[SQUEAKING]

[RUSTLING]

[CLICKING]

PROFESSOR: OK, so remember that projection theory works differently over-- if you look in finite fields, it works differently over a prime field or a not prime field. And here was the key example. So we're going to do projection theory and Fq and q is p squared. And our set of points is going to be Fp squared, which is a subset of Fq squared. And our set of directions is going to be Fp, which is a subset of Fq.

So remember that if theta is in Fq, then pi theta is going to be a projection, a linear map, from Fq squared to Fq, which is given by pi theta of x1, x2 is x1 plus theta x2. So this is our set of directions. And then S, which is the maximum size of the projection of x over all these directions is p because pi theta of x is just Fp for theta and D.

So if you just write down the sizes of all the things in this important example, x is p squared, which is q and S and D are p which is q to the 1/2. So in particular, notice that the size of each projection is the square root of the size of the set. So nothing like this is supposed to happen over Fp. There's a hard open conjecture that gives bounds that are much stronger than this example.

But the techniques that we've talked about for most of the class do not depend on the field. So the double counting does not distinguish prime fields from nonprime fields. And the Fourier method does not distinguish prime fields from nonprime fields.

The Szemerédi-Trotter theorem proves that this numerology cannot happen for a set of points in R2, but the proof is very important, but it has some limitations in how it could apply. It certainly won't apply over Fp. And it also doesn't seem to help very much from the point of view of sets of balls in R2 with some kind of spacing condition. So it depends what spacing condition, but for the most interesting spacing condition, it doesn't help very much.

Nevertheless, we know that this cannot happen over finite fields. And the main theorem that we'll-- so this week, we'll prove a theorem that says that this cannot happen. So this is the theorem of Bourgain, Katz, and Tau. So again, Katz-Tau projection theorem-- it says the following. So if we have x in Fp squared, and let's say that the size of x is p to the S, where S is somewhere between 0 and 2. And then we have a set of directions in Fp, and set of directions will be p to the t. And t is bigger than 0.

So then, if you look at the maximum size of a projection, it's significantly bigger than half over the square root of the size of x. So this is bigger than p to the S over 22 plus epsilon where this epsilon only depends on S and t. It's bigger than 0.

So some remarks about the epsilon-- it's an explicit function. I just don't write it down because it's a little bit messy. For example, it's continuous. It's not that hard to write it down, but it is also pretty small, pretty disappointingly small.

There's also something called Bourgain's projection theorem, which is what Pablo Shmerkin is going to talk about today, which is the analog of this over in the setting of the reel of balls in R2. So there's an analog of this example using C2 instead of R2. And then Bourgain's projection theorem is the analog of this theorem that rules out that example. This is an analogous theorem for balls in R2.

And these two theorems, in spite of the fact that this epsilon is very small, are very important landmark results in the field of projection theory, and they play a key role in many applications. This Bourgain projection theorem, it plays a key role in getting the sharp projection estimates in R2, the recent work that Pablo Shmerkin and others were involved in.

This Bourgain projection theorem also plays an important role in the solution of the k problem. And this finite field projection theorem, as well as this one, have an important role in some interesting applications about how fast different processes mix. If you take some generators of a finite group like SL2 or Fp and then they make a random walk, how fast does this random walk become evenly distributed in SL2 Fp? This is an important ingredient in studying that.

So in spite of the fact that the epsilon is small, these theorems are very important, and they're also qualitatively different from the other theorems because they're sensitive to what kind of field we're working in. Yeah?

AUDIENCE: What is the analog of p for balls in R2?

PROFESSOR: The analog of p-- so we would have the setting would be you'd have unit balls and a ball of radius R. And R is the analog of p. So all the sizes of things, we could think of them as powers of R. Yeah?

AUDIENCE: Do the proofs use similar arguments or are they completely different?

PROFESSOR: The question is, do these two proofs use similar arguments or are they completely different? There are multiple proofs of this, but at least one of them is very similar to this with one layer of additional ideas. So my plan is that we'll do this, and then we'll talk about the additional ideas to do this. OK, cool.

Well, so the key difference between Fq and Fp is that Fq has a subfield and Fp has no subfield. Now it's elementary to check that Fp has no subfield. But because we're proving some kind of quantitative estimates, we need some quantitative lemma that says that Fp not only has no subfield, but it doesn't have anything that's kind of approximately a subfield. So the main goal for today will be to develop lemmas like that.

And let me show you-- so here's the first version of lemma like that, lemma 1. Actually, let me do-- I think we need a little notation. So suppose that A is a subset of Fp. If I write A plus A, then that means the set of all the sums a1 plus a2 where a1 and a2 are in A. We could write A times A.

That's the set of all the products a1 times a2, a1, and a2 in A, and so on. So you can write a lot of similar things like this, and I think it'll be clear what they all mean. But if it's not, of course, we'll talk about it.

So here's the lemma. It's a quantitative lemma that says that no subset behaves too much like a subfield. So it says if A is a subset of Fp, then either one option is that A minus A over A minus A is all of Fp. And the second option is that if you multiply and add stuff in and subtract stuff, a lot of times, it will get bigger. 2, 3, 4, 5, 6-- 6 might be enough. I think it might be 8.

So one possibility is if you multiply, add, and subtract elements of A a lot of times, then you get a lot more stuff than just A. So this says A is not too close to a subfield. And the other options is if you do this, you get all of Fp. Now, of course, A could have been almost all of Fp already. So then it is kind of almost a field. But if A was originally a lot smaller than Fp, then, in this case, this thing is a lot bigger than A. Cool.

So here is the proof-- observation one. So if c is not in A minus A over A minus A, then A plus cA has size a squared. Let me make sure it's clear what all the notation means. So if I write this thing, I have four copies of A. So take a1, a2, a3, a4, any four guys in A, and plug them in for the capital A's. All the things you can get, that's what this set is.

And similarly, over here, the lowercase c is a particular element of Fp. And this means take any a1 and a2 and do this. So the proof of observation one is quite simple. So suppose that I have two different elements in here but that are equal to each other. So suppose a1 plus a2 is the same as a1 prime plus a2 prime.

Well, if I do a little algebra, I can solve this for c. And I discovered that c is a1 prime minus a1 divided by a2 minus a2 prime, which is an A minus A. So if c is not an A minus A-- sorry, which is an A minus A over A minus A-- so if c is not in here, then all of these different representations are actually different numbers. So the size of this set is A squared.

Now if you want to be really careful, maybe we should worry about whether I have divided by 0. But if a2 is equal to a2 prime, then the only way that the top equation could be true is if also a1 is equal to a1 prime. And then I just have the same thing. All right, great.

So if I can locate some c that is in the ring of stuff I can make by adding and multiplying-- maybe if I can add and subtract and multiply and divide a bunch of elements of A and I can locate some c which is not in here, then I can use this observation, and I can get some-- I can show that I can build out of A many different things. OK, cool.

Now somewhere in our proof, we have to use that Fp is a prime field. It wouldn't work in Fq and we haven't used it yet. Well, how are we going to use it. Well, let's just remember how we would prove that Fp is a prime field-- sorry, how would we prove that Fp has no subfields? How are we going to prove that?

Well, if it had a subfield it would have to contain 1, and then it would have to contain-- then it would be closed under addition, so it would have to contain 2 and 3 and 4 and so on. And then it would have to contain all of Fp. So we're basically going to use that argument in observation two.

So observation two, if A minus A over A minus A is not Fp, then there exists some B in A minus A over A minus A so that B plus 1 is not in A minus A over A minus A. Why is it? So 0 is an A minus A over A minus A. It's a proof of observation two. 0 is in there because you can choose these to be the same. And you can choose those to be different.

If one is not-- so then we just-- either everybody in Fp is in A minus A minus A minus A or somebody is not. And so then we take B plus 1 is the smallest number which is not an A minus A over A minus A. And there we go. And the special thing that we're using about Fp, we've used that we have the prime field, which is just we're using that. If you start at 0 and you keep adding 1, you get all of the elements. So that's the proof of observation two.

And so now we are basically done. So now we have seen that if A minus A over A minus A is not Fp, then if you take A and you add this B plus 1. So B is an A minus A over A minus A. And I'm going to add 1 to it. So B plus 1 is in here. There is bigger than A squared. So if I take six elements of A and I do this, the number of different guys I will get is really much bigger then.

And then this doesn't look exactly like my two, but I just clear the denominator and expand things out. So when I clear the denominator, I'll get A times A minus A times A from this guy, inside of here, I'll have A minus A plus A minus A. I'll multiplied by A. I have a bunch of stuff.

So I know-- So that's Katz and I are old collaborators. And I remember talking with him about this, and that it took quite a while for them to figure out how to get started on this problem.

Now, looking back at this, this proof is really clean. This lemma is perhaps not-- the statement of the lemma is perhaps not the nicest thing that you might like. So there are kind of cleaner things like, for example, later today, we'll show that just this is significantly bigger than A and different variations.

So maybe we should mention-- we could ask some much simpler questions. We could just say if you have a subset of Fp called A, is it true that A plus A is always much bigger than A? That's true for most subsets, but it's not true for all of them. But thinking about that much simpler question is actually-- so that's foundational question in additive combinatorics, to understand that, and understanding that well feeds into being able to understand this stuff better.

So let me pose this on the board and we'll start to talk about it. So my question for us is when is A plus A small? So here I have in mind that A is a subset of Fp, although we could have a very similar conversation if was a subset of E or was A subset of R or dot, dot, dot. Can anybody think of a subset of Fp where A plus A is only a tiny bit bigger than A. Yeah?

AUDIENCE: A is some set of [INAUDIBLE] that includes numbers and the negative values of those numbers in Fp, like only one negative 1, two negative 2, or something like that?

PROFESSOR: Yeah. So the comment is maybe I should have some numbers and negative in those numbers. Let me ask you a more precise question. So you have to choose L numbers in Fp, and you want to choose them to make A plus A as small as possible. Who would you choose? Yeah?

AUDIENCE: Could be an arithmetic [INAUDIBLE]

PROFESSOR: Yeah, you could choose an arithmetic progression. So example one-- suppose A was just the numbers from 1 up to L. So A plus A will be the numbers from negative 2 to 2L. So A plus A is at most 2 times A. It's the tiniest bit less than that, but not very important for our discussion. And this is the smallest that A plus A could possibly be.

And it doesn't have to be one up to L. It would work just as well if it was an arithmetic progression. So example one prime-- our set A is little a plus nd, where n goes from 1 up to L. And then if you think about it a little bit, the size of the subset behaves just the same.

There's another example that's a little bit more general than this. So this is an arithmetic progression where you have just one kind of difference. And you could have something-- so you could visualize it like this. And you could have a similar thing involving a two-dimensional grid or a higher-dimensional grid.

So example two is that A is a plus n1 d1 plus dot, dot, dot plus nr dr where ni goes from 1 up to Li. So what happens when you take A plus A? It is contained in 2a plus n1 d1 plus dot, dot, dot plus nr dr where, now, the ni go in between 2 and 2L.

And so we see from this-- well, which is contained in-- I could put a 1. So it's contained in something that is 2 to the r times bigger. So we get A plus A is bounded by 2 to the r times A. So this thing here is called a generalized arithmetic progression. It has a dimension, little r, and it has a volume or cardinality, which is L1 up to Lr.

Can anybody think of any others? So it is hard to think of other ones. And in some sense, and depending on how we quantify it a little bit, these sets or maybe these sets and their close cousins appear to be the only sets that have a really small subset.

And this was investigated by Freiman starting in the '60s and '70s, and he proved a theorem to that effect called Freiman's theorem. And this is a cornerstone of additive combinatorics. Freiman's proof was somewhat difficult to read, and Ruzsa thought a lot about it and clarified it. And so this is now called usually the Freiman-Ruzsa theorem.

So it says the following thing-- says that if A is in Z-- the same thing would be true in Z mod p-- and A plus A is less than or equal to KA, then A is contained in a gap with dimension little r that only depends on K and volume at most V. That only depends on K times the size of A.

So it roughly says that if A plus A is small, it is because a resembles example two, which is a generalization of example one. So in some sense these are the only sets that have a really small subset.

So this is an important theorem in additive combinatorics. But there are two caveats about it. So one caveat is that it's a pretty deep theorem, where the proof is substantial. And the other caveat is that the quantitative bounds are weak.

So in the original version, r of K was quite large. So r of K was something like x of K to a power and V of K was even larger, so xp of x of K to a power.

Now it is a trivial fact that any set A is contained in a generalized arithmetic progression of dimension equal to the size of A. So this is only interesting if r of K is smaller than the size of A. So this was only interesting, only meaningful, let's say, if k was quite small.

There is a big goal in additive combinatorics to improve the quantitative bounds in Friedman's theorem, and. one benchmark is a conjecture called the polynomial frame in Ruzsa conjecture, which would say something meaningful even if K was a small power of A.

So there's a conjecture that they would have a meaningful bound if K is A to the delta for some small but universal delta bigger than 0. And this is still an open conjecture. So it's out of range, maybe only a little out of range of current techniques. But if K was, say, I don't know, A to the 0.1, all this stuff about Freiman's theorem, we are very far from being able to deal with that.

Now, if you look at Freiman's theorem, what we're trying to do is to give a complete classification of all the sets a that do this. And the complete classification is something we only understand if K is really, really small. But you could also ask for something which is not as strong as a complete classification, but just some kind of interesting information about sets with small subset.

So if you look at this example, you'll notice that not only it has small subset, but it has also small a bunch of other stuff. In these examples, A plus A is small. Also, A minus A is small. Also, A plus A plus A is small. And for those things, we have much simpler proofs, and the quantitative bounds are much better. And they come from some lemmas that I think originally were designed as lemmas for this theorem but which have lots of independent applications.

So this theorem, I don't plan to prove in the class, but I wanted to mention it for historical context. And these lemmas are really important and have reasonable short proofs and, I think, are worth for a wide range of people knowing about them.

So the first of the lemmas is called the Ruzsa triangle inequality. So it says if Z is an abelian group, and A and B and C are subsets of Z, then size of A times the size of B minus C is bounded by the size of A minus B times the size of A minus C.

So this might take a little digesting. All of these letters feels a little bit like alphabet soup. The fact that we can put three different sets makes it a little harder to digest. But, of course, it makes it more flexible in general. And by plugging in different choices for these three sets, you can prove some simpler things.

Let me illustrate this with an example. As a corollary of this, we will see that if the sum set is small, then the difference set is also small. So corollary-- if A plus A is smaller than K times A, then A minus A is smaller than K squared K squared times L. So this lemma is meaningful as long as K is slightly smaller than the square root of A. So in a much wider range than the Freiman-Ruzsa theorem. This is a meaningful statement.

So proof-- we're just going to use Ruzsa, and I have to tell you who are A and B and C. So A will be A. And then I think B-- let me see. Yeah, B and C are both negative A. So if you look at B minus C, there's a lot of minus signs. This is a little bit silly looking. So that's just A minus A. And A minus B or A minus C-- they're the same as each other because B is the same as C. That's A minus negative A. So that's A plus A.

So now if we just plug in Ruzsa, it says A times this guy, A minus A, is less than this guy times this guy. That's A plus A squared. And by hypothesis, that's smaller than K squared A squared. And if you cancel the factor of A, that's it.

And this has a very simple proof that will fit on this board and which already says something interesting and nontrivial about how sums and differences and stuff fit together. So here's the proof. We will construct a map phi that goes from A cross B minus C into A minus B cross A minus C, which is injective.

So this is the cardinality of this set. And this is the cardinality of that set. And the reason that this set is bigger than that set is that we have an injection from one end to the other. How does the injection work? For every d in B minus C, we can choose-- so by definition, this d can be written as somebody in B minus somebody in C. Let's pick them. We choose B of d and B C of d and C so that d is B of d minus C of d

Now, what's our map? Phi takes an A and a d. A lives here, and d lives there. We need to output somebody an A minus so we take A minus B of d and then A minus C of d. So that is a map from here to here. Why is it injective? So to check that it's injective, we're going to suppose that phi of A d is given to us as xy. And then we're going to find A and d from x and y and from this choice.

So the choice we made, once and for all, we used it to build the map. And now we have to prove that there's only one A and d that give a certain x and y here. So how do we recover them?

Well, if this is x and this is y, let me see that y minus x is B of d minus C of d, which is d. So that's how we find d. And once we find d, it's easy to find-- once we find d, then we know B of d and C of d, and now it's easy to find A. So x minus x plus B of d is A. It's very short. It feels a teeny bit like a magic trick to me. But on this board and this board, we have seen that if the sum set is small, then the difference set is also small. Yeah?

AUDIENCE: Take the log, you get something that looks exactly like a triangle inequality is there any way to see that it's [INAUDIBLE]?

PROFESSOR: Yeah, so the question is it's called triangle inequality. And it looks like if we take the logarithm and play with this, then something will look like the triangle inequality. So Ruzsa did have that in mind when he named it that way. So he produced a pseudodistance between different sets, say, between A and B or B and C or whatever. And this translates into saying that the Ruzsa pseudodistance obeys the triangle inequality. The distance from B to C is bounded by the distance from A to B plus the different distance from B to A plus the distance from A to C.

I'm not sure whether that is helpful or not. Pseudodistance is a little bit funny. It's not true that the distance from A to itself is 0. So it's not quite like distances that I'm used to. So that intuition, may or may not be helpful. I guess we will see tomorrow that, sometimes, you use this many times.

How would you use the triangle inequality? Well, the distance from A to Z is bounded by the distance from A to B plus the distance from B to C plus the distance from C to D, duh, duh, duh, duh, duh, and maybe each of those things is easier to understand. And by the triangle inequality, we can put them together. So you can use this inequality in that way. And we'll see that tomorrow-- Thursday. Any other questions or comments?

AUDIENCE: Can I ask about the movie denominator trick? Just not sure how that worked out. Does it require something nontrivial like this?

PROFESSOR: The question is about the removing the denominator trick?

AUDIENCE: Can you use that [INAUDIBLE]

PROFESSOR: Like when we had an A minus A in the denominator and we multiplied it out? So that was just algebra. It's not something fancy like this. Let me bracket that. We'll see a little later, something else with removing denominators. And let's come back to it then. Do you think-- did I understand your question or--

AUDIENCE: Yeah, I'm just not sure how that [INAUDIBLE]

AUDIENCE: You only need 6 instead of 8 because that's the--

PROFESSOR: Yeah, let's check in about it at the end of class. The other important lemma from this field that went into the proof of Freiman's theorem is called Plunnecke inequality. Plunnecke inequality allows us to say things like if A plus A is small, then A plus A plus A is small.

So if A and B are subsets of Z, an abelian group, and A plus B is bounded by K times A, then-- let me make a little notation. So sometimes, we might want to talk about B plus B many times. So let's say this is n times. This is sometimes written as n times B, although I feel like that is slightly confusing. So I've decided to adopt this notation, B some n times. So I could take B plus m times minus B plus n times, and that's bounded by K to the m plus n times A.

So let's do a few corollaries of this. So just by plugging in A equals B, we see that if A plus A is less than or equal to KA, then A minus A is less than K squared A. That's actually the corollary we already proved. But also, we could say A plus A plus A is bounded by K cubed A. I'm just plugging in A equals B, and this is m is 3 and n is 0. And you can see you can put higher powers here.

Also another corollary we can get is we can switch the role of these guys in the first corollary. So we can say if A minus A is small, then A plus A is also small. So proof is that B is negative A. So this is A plus B. And then this is basically B plus B.

We can also use this. So we'll prove this. That will be our last big goal of the class. So this Ruzsa inequality and Plunnecke inequality have many, many uses. And one simple use is we can use it to clean up and improve the statement of our lemma that Fp has no quantitative approximate subfields. So let me recall what we proved so far, and then we'll improve it a little bit.

So lemma one was if A is in Fp, then either A minus A over A minus A is all of Fp or A times A minus A times A-- so now I can write this better. We have three or four of those minus three or four of those A squared.

So we can improve this in a way that you don't need to have so many different expressions floating around. So we can say that if A is in Fp and the size of A is p to the S, where S is strictly less than 1, then the size of A times A minus A times A is at least p to the S plus epsilon of S. And here, you could put either plus or minus. And this epsilon of S is bigger than 0. So again, it's continuous. It's explicit. But it's a little bit messy, and it's a little bit small.

You take any subset which is significantly smaller than the whole field, if you take A times A minus A times A, it will be significantly bigger than you started with. So if you just took A minus A, that wouldn't be good enough because A could be an arithmetic progression. So that might have almost the same size as A. If you just took A times A, that wouldn't be good enough, because A could be a geometric progression-- 2 to the 1, 2 to the 2, up to 2 to the L.

But if you take both sums and products, then you have to end up with significantly more stuff than you started with. So that's why this is called sum-product theory. If you have both sums and products interacting with each other, then something happens.

So proof-- so there are two cases, case 1 and case 2. But I'm actually going to do case 2 first. So it could be that A times A is already much bigger than A. Then we just declare victory. So if A times A is bigger than A to the plus delta and we declare victory. And here, delta is going to be much smaller than epsilon. Or maybe we could say that.

Otherwise, A times A is basically the same size as A. Now, if A times A plus A times A is much bigger than A, then we declare victory. Wait a second. Yeah, here. I guess let's just put this right here. Then we declare victory. Otherwise, we would have A times A plus A times A is smaller than K A times A where K is like p to the epsilon.

And then we can use Plunnecke. And that would tell us that A times to A big power minus A times to another big power. Here, we could put 4. That would be bounded by K to the eighth A times A. And so that would be bounded by maybe A times p to the 10 epsilon or something like that. And this contradicts the fact that this we know this set is big. And case 1 is similar, but I think maybe I'll make that an exercise. You can just practice using Plunnecke and Ruzsa things.

And I do one more corollary. So suppose you start with the set A and you start multiplying and adding and subtracting and see what you get. And we've proven that after you do this operation, it gets a bit bigger. But suppose you don't just-- yeah?

AUDIENCE: Question. So you said that the idea is that if you have some arithmetic progression or geometric progression, it can be small, but it has to be learned. Is it possible to prove that instead of the difference of A times A and A times A, you can just say A times A is large or A plus A is large?

PROFESSOR: OK, yes, great question. So the question is, so in the theme of lemma 2 is we tried to simplify as much as possible the expression that we put here. And there is a suggestion how to make it as simple as possible. So then I'm going to erase this proof and write that as a-- I'll write it as a theorem.

So even better, there is a theorem Bourgain-Katz-Tao So if A is subset of Fp, A equals p to the S 0 less than or equal to S less than 1, then you could take the maximum of A plus A and A times A, and that is bigger than p to the S plus epsilon of S. So this is better than this, qualitatively. And actually, the word sum product inequality-- it could refer to a lot of things, but the inequality it most often refers to is this one, so either the sums or the products grow. Yeah, that's right.

So all the stuff we've seen are steps towards the proof of this theorem, but there is actually still some more ideas to get all the way down to here. And we may or may not end up doing it in the class. It's unclear to me if getting all the way down to there is actually important in projection theory. Yeah, cool.

So one goal you might have in simplifying and clarifying this story is to make this expression as simple as possible and get some gain. But another goal that you might have is to make this gain really large, and perhaps this expression will be more complicated. And you can also do that. So let me make some notation. Let's say poly K of some polynomials of complexity K, so I take A to the K. So that means I multiply K different elements of A together. And then I add K things like that together. And then maybe I also want some minuses. So A to the K is A times A times A K times. So these are polynomials in of complexity.

And another corollary, which is at the same level, follows easily from this one is that if we have 0 less than S less than t less than 1 and A is in Fp, then there exists some K that only depends on S and t so that for any set A in any Fp, where the size of A is p to the S, the size of poly K of A is at least p to the t.

And the proof of this is easy. The proof is use lemma 2 many times. So I start with the set A. A times A minus A times is a bit bigger. Call this B. B times B minus B times B is even a bit bigger. And if you think about what B times B minus B times B means, it would fit in poly for an A, and you keep doing this. OK, cool.

So these lemmas, theorems, and stuff, they are important because-- inequality and Ruzsa's inequality, they are important because-- so if we see something like A plus A is small, then that tells us that A has some structure. And all these inequalities, then, imply that lots of other things are small. So it's like a contagious structure.

We input some structure, but we find out more and more structure. And that's a very useful tool. And so lots of problems that we see in projection theory, it seems to be helpful to try to phrase them in the form that some subset is small because, then, we can use as inequality and we can find out lots of other things.

So in the last part of the class, we will prove this inequality. This is the trickiest thing that we will prove today.

So the original proof of the inequality was somewhat difficult. And there was a short proof that was given by Georgios Petrides about 10 or 15 years ago, which is the one that I'll show. So it's based on a key lemma. So the lemma says that if A plus B is at most K times A, then there's a subset x contained in A so that for any set C, x plus C plus B divided by x plus C is also at most K.

By the way, this top inequality-- of course, we can divide by A. The top inequality says A plus B over A is bounded by K. The lemma says that if this is true, if it's true for the set A, then it's also true for the set x plus C, where x is carefully chosen. I'll explain in a bit how it's chosen, but C is a totally arbitrary set. So there are many choices for C. So there are many different-- this is many inequalities.

Let me tell you who x is, which is an important idea in the proof. So first of all, so x is a subset of A that we choose in order to minimize the ratio x plus B over x. So let me give an example that might help to motivate why you would want to look at this x.

So suppose that A is the numbers from 1 up to 100, which has a lot of additive structure together with some random number. So I put a million. And B is the numbers from 1 up to, say, 50. So if you add A and B together, this stuff plus this stuff is quite small. There's a lot of structure there. Then there's this stuff plus this stuff. That doesn't have any particular structure. But since there's only one stray element here, that's not so many of those either. So A plus B is pretty small.

Now, who would x be? x was the subset of A which is chosen to minimize this ratio. And including this guy is not so helpful. So x would actually be here, just the numbers from 1 up to 100.

So I think perhaps that, philosophically, the point of doing this is identifying the part of A that really has the additive structure and throwing away, possibly, some parts of A that are not that relevant. And then, once you have found the heart of the matter here, then you can add anything else to it. And you still have that amount of structure.

So let's give a name. Let's say that-- so that's who x is. And let's say x plus B over x is K lower bar, which is at most K. So A plus B over A is at most K. And x is allowed to be all of A. But we might choose a smaller set if we can make this ratio even smaller. So K bar is less than or equal to K. And really, the key claim is that x plus C plus B over x plus C is at most K lower bar for any x.

So now we're going to prove the claim by induction. So we're going to prove the claim by induction on the cardinality of C. And the cardinality of C is 1. Then x plus C plus B is just x plus B. And x plus C is just x. So if the cardinality of C is 1, I'm just shifting this set. And shifting that set doesn't change their cardinality.

So now we can do the inductive step. So let's say that C prime is C union-- one more guy. And by induction, we know that it's true for C. So we know x plus C plus B is bounded by K lower bar x plus C. And we want to check for C prime.

So the key character in this argument that Petrides came up with is a set y, which is the set of x and X so that x plus little C plus B is contained in big X plus big C plus B. Let's see how that naturally comes up.

So we're thinking about x plus C prime plus B. We want to see that it's not too big. And we're using induction. So we want to see how it changes when we added this one guy. So this is the previous guy, x plus C plus B plus the new ones, and I want them to be really new. So here are some new elements that live here, and I'm going to take out any elements I've already counted.

AUDIENCE: Sorry, I don't quite understand the definition of how can x plus C plus B not be a subset of x plus C plus B.

PROFESSOR: So C prime is a previous set C union with some little c. And little c is not in big C. Now I have to write all the little c's and big Cs really carefully. But this is a little c, and this is a big C. Cool. So this x is automatically in big X, but in a failure of functoriality of notation, little c is not in big C.

Now, one thing to note about this definition that helps to motivate it is that y plus little C plus big B is contained in x plus big C plus big B because for each element of y, little y plus little c plus big B is defined to be in here. So this is at most x plus c plus B plus x plus c plus B take away y plus c plus B.

All of these were already counted. So there are at most this many new guys. And this is x plus C plus B plus x plus B minus y plus B because this is a subset of this. And the plus c just translates things. So this thing is that big and I remove from it this thing, which is that big. So that's the upper bound for the numerator. So I'm trying to bound this thing with a C prime. I want to prove an upper bound, so an upper bound for the numerator and a lower bound for the denominator.

So the denominator is x plus C prime. And so that's x plus C plus the set how many x and x. So that little x plus little c is not contained in big X plus big C. So the guys I already had, and then I have guys of the form little x plus little c. And I only want the new ones. The ones that aren't already counted. So that's an equality. And I'm going to write it as x plus c plus x minus the x and x so that x plus c is in x plus c.

And now the key observation is that these guys are all in y. This is a subset of y because if little x plus little c is In big X plus big C-- so if little x plus little c is in big X plus big C, then I can add B to both sides. And this is in there. So those are all in y. So this is a subset of y. So the size of this guy is at most the size of y. And since I'm subtracting here, I can say this is at least x plus c plus x minus y.

So now we'll just put together everything that we know. We know that x plus C plus B over x plus C is at most K bar. We know that by induction. We know that x plus B over x is equal to K bar. We know that by definition. That's just what K bar was. And we know that y plus B over y is greater than or equal to K bar. That was the definition of x. x was chosen to minimize this ratio. y might perhaps be equal to x. But that's OK. But it's never going to be any smaller.

And so therefore, by algebra, by how fractions work, x plus C plus B-- oh, sorry. So now I can say-- I want to say x plus C prime plus B over x plus C prime, and I want an upper bound for that. So the numerator is bounded by 1 x plus C plus B plus x plus B minus y plus B. And the denominator is lower bounded by part two. And it's x plus C plus x minus y. And then because each of these ratios has the correct sign, this is at most K lower bar.

So this is short. It is a little tricky. And I must admit, I don't quite understand how Petrides thought to do this.

So from the key lemma, we can prove Plunnecke inequality and then see if anybody-- if you have room, you can turn over in your mind, philosophically, why did this work out so nicely? If anybody has thoughts about it, I would be happy to hear.

So proof-- so say we're starting with this. So we use our main lemma, so it tells us that there exists some x in A, and we have x plus C plus B is at most K times x plus C for any C. How might we use this? So C could be empty. So we get x plus B is at most K times x. C could be B, so we get x plus B plus B. That's at most K times x plus B. And x plus B is at most K times x. So that's at most K squared times x.

And you can see where this goes. So I'll do one more. You'll get the pattern. If I add one more B, That's at most K X plus B plus B. Plug in what I already know about this-- that's at most k cubed times x. So if I add x plus m copies of B, that will be at most k to the m times x.

And then we'll use the Ruzsa inequality. So this is already pretty good thing. If A equals B here, then I could say A to the m is bounded by K to the m times A because A to the m is obviously at least as big as x plus A to the m. So I get A to the m is bounded by K to the m times A. That's a typical corollary of Plunnecke.

Anyway, to get the advertised finale, we use Ruzsa's inequality. Ruzsa was A times-- so I can plug in-- so x times B plus m minus B plus n is bounded by x plus B plus m x plus B plus n.

And then we plug in each of these, and we get a K to the m plus n times x squared. Yeah, that's right. So then I get this by itself. So B plus m minus B plus n is bounded by K to the m plus n times x, which is bounded by K to the m plus n times A because x is a subset of A.

So this proof is short. It is a little tricky. But I think it is well worth spending some time with because this inequality is really quite important. I would say that it plays really a key role in all the later developments in projection theory and the solution to the problem in a lot of things. And so as we keep going tomorrow or Thursday and so on, we'll reflect more about why this is useful and important. And maybe I'll try to come up with some homework to try to reflect on how this proof got put together. Cool.