MAS114: Lecture 19

James Cranch

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

2021–2022

Reading group

Reading group

A second-year student is running a reading group on modern algebra: meeting in Hicks K14 at 3pm on Wednesdays. All are welcome!

An example

An example

Let's see an example.

Suppose Bob has low opinions of Eve's calculational skills, and chooses to use the (unrealistically small) primes $p = 101$ and $q = 103$.

An example

Let's see an example.
Suppose Bob has low opinions of Eve's calculational skills, and chooses to use the (unrealistically small) primes $p = 101$ and $q = 103$. Then $pq = 10403$.

An example

Let's see an example.
Suppose Bob has low opinions of Eve's calculational skills, and chooses to use the (unrealistically small) primes $p = 101$ and $q = 103$. Then $pq = 10403$. Suppose also that Bob chooses $e = 71$ for the exponent used for encryption.

An example

Let's see an example.
Suppose Bob has low opinions of Eve's calculational skills, and chooses to use the (unrealistically small) primes $p = 101$ and $q = 103$. Then $pq = 10403$. Suppose also that Bob chooses $e = 71$ for the exponent used for encryption.
Bob advertises that his public key is $pq = 10403$, $e = 71$.

An example

Let's see an example.
Suppose Bob has low opinions of Eve's calculational skills, and chooses to use the (unrealistically small) primes $p = 101$ and $q = 103$. Then $pq = 10403$. Suppose also that Bob chooses $e = 71$ for the exponent used for encryption.
Bob advertises that his public key is $pq = 10403$, $e = 71$. He must work out his private key, by inverting 71 modulo $(p-1)(q-1) = 10200$.

An example

Let's see an example.
Suppose Bob has low opinions of Eve's calculational skills, and chooses to use the (unrealistically small) primes $p = 101$ and $q = 103$. Then $pq = 10403$. Suppose also that Bob chooses $e = 71$ for the exponent used for encryption.
Bob advertises that his public key is $pq = 10403$, $e = 71$. He must work out his private key, by inverting 71 modulo $(p-1)(q-1) = 10200$. A quick use of Euclid's algorithm will do this for him, and he gets that $71^{-1} \equiv 431$.

An example

Let's see an example.
Suppose Bob has low opinions of Eve's calculational skills, and chooses to use the (unrealistically small) primes $p = 101$ and $q = 103$. Then $pq = 10403$. Suppose also that Bob chooses $e = 71$ for the exponent used for encryption.
Bob advertises that his public key is $pq = 10403$, $e = 71$. He must work out his private key, by inverting 71 modulo $(p-1)(q-1) = 10200$. A quick use of Euclid's algorithm will do this for him, and he gets that $71^{-1} \equiv 431$. Indeed,

$$71 \times 431 = 30601 = 3 \times 10200 + 1.$$

An example

Let's see an example.
Suppose Bob has low opinions of Eve's calculational skills, and chooses to use the (unrealistically small) primes $p = 101$ and $q = 103$. Then $pq = 10403$. Suppose also that Bob chooses $e = 71$ for the exponent used for encryption.
Bob advertises that his public key is $pq = 10403$, $e = 71$. He must work out his private key, by inverting 71 modulo $(p-1)(q-1) = 10200$. A quick use of Euclid's algorithm will do this for him, and he gets that $71^{-1} \equiv 431$. Indeed,

$$71 \times 431 = 30601 = 3 \times 10200 + 1.$$

Thus his private key is $pq = 10403$, $d = 431$.

An example

Let's see an example.
Suppose Bob has low opinions of Eve's calculational skills, and chooses to use the (unrealistically small) primes $p = 101$ and $q = 103$. Then $pq = 10403$. Suppose also that Bob chooses $e = 71$ for the exponent used for encryption.
Bob advertises that his public key is $pq = 10403$, $e = 71$. He must work out his private key, by inverting 71 modulo $(p-1)(q-1) = 10200$. A quick use of Euclid's algorithm will do this for him, and he gets that $71^{-1} \equiv 431$. Indeed,

$$71 \times 431 = 30601 = 3 \times 10200 + 1.$$

Thus his private key is $pq = 10403$, $d = 431$.
Suppose Alice decides she needs to send Bob message 1245,

An example

Let's see an example.
Suppose Bob has low opinions of Eve's calculational skills, and chooses to use the (unrealistically small) primes $p = 101$ and $q = 103$. Then $pq = 10403$. Suppose also that Bob chooses $e = 71$ for the exponent used for encryption.
Bob advertises that his public key is $pq = 10403$, $e = 71$. He must work out his private key, by inverting 71 modulo $(p-1)(q-1) = 10200$. A quick use of Euclid's algorithm will do this for him, and he gets that $71^{-1} \equiv 431$. Indeed,

$$71 \times 431 = 30601 = 3 \times 10200 + 1.$$

Thus his private key is $pq = 10403$, $d = 431$.
Suppose Alice decides she needs to send Bob message 1245, which they've agreed in advance should mean "please meet me after this lecture".

The calculations

The calculations

Then Alice has to calculate 1245^{71} modulo 10403.

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$1245^{71}$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$1245^{71} \equiv 1245 \cdot 1245^{70}$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$1245^{71} \equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35}$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$1245^{71} \equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35}$$

$$\equiv 1245 \cdot 10381^{35}$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$1245^{71} \equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35}$$
$$\equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34}$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$1245^{71} \equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35}$$
$$\equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17}$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$
\begin{aligned}
1245^{71} &\equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\
&\equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\
&\equiv 3819 \cdot 484^{17}
\end{aligned}
$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$
\begin{aligned}
1245^{71} \equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\
\equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\
\equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16}
\end{aligned}
$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$
\begin{aligned}
1245^{71} \equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\
\equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\
\equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} \equiv 7065 \cdot (484^2)^{8}
\end{aligned}
$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$
\begin{aligned}
1245^{71} &\equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\
&\equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\
&\equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} \equiv 7065 \cdot (484^2)^{8} \\
&\equiv 7065 \cdot 5390^{8}
\end{aligned}
$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$
\begin{aligned}
1245^{71} \equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\
\equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\
\equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} \equiv 7065 \cdot (484^2)^{8} \\
\equiv 7065 \cdot 5390^{8} \equiv 7065 \cdot (5390^2)^{4}
\end{aligned}
$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$\begin{aligned}
1245^{71} &\equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\
&\equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\
&\equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} \equiv 7065 \cdot (484^2)^8 \\
&\equiv 7065 \cdot 5390^8 \equiv 7065 \cdot (5390^2)^4 \equiv 7065 \cdot 6924^4
\end{aligned}$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$
\begin{aligned}
1245^{71} &\equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\
&\equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\
&\equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} \equiv 7065 \cdot (484^2)^8 \\
&\equiv 7065 \cdot 5390^8 \equiv 7065 \cdot (5390^2)^4 \equiv 7065 \cdot 6924^4 \\
&\equiv 7065 \cdot (6924^2)^2
\end{aligned}
$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$
\begin{aligned}
1245^{71} &\equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\
&\equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\
&\equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} \equiv 7065 \cdot (484^2)^{8} \\
&\equiv 7065 \cdot 5390^{8} \equiv 7065 \cdot (5390^2)^{4} \equiv 7065 \cdot 6924^{4} \\
&\equiv 7065 \cdot (6924^2)^{2} \equiv 7065 \cdot 4752^{2}
\end{aligned}
$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$\begin{aligned}
1245^{71} &\equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\
&\equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\
&\equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} \equiv 7065 \cdot (484^2)^8 \\
&\equiv 7065 \cdot 5390^8 \equiv 7065 \cdot (5390^2)^4 \equiv 7065 \cdot 6924^4 \\
&\equiv 7065 \cdot (6924^2)^2 \equiv 7065 \cdot 4752^2 \\
&\equiv 7065 \cdot 6994
\end{aligned}$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$
\begin{aligned}
1245^{71} &\equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\
&\equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\
&\equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} \equiv 7065 \cdot (484^2)^8 \\
&\equiv 7065 \cdot 5390^8 \equiv 7065 \cdot (5390^2)^4 \equiv 7065 \cdot 6924^4 \\
&\equiv 7065 \cdot (6924^2)^2 \equiv 7065 \cdot 4752^2 \\
&\equiv 7065 \cdot 6994 \equiv 8763.
\end{aligned}
$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$\begin{aligned}
1245^{71} &\equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\
&\equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\
&\equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} \equiv 7065 \cdot (484^2)^8 \\
&\equiv 7065 \cdot 5390^8 \equiv 7065 \cdot (5390^2)^4 \equiv 7065 \cdot 6924^4 \\
&\equiv 7065 \cdot (6924^2)^2 \equiv 7065 \cdot 4752^2 \\
&\equiv 7065 \cdot 6994 \equiv 8763.
\end{aligned}$$

So she sends Bob 8763.

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$
\begin{aligned}
1245^{71} &\equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\
&\equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\
&\equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} \equiv 7065 \cdot (484^2)^8 \\
&\equiv 7065 \cdot 5390^8 \equiv 7065 \cdot (5390^2)^4 \equiv 7065 \cdot 6924^4 \\
&\equiv 7065 \cdot (6924^2)^2 \equiv 7065 \cdot 4752^2 \\
&\equiv 7065 \cdot 6994 \equiv 8763.
\end{aligned}
$$

So she sends Bob 8763.

Bob receives this, and his task then is to calculate 8763^{431} modulo 10403.

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$\begin{aligned} 1245^{71} &\equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\ \equiv 1245 \cdot 10381^{35} &\equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\ &\equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} \equiv 7065 \cdot (484^2)^8 \\ &\equiv 7065 \cdot 5390^8 \equiv 7065 \cdot (5390^2)^4 \equiv 7065 \cdot 6924^4 \\ &\equiv 7065 \cdot (6924^2)^2 \equiv 7065 \cdot 4752^2 \\ &\equiv 7065 \cdot 6994 \equiv 8763. \end{aligned}$$

So she sends Bob 8763.
Bob receives this, and his task then is to calculate 8763^{431} modulo 10403. A similar strategy makes this possible, too, and he finds that

$$8763^{431} \equiv 1245 \pmod{10403},$$

so he has reconstructed Alice's message.

Square roots of 2

Square roots of 2

We've spent nine lectures now talking about $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$, laying the foundations of number theory.

Square roots of 2

We've spent nine lectures now talking about $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$, laying the foundations of number theory. The rest of this course will be about $\mathbb{R}$.

Square roots of 2

We've spent nine lectures now talking about $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$, laying the foundations of number theory. The rest of this course will be about $\mathbb{R}$. Perhaps sensibly enough, the study of $\mathbb{R}$ is called *real analysis*.

Square roots of 2

We've spent nine lectures now talking about $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$, laying the foundations of number theory. The rest of this course will be about $\mathbb{R}$. Perhaps sensibly enough, the study of $\mathbb{R}$ is called *real analysis*. Let's set ourselves back to a time before $\mathbb{R}$ was invented, and ask: why was it necessary to invent it?

Square roots of 2

We've spent nine lectures now talking about $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$, laying the foundations of number theory. The rest of this course will be about $\mathbb{R}$. Perhaps sensibly enough, the study of $\mathbb{R}$ is called *real analysis*. Let's set ourselves back to a time before $\mathbb{R}$ was invented, and ask: why was it necessary to invent it? Why should we feel that $\mathbb{Q}$ is not enough?

Square roots of 2

We've spent nine lectures now talking about $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$, laying the foundations of number theory. The rest of this course will be about $\mathbb{R}$. Perhaps sensibly enough, the study of $\mathbb{R}$ is called *real analysis*.
Let's set ourselves back to a time before $\mathbb{R}$ was invented, and ask: why was it necessary to invent it? Why should we feel that $\mathbb{Q}$ is not enough?
The result that set the ancient Greeks thinking was this:

No rational square root of two

No rational square root of two

Theorem

There is no rational number $x \in \mathbb{Q}$ *such that* $x^2 = 2$.

No rational square root of two

Theorem

There is no rational number $x \in \mathbb{Q}$ such that $x^2 = 2$.

Proof.

We'll prove this by contradiction; suppose there is such a number $x \in \mathbb{Q}$. Because it's in $\mathbb{Q}$, it takes the form $x = p/q$ for some integers p and q with $q \neq 0$.

We may as well take p and q to be coprime ("in lowest terms").

Then we have $p^2/q^2 = x^2 = 2$, so $p^2 = 2q^2$ with p and q coprime.

Now, the right-hand side is even (it's given as a multiple of 2, so the left-hand side, p^2 must be even too. That means that p itself must be even: so we can write $p = 2r$.

Then we have $(2r)^2 = 2q^2$, which simplifies to $4r^2 = 2q^2$, or $2r^2 = q^2$. Here the left-hand side is even, so q^2 must be even. Hence q itself must be even.

This is a contradiction: p and q can't both be even. So our initial assumption is absurd, and there is no rational x with $x^2 = 2$. $\square$

Comments

Comments

Remark

I felt obliged to word the statement of that theorem fairly carefully.

Comments

Remark

I felt obliged to word the statement of that theorem fairly carefully. What I wanted to say, of course, was:

The number $\sqrt{2}$ *is not in* $\mathbb{Q}$.

Comments

Remark

I felt obliged to word the statement of that theorem fairly carefully. What I wanted to say, of course, was:

The number $\sqrt{2}$ *is not in* $\mathbb{Q}$.

But I want to flag that up as being possibly inappropriate: our aim in this section is to define the reals.

Comments

Remark

I felt obliged to word the statement of that theorem fairly carefully. What I wanted to say, of course, was:

The number $\sqrt{2}$ *is not in* $\mathbb{Q}$.

But I want to flag that up as being possibly inappropriate: our aim in this section is to define the reals. We shouldn't even be confident that $\sqrt{2}$ exists yet.

Comments

Remark

I felt obliged to word the statement of that theorem fairly carefully. What I wanted to say, of course, was:

The number $\sqrt{2}$ *is not in* $\mathbb{Q}$.

But I want to flag that up as being possibly inappropriate: our aim in this section is to define the reals. We shouldn't even be confident that $\sqrt{2}$ exists yet.
However, thanks to this theorem, we can be confident at least that there's no number *inside* $\mathbb{Q}$ which deserves to be called $\sqrt{2}$.

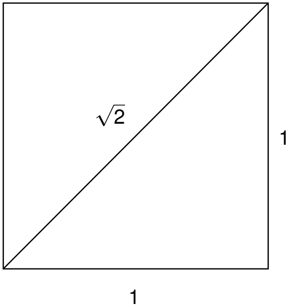
Irrational numbers

Irrational numbers

This, to the Greeks, was evidence that there was a world beyond $\mathbb{Q}$; a world of *irrational numbers* (numbers not in $\mathbb{Q}$).

Irrational numbers

This, to the Greeks, was evidence that there was a world beyond $\mathbb{Q}$; a world of *irrational numbers* (numbers not in $\mathbb{Q}$). They needed a number called $\sqrt{2}$, so they could talk about the diagonal of a unit square:



Irrational numbers today

Irrational numbers today

Over the years, more and more examples were found of numbers which one might want to talk about, but which cannot be in $\mathbb{Q}$: various powers, logarithms, sines, cosines, and other constructions besides.

Irrational numbers today

Over the years, more and more examples were found of numbers which one might want to talk about, but which cannot be in $\mathbb{Q}$: various powers, logarithms, sines, cosines, and other constructions besides.

One high point includes the proof by Lambert in 1761 that π and e are irrational.

Irrational numbers today

Over the years, more and more examples were found of numbers which one might want to talk about, but which cannot be in $\mathbb{Q}$: various powers, logarithms, sines, cosines, and other constructions besides.

One high point includes the proof by Lambert in 1761 that π and e are irrational.

On the other hand, modern mathematics is still not particularly good, in general, at proving that numbers are irrational.

Irrational numbers today

Over the years, more and more examples were found of numbers which one might want to talk about, but which cannot be in $\mathbb{Q}$: various powers, logarithms, sines, cosines, and other constructions besides.

One high point includes the proof by Lambert in 1761 that π and e are irrational.

On the other hand, modern mathematics is still not particularly good, in general, at proving that numbers are irrational. For example, if you want to become famous, simply prove (please. . .) that any one of the following numbers are irrational:

$$\pi + e,$$

Irrational numbers today

Over the years, more and more examples were found of numbers which one might want to talk about, but which cannot be in $\mathbb{Q}$: various powers, logarithms, sines, cosines, and other constructions besides.

One high point includes the proof by Lambert in 1761 that π and e are irrational.

On the other hand, modern mathematics is still not particularly good, in general, at proving that numbers are irrational. For example, if you want to become famous, simply prove (please. . .) that any one of the following numbers are irrational:

$$\pi + e, \quad \pi - e,$$

Irrational numbers today

Over the years, more and more examples were found of numbers which one might want to talk about, but which cannot be in $\mathbb{Q}$: various powers, logarithms, sines, cosines, and other constructions besides.

One high point includes the proof by Lambert in 1761 that π and e are irrational.

On the other hand, modern mathematics is still not particularly good, in general, at proving that numbers are irrational. For example, if you want to become famous, simply prove (please...) that any one of the following numbers are irrational:

$$\pi + e, \quad \pi - e, \quad \pi e,$$

Irrational numbers today

Over the years, more and more examples were found of numbers which one might want to talk about, but which cannot be in $\mathbb{Q}$: various powers, logarithms, sines, cosines, and other constructions besides.
One high point includes the proof by Lambert in 1761 that π and e are irrational.
On the other hand, modern mathematics is still not particularly good, in general, at proving that numbers are irrational. For example, if you want to become famous, simply prove (please. . .) that any one of the following numbers are irrational:

$$\pi + e, \quad \pi - e, \quad \pi e, \quad \pi / e,$$

Irrational numbers today

Over the years, more and more examples were found of numbers which one might want to talk about, but which cannot be in $\mathbb{Q}$: various powers, logarithms, sines, cosines, and other constructions besides.
One high point includes the proof by Lambert in 1761 that π and e are irrational.
On the other hand, modern mathematics is still not particularly good, in general, at proving that numbers are irrational. For example, if you want to become famous, simply prove (please...) that any one of the following numbers are irrational:

$$\pi + e, \quad \pi - e, \quad \pi e, \quad \pi / e, \quad \ln \pi,$$

Irrational numbers today

Over the years, more and more examples were found of numbers which one might want to talk about, but which cannot be in $\mathbb{Q}$: various powers, logarithms, sines, cosines, and other constructions besides.

One high point includes the proof by Lambert in 1761 that π and e are irrational.

On the other hand, modern mathematics is still not particularly good, in general, at proving that numbers are irrational. For example, if you want to become famous, simply prove (please...) that any one of the following numbers are irrational:

$$\pi + e, \quad \pi - e, \quad \pi e, \quad \pi/e, \quad \ln \pi, \quad e^e,$$

Irrational numbers today

Over the years, more and more examples were found of numbers which one might want to talk about, but which cannot be in $\mathbb{Q}$: various powers, logarithms, sines, cosines, and other constructions besides.

One high point includes the proof by Lambert in 1761 that π and e are irrational.

On the other hand, modern mathematics is still not particularly good, in general, at proving that numbers are irrational. For example, if you want to become famous, simply prove (please. . .) that any one of the following numbers are irrational:

$$\pi + e, \quad \pi - e, \quad \pi e, \quad \pi/e, \quad \ln \pi, \quad e^e, \quad e^{e^e}.$$

Investigating the reals

Investigating the reals

For centuries, the real numbers were considered in an informal way: nobody knew exactly how to define $\mathbb{R}$, but they knew what it ought to look like.

Investigating the reals

For centuries, the real numbers were considered in an informal way: nobody knew exactly how to define $\mathbb{R}$, but they knew what it ought to look like.

For the time being, and *for the time being only* we'll investigate the reals in a similar, informal way.

Investigating the reals

For centuries, the real numbers were considered in an informal way: nobody knew exactly how to define $\mathbb{R}$, but they knew what it ought to look like.
For the time being, and *for the time being only* we'll investigate the reals in a similar, informal way. For now, you can regard the real numbers $\mathbb{R}$ as being built out of decimals (as you did at school).

Investigating the reals

For centuries, the real numbers were considered in an informal way: nobody knew exactly how to define $\mathbb{R}$, but they knew what it ought to look like.

For the time being, and *for the time being only* we'll investigate the reals in a similar, informal way. For now, you can regard the real numbers $\mathbb{R}$ as being built out of decimals (as you did at school). In the last lecture of the course, we'll sort this out, and consider a modern construction of the reals.

A picture

A picture

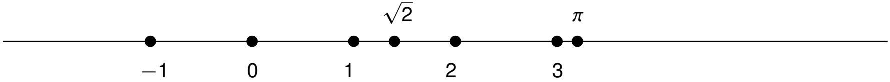
Our mental picture of the reals should be a picture of a numberline.

A picture

Our mental picture of the reals should be a picture of a numberline. Here's a numberline with some interesting points marked on:

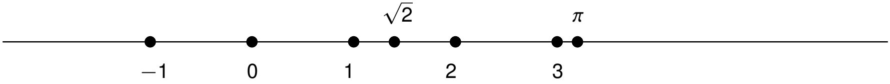
A picture

Our mental picture of the reals should be a picture of a numberline. Here's a numberline with some interesting points marked on:



A picture

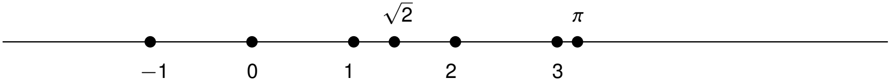
Our mental picture of the reals should be a picture of a numberline. Here's a numberline with some interesting points marked on:



I've marked on the integers -1, 0, 1, 2 and 3, which are all in $\mathbb{Z}$ and hence in $\mathbb{Q}$.

A picture

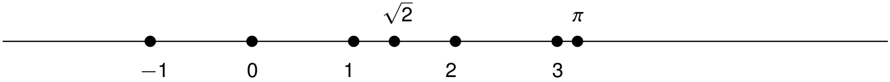
Our mental picture of the reals should be a picture of a numberline. Here's a numberline with some interesting points marked on:



I've marked on the integers -1, 0, 1, 2 and 3, which are all in $\mathbb{Z}$ and hence in $\mathbb{Q}$.
I've also marked on $\sqrt{2}$, which we now know to be irrational, and π, which I've claimed to you is irrational: these things are in the set $\mathbb{R}\backslash\mathbb{Q}$ of irrational numbers.

A picture

Our mental picture of the reals should be a picture of a numberline. Here's a numberline with some interesting points marked on:



I've marked on the integers -1, 0, 1, 2 and 3, which are all in $\mathbb{Z}$ and hence in $\mathbb{Q}$.

I've also marked on $\sqrt{2}$, which we now know to be irrational, and π, which I've claimed to you is irrational: these things are in the set $\mathbb{R}\backslash\mathbb{Q}$ of irrational numbers.

In my mind, I think of the real numbers $\mathbb{R}$ as a solid line, and the rational numbers $\mathbb{Q}$ as a very fine gauze net stretched out within it.

The rationals in $\mathbb{R}$

The rationals in $\mathbb{R}$

Bear in mind that that the rationals $\mathbb{Q}$ are a lovely system of numbers: we can add and subtract and multiply and divide rationals and remain inside the rationals.

The rationals in $\mathbb{R}$

Bear in mind that that the rationals $\mathbb{Q}$ are a lovely system of numbers: we can add and subtract and multiply and divide rationals and remain inside the rationals. Formally: if $x \in \mathbb{Q}$ and $y \in \mathbb{Q}$, then $x + y$, $x - y$, xy and x/y (if y is nonzero) are all elements of $\mathbb{Q}$.

The rationals in $\mathbb{R}$

Bear in mind that that the rationals $\mathbb{Q}$ are a lovely system of numbers: we can add and subtract and multiply and divide rationals and remain inside the rationals. Formally: if $x \in \mathbb{Q}$ and $y \in \mathbb{Q}$, then $x + y$, $x - y$, xy and x/y (if y is nonzero) are all elements of $\mathbb{Q}$. We say that $\mathbb{Q}$ is *closed* under addition, subtraction, multiplication and division.

The rationals in $\mathbb{R}$

Bear in mind that that the rationals $\mathbb{Q}$ are a lovely system of numbers: we can add and subtract and multiply and divide rationals and remain inside the rationals. Formally: if $x \in \mathbb{Q}$ and $y \in \mathbb{Q}$, then $x + y$, $x - y$, xy and x/y (if y is nonzero) are all elements of $\mathbb{Q}$. We say that $\mathbb{Q}$ is *closed* under addition, subtraction, multiplication and division.
The reals $\mathbb{R}$ are also a lovely system of numbers, closed not just those four operations but many others: square roots (of positive numbers), sines, cosines, and so on.

The irrationals in $\mathbb{R}$

The irrationals in $\mathbb{R}$

The irrational numbers $\mathbb{R} \backslash \mathbb{Q}$ are not a lovely system of numbers: they are not closed under any of these things.

The irrationals in $\mathbb{R}$

The irrational numbers $\mathbb{R}\backslash\mathbb{Q}$ are not a lovely system of numbers: they are not closed under any of these things.
For example, can we think of two irrational numbers whose sum is rational?

$$\sqrt{2} + (1 - \sqrt{2}) = 1.$$

The irrationals in $\mathbb{R}$

The irrational numbers $\mathbb{R} \backslash \mathbb{Q}$ are not a lovely system of numbers: they are not closed under any of these things.
For example, can we think of two irrational numbers whose sum is rational?

$$\sqrt{2} + (1 - \sqrt{2}) = 1.$$

Can we think of two irrational numbers whose product is rational?

$$(\sqrt{2})(\sqrt{2}) = 2.$$

The irrationals in $\mathbb{R}$

The irrational numbers $\mathbb{R}\backslash\mathbb{Q}$ are not a lovely system of numbers: they are not closed under any of these things.
For example, can we think of two irrational numbers whose sum is rational?

$$\sqrt{2} + (1 - \sqrt{2}) = 1.$$

Can we think of two irrational numbers whose product is rational?

$$(\sqrt{2})(\sqrt{2}) = 2.$$

So, the irrational numbers $\mathbb{R}\backslash\mathbb{Q}$ really are just the big messy clump left over in $\mathbb{R}$ when you remove $\mathbb{Q}$.

Irrationals and rationals

Irrationals and rationals

However, at least the following is true:

Irrationals and rationals

However, at least the following is true:

Proposition

Let x be irrational, and y be rational. Then $x + y$ is irrational. Also, if y is nonzero, then xy is irrational.

Irrationals and rationals

However, at least the following is true:

Proposition

Let x be irrational, and y be rational. Then $x + y$ is irrational. Also, if y is nonzero, then xy is irrational.

Proof.

We prove the first one by contradiction. Suppose that $x + y$ is rational. Then $(x + y) - y$ is also rational, being obtained by subtracting two rational numbers, but it's equal to x which we know to be irrational. That's the contradiction we wanted.

Irrationals and rationals

However, at least the following is true:

Proposition

Let x be irrational, and y be rational. Then $x + y$ is irrational. Also, if y is nonzero, then xy is irrational.

Proof.

We prove the first one by contradiction. Suppose that $x + y$ is rational. Then $(x + y) - y$ is also rational, being obtained by subtracting two rational numbers, but it's equal to x which we know to be irrational. That's the contradiction we wanted.
We prove the second one by contradiction too. Suppose that xy is rational. Then $(xy)/y$ is also rational, as it's obtained by dividing two rational numbers (with the latter nonzero), but it's equal to x which we know to be irrational. That's the contradiction we wanted. □

Approximation

Approximation

Now our mission is to study the real numbers.

Approximation

Now our mission is to study the real numbers. When we were studying the integers, the main theme running through it all was to do with divisibility.

Approximation

Now our mission is to study the real numbers. When we were studying the integers, the main theme running through it all was to do with divisibility. Divisibility is, of course, not a very sensible thing to ask about over the reals.

Approximation

Now our mission is to study the real numbers. When we were studying the integers, the main theme running through it all was to do with divisibility. Divisibility is, of course, not a very sensible thing to ask about over the reals.

As a result, real analysis (the study of $\mathbb{R}$), and the questions which are interesting and helpful to ask, is very different to number theory.

Approximation

Now our mission is to study the real numbers. When we were studying the integers, the main theme running through it all was to do with divisibility. Divisibility is, of course, not a very sensible thing to ask about over the reals.

As a result, real analysis (the study of $\mathbb{R}$), and the questions which are interesting and helpful to ask, is very different to number theory.

It turns out that the most interesting things you can ask about are to do with *approximation*.

Approximation

Now our mission is to study the real numbers. When we were studying the integers, the main theme running through it all was to do with divisibility. Divisibility is, of course, not a very sensible thing to ask about over the reals.

As a result, real analysis (the study of $\mathbb{R}$), and the questions which are interesting and helpful to ask, is very different to number theory.

It turns out that the most interesting things you can ask about are to do with *approximation*. Why is the notion of approximation so important?

Convergence

Convergence

When we write that

$$\pi = 3.14159265358979323846264 33 \cdots ,$$

the point is that the digits give a kind of address telling you how to find π on the numberline.

Convergence

When we write that

$$\pi = 3.14159265358979323846264 33 \cdots,$$

the point is that the digits give a kind of address telling you how to find π on the numberline. The number π is close to 3,

Convergence

When we write that

$$\pi = 3.14159265358979323846264 33\cdots ,$$

the point is that the digits give a kind of address telling you how to find π on the numberline. The number π is close to 3, closer to 3.1,

Convergence

When we write that

$$\pi = 3.14159265358979323846264 33\cdots\ ,$$

the point is that the digits give a kind of address telling you how to find π on the numberline. The number π is close to 3, closer to 3.1, closer still to 3.14,

Convergence

When we write that

$$\pi = 3.14159265358979323846264 33\cdots,$$

the point is that the digits give a kind of address telling you how to find π on the numberline. The number π is close to 3, closer to 3.1, closer still to 3.14, even closer still to 3.141, and so on.

Convergence

When we write that

$$\pi = 3.14159265358979323846264433\cdots,$$

the point is that the digits give a kind of address telling you how to find π on the numberline. The number π is close to 3, closer to 3.1, closer still to 3.14, even closer still to 3.141, and so on.

The notion of *convergence*, which I'll define shortly, is a way of encoding this concept of increasingly good approximation.

Convergence

When we write that

$$\pi = 3.14159265358979323846264 33\cdots,$$

the point is that the digits give a kind of address telling you how to find π on the numberline. The number π is close to 3, closer to 3.1, closer still to 3.14, even closer still to 3.141, and so on.

The notion of *convergence*, which I'll define shortly, is a way of encoding this concept of increasingly good approximation. We will say that the sequence of rational numbers

$$3, \quad 3.1, \quad 3.14, \quad 3.141, \quad 3.1415, \quad \ldots$$

"converges to π".

Convergence

When we write that

$$\pi = 3.14159265358979323846264 33 \cdots ,$$

the point is that the digits give a kind of address telling you how to find π on the numberline. The number π is close to 3, closer to 3.1, closer still to 3.14, even closer still to 3.141, and so on.

The notion of *convergence*, which I'll define shortly, is a way of encoding this concept of increasingly good approximation. We will say that the sequence of rational numbers

$$3, \quad 3.1, \quad 3.14, \quad 3.141, \quad 3.1415, \quad \ldots$$

"converges to π". That's supposed to mean that if you follow the address, you'll end up homing in on π.

Convergence

When we write that

$$\pi = 3.14159265358979323846264 33\cdots ,$$

the point is that the digits give a kind of address telling you how to find π on the numberline. The number π is close to 3, closer to 3.1, closer still to 3.14, even closer still to 3.141, and so on.

The notion of *convergence*, which I'll define shortly, is a way of encoding this concept of increasingly good approximation. We will say that the sequence of rational numbers

$$3, \quad 3.1, \quad 3.14, \quad 3.141, \quad 3.1415, \quad \ldots$$

"converges to π". That's supposed to mean that if you follow the address, you'll end up homing in on π.

The definition will seem complicated, and probably harder to get your head around than other definitions in the course.

Convergence

When we write that

$$\pi = 3.14159265358979323846264 33\cdots,$$

the point is that the digits give a kind of address telling you how to find π on the numberline. The number π is close to 3, closer to 3.1, closer still to 3.14, even closer still to 3.141, and so on.

The notion of *convergence*, which I'll define shortly, is a way of encoding this concept of increasingly good approximation. We will say that the sequence of rational numbers

$$3, \quad 3.1, \quad 3.14, \quad 3.141, \quad 3.1415, \quad \ldots$$

"converges to π". That's supposed to mean that if you follow the address, you'll end up homing in on π.

The definition will seem complicated, and probably harder to get your head around than other definitions in the course. However, that's because it really is a subtle concept: all the simpler approaches you might think of are wrong.

Wrong approach 1

Wrong approach 1

The most obvious wrong definition is this:

Wrong approach 1

The most obvious wrong definition is this:

Completely wrong definition

A sequence $a_0, a_1, a_2, \ldots$ *converges to x* if it gets closer and closer to x.

Wrong approach 1

The most obvious wrong definition is this:

Completely wrong definition

A sequence $a_0, a_1, a_2, \ldots$ *converges to x* if it gets closer and closer to x. In other words, if

$$|a_0 - x| > |a_1 - x| > |a_2 - x| > \cdots .$$

Wrong approach 1, continued

Wrong approach 1, continued

Why is this completely wrong? Well, for example, the sequence

$$3, \quad 3.1, \quad 3.14, \quad 3.141, \quad 3.1415, \quad \ldots$$

also gets closer and closer to 1000:

Wrong approach 1, continued

Why is this completely wrong? Well, for example, the sequence

$$3, \quad 3.1, \quad 3.14, \quad 3.141, \quad 3.1415, \quad \ldots$$

also gets closer and closer to 1000:

$$1000 - 3 \qquad = 997$$

Wrong approach 1, continued

Why is this completely wrong? Well, for example, the sequence

$$3, \quad 3.1, \quad 3.14, \quad 3.141, \quad 3.1415, \quad \ldots$$

also gets closer and closer to 1000:

$$\begin{aligned} 1000 - 3 &= 997 \\ 1000 - 3.1 &= 996.9 \end{aligned}$$

Wrong approach 1, continued

Why is this completely wrong? Well, for example, the sequence

$$3, \quad 3.1, \quad 3.14, \quad 3.141, \quad 3.1415, \quad \ldots$$

also gets closer and closer to 1000:

$$\begin{aligned} 1000 - 3 &= 997 \\ 1000 - 3.1 &= 996.9 \\ 1000 - 3.14 &= 996.86 \end{aligned}$$

Wrong approach 1, continued

Why is this completely wrong? Well, for example, the sequence

$$3, \quad 3.1, \quad 3.14, \quad 3.141, \quad 3.1415, \quad \ldots$$

also gets closer and closer to 1000:

$$\begin{aligned} 1000 - 3 &= 997 \\ 1000 - 3.1 &= 996.9 \\ 1000 - 3.14 &= 996.86 \\ 1000 - 3.141 &= 996.859 \end{aligned}$$

Wrong approach 1, continued

Why is this completely wrong? Well, for example, the sequence

$$3, \quad 3.1, \quad 3.14, \quad 3.141, \quad 3.1415, \quad \ldots$$

also gets closer and closer to 1000:

$$\begin{aligned} 1000 - 3 &= 997 \\ 1000 - 3.1 &= 996.9 \\ 1000 - 3.14 &= 996.86 \\ 1000 - 3.141 &= 996.859 \\ 1000 - 3.1415 &= 996.8585 \end{aligned}$$

Wrong approach 1, continued

Why is this completely wrong? Well, for example, the sequence

$$3, \quad 3.1, \quad 3.14, \quad 3.141, \quad 3.1415, \quad \ldots$$

also gets closer and closer to 1000:

$$\begin{aligned} 1000 - 3 &= 997 \\ 1000 - 3.1 &= 996.9 \\ 1000 - 3.14 &= 996.86 \\ 1000 - 3.141 &= 996.859 \\ 1000 - 3.1415 &= 996.8585 \end{aligned}$$

Of course, this sequence never gets particularly close to 1000 (the sequence never goes above 4, so it never gets within 996 of 1000), but it's always getting closer!

Wrong approach 1, continued

Wrong approach 1, continued

But this means that if our definition of “converging to x” were the completely wrong definition “gets closer and closer to x”, then the sequence

$$3, \quad 3.1, \quad 3.14, \quad 3.141, \quad 3.1415, \quad \ldots$$

would “converge to π”,

Wrong approach 1, continued

But this means that if our definition of “converging to x” were the completely wrong definition “gets closer and closer to x”, then the sequence

$$3, \quad 3.1, \quad 3.14, \quad 3.141, \quad 3.1415, \quad \ldots$$

would “converge to π”, but it would also “converge to 1000”.

Wrong approach 1, continued

But this means that if our definition of “converging to x” were the completely wrong definition “gets closer and closer to x”, then the sequence

$$3, \quad 3.1, \quad 3.14, \quad 3.141, \quad 3.1415, \quad \ldots$$

would “converge to π”, but it would also “converge to 1000”.
But that’s not what we want: this sequence is a terrible way of getting to 1000, but a good way of getting to π.