MAS114: Lecture 8

James Cranch

http://cranch.staff.shef.ac.uk/mas114/

2020–2021

Last time. . .

Last time. . .

I was telling you about well-orderings.

Last time…

I was telling you about well-orderings.
(A set is *well-ordered* if every nonempty subset has a least element).

Last time. . .

I was telling you about well-orderings.
(A set is *well-ordered* if every nonempty subset has a least element).
I mentioned that well-orderings give induction principles.

What does that tell us?

What does that tell us?

Part of the reason this is such good news is that there are other well-ordered sets, besides the natural numbers.

What does that tell us?

Part of the reason this is such good news is that there are other well-ordered sets, besides the natural numbers. Whenever you find a well-ordering, you get a notion of induction for free.

What does that tell us?

Part of the reason this is such good news is that there are other well-ordered sets, besides the natural numbers. Whenever you find a well-ordering, you get a notion of induction for free.
For example, consider the set of pairs (m, n) of naturals, where we say that $(m, n) < (m', n')$ if $m < m'$, or if $m = m'$ and $n < n'$.

What does that tell us?

Part of the reason this is such good news is that there are other well-ordered sets, besides the natural numbers. Whenever you find a well-ordering, you get a notion of induction for free.

For example, consider the set of pairs (m, n) of naturals, where we say that $(m, n) < (m', n')$ if $m < m'$, or if $m = m'$ and $n < n'$. (This is called the *lexicographic* ordering, because it's inspired by the way that words in dictionaries are ordered).

What does that tell us?

Part of the reason this is such good news is that there are other well-ordered sets, besides the natural numbers. Whenever you find a well-ordering, you get a notion of induction for free.

For example, consider the set of pairs (m, n) of naturals, where we say that $(m, n) < (m', n')$ if $m < m'$, or if $m = m'$ and $n < n'$. (This is called the *lexicographic* ordering, because it's inspired by the way that words in dictionaries are ordered).

It is not too hard to prove that that is well-ordered: any set of pairs of natural numbers has a "least" element with respect to this ordering.

What does that tell us?

Part of the reason this is such good news is that there are other well-ordered sets, besides the natural numbers. Whenever you find a well-ordering, you get a notion of induction for free.

For example, consider the set of pairs (m, n) of naturals, where we say that $(m, n) < (m', n')$ if $m < m'$, or if $m = m'$ and $n < n'$. (This is called the *lexicographic* ordering, because it's inspired by the way that words in dictionaries are ordered).

It is not too hard to prove that that is well-ordered: any set of pairs of natural numbers has a "least" element with respect to this ordering. Hence we can do (strong) induction on pairs of naturals!

Proofs as literature

Proofs as literature

In this section I simply give a few thoughts on how to write a good proof.

Proofs as literature

In this section I simply give a few thoughts on how to write a good proof.

Writing proofs which are easy to understand, enlightening, or fun to read is very difficult.

Proofs as literature

In this section I simply give a few thoughts on how to write a good proof.

Writing proofs which are easy to understand, enlightening, or fun to read is very difficult.

Like with other forms of literature, the best way to learn to write well is to read, and to think about what you read.

Proofs as literature

In this section I simply give a few thoughts on how to write a good proof.

Writing proofs which are easy to understand, enlightening, or fun to read is very difficult.

Like with other forms of literature, the best way to learn to write well is to read, and to think about what you read.

If you see a proof which you consider to be particularly well written, try to *learn from it* as an example of what's good to do.

Proofs as literature

In this section I simply give a few thoughts on how to write a good proof.

Writing proofs which are easy to understand, enlightening, or fun to read is very difficult.

Like with other forms of literature, the best way to learn to write well is to read, and to think about what you read.

If you see a proof which you consider to be particularly well written, try to *learn from it* as an example of what's good to do. Similarly, if you see a proof which you consider to be particularly badly written, maybe you can learn something from the experience about what to avoid!

Proofs as literature

In this section I simply give a few thoughts on how to write a good proof.

Writing proofs which are easy to understand, enlightening, or fun to read is very difficult.

Like with other forms of literature, the best way to learn to write well is to read, and to think about what you read.

If you see a proof which you consider to be particularly well written, try to *learn from it* as an example of what's good to do. Similarly, if you see a proof which you consider to be particularly badly written, maybe you can learn something from the experience about what to avoid!

Also, *read it back* to yourself (or better yet, get a colleague to read it).

Proofs as literature

In this section I simply give a few thoughts on how to write a good proof.

Writing proofs which are easy to understand, enlightening, or fun to read is very difficult.

Like with other forms of literature, the best way to learn to write well is to read, and to think about what you read.

If you see a proof which you consider to be particularly well written, try to *learn from it* as an example of what's good to do. Similarly, if you see a proof which you consider to be particularly badly written, maybe you can learn something from the experience about what to avoid!

Also, *read it back* to yourself (or better yet, get a colleague to read it). You're writing it so others can read: it's good to test it to make sure this is possible.

Proofs as literature

In this section I simply give a few thoughts on how to write a good proof.

Writing proofs which are easy to understand, enlightening, or fun to read is very difficult.

Like with other forms of literature, the best way to learn to write well is to read, and to think about what you read.

If you see a proof which you consider to be particularly well written, try to *learn from it* as an example of what's good to do. Similarly, if you see a proof which you consider to be particularly badly written, maybe you can learn something from the experience about what to avoid!

Also, *read it back* to yourself (or better yet, get a colleague to read it). You're writing it so others can read: it's good to test it to make sure this is possible. This goes particularly for proofs containing large amounts of symbols: these can be very hard to read, and reading it back to yourself is probably the best way of detecting this.

Use words *and* symbols

Use words *and* symbols

A common mistake that beginners make is to use very few words at all.

Use words *and* symbols

A common mistake that beginners make is to use very few words at all. Words are fantastic for *explaining* what you're doing.

Use words *and* symbols

A common mistake that beginners make is to use very few words at all. Words are fantastic for *explaining* what you're doing.
In particular, too many people overuse the symbol "$\therefore$" (meaning "therefore"), and the symbol "$\because$" (meaning "because").

Use words *and* symbols

A common mistake that beginners make is to use very few words at all. Words are fantastic for *explaining* what you're doing.
In particular, too many people overuse the symbol "$\therefore$" (meaning "therefore"), and the symbol "$\because$" (meaning "because"). I won't use them at all in my proofs in these notes.

Use words *and* symbols

A common mistake that beginners make is to use very few words at all. Words are fantastic for *explaining* what you're doing.
In particular, too many people overuse the symbol "$\therefore$" (meaning "therefore"), and the symbol "$\because$" (meaning "because"). I won't use them at all in my proofs in these notes. There are so many good phrases which do its job, and choosing one helps you write what you're actually thinking.

Use words *and* symbols

A common mistake that beginners make is to use very few words at all. Words are fantastic for *explaining* what you're doing.
In particular, too many people overuse the symbol "$\therefore$" (meaning "therefore"), and the symbol "$\because$" (meaning "because"). I won't use them at all in my proofs in these notes. There are so many good phrases which do its job, and choosing one helps you write what you're actually thinking. Also, it distracts the reader's eye from the symbols which matter — the actual maths you're doing — to things which don't.

Alternatives to symbols

Alternatives to symbols

Here are some phrases which do the job of "$\because$":

Alternatives to symbols

Here are some phrases which do the job of "$\therefore$":

so,

Alternatives to symbols

Here are some phrases which do the job of "$\therefore$":

so, hence,

Alternatives to symbols

Here are some phrases which do the job of "$\therefore$":

so, hence, therefore,

Alternatives to symbols

Here are some phrases which do the job of "$\therefore$":

so, hence, therefore, thus,

Alternatives to symbols

Here are some phrases which do the job of "$\because$":

so, hence, therefore, thus, consequently,

Alternatives to symbols

Here are some phrases which do the job of "$\therefore$":

so, hence, therefore, thus, consequently, as a result,

Alternatives to symbols

Here are some phrases which do the job of "$\therefore$":

so, hence, therefore, thus, consequently, as a result, accordingly, for this reason,

Alternatives to symbols

Here are some phrases which do the job of "$\therefore$":

so, hence, therefore, thus, consequently, as a result, accordingly, for this reason, and so,

Alternatives to symbols

Here are some phrases which do the job of "$\therefore$":

so, hence, therefore, thus, consequently, as a result, accordingly, for this reason, and so, and in particular,

Alternatives to symbols

Here are some phrases which do the job of "$\therefore$":

so, hence, therefore, thus, consequently, as a result, accordingly, for this reason, and so, and in particular, as a consequence,

Alternatives to symbols

Here are some phrases which do the job of "$\therefore$":

so, hence, therefore, thus, consequently, as a result, accordingly, for this reason, and so, and in particular, as a consequence, because of that,

Alternatives to symbols

Here are some phrases which do the job of "$\therefore$":

so, hence, therefore, thus, consequently, as a result, accordingly, for this reason, and so, and in particular, as a consequence, because of that, and then,

Alternatives to symbols

Here are some phrases which do the job of "$\therefore$":

so, hence, therefore, thus, consequently, as a result, accordingly, for this reason, and so, and in particular, as a consequence, because of that, and then, and from that,

Alternatives to symbols

Here are some phrases which do the job of "$\therefore$":

> *so, hence, therefore, thus, consequently, as a result, accordingly, for this reason, and so, and in particular, as a consequence, because of that, and then, and from that, . . .*

Alternatives to symbols

Here are some phrases which do the job of "$\therefore$":

> *so, hence, therefore, thus, consequently, as a result, accordingly, for this reason, and so, and in particular, as a consequence, because of that, and then, and from that, . . .*

Here are some which do the job of "$\because$":

Alternatives to symbols

Here are some phrases which do the job of "$\therefore$":

so, hence, therefore, thus, consequently, as a result, accordingly, for this reason, and so, and in particular, as a consequence, because of that, and then, and from that, . . .

Here are some which do the job of "$\because$":

because,

Alternatives to symbols

Here are some phrases which do the job of "$\therefore$":

so, hence, therefore, thus, consequently, as a result, accordingly, for this reason, and so, and in particular, as a consequence, because of that, and then, and from that, …

Here are some which do the job of "$\because$":

because, since,

Alternatives to symbols

Here are some phrases which do the job of "$\therefore$":

so, hence, therefore, thus, consequently, as a result, accordingly, for this reason, and so, and in particular, as a consequence, because of that, and then, and from that, ...

Here are some which do the job of "$\because$":

because, since, as a result of,

Alternatives to symbols

Here are some phrases which do the job of "$\therefore$":

so, hence, therefore, thus, consequently, as a result, accordingly, for this reason, and so, and in particular, as a consequence, because of that, and then, and from that, . . .

Here are some which do the job of "$\because$":

because, since, as a result of, as we have,

Alternatives to symbols

Here are some phrases which do the job of “$\therefore$”:

so, hence, therefore, thus, consequently, as a result, accordingly, for this reason, and so, and in particular, as a consequence, because of that, and then, and from that, . . .

Here are some which do the job of “$\because$”:

because, since, as a result of, as we have, as we know,

Alternatives to symbols

Here are some phrases which do the job of "$\therefore$":

so, hence, therefore, thus, consequently, as a result, accordingly, for this reason, and so, and in particular, as a consequence, because of that, and then, and from that, . . .

Here are some which do the job of "$\because$":

because, since, as a result of, as we have, as we know, as we have seen that,

Alternatives to symbols

Here are some phrases which do the job of "$\therefore$":

so, hence, therefore, thus, consequently, as a result, accordingly, for this reason, and so, and in particular, as a consequence, because of that, and then, and from that, . . .

Here are some which do the job of "$\because$":

because, since, as a result of, as we have, as we know, as we have seen that, because we saw,

Alternatives to symbols

Here are some phrases which do the job of "$\therefore$":

so, hence, therefore, thus, consequently, as a result, accordingly, for this reason, and so, and in particular, as a consequence, because of that, and then, and from that, . . .

Here are some which do the job of "$\because$":

because, since, as a result of, as we have, as we know, as we have seen that, because we saw, . . .

Bad things with words

Bad things with words

On the other hand, if you do write words, don't write them all in one paragraph.

Bad things with words

On the other hand, if you do write words, don't write them all in one paragraph. Try to write in a structured fashion, and if you are producing paragraph after paragraph after paragraph, ask yourself if you could use symbols to make your life easier in places.

Bad things with words

On the other hand, if you do write words, don't write them all in one paragraph. Try to write in a structured fashion, and if you are producing paragraph after paragraph after paragraph, ask yourself if you could use symbols to make your life easier in places.

The clearest pieces of mathematical writing I've read often make good use of words and symbols, working together.

Bad things with words

On the other hand, if you do write words, don't write them all in one paragraph. Try to write in a structured fashion, and if you are producing paragraph after paragraph after paragraph, ask yourself if you could use symbols to make your life easier in places.

The clearest pieces of mathematical writing I've read often make good use of words and symbols, working together.

When it's really important, I like to use both to make sure the point is clear.

Bad things with words

On the other hand, if you do write words, don't write them all in one paragraph. Try to write in a structured fashion, and if you are producing paragraph after paragraph after paragraph, ask yourself if you could use symbols to make your life easier in places.

The clearest pieces of mathematical writing I've read often make good use of words and symbols, working together.

When it's really important, I like to use both to make sure the point is clear. I might write,

> *Let* $A = \sum_{i=1}^{n} a(i)$ *be the sum of the first* n *values of* a, *and let* $p > A$ *be a prime number greater than* A.

Bad things with symbols

Bad things with symbols

There are also ways of abusing symbols. Consider the following sentence:

The square of $5 = 25$*.*

Bad things with symbols

There are also ways of abusing symbols. Consider the following sentence:

The square of $5 = 25$.

Many novices write this, wanting it to mean:

$($*The square of* $5) = 25$.

Bad things with symbols

There are also ways of abusing symbols. Consider the following sentence:

The square of $5 = 25$.

Many novices write this, wanting it to mean:

$($*The square of* $5) = 25$.

However, experienced readers will read it as

The square of $(5 = 25)$.

This is of course nonsense: equations don't really have squares, and $5 = 25$ is a false equation anyway.

Bad things with symbols

Bad things with symbols

Some of the worst notational abuses are possible with induction.

Bad things with symbols

Some of the worst notational abuses are possible with induction. When writing an induction proof, don't explain what you need to prove as

Let $P(n) = a_n = 3^n + 1$.

This has $P(n)$ as a *number*, not a *statement*.

Bad things with symbols

Some of the worst notational abuses are possible with induction. When writing an induction proof, don't explain what you need to prove as

> *Let* $P(n) = a_n = 3^n + 1$.

This has $P(n)$ as a *number*, not a *statement*. Instead, if you want to name the statement, write:

> *Let* $P(n)$ *be the statement that* $a_n = 3^n + 1$.

The importance of clear structure

The importance of clear structure

Every sentence (and equation) of a proof needs to be justified:

The importance of clear structure

Every sentence (and equation) of a proof needs to be justified:

- Usually, most sentences simply follow on from the one before. It is helpful to say so (using the connection words above, for example).

The importance of clear structure

Every sentence (and equation) of a proof needs to be justified:

- Usually, most sentences simply follow on from the one before. It is helpful to say so (using the connection words above, for example).
- Whenever a sentence doesn't just follow on from the one before (but is a radical new idea, or draws on things said a while earlier), it's even more important to say so.

The importance of clear structure

Every sentence (and equation) of a proof needs to be justified:

- Usually, most sentences simply follow on from the one before. It is helpful to say so (using the connection words above, for example).
- Whenever a sentence doesn't just follow on from the one before (but is a radical new idea, or draws on things said a while earlier), it's even more important to say so. For example, you could:

The importance of clear structure

Every sentence (and equation) of a proof needs to be justified:

- Usually, most sentences simply follow on from the one before. It is helpful to say so (using the connection words above, for example).
- Whenever a sentence doesn't just follow on from the one before (but is a radical new idea, or draws on things said a while earlier), it's even more important to say so. For example, you could:
  - use words which introduce a change of pace ("now we do this..");

The importance of clear structure

Every sentence (and equation) of a proof needs to be justified:

- Usually, most sentences simply follow on from the one before. It is helpful to say so (using the connection words above, for example).
- Whenever a sentence doesn't just follow on from the one before (but is a radical new idea, or draws on things said a while earlier), it's even more important to say so. For example, you could:
    - use words which introduce a change of pace ("now we do this..");
    - name or number something earlier, and refer back to it by name or number;

The importance of clear structure

Every sentence (and equation) of a proof needs to be justified:

- Usually, most sentences simply follow on from the one before. It is helpful to say so (using the connection words above, for example).
- Whenever a sentence doesn't just follow on from the one before (but is a radical new idea, or draws on things said a while earlier), it's even more important to say so. For example, you could:
  - use words which introduce a change of pace ("now we do this..");
  - name or number something earlier, and refer back to it by name or number;
  - leave a paragraph break;

The importance of clear structure

Every sentence (and equation) of a proof needs to be justified:

- Usually, most sentences simply follow on from the one before. It is helpful to say so (using the connection words above, for example).
- Whenever a sentence doesn't just follow on from the one before (but is a radical new idea, or draws on things said a while earlier), it's even more important to say so. For example, you could:
  - use words which introduce a change of pace ("now we do this..");
  - name or number something earlier, and refer back to it by name or number;
  - leave a paragraph break;
  - leave a space;

The importance of clear structure

Every sentence (and equation) of a proof needs to be justified:

- Usually, most sentences simply follow on from the one before. It is helpful to say so (using the connection words above, for example).
- Whenever a sentence doesn't just follow on from the one before (but is a radical new idea, or draws on things said a while earlier), it's even more important to say so. For example, you could:
  - use words which introduce a change of pace ("now we do this..");
  - name or number something earlier, and refer back to it by name or number;
  - leave a paragraph break;
  - leave a space;
  - have a descriptive section heading.

Things you haven't told us

Things you haven't told us

It is particularly important to avoid unstated assumptions.

Things you haven't told us

It is particularly important to avoid unstated assumptions.
For example, if a proof contains an assertion that some construction is a function, then the definition of a function gives you some things to check:

Things you haven't told us

It is particularly important to avoid unstated assumptions.

For example, if a proof contains an assertion that some construction is a function, then the definition of a function gives you some things to check: that *every* element of the domain gives a *unique* element lying *inside* the codomain.

Things you haven't told us

It is particularly important to avoid unstated assumptions. For example, if a proof contains an assertion that some construction is a function, then the definition of a function gives you some things to check: that *every* element of the domain gives a *unique* element lying *inside* the codomain. Unless they're obviously true, it could be that these checks are the hardest and most interesting part of the proof. They could even be lies.

Explain the structure

Explain the structure

Here is a classic account of a public speaking strategy:

Explain the structure

Here is a classic account of a public speaking strategy:

First I tell them what I'm going to tell them.

Explain the structure

Here is a classic account of a public speaking strategy:

First I tell them what I'm going to tell them.
Then I tell them.

Explain the structure

Here is a classic account of a public speaking strategy:

First I tell them what I'm going to tell them.
Then I tell them.
And then I tell them what I've told them.

Explain the structure

Here is a classic account of a public speaking strategy:

First I tell them what I'm going to tell them.
Then I tell them.
And then I tell them what I've told them.

This approach is even better in proofs than it is in public speaking.

Explain the structure

Here is a classic account of a public speaking strategy:

> *First I tell them what I'm going to tell them.*
> *Then I tell them.*
> *And then I tell them what I've told them.*

This approach is even better in proofs than it is in public speaking. Some explanation at the beginning is important. It may well be that your reader doesn't know even what you're aiming to do, and it's even more likely that your reader doesn't know how you're planning to do it.

Explain the structure

Here is a classic account of a public speaking strategy:

First I tell them what I'm going to tell them.
Then I tell them.
And then I tell them what I've told them.

This approach is even better in proofs than it is in public speaking. Some explanation at the beginning is important. It may well be that your reader doesn't know even what you're aiming to do, and it's even more likely that your reader doesn't know how you're planning to do it.

Also, some explanation at the end is important. When you reach a conclusion, why do you think that what you have written actually means you have finished the proof?

Explain the structure

Here is a classic account of a public speaking strategy:

> *First I tell them what I'm going to tell them.*
> *Then I tell them.*
> *And then I tell them what I've told them.*

This approach is even better in proofs than it is in public speaking.
Some explanation at the beginning is important. It may well be that your reader doesn't know even what you're aiming to do, and it's even more likely that your reader doesn't know how you're planning to do it.
Also, some explanation at the end is important. When you reach a conclusion, why do you think that what you have written actually means you have finished the proof?
If the proof is long, then regard it as being made of several parts. Give each part an explanation when you start and when you finish it.

A pleasant structure

A pleasant structure

I quite like proofs with the following kind of framework:

A pleasant structure

I quite like proofs with the following kind of framework:

We'll prove this by induction on n.

A pleasant structure

I quite like proofs with the following kind of framework:

> *We'll prove this by induction on n.*
> *The base case, where $n = 0$, is the statement "blah blah blah".*

A pleasant structure

I quite like proofs with the following kind of framework:

We'll prove this by induction on n.

The base case, where $n = 0$, is the statement "blah blah blah". But that's true, because blah blah blah blah blah.

A pleasant structure

I quite like proofs with the following kind of framework:

> *We'll prove this by induction on n.*
> *The base case, where $n = 0$, is the statement "blah blah blah". But that's true, because blah blah blah blah blah.*
> *Now we need the induction step: we assume the statement true for $n = k$, and prove it for $n = k + 1$.*

A pleasant structure

I quite like proofs with the following kind of framework:

> *We'll prove this by induction on n.*
>
> *The base case, where $n = 0$, is the statement "blah blah blah". But that's true, because blah blah blah blah blah.*
>
> *Now we need the induction step: we assume the statement true for $n = k$, and prove it for $n = k + 1$. So we're assuming that blah blah blah, and have to prove that blah blah blah.*

A pleasant structure

I quite like proofs with the following kind of framework:

> *We'll prove this by induction on n.*
> *The base case, where $n = 0$, is the statement "blah blah blah". But that's true, because blah blah blah blah blah.*
> *Now we need the induction step: we assume the statement true for $n = k$, and prove it for $n = k + 1$. So we're assuming that blah blah blah, and have to prove that blah blah blah.*
> *But blah blah blah blah blah.*

A pleasant structure

I quite like proofs with the following kind of framework:

> *We'll prove this by induction on n.*
> *The base case, where $n = 0$, is the statement "blah blah blah". But that's true, because blah blah blah blah blah.*
> *Now we need the induction step: we assume the statement true for $n = k$, and prove it for $n = k + 1$. So we're assuming that blah blah blah, and have to prove that blah blah blah.*
> *But blah blah blah blah blah. Also, blah blah blah blah blah.*

A pleasant structure

I quite like proofs with the following kind of framework:

We'll prove this by induction on n.

The base case, where $n = 0$, is the statement "blah blah blah". But that's true, because blah blah blah blah blah.

Now we need the induction step: we assume the statement true for $n = k$, and prove it for $n = k + 1$. So we're assuming that blah blah blah, and have to prove that blah blah blah.

But blah blah blah blah blah. Also, blah blah blah blah blah. So, in conclusion, blah blah blah, which is what we had to prove.

A pleasant structure

I quite like proofs with the following kind of framework:

> *We'll prove this by induction on n.*
>
> *The base case, where $n = 0$, is the statement "blah blah blah". But that's true, because blah blah blah blah blah.*
>
> *Now we need the induction step: we assume the statement true for $n = k$, and prove it for $n = k + 1$. So we're assuming that blah blah blah, and have to prove that blah blah blah.*
>
> *But blah blah blah blah blah. Also, blah blah blah blah blah. So, in conclusion, blah blah blah, which is what we had to prove. That finishes off the induction step, and so completes the proof.*

Reason forwards

Reason forwards

It's quite normal to find yourself solving problems, where you start by thinking about where you want to be, and end up working out how to get there from where you are.

Reason forwards

It's quite normal to find yourself solving problems, where you start by thinking about where you want to be, and end up working out how to get there from where you are.

For example, a while ago I visited my family back home in Guernsey, and wondered about the timings of my journey from Sheffield.

Reason forwards

It’s quite normal to find yourself solving problems, where you start by thinking about where you want to be, and end up working out how to get there from where you are.

For example, a while ago I visited my family back home in Guernsey, and wondered about the timings of my journey from Sheffield. My plane left Gatwick at 1600,

Reason forwards

It's quite normal to find yourself solving problems, where you start by thinking about where you want to be, and end up working out how to get there from where you are.

For example, a while ago I visited my family back home in Guernsey, and wondered about the timings of my journey from Sheffield. My plane left Gatwick at 1600, so I worked out I had to check in by 1515.

Reason forwards

It's quite normal to find yourself solving problems, where you start by thinking about where you want to be, and end up working out how to get there from where you are.

For example, a while ago I visited my family back home in Guernsey, and wondered about the timings of my journey from Sheffield. My plane left Gatwick at 1600, so I worked out I had to check in by 1515. Hence I wanted to be at Gatwick rail station by 1500 at the latest,

Reason forwards

It's quite normal to find yourself solving problems, where you start by thinking about where you want to be, and end up working out how to get there from where you are.

For example, a while ago I visited my family back home in Guernsey, and wondered about the timings of my journey from Sheffield. My plane left Gatwick at 1600, so I worked out I had to check in by 1515. Hence I wanted to be at Gatwick rail station by 1500 at the latest, so. . .

Reason forwards

It's quite normal to find yourself solving problems, where you start by thinking about where you want to be, and end up working out how to get there from where you are.

For example, a while ago I visited my family back home in Guernsey, and wondered about the timings of my journey from Sheffield. My plane left Gatwick at 1600, so I worked out I had to check in by 1515. Hence I wanted to be at Gatwick rail station by 1500 at the latest, so…

This was a very efficient process for working out what time to do everything

Reason forwards

It's quite normal to find yourself solving problems, where you start by thinking about where you want to be, and end up working out how to get there from where you are.

For example, a while ago I visited my family back home in Guernsey, and wondered about the timings of my journey from Sheffield. My plane left Gatwick at 1600, so I worked out I had to check in by 1515. Hence I wanted to be at Gatwick rail station by 1500 at the latest, so. . .

This was a very efficient process for working out what time to do everything (much better than trial and error, where you repeatedly guess times to leave your house, working out when you arrive).

Reason forwards

It's quite normal to find yourself solving problems, where you start by thinking about where you want to be, and end up working out how to get there from where you are.
For example, a while ago I visited my family back home in Guernsey, and wondered about the timings of my journey from Sheffield. My plane left Gatwick at 1600, so I worked out I had to check in by 1515. Hence I wanted to be at Gatwick rail station by 1500 at the latest, so. . .
This was a very efficient process for working out what time to do everything (much better than trial and error, where you repeatedly guess times to leave your house, working out when you arrive). But the paragraph above is a terrible set of instructions for someone else who wants to get from Sheffield to Guernsey: it's backwards.

Reason forwards

It's quite normal to find yourself solving problems, where you start by thinking about where you want to be, and end up working out how to get there from where you are.

For example, a while ago I visited my family back home in Guernsey, and wondered about the timings of my journey from Sheffield. My plane left Gatwick at 1600, so I worked out I had to check in by 1515. Hence I wanted to be at Gatwick rail station by 1500 at the latest, so...

This was a very efficient process for working out what time to do everything (much better than trial and error, where you repeatedly guess times to leave your house, working out when you arrive). But the paragraph above is a terrible set of instructions for someone else who wants to get from Sheffield to Guernsey: it's backwards.

It's the same with proofs: when you write them down, you're supposed to *finish* with the result you're trying to prove,

Reason forwards

It's quite normal to find yourself solving problems, where you start by thinking about where you want to be, and end up working out how to get there from where you are.

For example, a while ago I visited my family back home in Guernsey, and wondered about the timings of my journey from Sheffield. My plane left Gatwick at 1600, so I worked out I had to check in by 1515. Hence I wanted to be at Gatwick rail station by 1500 at the latest, so. . .

This was a very efficient process for working out what time to do everything (much better than trial and error, where you repeatedly guess times to leave your house, working out when you arrive). But the paragraph above is a terrible set of instructions for someone else who wants to get from Sheffield to Guernsey: it's backwards.

It's the same with proofs: when you write them down, you're supposed to *finish* with the result you're trying to prove, and on the way things are supposed to follow from your assumptions and the things you said earlier.

Backwards to forwards

Backwards to forwards

Often that means you have to do your working on one piece of paper and then write it up again in the opposite order! This is normal.

Backwards to forwards

Often that means you have to do your working on one piece of paper and then write it up again in the opposite order! This is normal. In proofs later in this course I'll sometimes try to talk you through how you'd think about it.

Backwards to forwards

Often that means you have to do your working on one piece of paper and then write it up again in the opposite order! This is normal. In proofs later in this course I'll sometimes try to talk you through how you'd think about it.
A very common sign you're going the wrong way is when you finish up with something obvious (like $1 = 1$).

Backwards to forwards

Often that means you have to do your working on one piece of paper and then write it up again in the opposite order! This is normal. In proofs later in this course I'll sometimes try to talk you through how you'd think about it.
A very common sign you're going the wrong way is when you finish up with something obvious (like $1 = 1$).
This is especially bad when you mix forwards and backwards reasoning, and what you're writing is likely to be *badly wrong* in this situation.

Backwards to forwards

Often that means you have to do your working on one piece of paper and then write it up again in the opposite order! This is normal. In proofs later in this course I'll sometimes try to talk you through how you'd think about it.

A very common sign you're going the wrong way is when you finish up with something obvious (like $1 = 1$).

This is especially bad when you mix forwards and backwards reasoning, and what you're writing is likely to be *badly wrong* in this situation. For example, we could prove $9 = 11$ as follows:

Backwards to forwards

Often that means you have to do your working on one piece of paper and then write it up again in the opposite order! This is normal. In proofs later in this course I'll sometimes try to talk you through how you'd think about it.

A very common sign you're going the wrong way is when you finish up with something obvious (like $1 = 1$).

This is especially bad when you mix forwards and backwards reasoning, and what you're writing is likely to be *badly wrong* in this situation. For example, we could prove $9 = 11$ as follows: subtract 10 from both sides to get $-1 = 1$, and then square both sides to get $1 = 1$. This is true, so we're done.

More weird backwards reasoning

More weird backwards reasoning

Here's an example of weird backwards reasoning: earlier in the course we had to prove that

$$\frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2},$$

More weird backwards reasoning

Here's an example of weird backwards reasoning: earlier in the course we had to prove that

$$\frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2},$$

and we might have written

More weird backwards reasoning

Here's an example of weird backwards reasoning: earlier in the course we had to prove that

$$\frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2},$$

and we might have written

$$\frac{k(k+1)}{2} + k + 1 \qquad = \tfrac{(k+1)(k+2)}{2}$$

More weird backwards reasoning

Here's an example of weird backwards reasoning: earlier in the course we had to prove that

$$\frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2},$$

and we might have written

$$\begin{aligned} \frac{k(k+1)}{2} + k + 1 &= \tfrac{(k+1)(k+2)}{2} \\ k(k+1) + 2k + 2 &= (k+1)(k+2) \end{aligned}$$

More weird backwards reasoning

Here's an example of weird backwards reasoning: earlier in the course we had to prove that

$$\frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2},$$

and we might have written

$$\begin{aligned}
\frac{k(k+1)}{2} + k + 1 &= \tfrac{(k+1)(k+2)}{2} \\
k(k+1) + 2k + 2 &= (k+1)(k+2) \\
k^2 + k + 2k + 2 &= k^2 + k + 2k + 2
\end{aligned}$$

More weird backwards reasoning

Here's an example of weird backwards reasoning: earlier in the course we had to prove that

$$\frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2},$$

and we might have written

$$\begin{aligned}
\frac{k(k+1)}{2} + k + 1 &= \tfrac{(k+1)(k+2)}{2} \\
k(k+1) + 2k + 2 &= (k+1)(k+2) \\
k^2 + k + 2k + 2 &= k^2 + k + 2k + 2 \\
k^2 + 3k + 2 &= k^2 + 3k + 2,
\end{aligned}$$

More weird backwards reasoning

Here's an example of weird backwards reasoning: earlier in the course we had to prove that

$$\frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2},$$

and we might have written

$$\begin{aligned}
\frac{k(k+1)}{2} + k + 1 &= \tfrac{(k+1)(k+2)}{2} \\
k(k+1) + 2k + 2 &= (k+1)(k+2) \\
k^2 + k + 2k + 2 &= k^2 + k + 2k + 2 \\
k^2 + 3k + 2 &= k^2 + 3k + 2, \qquad \text{which is true!}
\end{aligned}$$

More weird backwards reasoning

Here's an example of weird backwards reasoning: earlier in the course we had to prove that

$$\frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2},$$

and we might have written

$$\begin{aligned}
\frac{k(k+1)}{2} + k + 1 &= \tfrac{(k+1)(k+2)}{2} \\
k(k+1) + 2k + 2 &= (k+1)(k+2) \\
k^2 + k + 2k + 2 &= k^2 + k + 2k + 2 \\
k^2 + 3k + 2 &= k^2 + 3k + 2, \qquad \text{which is true!}
\end{aligned}$$

How could we mend this? You could just write it backwards, but in fact there are more natural ways of explaining it.

Help your reader

Help your reader

It is often well worthwhile supplying an example or a diagram.

Help your reader

It is often well worthwhile supplying an example or a diagram. If your proof depends critically on it, on the other hand, you are probably not supplying enough information.

Help your reader

It is often well worthwhile supplying an example or a diagram. If your proof depends critically on it, on the other hand, you are probably not supplying enough information. But it's quite sensible to use an example or a diagram as an aid.

Proofs should fit the statements!

Proofs should fit the statements!

This is perhaps my vaguest (but perhaps also my most helpful) piece of advice.

Proofs should fit the statements!

This is perhaps my vaguest (but perhaps also my most helpful) piece of advice.

Often (but not always) it's possible to guess what a proof will look like, at least roughly, based on the appearance of the thing you're trying to prove.

Proofs should fit the statements!

This is perhaps my vaguest (but perhaps also my most helpful) piece of advice.

Often (but not always) it's possible to guess what a proof will look like, at least roughly, based on the appearance of the thing you're trying to prove. Don't try to fight it.

Proofs and their statements

Proofs and their statements

Here are some examples:

Proofs and their statements

Here are some examples:

- If you're trying to prove $P \wedge Q$,

Proofs and their statements

Here are some examples:

- If you’re trying to prove $P \wedge Q$, you’re likely to prove P and then prove Q.

Proofs and their statements

Here are some examples:

- If you're trying to prove $P \wedge Q$, you're likely to prove P and then prove Q.
- If you're trying to prove $P \vee Q$,

Proofs and their statements

Here are some examples:

- If you're trying to prove $P \wedge Q$, you're likely to prove P and then prove Q.
- If you're trying to prove $P \vee Q$, you're likely to prove P or prove Q (after fiddling around to try to see which of those is easiest).

Proofs and their statements

Here are some examples:

- If you're trying to prove $P \wedge Q$, you're likely to prove P and then prove Q.
- If you're trying to prove $P \vee Q$, you're likely to prove P or prove Q (after fiddling around to try to see which of those is easiest).
- If you're trying to prove something of the form $P \Rightarrow Q$,

Proofs and their statements

Here are some examples:

- If you're trying to prove $P \wedge Q$, you're likely to prove P and then prove Q.
- If you're trying to prove $P \vee Q$, you're likely to prove P or prove Q (after fiddling around to try to see which of those is easiest).
- If you're trying to prove something of the form $P \Rightarrow Q$, your proof is likely to start with "We'll assume P" and to continue by deducing Q.

Proofs and their statements

Proofs and their statements

- If you're trying to prove something of the form $\forall x \in X, \quad P(x)$,

Proofs and their statements

- If you're trying to prove something of the form $\forall x \in X, \quad P(x)$, your proof is likely to start "Let x be an element of X" and then continue by proving $P(x)$.

Proofs and their statements

- If you're trying to prove something of the form $\forall x \in X, \quad P(x)$, your proof is likely to start "Let x be an element of X" and then continue by proving $P(x)$.
- If you're trying to prove something of the form $\exists x \in X \quad \text{s.t.} \quad P(x)$,

Proofs and their statements

- If you're trying to prove something of the form $\forall x \in X, \quad P(x)$, your proof is likely to start "Let x be an element of X" and then continue by proving $P(x)$.
- If you're trying to prove something of the form $\exists x \in X \quad \text{s.t.} \quad P(x)$, your proof is likely to start by giving one particular (cleverly chosen) value of x, and then proving that $P(x)$ is true of it.

Proofs and their statements

- If you're trying to prove something of the form $\forall x \in X, \quad P(x)$, your proof is likely to start "Let x be an element of X" and then continue by proving $P(x)$.
- If you're trying to prove something of the form $\exists x \in X \quad \text{s.t.} \quad P(x)$, your proof is likely to start by giving one particular (cleverly chosen) value of x, and then proving that $P(x)$ is true of it.
- If you're trying to prove something about a sequence with a recurrence relation, your proof may well be by an induction, where the induction step refers to the same previous cases as the recurrence relation.

Elementary number theory

Elementary number theory

Now we have language to do so, the rest of this course will be concerned with beginning a study of the sets of numbers we have discussed earlier: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.

Elementary number theory

Now we have language to do so, the rest of this course will be concerned with beginning a study of the sets of numbers we have discussed earlier: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.

We're going to spend two-thirds of that time (or thereabouts) laying the foundations for *elementary number theory*: the study of $\mathbb{N}$ and $\mathbb{Z}$.

Elementary number theory

Now we have language to do so, the rest of this course will be concerned with beginning a study of the sets of numbers we have discussed earlier: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.

We're going to spend two-thirds of that time (or thereabouts) laying the foundations for *elementary number theory*: the study of $\mathbb{N}$ and $\mathbb{Z}$.

This used to be a beautiful, isolated and useless subject, until the 20th century came along. Now it is beautiful, well-connected and vitally important.

Elementary number theory

Now we have language to do so, the rest of this course will be concerned with beginning a study of the sets of numbers we have discussed earlier: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.

We're going to spend two-thirds of that time (or thereabouts) laying the foundations for *elementary number theory*: the study of $\mathbb{N}$ and $\mathbb{Z}$.

This used to be a beautiful, isolated and useless subject, until the 20th century came along. Now it is beautiful, well-connected and vitally important.

Remark

In the sense that mathematicians use the word, "elementary" doesn't mean "easy": it means "using no deep theory" (we're only four weeks into your first semester, so haven't had time to develop any deep theory).

Elementary number theory

Now we have language to do so, the rest of this course will be concerned with beginning a study of the sets of numbers we have discussed earlier: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.

We're going to spend two-thirds of that time (or thereabouts) laying the foundations for *elementary number theory*: the study of $\mathbb{N}$ and $\mathbb{Z}$.

This used to be a beautiful, isolated and useless subject, until the 20th century came along. Now it is beautiful, well-connected and vitally important.

Remark

In the sense that mathematicians use the word, "elementary" doesn't mean "easy": it means "using no deep theory" (we're only four weeks into your first semester, so haven't had time to develop any deep theory). It can still be difficult, and in fact it can still be deep.

Divisibility

Divisibility

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division.

Divisibility

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division. We remarked a while ago that it's not always possible to do division inside $\mathbb{Z}$ or $\mathbb{N}$:

Divisibility

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division. We remarked a while ago that it's not always possible to do division inside $\mathbb{Z}$ or $\mathbb{N}$: that suggests there's something interesting going on!

Divisibility

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division. We remarked a while ago that it's not always possible to do division inside $\mathbb{Z}$ or $\mathbb{N}$: that suggests there's something interesting going on!

Here's the basic definition:

Divisibility

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division. We remarked a while ago that it's not always possible to do division inside $\mathbb{Z}$ or $\mathbb{N}$: that suggests there's something interesting going on!
Here's the basic definition:

Definition

Let a and b be integers. We say that a *divides* b if there exists an integer n such that $an = b$.

Divisibility

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division. We remarked a while ago that it's not always possible to do division inside $\mathbb{Z}$ or $\mathbb{N}$: that suggests there's something interesting going on!
Here's the basic definition:

Definition

Let a and b be integers. We say that a *divides* b if there exists an integer n such that $an = b$.
We also might say that b *is a multiple of* a,

Divisibility

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division. We remarked a while ago that it's not always possible to do division inside $\mathbb{Z}$ or $\mathbb{N}$: that suggests there's something interesting going on!
Here's the basic definition:

Definition

Let a and b be integers. We say that a *divides* b if there exists an integer n such that $an = b$.
We also might say that b *is a multiple of* a, or that a *is a divisor of* b,

Divisibility

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division. We remarked a while ago that it's not always possible to do division inside $\mathbb{Z}$ or $\mathbb{N}$: that suggests there's something interesting going on!
Here's the basic definition:

Definition

Let a and b be integers. We say that *a divides b* if there exists an integer n such that $an = b$.
We also might say that *b is a multiple of a*, or that *a is a divisor of b*, or that *a is a factor of b*,

Divisibility

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division. We remarked a while ago that it's not always possible to do division inside $\mathbb{Z}$ or $\mathbb{N}$: that suggests there's something interesting going on!
Here's the basic definition:

Definition

Let a and b be integers. We say that *a divides b* if there exists an integer n such that $an = b$.
We also might say that *b is a multiple of a*, or that *a is a divisor of b*, or that *a is a factor of b*, or that *a goes into b*.

Divisibility

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division. We remarked a while ago that it's not always possible to do division inside $\mathbb{Z}$ or $\mathbb{N}$: that suggests there's something interesting going on!
Here's the basic definition:

Definition

Let a and b be integers. We say that *a divides b* if there exists an integer n such that $an = b$.
We also might say that *b is a multiple of a*, or that *a is a divisor of b*, or that *a is a factor of b*, or that *a goes into b*.
In symbols, we write $a \mid b$ to say that a divides b,

Divisibility

The most obvious way to start investigating properties of $\mathbb{N}$ and $\mathbb{Z}$ is to ask about division. We remarked a while ago that it's not always possible to do division inside $\mathbb{Z}$ or $\mathbb{N}$: that suggests there's something interesting going on!
Here's the basic definition:

Definition

Let a and b be integers. We say that a *divides* b if there exists an integer n such that $an = b$.
We also might say that b *is a multiple of* a, or that a *is a divisor of* b, or that a *is a factor of* b, or that a *goes into* b.
In symbols, we write $a \mid b$ to say that a divides b, and write $a \nmid b$ to say that a does not divide b.

Examples

Examples

For example, $91 = 7 \times 13$, so we have $7 \mid 91$.

Examples

For example, $91 = 7 \times 13$, so we have $7 \mid 91$. Also, $91 = (-7) \times (-13)$, so we have $-7 \mid 91$.

Examples

For example, $91 = 7 \times 13$, so we have $7 \mid 91$. Also, $91 = (-7) \times (-13)$, so we have $-7 \mid 91$. Also, $-91 = 7 \times (-13)$, so we have $7 \mid -91$.

Examples

For example, $91 = 7 \times 13$, so we have $7 \mid 91$. Also, $91 = (-7) \times (-13)$, so we have $-7 \mid 91$. Also, $-91 = 7 \times (-13)$, so we have $7 \mid -91$.
However, 7 cannot be written as an integer multiple of 91, so we have $91 \nmid 7$.

Examples

For example, $91 = 7 \times 13$, so we have $7 \mid 91$. Also, $91 = (-7) \times (-13)$, so we have $-7 \mid 91$. Also, $-91 = 7 \times (-13)$, so we have $7 \mid -91$.
However, 7 cannot be written as an integer multiple of 91, so we have $91 \nmid 7$.

Remark

What does it mean to say that *a* does not divide *b*? Well, it means:

Examples

For example, $91 = 7 \times 13$, so we have $7 \mid 91$. Also, $91 = (-7) \times (-13)$, so we have $-7 \mid 91$. Also, $-91 = 7 \times (-13)$, so we have $7 \mid -91$.
However, 7 cannot be written as an integer multiple of 91, so we have $91 \nmid 7$.

Remark

What does it mean to say that a does not divide b? Well, it means:

there does not exist any integer n, such that $an = b$,

Examples

For example, $91 = 7 \times 13$, so we have $7 \mid 91$. Also, $91 = (-7) \times (-13)$, so we have $-7 \mid 91$. Also, $-91 = 7 \times (-13)$, so we have $7 \mid -91$.
However, 7 cannot be written as an integer multiple of 91, so we have $91 \nmid 7$.

Remark

What does it mean to say that a does not divide b? Well, it means:

there does not exist any integer n, such that $an = b$, or

(equivalently)

Examples

For example, $91 = 7 \times 13$, so we have $7 \mid 91$. Also, $91 = (-7) \times (-13)$, so we have $-7 \mid 91$. Also, $-91 = 7 \times (-13)$, so we have $7 \mid -91$.
However, 7 cannot be written as an integer multiple of 91, so we have $91 \nmid 7$.

Remark

What does it mean to say that a does not divide b? Well, it means:

there does not exist any integer n, such that $an = b$, or

(equivalently)

for all $n \in \mathbb{Z}$, we have $an \neq b$.

The trivial cases

The trivial cases

It’s worth sorting out the trivial cases:

The trivial cases

It's worth sorting out the trivial cases:

- When do we have $a \mid 0$?

The trivial cases

It's worth sorting out the trivial cases:

- When do we have $a \mid 0$?

  Always (since $a0 = 0$ for all a).

The trivial cases

It's worth sorting out the trivial cases:

- When do we have $a \mid 0$?

  Always (since $a0 = 0$ for all a).

- When do we have $0 \mid b$?

The trivial cases

It's worth sorting out the trivial cases:

- When do we have $a \mid 0$?

  Always (since $a0 = 0$ for all a).

- When do we have $0 \mid b$?

  When $b = 0$.

The trivial cases

It's worth sorting out the trivial cases:

- When do we have $a \mid 0$?
  Always (since $a0 = 0$ for all a).
- When do we have $0 \mid b$?
  When $b = 0$.
- When do we have $a \mid 1$?

The trivial cases

It's worth sorting out the trivial cases:

- When do we have $a \mid 0$?

  Always (since $a0 = 0$ for all a).

- When do we have $0 \mid b$?

  When $b = 0$.

- When do we have $a \mid 1$?

  When $a = \pm 1$.

The trivial cases

It's worth sorting out the trivial cases:

- When do we have $a \mid 0$?
  Always (since $a0 = 0$ for all a).
- When do we have $0 \mid b$?
  When $b = 0$.
- When do we have $a \mid 1$?
  When $a = \pm 1$.
- When do we have $1 \mid b$?

The trivial cases

It's worth sorting out the trivial cases:

- When do we have $a \mid 0$?
  Always (since $a0 = 0$ for all a).
- When do we have $0 \mid b$?
  When $b = 0$.
- When do we have $a \mid 1$?
  When $a = \pm 1$.
- When do we have $1 \mid b$?
  Always (since $1b = b$ for all b).

The trivial cases

It's worth sorting out the trivial cases:

- When do we have $a \mid 0$?

  Always (since $a0 = 0$ for all a).

- When do we have $0 \mid b$?

  When $b = 0$.

- When do we have $a \mid 1$?

  When $a = \pm 1$.

- When do we have $1 \mid b$?

  Always (since $1b = b$ for all b).

For the next few lectures, we'll be studying the integers from the point of view of divisibility.