defined as $\{x \in A : x \in B\}$, which exists by the axiom of separation. $A - B$ can be defined as $\{x \in A : x \notin B\}$, again provided by the axiom of separation. For unions, we need the

Axiom of Binary Union: For any sets A, B there is a set $A \cup B$ such that for any x, $x \in A \cup B$ if and only if either $x \in A$ or $x \in B$.

Using the axioms of pairing and binary union, we can construct all finite sets.

Definition: We are given the notation $\{x_1, x_2\}$ for a finite set with two elements. If we have defined the notation $\{x_1, \ldots, x_n\}$, we define $\{x_1, \ldots, x_n, x_{n+1}\}$ as $\{x_1, \ldots, x_n\} \cup \{x_{n+1}\}$.

We are given some infinite sets, such as $\mathbb{N}$. We can simply postulate this set and its axioms as earlier in the book.

We could also present an implementation. We give the original approach of Zermelo. Define 0 as $\emptyset$. Define $n+1$ (temporarily) as $\{n\}$.

Axiom of Infinity: There is a set $\mathcal{Z}$ such that $0 \in \mathcal{Z}$ and for every x, if $x \in \mathcal{Z}$ then $x+1 = \{x\} \in \mathcal{Z}$.

Definition: We say that a set I is *inductive* iff $0 \in I$ and for every x, if $x \in I$ then $x+1 = \{x\} \in I$. Notice that the axiom of infinity simply says that there is an inductive set.

Definition: Let $\mathcal{Z}$ be an inductive set. Define $\mathcal{Z}_0$ as the collection of all n such that for every inductive element I of $\mathcal{P}(\mathcal{Z})$, $n \in I$.

Theorem: Any element of $\mathcal{Z}_0$ belongs to *every* inductive set. And any object which belongs to all inductive sets belongs to $\mathcal{Z}_0$.

Proof: Let $n \in \mathcal{Z}_0$. Let J be an inductive set. Then $J \cap \mathcal{Z}$ is an inductive set and an element of $\mathcal{P}(\mathcal{Z})$. So $n \in J \cap \mathcal{Z}$. So $n \in J$.

If x belongs to every inductive set, of course it belongs to every inductive set in the power set of $\mathcal{Z}$, and so belongs to $\mathcal{Z}_0$.

The previous theorem shows that the set $\mathcal{Z}_0$ is the same set no matter what inductive set $\mathcal{Z}$ we start with, and so should have a name of its own. We might suggest $\mathbb{N}$ as its name, if we were comfortable with the construction $0 = \emptyset; 1 = \{0\}; 2 = \{1\}; 3 = \{2\}$, and so forth (and if we included 0 in the natural numbers).

We note that nowadays there is a standard definition of the non-negative integers as sets, a somewhat different one, which works equally well and has one nice property that Zermelo's definition does not have. Define 0 as $\emptyset$ and $n+1$ as $n \cup \{n\}$, and state the axiom of infinity using this operation instead of the singleton operation. This leads to the construction $0 = \emptyset; 1 = \{0\}; 2 = \{0,1\}; 3 = \{0,1,2\}$, and so forth. This has the nice property that the set we identify with n has n elements.

I'm not going to say that either of these is our official definition. I think it is much more interesting to notice that an implementation of the system of natural numbers using sets is possible, and also that more than one such

implementation is possible. We have given only a hint of the full implementation in either case, since one would also need to define the operations of addition and multiplication (which can certainly be done).

I could specifically assert the existence of further sets such as the set of rational numbers or the set of real numbers, but it turns out that just asserting the existence of an infinite set is enough to construct sets implementing these familiar number systems and basically all mathematical structures that you will study.

The set of axioms we have given here is hardly a complete set of axioms, but it ought to support most of the work that is described in this book. And I am again rather more interested in you being aware that axioms for the set concept can be presented than in the details.

6 More remarks on sets, from the Feb 24 Lecture

In this lecture, I worked directly from the set section of the Art of Proof. I'll record some comments in these notes whcih aren't directly from their text, or which I think are particularly interesting.

I note as important a general proof strategy (really, two of them):

To prove $A \subseteq B$: If A and B are sets, to prove that A is a subset of B, introduce an arbitarily chosen object x, assume $x \in A$, and then deduce $x \in B$.

To prove equality of two sets: If A and B are sets:

Goal: $A = B$

Part I: Let: x be arbitrarily chosen

Assume: $x \in A$

Goal: $x \in B$

proof steps $\vdots$

finishing part I: $x \in B$

Part II: Let: y be arbitrarily chosen

Assume: $y \in B$

Goal: $y \in A$

proof steps $\vdots$
finishing part II: $y \in A$

Notice that Part I shows $A \subseteq B$ and Part II shows $B \subseteq A$.

I discussed set definitions with expressions to the left of the colon. The sets we are allowed by the Axiom of Separation all have the form $\{x \in A : P(x)\}$. How do we explain a set like $\{7m+1 : m \in \mathbb{Z}\}$ in a way which makes it clear that we are allowed to assume this set?

$\{7m + 1 : m \in \mathbb{Z}\} = \{k \in \mathbb{Z} : (\exists m \in \mathbb{Z} : k = 7m + 1)\}$ is an explanation of this notation: it is clear that the second expression is given to us by the axiom of separation.

A general explanation where there is one variable to the left of the colon is, when $f(x)$ is an expression that we know will be in set A if x is in set B, then $\{f(x) : x \in B\}$ means $\{k \in A : (\exists x \in B : k = f(x))\}$.

A more complicated example could appear in a definition of the gcd. We could define $\texttt{gcd}(a, b)$ as $\{ax + by \in \mathbb{N} : x \in \mathbb{Z} \wedge y \in \mathbb{Z}\}$. This would expand to

$$\{k \in \mathbb{N} : (\exists x, y \in \mathbb{Z} : k = ax + by\}.$$

Notice that both variables appearing to the left of the colon in the first definition end up being existentially quantified in the body of the second set definition. It is interesting to observe that I proposed this example then looked back to see what the authors had done in their definition...and they had given the second form!

I believe that you have all been expected in the past and will be expected in the future to read set definitions with complex terms to the left of the colon; I think a detailed formal definition here would be threatening, but a couple of examples of how to explain these definitions, which I have given, should help you to see that this kind of set definition fits into the framework I am presenting.

I suggest reading the proof the authors give of proposition 5.2.

I discussed the difference between the two set definitions given in project 5.5 part b. The crucial thing to recognize is that m is a dummy variable in the definition of U, but a fixed number given before the set is defined in the definition of V, and this gives quite different results for what the sets look like.

The authors use definitions of the form $\{x : P(x)\}$ without a bounding set in defining intersection, union, and set difference. You will see above

that we avoid doing this, basically because we cannot assume for a general sentence $P(x)$ that there even *is* a set $\{x : P(x)\}$: we know that $\{x : x \notin x\}$ does not exist!

What I prefer to do is to define $A \cap B$ as $\{x \in A : x \in B\}$ (or equivalently $\{x \in B : x \in A\}$) and define $A - B$ as $\{x \in A : x \notin B\}$, both of which set constructions are justified by the axiom of separation, and then appeal to the axiom of binary unions above, and simply assert that for any A, B, there is a set $A \cup B$, and for any c, $c \in A \cup B$ if and only if $c \in A \vee c \in B$. The problem with union is that for completely general sets A, B we don't have an obvious way to define a bounding set X such that $\{x \in X : x \in A \vee x \in B\}$ is actually $A \cup B$ without in effect assuming an axiom that for any sets A, B, there is a set X of which both are subsets (the axiom of binary union does this, of course).

It isn't an error to use the notation $\{x : P(x)\}$ as long as one understands this is the set of all x such that $P(x)$...**if there is such a set**. This notation might be undefined for some sentences.

The use of the complement notation A^c is harmless as long as one understands that there is a fixed "universal set" X one has in mind from context: this is really $X - A$ for some set understood from context. We cannot really have a complement of a set A in the absolute sense, $A^c = \{x : x \notin A\}$. If we did, then $A \cup A^c$ would be the universal set V such that $x \in V$ for any x at all, and then the axiom of separation would give us the set $\{x \in V : x \notin x\}$, which we already know cannot exist.

I am expecting that you are all familiar with the method of Venn diagrams for giving visual demonstrations of relatively simple statements in set theory. I will do some examples in class on Tuesday.

The definition of the Cartesian product

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}$$

presupposes that you know what an ordered pair is. You might not even notice this (the authors do not make heavy weather of it) but it is worth noting that this concept must either be postulated or explained in terms of sets.

The basic property of ordered pairs is that $(a, b) = (c, d)$ implies $a = c$ and $b = d$. Defining (a, b) as $\{a, b\}$ would not work, because if a and b are distinct, we want (a, b) and (b, a) to be distinct, and $\{a, b\}$ is the same set as $\{b, a\}$.

In fact, it is possible to define (a, b) as $\{\{a\}, \{a, b\}\}$. To justify this requires work we will not do: one has to prove that $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$ implies $a = b$ and $c = d$, which is a bit tricky. Other definitions of the ordered pair as a set construction are also possible.

Notice that if $a \in A$ and $b \in b$ it follows that (a, b) as we have defined it is in $\mathcal{P}(\mathcal{P}(A \cup B))$, which we will write more briefly as $\mathcal{P}^2(A \cup B)$.

This allows us to show that $A \times B$ is provided by our axioms:

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}$$

$$= \{k \in \mathcal{P}^2(A \cup B) : (\exists a, b \in A \cup B : a \in A \wedge b \in B \wedge k = (a, b))\}.$$

This depends on (a, b) being defined in the particular way given: this determines the bounding set we use. Other definitions might involve different bounding sets, but in any case no additional axioms are required to get Cartesian products. Since I have given axioms for set theory, I should show the flag about this! You are not responsible for the details of this definition, but that doesn't mean it might not be good for you to read it.

7 Homework 6

1. Do project 5.3.

2. Do project 5.12.

3. Do project 5.16.

   In projects 5.12 and 5.16, if an equation is false, give a counterexample using specific finite sets for A, B, C; if an equation is true, give a Venn diagram illustration but also write a proof using the strategies outlined above. I'll do some similar examples on Tuesday to illustrate these instructions.

4. Give a Venn diagram illustration of the identity $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$: a formal proof is not expected.

5. Write the recursive definitions requested in project 5.17: statement and/or proof of versions of the de Morgan laws will carry extra credit (the proofs would be induction proofs).

   continued on next page!

6. Do project 5.21.

7. Prove the statement I gave in class: for any sets A, B, if $A \times B = B \times A$, then $A = B$ or one of A and B is empty.

   I will prove both parts of Proposition 5.20 in class Tuesday to give you an idea how to approach the last two problems.

8 March 1 lecture: Talking about functions using sets

The concept we are attempting to clarify is $f : A \to B$, f is a function from the set A to the set B.

The book gives two separate definitions of this concept. One of them is unsatisfactory because it uses vague terms; the other uses set language cleverly to reduce the concept of functions entirely to that of sets, but the problem I point out that it does not express precisely the same notion!

First definition of a function: Let A and B be sets. A function f from A to B is determined by three ingredients:

1. The set A, which is the domain of the function.
2. The set B, which is the codomain of the function.
3. A rule which determines for each element x of A a unique element $f(x)$ of B.

A typical example from your earlier mathematical experience: in calculus, we write $f(x) = x^2 + 1$ for the function which takes a (real) input and gives a (real) output $x^2 + 1$. The only thing that is given explicitly in this rule is the rule, but the context tells us what the domain and codomain are.

In this example we can bring up a related concept and point out that it is not the same as one we have listed. The *range* of the function $f(x) = x^2 + 1$ is the set of real numbers greater than or equal to 1. This is not the same as the codomain, the expected type of output of the function. This relates to the vexed issue we will talk about below.

The weakness of this definition is...what is a rule, precisely?

The second definition attempts to fix this.

Second definition of a function: A function from A to B is a subset of $A \times B$ with the property that for each $a \in A$ there is exactly one pair (a, b) such that $(a, b) \in f$. For each $a \in A$, we define $f(a)$ as the unique b such that $(a, b) \in f$.

This is a mathematically satisfactory definition of what a function is. I do not dispute that. In fact, it is my favorite definition of what a function

is. The problem in this as in many books is that it is not equivalent to the first definition, and the authors act as if it is.

The exact difficulty is that the set f implementing a function from A to B exactly captures the *rule* component of a function in the first sense, and the set of all first components of pairs in f captures the *domain* component of the function in the first sense, but it is impossible to determine what the codomain is from the subset of $A \times B$. The range of f, $\texttt{rng}(f)$, can be defined as the set of all second components of pairs belonging to f, and then any set B at all such that $\texttt{rng}(f) \subseteq B$ might be the codomain.

On page 86 in the book, there is a definition:

Definition: A function $f : A \to B$ is *surjective* if for each $b \in B$ there exists $a \in A$ such that $f(a) = b$.

This is a commonly used and important mathematical concept. But it doesn't make sense with the second definition of function, which is presumably the one the authors are using.

Let f be the calculus function $\{(x, y) \in \mathbb{R} \times \mathbb{R} : y = x^2 + 1\}$. This is clearly a function from $\mathbb{R}$ to $\mathbb{R}$, and it is not surjective, because for example there is no a such that $f(a) = 0$.

Let g be the calculus function $\{(x, y) \in \mathbb{R} \times [1, \infty) : y = x^2 + 1\}$. This is clearly a function from $\mathbb{R}$ to $[1, \infty)$, and it is surjective, because for every $b \in [1, \infty)$, $f(\sqrt{b-1}) = b$.

But f and g are exactly the same set; the same set cannot both have and not have a well-defined property. And the definition of surjection is not a valid definition, because it depends on B, and, if using the second definition, given f you cannot tell what B is.

There are two ways to fix this. Either we say that a function is a "surjection to B" (or "onto B", onto being another common word for this concept) so that the missing B is supplied, or we define a function in such a way that the codomain is actually a component.

A standard approach is to define a function f as an ordered triple (A, B, G) where A is a set, B is a set, and G is a subset of $A \times B$ such that for each $a \in A$ there is exactly one pair in G with first component a. We then refer to A as the domain of f, B as the codomain of f, and G as the graph of f.

I have to admit I am not quite sure how I will handle this. If I have occasion to talk about onto maps (surjections) I can avoid difficulty by explicitly saying what the maps are onto. I can show the flag by talking about subsets

of $A \times B$ as graphs of functions $f : A \to B$ without necessarily being explicit about whether I think the graph is the same thing as the function. Most of the time it will make no difference. But precise and consistent definitions are part of what is taught in this course: it causes me pain that this otherwise excellent book falls into this common and unnecessary sloppy error.

The book does very little with this concept in this section. I asked you in class about counting the functions from A to B for small finite sets A and B, presenting them in arrow diagram form and indicating whether they are one-to-one (injections) or onto the intended codomain (surjections). I give definitions to support homework questions along these lines:

one-to-one: A function f from A to B is one to one or an injection just in case for any $x, y \in A$, if $f(x) = f(y)$ then $x = y$ (or, equivalently, if $x \neq y$, it follows that $f(x) \neq f(y)$).

onto (B): A function $f : A \to B$ is onto (B) or a surjection (to B) if for each $b \in B$ there exists $a \in A$ such that $f(a) = b$.

9 March 3 lecture: Talking about relations using sets; equivalence relations and partitions

I'm going to give a more general definition of what a relation is than the book does.

Definition of relation?: A relation R from A to B is a subset of $A \times B$. We write $a\,R\,b$ for $(a, b) \in R$.

Definition of relation?: A relation R is a triple (A, B, G) such that A is a set, B is a set, and $G \subseteq A \times B$. We call A the domain of R, B the codomain of R, G the graph of R, and write $x\,R\,y$ for $(x, y) \in G$.

This is different from the definition in the book in two ways. I am more general in allowing different domain and codomain. A relation from A to A I'll call a relation on A just as the book does. The tension between forms of the definition exists because the domain A (and codomain B if it is distinct) cannot actually be deduced from the graph of the relation.

In this section the only kind of relation we are discussing is an equivalence relation. An equivalence relation is a relation E from A to A such that

1. E is reflexive: for every $a \in A$, $a\,E\,a$
2. E is symmetric: for every $a, b \in A$ if $a\,E\,b$ then $b\,E\,a$.
3. E is transitive: for every $a, b, c \in A$, if $a\,E\,b$ and $b\,E\,c$ then $a\,E\,c$

The problem I have with the author's way of presenting the definition is that whether a relation on A is reflexive depends on what A is: the relation $\{(1, 1), (2, 2), (3, 3)\}$ is reflexive (and an equivalence relation) on $\{1, 2, 3\}$ but not on $\{1, 2, 3, 4\}$. And for a general relation on A, one cannot tell what the domain of the relation is from its graph: there might be objects in the intended domain which do not have the relation to anything, as in this example.

There are two ways to fix this: one can either use the second definition of what a relation is, which adds the domain as a component of the function, or one can always say "equivalence relation on A" and identify relations with

their graphs: then $\{(1,1),(2,2),(3,3)\}$ is an equivalence relation on $\{1,2,3\}$ but not an equivalence relation on $\{1,2,3,4\}$.

Most of the time the issue simply won't arise. We will see what style we settle on.

An equivalence relation E on A generally expresses the idea that the objects related by it are the same in some respect. The relation on the members of the class of having the same birthday is an equivalence relation, for example.

An equivalence relation E on A divides A into sets which we call "equivalence classes":

Definition: If $a \in A$ and E is an equivalence class on A, we define $[a]_E$ (which may be written just $[a]$ if we know what relation we are talking about) as $\{x \in A : x\,E\,a\}$.

So the equivalence classes in a section of Math XXX under the relation of having the same letter grade on Test I would be no more than five sets, for each student the set of students with the same letter grade as theirs.

We give an extended account of defining a relation, verifying that it is an equivalence relation, and describing its equivalence classes, which is closely related to the application of these ideas which will follow.

Definition: We define the relation E on the integers: $x\,E\,y$ iff $x - y$ is divisible by 3.

Theorem: E is an equivalence relation on the set of integers.

Comment: A proof of such a statement follows a natural strategy: we need to show that the relaiton is reflexive symmetric and transitive, and the definition of each of these properties suggests a logical setup.

Proof: First we show that E is reflexive. What we need to show is that for any integer x, $x - x$ is divisible by 3. Let x be chosen arbitrarily. $x - x = 0$ and 0 is divisible by 3, finishing this part.

Now we show that E is symmetric. Let x, y be arbitrarily chosen integers. Assume that $3|(x - y)$ Our goal is to show that $3|(y - x)$. Pause: do you see that this is a strategy to prove that E is symmetric?

Since $3|(x - y)$ there is an integer k such that $3k = x - y$. It follows that $y - x = -(x - y) = -3k = 3(-k)$, so $y - x$ is divisible by 3.

Now we show that E is transitive. Let x, y, z be arbitrarily chosen integers. Assume $3|(x-y)$ and $3|(y-z)$. Our goal is to show $3|(x-z)$: this will establish that E is transitive.

Because $3|(x-y)$ and $3|(y-z)$ we have integers k, l such that $3k = x-y$ and $3l = y-z$. Then $x - z = (x-y) + (y-z) = 3k + 3l = 3(k+l)$, so $x - z = 3(k+l)$ is divisible by 3.

This completes the proof that E is an equivalence relation.

Having shown that E is an equivalence relation, we might ask what is the same about two numbers that stand in this relation. In short, they have the same remainder on division by 3. The equivalence classes are $[0] = \{\ldots, 0, 3, 6, 9, \ldots\}$, $[1] = \{\ldots, 1, 4, 7, 10, \ldots\}$, $[2] = \{\ldots, 2, 5, 8, 11, \ldots\}$ there are no other equivalence classes, though of course every integer has an equivalence class: $[5] = [2]$ for example.

Some theorems about equivalence classes which I proved in class. In everything that follows, E is an equivalence class on A, and $[a]$ is shorthand for $[a]_E$.

Theorem: $a \in [a]$

Proof: $a\,E\,a$, because E is reflexive, so $a \in \{x \in A : x\,E\,a\} = [a]$. Notice that this shows that every equivalence class is nonempty.

Theorem: $a\,E\,b \leftrightarrow [a] = [b]$

Proof: Let $a, b \in A$ be chosen arbitrarily.

To prove that $[a] = [b]$ implies $a\,E\,b$, assume $[a] = [b]$. Observe that $a \in [a]$ (previous theorem) so $a \in [b]$ (hypothesis) so $a \in \{x \in A : x\,E\,b\}$ (definition of $[b]$) so $a\,E\,b$.

To prove that $a\,E\,b$ implies $[a] = [b]$ we assume $a\,E\,b$ then argue that $[a] = [b]$. For this we need our strategy for proving that two sets are equal.

Assume $x \in [a]$: we need to show that $x \in [b]$. Since $x \in [a] = \{y \in A : y\,E\,a\}$, we have $x\,E\,a$. We also have $a\,E\,b$ so by transitivity we have $x\,E\,b$, so we have $x \in \{y \in A : y\,E\,b\} = [b]$.

Now assume $x \in [b]$ and show that this implies $x \in [a]$: $x \in [b]$ implies $x\,E\,b$, so $b\,E\,x$ (symmetry) and we have $a\,E\,b$ and so $a\,E\,x$ by transitivity, and so $x\,E\,a$ by symmetry, and so $x \in [a]$.

This completes the proof. Part of the purpose of the exercise is to recognize both that this is a proof, and that at every step I did what the situation naturally called for (this was not pulled out of the air).

Theorem: For any $a, b \in A$, either $[a] = [b]$ or $[a] \cap [b] = \emptyset$ (any two equivalence classes are either identical or disjoint).

Proof: If $[a] \cap [b] = \emptyset$ is true, we are done. So let's suppose that $[a] \cap [b] \neq \emptyset$ and show that $[a] = [b]$ must follow.

Because we have assumed that $[a] \cap [b] \neq \emptyset$ we can postulate an element x of $[a] \cap [b]$ (this is a useful general principle: if we suppose a set nonempty, we can conjure up an element of it).

$x \in [a] \cap [b]$ implies $x \in [a]$ and $x \in [b]$ (definition of intersection)

thus $x \, E \, a$ and $x \, E \, b$ (def of equivalence classes)

thus $a \, E \, x$ and $x \, E \, b$ (symmetry)

thus $a \, E \, b$ (transitivity)

thus $[a] = [b]$ (previous theorem)

and we are done.

Definition: Let A be a set. We say that $P \subseteq \mathcal{P}(A)$ (a collection of subsets of A) is a partition of A just in case

1. each set $B \in P$ is nonempty
2. For any $B, C \in P$, either $B = C$ or $B \cup C = \emptyset$
3. For any $a \in A$, there is $B \in P$ such that $a \in B$

Claim 1: We have already shown that for any equivalence relation E on A, the set $\{[a]_E : a \in A\}$ is a partition of A. I will ask you to give the (very short) justification that this is the case, using theorems proved above.

Claim 2: If P is a partition of A, define $x \equiv_P y$ as $(\exists B \in P : x \in B \wedge y \in B)$. Prove that $\equiv_P$ is an equivalence relation on A. I outlined this in intuitive terms during lecture.

The two claims establish an exact correspondence between equivalence relations on A and partitions of A.

10 Homework 7

1. How many functions are there from $\{a, b, c\}$ to $\{1, 2\}$? List all of them. You may use arrow diagrams or explicit lists of ordered pairs. Which of them are one-to-one? Which of them are onto $\{1, 2\}$?

2. How many functions are there from $\{a, b\}$ to $\{1, 2, 3\}$? List all of them. You may use arrow diagrams or explicit lists of ordered pairs. Which of them are one-to-one? Which of them are onto $\{1, 2, 3\}$?

3. How many functions are there from $\{1, 2, 3\}$ to $\{1, 2, 3\}$ which are onto $\{1, 2, 3\}$? List all of them. You may use arrow diagrams or explicit lists of ordered pairs. Which of them are one-to-one?

4. Verify claim 1. The verification of each part of the proof that the set of equivalence classes under E is a partition is straight from one of our theorems.

5. Verify claim 2.

6. Do all parts of project 6.7. For each part indicate whether the relation has each of the three properties defining an equivalence relation (reflexive, symmetric, transitive).

7. We define a relation on $\mathbf{N} \times \mathbf{N}$ (the set of pairs of positive integers). $(x, y)SD(z, w)$ is defined as holding iff $x + w = y + z$.

   Prove that SD is an equivalence relation. What is the same about (x, y) and (z, w) if they stand in this relation?

11 3/8/2022: the Division Algorithm and the Euclidean Algorithm

I talked about computational things to do with the integers (mostly with the positive natural numbers).

First, I talked about the familiar operation of division: as it is taught in elementary school, with whole number quotients and remainders.

Division Algorithm: Let a be an integer and b be a positive integer. Then there are uniquely determined integers q and r such that $a = bq + r$ and $0 \leq r < b$.

Proof: We prove this for nonnegative a by induction on a.

Fix $b > 0$.

Basis step: let $a = 0$.

$q = 0$ and $r = 0$ will work: $0 = a = b0 + 0$.

And the only way that $0 = a = bq + r$ can be true with $0 \leq r < b$ is if $q = 0$ and $r = 0$: we would have $bq = -r$ and since b is positive, if q were not zero we would have either $bq \geq b$ or $bq \leq -b$, and $-b < -r < b$ makes this impossible. Of course, if $0 = a = b0 + r$, we have $r = 0$.

Induction step: Fix a nonnegative integer k. Suppose that there are unique q', r' with $0 \leq r' < b$ such that $k = bq' + r'$. We want to show that there are unique q, r such that $k + 1 = bq + r$ and $0 \leq r < b$.

If $r' < b - 1$, then let $q = q'$, $r = r' + 1$ and we have the desired result. $qb + r = q'b + r' + 1 = k + 1$, and $0 < 1 \leq r' + 1 = r < b$.

If $r' = b - 1$, then let $q = q' + 1$, $r = 0$ and we have the desired result. $qb + r = (q' + 1)b + 0 = q'b + b = q'b + r' + 1 = k + 1$ and $0 \leq 0 = r < b$ is obvious.

Now if $qb + r = k + 1$ and $1 \leq r < b$, we have $qb + (r - 1) = k$ and still $0 \leq r - 1 < b$, so by ind hyp $q = q'$ and $r - 1 = r'$, so $q = q', r = r' + 1$ when $r' < b$.

If $qb + r = k + 1$ and $r = 0$, then $(q - 1)b + (b - 1) = k$ and we have $0 \leq b - 1 < b$, so by ind hyp $q - 1 = q'$ and $b - 1 = r'$, so $q = q' + 1$ and $r = 0$ when $r' = b - 1$.

In both cases, we have verified uniqueness of q and r.

This proof differs from what I did in class in proving uniqueness at the same time as existence.

Now the proof of existence and uniqueness of q and r when $a < 0$: if $a < 0$ then $-a > 0$, so there are unique q' and $0 \leq r' < b$ such that $-a = bq' + r'$. If $r' = 0$ we get $-a = b(-q') + r' = b(-q')$ and we can set $q = -q'$ and $r = r' = 0$. If $r' > 0$ we get $-a = b(-q' - 1) + (b - r')$. Notice that $0 \leq b - r' < b$ in this case. So we set $q = -q' - 1$ and $r = b - r'$.

For uniqueness, if $-a = bq + r$ with $r = 0$, we have $a = b(-q) + 0$ so in fact $-q = q'$ and we have the same values as above. If $-a = bq + r$ with $r > 0$ then $a = b(-q) + (-r) = b(-q - 1) + b - r$ and we must have $-q - 1 = q'$ and $b - r = r'$ by the uniqueness of q' and r' from which $q = -q' - 1$ and $r = b - r'$ as above.

Definition: For a an integer and b a positive integer, we define $a\texttt{div}b$ and $a\texttt{mod}b$ as the unique q and r such that $a = bq + r$ and $0 \leq r < b$.

Note about calculation: Note that (for positive a) you can compute $a\texttt{div}b$ by dividing a by b and throwing out what occurs after the decimal point. Then $a\texttt{mod}b = a - b(a\texttt{div}b)$. This is how to compute remainders with a limited calculator.

Now we discuss the greatest common divisor (gcd) a concept for which the author gives a definition which seems to have little to do with the words in the phrase "greatest common divisor".

If a, b are integers, not both equal to 0, the author defines $\texttt{gcd}(a, b)$ as the smallest element of the set $\{ax + by : x \in \mathbb{Z} \wedge y \in \mathbb{Z} \wedge ax + by > 0\}$. It is straightforward to show that this set is nonempty if one of a, b is not zero.

The natural definition goes as follows: a common divisor of a, b is an integer d such that $d|a$ and $d|b$. Notice that if $a \neq 0$, any divisor of a is less than $|a|$: this means that there is an upper bound $\texttt{max}(|a|, |b|)$ on common divisors of a, b if a, b are not both zero, and this in turn means that there is a largest common divisor of a, b, because any nonempty set of integers with an upper bound has a largest element. and this is what we mean by $\texttt{gcd}(a, b)$.

That these two definitions are equivalent is a substantial theorem.

That a nonempty set of integers which has an upper bound has a largest element is worth proving. Suppose A is a nonempty set and b is an upper bound for A: this means $(\forall x \in A : x \leq b)$. Notice that this implies $(\forall x \in A : x \leq b + 1)$: $b + 1$ is then a strict upper bound for A. Now consider the

set $S = \{(b+1) - x : x \in A\}$. S is a nonempty set of positive integers and so has a smallest element m. To make a long story short, $m = (b+1) - g$ for some $g \in A$, by the definition of S, and this g must be the largest element of A.

If a, b are not both zero, the set of common divisors of a and b is nonempty, because it contains 1, and it is bounded above by $\texttt{max}(|a|, |b|)$, so it has a largest element, and this we call $\texttt{gcd}(a, b)$.

Now we state and justify two facts about the gcd, using the natural definition.

$\texttt{gcd}(a, 0) = |a|$. This is obvious. We will usually be working with positive integers, for which $\texttt{gcd}(a, 0) = a$.

$\texttt{gcd}(a, b) = \texttt{gcd}(b, a\texttt{mod}b)$. This requires a supporting argument. We prove this by showing that $\{d \in \mathbb{Z} : d|a \wedge d|b\}$ and $\{d \in \mathbb{Z} : d|b \wedge d|a\texttt{mod}b\}$ are the same set, so of course they have the same largest elements, and this proves the result.

If $d|a$ and $d|b$ then $d|b$ (of course) and $d|a\texttt{mod}b$ because $a\texttt{mod}b = a = b(a\texttt{div}b)$: anything which goes into both a and b will go into a number of the form $a - qb$ where q is an integer.

If $d|b$ and $d|a\texttt{mod}b$ then $d|a$ because $a = b(a\texttt{div}b) + a\texttt{mod}b$ and anything going into both b and $a\texttt{mod}b$ will go into both terms of this sum. Of course $d|b$.

So we have shown that these two sets are equal, and so that their maxima, the two gcds, are equal.

This gives a procedure for evaluating $\texttt{gcd}(a, b)$: define a sequence by $r_1 = a; r_2 = b; r_{k+2} = r_k\texttt{mod}r_{k+1}$ for each k, or r_{k+2} is undefined if $r_{k+1} = 0$. Notice that if r_{k+2} exists, it must be smaller than r_{k+1}, because $c\texttt{mod}d$ is always less than d. Since the sequence always gets smaller (after r_2 at least) it must eventually end in an $r_n = 0$ by the well-ordering principle. The second fact about gcd's tells us that $\texttt{gcd}(r_k, r_{k+1}) = \texttt{gcd}(r_1, r_2) = \texttt{gcd}(a, b)$ for every k. So $\texttt{gcd}(r_{n-1}, r_n) = r_{n-1} = \texttt{gcd}(a, b)$: the last nonzero term of this sequence will be the gcd.

This procedure is called the *Euclidean algorithm*.

A stronger version of the Euclidean algorithm can be used to show that for any a, b, not both zero, there are integers x, y such that $ax + by = \texttt{gcd}(a, b)$.

What we do is show how to compute x_i and y_i such that $ax_i = by_i = r_i$ for each i: then a_{n-1} and b_{n-1} are what we are looking for.

Define x_1 as 1 and y_1 as 0. Notice that $ax_1 + by_1 = a = r_1$.

Define x_2 as 0 and y_2 as 1. Notice that $ax_2 + by_2 = b = r_2$.

Now define $x_{k+2} = x_k - x_{k+1}(r_k \texttt{div} r_{k+1})$ and $y_{k+2} = y_k - y_{k+1}(r_k \texttt{div} r_{k+1})$.

Assume as inductive hypothesis that $ax_i + by_i = r_i$ for $i < k+2$.

$ax_{k+2} + by_{k+2} = ax_k - ax_{k+1}(r_k \texttt{div} r_{k+1}) + by_k - by_{k+1}(r_k \texttt{div} r_{k+1}) = (ax_k + by_k) - (ax_{k+1} + by_{k+1})(r_k \texttt{div} r_{k+1}) =$ [by ind hyp] $r_k - r_{k+1}(r_k \texttt{div} r_{k+1}) = r_k \texttt{mod} r_{k+1} = r_{k+2}$.

So since, if n is the last term of the r sequence, $r_n = 0$, we have $r_{n-1} = \texttt{gcd}(a, b)$, it follows that $ax_{n-1} + by_{n-1} = \texttt{gcd}(a, b)$.

This computational procedure is called the extended Euclidean algorithm. It is an exact description of the tables I draw: the first three columns have at row i the numbers r_i, x_i, y_i (and I write $r_{i-2} \texttt{div} r_{i-1}$ in the third column at and after row 3).

This in turn allows us to justify the assertion that $\texttt{gcd}(a, b)$ is the smallest positive number of the form $ax + by$ with x, y integers. We have just shown that $\texttt{gcd}(a, b)$ is a positive number of this form. Now, since it goes intq a and goes into b, it must go into every number $ax + by$. No positive number less than $\texttt{gcd}(a, b)$ can have $\texttt{gcd}(a, b)$ as a divisor, so in fact no positive number less than $\texttt{gcd}(a, b)$ can be of the form $ax + by$.

12 3/10/2022: Modular arithmetic, elementary definitions and results

We developed basic definitions and theorems of modular arithmetic, which provide applications of both the abstract machinery of equivalence relations and the division algorithm (and will give applications of the extended Euclidean algorithm, as we will soon see).

Definition: Fix an integer $n > 1$. For integers x, y, we define $x \equiv_n y$ (also written $x \equiv y (\texttt{mod}\, n)$) as holding iff $n|(x - y)$. We say in English, x is congruent to y mod n.

Theorem: $\equiv_n$ is an equivalence relation.

Proof: We first prove that $\equiv_n$ is reflexive. $x \equiv_n x$ is true iff $n|(x - x)$, which is true because $n|0$ is true.

Then we prove that $\equiv_n$ is symmetric. Suppose that $x \equiv_n y$. Our goal is to prove $y \equiv_n x$. Since $x \equiv_n y$, so $n|(x - y)$, there is an integer k

such that $x - y = kn$, Now this implies that $y - x = (-k)n$ and so is divisible by n, and so $y \equiv_n x$.

Then we prove that $\equiv_n$ is transitive. Suppose that $x \equiv_n y$ and $y \equiv_n z$. Our goal is to show $x \equiv_n z$. Since $x \equiv_n y$ there is an integer k such that $x - y = kn$. Since $y \equiv_n z$ there is an integer l such that $y - z = ln$. It follows that $x - z = (x - y) + (y - z)$ [this is the clever bit] $= kn + ln = (k + l)n$ is divisible by n, so $y \equiv_n z$.

An equivalence relation is to be thought of as saying that objects in its domain standing in this relation are the same in some way. We show what is the same about x, y if $x \equiv_n y$:

Theorem: $x \equiv_n y$ if and only if $x \,\texttt{mod}\, n = y \,\texttt{mod}\, n$.

Proof: The proof has two parts, like the proof of any if and only if statement.

First, suppose that $x \equiv_n y$. Our goal is to show that $x \,\texttt{mod}\, n = y \,\texttt{mod}\, n$.

By the division algorithm, $x = (x\texttt{div}n)n + x\texttt{mod}n$ and $y = (y\texttt{div}n)n + y\texttt{mod}n$. So $x - y = (x\texttt{div}n - y\texttt{div}n)(n) + (x\texttt{mod}n - y\texttt{mod}n)$. This is divisible by n (and so $x \equiv_n y$) exactly if $(x\texttt{mod}n - y\texttt{mod}n)$ is divisible by n. The difference of two nonnegative integers less than n can only be divisible by n if they are equal (try proving this!) and so if $x \equiv_n y$ we must have $(x\texttt{mod}n - y\texttt{mod}n) = 0$ and so $x \,\texttt{mod}\, n = y \,\texttt{mod}\, n$.

Second, suppose that $x \,\texttt{mod}\, n = y \,\texttt{mod}\, n$. Our goal is to show that $x \equiv_n y$.

We have $x = (x\texttt{div}n)n + x\texttt{mod}n$ and $y = (y\texttt{div}n)n + y\texttt{mod}n$ Thus, as above,

$$x - y = (x\texttt{div}n - y\texttt{div}n)(n) + (x\texttt{mod}n - y\texttt{mod}n)$$

$= (x\texttt{div}n - y\texttt{div}n)(n)$ (because $x \,\texttt{mod}\, n = y \,\texttt{mod}\, n$) and this is divisible by n, so $x \equiv_n y$.

Equivalence relations determine a partition of their domain into equivalence classes. In the case of $\equiv_n$, we partition the integers into n equivalence classes, one for each remainder mod n (classes $[0], [1], \ldots, [n-2], [n-1]$). We could write these classes $[k]_{\equiv_5}$, but we can tell what the intended equivalence relation is from context.

For $n = 5$ for example we have
$[0] = \{\ldots, -10, -5, 0, 5, 10 \ldots\}$
$[1] = \{\ldots, -9, -4, 1, 6, 11 \ldots\}$
$[2] = \{\ldots, -8, -3, 2, 7, 12 \ldots\}$
$[3] = \{\ldots, -7, -2, 3, 8, 13 \ldots\}$
$[4] = \{\ldots, -6, -1, 4, 9, 14 \ldots\}$

The class $[k]$ exists for any integer k, but it will be the same as $[k \texttt{mod} 5]$, one of these four classes. For example, [19] is another name for [4].

The objects of the mathematical system called mod n arithmetic, or $\mathbb{Z}_n$, are the equivalence classes under $\equiv_n$. What makes this an interesting mathematical system is that addition and multiplication have natural definitions on this system, which is the content of the following

Theorem: Suppose $x \equiv_n x'$ and $y \equiv_n y'$. Then $x + y \equiv_n x' + y'$ and $xy \equiv_n x'y'$.

Proof: Because $x \equiv_n x'$ and $y \equiv_n y'$ we have $x' - x$ and $y' - y$ divisible by n, so for some integers k, l we have $x' = x + kn$ and $y' = y + ln$.

Now $(x' + y') - (x + y) = (x + kn + y + ln) - (x + y) = kn + ln$ which is divisible by n. so $x + y \equiv_n x' + y'$.

Also, $x'y' - xy = (x + kn)(y + ln) - xy = xln + ykn + kln^2$, which is divisible by n, so $xy \equiv_n x'y'$.

The careful reader might notice that we are freely using the fact that the equivalence relation is symmetric.

Definition: For sets of integers A, B, we define $A + B = \{a + b : a \in A \wedge b \in B\}$ and $AB = \{ab : a \in A \wedge b \in B\}$. We only use this definition in the special case where the sets are equivalence classes mod a fixed n (at least, that is the only way we use it here: it is not an unusual definition).

Theorem: Fix $n > 1$ and let $[x], [y]$ be equivalence classes mod n. Then $[x] + [y] = [x + y] = [(x + y) \texttt{mod} n]$ and $[x][y] \subseteq [xy] = [(xy) \texttt{mod} n]$.

Proof: Any element of $[x] + [y]$ is of the form $x' + y'$ where $x' \in [x]$ and $y' \in [y]$ so $x' \equiv_n x$ and $y' \equiv_n y$, and by the theorem above this means that every element of $[x] + [y]$ is congruent mod n to $x + y$ and belongs to $[x + y]$. Any element of $[x + y]$ is congruent mod n to $x + y$, so is

of the form $(x+y)+kn$, so is of the form $x+(y+kn)$, the sum of a number congruent mod n to x and a number congruent mod n to y, and so an element of $[x]+[y]$, so we have shown that $[x+y]=[x]+[y]$.

Any element of $[x][y]$ is of the form $x'y'$ where $x' \in [x]$ and $y' \in [y]$ so $x' \equiv_n x$ and $y' \equiv_n y$, and by the theorem above this means that every element of $[x][y]$ is congruent mod n to xy and belongs to $[xy]$. But we can't show in general that any element of $[xy]$ can be expressed as the product of an element of $[x]$ and an element of y: $[xy]$ will have prime numbers in it for example which cannot typically be expressed as such a product. (I said this wrong in class: this is a correction).

Definition: We define $[x]+[y]$ as $[x+y]$ and (re!)define $[x][y]$ as $[xy]$. In the case of each operation, if I take x' from $[x]$ and y' from $[y]$, all results of applying the operation to x' and y' will end up in the same equivalence class, so this definition works.

Notice that subtraction $[x]-[y]$ can also be defined as $[x-y]$. We will have an notion of division in modular arithmetic, but it will be defined quite differently.

We give an example of the computation of addition and multiplication tables for a modulus, namely, $n=5$.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$*$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Notice that each number mod 5 has an additive inverse: the additive inverse of 0 is 0, the additive inverse of 1 is 4, the additive inverse of 2 is 3, the additive inverse of 3 is 2, the additive inverse of 4 is 1. In a general

modulus, the additive inverse of x a nonzero remainder on division by n will be $n-x$: obviously $n-x \equiv_n -x$ and for x a nonzero remainder, $n-x$ is also a nonzero remainder. This is not surprising: the integers mod n are derived from the integers and inherit the additive inverse property from the system of integers.

More surprisingly, each nonzero remainder has a *multiplicative* inverse. We merely note this here for mod 5: this will turn out to be true in general for moduli which are prime. 1 has multiplicative inverse 1, 2 has multiplicative inverse 2 ($2 \cdot 3 = 1$), 3 has multiplicative inverse 2, 4 has itself as its multiplicative inverse.

It is easy-ish to see that systems of modular arithmetic have the properties of commutativity and associativity of each operation, distributivity, identities for both operations and the additive inverse property.

We show an example of the failure of the multiplicative cancellation property of the integers:

In mod 6 arithmetic, $(3)(2) \equiv_6 0$ and $(0)(2) \equiv_6 0$, with $2 \not\equiv_6 0$, but $3 \not\equiv_6 0$.

In the integers, if $ac = bc$ and $c \neq 0$ then we must have $a = b$. This does not work in mod 6 arithmetic.

Even more striking is the fact that $(3)(2) \equiv_6 0$ illustrates that the zero factorization property of the integers fails in mod 6 arithmetic.

We will have more to say about this in the next lecture.

13 Homework 8

1. (old business, I forgot to put this in an earlier assignment) Do project 4.30 and project 4.31: these are induction proofs involving the Fibonacci numbers, and I do want you to be able to do these kinds of problems. You might notice that there was a proof of this kind in this week's notes!

2. Evaluate each of the following expressions if it is possible to do so, and explain why it is not possible if it is not.

   $200\texttt{div}3, 200\texttt{mod}3, (-200)\texttt{div}3, (-200)\texttt{mod}3, 200\texttt{div}(-3), 200\texttt{mod}(-3)$

3. Find x and y such that $137x+111y = \texttt{gcd}(137, 111)$, using the extended Euclidean algorithm. Your paper should show work following my table

format. I strongly suggest that you do this by hand, and only after that check using the spreadsheet. You will need to be able to carry out this procedure efficiently on the next exam, several times, using a nongraphing calculator, so you should practice.

4. Do the same thing as in the previous problem but for larger numbers: Find x and y such that $54321x + 12345y = \texttt{gcd}(54321, 12345)$

5. Construct the addition and multiplication tables for mod 11 arithmetic, and make a table of multiplicative inverses of the nonzero remainders in mod 11 arithmetic, using your multiplication table.

6. Find the square roots of 1 in mod 11 arithmetic. These should be exactly what you expect, if you think carefully. Now find the square roots of 1 in mod 8 arithmetic. List them all. Do you find something disturbing about this?

7. This question is about square roots of -1. Notice that $n - 1 \equiv_n -1$: in mod n arithmetic, when we talk about -1, the additive inverse of 1, we are actually talking about the remainder $n - 1$.

   This question is an exploration. In each system of modular arithmetic for $n = 2$ to 20, see if there is a square root of -1. Just to help you see what is meant, there is one in mod 5 arithmetic, since $2^2 = 4 \equiv_5 -1$. Notice that 3 is also a square root of -1 in mod 5 arithmetic.

   If you can see a pattern to which moduli have square roots of -1, I will be impressed.

14 March 16: Division and Exponentiation in Modular Arithmetic

In this lecture, we talked about more mathematical operations in modular arithmetic. I noted above that in mod 5 (for example) every nonzero number has a multiplicative inverse, so in fact it is possible to *divide*. I give a general discussion of the situations under which division is possible in modular arithmetic.

First we prove a couple of theorems using the EEA (extended Euclidean algorithm) which you might think would normally be proved using facts

about prime factorization; in fact, it is quite the reverse: the proof of the basic results about primes actually depend on EEA...

Theorem (Euclid's Lemma): If p is a prime and $p|ab$, then either $p|a$ or $p|b$.

Observation: It is not true for general natural numbers n that $n|ab$ implies that either $n|a$ or $n|b$: for example, $6|24 = 3 \cdot 8$, but $6 \nmid 3$ and $6 \nmid 8$.

Proof of Euclid's Lemma: If $p|a$, we are done. So suppose $p \not| a$ and we will show that $p|b$ has to be true.

Since $p \not| a$ and p is prime, $\texttt{gcd}(a, p) = 1$ (the only positive divisors of p are 1 and p, so these are the only possible values of the gcd, and the value p is ruled about because $p \not| a$).

By the EEA, there are integers x and y such that $ax + py = 1$.

Now $b = 1b = (ax + py)b = abx + byp$. abx is divisible by ab which is divisible by p. byp is divisible by p. So $b = abx + byp$ is divisible by p, which completes the proof.

Theorem: If $\texttt{gcd}(m, n) = 1$ and $n|mx$ then $n|x$. This is a more general result which has Euclid's Lemma as a special case.

Proof: Since $\texttt{gcd}(m, n) = 1$, we have integers u and v such that $mu+nv = 1$. So $x = 1x = (mu + nv)x = mxu + nvx$. mxu is divisible by mx which is divisible by n. nvx is divisible by n. Thus $x = mxu+nvx$ is divisible by n.

Theorem (multiplicative inverses in modular arithmetic): Let $n > 1$. Suppose $\texttt{gcd}(m, n) = 1$. Then there is an a such that $am \equiv_n 1$. Moreover, if $am \equiv_n 1$ and $a'm \equiv_n 1$ then $a \equiv_n a'$: each equivalence class mod n whose members are relatively prime to n has a unique multiplicative inverse in our system of modular arithmetic.

Proof: Because $\texttt{gcd}(m, n) = 1$, there are integers a, b such that $ma+nb = 1$. It follows that $ma \equiv_n 1$.

Now suppose that $ma \equiv_n 1$ and $ma' \equiv_n 1$. It follows that $ma = 1 + kn$ for some integer n and $ma' = 1 + k'n$ for some integer k', from which it follows that $ma - ma' = kn - k'n$ is divisible by n.

So we have $n|m(a-a')$ and by the previous theorem, since $\texttt{gcd}(m,n) = 1$, it follows that $n|(a-a')$ so $a \equiv_n a'$.

Definition: We define $m^{-1}\,\texttt{mod}\,n$ as the unique remainder mod n such that $mn \equiv_n 1$, if there is one (this exists if and only if $\texttt{gcd}(m,n) = 1$).

Remarks: Please note that the proofs of each of these three theorems are examinable: they could appear on Test II.

The proof shows us not only that each m has a unique multiplicative inverse, but also shows how to compute it (using the EEA).

Example 1: Compute $12^{-1}\texttt{mod}137$

r	x	y	q
137	1	0	
12	0	1	
5	1	-11	11
2	-2	23	2
1	5	-57	2

From this calculation, we see that $(5)(137)+(-57)(12) = 1$, so $(-57)(12) \equiv_{137} 1$. -57 is not a remainder mod 137; add 137 to get the value 80 of $12^{-1}\texttt{mod}137$.

Check: $(80)(12) = 960 = 1 + 7(137) \equiv_{137} 1$.

Example 2: Solve $5x \equiv_{123} 12$.

Observe that 5 is relatively prime to 123, so it has a multiplicative inverse mod 123. Multiplying both sides of the equation by $5^{-1}\texttt{mod}123$ will give the result, and this is actually a familiar mathematical procedure, though in an unfamiliar system: to solve $ax = b$. divide both sides bt a.

r	x	y	q
123	1	0	
5	0	1	
3	1	-24	24
2	-1	25	1
1	2	-49	1

This calculation shows that $(2)(123) + (-49)(5) = 1$, so $(-49)(5) \equiv_{123} (74)(5) \equiv_{123} 1$.

Thus if $5x \equiv_{123} 12$ we have $x \equiv_{123} (74)(5x) \equiv_{123} (74)(12) = 888 \equiv_{123} 888 - 7(123) = 27$.

We check: $27 \cdot 5 = 135 = 123 + 12 \equiv_{123} 12$.

Now we look at exponentation (computation of $a^b \texttt{mod} n$). Since exponentiation is repeated multiplication, we do have that $(a^b \texttt{mod} n \equiv_n (a \texttt{mod} n)^b \texttt{mod} n$. Simple examples show that we cannot reduce the exponent b mod n in the same way we can reduce the base a.

For example, $2^2 \texttt{mod} 10 = 4 \equiv_{10} 4$, but $2^{12} = 4096 \equiv_{10} 6$, so though we have $2 \equiv_{10} 12$ we do not have $2^2 \equiv 2^{12}$.

Nonetheless, we can effectively compute powers in modular arithmetic with very large exponents. We give two examples.

Example 1: Compute $17^{256} \texttt{mod} 100$.

One thing we are doing which makes this example easier is using mod 100: all we have to do to find the remainder mod 100 of a positive integer is take the last two digits.

The other thing which makes this a relatively easy problem is that the exponent is a power of 2, which gives a hint of our approach to computing powers with general exponents in modular arithmetic.

$17^2 = 289 \equiv_{100} 89$

$17^4 \equiv_{100} 89^2 = 7921 \equiv_{100} 21$

$17^8 \equiv_{100} 21^2 = 441 \equiv_{100} 41$

$17^{16} \equiv_{100} 41^2 = 1681 \equiv_{100} 81$

$17^{32} \equiv_{100} 81^2 = 6561 \equiv_{100} 61$

$17^{64} \equiv_{100} 61^2 = 3721 \equiv_{100} 21$

$17^{128} \equiv_{100} 21^2 = 441 \equiv_{100} 41$

$17^{256} \equiv_{100} 41^2 = 1681 \equiv_{100} 81$

17^{256} is a number with probably at least 500 digits, and it would be an enormous calculation to determine it and then extract its last two digits. We have done much less work here, by this method of repeated squaring.

An exponent which is a power of 2 makes an exceptionally easy example but we can actually do this for any exponent, with one more computational observation.

Example 2: Compute $17^{355} \texttt{mod} 100$

In this example we stick with the easy modulus of 100 to minimize the work of computing remainders. We start by setting up the powers we will compute, by starting with the exponent 355 and successively dividing it by two, throwing away remainders, until 1 is reached.

$17^{355} = (17^{177})^2(17) \equiv_{100} 77^2(17) = 100793 \equiv_{100} 93$

$17^{177} = (17^{88})^2(17) \equiv_{100} 41^2(17) = 28577 \equiv_{100} 77$

$17^{88} = (17^{44})^2 \equiv_{100} 21^2 = 441 \equiv_{100} 41$

$17^{44} = (17^{22})^2 \equiv_{100} 89^2 = 7921 \equiv_{100} 21$

$17^{22} = (17^{11})^2 \equiv_{100} 33^2 = 1089 \equiv_{100} 89$

$17^{11} = (17^5)^2(17) \equiv_{100} 57^2(17) = 55233 \equiv_{100} 33$

$17^5 = (17^2)^2(17) \equiv_{100} 89^2(17) = 134657 \equiv_{100} 57$

$17^2 = 289 \equiv_{100} 89$

$17^1 = 17$

Notice that we handle odd exponents by squaring the previous exponent and adding one more factor equal to the base (in this case one more factor of 17). This allows calculation of any exponent. The number of multiplications is proportional to the log base 2 of the exponent. Notice that no number larger than the cube of the base is ever computed.

An example in full generality (we will see some in RSA computations in the next section) is a bit harder than this because in the general case one has to compute remainders on division by numbers less convenient than 100.

15 March 18: Euler's Theorem about exponentiation in modular arithmetic, and the RSA encryption algorithm

There were two topics in the March 18 lecture, Euler's Theorem on efficient evaluation of exponentials in modular arithmetic, and a description of the

RSA cryptosystem, a practical application of the mathematics we have been discussing and, I think, a nice capstone to this unit before we switch to continuous mathematics after the break.

We begin with a definition of a concept you would see more about in classes in number theory or related subjects:

Definition (Euler phi function): For each positive integer n, we define $\phi(n)$ as the number of elements in the set

$$\{m \in \mathbb{Z}^+ : m \leq n \wedge \texttt{gcd}(m, n) = 1\}.$$

Another way of putting this is that $\phi(n) = 1$ and for each $n > 1$, $\phi(n)$ is the number of remainders mod n which are relatively prime to n, or equivalently, the number of equivalence classes mod n whose elements are relatively prime to n.

Notice that for any prime p, $\phi(p) = p - 1$. $\phi(10)$, for example, is 4, the number of elements in the set $\{1, 3, 7, 9\}$.

Lemma: If p and q are primes, $\phi(pq) = (p - 1)(q - 1)$.

Proof of Lemma: The remainders mod pq which are *not* relatively prime to pq are 0, $q - 1$ positive multiples of p, and $p - 1$ positive multiples of q, so there are $pq - 1 - (p - 1) - (q - 1) = pq - p - q + 1 = (p - 1)(q - 1)$ remainders mod pq which are relatively prime to pq.

Euler's Theorem: For each $n > 1$, for each a with $\texttt{gcd}(a, n) = 1$, $a^{\phi(n)} \equiv_n 1$.

Proof of Euler's Theorem: Consider the product $\prod_{0<i<n\wedge\texttt{gcd}(i,n)=1} ai$ of all the products of remainders mod n which are relatively prime to n with a.

This product is equal to $a^{\phi(n)} \prod_{0<i<n\wedge\texttt{gcd}(i,n)=1} i$ by pulling out the factor of a from each of the $\phi(n)$ factors ai of the original product,

This product is also equivalent mod n to $\prod_{0<i<n\wedge\texttt{gcd}(i,n)=1} ai\texttt{mod}n$, obviously.

Less obviously, $\prod_{0<i<n\wedge\texttt{gcd}(i,n)=1} ai\texttt{mod}n = \prod_{0<i<n\wedge\texttt{gcd}(i,n)=1} i$, because these two products are in fact products of the same numbers in a different order. The factors $ai\texttt{mod}n$ in the first product are all different

because we have

$$ai \equiv_n aj \rightarrow (a^{-1}\texttt{mod}n)ai \equiv_n (a^{-1}\texttt{mod}n)aj \rightarrow i = j,$$

and of course each ai is relatively prime to n since both a and each i are so, from which it follows that both these products are the same, the product of all the remainders mod n which are relatively prime to n.

We give an example. If $n = 10$ and $a = 3$, $\prod_{0<i<10\wedge\texttt{gcd}(i,n)=1} 3i\texttt{mod}10 = 3 \cdot 9 \cdot 1 \cdot 7 = 1 \cdot 3 \cdot 7 \cdot 9 = \prod_{0<i<10\wedge\texttt{gcd}(i,n)=1} i\texttt{mod}10$. The products are the same but in a different order.

It follows from the calculations above that $a^{\phi(n)} \prod_{0<i<n\wedge\texttt{gcd}(i,n)=1} i \equiv_n \prod_{0<i<n\wedge\texttt{gcd}(i,n)=1} i$, and since $\prod_{0<i<n\wedge\texttt{gcd}(i,n)=1} i$ is relatively prime to n, it has a multiplicative inverse mod n, and we can multiply both sides of the congruence by this inverse to get $a^{\phi(n)} \equiv_n 1$..

Corollary (Fermat's Little Theorem): If p is a prime and $p \not| a$, then $a^{p-1} \equiv_p 1$. This follows immediately from Euler's Theorem because $\phi(p) = p - 1$ and $p \not| a \rightarrow \texttt{gcd}(a, p) = 1$.

Observation: This implies that $a^b \equiv_n (a\texttt{mod}n)^{b\texttt{mod}\phi(n)}$, which allows more efficient calculation of exponentials, at least for small n than is supported by the method of completed squaring.

Now we have all the setup we need to describe the RSA cryptosystem, our final topic in this unit of our class on number theory. Though it might not be evident from anything we have said so far, this is applied math. The number theory we have been talking about is the basis of modern public-key cryptography. We are going to describe the oldest of the modern public key ciphers, proposed in 1978, which made number theory a branch of applied mathematics.

The distinguishing characteristic of public key cryptography is that the method of sending me a secure message is public, and the message can be transmitted over public channels. The reason for this is that decryption of the message depends on secret information which I have and do not need to share with anyone, which so far as anyone knows is very difficult to determine from my public key.

The public key consists of two numbers, N and r. A message M is scrambled to send to be by computing $M' = M^r\texttt{mod}N$ and transmitting it to

me. N is typically a number of hundreds or thousands of digits. The message M should be a positive integer less than N: a longer message is encrypted by breaking it into blocks.

Now to reveal my secrets...in very general terms which do not compromise the security of any particular RSA key. I know that N is the product of two (large) primes p and q. I do not share these with anyone. I know (because I chose r, that r is relatively prime to $\phi(N) = \phi(pq) = (p-1)(q-1)$ [using the Lemma above].

Now I have computed $s = r^{-1} \mathtt{mod} (p-1)(q-1)$. I can decrypt M' by computing $(M')^s \mathtt{mod} N$.

We verify that this works. $(M')^s \mathtt{mod} N = (M^r \mathtt{mod} N)^s \mathtt{mod} N = (M^r)^s \mathtt{mod} N = M^{rs} \mathtt{mod} N = M^{rs \,\mathtt{mod}\, (p-1)(q-1)} \mathtt{mod} N$ by Euler's Theorem, which is $M \mathtt{mod} N$ because $rs \,\mathtt{mod}\, (p-1)(q-1) = 1$ because $s = r^{-1} \mathtt{mod} (p-1)(q-1)$, and this is simply M because $0 < M < N$.

All of this hinges on the apparent fact that factoring N into p and q if p and q are large enough and chosen with only moderate care appears to be extremely difficult.

The usefulness of this method depends, though, on the ability to find primes p and q. There are efficient tests for whether a number of hundreds of digits is prime or not. And primes are fairly frequent: if you generate a random number p_0 with say 500 digits, you can expect that there will be a prime within $\mathtt{log}(P) \sim 1500$ of p_0, so just test odd numbers 1 by 1 until one is found to get a prime p.

What might make one a little nervous is that this primality test can be applied to our key component N and will say unequivocally that N is composite. How can we tell that N is composite without threatening to be able to find its factors p and q, which might seem to be the only evidence that N is composite?

We give a hint of how we can test a number for being prime (or composite) without finding its factors. Suppose we believe m to be prime. Fermat's little theorem tells us that if we choosa $a < m$ at random, and verify that $\mathtt{gcd}(a, m) = 1$ (of course, if it is not, m is not prime) and then compute $a^{m-1} \mathtt{mod} m$, we expect this to be 1. If it is not, we have discovered that m is composite. The most common primality test in cryptography involves applying a test like this (but slightly more sophisticated) to randomly chosen numbers below m until excellent confidence is obtained that m is prime. This method does not seem to tell us anything about the factors of m if it reports that m is composite. I've described this primality test and proved its

basic properties in Math 406 here, for undergraduates: it is not that much more sophisticated than the test using Fermat's little theorem which I have described, but avoids some technical problems with this test.

Suppose we apply this test to our $N = pq$. Choose a randomly less than pq (which will almost certainly be relatively prime to N). Compute $a^{pq-1}\mathtt{mod}N$. This is equivalent to $a^{(pq-1)\mathtt{mod}(p-1)(q-1)}\mathtt{mod}N$, and $pq-1\mathtt{mod}pq-p-q+1$ will be $p+q-2$, and a^{p+q-2} is most unlikely to be congruent to 1 mod N. But knowing the value of $a^{p+q-2}\mathtt{mod}N$ does not seem to give us any particular handle on what p and q are.

Now we finish up by giving an extended example of encryption and decryption of a message in RSA. We will correct the one we got wrong at the end of the lecture on Thursday, to really wrap things up. This is as I said an illustration of why one needs to do such calculations very carefully and check regularly.

We proposed in class to give a full account where $N = 247$, $r = 5$, $M = 42$.

First, we consider the public transmission of the message: $M' = M^r\mathtt{mod}N = 42^5\mathtt{mod}247 = 74$,

Secretly, as no one could possibly guess, $247 = (13)(19)$: $p = 13$, $q = 19$, and $\phi(N) = (12)(18) = 216$.

Notice that $r = 5$ is relatively prime to 216.

Our decryption exponent s will be $5^{-1}\mathtt{mod}216$.

$$\begin{array}{c|c|c|c} 216 & 1 & 0 & \\ 5 & 0 & 1 & \\ 1 & 1 & -43 & -43 \end{array}$$

The reciprocal of 5 mod 216 is 216-43 = 173.

Below is the calculation by repeated squaring showing that $74^{173}\mathtt{mod}247 = 42$: the decryption succeeds.

$$\begin{array}{cc} 173 & 120^2(74)mod247 = 42 \\ 86 & 100^2mod247 = 120 \\ 43 & 144^2(74)mod247 = 100 \\ 21 & 74^2(74)mod247 = 144 \\ 10 & 120^2mod247 = 74 \\ 5 & 42^2(74)mod247 = 120 \\ 2 & 74^2mod247 = 42 \\ 1 & 74 \end{array}$$

16 Homework 9

A few little exercises:

1. Compute $108^{-1} \texttt{mod} 211$

2. Solve $108x \equiv_{211} 37$ (hint: you can use the previous part!)

3. Describe all solutions (if there are any) of $10x \equiv_{30} 20$. Notice that 10 is not relatively prime to 30: you need to test lots of values. One solution is obvious: there are more.

   Now describe all solutions of $10x \equiv_{30} 15$.

   This question is just a hint that things are more complicated when one solves linear equations in modular arithmetic and a multiplicative inverse is not available.

4. Compute $13^{211} \texttt{mod} 100$

5. Use Fermat's Little Theorem to compute $5^{21355} \texttt{mod} 17$.

   Use the lemma about computation of $\phi(pq)$ to compute $7^{1000} \texttt{mod} 35$. This calculation will end up with some easy repeated squaring, not nearly as much as with an exponent of 1000.

6. Let $N = (13)(17) = 221$. Leet $r = 5$. Verify that r is an appropriate encryption exponent and determine the decryption exponent s.

   Encrypt the message 100 then decrypt the result.