[SQUEAKING]

[RUSTLING]

[CLICKING]

ANKUR MOITRA: Hello, class. Welcome to 18.200. So if you're in the right place, this is Principles of Discrete Applied Math. I'll be one of your co-lecturers. I'm Ankur Moitra, and the other co-lecturer is Peter Shor So, Peter, do you want to stand up and take a bow? So the basic topics that we're going to be covering is we're going to cover topics like probability counting. This will be the beginning part of the class. Some of you may have seen these topics before.

But really in the later parts of the class, we're going to cover some quite new things. We'll talk a lot about generating functions, number theory, cryptography, coding theory, things like noiseless coding, linear programming, and lots of other fun topics. I want to mention that-- I mean, the goal for this class is to try and teach you how to express proofs in an understandable way.

This is one of these skills at MIT that you can pick up a little bit from various classes along the way, but sitting down and conscientiously thinking about what makes a proof easy to follow, how to make it more modular and understandable for the audience is something that's going to help you a lot with other parts of math, and also other parts of computer science in general. A lot of the things that go into good coding practices in terms of modularity are the same types of things we think about when we're writing good proofs.

So that's enough boilerplate for me. I can only go so long without talking about math. So what we're going to be talking about today is we're going to talk about the pigeonhole principle. Actually, first let me hand it off to Susan, who's going to tell you a little bit more about the recitations, and then I'll take it away after that.

SUSAN: Thank you very much, Ankur. So as Ankur noted, this is a CIM, a communication intensive class in the major. And the purpose of CIMs is to help you to communicate effectively as mathematicians. That's for CIMs in the math department. So communicating successfully in a new discipline requires expertise in several different domains. This is based on a model by Anne Beaufort.

We will teach you in these different domains over the course of this semester in the recitations. So you need expertise, of course, with the content. And so the recitations will be designed to help you reinforce your understanding of the mathematics, in addition to other aspects of communication. To communicate successfully as a mathematician, you need to know the norms of mathematics, because they vary. There are differences between norms in CORE 6 and norms in mathematics, and you'll become familiar with some of those.

For example, what goes into the introduction of a paper? For the term paper, that will be basically a multi-page proof and we'll tell you the differences what goes in the introduction there. Also norms of wording, like how to use the word we. Mathematicians use we in different ways than some other disciplines. Also, to communicate successfully as a mathematician, you also need expertise with processes for generating effective communication. That includes drafting.

We'll have multiple drafts built into the term paper, as well as things like how to use LaTeX. And you'll start learning that right off with the first p set. If you're unfamiliar with LaTeX, please reach out. We can help you in office hours. You also need expertise with rhetoric. And by this I mean. rhetorical strategies, strategies for accomplishing your goals as a communicator. For example, mathematicians, if they have a complicated proof, one way to communicate the logic clearly is to use modularity.

Break the proof apart, pull out a lemma. Other strategies that you'll learn in recitation are how to structure the ordering of information within sentences, within sections, within the paper, to make the paper flow well, to reveal the flow of the underlying logic, so that readers can easily follow the logic, and also how to use what we call guiding text to guide readers through the logic. And we'll give other strategies in recitation also.

ANKUR MOITRA: All right. So back to me. So I'm going to tell you about one of the first topics we're going to cover in class, which is a very simple but powerful idea. We're going to be discussing something called the pigeonhole principle. Now the pigeonhole principle, let me tell you the main takeaways before we get into it. It's a very simple idea. I'll tell you what exactly it is, and then we'll go through some neat applications of it.

It turns out to be shockingly powerful, even though you'll think of it as a very obvious statement. I guess the other thing, which is important to keep in mind, it's also quite oddly named. I don't really know the etymology of why it's called the pigeonhole principle, but the basic idea-- let's explain it through an example, and then I'll tell you about where the pigeons come in. So here's a problem that many of us face every day. So imagine that we have five colors of socks in your drawer.

And it's early in the morning, so you're trying to find a match that you can get dressed and go to work. And one of the basic problems you could ask is, how many socks do you have to pick out from your drawer to guarantee that even if you're very, very unlucky, no matter what, you must have a match? So this is really an example of the pigeonhole principle in action. We'll see why exactly it's the pigeonhole principle in a minute.

But any ideas? So how many pairs, how many socks do I have to pull out so that I'm guaranteed a pair? Yeah? Six. Perfect. Because you could get very unlucky in the beginning and your first five could be each different colors, and then no matter what the sixth one is, it's going to match with one of the ones you've selected so far. This is really an example of a much more general principle. So let me explain it with pigeons, and then we'll talk about some more fun applications.

So more generally, we can imagine that we've got n pigeons. I'll even draw them for you. And we're placing them in m pigeonholes. I don't know why they want to go in the pigeonholes, but they do. And let's imagine that n are a number of pigeons is strictly larger than m. Then what I claim is that there must be at least two pigeons in the same pigeonhole. That's the pigeonhole principle.

Now we're going to talk a lot about how to write good proofs, and honestly, a lot of us professors spend a lot of time thinking about how to teach in class and make it engaging. I remember back when I used to teach 042, when I covered things like the pigeonhole principle, there was a bit of an arms race between faculty to come up with the best props for how to explain simple things, and I borrowed from one of my colleagues a whole box of fake dead pigeons, which was very strange because I was going down the elevators in the status center with my box of dead pigeons, and I got a lot of strange looks.

People would ask me, what's going on? And then I had to explain to them that I'm teaching the pigeonhole principle. I don't know why it's called the pigeonhole principle. But then someone asked me when I was on the elevator, does that really help people understand the pigeonhole principle? And I got to say, I don't think it does. Once you get that question, you have to reevaluate your teaching preferences and priorities.

But in any case, this is the pigeonhole principle. I don't know why the pigeons want to go into the pigeonholes, but you can see how the simple example of socks and finding a pair is an example of the pigeonhole principle. You just have to be careful about what are the pigeons and what are the holes. In this case, it's pretty obvious that the pigeons are individual socks and the holes are colors of different socks.

But there are other applications that we're going to see where it's a little bit more subtle how exactly to get this principle to work. Let me tell you one generalization, which is also powerful, which is, in general, imagine I had way more pigeons than pigeonholes. It turns out you can guarantee that there's at least the ceiling of n over m pigeons in the same pigeonhole.

So this is a very simple idea. Let's actually try and prove it, even though it might seem obvious. So it turns out there's a very simple way to prove it. This is one example of a proof technique we're going to see all throughout class, which is a proof by contradiction. And I'm going to try and practice what I preach in today's lecture and show you what are the right ways to write proofs. This won't be quite as formal as you do for your writing exercise, but pretty close.

You can see that the first thing I'm doing when I write a proof by contradiction is I'm putting very clearly the fact that it's a proof by contradiction. You don't want your readers to be confused until the very end where the pieces come together. You want as much as possible that they see the blueprint of how the proof is supposed to go before they get through all of it, right? And so what we're going to do is we're going to suppose not. We'll suppose that the pigeonhole principle is false.

Then what I can do is I can really just count the number of pigeons and the number of holes in two different ways. So what I can do is n is my number of pigeons. Now each pigeon has to be assigned to some hole. So I can sum over all of the different holes h that I'm interested in. And I can look at Nh3, where Nh3 here is just defined to be the number of pigeons that are in some particular hole h. So it's just the count of how many pigeons ended up in that hole.

And all I'm doing is I'm just counting the different pigeons in a different way. So that's definitely equal to n. But now, by assumption, since the pigeonhole principle is false, I'm assuming that each one of the holes has at most one pigeon in it, right? And then the total number of holes I get is m. So now what I claim is I have a contradiction. Why?

Because I've just shown for you that if the pigeonhole principle is false, then n is less than or equal to m. But what was my starting assumption was just that n is strictly larger than m. So this is my proof. But m is larger than n. That's one of the assumptions. And so we get a contradiction. That's it. That's our first proof in this class. This is an example of how you might write up a proof by contradiction. A lot of times in class they'll be a lot more complicated than this, but they all follow this basic blueprint. Yes?

AUDIENCE: Is n greater than m?

ANKUR MOITRA: Ah, sorry. n is greater than m. Thank you n is greater than m. Any other questions, or that was it? OK, good. Feel free to interject any time with questions. All right. Let me show you one other principle in action. So let's talk about some cooler applications of the pigeonhole principle, now that we know what it is and we know why it's true, and we've seen some simple illustrations of it.

What I claim is that a lot of times, writing a good proof is also about finding the right abstraction for how to think about something, how to model it. So let me give you a simple lemma that we're going to prove. So first, this lemma isn't going to sound like the pigeonhole principle, but we'll turn it into the pigeonhole principle. Let's imagine you're going to a party. Let's say you're going to the Super Bowl party this weekend. And you've got n people. There are n total people, including yourself, at the party.

What I claim is that no matter who's there, there are always two people, at least two people who know the same number of other people. This is a mathematical fact about parties. This doesn't quite look like the pigeonhole principle, but I claim it is. And moreover, what we really need is we need the right way to think about this. And we'll practice this type of skill a lot in recitations. This is an example of something which is a lot easier to prove when you have the right way to visualize it.

So it turns out that the right way to visualize it is to draw a graph. Namely, something with nodes that represent people at the party. So there are n different nodes in my graph. And then there are edges that represent different relationships, whether the two people know each other or not. So for example, I could have that the people in my party look like they define this graph. I've got four people in my party n equals 4.

Again, as I mentioned, each of these nodes are people. They're individual people. And these edges represent people who know each other. And then when I draw in all my edges, maybe I'll end up with a graph like this. And you can see that there are two people who know the same number of people at the party, like this node right here, and this node right here. The number of edges that are incident to that node, which represents how many other people they know is both two. So my lemma is true in this simple example.

And now I can understand, through this visual, how exactly a graph relates to this lemma that I asserted to begin with. So now we can actually prove it once we have this abstraction in hand. So let's talk about how that works. Let me define one more quantity which will be of interest for us today just called the degree. That's just the number of edges that are incident to a node.

So the degree of a node is the number of edges incident to it. That share an end point, that have that node as an point. So now let's try and prove this using the pigeonhole principle. In fact, the crucial thing in applying the pigeonhole principle is to figure out what are the pigeons and what are the holes. Does anyone have any idea what we should make the pigeons be, and what we should make the holes be to try and prove this lemma? Yeah?

AUDIENCE: Maybe nodes are the holes and the connections are--

ANKUR MOITRA: OK. We could try that way. I might have a little bit of difficulty that way. Yeah? Yeah, exactly. OK. Because where do I want the collision? So the collision happens between two pigeons who land in the same hole. So what I want is I want two people to collide. And what does it mean to collide? I want them to have the same degree. So that tells me what should be the pigeons and what should be the holes.

So what I claim is that the degree of each node. Well, first of all, it's an integer that's in this set from 0, 1, all the way up to n minus 1. And each node is going to be this pigeon. And the way that I'm going to choose which particular hole it gets mapped to is what the associated degree is.

So I have a hole. Each name is an integer from up to n minus 1. And then each particular node that represents a person is going to get mapped to whatever their degree is. So sounds like I'm done. Am I done here? Can I just appeal to the pigeonhole principle and say that two nodes must collide? Yeah?

AUDIENCE: [INAUDIBLE] the nodes and the set of possible degrees.

ANKUR MOITRA: That's right. So I'm definitely not done right now, because the pigeonhole principle only works when n is strictly larger than m. That's when I picked out six socks from my drawer and I had five colors. I really needed one more pigeon than the number of holes. And the trouble is here. How many pigeons do I have? Well, it's each node in the graph.

That's the number of the people at the party that's n. How many holes do I have? Well, unfortunately, that's also n because it's the integers from 0 to n minus 1. But now we need a clever idea. So I wonder, is it possible to have a node of degree 0 and a node of degree n minus 1 at the same time? So who can help me out? Yeah?

AUDIENCE: If you know n people, that means everybody. Then there's a contradiction because--

ANKUR MOITRA: That's perfect. Exactly right. Let me say it again because I have the mic. So if there's someone at the party who knows n minus 1 people, well, there's n nodes, and that means he's connected to every other node. And that means there isn't anyone at the party who knows no one. So actually, these two endpoints are mutually exclusive. They can't both happen. So if I wanted to write this out formally as a proof, I would actually have to do a case analysis here.

In order to create my contradiction, I would say, case number one, there is a node of degree n minus 1, in which case that means there is no node of degree 0 and I'm back down to having n minus 1 holes and n pigeons, and then I can appeal to the pigeonhole principle and call it a day. And in case two where there's no node of degree n minus 1, again, I only have n minus 1 possibilities for the holes. So I'm not going to be able to write up the full blown proofs when we do them in lecture.

But you can see that to really make this a full bulletproof proof, there are a lot of steps that go into how exactly you can lay out the proof. So I'll just stop here and say that can't be both degree n minus 1 and 0. And that lets us appeal to the pigeonhole principle, so we're good. So this is another example of the pigeonhole principle in action, even though it doesn't look like it at first because you have to figure out what's the right abstraction-- namely a graph for how to think about and visualize what's actually happening underneath this lemma.

Let's do another example. We're going to get harder and harder, unfortunately. So let me give you another of my favorite examples of the pigeonhole principle in action. Which is a very easy to state problem, but turns out to be very difficult from a complexity standpoint. So let's imagine, let me tell you the statement of this lemma and then we'll get into how exactly to prove it.

Suppose I give you 20 four digit numbers. Positive numbers. Let's just call them x1 up to x20. Then what I claim is that there are two disjoint sets of them. And I'll say specifically nonempty sets with the same sum. So what am I asking here? So I give you any 20 four digit numbers. They have to be strictly positive.

And what I'm going to do is I'm going to take some subset of them, maybe x1 plus x3 plus x5, and then I'll take some other subset of them that doesn't overlap in any of those integers, x2 and x4 and x6. And what I claim is that there's a way of doing this, so that the sum of the integers in one set is equal to the sum of the integers in the other set.

Now, moreover, this would be a trivial lemma if I let these sets be empty, because I could just take the empty set for one and the empty set for the other. They're definitely disjoint. They don't share anything in common. And their sum is zero, so this would be a really boring way for this lemma to be true. What I'm saying by nonempty is I'm ruling out that trivial case. There's always an interesting way to do this where you've really created a positive sum for these integers two different ways.

All right. So let's try and prove this, and then I'll tell you some interesting facts about this very simple statement. And again, what we have to do to write up a proof here is we have to do the usual things where we have to figure out what the pigeons are, what the holes are. But moreover, we have to figure out the right mathematical notation for expressing what's going on in this problem. And so, in fact, a lot of times the first step is really to figure out some mathematical way to express the statement right here that I've written out in English.

So another way to think about this is that I claim there are sets I and J, which are subsets of the integers from 1 up to 20. What are these subsets supposed to represent? Just which of the numbers I'm taking in my sum. I want that these sets are both nonempty. So I and J had better not be equal to the empty set. I need that they're disjoint, which just says that the intersection between I and J is equal to the empty set.

So this is just the mathematical way of expressing all of the things I have here. And now for the most important piece of the puzzle, I want that the sum over all of the x sub I's in this first set is equal to the sum of all of the x sub J's in the second set. So a lot of times it's hard to write a mathematical proof unless you have the right mathematical notation to begin with.

Because even though I could have expressed this in English now to actually prove this statement, I'm going to have to do a bunch of manipulations on these sets. And this will be a lot easier with this notation in hand. So another thing that we're going to teach you a lot in recitation is how exactly to set up convenient notation so that your proofs will be easier to write.

So now how exactly are we going to prove this? Let's see if you guys have any intuition. So obviously we're going to be using the pigeonhole principle because I've only taught you one thing so far, so we better use it. But what should we use as the pigeons? Yeah?

AUDIENCE: The sum is divided by 200,000.

ANKUR MOITRA: OK. You're right. But for the holes, I think. So let's be careful. Yeah. So I'll take your answer for the holes, because the way to think about it is that we want a collision among the pigeons. So we really want the collision among what objects? Was there an answer in the back? Yeah? Yeah. I like that. I'm going to strike number of and let's just say subsets, because really, it's the subsets that I care about. Each one of them is a pigeon. But perfect.

All right. So that's exactly what the pigeons will be. They'll just be the appropriate subsets. So in particular, I want them to be nonempty subsets. That's definitely one of the constraints I have in this constraint on I and J here. I'll have to worry about this disjointness constraint later, and we'll get to that. And then exactly as you guys already mentioned, the holes are going to be the possible sums. That's exactly right.

So what can we say about the possible sums? So let's say that the number of possible sums-- let's just call that m. I can just come up with an upper bound, because I just need to show that the number of holes is smaller than the number of pigeons. And definitely an upper bound on this is the largest that the sum can be, which is the sum from I equals 1 to 20 of x sub i. And this is comfortably less than 20 times 10 to the 4, which is strictly less than 10 to the 6. Was there a question here? No? OK.

All right. So now we're in business because we can try and appeal to the pigeonhole principle again. But we have to be a little bit careful here. So what this is going to do is that the number of nonempty subsets, well, this is equal to 2 to the 20 minus 1. So the way to think about this-- and we'll talk more about this when we get into counting-- is really through what's called a bijection. We'll do lots of examples of bijections. But the way to think about that is that each subset of the integers from 1 to 20 is really associated with a bit string.

The first coordinate, which is 1 or 0, tells you whether the first element is in the set or not. The second entry in that string tells you whether the second element is in it, and so on. So a priori, there are 2 to the 20 possibilities, because for each coordinate I have the choice of whether I include it or don't include it in my subset. This minus 1 is because I want the subset to be nonempty. So I have to rule out the subset that takes nothing.

So this is still comfortably much larger than 10 to the 6. So now I'm in good shape because n is strictly larger than m, but there's a catch. So what exactly does this imply? It implies when I use the pigeonhole principle that there exists nonempty A which is not equal to B, because they are different pigeons that end up in the same pigeonhole. And yet, the sum is equal. The sum of all of the xi's in the set A is equal to the sum of all of the xj's in the set B. So I'm not done yet. Why am I not done? Yes?

AUDIENCE: Because it says might not be--

ANKUR MOITRA: The sets might not be disjoint. So I haven't proven what I promised you because I didn't meet this condition. Also notice something about how I wrote this proof. So I did not use I and J here. Because at the end of the day, what I want to show is that there exists this I and J, and I already know that I'm not done. So I left myself some slack in the notation for me to later choose what I and J should be. If I had made these things be I and J, I would have really confused my audience.

So how exactly can we now make these things disjoint? I claim we're almost home. We just have to fix what A and B are. So anyone who hasn't answered yet have a fix for how I can fix A and B? So I've gotten most of it that are nonempty. Have you answered yet? No? OK. All right.

AUDIENCE: Take the intersection of A and B and you remove that common section from both sets.

ANKUR MOITRA: That's right. That's right. So here, let's think about a baby version of this first before we explain it with all of the full blown mathematical notation. A and B might not be disjoint because maybe they share one element in common. Maybe they both contain x1. But then the point is that these two sums are equal and they both have an x1 in them. So I can just remove that common element, and then I'm removing that x1 from the sum.

When I take it out, I've made the sets be disjoint because they no longer share that element in common. And yet, I haven't changed the fact that the sums are equal, even though I've changed the sums themselves. So that's the rest of the proof. You're exactly right. So let's finish up with that proof. So the problem is A and B need not be disjoint.

Now I'm deliberately trying to explain a bit of how I think about the pedagogy of explaining these proofs, not just the proofs themselves. See, one of the things I could have done for proving this is I could have just told you what I want I and J to be. So in fact, what I'm going to do is I'm going to define I is equal to A minus B and J is equal to B minus A.

So what this notation means is I take my set A and I remove every element that shows up in B from that set. And whatever I have left over with is I. Now, notice, B does not have to be a subset of A for this to make sense. If B contains an element that isn't an A, I just ignore that element. It wasn't there before. And I keep it out of my set. But if B and A both contain the element, then I remove it.

So you can think about this pictorially. Maybe these two sets A and B, they look like this. And so what is my set I going to look like? It's going to be exactly this shaded region right here. Because I'm taking out everything that belongs to B and removing it from my set so that I create two disjoint things. So this right here would be I and this right here would be J. So let's think a little bit about pedagogy again.

You see how this visual helps me understand what's going on mathematically in the notation. If I just defined for you what A minus B is, that's a perfectly valid definition. But a lot of times these visuals can help people understand them more easily. And if you notice, the other thing I did in terms of writing up this proof, I could have actually skipped this entire discussion about what happens when I choose A and B. I could have jumped first to I and J.

I could have said A and B come from this pigeonhole principle, and then I could have defined I as A minus B and J as B minus A. But then you would have missed the point about why I needed to do that. So in fact, when you're writing proofs, not everything you write is mathematically necessary, but a lot of times it's pedagogically very useful because you can walk the reader through not just the formal verification that the statement is true, but how exactly you arrived at the proof yourself and the missteps you made along the way but that led you to the right answer.

All right, so finishing this up, the rest of it is just notation. So when we look at this expression, the sum over all xi in the set A, we can break this up into two pieces. It's the sum for all I that are in both A and B of xi. And it's the sum of all xi for I that belongs to my set A. I. Capital I, which is the things that belong here. So I'm just taking the sum over this entire set A, and I'm breaking it up into this piece right here and this piece right here.

But now, by assumption, I know, using the pigeonhole principle, that this is the same thing as the sum from all I and B of xi, and I can break this sum up the same way. It's the sum of all I in the intersection of xi, plus the sum of all of these things in my set capital J. So I'm just breaking up the sum to different ways. And now when I take this equation that the whole thing is equal, I can just cross off these two pieces because they're the same thing.

And that gives me what I want. These sets I and J are definitely disjoint because I've made them be disjoint, and they have the same sum. You should double check that you never end up with these things being nonempty. That's a technicality you have to check, but it is true. And it follows from the assumptions. But that's the end of our next proof. All right? So are there any questions? Makes sense? Yeah?

AUDIENCE: The minimum number--

ANKUR MOITRA: It's about the minimum. But since you asked, let me tell you something interesting about this. This lemma is very easy to state. It's not so bad to prove. We proved it pretty quickly. What's kind of shocking is I can write down 20 four digit numbers for you, and you would have no way-- you could prove to yourself using this proof right here that there are two subsets whose sum is the same, but it would be very hard to actually find them.

So you can do this, for example, with populations of different countries, we know that there are subsets of countries that have literally the same number of people. But it would be exhaustive to try and search all possible subsets to figure out which pair collide. And we don't actually know any faster algorithms. It's related to some things in cryptography. All right. Any other questions? Makes sense so far? All right.

All right. So we got to do our hardest result today. And then I'll do a fun end for one of my favorite applications of the pigeonhole principle. So let's do our hardest theorem. And I'm going to tell you it's the hardest result because I'm going to call it a theorem. And we'll be talking about extensions of this on your first p sets. You'll get more practice with this proof. But let me tell you about a beautiful result in combinatorics.

All right. What I claim is that in any permutation-- I'll tell you what I mean by that in a second. We'll be talking much more about permutations later. Any permutation of the integers 1, 2, 3, all the way up to something n times m plus 1. What I claim is that there is an increasing subsequence of length m plus 1, or a decreasing subsequence of length n plus 1. OK? So I owe you a bunch of things to explain what this theorem means. Yes?

AUDIENCE: Is subsequence [INAUDIBLE]?

ANKUR MOITRA: I'll get to that, but no, it's not. So that's one of the things I owe you. But first, let's start with the simpler thing. So I owe you this. What do I mean by a permutation? So what I mean is you can take these integers 1, 2, 3 all the way up to nm plus 1. n and m are just parameters in this theorem statement. And instead of considering them all in increasing order. I can put all of the numbers in any order I want.

So basically, I take this deck of cards and I shuffle it, and I consider any possible ordering, that's what I mean by permutation. We'll talk more about them formally later when we get to counting. But I take any ordering for these integers. And what I claim is that there's some of subsequence where the numbers are going up by one at least one each time, and that's long. Or if not, there is some long subsequence where the numbers are going down at least by one each time.

So let's do an example, because I should really be more precise by what I mean by a subsequence. So let's take, for example, m equals n equals 3. So then I'm really just asking for a permutation of the integers from 1 up to 10. So some shuffling of that deck of cards. Let's take an example. We could take 3, 2, 1, 6, 5, 4, 9, 8, 7, and then 10.

So now an example of a long increasing sequence is this one right here. I take 3, then I take 6, then I take 9, and then I take 10. So this sequence does not have to be contiguous. These positions I'm interested in don't have to be right next to each other. But what I want is that when I consider the sequence of integers just in those positions where I've put the arrows, that the corresponding sequence I get is strictly increasing as I go up the arrows.

So that's an increasing subsequence. I can also think about having a decreasing one like 3, 2, 1. And that's the longest increasing subsequence I can get here. So you can see that this example illustrates, A, it helps me understand what exactly these abstract definitions mean, like a permutation and an increasing subsequence. It also tells me something even more powerful, which is that this theorem really is tight. Because in the case where n equals m equals 3, what I'm promising you is that there is a length for increasing subsequence, or there's a length for decreasing subsequence.

And even though I found one that has length 4 and is increasing, what I claim in this simple example is that I can't create anything longer, and I can't even create a decreasing subsequence that's longer than 3, because if I did 3, 2, 1, then I'm in trouble. Everything after it is larger. If I do 6, 5, 4 again, I'm in trouble. Everything after it is larger. All right. Any questions?

So I claim that we can prove this using the pigeonhole principle. But we're going to have the same difficulties we usually have, which is where are where the pigeons and where are the holes. In fact, it'll be even more abstract because if you try and guess things like the sequences are the pigeons or the positions are the pigeons, you're going to have a hard time. That's not how this proof is going to go. Instead, we're going to need a very delicate definition to tell us where the pigeons are and how this relates to the pigeonhole principle.

And the idea, basically, is that I can't-- this theorem, if you think about it, it's not telling me which of them I have, whether I have a long increasing or a long decreasing sequence. So in some sense, what I want to do is I want to keep track of my progress on both of them. How long is my largest increasing subsequence? How long is my largest decreasing sequence?

And I want to see how those progress measures grow. So the proof is going to involve this very careful definition. Let's consider these integers in order, and let's consider the S-th element in the sequence. And what we're going to do is we're going to define these helper variables. So we're going to let I sub S denote the length of the longest increasing subsequence ending at the S-th location.

OK? That's one progress measure. I is for increasing. So I've chosen notation that at least has a mnemonic associated with it. I have ds is going to be the same thing, but it'll be the longest decreasing Subsequence. But again, ending at the S-th location. OK? So this is my progress measure. In fact, this is a little bit abstract, so I'll go about it. So how are we going to prove this thing?

So first, does anyone know what this term right here means? WLOG. Just out of curiosity. Yeah? Without loss of generality. OK. So I told you that when I was proving things with the number of people in a party that I had to do this case analysis, well, to prevent my proof from being too long, let me just pretend s is larger than t, because if it was the other way around, I would just switch what's S and what's t. Yeah?

AUDIENCE: [INAUDIBLE]? Like, what are the-- the longest increasing one is six and the last [INAUDIBLE]?

ANKUR MOITRA: Sorry. Which entry in the table here? Yeah?

AUDIENCE: Yeah. Three and six.

ANKUR MOITRA: OK. All right. So here. So we want the longest increasing sequence that ends at three.

AUDIENCE: That ends at six.

ANKUR MOITRA: So do you want this entry in the table? OK. So the longest increasing one that ends at six. So what would it be?

AUDIENCE: Oh, it's [INAUDIBLE].

ANKUR MOITRA: Yeah. Yeah. So it's not required to be contiguous, but it has to include that end point. So that's why these numbers are not monotonically increasing. So when I have the longest decreasing sequence that ends at three, that's pretty long, because I could go 5, 4, 3 and end there. But as soon as I move over to this next column right here, if I have to end at 6, that makes the longest decreasing sequence only of length 1.

So the key is that I'm fixing that my point has to belong to that subsequence and I'm considering progress as I go left to right. So any other questions? This is a crucial part. If you don't understand the table, you won't understand the proof. Good? All right. So without loss of generality, s is larger than t.

And so let's do the following. So if the element at the S-th location is strictly larger than the element at the t-th location, what I claim is that is at least it plus 1. It's the morning and I'm lazy, so who can prove this for me and justify this? Why is this true? Someone who hasn't answered. Especially my back row is very quiet. Yeah?

That's exactly right. So let me say that again. So we can just use the increasing subsequence that ended at the t-th location. And because the element at the S-th location is after the one that happens at the t-th location because S is larger than t, and the element itself is bigger too, I can just append that element and make my subsequence longer.

All right. So how does the rest of the proof go? Who can fill in the rest of the proof for me? So this is one case in the case analysis. I've said without loss of generality S is larger than t. And if the element at the S-th location is larger than the element at the t-th location, my is is at least it plus 1. Yeah?

AUDIENCE: Do the same thing without the generality S greater than t.

ANKUR MOITRA: Yeah.

AUDIENCE: Instead, the element at the S location is less than the element at the t-th location. Then you can do the same for ds and dt.

ANKUR MOITRA: Perfect. That's right. And it's basically the same reasoning but backwards. So otherwise, in particular, if the element at the S-th location is strictly less than the element of the t-th location, I can just take the decreasing subsequence that ends at the t-th location, and append what happens at the S-th location. That's smaller, so that's a valid decreasing sequence. And that's the proof.

I just proved for you that these two pairs of integers are different, because I showed you that either this one is larger than this, or this one is larger than this. And now we're in good shape because, how does the entire thing work? So just returning to the proof, putting it all together. Even though I said it in words, let's just be precise about it. So returning to the proof.

Let's suppose the theorem is false for the purposes of contradiction. Then what I claim is that there are at most nm possible values for these pairs is, ds, because that's what it means for the theorem to be false. There's no n plus 1 length increasing subsequence. There's no length m plus 1 decreasing subsequence. When I look at my pairs of integers, is never becomes larger than n, and ds never becomes larger than m.

And these are my holes is because each one of the possible positions is going to get mapped just by this definition that I gave you right here of is, ds to the signature of these pair of integers that just tells me the name of my hole. But how long is my sequence? There are nm plus 1 values in the sequence. These are all my pigeons, which, by the pigeonhole principle, means there is S not equal to t that collide in some hole with is, ds equal to it, dt.

That's what it means for them to collide to the same hole, because they get mapped to the same thing. And we know that that's impossible. But this is impossible. So that contradicts the assumption we made at the beginning, which was just that the theorem was false. Yes?

AUDIENCE: Without loss of generality, why are we comparing is to i of t plus 1 instead of directly to it?

ANKUR MOITRA: Sorry. Say it again. So why are we comparing?

AUDIENCE: We compare that to i of t plus 1 instead of to it.

ANKUR MOITRA: OK. So just to be careful right here, this is i sub t and then plus 1 is outside. Yeah. So this is really just saying that whatever my length of my increasing sequence is right here, this value right here, I can add 1 to the length. So the plus 1 is not in the subscript. Does that make sense?

AUDIENCE: Why not? Would it hold true that I ask is strictly greater than it or no?

ANKUR MOITRA: is strictly greater-- yes, definitely. is definitely strictly greater than it because these are integers. Yeah. In fact, is not necessarily equal to it plus 1 because there might be some totally different other subsequence that's way longer that just doesn't involve what happens in the t-th location. But all right. Any other questions? This was our hardest proof for today. Yeah?

AUDIENCE: What are we doing in this case?

ANKUR MOITRA: Yeah. So the pigeons. This is why I told you have to be a little bit careful with this. The pigeons are actually the positions. So what's happening here is each one of these positions, the first element, the second element, the third element, the fourth element, the fifth, the sixth. These are my pigeons. How are they getting mapped to a hole is I map them to the hole whose name is this integer, comma, this integer.

It's just the pairs right here. It's the pairs. So my holes-- that's why I drew the little hole right there is that this is the name of the hole. And by assumption, if the theorem is false, is doesn't go larger than n, ds doesn't go larger than m. So there are at most n times m possibilities for this. Yeah?

AUDIENCE: So here, maybe you could have guessed the kind of thing, because the problem is like a product.

ANKUR MOITRA: Yeah.

AUDIENCE: But if you're-- I guess if it didn't have this nice [INAUDIBLE], how would you know?

ANKUR MOITRA: Math is hard. I mean, we're teaching you things which we're not going to give you this on a test and ask you to miraculously guess it. But, for example, we will ask you on the set to do a version of this with three types of subsequences, and you're going to have this as a blueprint to go off of to try and understand what's going on.

So this would be extraordinarily clever if you just came up with this on the spot. There are also twists to very simple problems that will make things very difficult and open. But yeah, let's go with it. All right. Any other questions? Good? All right. Yeah.

AUDIENCE: [INAUDIBLE]?

ANKUR MOITRA: Well, OK, that's maybe a bit of a digression, but basically if I-- this really mimics, if you've taken algorithms classes, a dynamic programming type of solution. Because if I want to know what is the longest subsequence that ends here, I really want to piece it together by answers the subproblems before. And this often has the structure is that once I tell you that the subsequence includes this element and it's increasing, I don't actually have to know anything else about which elements belong to it.

I just have to know it's increasing and its length, and the fact that it belongs to it in order to be able to piece together what happens to the rest. So this, a lot of these things in mathematics, they really mimic what we do algorithmically in terms of how we would go about finding it. And we'll see that more and more in class. That's true even when it comes to writing proof and writing code. OK. Good? All right.

So let's do one of my favorite examples of the pigeonhole principle. Does anyone want to be my victim? Oh, boy. You guys volunteered very quickly. All right. Sure. Can you tell me about-- you can stay there. Can you tell me something about yourself, where you're from, what your name is. Introduce yourself to the class.

AUDIENCE: I'm Anthony. I'm from Saint Louis, Missouri. I don't know.

ANKUR MOITRA: Do you have any hobbies?

AUDIENCE: Oh. I have a two letter curve.

ANKUR MOITRA: OK. Wow. All right. There are not many possibilities for that one. All right. Now, I can, just based on that, using my MIT superpowers, I can tell you something deeply personal about your life history. In your family tree, it's not a tree. And I know that for a fact. So we're going to prove that using the pigeonhole principle. I should confess that I once used this in 042 and I asked for a volunteer or a victim. That's why I call it a victim now.

And the girl raised her hand and told me a bit about herself, and I told her, your family tree is not a family tree. And then she got very red and she said, I know. And I've been a little bit scared to use this since then, so that's why I call it a victim. So you signed up for it. But it's not really just true about you. It's true about everyone in class. It's just a mathematical fact that follows from some very basic axioms of biology, things which are you really can't poke holes in. And it's true for all of us.

So let me tell you about this fun application of the pigeonhole principle. First, let me state the lemma, and then we'll figure out, as usual, how to model it and how exactly to think about it as pigeons and holes. So what I claim is that everyone's family tree contains someone whose parents are blood relatives. It's just true.

OK. So now I'm just going to assert some very incontrovertible things biologically that are pretty safe. But this will be enough to be able to prove this fact. So let's do the setup for this. So what are the axioms we're using? So first of all, everyone has two biological parents. Of course, if I removed biological, it would be more complicated. But I'm just saying this biologically. Everyone has two biological parents.

No one has children after 100. Seems pretty safe. The human race is at least 4,000 years old. That's a very safe assumption. And this is something that can be checked by a biologist, is that we have upper bounds for the number of total humans who've ever lived. What I claim is that there are at most 10 to the 12 humans who've lived all throughout history. And just from these axioms, I claim that we can prove this.

So let's prove it. And we have to figure out the right mathematical abstraction for how to think about this. It's the same way as the friends at a party where we had this way of thinking about it as degrees in a graph. And what we can do here is we can do the same kind of thing, but we can trace back our family tree. In essence, what I'm doing when I trace back this family tree is I'm defining a whole bunch of nodes who have jobs or roles in your family tree.

So there's you at the start. Then if I trace it back, you have your parents. If I trace it back further, I have your grandparents. And when I do this, I'm going to trace this back at least 40 generations, because human history is at least 4,000 years old and no one has children after 100. So I get at least that my depth is at least 40.

So what this means is that there are at least 2 to the 40 nodes in this abstract family tree which are just job descriptions. Your maternal father of-- I mean, all the way back of tracing all the possibilities. And the trouble is that, but 2 to the 40 is larger, is strictly larger than 10 cubed raised to the fourth power, because 2 to the 10 is larger than 1,000. And so this is larger than the number of nodes, all of the possibilities, all the possible humans in human history.

So by the pigeonhole principle, what we get is that at least two nodes, two jobs get mapped to the same person. So that's pretty cool. This is just the mathematical fact that you can use on your friends to annoy them. Please don't do that. So this is what I wanted to tell you about the pigeonhole principle. Now, as I told you, we're going to be covering a bunch of introductory topics in the first few lectures, so pigeonhole principle will get more practice on the p sets.

We're actually going to be spending the next couple of lectures on probability and then counting. So we'll also be talking a little bit about elementary probability in the first recitation, the first homework. So let me tell you at least about the formalisms for probability, and then we're going to go into a lot more detail over the next couple lectures that I'll be explaining. So let me tell you about probability just as an intro for later lectures. And we're going to connect all of this, obviously, to counting as well.

So basically in class, especially for our later topics, everything is going to be built on counting one way or another. We're going to use it for all kinds of fun things. But let me give you a little bit of motivation before we get there. So we're going to be focusing mostly on discrete probability.

So why study discrete probability? Well, it's very useful for things like counting. You want to understand basic setups like, what are the chances of creating certain kinds of objects that are nice when you choose an object at random? That's very related to counting, and it's intertwined with basic questions about probability. Later when we do more advanced topics, we're going to use probability in really cool ways to show the existence of very strange objects that are otherwise hard to construct.

And we're going to be doing this through something called the probabilistic method. It's another example where you can use the language of probability to show that these very strange objects exist, even though no one knows how to find any particular one. So it's kind of like the way that we reason about those subsets of sums of 20 four digit numbers, that we knew that there were subsets whose sum was the same without actually knowing which ones.

Later, when we talk a little bit more about some topics in algorithms, things like primality testing using some of the elementary number theory that we do, deciding whether a given huge integer is prime or not, it'll turn out that, fundamentally, these algorithms are randomized. So really, to reason about it, we'll have to have the language of probability to begin with. And much later in class, when we talk about things like coding theory, we're going to use probability intrinsically to model types of communication.

For example, when there's noise between us. Like when a satellite is sending images back to Earth, what are ways to reliably communicate in the face of errors that are introduced when one party is communicating with the other? So we're going to use probability in all of these different contexts. I want to give you a little bit of the setup for probability before we get into a lot of the key rules and definitions next time.

So probability, even though it's familiar to all of us, it uses some very powerful abstractions and definitions. So the most important of which is what's called the sample space. So in a basic probabilistic setup, the way to think about it is that points in this sample space. We associate them with possible outcomes, things that can happen out of the range of all possibilities.

Just to do a familiar example, we could do something like roll a die. And if it's a normal die, we have six possibilities. That's our sample space, because that describes all of the possible things that could happen, what number shows up. Now the important thing is not just what's the range of possibilities, but really, what's the likelihood of each of these different outcomes. So to each point x in this sample space, we're going to assign some probability p of x which has the following properties.

These are all very intuitive, so we need that the probability is non-negative, and this should be true for all points in the sample space. And we want that, in total, the sum of all the probabilities over the entire sample space is 1. So these are the things that define the setup for basic probability. We have a sample space and we have this probability associated with each one of the outcomes. We can certainly do simple examples like rolling a dice. If it's a fair die, then each one of these possibilities has one sixth probability.

We're going to do a lot more exotic examples in class, things where the sample space might be infinite. That's perfectly fine. We can still have these axioms hold. An example of something we might be interested in is the number of times we flip a coin before we see our first heads. That, in principle, can go on forever. There's no bound on how large that sample space is, and we can still talk about all of the basic axioms of probability and reason about things.

And we'll be particularly interested in what are called events. So events are just subsets of the sample space. They're just some subset of possibilities. And in that case, we can think about this probability of the entire event as just the sum of all of the individual outcomes that land in this event, their total probability. OK? So for example, you could think about an event like rolling an even number. That's not just one possible outcome in the sample space, but it's the set 2, 4, 6.

And the last little baby piece of background is that we'll also be interested in complements of events. So for example, I could look at the probability of t bar. Sometimes you'll see it written as not T as well. And that's just everything that is in the sample space outside the set t. So for example, this is defined as all of the points in the outcome space that don't occur in this original event. So we can define this notion of complementary events, which is everything else besides the events in T.

Basic fact is that a lot of these things behave the way you'd expect them to. So the probability of the complement is just 1 minus the probability of the event itself. It's a very simple proof. We're going to stop now, but I'll tell you a little bit about what we're going to be doing next time. So now that we know at least the basic definitions for probability theory, we're going to be talking about conditional probability, which is always something that's very counterintuitive. So we're going to define what conditional probabilities are. I'll tell you some of the basic results and conditional probability.

And then I'm going to give you a lot of fun examples of how people get conditional probability wrong. So there are a lot of famous examples, like the Monty Hall problem that many of you may have seen. For me, this was always a little bit abstract. Like, it's a cute mathematical puzzle. But I'm going to give you some scarier examples of real world things that happen with doctors where they misinterpret conditional probabilities. So we'll do that next time and I'll tell you some personal stories about that one. So see you on Thursday.