MT181 Number Systems

Mark Wildon, mark.wildon@rhul.ac.uk

Administration:

- Workshops begin next week.
- Sign-in sheet. **Please return to the lecturer after each lecture.**
- Make sure you get the Section 1 Notes, Problem Sheet 1, and the sheet of Challenge Problems when they are passed around. **Please pass everything onwards, and eventually to the back, even if you the person you are passing to already has a copy.**
- All handouts will be put on Moodle.

MT181 Number Systems

Mark Wildon, mark.wildon@rhul.ac.uk

Administration:

- Workshops begin next week.
- Sign-in sheet. **Please return to the lecturer after each lecture.**
- Make sure you get the Section 1 Notes, Problem Sheet 1, and the sheet of Challenge Problems when they are passed around. **Please pass everything onwards, and eventually to the back, even if you the person you are passing to already has a copy.**
- All handouts will be put on Moodle.
- **Lectures in BLT1:** Tuesday 1pm, Thursday 9am and Friday 2pm.
- **Office hours in McCrea 240:** Monday 4pm, Wednesday 10am and Friday 4pm.

Recommended Reading and Other Resources

[1] *How to think like a mathematician*. Kevin Houston, Cambridge University Press, 2009.

[2] *A concise introduction to pure mathematics*. Martin Liebeck, Chapman and Hall, 2000.

[3] *Discrete Mathematics*. Norman L. Biggs, Oxford University Press, 2002.

- Printed notes. But you should also make your own notes.
- Handouts and slides on Moodle.
- Problem sheets. Each of the eight marked problem sheets is worth 1.25% of your overall grade. This mark is awarded for any reasonable attempt.
- Discuss questions with your colleagues.
- Web: `planetmath.org`, `http://math.stackexchange.com`.
- Check your answers to computational problems with computer algebra packages such as MATHEMATICA.

§1 Introduction: Sets of Numbers

One of the unifying ideas in this course is solving equations. I hope we can all agree this is an useful and interesting thing to do. For example, consider the equation

$$2x + 3y = 18.$$

How many solutions are there?

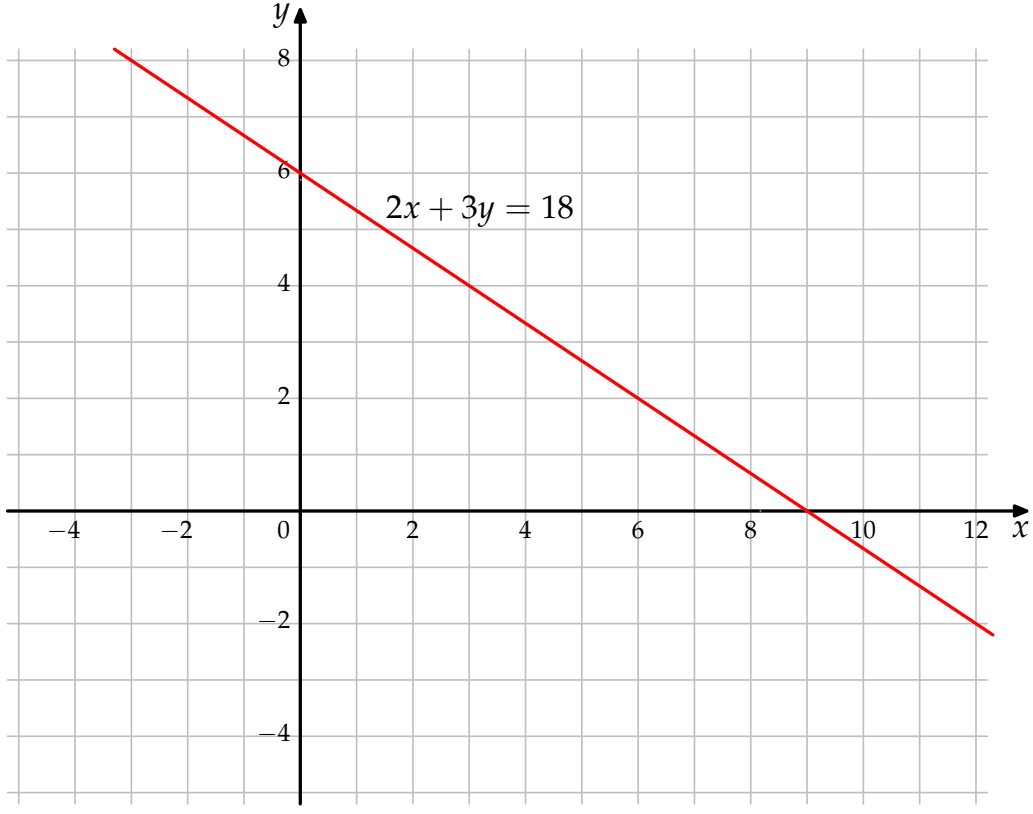
Part A: Sets, Functions and Complex Numbers

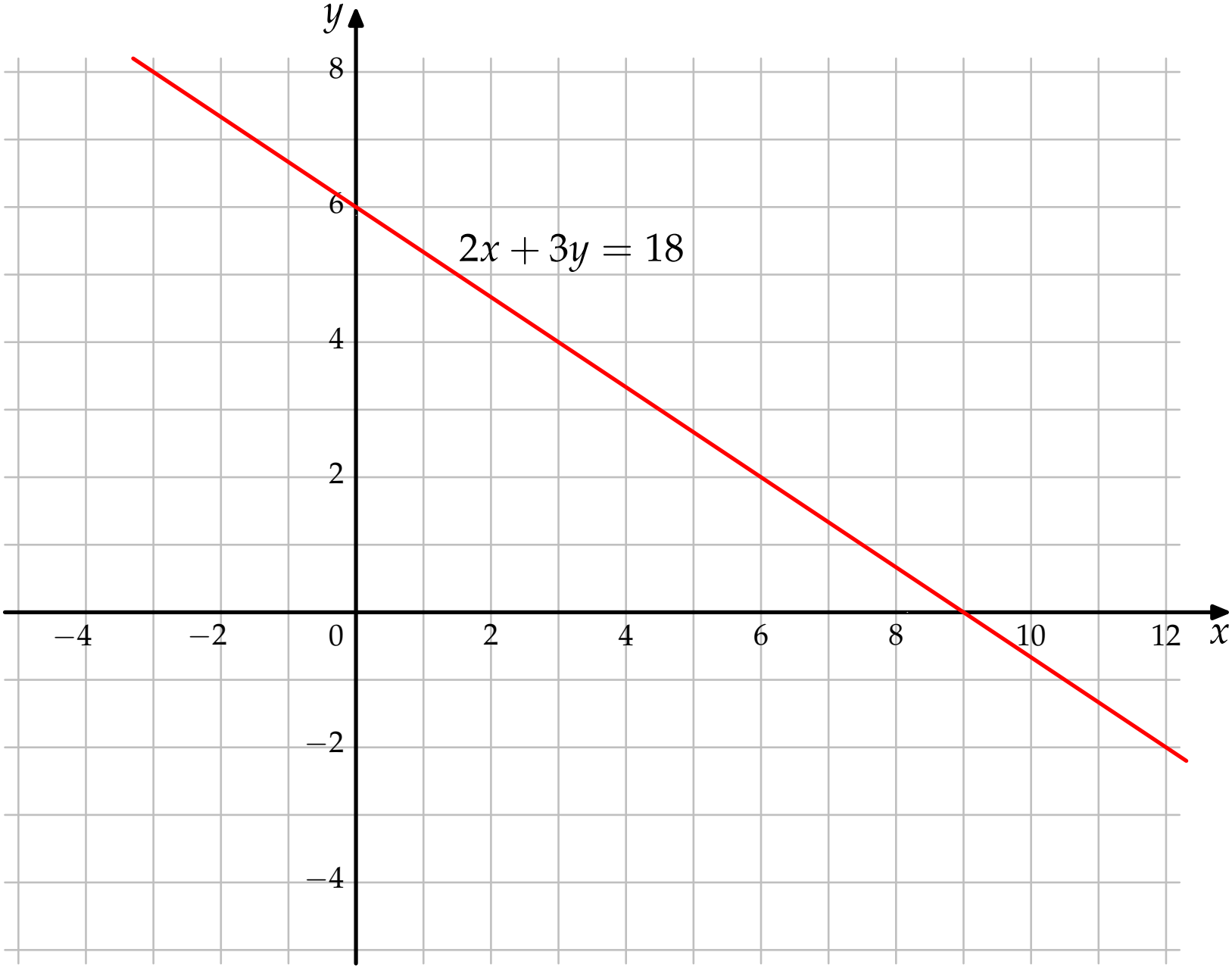
§1 Introduction: Sets of Numbers

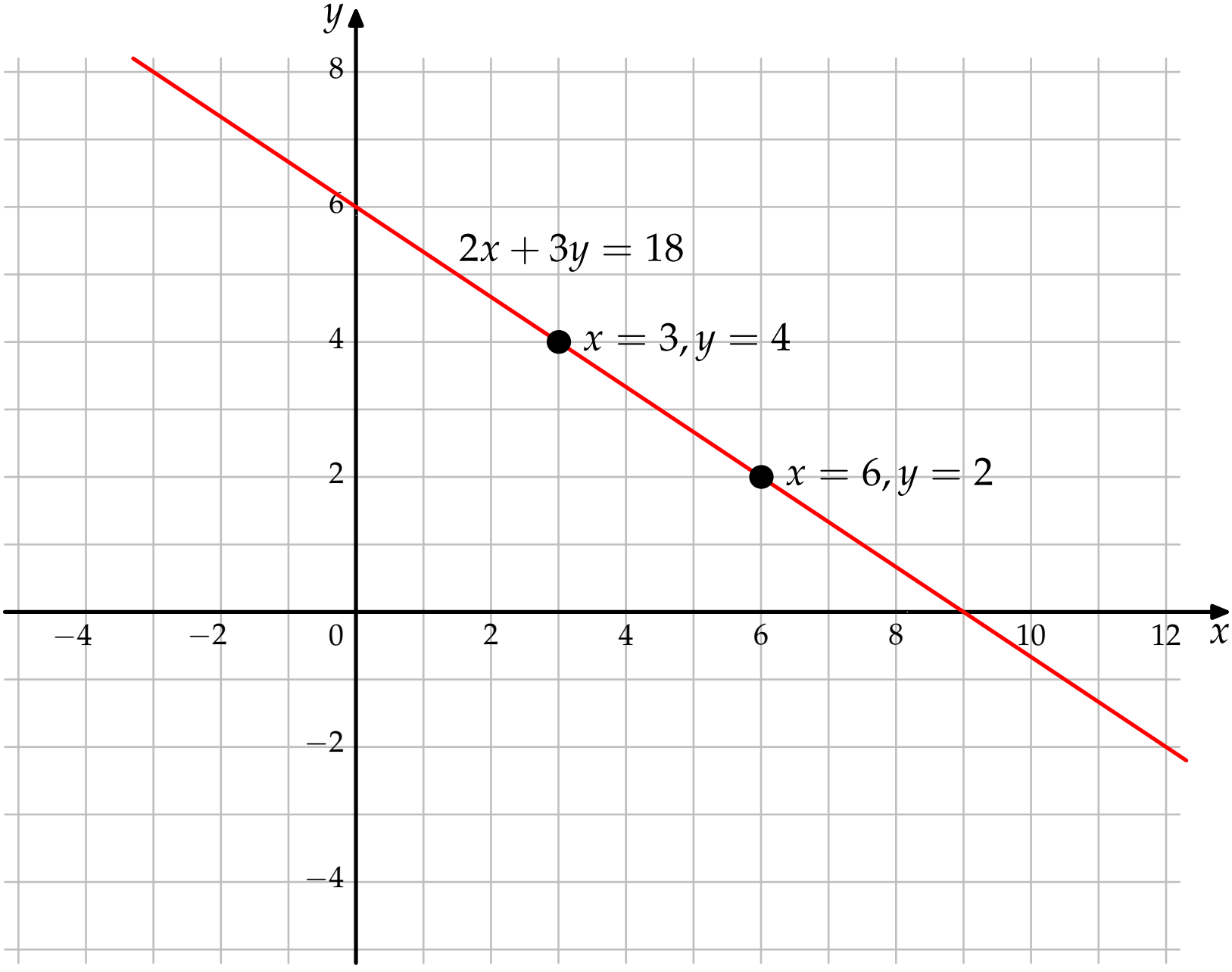
One of the unifying ideas in this course is solving equations. I hope we can all agree this is an useful and interesting thing to do. For example, consider the equation

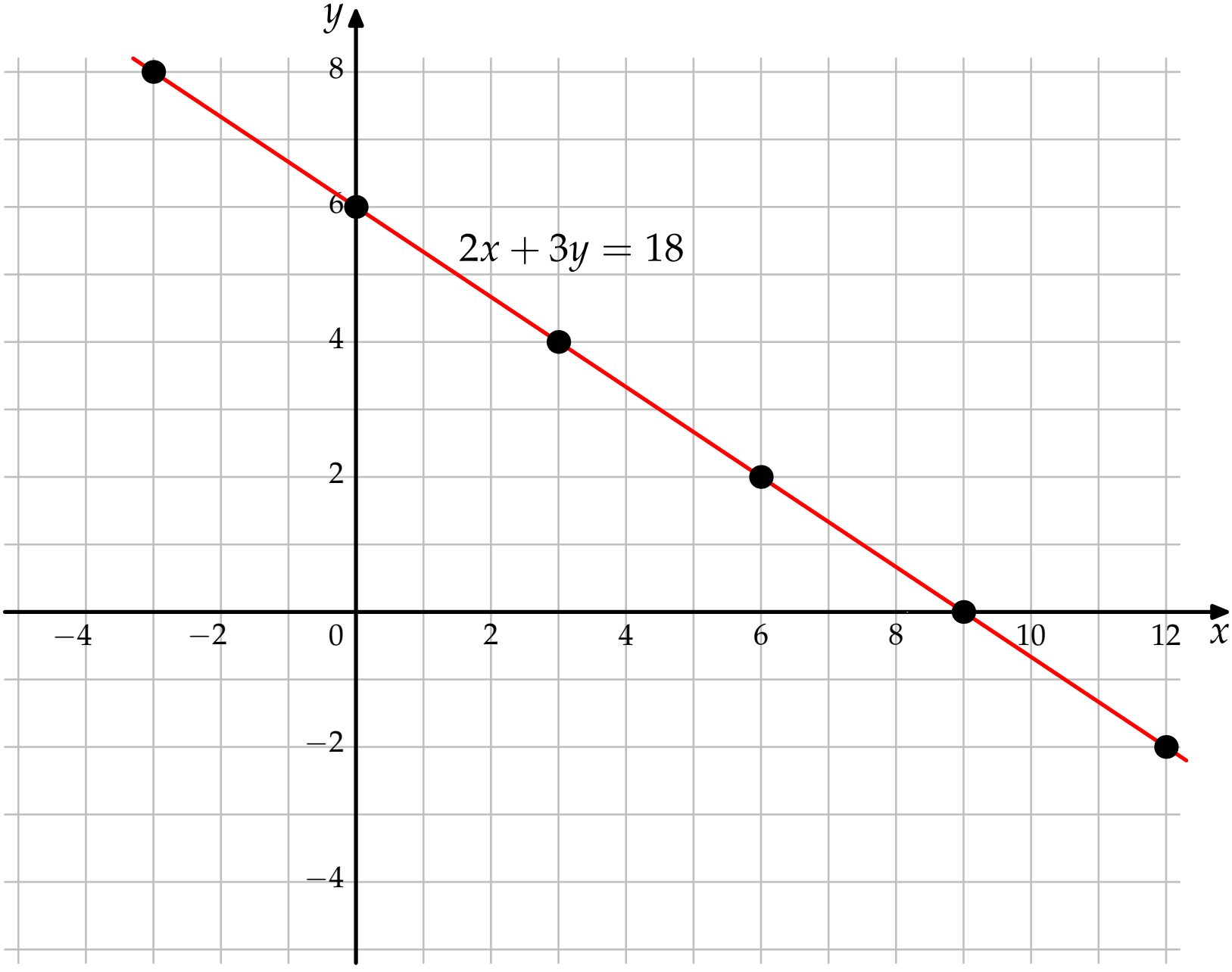
$$2x + 3y = 18.$$

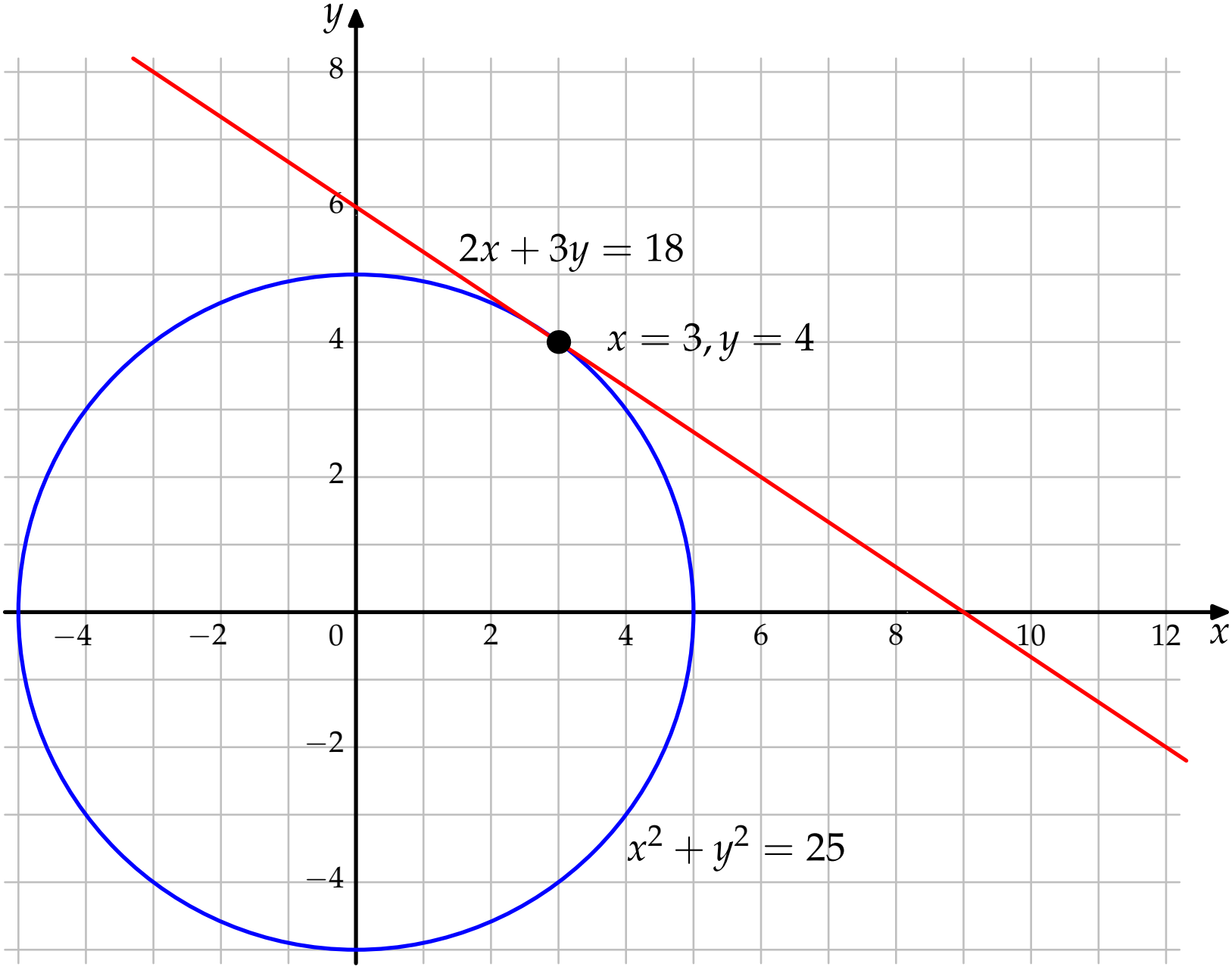
How many solutions are there?

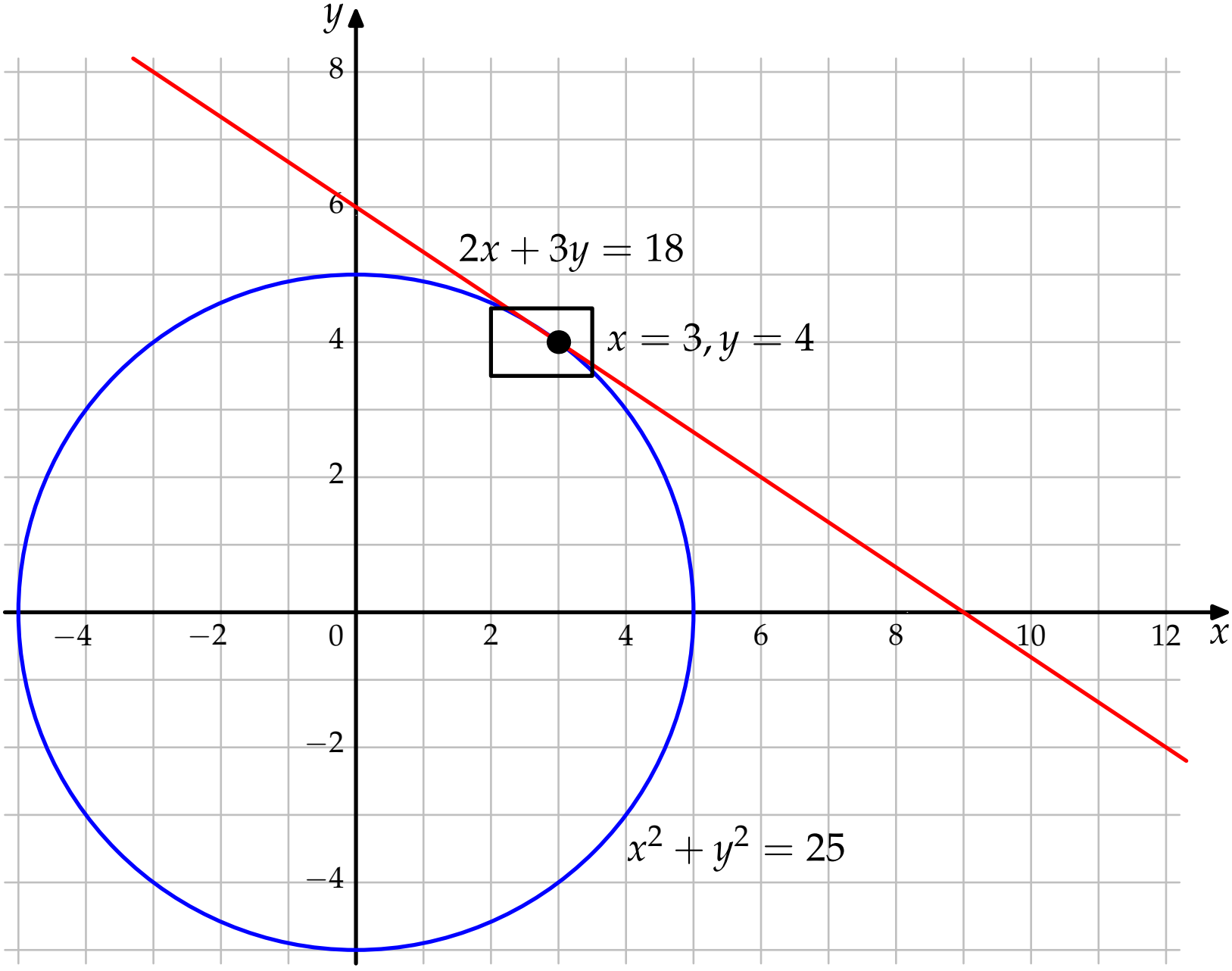


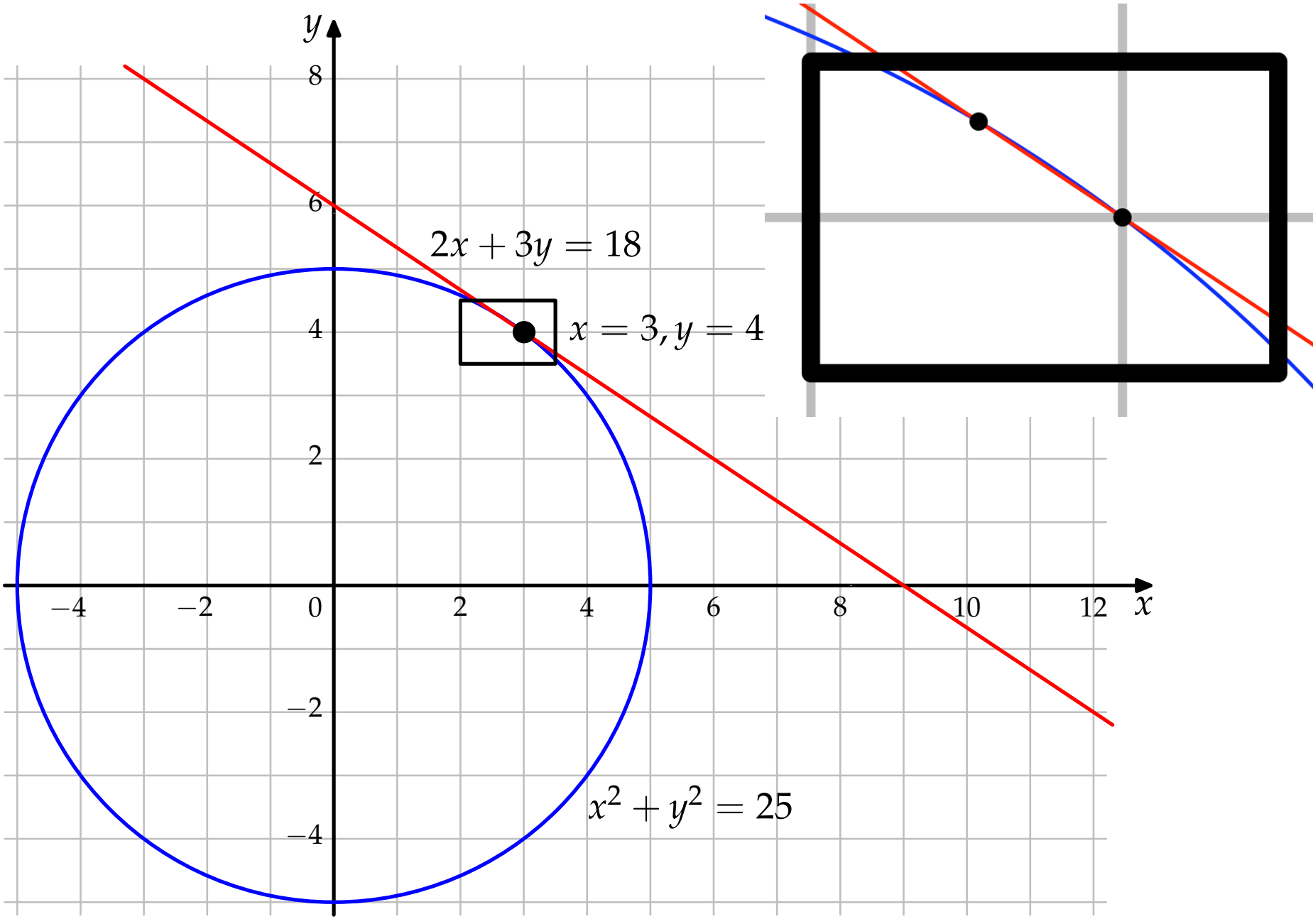

y
8
6
4
2
−2
−4
−4
−2
0
2
4
6
8
10
12
x
2x + 3y = 18


y
8
6
4
2
0
−2
−4
−4
−2
2
4
6
8
10
12
x
2x + 3y = 18
x = 3, y = 4
x = 6, y = 2


y
8
6
4
2
−2
−4
−4
−2
0
2
4
6
8
10
12
x
2x + 3y = 18


y
8
6
4
2
−2
−4
−4
−2
0
2
4
6
8
10
12
x
2x + 3y = 18
x = 3, y = 4
x² + y² = 25


y
x
8
6
4
2
−2
−4
−4
−2
0
2
4
6
8
10
12
2x + 3y = 18
x = 3, y = 4
x² + y² = 25


y
x
8
6
4
2
−2
−4
−4
−2
0
2
4
6
8
10
12
$2x + 3y = 18$
$x = 3, y = 4$
$x^2 + y^2 = 25$

Sets

A *set* is any collection of objects. These objects are called the *members* or *elements* of the set.

If X is a set and x is an element of X then we write $x \in X$. (This can be read as 'x is in X', or 'X contains x'.) If y is not an element of X then we write $y \notin X$. For example,
$7 \in \{2, 3, 5, 7, 11, 13\}$ and $8 \notin \{2, 3, 5, 7, 11, 13\}$.

Exercise 1.1

True or false?

(i) 29 is a member of the set of prime numbers,

(ii) 87 is a member of the set of prime numbers,

(iii) $\{2, 3, 5, 7, 11\} = \{5, 7, 11, 2, 3\}$.

Sets

A *set* is any collection of objects. These objects are called the *members* or *elements* of the set.

If X is a set and x is an element of X then we write $x \in X$. (This can be read as 'x is in X', or 'X contains x'.) If y is not an element of X then we write $y \notin X$. For example,
$7 \in \{2, 3, 5, 7, 11, 13\}$ and $8 \notin \{2, 3, 5, 7, 11, 13\}$.

Exercise 1.1

True or false?

(i) 29 is a member of the set of prime numbers, True

(ii) 87 is a member of the set of prime numbers,

(iii) $\{2, 3, 5, 7, 11\} = \{5, 7, 11, 2, 3\}$.

Sets

A *set* is any collection of objects. These objects are called the *members* or *elements* of the set.

If X is a set and x is an element of X then we write $x \in X$. (This can be read as 'x is in X', or 'X contains x'.) If y is not an element of X then we write $y \notin X$. For example,
$7 \in \{2, 3, 5, 7, 11, 13\}$ and $8 \notin \{2, 3, 5, 7, 11, 13\}$.

Exercise 1.1

True or false?

(i) 29 is a member of the set of prime numbers, True

(ii) 87 is a member of the set of prime numbers, False

(iii) $\{2, 3, 5, 7, 11\} = \{5, 7, 11, 2, 3\}$.

Sets

A *set* is any collection of objects. These objects are called the *members* or *elements* of the set.

If X is a set and x is an element of X then we write $x \in X$. (This can be read as 'x is in X', or 'X contains x'.) If y is not an element of X then we write $y \notin X$. For example,
$7 \in \{2, 3, 5, 7, 11, 13\}$ and $8 \notin \{2, 3, 5, 7, 11, 13\}$.

Exercise 1.1

True or false?

(i) 29 is a member of the set of prime numbers, True

(ii) 87 is a member of the set of prime numbers, False

(iii) $\{2, 3, 5, 7, 11\} = \{5, 7, 11, 2, 3\}$. True

Sets of Numbers

We write $\mathbb{N}$ for the set of natural numbers:

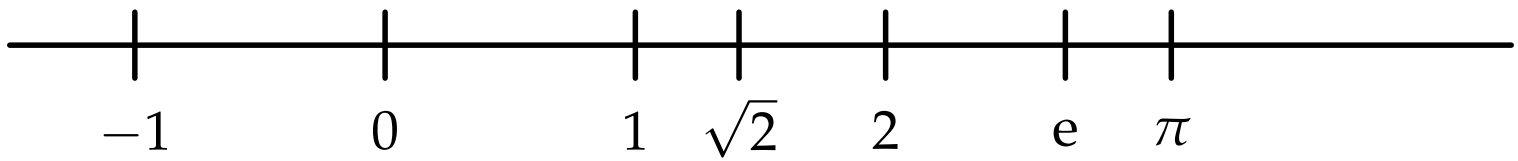
$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}.$$

We write $\mathbb{Z}$ for the set of integers:

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

A number r/s with $r \in \mathbb{Z}$, $s \in \mathbb{Z}$ and $s \neq 0$ is said to be *rational*. We write $\mathbb{Q}$ for the set of rational numbers. Finally we write $\mathbb{R}$ for the set of real numbers.

Some important real numbers are marked below.



Rational and Irrational Numbers

It is an important fact that there are real numbers that are not rational numbers. For example $\sqrt{2} \notin \mathbb{Q}$. We say that such numbers are *irrational*. So what sort of numbers are rational?

Example 1.2 (See board)

Rational and Irrational Numbers

It is an important fact that there are real numbers that are not rational numbers. For example $\sqrt{2} \notin \mathbb{Q}$. We say that such numbers are *irrational*. So what sort of numbers are rational?

Example 1.2 (See board)

Note that '$\implies$' means 'implies'. If A and B are mathematical statements then

$$A \implies B$$

means 'A implies B' or equivalently

'if A is true, then B is true'.

Using implies signs (and also importantly, words!) will help to clarify the structure of your arguments.

Rational and Irrational Numbers

It is an important fact that there are real numbers that are not rational numbers. For example $\sqrt{2} \notin \mathbb{Q}$. We say that such numbers are *irrational*. So what sort of numbers are rational?

Example 1.2 (See board)

Note that '$\Longrightarrow$' means 'implies'. If A and B are mathematical statements then

$$A \implies B$$

means 'A implies B' or equivalently

'if A is true, then B is true'.

Using implies signs (and also importantly, words!) will help to clarify the structure of your arguments.

Exercise 1.3′. Find a simple expression for $0.99999\ldots$. Are you happy with the answer? (For another exercise on Example 1.2, see printed notes.)

An Encouragement to Use Implication Signs ' $\Longrightarrow$ '

$\sqrt{x} = x - 2, x = (x-2)^2, x^2 - 5x + 4 = 0$, $x = 4$ and $x = 1$.

This gets an incorrect answer. The logical structure is unclear and it is unpleasant to read.

$$\begin{aligned} \sqrt{x} = x - 2 &\Longrightarrow x = (x-2)^2 \\ &\Longrightarrow x = x^2 - 4x + 4 \\ &\Longrightarrow x^2 - 5x + 4 = 0 \\ &\Longrightarrow (x-4)(x-1) = 0 \\ &\Longrightarrow x = 4 \text{ or } x = 1. \end{aligned}$$

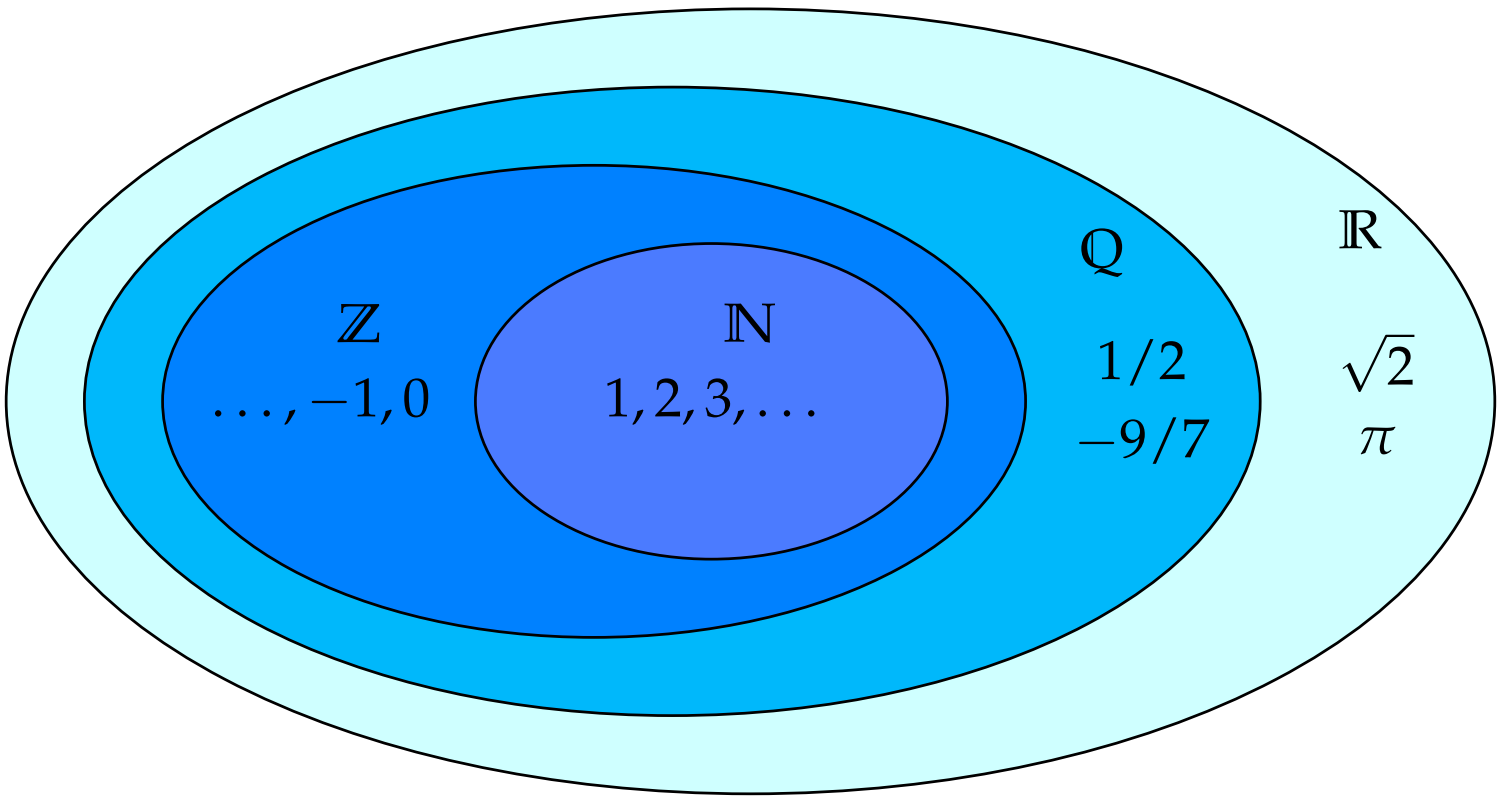
Now $\sqrt{4} = 2 = 4 - 2$ but $\sqrt{1} = 1 \neq 1 - 2$. So $x = 4$ is the unique solution.

The logical structure is clear and the answer is correct.

Number Systems Seen So Far

In this diagram, sets are drawn as regions in the plane.

Note that a set contains all the numbers in the sets drawn inside it. It is therefore entirely correct to say that 1 is a real number, or that -1 is a rational number.



Quiz on Different Numbers

True or False:

(a) $\sqrt{3}$ is a real number

(b) $\sqrt{3}$ is a rational number

(c) $0.123456789\,123456789\ldots$ is a rational number

(d) 3.141592 is a rational number

(e) 1 is a real number

(f) $0.3999\ldots$ (repeating 9s) is a rational number

Quiz on Different Numbers

True or False:

(a) $\sqrt{3}$ is a real number — True

(b) $\sqrt{3}$ is a rational number

(c) $0.123456789\,123456789\ldots$ is a rational number

(d) 3.141592 is a rational number

(e) 1 is a real number

(f) $0.3999\ldots$ (repeating 9s) is a rational number

Quiz on Different Numbers

True or False:

(a) $\sqrt{3}$ is a real number — True

(b) $\sqrt{3}$ is a rational number — False

(c) $0.123456789\,123456789\ldots$ is a rational number

(d) 3.141592 is a rational number

(e) 1 is a real number

(f) $0.3999\ldots$ (repeating 9s) is a rational number

Quiz on Different Numbers

True or False:

(a) $\sqrt{3}$ is a real number — True

(b) $\sqrt{3}$ is a rational number — False

(c) $0.123456789\,123456789\ldots$ is a rational number — True

(d) 3.141592 is a rational number

(e) 1 is a real number

(f) $0.3999\ldots$ (repeating 9s) is a rational number

Quiz on Different Numbers

True or False:

(a) $\sqrt{3}$ is a real number — True

(b) $\sqrt{3}$ is a rational number — False

(c) $0.123456789\,123456789\ldots$ is a rational number — True

(d) 3.141592 is a rational number — True

(e) 1 is a real number

(f) $0.3999\ldots$ (repeating 9s) is a rational number

For (d): $\dfrac{3\,141\,592}{1\,000\,000} = 3.141592 \neq \pi$ (in fact $\pi = 3.141592653\ldots$)

Quiz on Different Numbers

True or False:

(a) $\sqrt{3}$ is a real number — True

(b) $\sqrt{3}$ is a rational number — False

(c) $0.123456789\,123456789\ldots$ is a rational number — True

(d) 3.141592 is a rational number — True

(e) 1 is a real number — True

(f) $0.3999\ldots$ (repeating 9s) is a rational number

For (d): $\dfrac{3\,141\,592}{1\,000\,000} = 3.141592 \neq \pi$ (in fact $\pi = 3.141592653\ldots$)

Quiz on Different Numbers

True or False:

(a) $\sqrt{3}$ is a real number — True

(b) $\sqrt{3}$ is a rational number — False

(c) $0.123456789\,123456789\ldots$ is a rational number — True

(d) 3.141592 is a rational number — True

(e) 1 is a real number — True

(f) $0.3999\ldots$ (repeating 9s) is a rational number

For (d): $\dfrac{3\,141\,592}{1\,000\,000} = 3.141592 \neq \pi$ (in fact $\pi = 3.141592653\ldots$)

For (e): 1 is a natural number, and every natural number is also a real number.

Quiz on Different Numbers

True or False:

(a)	$\sqrt{3}$ is a real number	True
(b)	$\sqrt{3}$ is a rational number	False
(c)	$0.123456789\,123456789\ldots$ is a rational number	True
(d)	3.141592 is a rational number	True
(e)	1 is a real number	True
(f)	$0.3999\ldots$ (repeating 9s) is a rational number	True

For (d): $\dfrac{3\,141\,592}{1\,000\,000} = 3.141592 \neq \pi$ (in fact $\pi = 3.141592653\ldots$)

For (e): 1 is a natural number, and every natural number is also a real number.

Quiz on Different Numbers

True or False:

(a) $\sqrt{3}$ is a real number — True

(b) $\sqrt{3}$ is a rational number — False

(c) $0.123456789\,123456789\ldots$ is a rational number — True

(d) 3.141592 is a rational number — True

(e) 1 is a real number — True

(f) $0.3999\ldots$ (repeating 9s) is a rational number — True

For (d): $\dfrac{3\,141\,592}{1\,000\,000} = 3.141592 \neq \pi$ (in fact $\pi = 3.141592653\ldots$)

For (e): 1 is a natural number, and every natural number is also a real number.

For (f): $0.3999\ldots = 0.4 = 2/5$.

Closure

One important property of the natural numbers, which I hope you will agree is obviously true, is that if $m, n \in \mathbb{N}$ then $m + n \in \mathbb{N}$ and $mn \in \mathbb{N}$.

Definition 1.4

Let X be a set of numbers. We say that X is

- *closed under addition* if $x + y \in X$ whenever $x \in X$ and $y \in X$;
- *closed under multiplication* if $xy \in X$ whenever $x \in X$ and $y \in X$;
- *closed under subtraction* if $x - y \in X$ whenever $x \in X$ and $y \in X$;
- *closed under division* if $x/y \in X$ whenever $x \in X$, $y \in X$ and $y \neq 0$.

Assume that $\mathbb{Z}$ is closed under addition, subtraction and multiplication. Let $\mathbb{Z}_{\leq 0} = \{0, -1, -2, -3, \ldots\}$.

Exercise 1.5

- Is $\mathbb{N}$ closed under division?
- Is $\mathbb{Z}$ closed under division?
- Is $\mathbb{Z}_{\leq 0}$ closed under addition?
- Is $\mathbb{Q}$ closed under addition?

Closure

One important property of the natural numbers, which I hope you will agree is obviously true, is that if $m, n \in \mathbb{N}$ then $m + n \in \mathbb{N}$ and $mn \in \mathbb{N}$.

Definition 1.4

Let X be a set of numbers. We say that X is

- *closed under addition* if $x + y \in X$ whenever $x \in X$ and $y \in X$;
- *closed under multiplication* if $xy \in X$ whenever $x \in X$ and $y \in X$;
- *closed under subtraction* if $x - y \in X$ whenever $x \in X$ and $y \in X$;
- *closed under division* if $x/y \in X$ whenever $x \in X$, $y \in X$ and $y \neq 0$.

Assume that $\mathbb{Z}$ is closed under addition, subtraction and multiplication. Let $\mathbb{Z}_{\leq 0} = \{0, -1, -2, -3, \ldots\}$.

Exercise 1.5

- Is $\mathbb{N}$ closed under division? No: $1/2 \notin \mathbb{N}$
- Is $\mathbb{Z}$ closed under division?
- Is $\mathbb{Z}_{\leq 0}$ closed under addition?
- Is $\mathbb{Q}$ closed under addition?

Closure

One important property of the natural numbers, which I hope you will agree is obviously true, is that if $m, n \in \mathbb{N}$ then $m + n \in \mathbb{N}$ and $mn \in \mathbb{N}$.

Definition 1.4

Let X be a set of numbers. We say that X is

- *closed under addition* if $x + y \in X$ whenever $x \in X$ and $y \in X$;
- *closed under multiplication* if $xy \in X$ whenever $x \in X$ and $y \in X$;
- *closed under subtraction* if $x - y \in X$ whenever $x \in X$ and $y \in X$;
- *closed under division* if $x/y \in X$ whenever $x \in X$, $y \in X$ and $y \neq 0$.

Assume that $\mathbb{Z}$ is closed under addition, subtraction and multiplication. Let $\mathbb{Z}_{\leq 0} = \{0, -1, -2, -3, \ldots\}$.

Exercise 1.5

- Is $\mathbb{N}$ closed under division? No: $1/2 \notin \mathbb{N}$
- Is $\mathbb{Z}$ closed under division? No: $1/2 \notin \mathbb{N}$
- Is $\mathbb{Z}_{\leq 0}$ closed under addition?
- Is $\mathbb{Q}$ closed under addition?

Closure

One important property of the natural numbers, which I hope you will agree is obviously true, is that if $m, n \in \mathbb{N}$ then $m + n \in \mathbb{N}$ and $mn \in \mathbb{N}$.

Definition 1.4

Let X be a set of numbers. We say that X is

- *closed under addition* if $x + y \in X$ whenever $x \in X$ and $y \in X$;
- *closed under multiplication* if $xy \in X$ whenever $x \in X$ and $y \in X$;
- *closed under subtraction* if $x - y \in X$ whenever $x \in X$ and $y \in X$;
- *closed under division* if $x/y \in X$ whenever $x \in X$, $y \in X$ and $y \neq 0$.

Assume that $\mathbb{Z}$ is closed under addition, subtraction and multiplication. Let $\mathbb{Z}_{\leq 0} = \{0, -1, -2, -3, \ldots\}$.

Exercise 1.5

- Is $\mathbb{N}$ closed under division? No: $1/2 \notin \mathbb{N}$
- Is $\mathbb{Z}$ closed under division? No: $1/2 \notin \mathbb{N}$
- Is $\mathbb{Z}_{\leq 0}$ closed under addition? Yes (but why?)
- Is $\mathbb{Q}$ closed under addition?

Closure

One important property of the natural numbers, which I hope you will agree is obviously true, is that if $m, n \in \mathbb{N}$ then $m + n \in \mathbb{N}$ and $mn \in \mathbb{N}$.

Definition 1.4

Let X be a set of numbers. We say that X is

- *closed under addition* if $x + y \in X$ whenever $x \in X$ and $y \in X$;
- *closed under multiplication* if $xy \in X$ whenever $x \in X$ and $y \in X$;
- *closed under subtraction* if $x - y \in X$ whenever $x \in X$ and $y \in X$;
- *closed under division* if $x/y \in X$ whenever $x \in X$, $y \in X$ and $y \neq 0$.

Assume that $\mathbb{Z}$ is closed under addition, subtraction and multiplication. Let $\mathbb{Z}_{\leq 0} = \{0, -1, -2, -3, \ldots\}$.

Exercise 1.5

- Is $\mathbb{N}$ closed under division? No: $1/2 \notin \mathbb{N}$
- Is $\mathbb{Z}$ closed under division? No: $1/2 \notin \mathbb{N}$
- Is $\mathbb{Z}_{\leq 0}$ closed under addition? Yes (but why?)
- Is $\mathbb{Q}$ closed under addition? Yes (but why?)

Discussion of Proof

Discussion: Does this proof make you more convinced that $\mathbb{Q}$ is closed under addition?

Discussion of Proof

Discussion: Does this proof make you more convinced that $\mathbb{Q}$ is closed under addition? Would you accept a bet for £10 at odds of 10000 to 1 that $\mathbb{Q}$ is closed under addition?

Discussion of Proof

Discussion: Does this proof make you more convinced that $\mathbb{Q}$ is closed under addition? Would you accept a bet for £10 at odds of 10000 to 1 that $\mathbb{Q}$ is closed under addition?

- 'Why so many words? I thought we were here to do mathematics.' Reply: We are, and we did.

Discussion of Proof

Discussion: Does this proof make you more convinced that $\mathbb{Q}$ is closed under addition? Would you accept a bet for £10 at odds of 10000 to 1 that $\mathbb{Q}$ is closed under addition?

- 'Why so many words? I thought we were here to do mathematics.' Reply: We are, and we did.
- 'All we showed is that the sum of two fractions is a fraction. Isn't this just obvious?' Reply: maybe it is.

Discussion of Proof

Discussion: Does this proof make you more convinced that $\mathbb{Q}$ is closed under addition? Would you accept a bet for £10 at odds of 10000 to 1 that $\mathbb{Q}$ is closed under addition?

- 'Why so many words? I thought we were here to do mathematics.' Reply: We are, and we did.
- 'All we showed is that the sum of two fractions is a fraction. Isn't this just obvious?' Reply: maybe it is. But many obvious sounding statements have turned out to be false.

  We will prove much more interesting results later in the course.

Discussion of Proof

Discussion: Does this proof make you more convinced that $\mathbb{Q}$ is closed under addition? Would you accept a bet for £10 at odds of 10000 to 1 that $\mathbb{Q}$ is closed under addition?

- 'Why so many words? I thought we were here to do mathematics.' Reply: We are, and we did.
- 'All we showed is that the sum of two fractions is a fraction. Isn't this just obvious?' Reply: maybe it is. But many obvious sounding statements have turned out to be false.

  We will prove much more interesting results later in the course.

- 'In the proof you assumed that $\mathbb{Z}$ is closed under addition and multiplication. How do we know this?' Reply: good point.

Discussion of Proof

Discussion: Does this proof make you more convinced that $\mathbb{Q}$ is closed under addition? Would you accept a bet for £10 at odds of 10000 to 1 that $\mathbb{Q}$ is closed under addition?

- 'Why so many words? I thought we were here to do mathematics.' Reply: We are, and we did.
- 'All we showed is that the sum of two fractions is a fraction. Isn't this just obvious?' Reply: maybe it is. But many obvious sounding statements have turned out to be false.

  We will prove much more interesting results later in the course.

- 'In the proof you assumed that $\mathbb{Z}$ is closed under addition and multiplication. How do we know this?' Reply: good point.

  But at least this proof reduces the problem of showing that $\mathbb{Q}$ is closed under adddition to proving that $\mathbb{Z}$ is closed under addition and multiplication (which you were told to assume).

Solving equations

There is a close connection between the closure properties of a set and the equations that can be solved using numbers from that set.

For example, $1 - 2 \notin \mathbb{N}$, and correspondingly, the equation $1 = 2 + x$ has no solution in $\mathbb{N}$. Going the other way, the equation $3x = 4$ has no solution in $\mathbb{Z}$, and correspondingly, $\mathbb{Z}$ is not closed under division.

Quiz

(i) Is the equation $x^2 = 2$ soluble in (i) $\mathbb{Q}$, (ii) $\mathbb{R}$?

(ii) Is the equation $x^2 = -1$ soluble in (i) $\mathbb{Q}$, (ii) $\mathbb{R}$?

(iii) Write down an equation that has exactly three solutions in $\mathbb{R}$, exactly one solution in $\mathbb{Z}$, and no solutions in $\mathbb{N}$.

Solving equations

There is a close connection between the closure properties of a set and the equations that can be solved using numbers from that set.

For example, $1 - 2 \notin \mathbb{N}$, and correspondingly, the equation $1 = 2 + x$ has no solution in $\mathbb{N}$. Going the other way, the equation $3x = 4$ has no solution in $\mathbb{Z}$, and correspondingly, $\mathbb{Z}$ is not closed under division.

Quiz

(i) Is the equation $x^2 = 2$ soluble in (i) $\mathbb{Q}$, (ii) $\mathbb{R}$? No, Yes

(ii) Is the equation $x^2 = -1$ soluble in (i) $\mathbb{Q}$, (ii) $\mathbb{R}$?

(iii) Write down an equation that has exactly three solutions in $\mathbb{R}$, exactly one solution in $\mathbb{Z}$, and no solutions in $\mathbb{N}$.

Solving equations

There is a close connection between the closure properties of a set and the equations that can be solved using numbers from that set.

For example, $1 - 2 \notin \mathbb{N}$, and correspondingly, the equation $1 = 2 + x$ has no solution in $\mathbb{N}$. Going the other way, the equation $3x = 4$ has no solution in $\mathbb{Z}$, and correspondingly, $\mathbb{Z}$ is not closed under division.

Quiz

(i) Is the equation $x^2 = 2$ soluble in (i) $\mathbb{Q}$, (ii) $\mathbb{R}$? No, Yes

(ii) Is the equation $x^2 = -1$ soluble in (i) $\mathbb{Q}$, (ii) $\mathbb{R}$? No, No

(iii) Write down an equation that has exactly three solutions in $\mathbb{R}$, exactly one solution in $\mathbb{Z}$, and no solutions in $\mathbb{N}$.

Subsets

If X and Y are sets and every element of X is an element of Y, then we say that X is a *subset* of Y, and write $X \subseteq Y$. In symbols the condition $X \subseteq Y$ is

$$x \in X \implies x \in Y.$$

For example $\mathbb{N}$ is a subset of $\mathbb{Z}$, $\mathbb{Z}$ is a subset of $\mathbb{Q}$ and $\mathbb{Q}$ is a subset of $\mathbb{R}$. In symbols

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}.$$

Subsets

If X and Y are sets and every element of X is an element of Y, then we say that X is a *subset* of Y, and write $X \subseteq Y$. In symbols the condition $X \subseteq Y$ is

$$x \in X \implies x \in Y.$$

For example $\mathbb{N}$ is a subset of $\mathbb{Z}$, $\mathbb{Z}$ is a subset of $\mathbb{Q}$ and $\mathbb{Q}$ is a subset of $\mathbb{R}$. In symbols

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}.$$

There is a special notation for defining subsets of a set. For example if Y is the set of prime numbers and

$$X = \{x \in Y : x \leq 13\}$$

then X is the set of prime numbers x such that $x \leq 13$. The set $\mathbb{Q}$ of rational numbers can be defined as

$$\mathbb{Q} = \{r/s : r \in \mathbb{Z}, s \in \mathbb{Z}, s \neq 0\}.$$

Example of Subsets

Example 1.6

Let

$$X = \{x \in \mathbb{R} : x \geq 2 + \sqrt{5}.\}$$
$$Y = \{x \in \mathbb{R} : x^2 - 4x + 1 \geq 2\}$$

We will show that $X \subseteq Y$. Is it true that $X = Y$?

Example of Subsets

Example 1.6

Let

$$X = \{x \in \mathbb{R} : x \geq 2 + \sqrt{5}.\}$$
$$Y = \{x \in \mathbb{R} : x^2 - 4x + 1 \geq 2\}$$

We will show that $X \subseteq Y$. Is it true that $X = Y$?

Exercise 1.7

Give an example of English sentences A and B such that $P \implies Q$ is true, but $Q \implies P$ is false.

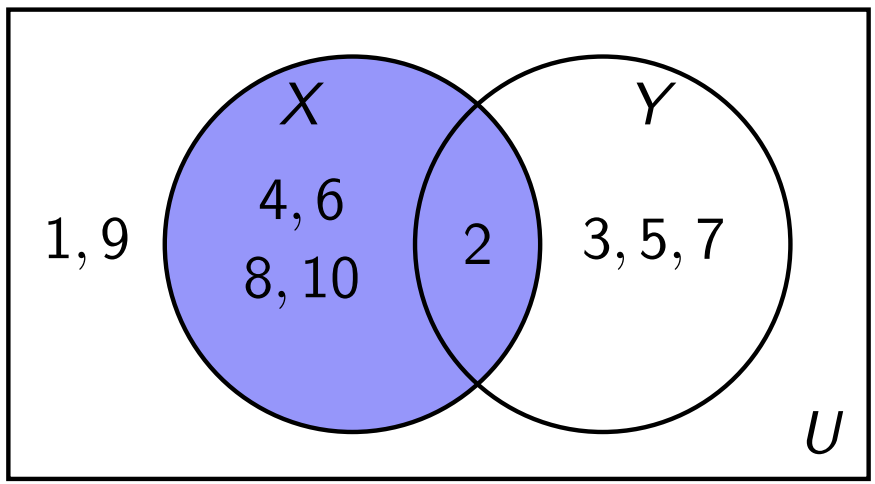
If $P \implies Q$ and $Q \implies P$ then we write $P \iff Q$, read as 'if and only if'.

Venn Diagrams

A *Venn diagram* is a diagram, like the one on page 6, that represents sets by regions of the plane. For example, the sets

$$U = \{1, 2, 3, \ldots, 9, 10\}$$
$$X = \{n \in U : n \text{ is even}\}$$
$$Y = \{n \in U : n \text{ is a prime number}\}$$

are shown in the Venn diagram below. The region representing X is shaded.



Intersection, Union, Complement and de Morgan's Laws

Let X and Y be sets.

- The *intersection* of X and Y, written $X \cap Y$, is the set of elements that are in both X and Y.
- The *union* of X and Y, written $X \cup Y$, is the set of elements in at least one of X and Y.
- If X is a subset of a set U then we define the *complement of X in U* by $X' = \{y \in U : y \notin X\}$.

Intersection, Union, Complement and de Morgan's Laws

Let X and Y be sets.

- The *intersection* of X and Y, written $X \cap Y$, is the set of elements that are in both X and Y.
- The *union* of X and Y, written $X \cup Y$, is the set of elements in at least one of X and Y.
- If X is a subset of a set U then we define the *complement of X in U* by $X' = \{y \in U : y \notin X\}$.

Exercise 1.8

Draw Venn diagrams representing $X \cap Y$, $X \cup Y$ and X'.

Claim 1.9 (De Morgan's Laws)

Let X and Y be subsets of a set U. Then

(i) $(X \cup Y)' = X' \cap Y'$,

(ii) $(X \cap Y)' = X' \cup Y'$.

Administration

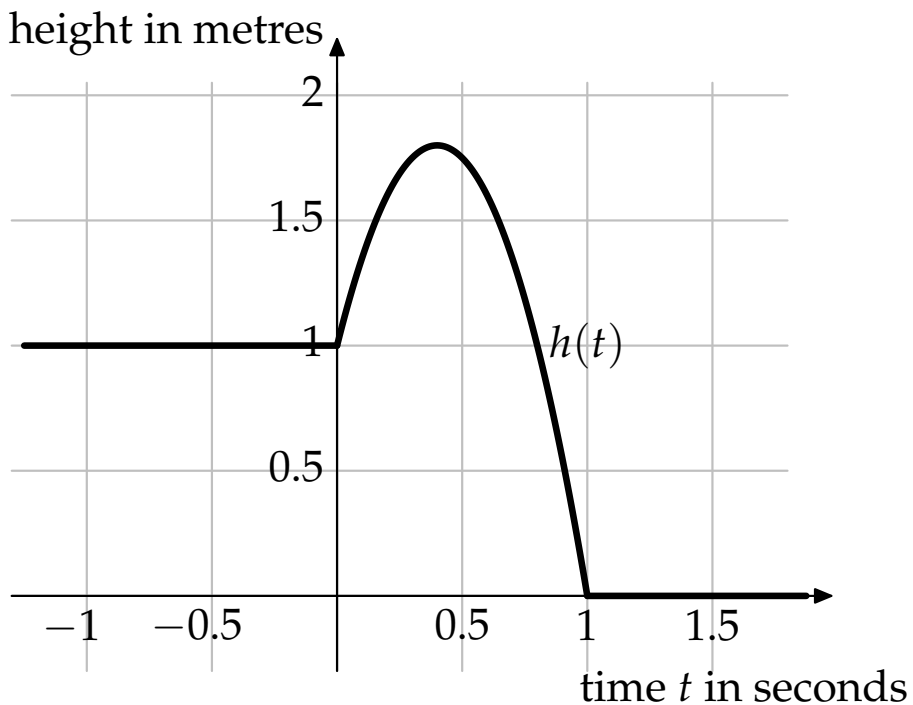
- Student Representative Elections
  [see `www.su.rhul.ac.uk/voice/representation/`]

  Through discussions with their fellow students, Course Reps identify the issues affecting their course and relate these back to staff through informal meetings and the course boards or staff / student committees. Course reps don't only criticise when things go wrong, but also provide positive and constructive feedback from students to the course team letting them know what works well. They also have an important role in feeding back information from these meetings to their course mates — keeping everyone fully informed.
- Please take pages 11 to 18 of the handout and Problem Sheet 2.
- Hand in Sheet 1 at the end of this lecture. Question 5 will be done today (you are welcome to add another answer).
- Answers to Sheet 1 will be posted to Moodle shortly. I will update these with feedback on common errors by Friday.

§2 Functions

We need an idea of a function that is broad enough to cover everything that might be needed in pure mathematics, applied mathematics, probability and statistics. For example, this should definitely be a function:

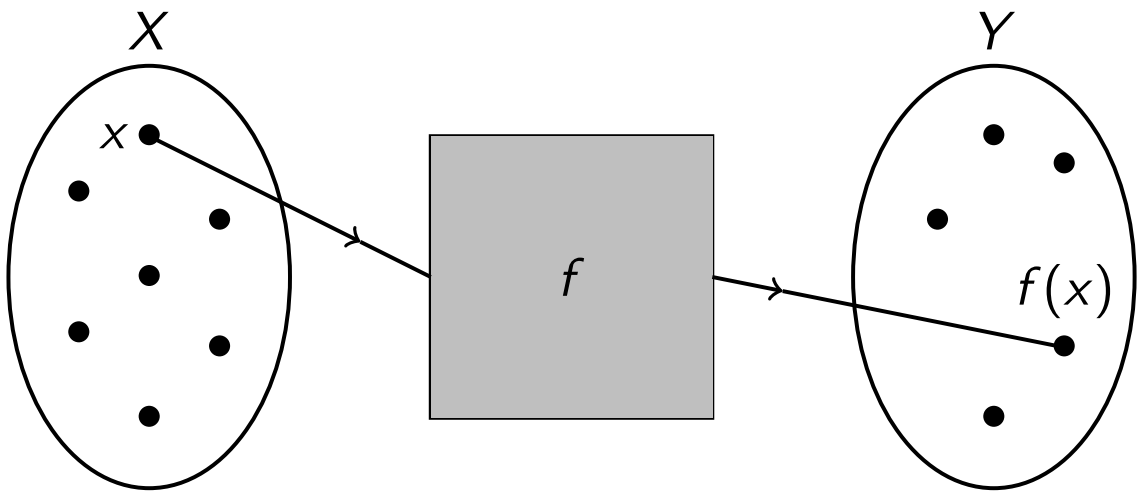
$$h(t) = \begin{cases} 1 & \text{if } t \leq 0 \\ 1 + 4t - 5t^2 & \text{if } 0 \leq t \leq 1 \\ 0 & \text{if } t \geq 1, \end{cases}$$



Definition of Functions

Definition 2.1

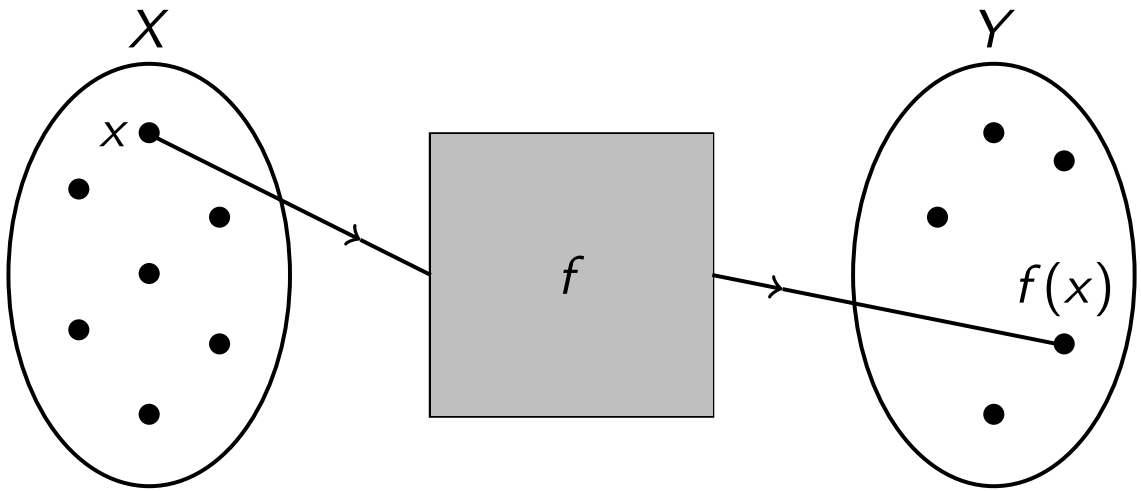
Let X and Y be sets. A *function* from X to Y is a black box such that, when an element $x \in X$ is put in, an element $y \in Y$ comes out. If the function is called f, then we write $f : X \to Y$. The output for the input x is written $f(x)$.



Definition of Functions

Definition 2.1

Let X and Y be sets. A *function* from X to Y is a black box such that, when an element $x \in X$ is put in, an element $y \in Y$ comes out. If the function is called f, then we write $f : X \to Y$. The output for the input x is written $f(x)$.



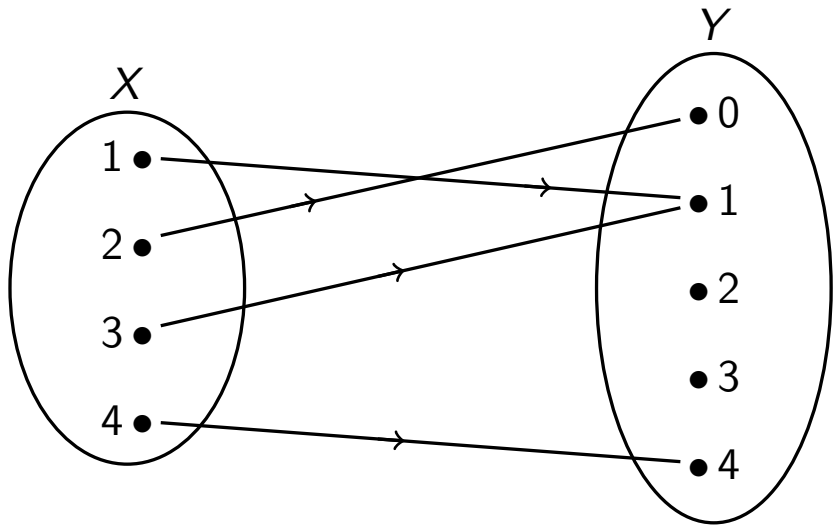
Question: When should two functions be said to be equal?

Example 2.2

Let $f : \{1, 2, 3, 4\} \to \{0, 1, 2, 3, 4\}$ be the function defined by

$$f(1) = 1, \quad f(2) = 0, \quad f(3) = 1, \quad f(4) = 4.$$

Define $g : \{1, 2, 3, 4\} \to \{0, 1, 2, 3, 4\}$ by $g(x) = (x - 2)^2$. Then $f = g$, since $f(x) = g(x)$ for all $x \in \{1, 2, 3, 4\}$.



Definition 2.3

Let $f : X \to Y$ be a function. The set X of allowed inputs to f is called the *domain* of f. The set Y of allowed outputs is called the *codomain* of f. The set $\{f(x) : x \in X\}$ of all outputs that actually appear is called the *range* of f.

Administration

- Please take the handout
- Spare copies of Section 2 Printed Notes and Problem Sheet 2 at front
- Sheet 1 was mostly done very well. I have updated the answers to Sheet 1 on Moodle with some feedback on common errors. Your work will be returned tomorrow.

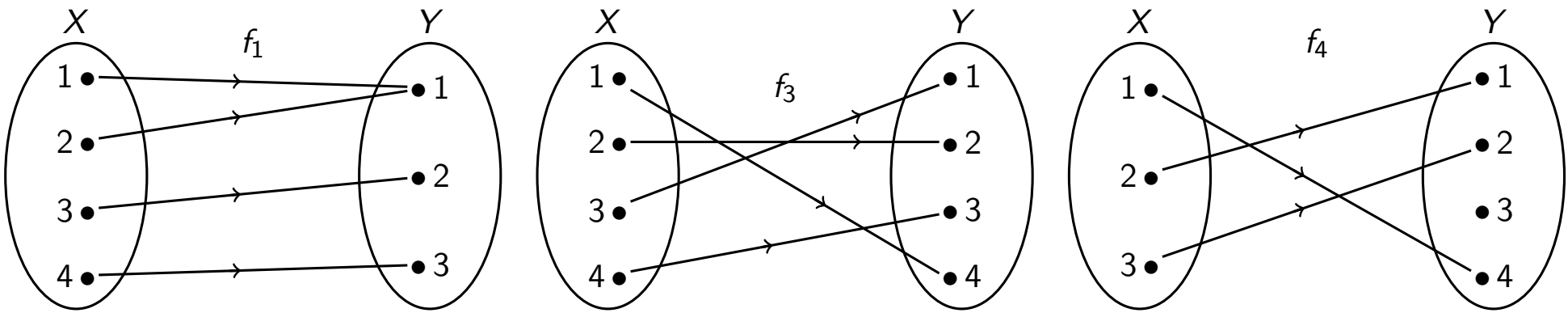
Bijective functions

Definition 2.5

Let X and Y be sets and let $f : X \to Y$ be a function. We say that f is *bijective* if for all $y \in Y$ there exists a unique $x \in X$ such that $f(x) = y$.

Example 2.6

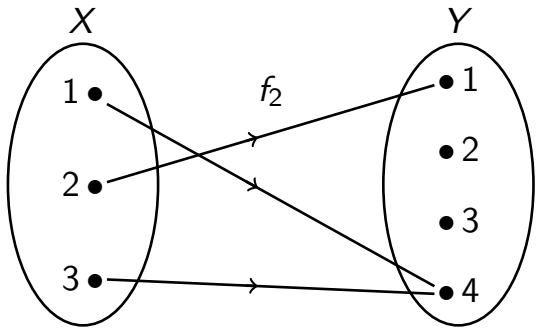
The function f_3 is the only bijective function below. For example f_4 is not bijective because there does not exists any $x \in X$ such that $f_4(x) = 3$, and f_1 is not bijective because $f(1) = f(2) = 1$.



Quiz on Bijective Functions

Which of the following functions are bijective? In (b) and (c) define $\mathbb{R}_{\geq 0} = \{x \in \mathbb{R} : x \geq 0\}$.

(a) $f_2 : \{1, 2, 3\} \to \{1, 2, 3, 4\}$ defined by the diagram below

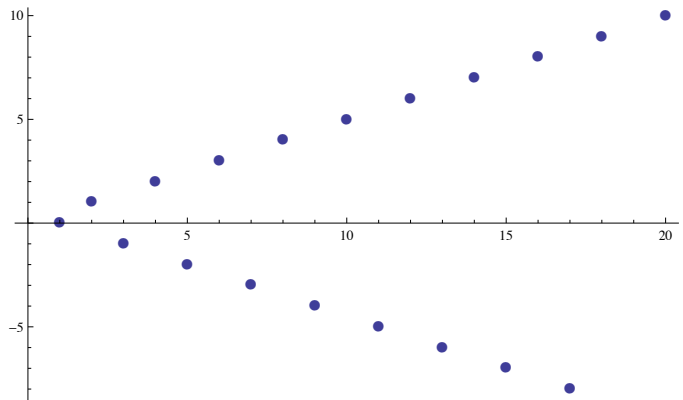


(b) $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ where $f(x) = x^2$,

(c) $g : \mathbb{R} \to \mathbb{R}_{\geq 0}$ where $g(x) = x^2$,

(d) $h : \mathbb{N} \to \mathbb{Z}$ defined by $h(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ -\frac{n-1}{2} & \text{if } n \text{ is odd.} \end{cases}$

n	1	2	3	4	5	6	7	...
$h(n)$	0	1	-1	2	-2	3	-3	...



Bijective Functions and Inverse Functions

A bijective function is also called a *bijection*. For example, the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3$ is a bijection.

Exercise 2.7

Let $X = \{x \in \mathbb{R} : x \geq 2\}$. What subset Y of $\mathbb{R}$ should you choose so that the function $f : X \to Y$ defined by $f(x) = x^2 - 4x + 1$ is bijective?

Bijective Functions and Inverse Functions

A bijective function is also called a *bijection*. For example, the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3$ is a bijection.

Exercise 2.7

Let $X = \{x \in \mathbb{R} : x \geq 2\}$. What subset Y of $\mathbb{R}$ should you choose so that the function $f : X \to Y$ defined by $f(x) = x^2 - 4x + 1$ is bijective?

Suppose that $f : X \to Y$ is a bijection. We define the *inverse function to* f to be the function $f^{-1} : Y \to X$ such that $f^{-1}(y)$ is the unique $x \in X$ such that $f(x) = y$. In symbols

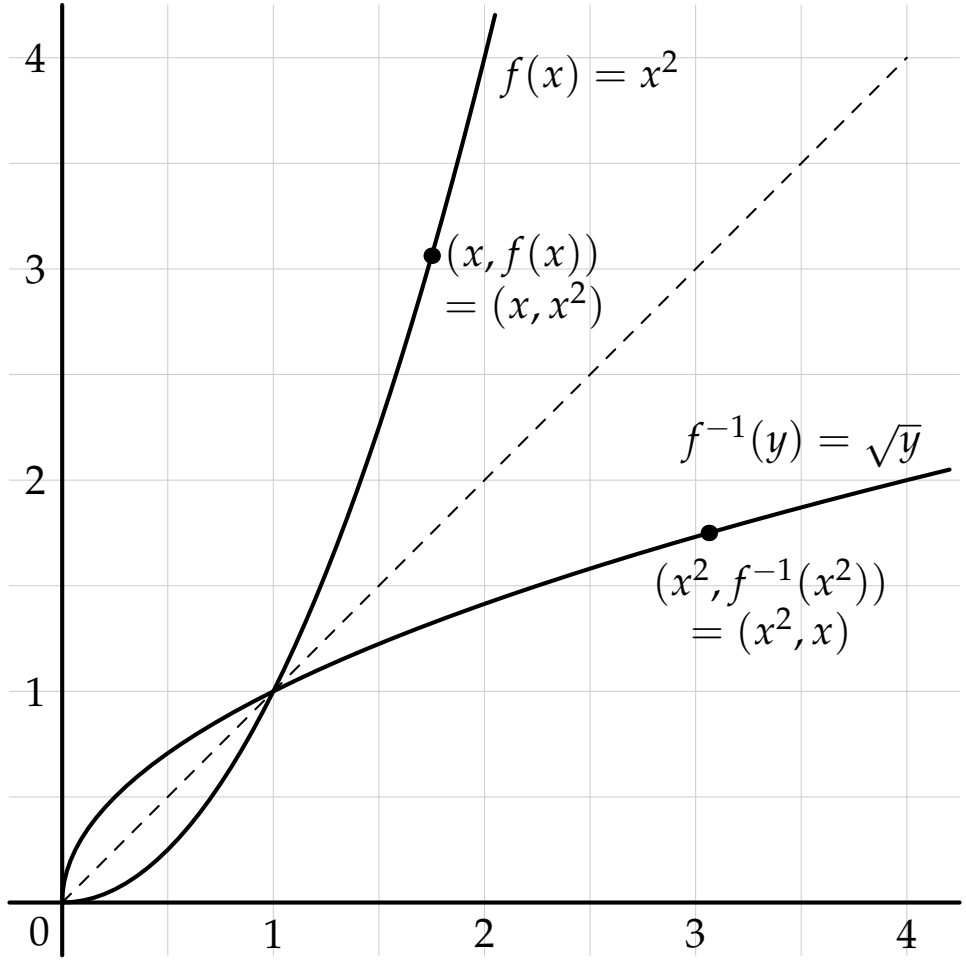
$$f^{-1}(y) = x \iff f(x) = y.$$

Exercise 2.8

Suppose that $f : X \to Y$ is represented by a diagram, as in Example 2.6. How can you obtain the diagram representing the inverse function $f^{-1} : Y \to X$?

Graph of a Bijective Function and its Inverse

Let $\mathbb{R}_{\geq 0} = \{x \in \mathbb{R} : x \geq 0\}$. The graph below shows the function $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ defined by $f(x) = x^2$. The inverse function to f is $f^{-1}(y) = \sqrt{y}$.



Further Examples of Inverse Functions

Example 2.9

Let $Y = \{y \in \mathbb{R} : 0 \leq y < 2\}$. Let $f : \mathbb{R}_{\geq 0} \to Y$ be the function defined by $f(x) = 2x/(1+x)$. For $y \in Y$ we have

$$\frac{2x}{1+x} = y \iff y + xy = 2x \iff y = x(2-y) \iff \frac{y}{2-y} = x.$$

Hence $f(x) = y \iff x = y/(2-y)$. Since $y \geq 0$ and $2 - y > 0$, the solution $x = y/(2-y)$ is in the domain $\mathbb{R}_{\geq 0}$ of h.

Therefore f is a bijection with inverse $f^{-1}(y) = y/(2-y)$.

Further Examples of Inverse Functions

Example 2.9

Let $Y = \{y \in \mathbb{R} : 0 \leq y < 2\}$. Let $f : \mathbb{R}_{\geq 0} \to Y$ be the function defined by $f(x) = 2x/(1+x)$. For $y \in Y$ we have

$$\frac{2x}{1+x} = y \iff y + xy = 2x \iff y = x(2-y) \iff \frac{y}{2-y} = x.$$

Hence $f(x) = y \iff x = y/(2-y)$. Since $y \geq 0$ and $2 - y > 0$, the solution $x = y/(2-y)$ is in the domain $\mathbb{R}_{\geq 0}$ of h.

Therefore f is a bijection with inverse $f^{-1}(y) = y/(2-y)$.

Example 2.10

Let $Y = \{y \in \mathbb{R} : -1 \leq y \leq 1\}$. Consider $\sin : \mathbb{R} \to Y$. This function is not bijective. For example, $\sin 0 = \sin 2\pi = 0$, so the equation $\sin x = 0$ does not have a unique solution. To find an inverse we must first restrict the domain.

Injective and Surjective Functions

Definition 2.11

Let $f : X \to Y$ be a function.

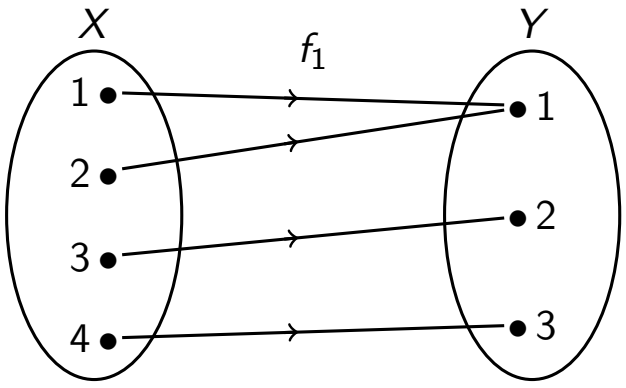
(i) We say that f is *injective* if for all $x, x' \in X$,

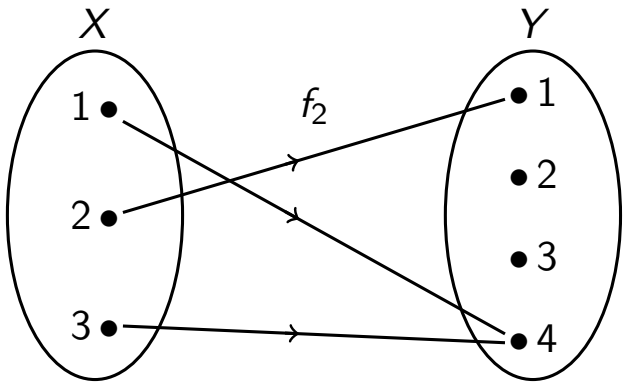
$$f(x) = f(x') \implies x = x'.$$

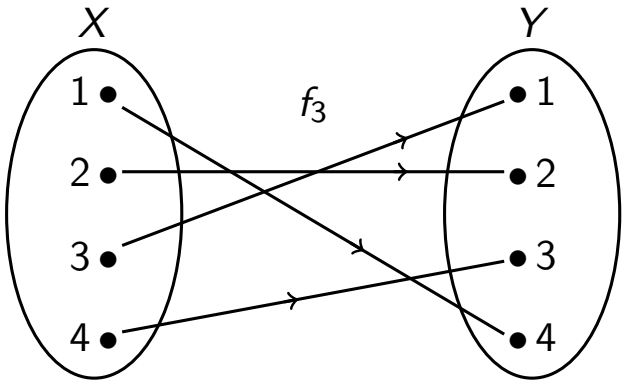
(ii) We say that f is *surjective* if for all $y \in Y$ there exists $x \in X$ such that $f(x) = y$.

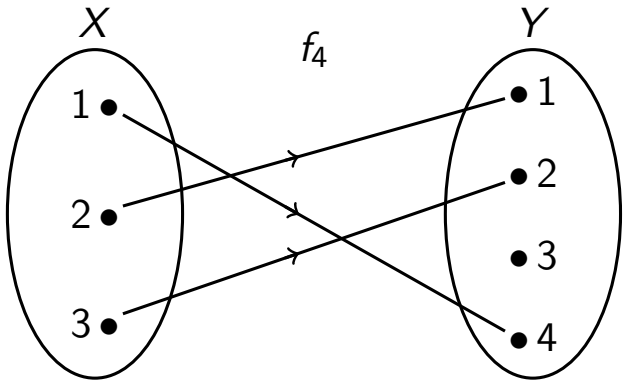
Example 2.12

Consider the functions from Example 2.6.



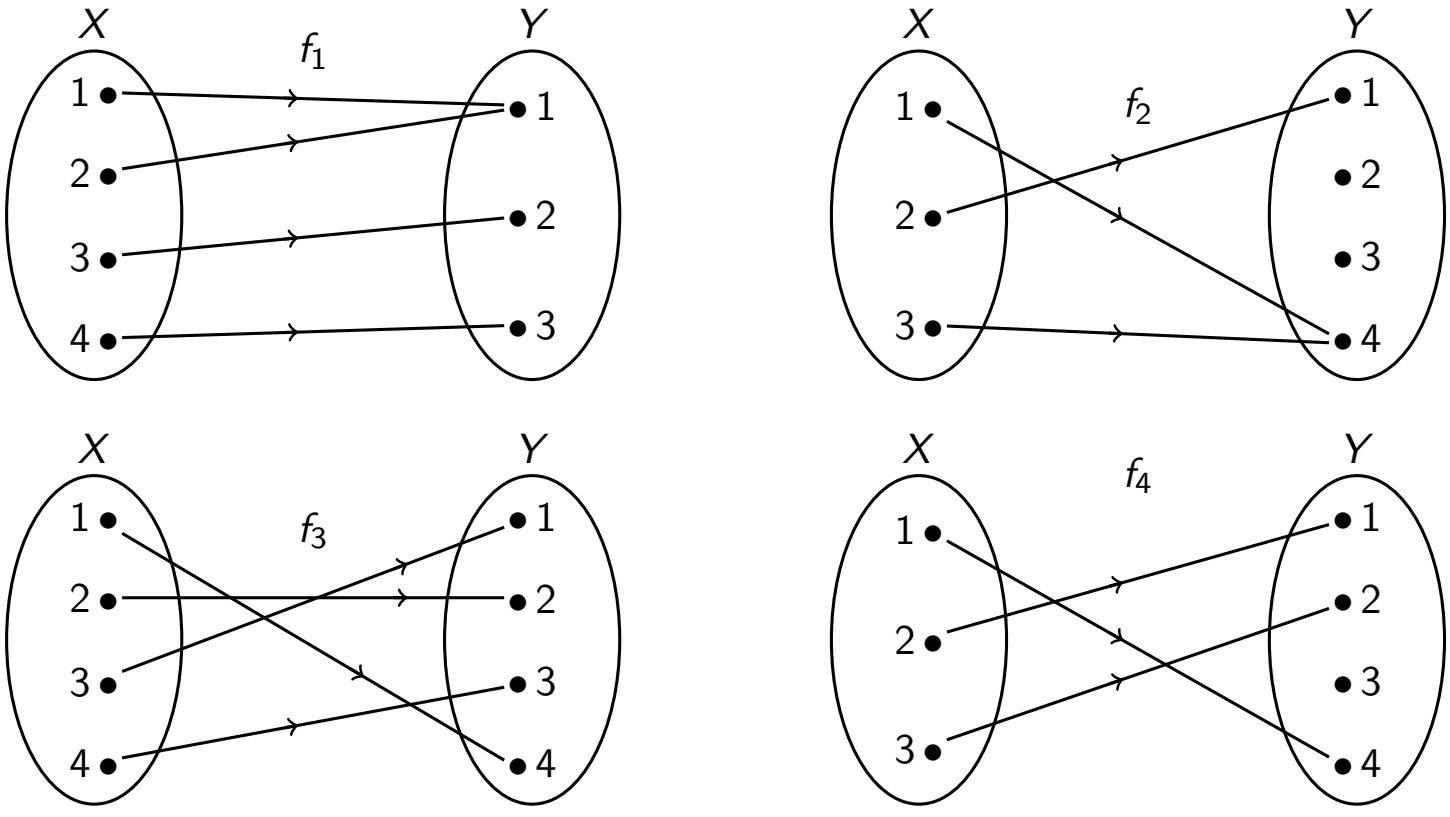






Example 2.12

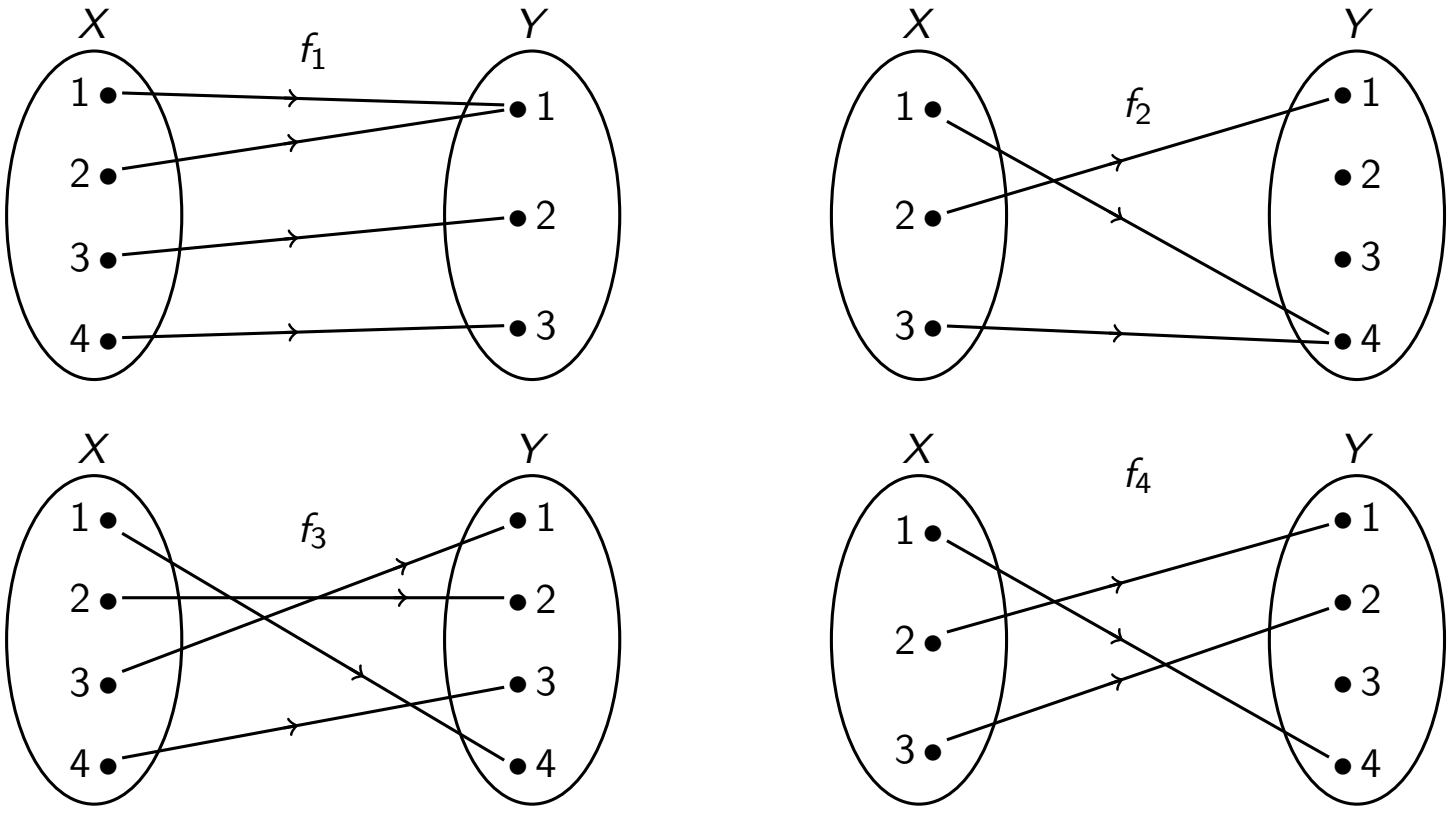
Consider the functions from Example 2.6.



- f_1 is not injective, since $f(1) = f(2)$; f_1 is surjective,

Example 2.12

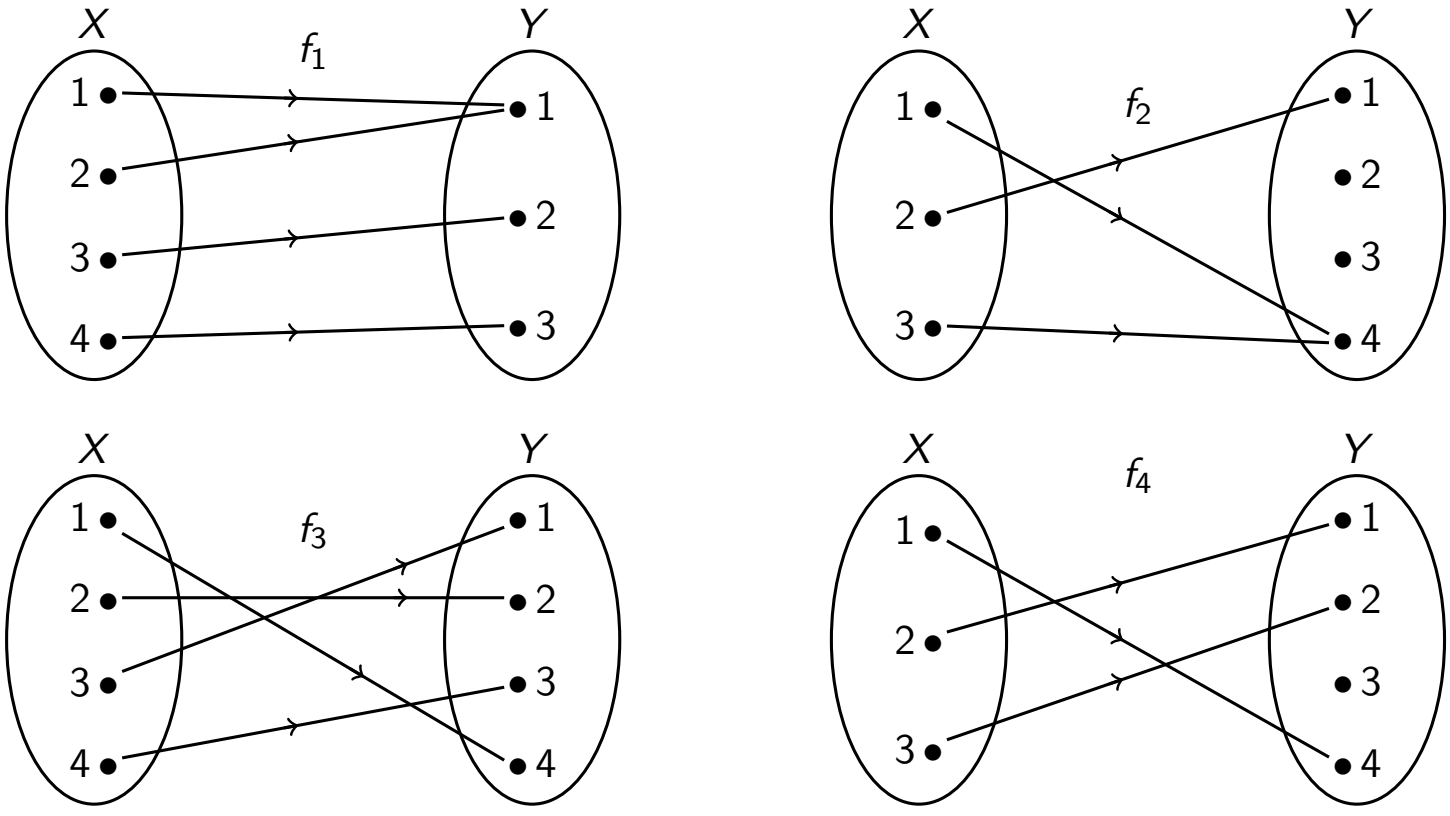
Consider the functions from Example 2.6.



- f_1 is not injective, since $f(1) = f(2)$; f_1 is surjective,
- f_2 is not injective and not surjective,

Example 2.12

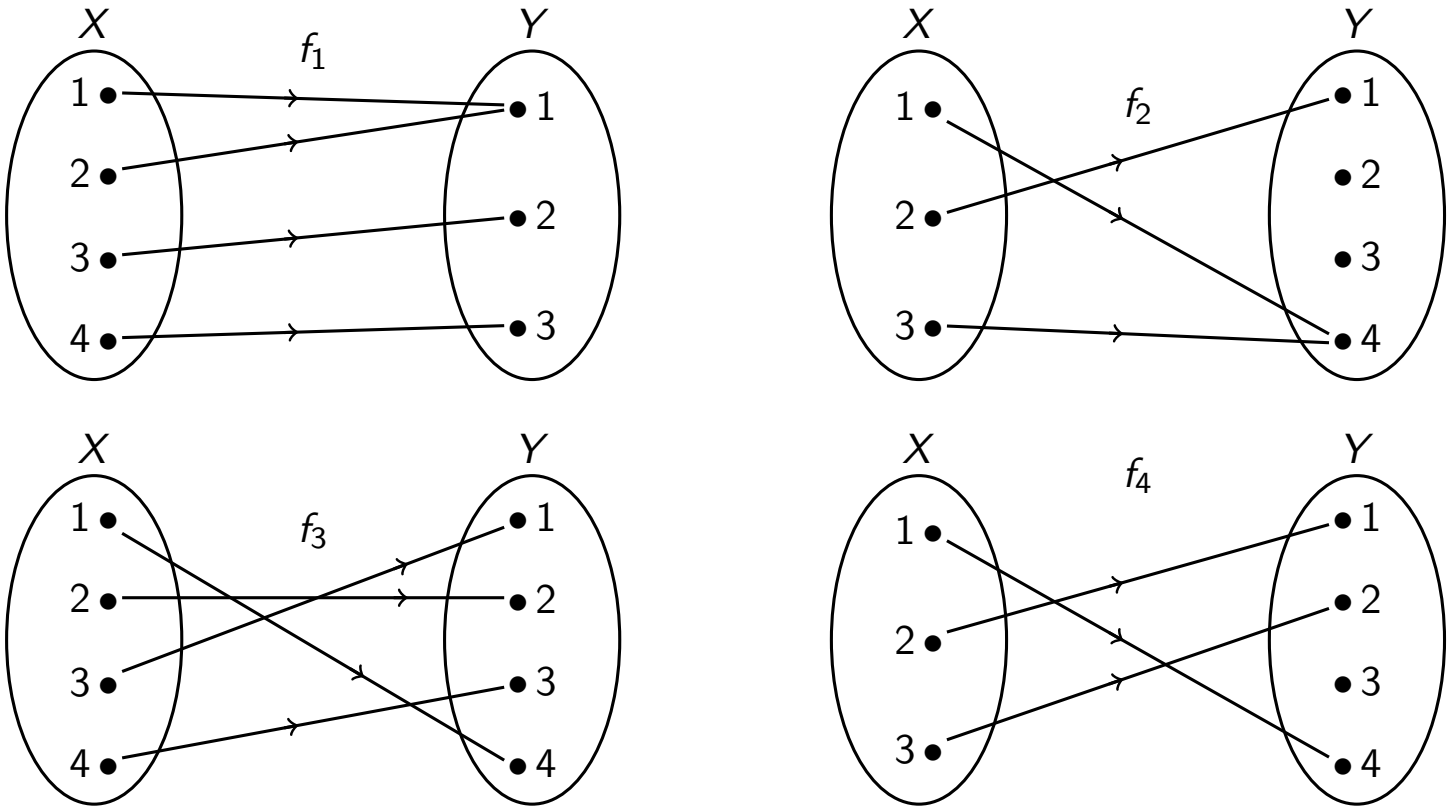
Consider the functions from Example 2.6.



- f_1 is not injective, since $f(1) = f(2)$; f_1 is surjective,
- f_2 is not injective and not surjective,
- f_3 is injective and surjective,

Example 2.12

Consider the functions from Example 2.6.



- f_1 is not injective, since $f(1) = f(2)$; f_1 is surjective,
- f_2 is not injective and not surjective,
- f_3 is injective and surjective,
- f_4 is injective; f_4 is not surjective, since there does not exist $x \in X$ such that $f(x) = 3 \in Y$.

Exercise on Injective, Surjective and Bijective Functions

We will see equivalent ways to state injective, surjective and bijective in Lecture 5. In particular we will see that

$$f \text{ is bijective } \iff f \text{ is injective and } f \text{ is surjective.}$$

A sadly **common error** is to write 'for all $x \in X$ there exists a unique $y \in Y$ such that $f(x) = y$' to mean f is injective. This is true by definition of a function, and **is nothing to do with f being injective**.

Feedback on Sheet 1

A–J in blue folder, K–Z in green folder.

- Sheet 1 was mostly done very well. I have updated the answers to Sheet 1 on Moodle with some feedback on common errors.
- **Q2** and **Q3** were used for the numerical mark. Some people gave examples when a general argument was needed. E.g.
  - To show $\mathbb{Q}_{<0}$ is not closed under multiplication, one example suffices, e.g. $-1 \times -1 = 1$;
  - To show $\mathbb{Q}_{<0}$ is closed under addition, a general argument is needed. One example is **not** enough.
- Many people had an extra 'false' solution in **Q4(b)**. Correct use of implication signs would have avoided this: see model answers.
- In **Q5**, many answers showed that $z \in (X \cap Y)' \implies z \in X' \cup Y'$, and so $(X \cap Y)' \subseteq X' \cup Y'$, and then announced that $(X \cap Y)' = X' \cup Y'$. This does not follow. You must also show $X' \cup Y' \subseteq (X \cap Y)'$.

Diagrams and the Horizontal Line Test

Exercise 2.13

Let $f : X \to Y$ be represented by a diagram. Then

$$f \text{ is injective} \iff \begin{array}{c}\text{no element of the codomain } Y \text{ has two} \\ \text{(or more) arrows coming into it.}\end{array}$$

Give a similar condition for f to be surjective. Give a similar condition for f to be bijective.

Exercise 2.14

By looking at the graph of a function $f : X \to \mathbb{R}$, where $X \subseteq \mathbb{R}$, we can detect whether f is injective by looking at the horizontal lines going through $(0, y)$ for each $y \in \mathbb{R}$. This is called the *horizontal line test*:

$$f \text{ is injective} \iff \begin{array}{c}\text{each horizontal line hits the graph of } f \text{ at} \\ \text{most once.}\end{array}$$

Give similar conditions for f to be surjective and bijective.

Composing Functions

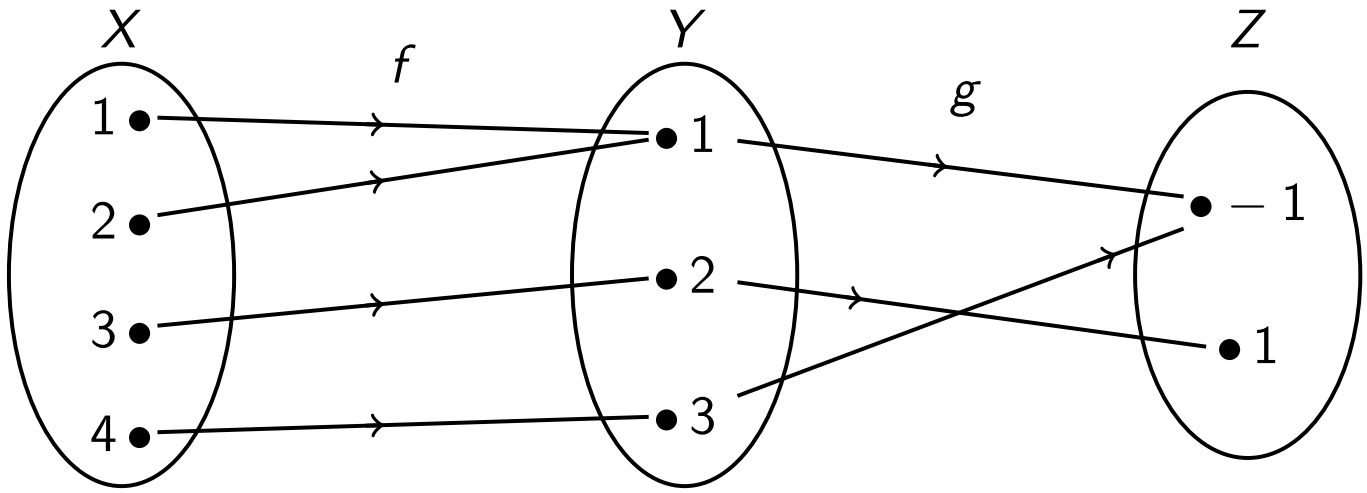
Let $f : X \to Y$ and $g : Y \to Z$ be functions. The *composition of f and g* is the function $gf : X \to Z$, defined by

$$(gf)(x) = g\big(f(x)\big).$$

Note that gf means 'do f, then do g'. One has to get used to reading function compositions from right to left.

Example 2.15

Let $f : \{1, 2, 3, 4\} \to \{1, 2, 3\}$ be the function f_1 from Example 2.6.
Let $g : \{1, 2, 3\} \to \{-1, 1\}$ be defined by $g(x) = (-1)^x$.



Composing Functions

Lemma 2.16 (Examinable)

Let $f : X \to Y$ and $g : Y \to Z$ be functions.

(i) *If f and g are injective then gf is injective.*

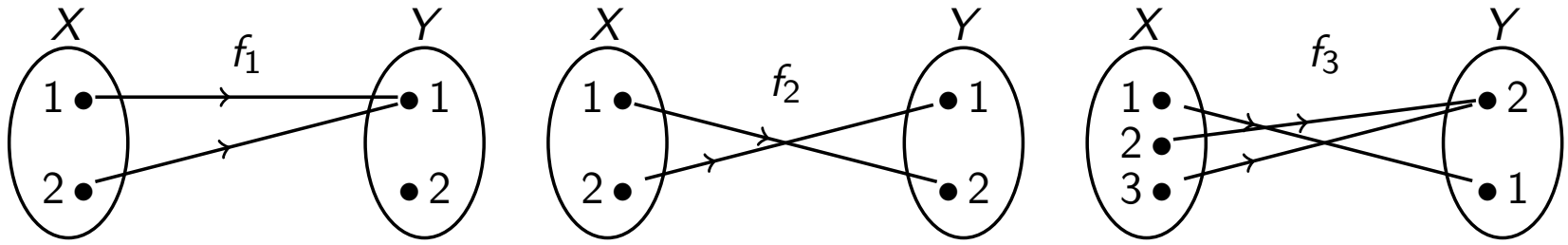
(ii) *If f and g are surjective then gf is surjective.*

(iii) *If f and g are bijective then gf is bijective.*

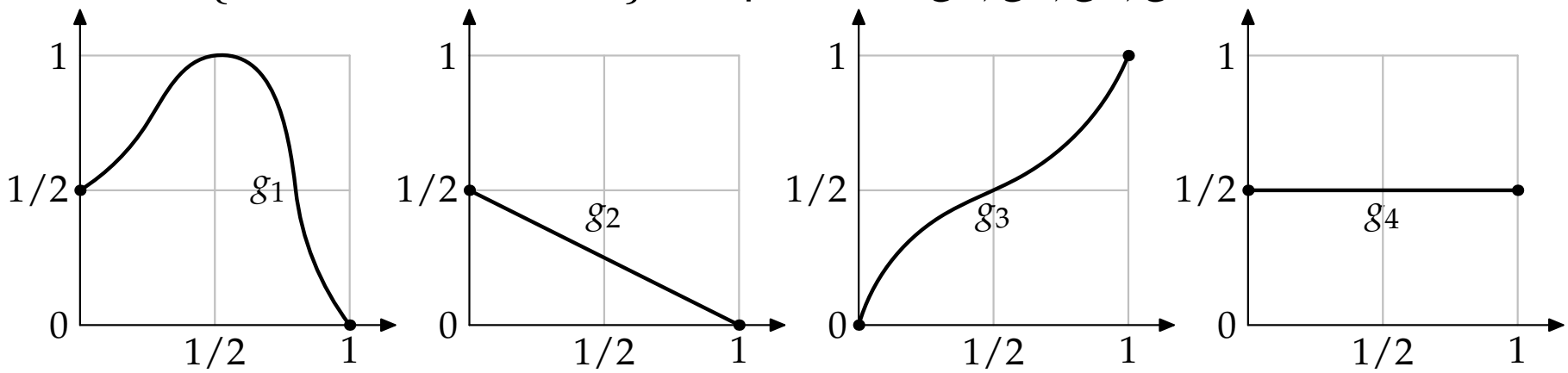
For (ii) see Question 5(a) on Sheet 2.

Final Quiz on Injective, Surjective and Bijective Functions

Which of the functions f_1, f_2, f_3 shown below are (a) injective, (b) surjective, (c) bijective?



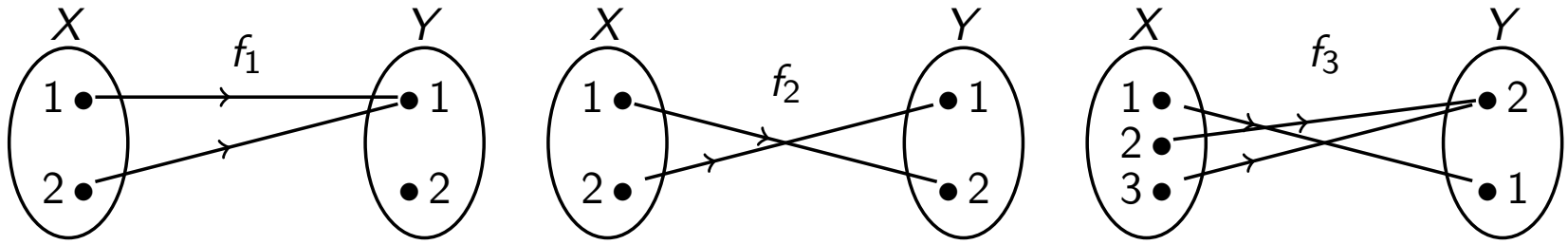
Let $X = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$. Repeat for $g_1, g_2, g_3, g_4 : X \to X$.



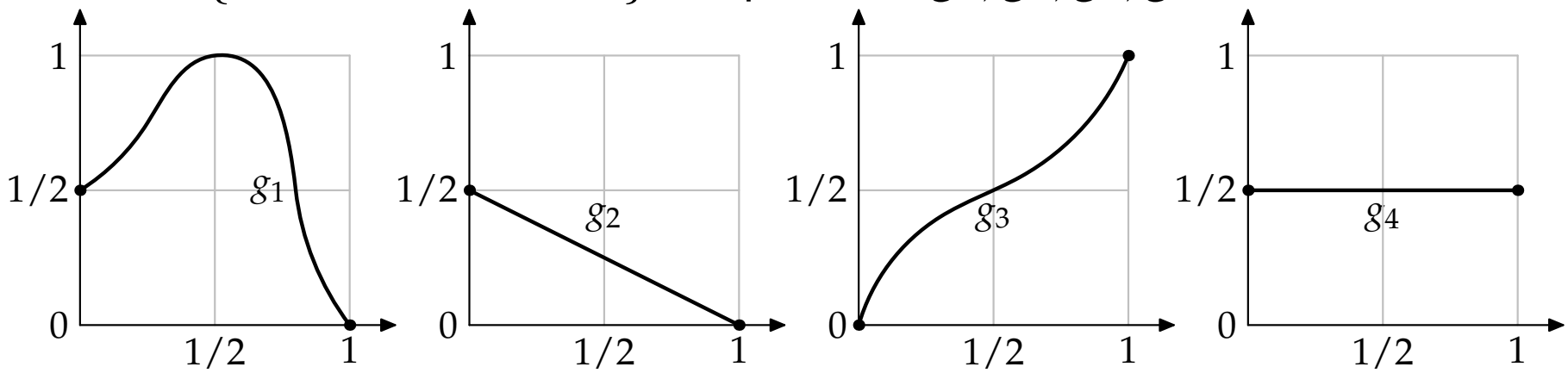
	Injective	Surjective	Bijective
g_1			
g_2			
g_3			
g_4			

Final Quiz on Injective, Surjective and Bijective Functions

Which of the functions f_1, f_2, f_3 shown below are (a) injective, (b) surjective, (c) bijective?



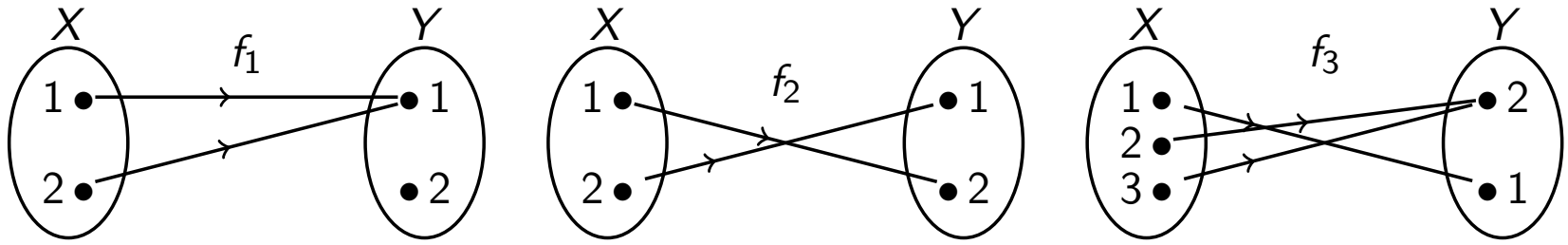
Let $X = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$. Repeat for $g_1, g_2, g_3, g_4 : X \to X$.



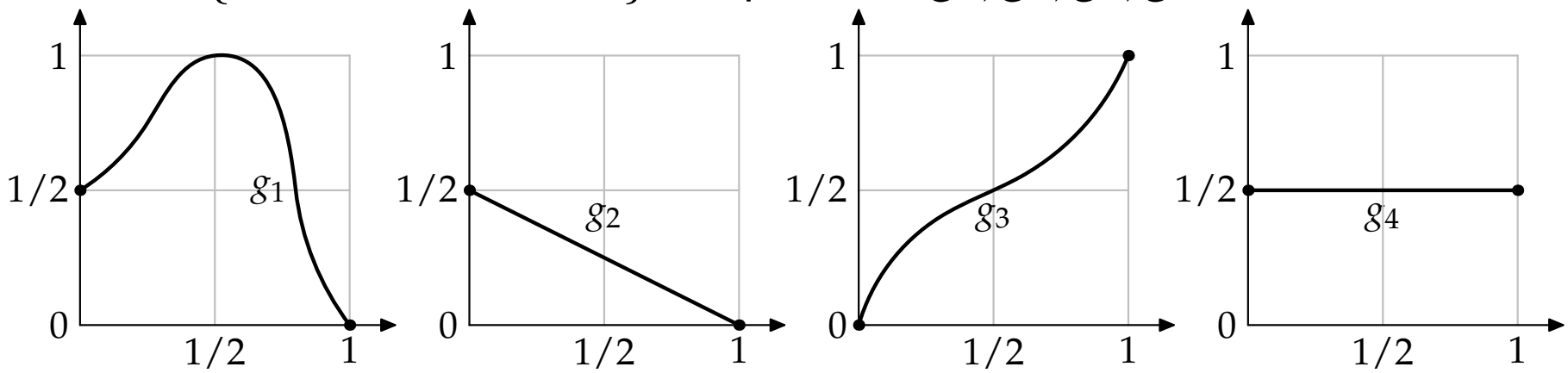
	Injective	Surjective	Bijective
g_1	No	Yes	No
g_2			
g_3			
g_4			

Final Quiz on Injective, Surjective and Bijective Functions

Which of the functions f_1, f_2, f_3 shown below are (a) injective, (b) surjective, (c) bijective?



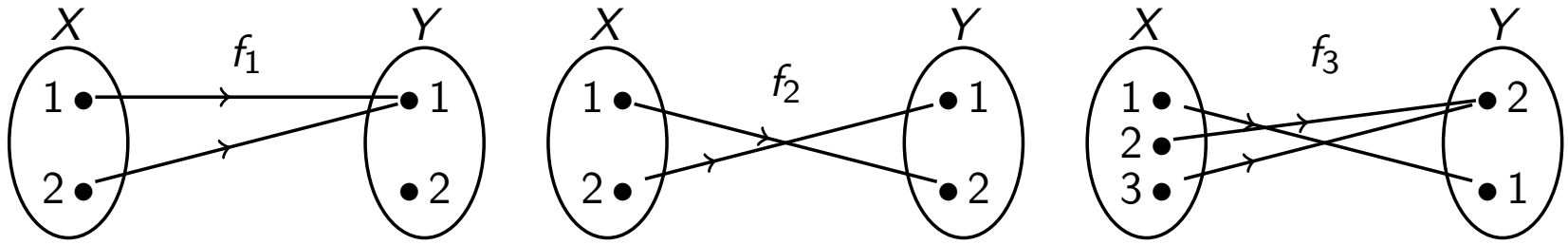
Let $X = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$. Repeat for $g_1, g_2, g_3, g_4 : X \to X$.



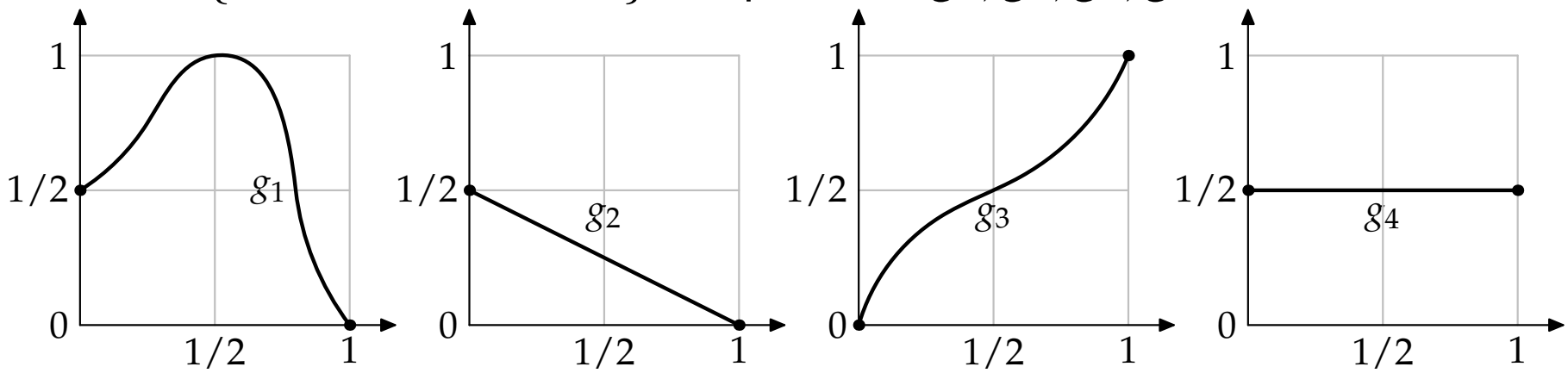
	Injective	Surjective	Bijective
g_1	No	Yes	No
g_2	Yes	No	No
g_3			
g_4			

Final Quiz on Injective, Surjective and Bijective Functions

Which of the functions f_1, f_2, f_3 shown below are (a) injective, (b) surjective, (c) bijective?



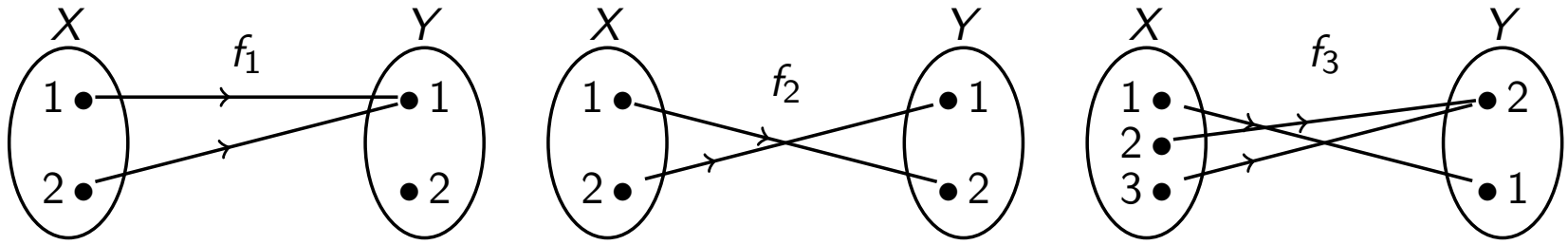
Let $X = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$. Repeat for $g_1, g_2, g_3, g_4 : X \to X$.



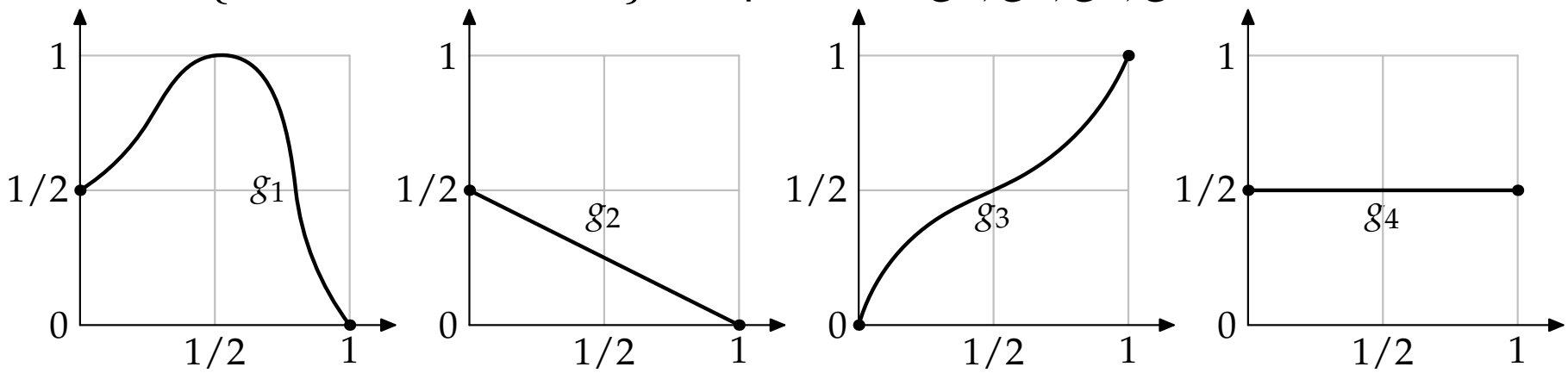
	Injective	Surjective	Bijective
g_1	No	Yes	No
g_2	Yes	No	No
g_3	Yes	Yes	Yes
g_4			

Final Quiz on Injective, Surjective and Bijective Functions

Which of the functions f_1, f_2, f_3 shown below are (a) injective, (b) surjective, (c) bijective?



Let $X = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$. Repeat for $g_1, g_2, g_3, g_4 : X \to X$.



	Injective	Surjective	Bijective
g_1	No	Yes	No
g_2	Yes	No	No
g_3	Yes	Yes	Yes
g_4	No	No	No

Inverse of a Composition of Functions

By (c), if $f : X \to Y$ and $g : Y \to Z$ are bijections, then $gf : X \to Z$ is a bijection, and so it has an inverse function. To undo the composition $gf : X \to Z$ we must first undo $g : Y \to Z$, then undo $f : X \to Y$. Hence

$$(gf)^{-1} = f^{-1}g^{-1}.$$

This result can be useful when finding inverse functions.

Example 2.17

Let

$$f(x) = \sqrt{\frac{2x^2}{1+x^2}}.$$

We can write f as a composition: $f = f_3 f_2 f_1$ where $f_1(x) = x^2$, $f_2(x) = 2x/(1+x)$ and $f_3(x) = \sqrt{x}$. In the lecture we will sort out the domains and codomains of f and f_1, f_2, f_3, and hence find the inverse to f.

Associativity and Identity Functions

The *associative property of composition* states that if $f : X \to Y$, $g : Y \to Z$ and $h : Z \to W$ are any functions then

$$(hg)f = h(gf) : X \to W.$$

This has a one-line proof.

We will see associativity again in §10 of the course on rings.

Associativity and Identity Functions

The *associative property of composition* states that if $f : X \to Y$, $g : Y \to Z$ and $h : Z \to W$ are any functions then

$$(hg)f = h(gf) : X \to W.$$

This has a one-line proof.

We will see associativity again in §10 of the course on rings.

Suppose $f : X \to Y$ is a bijection. We have seen that f has an inverse function $f^{-1} : Y \to X$, with the defining property

$$f^{-1}(y) = x \iff f(x) = y.$$

What happens when we compose f and f^{-1}?

Associativity and Identity Functions

The *associative property of composition* states that if $f : X \to Y$, $g : Y \to Z$ and $h : Z \to W$ are any functions then

$$(hg)f = h(gf) : X \to W.$$

This has a one-line proof.

We will see associativity again in §10 of the course on rings.

Suppose $f : X \to Y$ is a bijection. We have seen that f has an inverse function $f^{-1} : Y \to X$, with the defining property

$$f^{-1}(y) = x \iff f(x) = y.$$

What happens when we compose f and f^{-1}?

The *identity* function on a set X is the function $\mathrm{id}_X : X \to X$ defined by $\mathrm{id}_X(x) = x$ for all $x \in X$.

Extra: Non-examinable, but Interesting Mathematics

Lemma 2.18

Let X and Y be non-empty sets and let $f : X \to Y$ be a function.

(a) *f is injective $\iff$ there exists $g : Y \to X$ such that $gf = \mathrm{id}_X$.*

(b) *f is surjective $\iff$ there exists $h : Y \to X$ such that $fh = \mathrm{id}_Y$.*

Moreover, if $gf = \mathrm{id}_X$ and $fh = \mathrm{id}_Y$ then f is bijective and $g = h = f^{-1}$.

§3 Complex Numbers

Introduce a new symbol i with the property that $i^2 = -1$.

Definition 3.1

A *complex number* is defined to be a symbol of the form $a + bi$ where $a, b \in \mathbb{R}$. If $z = a + bi$ then we say that a is the *real part* of z, and b is the *imaginary part of* z, and write $\operatorname{Re} z = a$, $\operatorname{Im} z = b$. We write $\mathbb{C}$ for the set of all complex numbers.

§3 Complex Numbers

Introduce a new symbol i with the property that $i^2 = -1$.

Definition 3.1

A *complex number* is defined to be a symbol of the form $a + bi$ where $a, b \in \mathbb{R}$. If $z = a + bi$ then we say that a is the *real part* of z, and b is the *imaginary part of* z, and write $\operatorname{Re} z = a$, $\operatorname{Im} z = b$. We write $\mathbb{C}$ for the set of all complex numbers.

Please interpret the 'complex' in complex number as meaning 'made of more than one part', rather than 'difficult'. The word 'imaginary' is also standard—please do not be put off by it.

Exercise 3.2

Calculate $(1 + i)^3$.

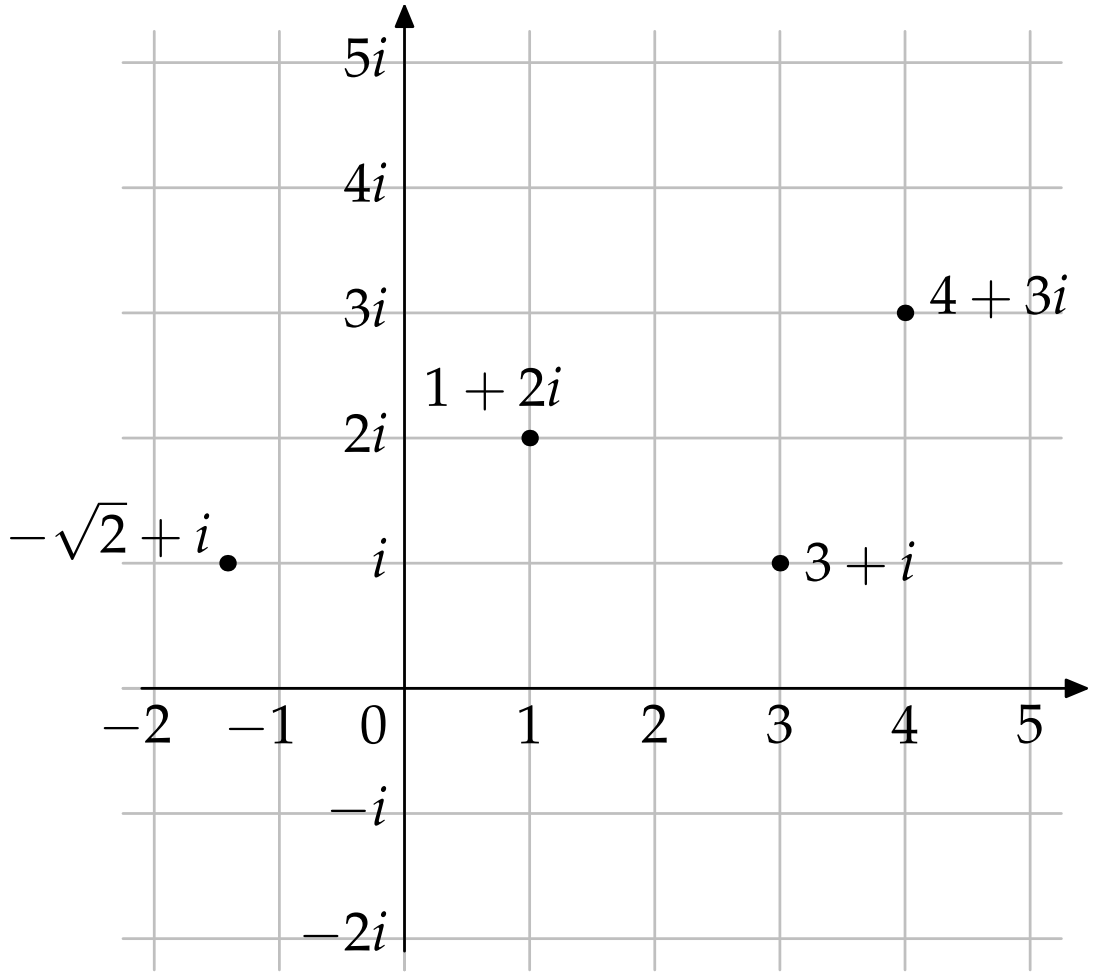
Adding, Subtracting and Multiplying in $\mathbb{C}$

The rules for adding, multiplying and subtracting complex numbers follow from the property that $i^2 = -1$. If $a + bi$ and $c + di \in \mathbb{C}$ are complex numbers in Cartesian form then

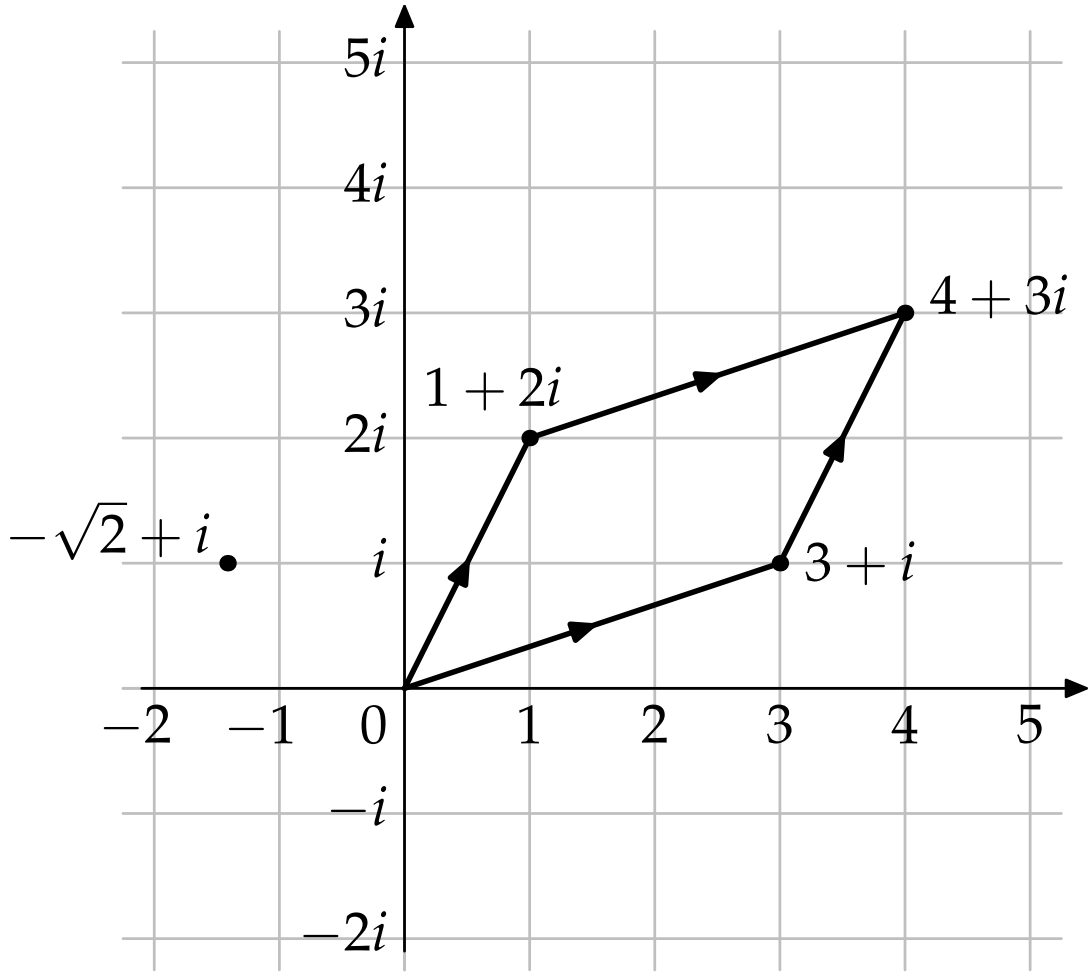
$$(a + bi) + (c + di) = (a + c) + (b + d)i$$
$$(a + bi) - (c + di) = (a - c) + (b - d)i$$
$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

So the set $\mathbb{C}$ of complex numbers is closed under addition, subtraction and multiplication.

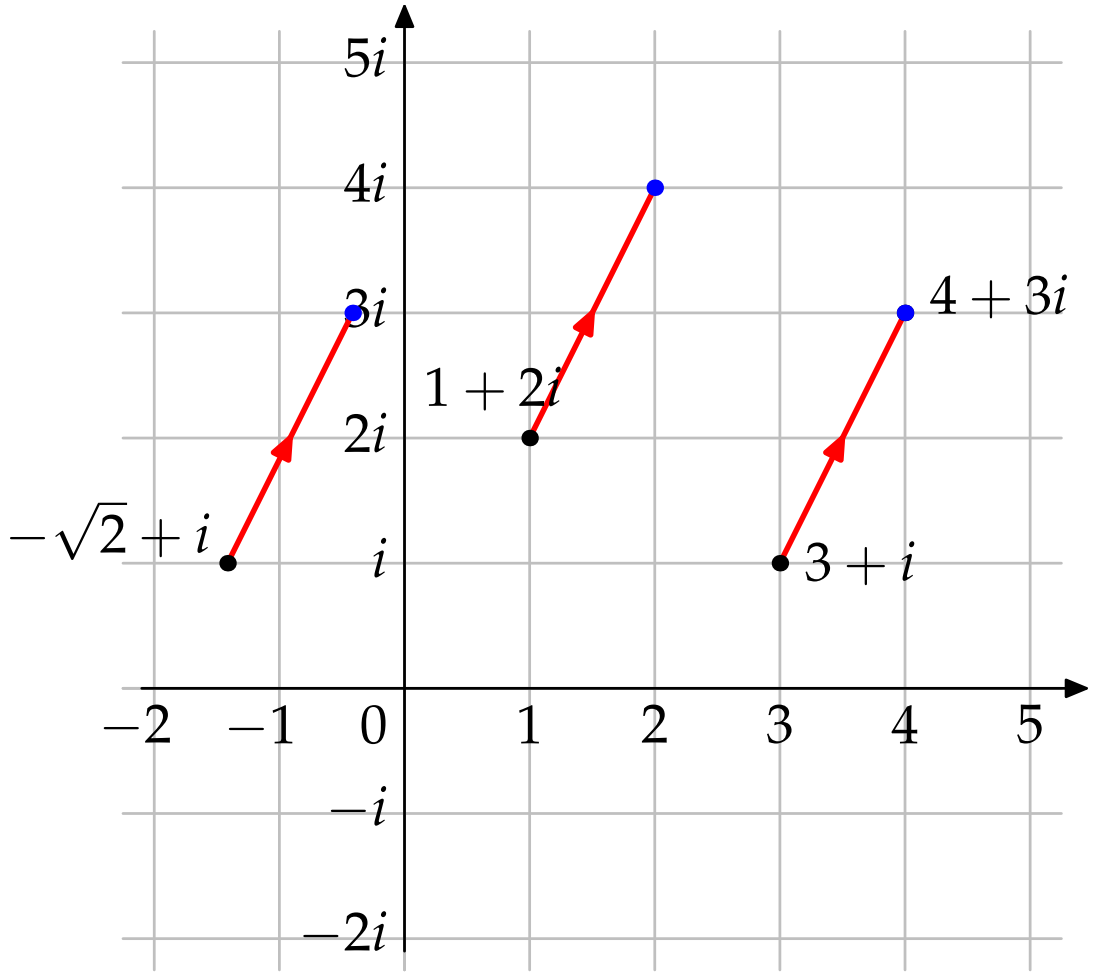
Argand Diagram



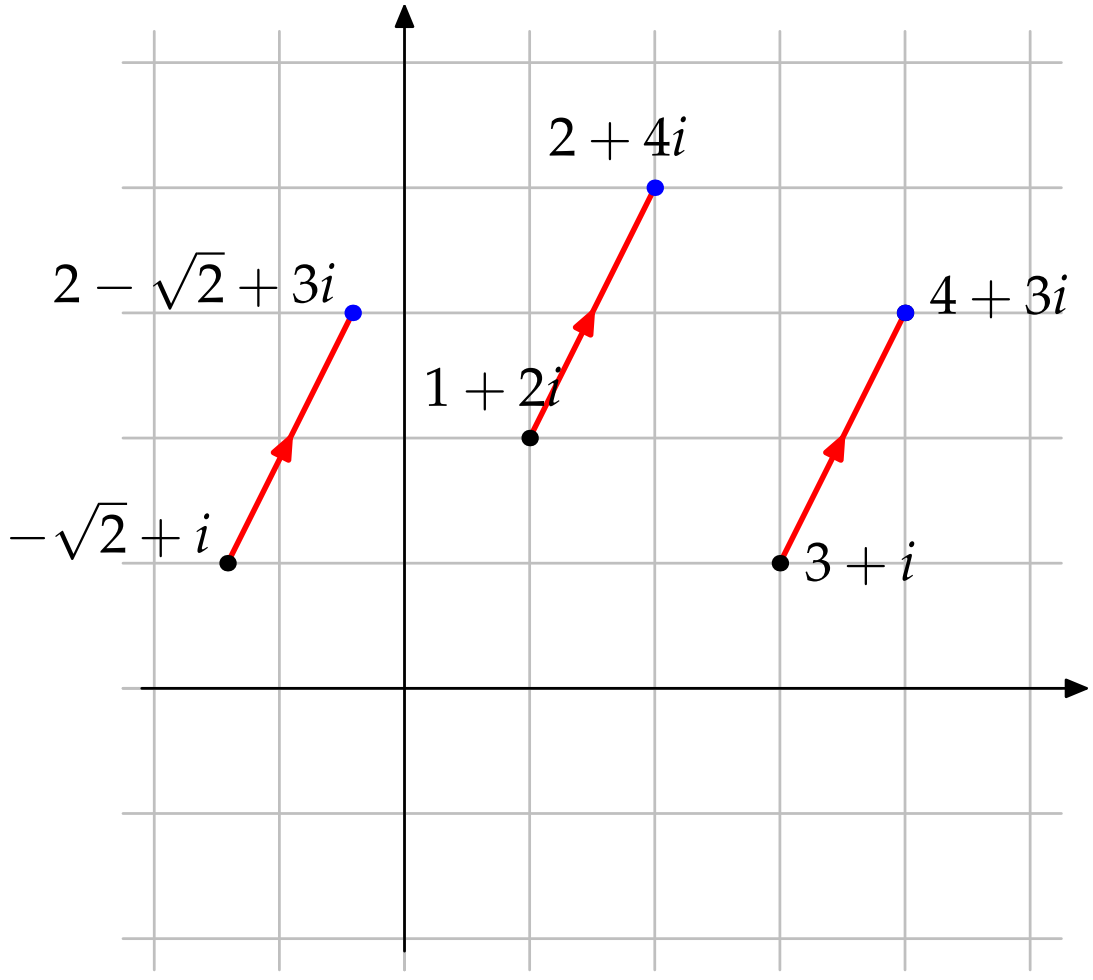
Argand Diagram



Argand Diagram: Adding $1 + 2i$



Argand Diagram: Adding $1 + 2i$



Complex Conjugate and Modulus

We define the *modulus* of z, written $|z|$, to be $\sqrt{a^2 + b^2}$. We define the *complex conjugate* of z, written $\overline{z}$, to be $a - bi$.

We read $|z|$ as 'mod z' and $\overline{z}$ as 'z bar'.

Lemma 3.4 (Examinable)

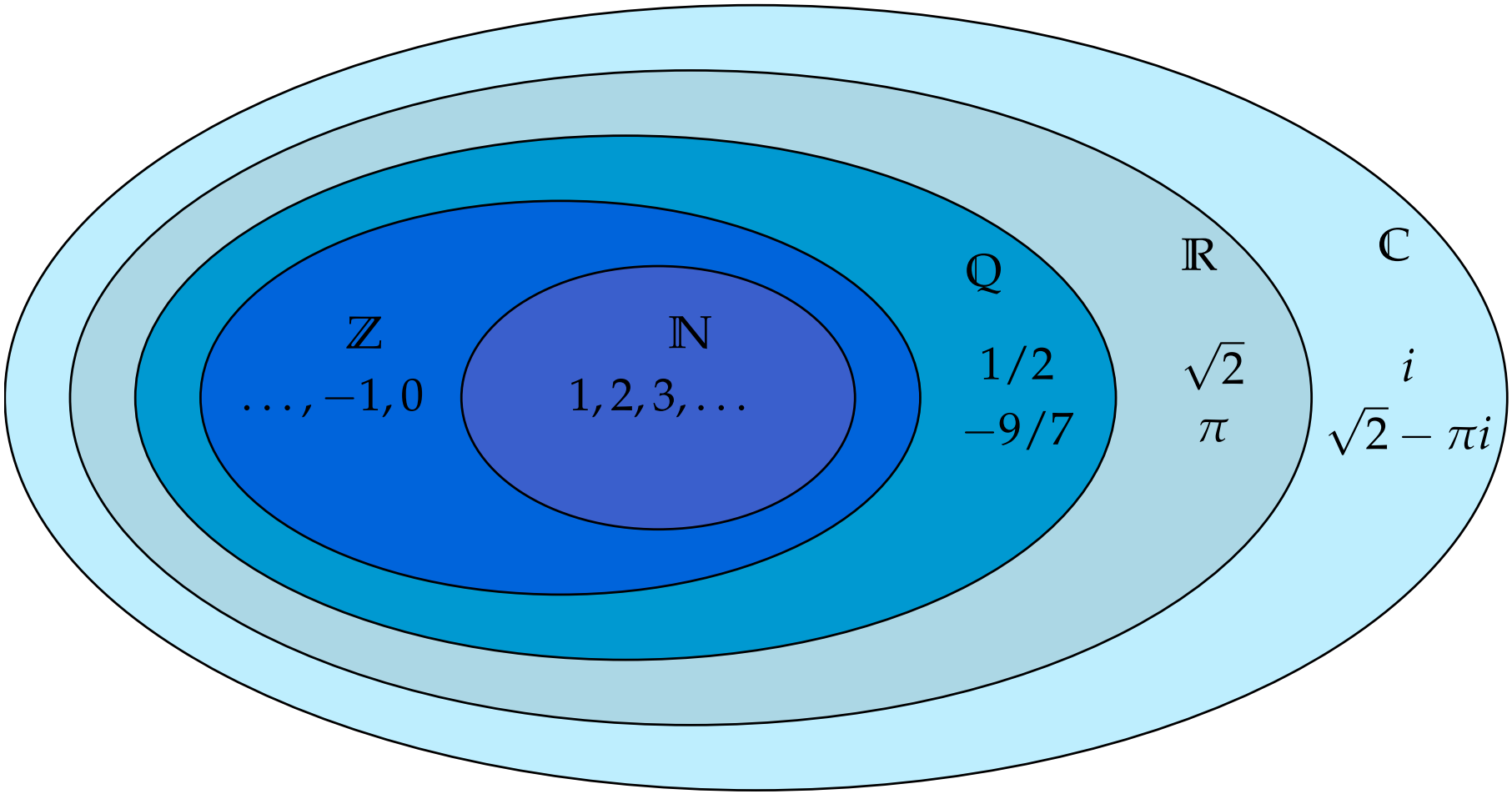
Let $z \in \mathbb{C}$. Then

(a) $|z|^2 = z\overline{z}$.

(b) *If $z \neq 0$ then $1/z = \overline{z}/|z|^2$.*

(c) *The set $\mathbb{C}$ of complex numbers is closed under division.*

Number Systems So Far



Quiz

True or false?

(i) The equation $z^2 = -2$ has a solution in $\mathbb{C}$.

(ii) $\mathrm{Im}(\overline{1+i}) = 1$.

(iii) $(-1+3i)+(5-3i) = 4$.

(iv) $z = 1+2i \implies \bar{z}z = 5$.

(v) $\dfrac{2}{1+i} = 1-i$.

Quiz

True or false?

(i) The equation $z^2 = -2$ has a solution in $\mathbb{C}$.

True: $z^2 = -2 \iff z = i\sqrt{2}$ or $z = -i\sqrt{2}$

(ii) $\mathrm{Im}(\overline{1+i}) = 1$.

(iii) $(-1+3i)+(5-3i) = 4$.

(iv) $z = 1+2i \implies \bar{z}z = 5$.

(v) $\dfrac{2}{1+i} = 1-i$.

Quiz

True or false?

(i) The equation $z^2 = -2$ has a solution in $\mathbb{C}$.

True: $z^2 = -2 \iff z = i\sqrt{2}$ or $z = -i\sqrt{2}$

(ii) $\mathrm{Im}(\overline{1+i}) = 1$.

False: $\overline{1+i} = 1 - i \implies \mathrm{Im}(\overline{1+i}) = -1$

(iii) $(-1 + 3i) + (5 - 3i) = 4$.

(iv) $z = 1 + 2i \implies \bar{z}z = 5$.

(v) $\dfrac{2}{1+i} = 1 - i$.

Quiz

True or false?

(i) The equation $z^2 = -2$ has a solution in $\mathbb{C}$.

True: $z^2 = -2 \iff z = i\sqrt{2}$ or $z = -i\sqrt{2}$

(ii) $\mathrm{Im}(\overline{1+i}) = 1$.

False: $\overline{1+i} = 1 - i \implies \mathrm{Im}(\overline{1+i}) = -1$

(iii) $(-1+3i) + (5-3i) = 4$.

True

(iv) $z = 1 + 2i \implies \bar{z}z = 5$.

(v) $\dfrac{2}{1+i} = 1 - i$.

Quiz

True or false?

(i) The equation $z^2 = -2$ has a solution in $\mathbb{C}$.

True: $z^2 = -2 \iff z = i\sqrt{2}$ or $z = -i\sqrt{2}$

(ii) $\mathrm{Im}(\overline{1+i}) = 1$.

False: $\overline{1+i} = 1 - i \implies \mathrm{Im}(\overline{1+i}) = -1$

(iii) $(-1+3i) + (5-3i) = 4$. True

(iv) $z = 1 + 2i \implies \bar{z}z = 5$. True

(v) $\dfrac{2}{1+i} = 1 - i$.

Quiz

True or false?

(i) The equation $z^2 = -2$ has a solution in $\mathbb{C}$.

True: $z^2 = -2 \iff z = i\sqrt{2}$ or $z = -i\sqrt{2}$

(ii) $\mathrm{Im}(\overline{1+i}) = 1$.

False: $\overline{1+i} = 1 - i \implies \mathrm{Im}(\overline{1+i}) = -1$

(iii) $(-1+3i) + (5-3i) = 4$. True

(iv) $z = 1 + 2i \implies \bar{z}z = 5$. True

(v) $\dfrac{2}{1+i} = 1 - i$. True

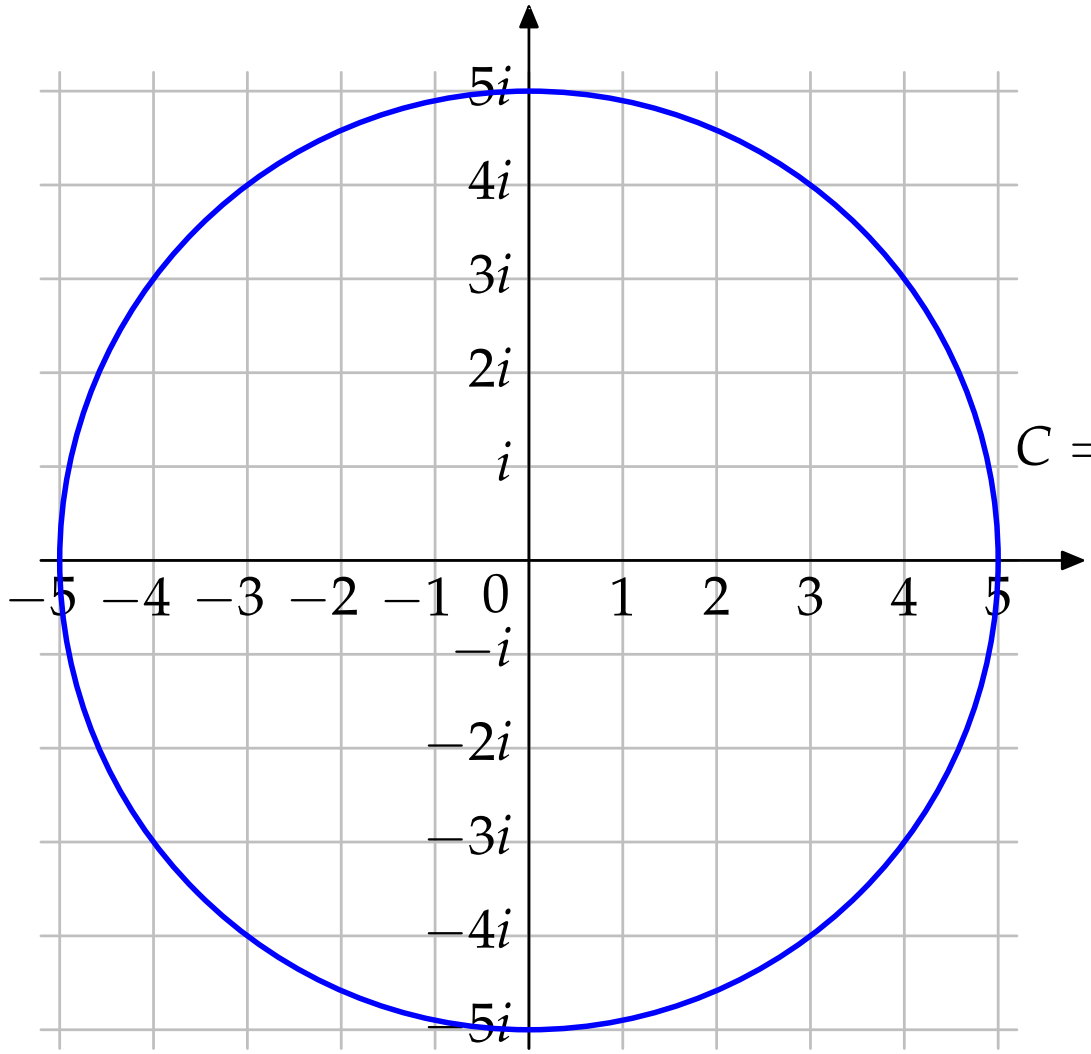
Administration

- Please take work from Sheet 2: A–J in green folder, L–Z in blue folder
- Uncollected work is left outside my office, making the department look untidy. Please claim it.
- Link to answers to Sheet 1 on Moodle fixed. (Please email me immediately if it seems something is missing.)
- Answers to Sheet 2 on Moodle updated with some feedback on common errors.
  - Q2 is basic: please check model answers.
  - Q3 and Q4 were marked by the postgraduates.
  - I looked at all Q5s. Many people made similar mistakes: see feedback on Moodle. (They were also some very good answers.)

  Please see lecturer if you have any queries about the marking.

Example 3.5(2): Equation Solving in $\mathbb{C}$

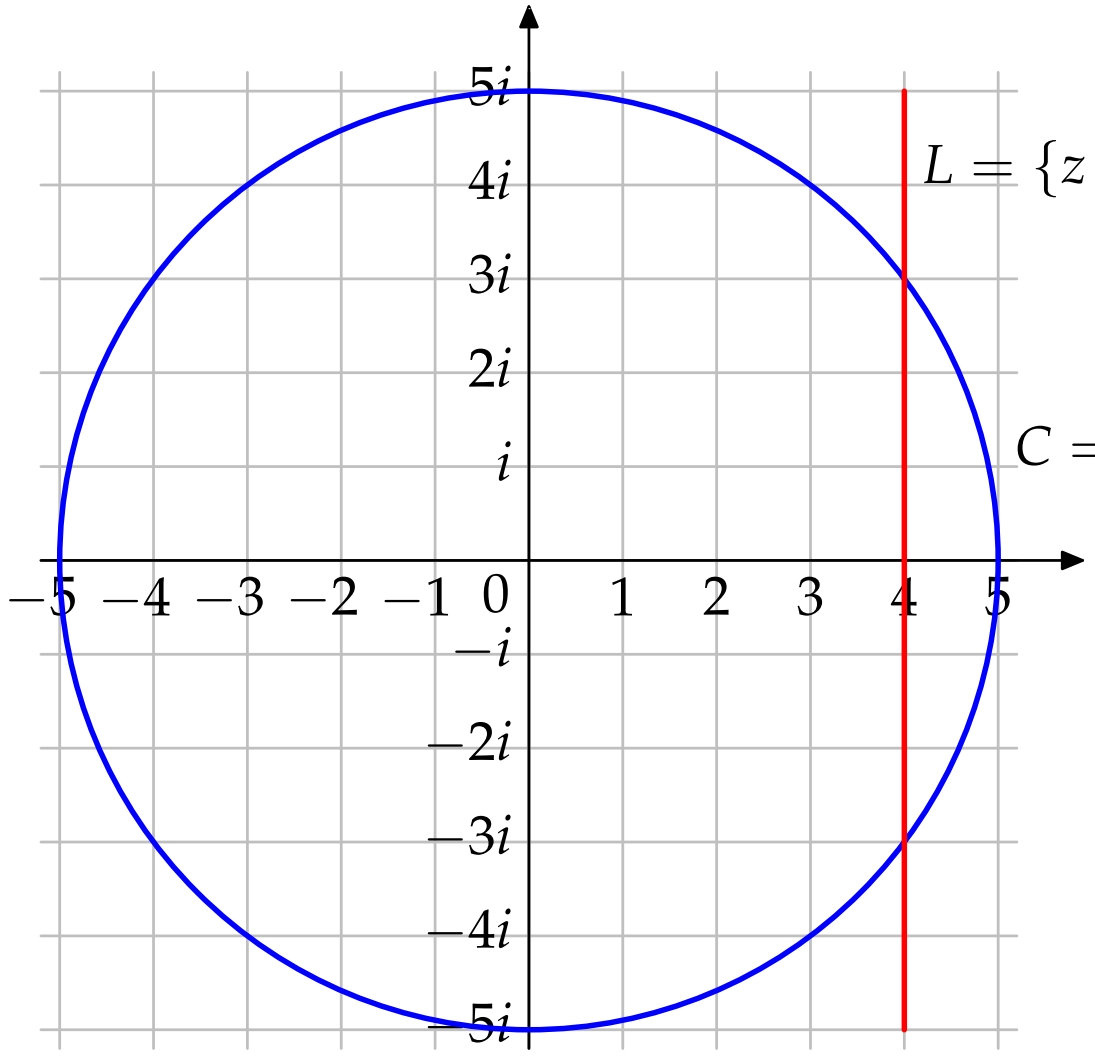
Consider the simultaneous equations $|z| = 5$ and $z + \overline{z} = 8$.



$C = \{z \in \mathbb{C} : |z| = 5\}$

Example 3.5(2): Equation Solving in $\mathbb{C}$

Consider the simultaneous equations $|z| = 5$ and $z + \bar{z} = 8$.

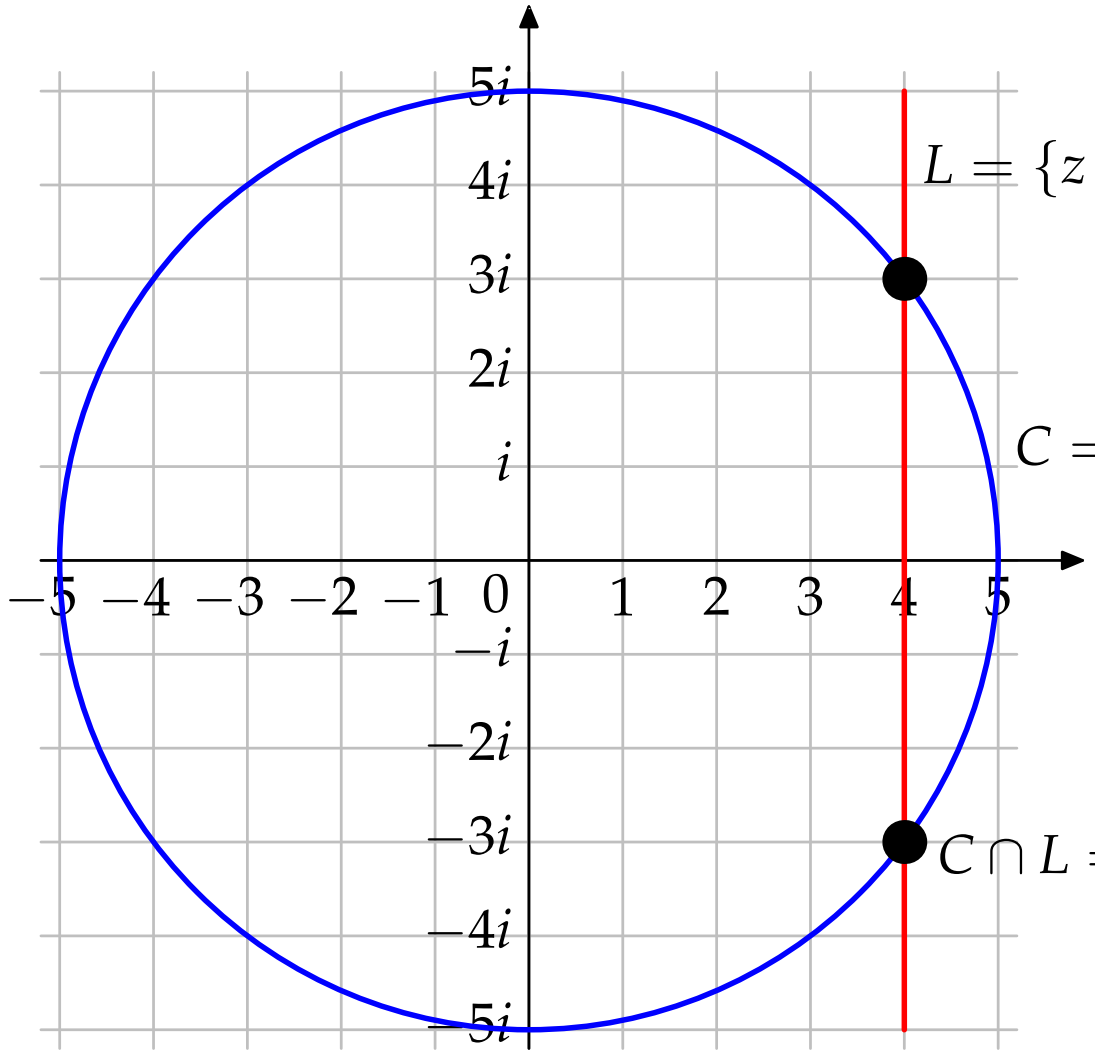


$L = \{z \in \mathbb{C} : z + \bar{z} = 8\}$

$C = \{z \in \mathbb{C} : |z| = 5\}$

Example 3.5(2): Equation Solving in $\mathbb{C}$

Consider the simultaneous equations $|z| = 5$ and $z + \bar{z} = 8$.



$L = \{z \in \mathbb{C} : z + \bar{z} = 8\}$

$C = \{z \in \mathbb{C} : |z| = 5\}$

$C \cap L = \{4 + 3i, 4 - 3i\}$

Polar Form and Arguments

Any complex number z can be written in the form

$$z = r(\cos\theta + i\sin\theta)$$

where $r \in \mathbb{R}_{\geq 0}$ and θ is an angle, measured in radians. This is called the *polar form* of z. Observe that $r = |z|$. We say that θ is an *argument* of z.

Definition 3.6

Let $z \in \mathbb{C}$ be non-zero. If $z = r(\cos\theta + i\sin\theta)$ where $0 \leq \theta < 2\pi$, then we say that θ is the *principal argument* of z, and write $\theta = \mathrm{Arg}(z)$.

Example 3.7 (See board)

Polar Form and Arguments

Any complex number z can be written in the form

$$z = r(\cos\theta + i\sin\theta)$$

where $r \in \mathbb{R}_{\geq 0}$ and θ is an angle, measured in radians. This is called the *polar form* of z. Observe that $r = |z|$. We say that θ is an *argument* of z.

Definition 3.6

Let $z \in \mathbb{C}$ be non-zero. If $z = r(\cos\theta + i\sin\theta)$ where $0 \leq \theta < 2\pi$, then we say that θ is the *principal argument* of z, and write $\theta = \mathrm{Arg}(z)$.

Example 3.7 (See board)

Quiz: What is the domain of the function Arg?

Polar Form and Arguments

Any complex number z can be written in the form

$$z = r(\cos\theta + i\sin\theta)$$

where $r \in \mathbb{R}_{\geq 0}$ and θ is an angle, measured in radians. This is called the *polar form* of z. Observe that $r = |z|$. We say that θ is an *argument* of z.

Definition 3.6

Let $z \in \mathbb{C}$ be non-zero. If $z = r(\cos\theta + i\sin\theta)$ where $0 \leq \theta < 2\pi$, then we say that θ is the *principal argument* of z, and write $\theta = \mathrm{Arg}(z)$.

Example 3.7 (See board)

Quiz: What is the domain of the function Arg?

Arg is a function with domain $\{z \in \mathbb{C} : z \neq 0\}$ and codomain $\{\theta \in \mathbb{R} : -\pi < \theta \leq \pi\}$.

Polar Form and Arguments

Any complex number z can be written in the form

$$z = r(\cos\theta + i\sin\theta)$$

where $r \in \mathbb{R}_{\geq 0}$ and θ is an angle, measured in radians. This is called the *polar form* of z. Observe that $r = |z|$. We say that θ is an *argument* of z.

Definition 3.6

Let $z \in \mathbb{C}$ be non-zero. If $z = r(\cos\theta + i\sin\theta)$ where $0 \leq \theta < 2\pi$, then we say that θ is the *principal argument* of z, and write $\theta = \mathrm{Arg}(z)$.

Example 3.7 (See board)

Quiz: What is the domain of the function Arg?

Arg is a function with domain $\{z \in \mathbb{C} : z \neq 0\}$ and codomain $\{\theta \in \mathbb{R} : -\pi < \theta \leq \pi\}$. Is it injective? Is it surjective?

Administration and Coulter McDowell Lecture

- Please take Problem Sheet 4
- Please take the rest of the Part A handout

Dr Vicky Neale (Cambridge) on

'**7 Things you really need to know about prime numbers!**'

Time: Wednesday 22nd October, 5.30pm (tea/cakes) for 6.15pm

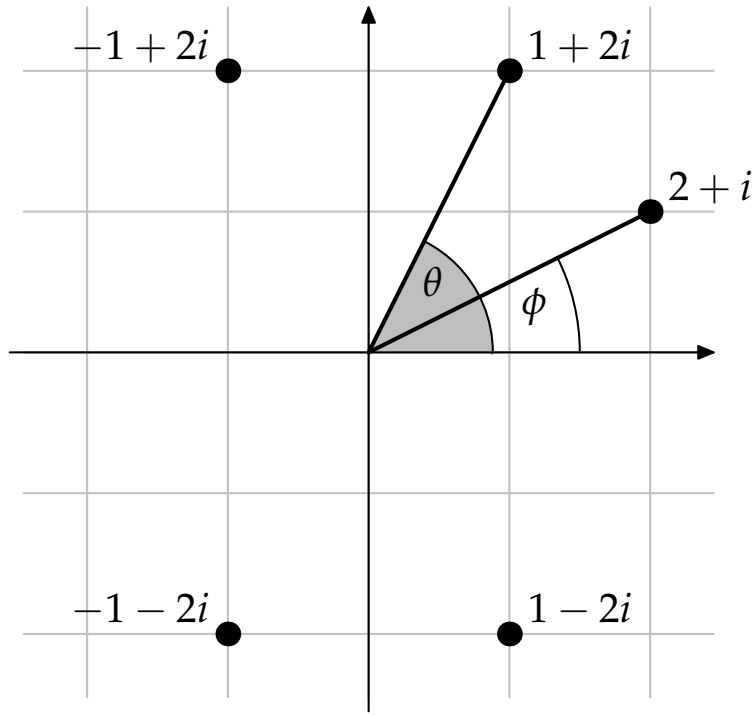
Place: Windsor Building

Abstract: Prime numbers are fundamentally important in mathematics. Join Dr Vicky Neale to discover some of the beautiful properties of prime numbers, and learn about some of the unsolved problems that mathematicians are working on today.

Principal Arguments

Example 3.7

We will find the principal arguments of the complex numbers shown on the Argand diagram below in terms of the angles θ and ϕ.



There is an often misapplied 'rule' that $\text{Arg}(a+bi) = \tan^{-1}(b/a)$.
This only works when $a > 0$ and $b > 0$.

Multiplication (and Division) in Polar Form

Example 3.8 (See board)

Example 3.9

Let $z = r(\cos\theta + i\sin\theta)$ and $w = s(\cos\phi + i\sin\phi)$ be complex numbers in polar form. Using the formulae

$$\cos(\theta + \phi) = \cos\theta\cos\phi - \sin\theta\sin\phi$$
$$\sin(\theta + \phi) = \cos\theta\sin\phi + \sin\theta\cos\phi$$

it follows that

$$zw = rs\big(\cos(\theta + \phi) + i\sin(\theta + \phi)\big).$$

In short: to multiply numbers in polar form, multiply the moduli and add the arguments.

Exercise 3.10

Let z and w be as in Example 3.10 and suppose that $w \neq 0$. Express z/w in polar form.

De Moivre's Theorem

If $\theta \in \mathbb{R}$ and $n \in \mathbb{N}$ then

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta.$$

De Moivre's Theorem can be proved using mathematical induction and Example 3.9. We will shortly see a quicker proof, using the exponential function.

Example 3.11

The $n = 3$ case of De Moivre's Theorem implies that

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

De Moivre's Theorem

If $\theta \in \mathbb{R}$ and $n \in \mathbb{N}$ then

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta.$$

De Moivre's Theorem can be proved using mathematical induction and Example 3.9. We will shortly see a quicker proof, using the exponential function.

Example 3.11

The $n = 3$ case of De Moivre's Theorem implies that

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

So we proved an identity about the **real** cosine function, $\cos : \mathbb{R} \to \mathbb{R}$ using **complex** numbers.

> *Il apparut que, entre deux vérités du domaine réel, le chemin le plus facile et le plus court passe bien souvent par le domaine complexe*
>
> Paul Painlevé (1900)

De Moivre's Theorem

If $\theta \in \mathbb{R}$ and $n \in \mathbb{N}$ then

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta.$$

De Moivre's Theorem can be proved using mathematical induction and Example 3.9. We will shortly see a quicker proof, using the exponential function.

Example 3.11

The $n = 3$ case of De Moivre's Theorem implies that

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

So we proved an identity about the **real** cosine function, $\cos : \mathbb{R} \to \mathbb{R}$ using **complex** numbers.

> *It came to appear that, between two truths of the real domain, the easiest and shortest path quite often passes through the complex domain.*
>
> Paul Painlevé (1900)

A Cubic Equation

Example 3.12

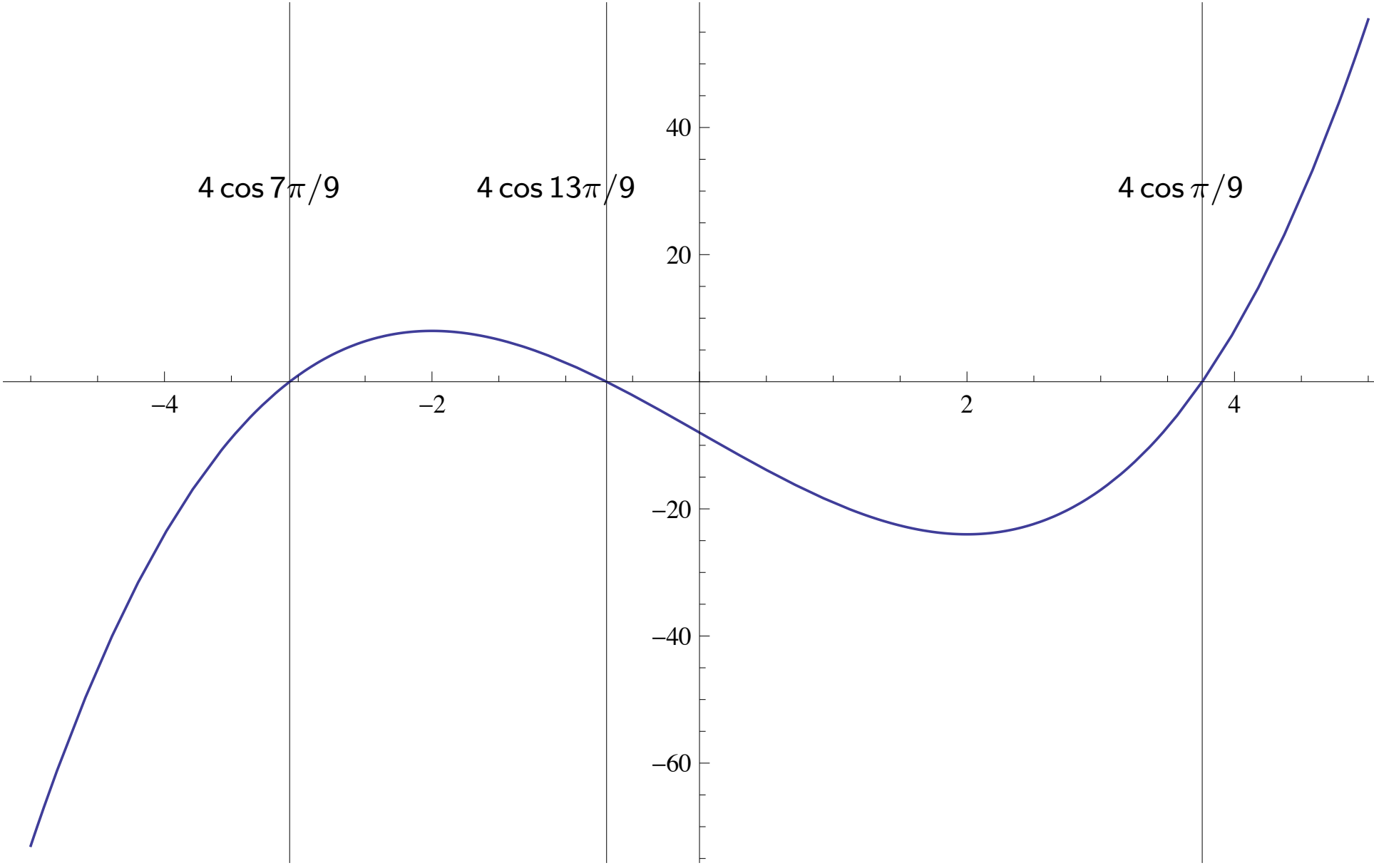
Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^3 - 12x - 8$. Substitute $x = 4\cos\theta$. Then

$$\begin{aligned} f(x) = 0 &\iff 64\cos^3\theta - 48\cos\theta - 8 = 0 \\ &\iff 16(4\cos^3\theta - 3\cos\theta) = 8 \\ &\iff 16\cos 3\theta = 8 \\ &\iff \cos 3\theta = 1/2. \end{aligned}$$

Exercise: [this got rushed in the lecture on Tuesday: I will do it carefully on Thursday] by drawing the graph for cos show that $\cos 3\theta = 1/2 \iff 3\theta = \pm\pi/3 + 2n\pi$ for some $n \in \mathbb{Z}$. Deduce that the roots of f are

$$4\cos\tfrac{\pi}{9}, \quad 4\cos\tfrac{7\pi}{9}, \quad 4\cos\tfrac{13\pi}{9}.$$

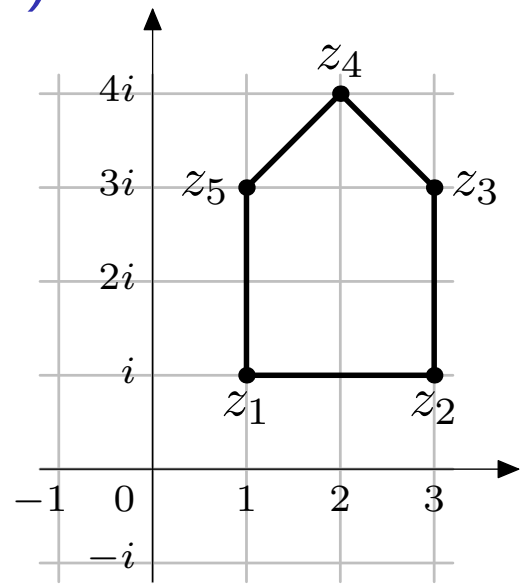
Graph of $f(x) = x^3 - 12x - 8$



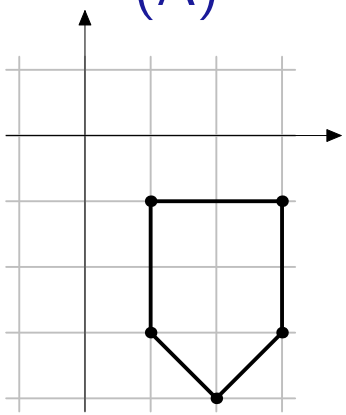
Quiz (relevant to Question 5 on Sheet 4)

The Argand diagram to the right shows $z_1, z_2, z_3, z_4, z_5 \in \mathbb{C}$.

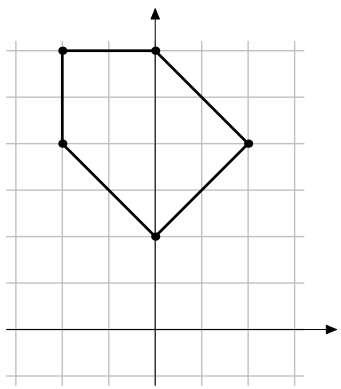
What is $|z_3 - z_1|$?



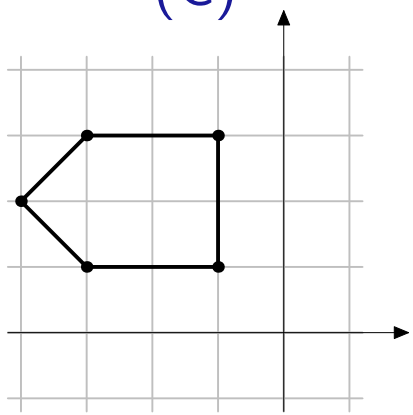
(A)



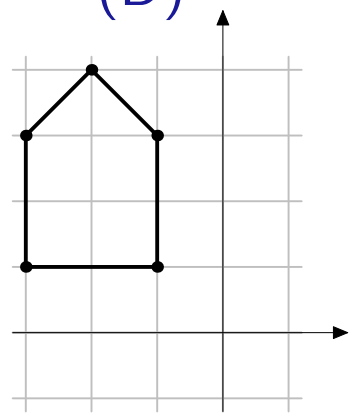
(B)



(C)



(D)



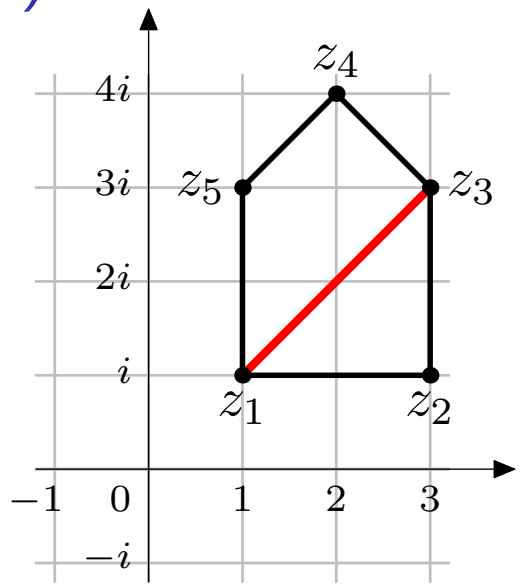
The diagrams above are drawn with the same scale.

Which diagram shows $iz_1, iz_2, iz_3, iz_4, iz_5$?

Which diagram shows $\overline{z_1}, \overline{z_2}, \overline{z_4}, \overline{z_4}, \overline{z_5}$?

Quiz (relevant to Question 5 on Sheet 4)

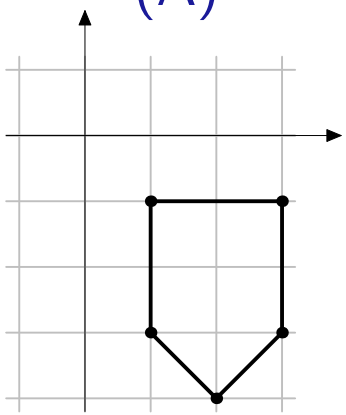
The Argand diagram to the right shows $z_1, z_2, z_3, z_4, z_5 \in \mathbb{C}$.



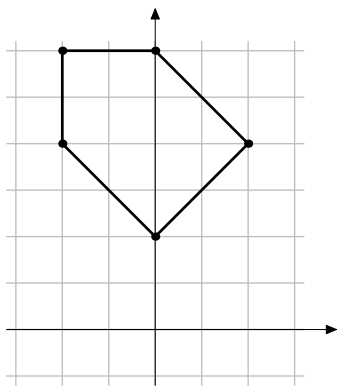
What is $|z_3 - z_1|$?

Answer: $|z_3 - z_1| = 2\sqrt{2}$. Geometrically, $|z_3 - z_1|$ is the length of the red line.

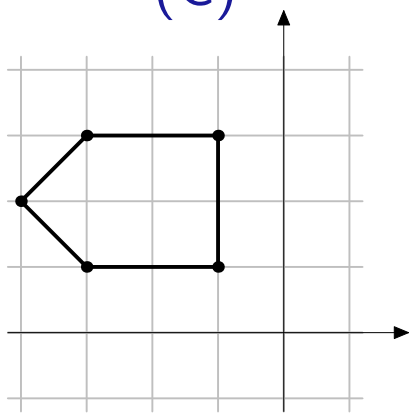
(A)



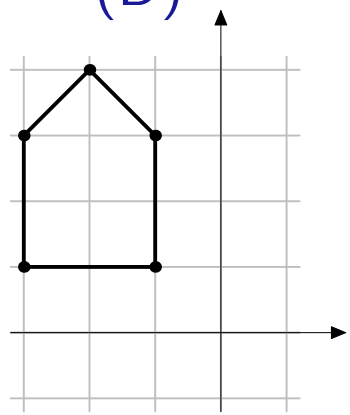
(B)



(C)



(D)



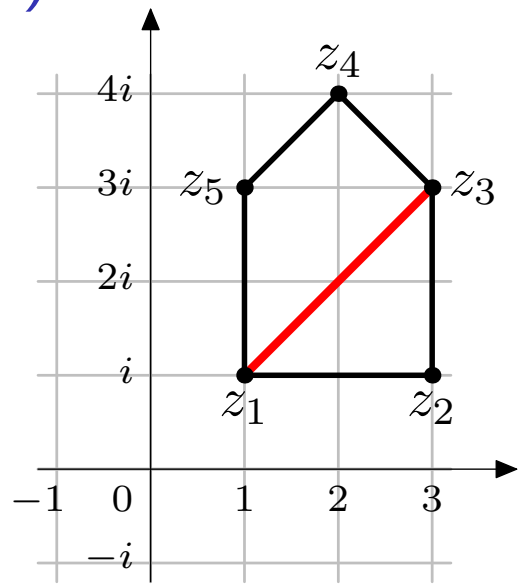
The diagrams above are drawn with the same scale.

Which diagram shows $iz_1, iz_2, iz_3, iz_4, iz_5$?

Which diagram shows $\overline{z_1}, \overline{z_2}, \overline{z_4}, \overline{z_4}, \overline{z_5}$?

Quiz (relevant to Question 5 on Sheet 4)

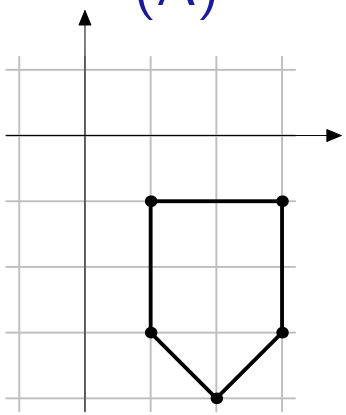
The Argand diagram to the right shows $z_1, z_2, z_3, z_4, z_5 \in \mathbb{C}$.



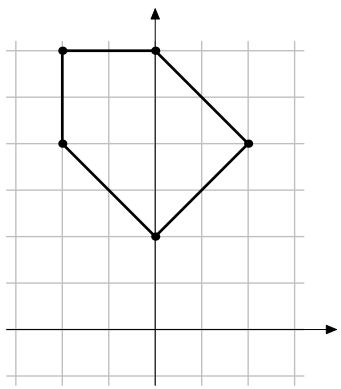
What is $|z_3 - z_1|$?

Answer: $|z_3 - z_1| = 2\sqrt{2}$. Geometrically, $|z_3 - z_1|$ is the length of the red line.

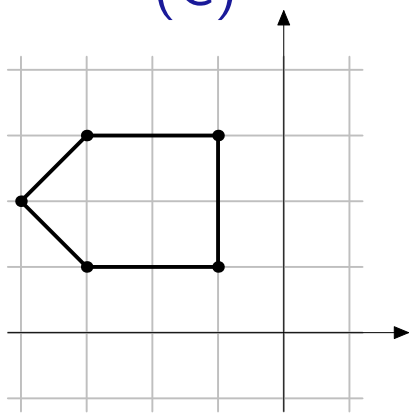
(A)



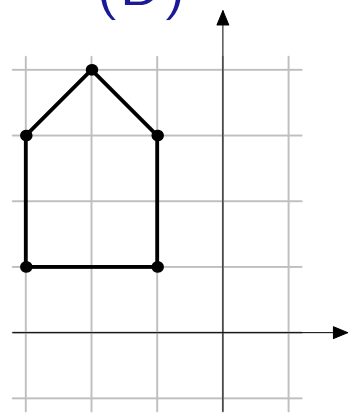
(B)



(C)



(D)



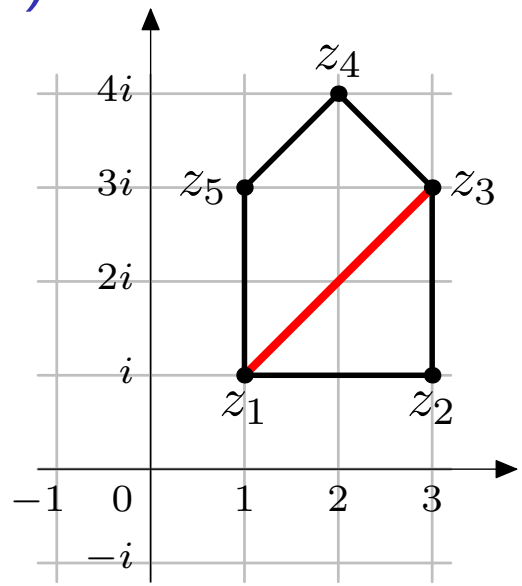
The diagrams above are drawn with the same scale.

Which diagram shows $iz_1, iz_2, iz_3, iz_4, iz_5$? Answer: (C)

Which diagram shows $\overline{z_1}, \overline{z_2}, \overline{z_4}, \overline{z_4}, \overline{z_5}$?

Quiz (relevant to Question 5 on Sheet 4)

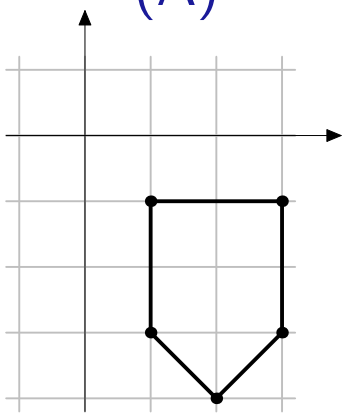
The Argand diagram to the right shows $z_1, z_2, z_3, z_4, z_5 \in \mathbb{C}$.



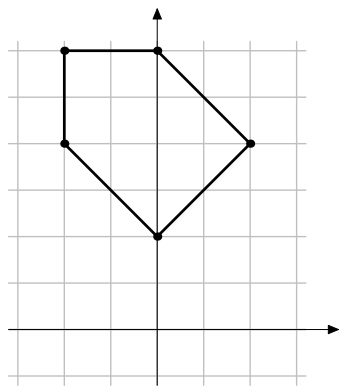
What is $|z_3 - z_1|$?

Answer: $|z_3 - z_1| = 2\sqrt{2}$. Geometrically, $|z_3 - z_1|$ is the length of the red line.

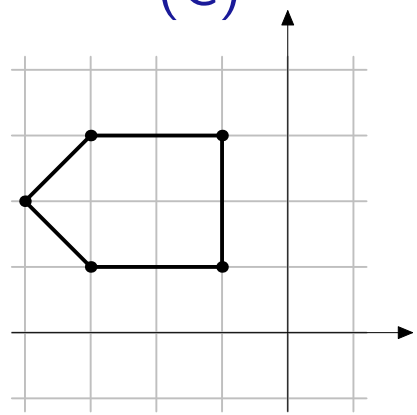
(A)



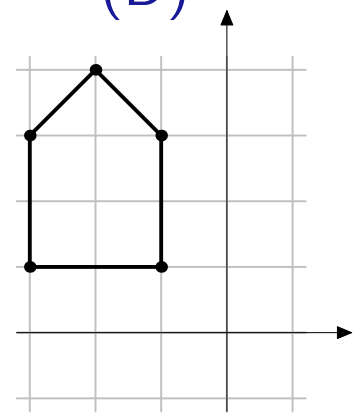
(B)



(C)



(D)

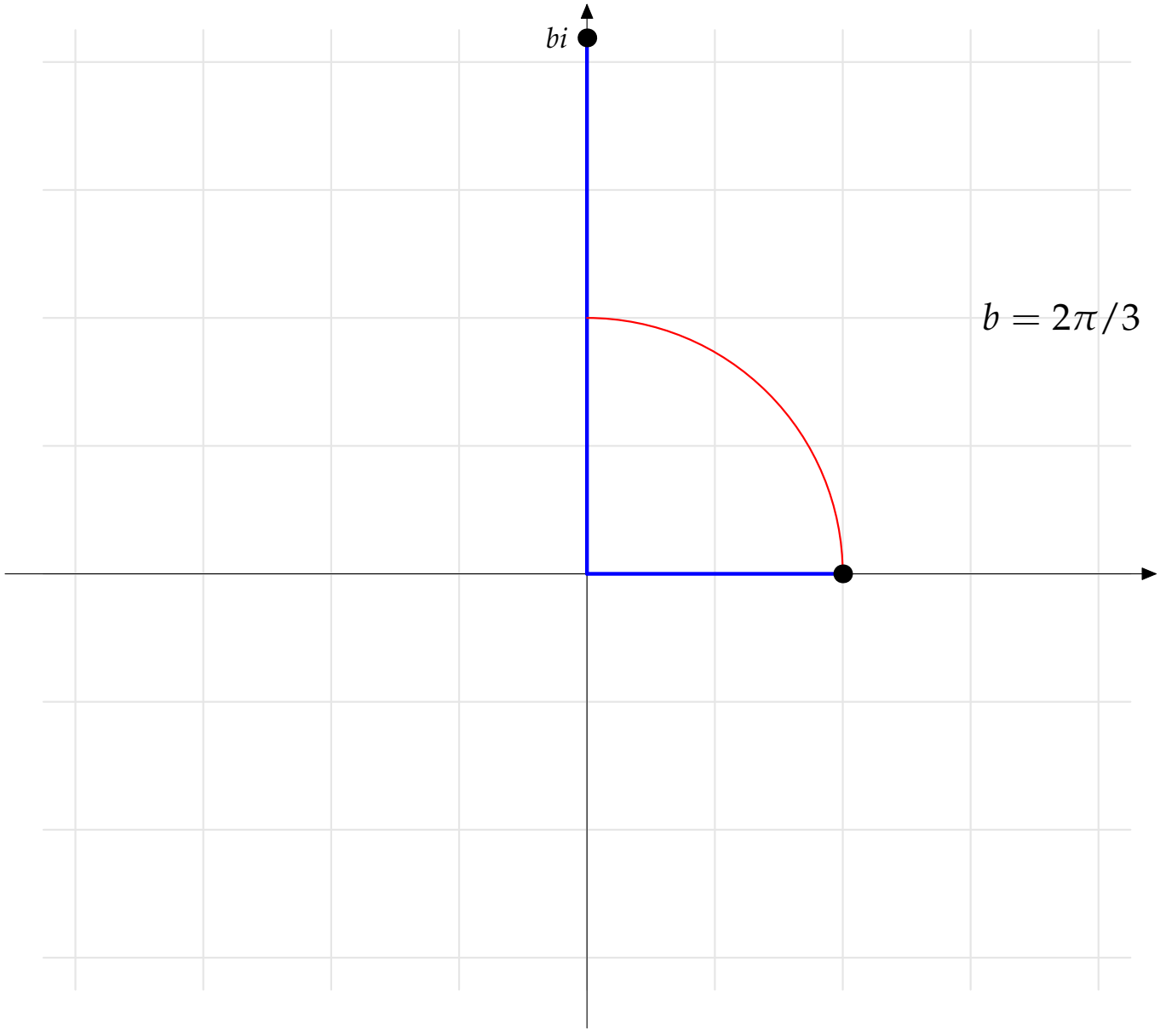


The diagrams above are drawn with the same scale.

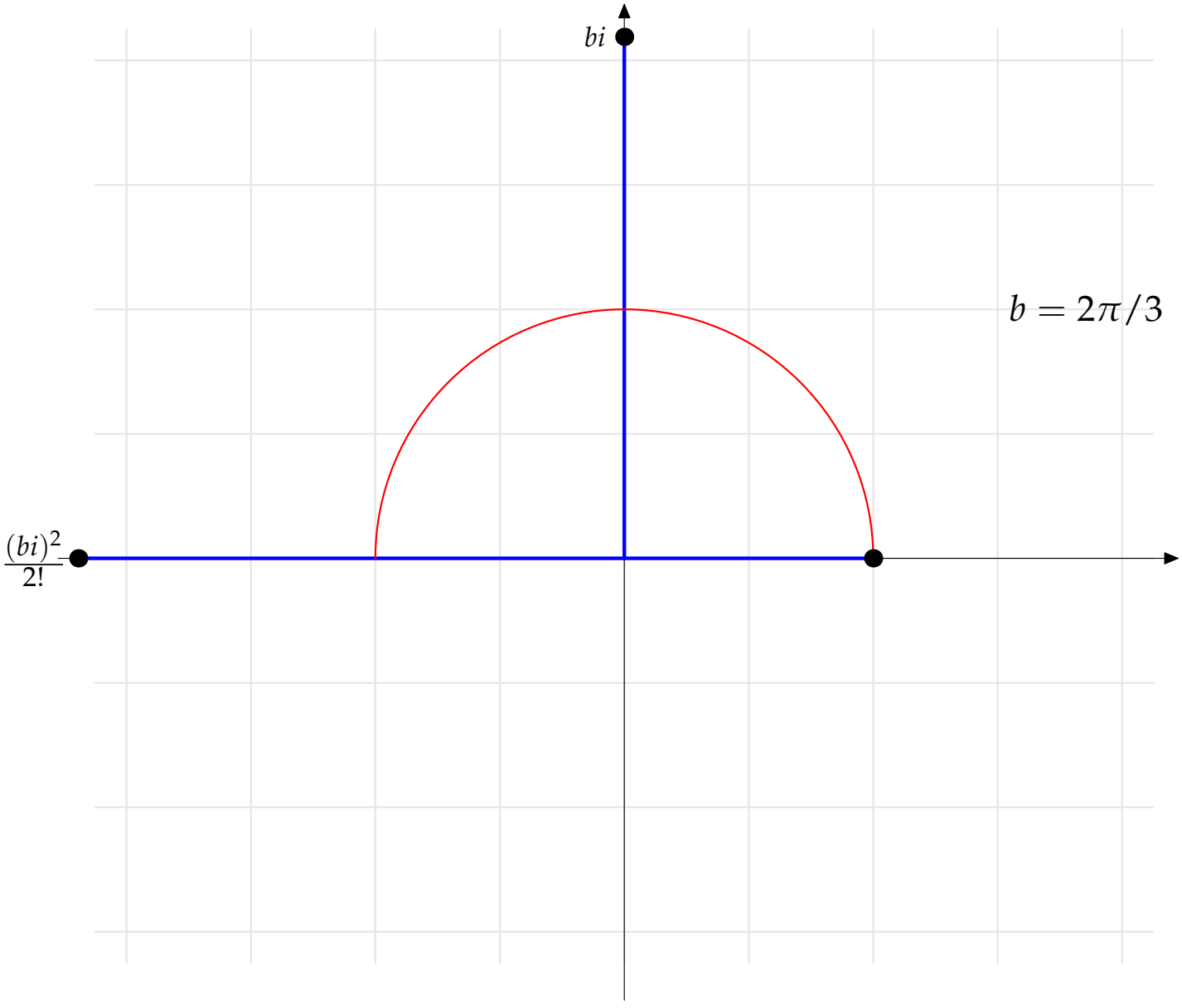
Which diagram shows $iz_1, iz_2, iz_3, iz_4, iz_5$? Answer: (C)

Which diagram shows $\overline{z_1}, \overline{z_2}, \overline{z_4}, \overline{z_4}, \overline{z_5}$? Answer: (A)

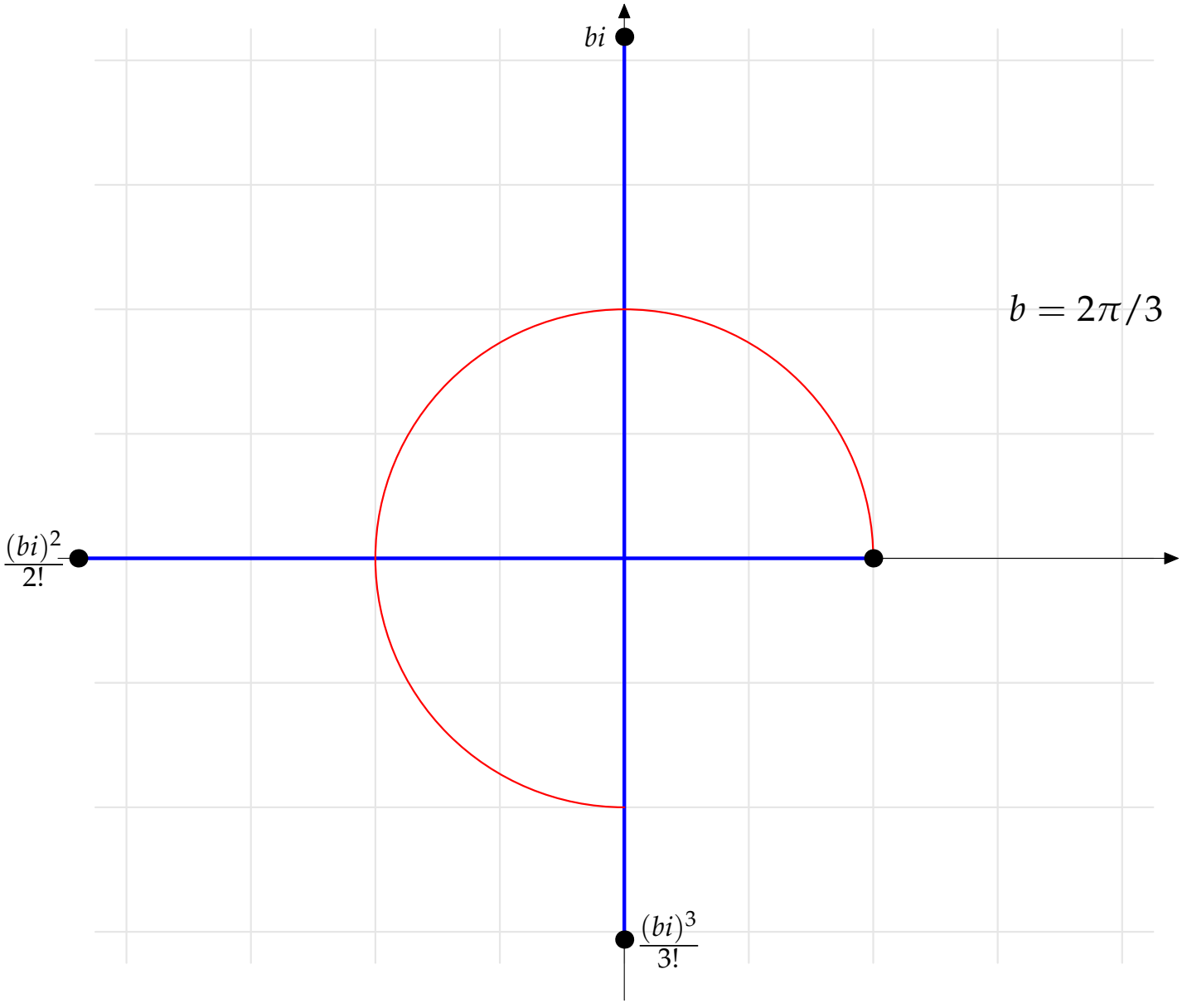
Summands in the Infinite Sum for $e^{2\pi i/3}$



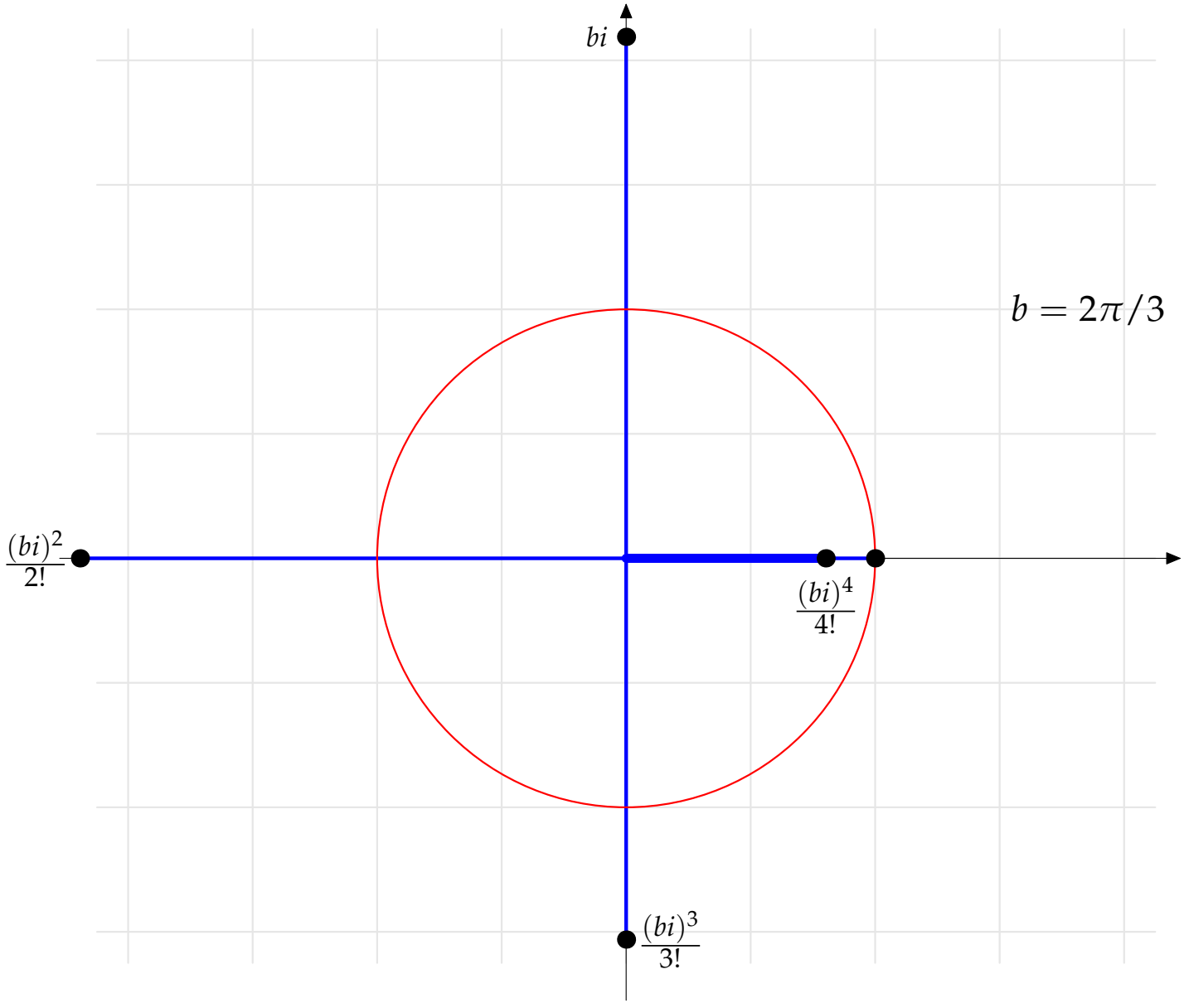
Summands in the Infinite Sum for $e^{2\pi i/3}$



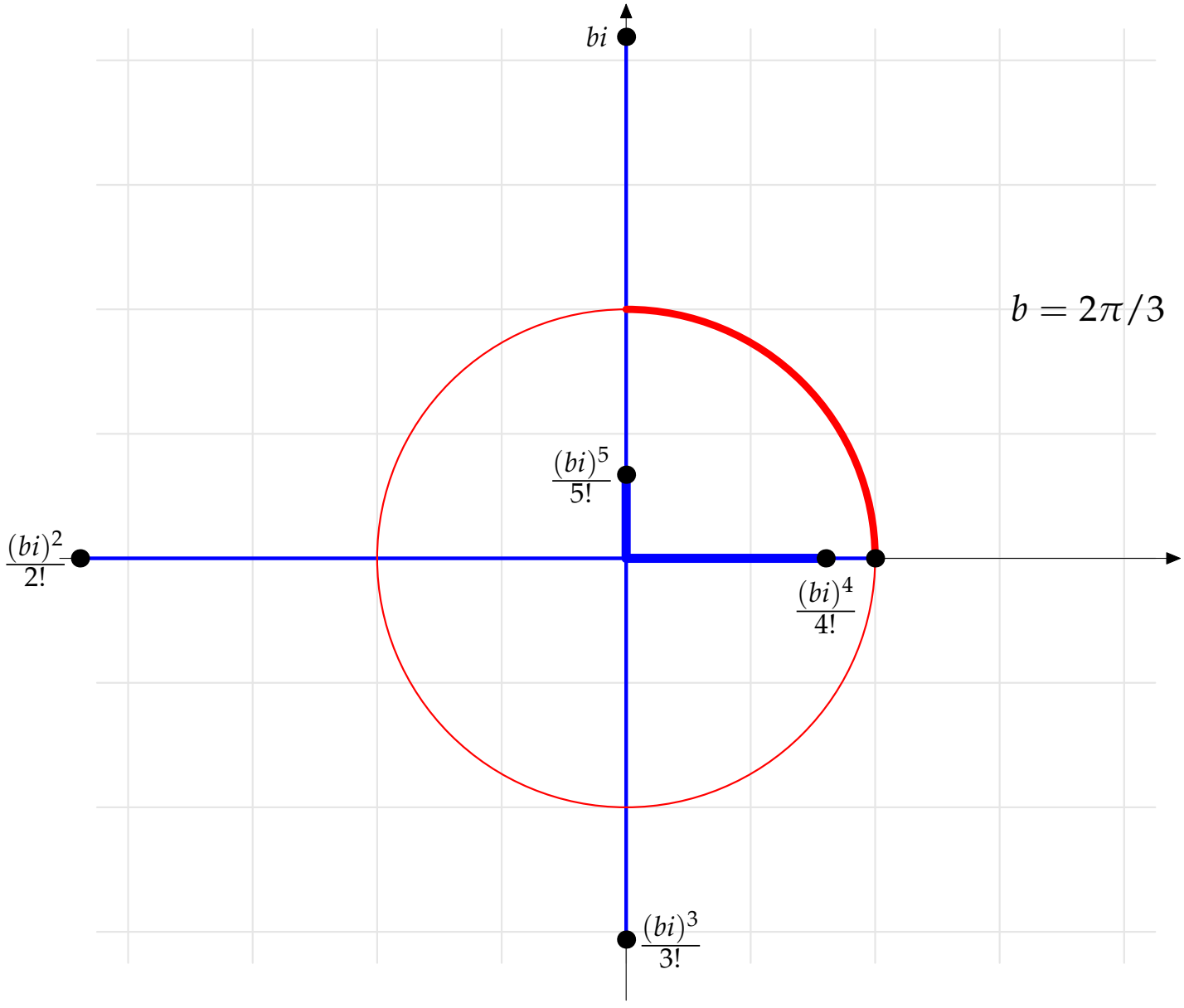
Summands in the Infinite Sum for $e^{2\pi i/3}$



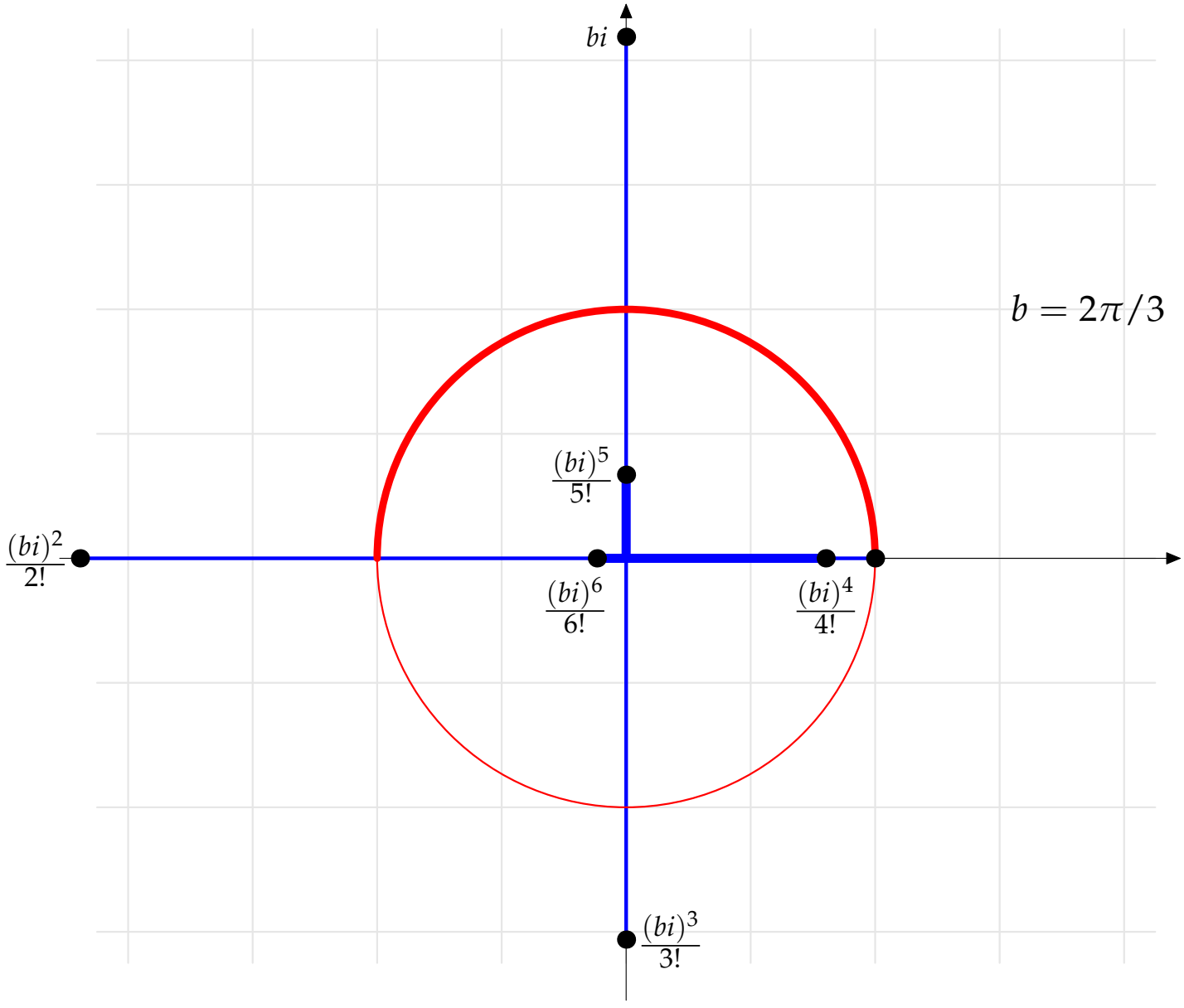
Summands in the Infinite Sum for $e^{2\pi i/3}$



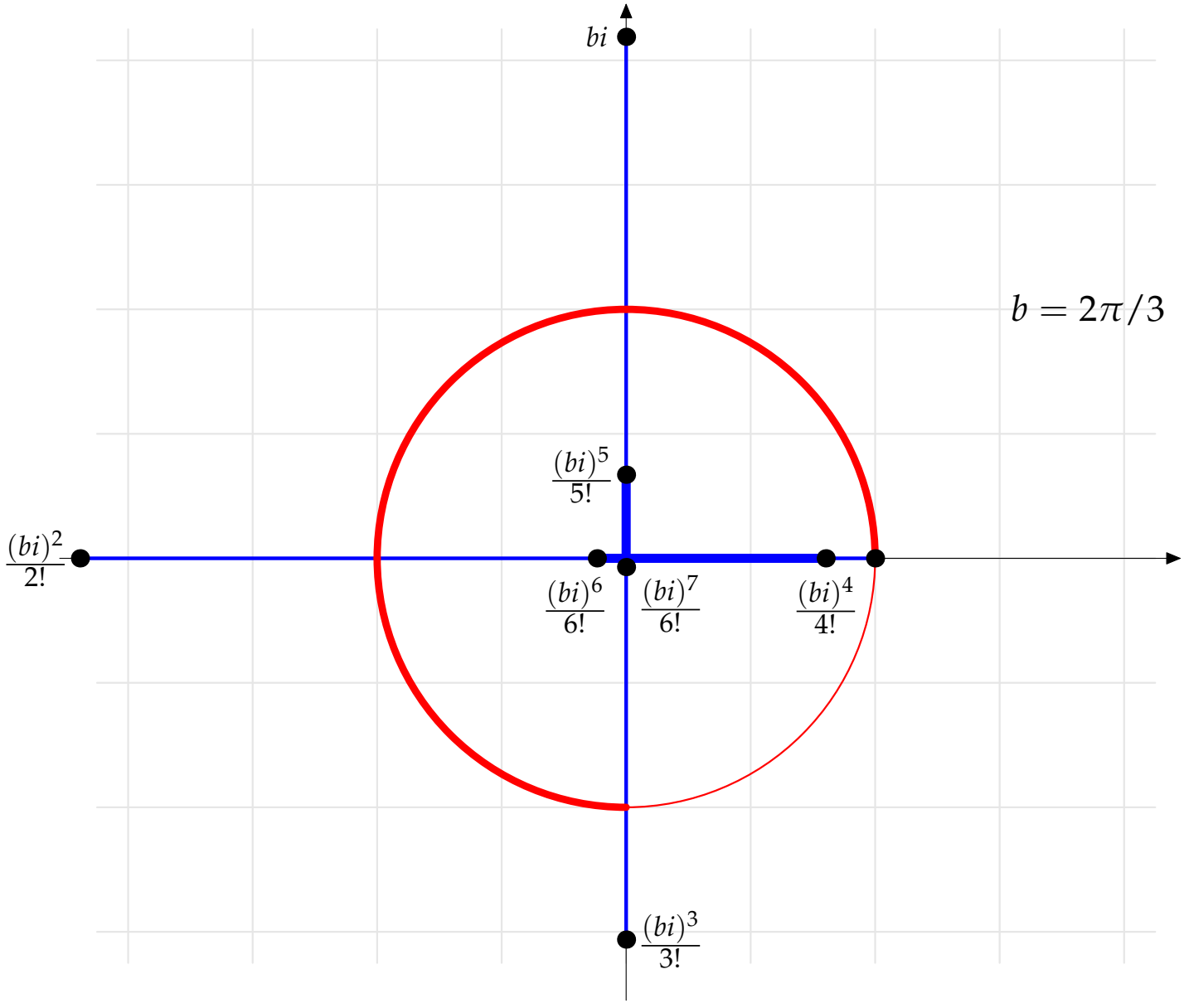
Summands in the Infinite Sum for $e^{2\pi i/3}$



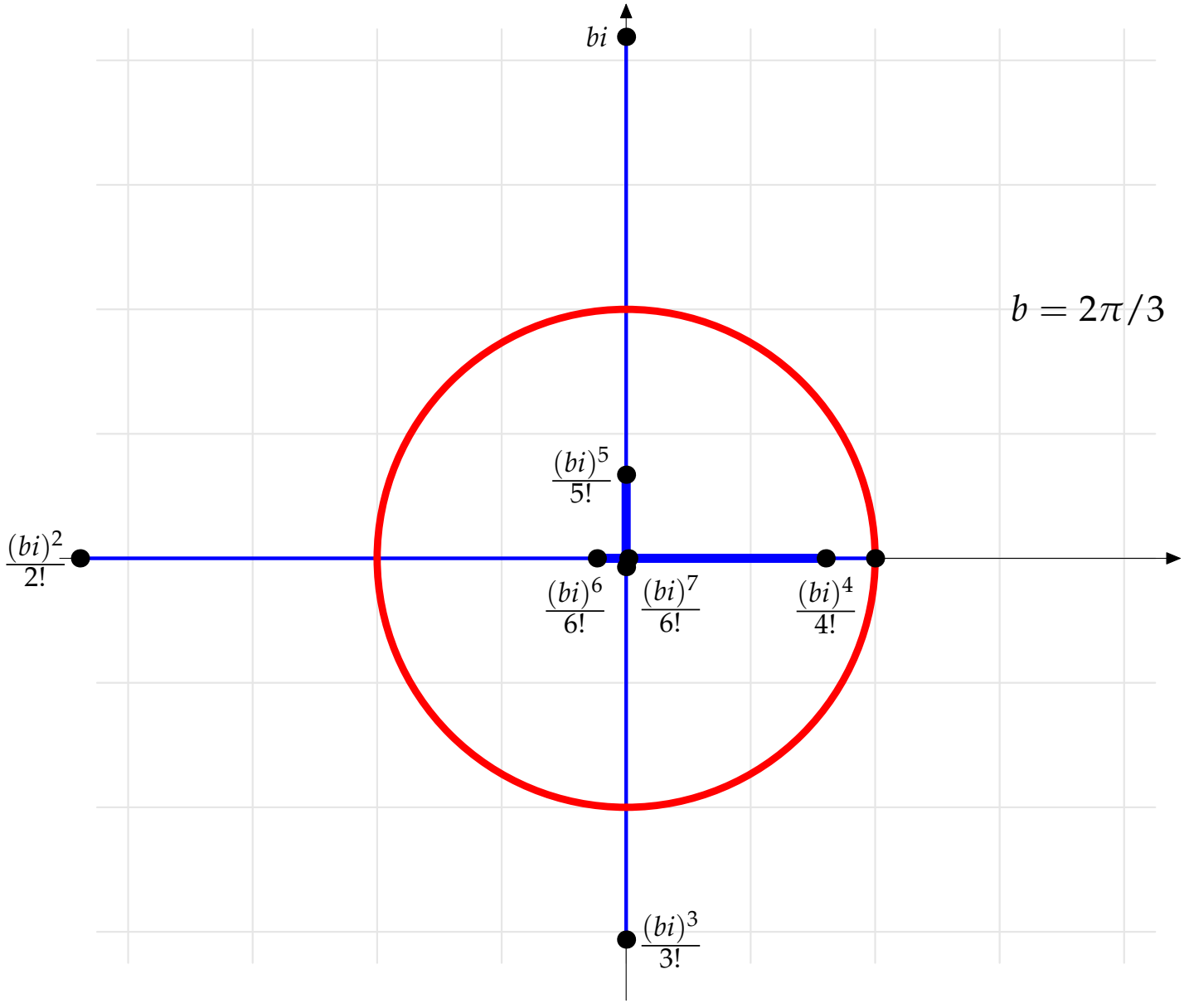
Summands in the Infinite Sum for $e^{2\pi i/3}$



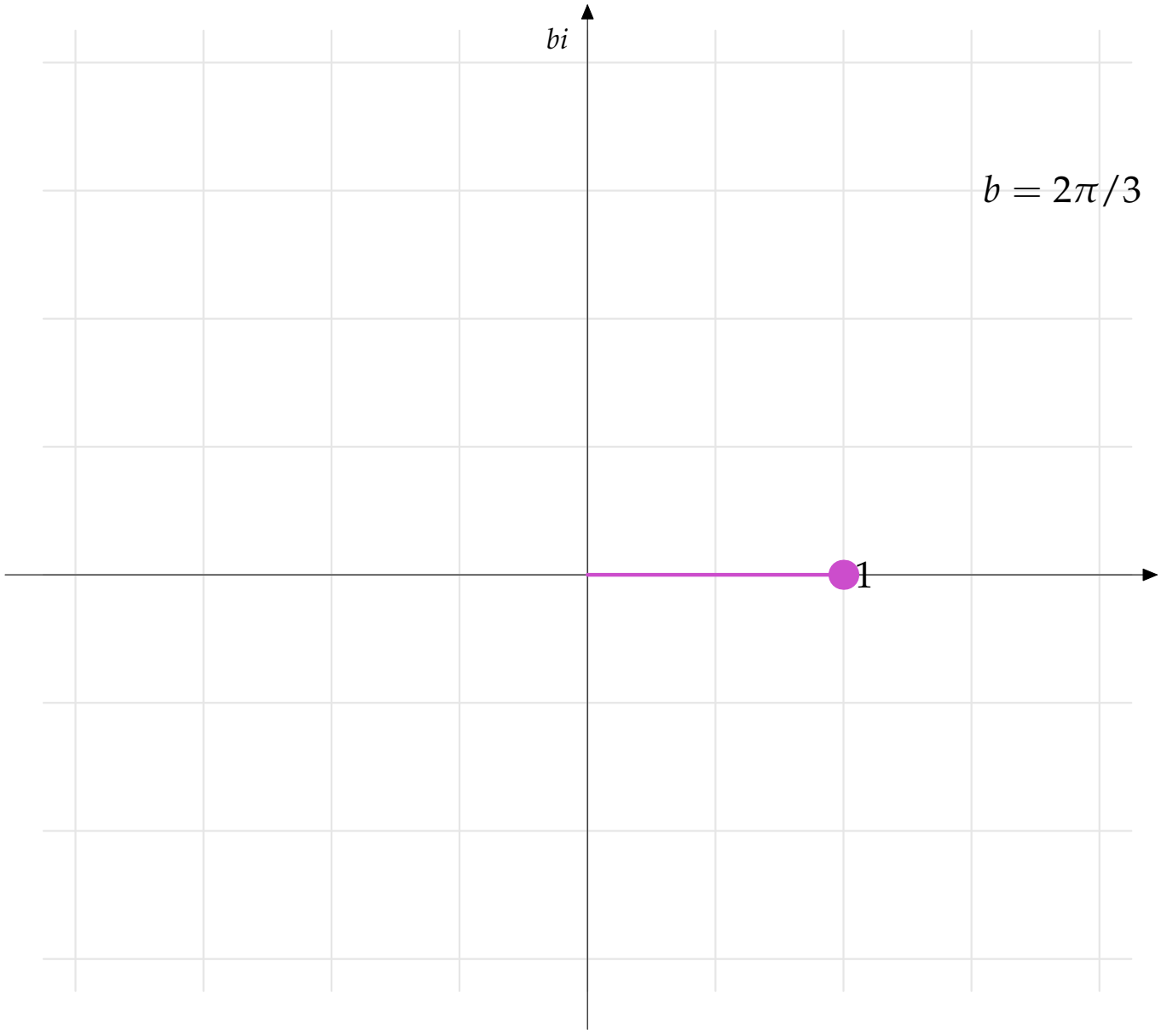
Summands in the Infinite Sum for $e^{2\pi i/3}$



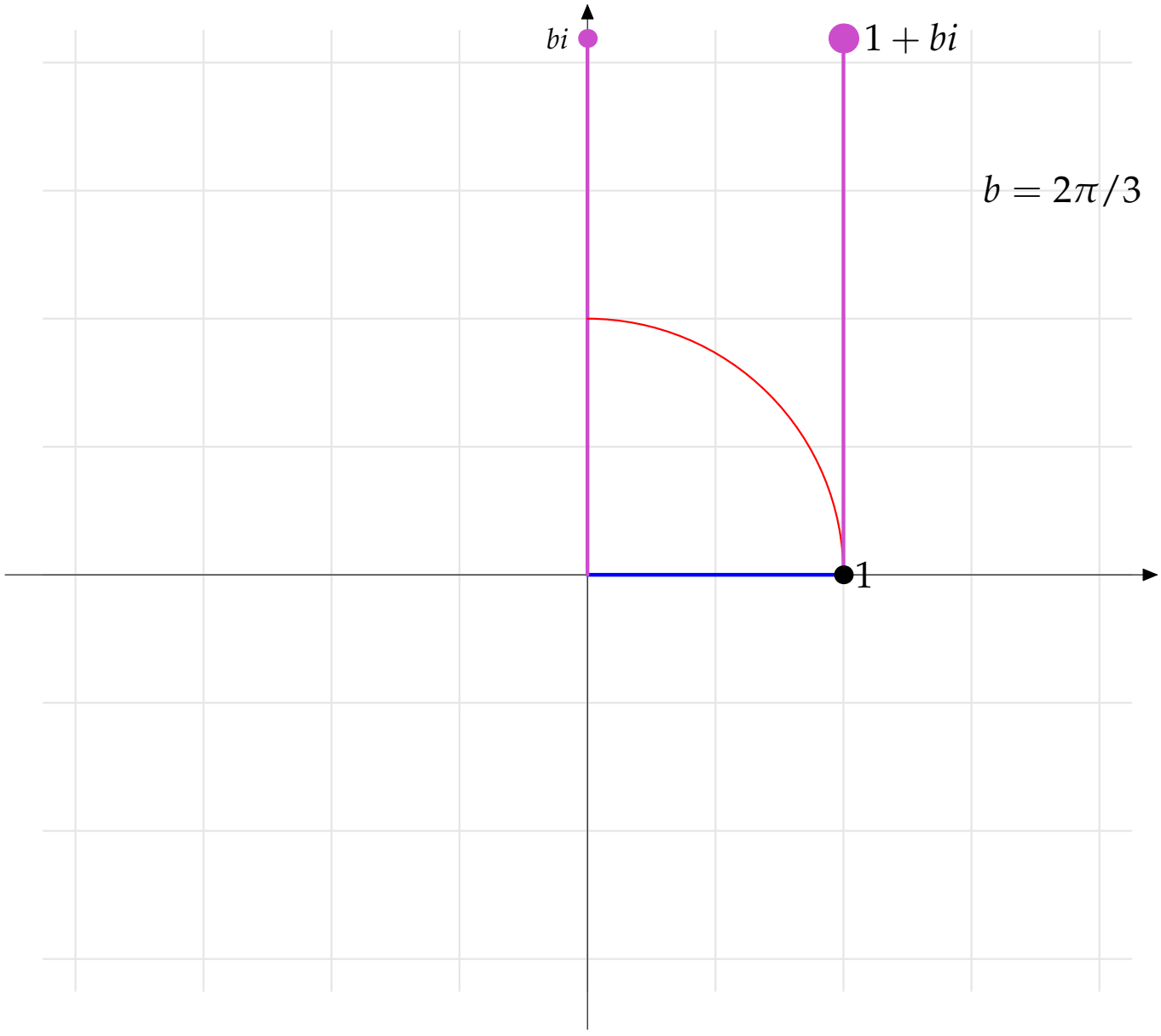
Summands in the Infinite Sum for $e^{2\pi i/3}$



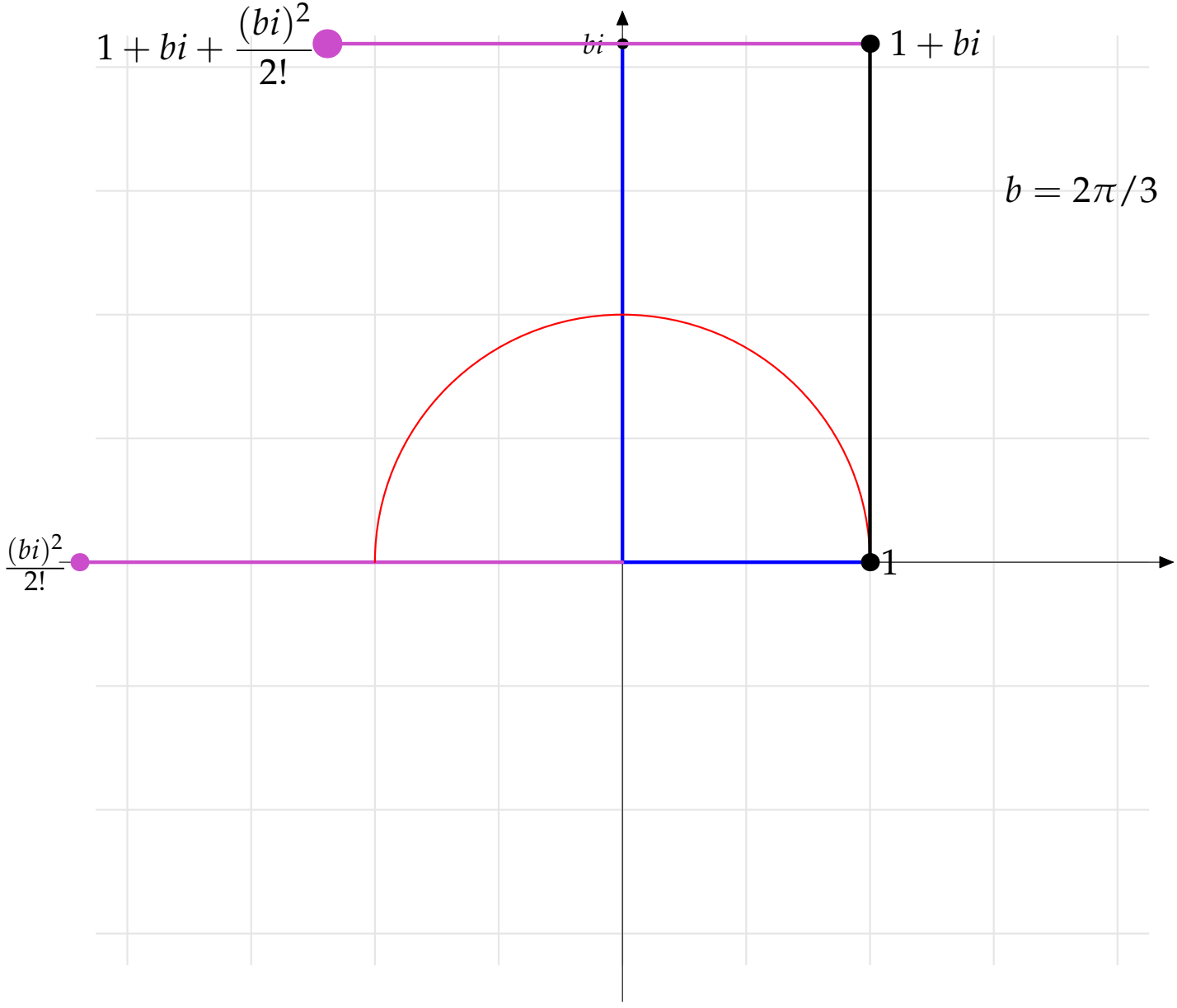
Infinite Sum for $e^{2\pi i/3}$



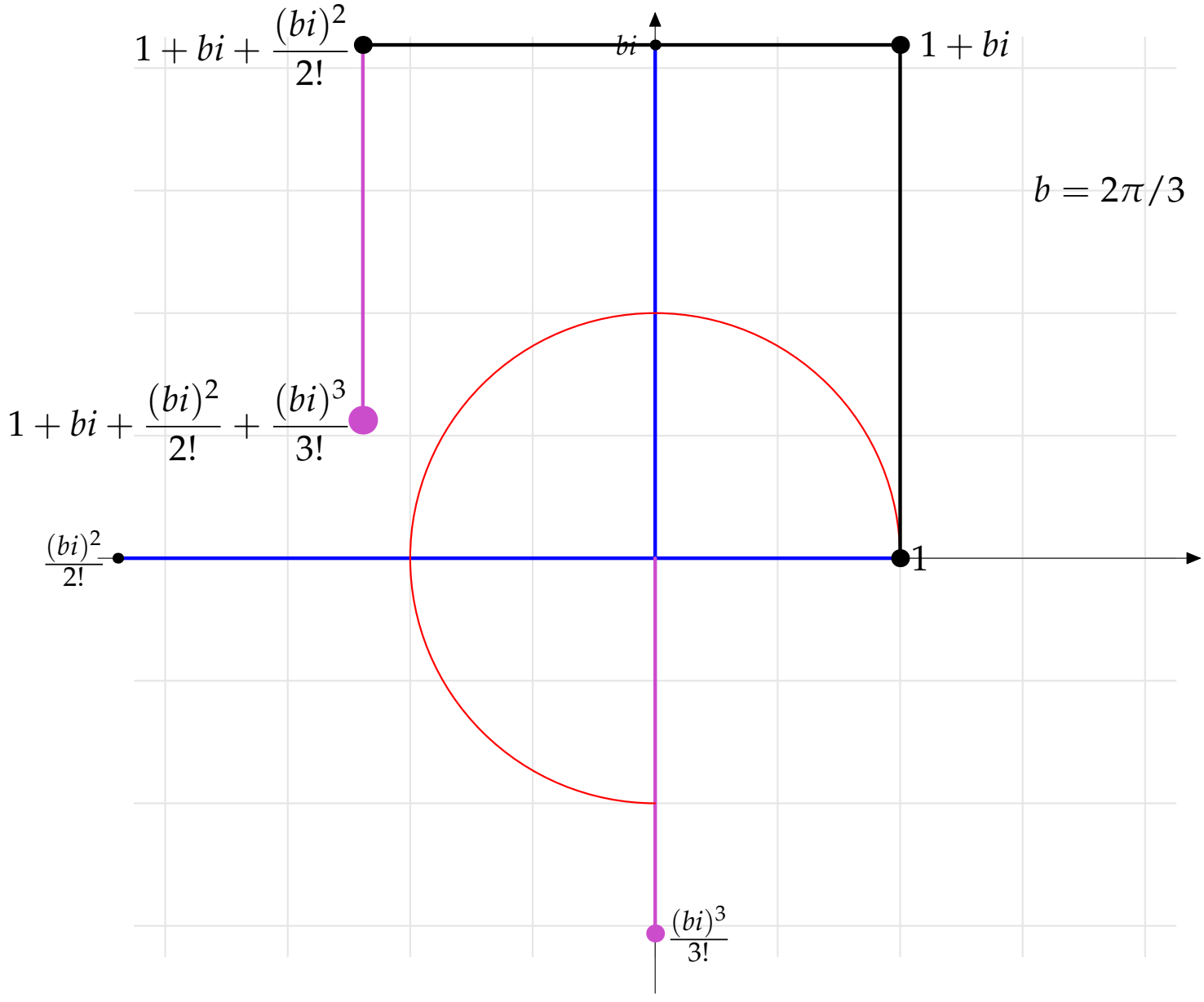
Infinite Sum for $e^{2\pi i/3}$



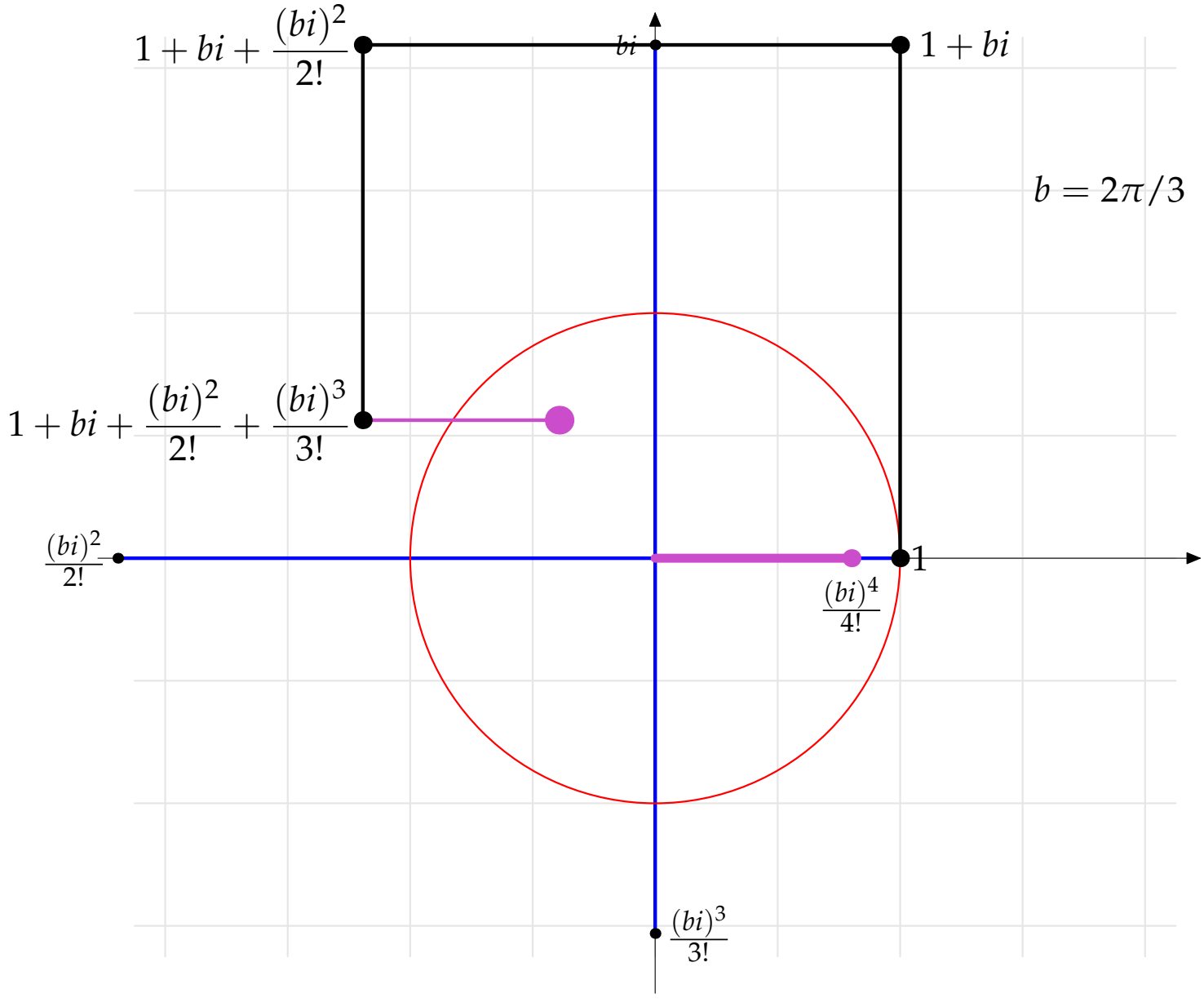
Infinite Sum for $e^{2\pi i/3}$



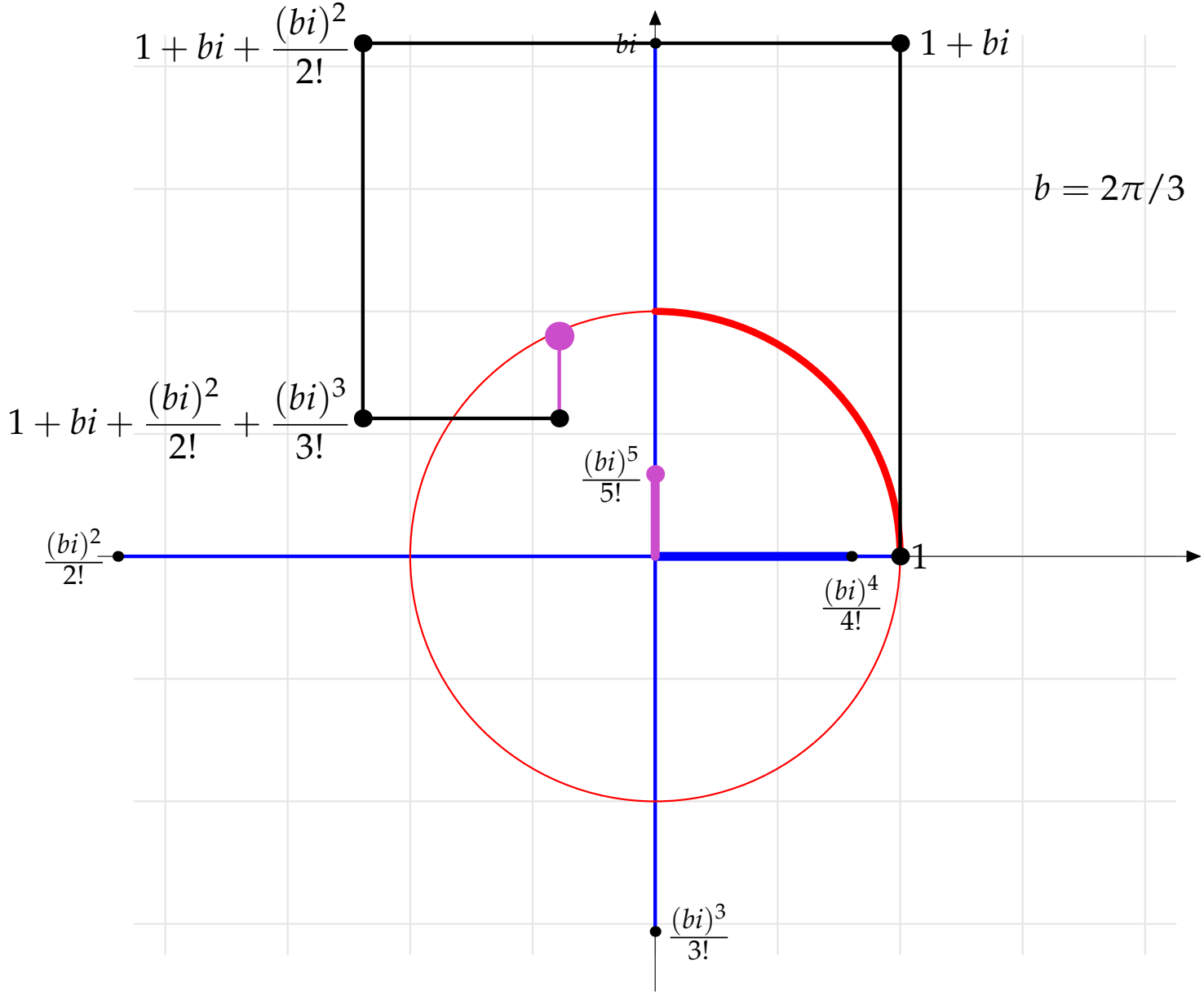
Infinite Sum for $e^{2\pi i/3}$



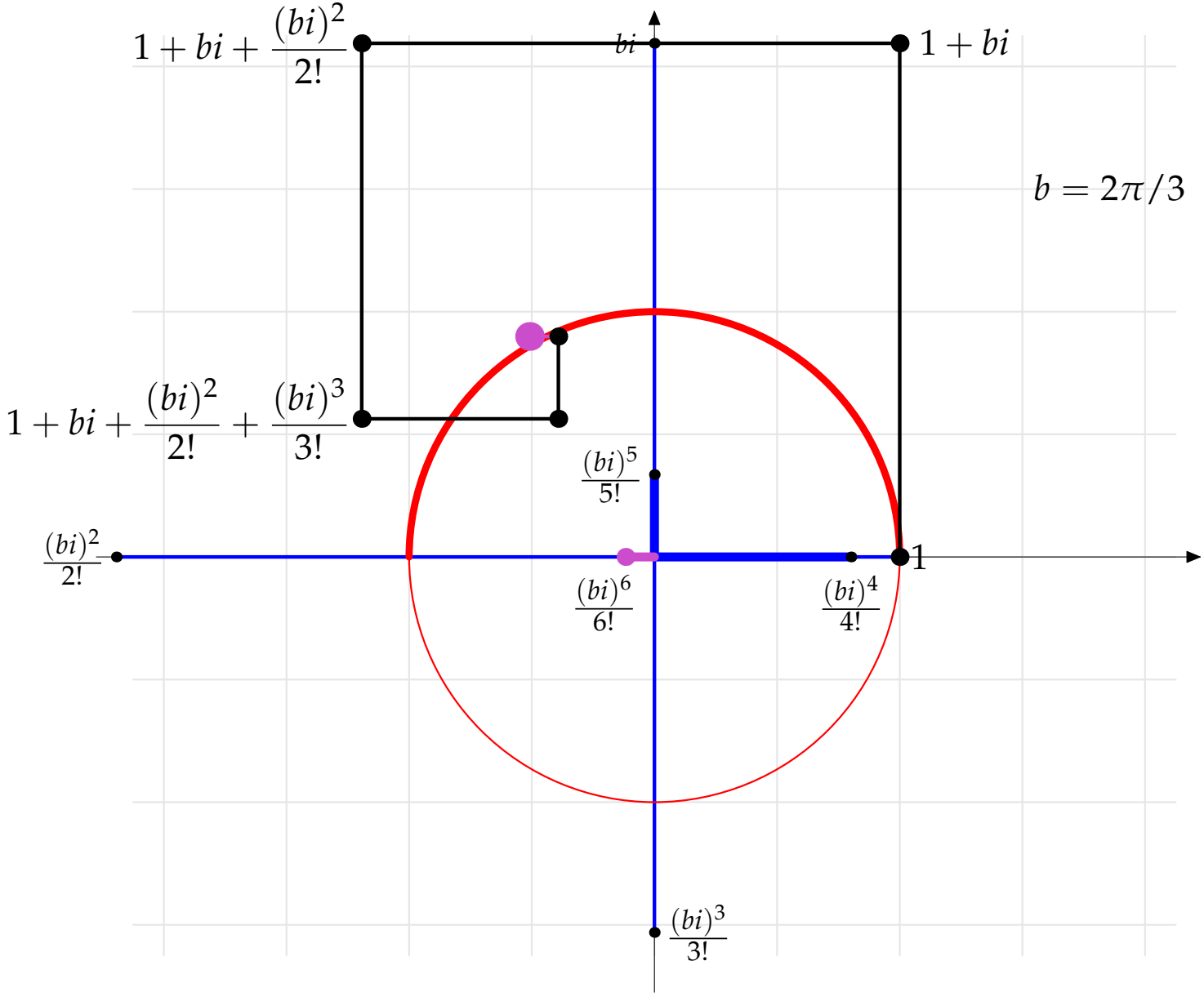
Infinite Sum for $e^{2\pi i/3}$



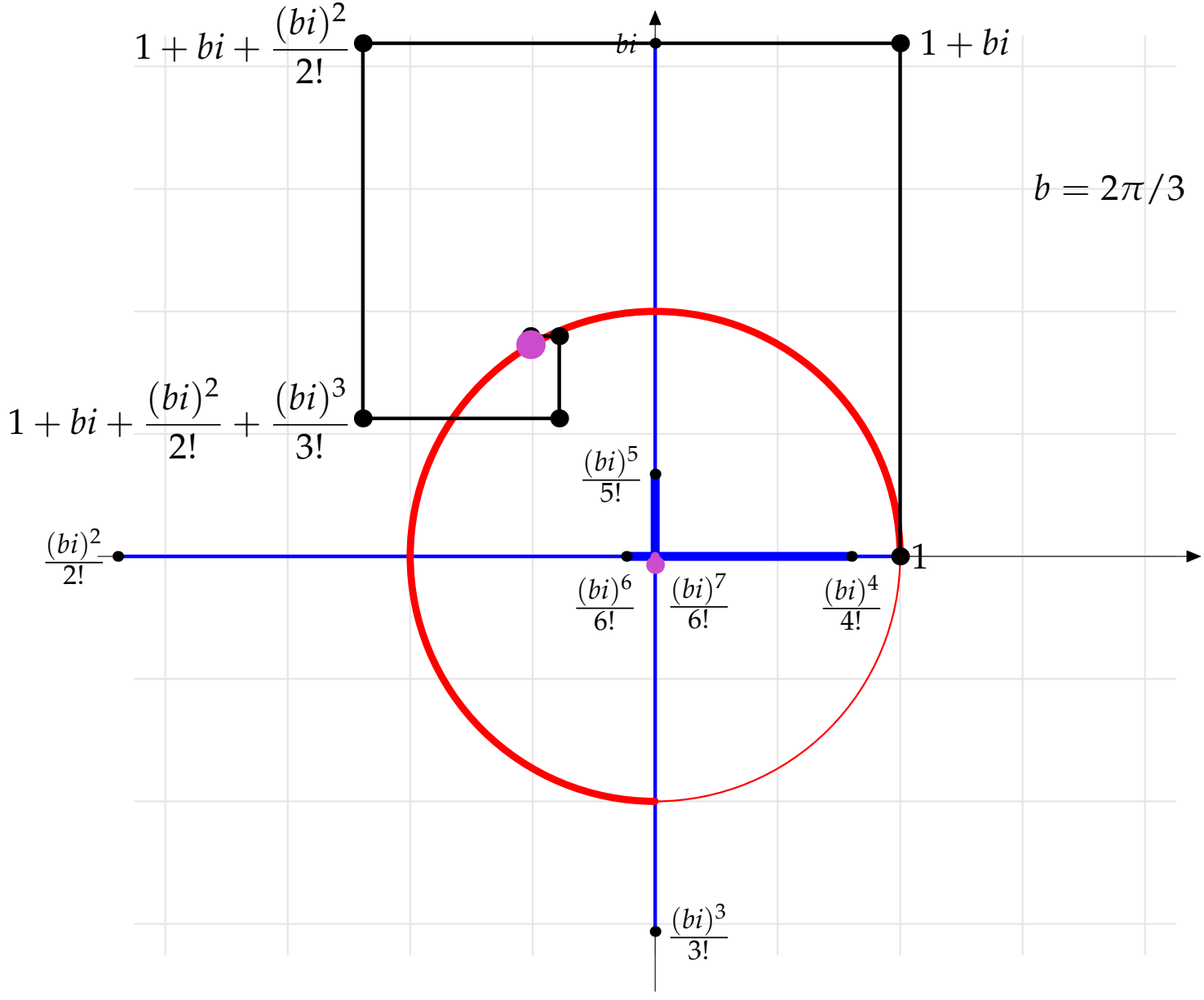
Infinite Sum for $e^{2\pi i/3}$



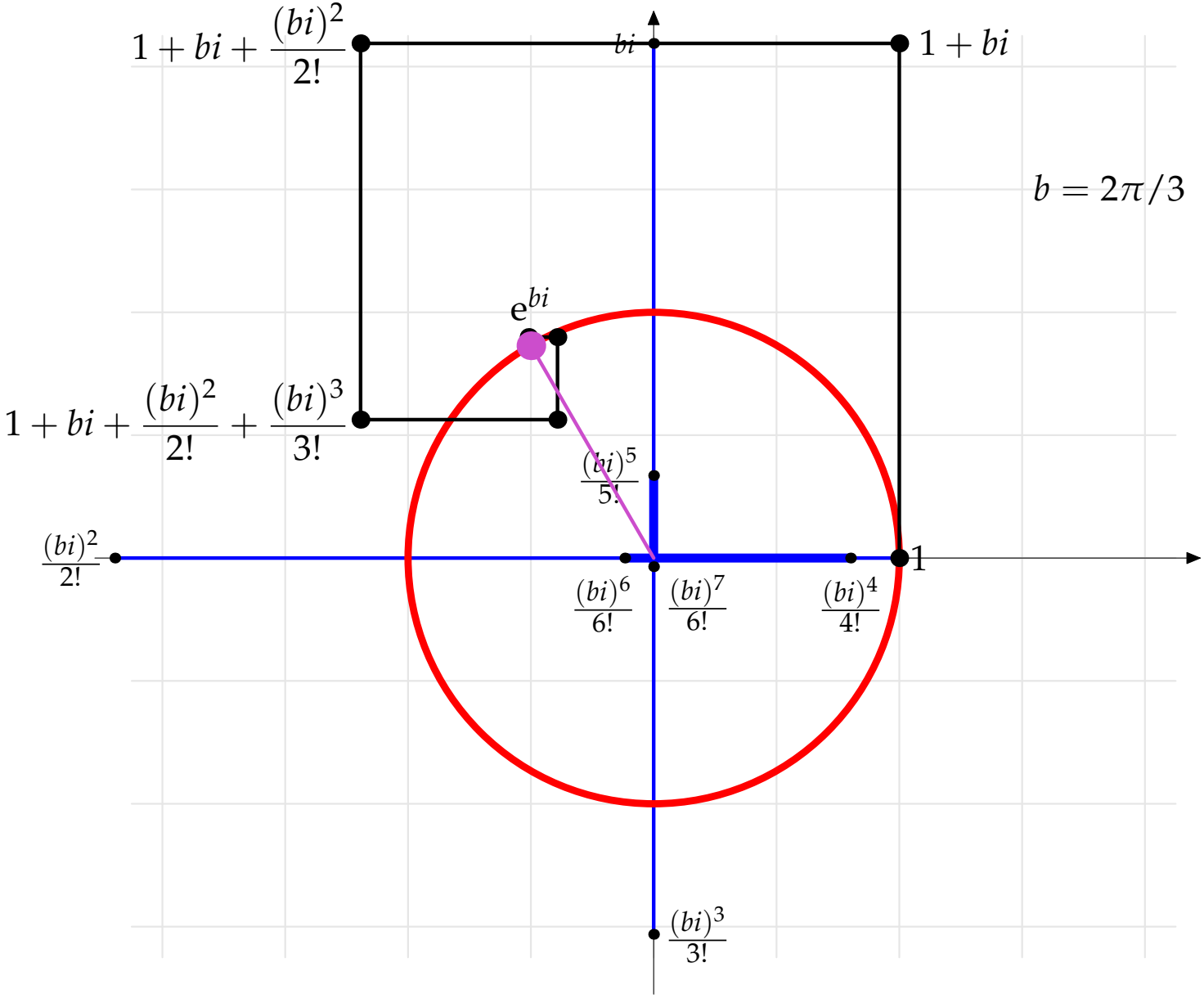
Infinite Sum for $e^{2\pi i/3}$



Infinite Sum for $e^{2\pi i/3}$



Infinite Sum for $e^{2\pi i/3}$



Complex Exponential Function

Definition 3.13

Let $z = a + bi \in \mathbb{C}$ be a complex number in Cartesian form. We define the *complex exponential function* $\exp : \mathbb{C} \to \mathbb{C}$ by

$$\exp(z) = \mathrm{e}^a(\cos b + i \sin b).$$

It is fine to write e^z for $\exp(z)$.

Complex Exponential Function

Definition 3.13

Let $z = a + bi \in \mathbb{C}$ be a complex number in Cartesian form. We define the *complex exponential function* $\exp : \mathbb{C} \to \mathbb{C}$ by

$$\exp(z) = \mathrm{e}^a(\cos b + i \sin b).$$

It is fine to write e^z for $\exp(z)$.

Exercise 3.14

Show that $\exp(z + w) = \exp z \exp w$ for all complex numbers z and w. [*Hint:* write $z = a + bi$, $w = c + di$ and use Example 3.9.]

A complex number written as $r\mathrm{e}^{i\theta}$ where $r \in \mathbb{R}_{\geq 0}$ and $\theta \in \mathbb{R}$ is said to be in *exponential form*. It is easy to convert between polar and exponential form:

$$z = r(\cos\theta + i \sin\theta) \iff z = r\mathrm{e}^{i\theta}.$$

Examples of the Complex Exponential Function

Example 3.15

(1) Put $z = i\pi$ in the complex exponential function. We get $\mathrm{e}^{i\pi} = -1$, or equivalently,

$$\mathrm{e}^{i\pi} + 1 = 0.$$

This is *Euler's Identity*. It relates five fundamental mathematical constants: 0, 1, e, π and i.

Examples of the Complex Exponential Function

Example 3.15

(1) Put $z = i\pi$ in the complex exponential function. We get $\mathrm{e}^{i\pi} = -1$, or equivalently,

$$\mathrm{e}^{i\pi} + 1 = 0.$$

This is *Euler's Identity*. It relates five fundamental mathematical constants: 0, 1, e, π and i.

(2) Let $\theta \in \mathbb{R}$. Put $z = n\theta i$ in the complex exponential funtion to get

$$\cos n\theta + i \sin n\theta = e^{n\theta i} = (e^{\theta i})^n = (\cos\theta + i \sin\theta)^n.$$

This proves De Moivre's Theorem.

Gaussian Primes (after Dr Vicky Neale's Talk Yesterday)

Let $S = \{a + bi : a, b \in \mathbb{Z}\}$. A similar argument to Question 4 on Sheet 3 (the one about $a + bi\sqrt{3}$ with a, $b \in \mathbb{Q}$) shows that S is closed under addition and multiplication.

What are the prime numbers in S?

Gaussian Primes (after Dr Vicky Neale's Talk Yesterday)

Let $S = \{a + bi : a, b \in \mathbb{Z}\}$. A similar argument to Question 4 on Sheet 3 (the one about $a + bi\sqrt{3}$ with a, $b \in \mathbb{Q}$) shows that S is closed under addition and multiplication.

What are the prime numbers in S?

For example, 3 is an S-prime. So are

$$1 + 2i,\ 1 + 3i,\ 2 - i,\ 5 + 4i,\ (1 + i)^{1203793} - 1, \ldots$$

Gaussian Primes (after Dr Vicky Neale's Talk Yesterday)

Let $S = \{a + bi : a, b \in \mathbb{Z}\}$. A similar argument to Question 4 on Sheet 3 (the one about $a + bi\sqrt{3}$ with a, $b \in \mathbb{Q}$) shows that S is closed under addition and multiplication.

What are the prime numbers in S?

For example, 3 is an S-prime. So are

$$1 + 2i,\ 1 + 3i,\ 2 - i,\ 5 + 4i,\ (1 + i)^{1203793} - 1, \ldots$$

But 5 is *not* an S-prime, even though 5 is a prime in $\mathbb{Z}$,

Gaussian Primes (after Dr Vicky Neale's Talk Yesterday)

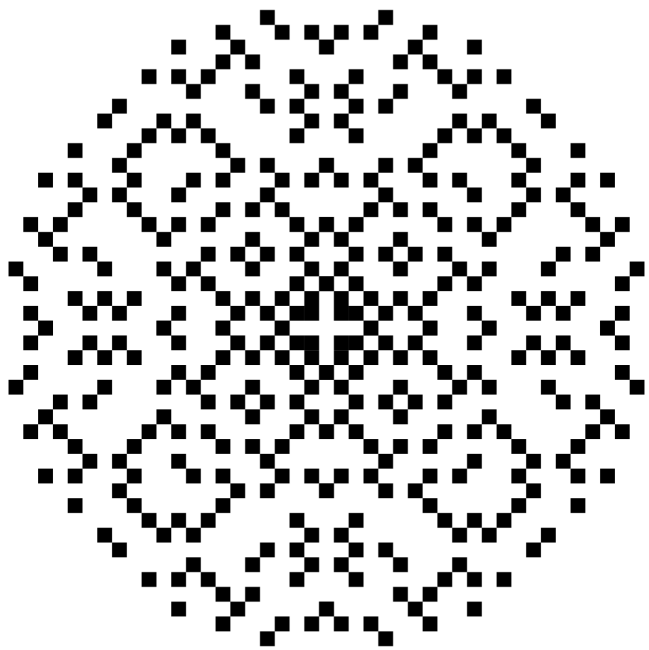
Let $S = \{a + bi : a, b \in \mathbb{Z}\}$. A similar argument to Question 4 on Sheet 3 (the one about $a + bi\sqrt{3}$ with a, $b \in \mathbb{Q}$) shows that S is closed under addition and multiplication.

What are the prime numbers in S?

For example, 3 is an S-prime. So are

$$1 + 2i,\ 1 + 3i,\ 2 - i,\ 5 + 4i,\ (1 + i)^{1203793} - 1, \ldots$$

But 5 is *not* an S-prime, even though 5 is a prime in $\mathbb{Z}$, because $5 = (1 + 2i)(1 - 2i)$.



Using Exponential Form to Find Roots

The exponential form has the same lack of uniqueness as the polar form: if $r > 0$ then

$$re^{i\theta} = se^{i\phi} \iff r = s \text{ and } \phi = \theta + 2n\pi \text{ for some } n \in \mathbb{Z}.$$

Example 3.16

See board for solution to equation $z^3 = 8i$.

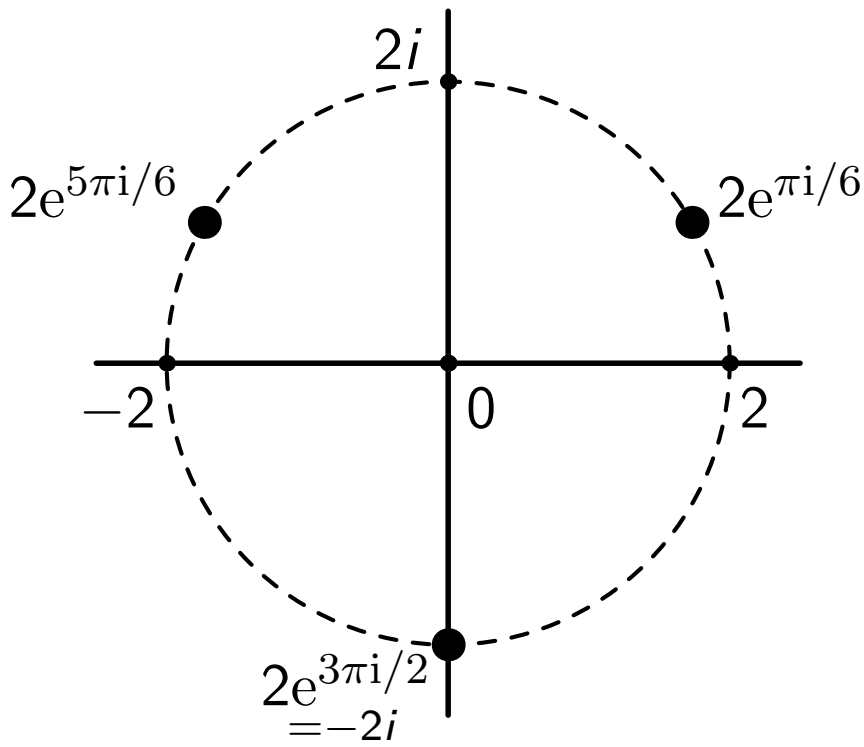
Using Exponential Form to Find Roots

The exponential form has the same lack of uniqueness as the polar form: if $r > 0$ then

$$re^{i\theta} = se^{i\phi} \iff r = s \text{ and } \phi = \theta + 2n\pi \text{ for some } n \in \mathbb{Z}.$$

Example 3.16

See board for solution to equation $z^3 = 8i$.



Using Exponential Form to Find Roots

The exponential form has the same lack of uniqueness as the polar form: if $r > 0$ then

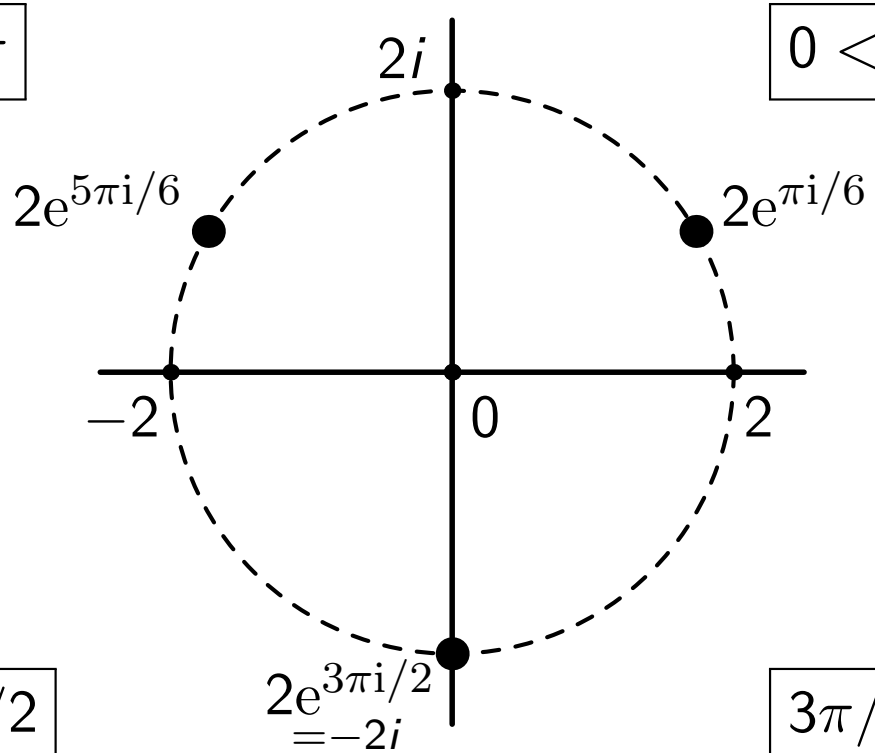
$$re^{i\theta} = se^{i\phi} \iff r = s \text{ and } \phi = \theta + 2n\pi \text{ for some } n \in \mathbb{Z}.$$

Example 3.16

See board for solution to equation $z^3 = 8i$.

$\pi/2 < \mathrm{Arg}(z) < \pi$

$0 < \mathrm{Arg}(z) < \pi/2$



$\pi < \mathrm{Arg}(z) < 3\pi/2$

$3\pi/2 < \mathrm{Arg}(z) < 2\pi$

Using Exponential Form to Find Roots

The exponential form has the same lack of uniqueness as the polar form: if $r > 0$ then

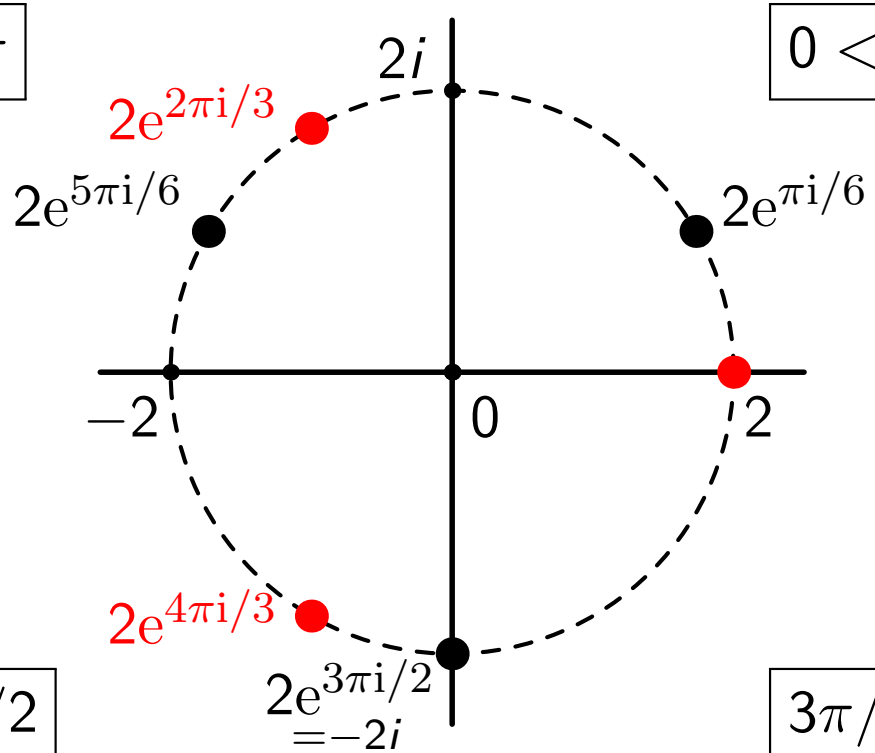
$$re^{i\theta} = se^{i\phi} \iff r = s \text{ and } \phi = \theta + 2n\pi \text{ for some } n \in \mathbb{Z}.$$

Example 3.16

See board for solution to equation $z^3 = 8i$.

$\pi/2 < \mathrm{Arg}(z) < \pi$

$0 < \mathrm{Arg}(z) < \pi/2$



$\pi < \mathrm{Arg}(z) < 3\pi/2$

$3\pi/2 < \mathrm{Arg}(z) < 2\pi$

Log of a Complex Number

Let $z = re^{i\theta}$ be a complex number in exponential form. If $z = 0$ then there is no $w \in \mathbb{C}$ such that $e^w = z$, since $|e^{a+bi}| = e^a$ and $e^a > 0$ for all $a \in \mathbb{R}$. If $z \neq 0$ then

$$e^w = z \iff w = \ln r + (\theta + 2\pi n)i \text{ for some } n \in \mathbb{Z}.$$

Any such number w is called a *logarithm* of z.

Example 3.17

In exponential form $2i = 2e^{i\pi/2}$. So the set of logarithms of $2i$ is

$$\left\{\ln 2 + (\frac{\pi}{2} + 2n\pi)i \text{ for some } n \in \mathbb{Z}\right\}.$$

Log of a Complex Number

Let $z = re^{i\theta}$ be a complex number in exponential form. If $z = 0$ then there is no $w \in \mathbb{C}$ such that $e^w = z$, since $|e^{a+bi}| = e^a$ and $e^a > 0$ for all $a \in \mathbb{R}$. If $z \neq 0$ then

$$e^w = z \iff w = \ln r + (\theta + 2\pi n)i \text{ for some } n \in \mathbb{Z}.$$

Any such number w is called a *logarithm* of z.

Example 3.17

In exponential form $2i = 2e^{i\pi/2}$. So the set of logarithms of $2i$ is

$$\left\{\ln 2 + (\frac{\pi}{2} + 2n\pi)i \text{ for some } n \in \mathbb{Z}\right\}.$$

Exercise 3.18

Consider exp : $\mathbb{C} \to \mathbb{C}$. What are the domain, codomain and range of exp? Is exp surjective? Is exp injective?

Quadratic Equations

- Please take Part B handout and Problem Sheet 5.
- Please leave Sheet 4 answers promptly at end of lecture.

You are probably familiar with how to solve quadratic equations over the real numbers. Essentially the same method works over $\mathbb{C}$. Exponential form might be useful for finding square roots.

Lemma 3.19 (Examinable)

Let $a, b, c \in \mathbb{C}$ and suppose that $a \neq 0$. The solutions to the quadratic equation $az^2 + bz + c = 0$ are

$$z = \frac{-b \pm D}{2a}$$

where $D \in \mathbb{C}$ satisfies $D^2 = b^2 - 4ac$.

Quadratic Equations

- Please take Part B handout and Problem Sheet 5.
- Please leave Sheet 4 answers promptly at end of lecture.

You are probably familiar with how to solve quadratic equations over the real numbers. Essentially the same method works over $\mathbb{C}$. Exponential form might be useful for finding square roots.

Lemma 3.19 (Examinable)

Let $a, b, c \in \mathbb{C}$ and suppose that $a \neq 0$. The solutions to the quadratic equation $az^2 + bz + c = 0$ are

$$z = \frac{-b \pm D}{2a}$$

where $D \in \mathbb{C}$ satisfies $D^2 = b^2 - 4ac$.

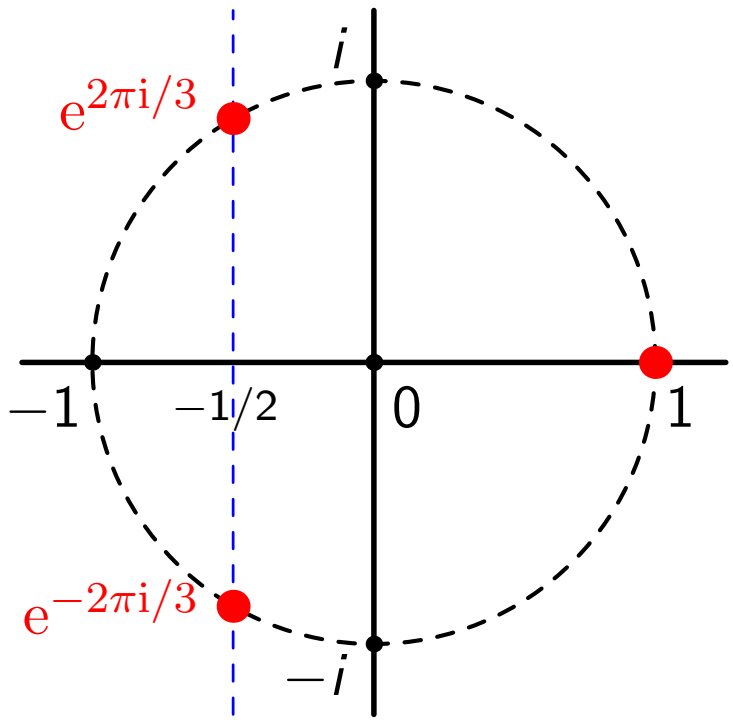
Bear in mind that $\sqrt{b^2 - 4ac}$ is ambiguous when $b^2 - 4ac \notin \mathbb{R}_{\geq 0}$. See Bonus Question A on Sheet 3 for one problem this causes.

Example 3.20

Observe that $z^3 - 1 = (z-1)(z^2+z+1)$. So if z is a third root of unity other than 1 then z is a solution of $z^2 + z + 1 = 0$. Using Lemma 3.19 we get

$$z = -\frac{1}{2} \pm \frac{\sqrt{3}}{2} i.$$

Since the third roots of unity are 1, $\mathrm{e}^{2\pi i/3}$ and $\mathrm{e}^{4\pi i/3}$, this shows that $\cos \frac{2\pi}{3} = -\frac{1}{2}$ and $\sin \frac{2\pi}{3} = \frac{\sqrt{3}}{2}$.



Fundamental Theorem of Algebra

Theorem 3.21 (Fundamental Theorem of Algebra)

Let $d \in \mathbb{N}$ and let $a_0, a_1, \ldots, a_d \in \mathbb{C}$ with $a_d \neq 0$. Then the equation

$$a_d z^d + a_{d-1} z^{d-1} + \cdots + a_1 z + a_0 = 0$$

has a solution in $\mathbb{C}$.

An Easyish Quartic

Exercise 3.22

Find all solutions to the quartic equation
$z^4 + 2z^3 + 3z^2 + 4z + 2 = 0$. (*Hint:* one solution is in $\mathbb{Z}$.)

An Easyish Quartic

Exercise 3.22

Find all solutions to the quartic equation
$z^4 + 2z^3 + 3z^2 + 4z + 2 = 0$. (*Hint:* one solution is in $\mathbb{Z}$.)

Solution. Since

$$(-1)^4 + 2(-1)^3 + 3(-1)^2 + 4(-1) + 2 = 0,$$

-1 is a root. So $z - (-1) = z + 1$ is a factor and

$$z^4 + 2z^3 + 3z^2 + 4z + 2 = (z + 1)(z^3 + z^2 + 2z + 2).$$

Now -1 is again a root of the cubic $z^3 + z^2 + 2z + 2$, and we get

$$z^3 + z^2 + 2z + 2 = (z + 1)(z^2 + 2).$$

Hence

$$z^4 + 2z^3 + 3z^2 + 4z + 2 = (z + 1)^2(z^2 + 2)$$

and the roots are -1 (twice), $i\sqrt{2}$ and $-i\sqrt{2}$.

Part B: Natural Numbers and Induction

§4 Induction

A *proposition* is a self-contained statement which is either true or false. For example the statement

There is a real number x such that $x^2 + 1 = 0$

is a false proposition. More briefly, we can write

P : The integers are closed under addition.

This defines P to be the true proposition that the integers are closed under addition. Some statements are too vague or subjective to be considered propositions. For instance:

Q : Houses in Englefield Green are too expensive.

More propositions

We often want to consider statements that depend on the value of a variable. For example, for each $x \in \mathbb{R}$, define

$$P(x): \quad x^2 - 4x + 1 \geq 2.$$

This defines an infinite collection of propositions, one proposition for each real number. Some of these propositions are true, and others are false. For example $P(6)$ and $P(2+\sqrt{5})$ are true, and $P(1)$ is false.

More propositions

We often want to consider statements that depend on the value of a variable. For example, for each $x \in \mathbb{R}$, define

$$P(x): \quad x^2 - 4x + 1 \geq 2.$$

This defines an infinite collection of propositions, one proposition for each real number. Some of these propositions are true, and others are false. For example $P(6)$ and $P(2+\sqrt{5})$ are true, and $P(1)$ is false.

Quiz: Define

$$Q(n): \quad 2^n \geq 4n.$$

Which of the following are propositions?

(A) $Q(4)$
(B) $Q(3)$
(C) $x^2 + y^2 = 25$
(D) There exist $x, y \in \mathbb{N}$ such that $x^2 + y^2 = 25$

More propositions

We often want to consider statements that depend on the value of a variable. For example, for each $x \in \mathbb{R}$, define

$$P(x): \quad x^2 - 4x + 1 \geq 2.$$

This defines an infinite collection of propositions, one proposition for each real number. Some of these propositions are true, and others are false. For example $P(6)$ and $P(2+\sqrt{5})$ are true, and $P(1)$ is false.

Quiz: Define

$$Q(n): \quad 2^n \geq 4n.$$

Which of the following are propositions?

(A) $Q(4)$ Is a proposition

(B) $Q(3)$

(C) $x^2 + y^2 = 25$

(D) There exist $x, y \in \mathbb{N}$ such that $x^2 + y^2 = 25$

More propositions

We often want to consider statements that depend on the value of a variable. For example, for each $x \in \mathbb{R}$, define

$$P(x): \quad x^2 - 4x + 1 \geq 2.$$

This defines an infinite collection of propositions, one proposition for each real number. Some of these propositions are true, and others are false. For example $P(6)$ and $P(2+\sqrt{5})$ are true, and $P(1)$ is false.

Quiz: Define

$$Q(n): \quad 2^n \geq 4n.$$

Which of the following are propositions?

(A) $Q(4)$ — Is a proposition

(B) $Q(3)$ — Is a proposition

(C) $x^2 + y^2 = 25$

(D) There exist $x, y \in \mathbb{N}$ such that $x^2 + y^2 = 25$

More propositions

We often want to consider statements that depend on the value of a variable. For example, for each $x \in \mathbb{R}$, define

$$P(x): \quad x^2 - 4x + 1 \geq 2.$$

This defines an infinite collection of propositions, one proposition for each real number. Some of these propositions are true, and others are false. For example $P(6)$ and $P(2+\sqrt{5})$ are true, and $P(1)$ is false.

Quiz: Define

$$Q(n): \quad 2^n \geq 4n.$$

Which of the following are propositions?

(A) $Q(4)$ — Is a proposition

(B) $Q(3)$ — Is a proposition

(C) $x^2 + y^2 = 25$ — Is not a proposition (not self contained)

(D) There exist $x, y \in \mathbb{N}$ such that $x^2 + y^2 = 25$

More propositions

We often want to consider statements that depend on the value of a variable. For example, for each $x \in \mathbb{R}$, define

$$P(x): \quad x^2 - 4x + 1 \geq 2.$$

This defines an infinite collection of propositions, one proposition for each real number. Some of these propositions are true, and others are false. For example $P(6)$ and $P(2+\sqrt{5})$ are true, and $P(1)$ is false.

Quiz: Define

$$Q(n): \quad 2^n \geq 4n.$$

Which of the following are propositions?

(A) $Q(4)$ — Is a proposition

(B) $Q(3)$ — Is a proposition

(C) $x^2 + y^2 = 25$ — Is not a proposition (not self contained)

(D) There exist $x, y \in \mathbb{N}$ such that $x^2 + y^2 = 25$ — Is a proposition

More Propositions

Example 4.1

For $n \in \mathbb{N}$ define

$P(n)$: The sum of the odd numbers from 1 up to and including $2n-1$ is equal to n^2.

Looking at small cases will probably convince you that $P(n)$ is true for all $n \in \mathbb{N}$.

Example 4.2

For $n \in \mathbb{N}$ define

$$Q(n): \quad n^2 + n + 41 \text{ is a prime number}$$

So we have defined propositions

$$Q(1): \quad 1^2 + 1 + 41 \text{ is a prime number}$$
$$Q(2): \quad 2^2 + 2 + 41 \text{ is a prime number}$$
$$Q(3): \quad 3^2 + 3 + 41 \text{ is a prime number}$$

and so on.

More Propositions

Example 4.1

For $n \in \mathbb{N}$ define

$P(n)$: The sum of the odd numbers from 1 up to and including $2n-1$ is equal to n^2.

Looking at small cases will probably convince you that $P(n)$ is true for all $n \in \mathbb{N}$.

Example 4.2

For $n \in \mathbb{N}$ define

$$Q(n): \quad n^2 + n + 41 \text{ is a prime number}$$

So we have defined propositions

$$Q(1): \quad 1^2 + 1 + 41 \text{ is a prime number}$$
$$Q(2): \quad 2^2 + 2 + 41 \text{ is a prime number}$$
$$Q(3): \quad 3^2 + 3 + 41 \text{ is a prime number}$$

and so on. In this case $Q(1), Q(2), \ldots, Q(39)$ are all true propositions. But $Q(40)$ and $Q(41)$ are false.

The Principle of Mathematical Induction

Suppose that $P(n)$ is a proposition for each $n \in \mathbb{N}$. The Principle of Mathematical Induction states that if

- $P(1)$ is true
- $P(n) \Longrightarrow P(n+1)$ for each $n \in \mathbb{N}$,

then $P(n)$ is true for all $n \in \mathbb{N}$.

Example 4.3

For all $n \in \mathbb{N}$ we have

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Administration

- Please collect work:
  - A–K in green folder
  - L–Z in blue folder
- Questions 3, 5 and 6 were marked. All answers on Moodle.
- I will go through Question 5 today. Question 6 was done better, but often the algebra could be simplified. E.g. for 6(b)

$$\begin{aligned} z &= (a+bi)(a-bi)(c+di)(c-di) \\ &= \Big((a+bi)(c+di)\Big)\Big(a-bi)(c-di)\Big) \\ &= \Big((ac-bd)+(ad+bc)i\Big)\Big((ac-bd)-(ad+bc)i\Big) \\ &= (ac-bd)^2+(ad+bc)^2 \end{aligned}$$

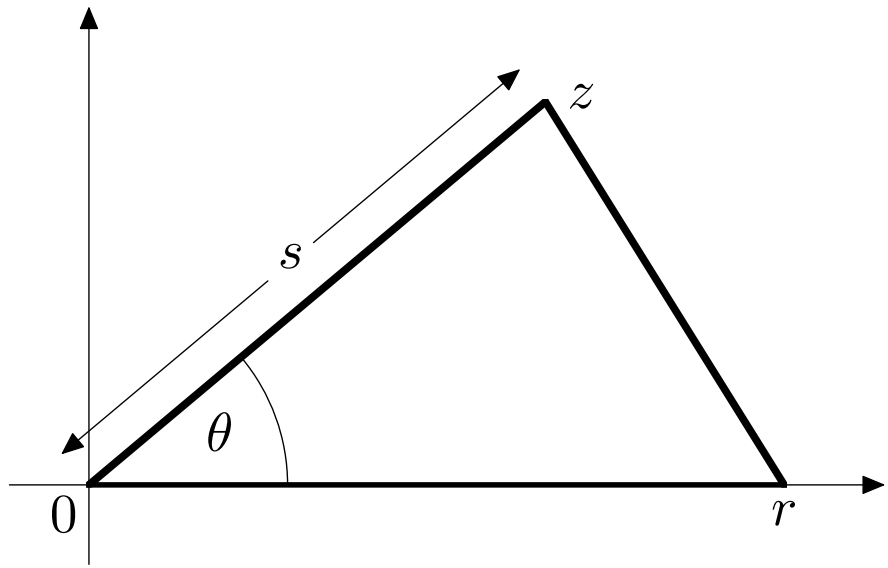
  where the final step uses the identity

$$(x+iy)(x-iy) = x^2+y^2.$$

- Please see the lecturer after the lecture or in office hours if you have any queries about the marking, or want to discuss any of the questions.

Sheet 4 Question 5

The Argand diagram below shows a triangle with vertices at 0, $r \in \mathbb{R}$ and $z \in \mathbb{C}$. Let s be the length of the side with vertices at 0 and z and let θ be the marked angle.



(a) Express the lengths of the other two sides of the triangle in terms of r and z. [*Hint:* for the side from r to z, Question 4(a) has a relevant idea.]

(b) Show that $z + \overline{z} = 2s\cos\theta$. [*Hint:* what is z in polar form?]

(c) By expanding $|z - r|^2 = (z - r)\overline{(z - r)}$ prove the cosine rule.

Induction: General Strategy and Example 4.4

(1) Formulate the statement you want to prove as a proposition $P(n)$, depending on a natural number n.

(2) Prove $P(1)$. This is called the *base case*.

(3) Prove that $P(n) \implies P(n+1)$ for each $n \in \mathbb{N}$. In other words: **assume $P(n)$ and use it to prove $P(n+1)$**. This is called the *inductive step*.

(4) Announce that you have finished!

Induction: General Strategy and Example 4.4

(1) Formulate the statement you want to prove as a proposition $P(n)$, depending on a natural number n.

(2) Prove $P(1)$. This is called the *base case*.

(3) Prove that $P(n) \implies P(n+1)$ for each $n \in \mathbb{N}$. In other words: **assume $P(n)$ and use it to prove $P(n+1)$**. This is called the *inductive step*.

(4) Announce that you have finished!

For the inductive step: imagine you are given a card, that says:

> *'The bearer of this card is faithfully promised that $P(n)$ is true'*

You can play this card at any time in your proof of $P(n+1)$. You can even play it more than once, if that seems helpful.

Induction: General Strategy and Example 4.4

(1) Formulate the statement you want to prove as a proposition $P(n)$, depending on a natural number n.

(2) Prove $P(1)$. This is called the *base case*.

(3) Prove that $P(n) \implies P(n+1)$ for each $n \in \mathbb{N}$. In other words: **assume $P(n)$ and use it to prove $P(n+1)$**. This is called the *inductive step*.

(4) Announce that you have finished!

For the inductive step: imagine you are given a card, that says:

> *'The bearer of this card is faithfully promised that $P(n)$ is true'*

You can play this card at any time in your proof of $P(n+1)$. You can even play it more than once, if that seems helpful.

Remember, $P(n)$ is a specific proposition concerning the number $n \in \mathbb{N}$. At A-level you might have written $n = k$ to emphasise this.

Changing the Base Case

Sometimes we need to take the base case to be $P(b)$ for some $b > 1$.

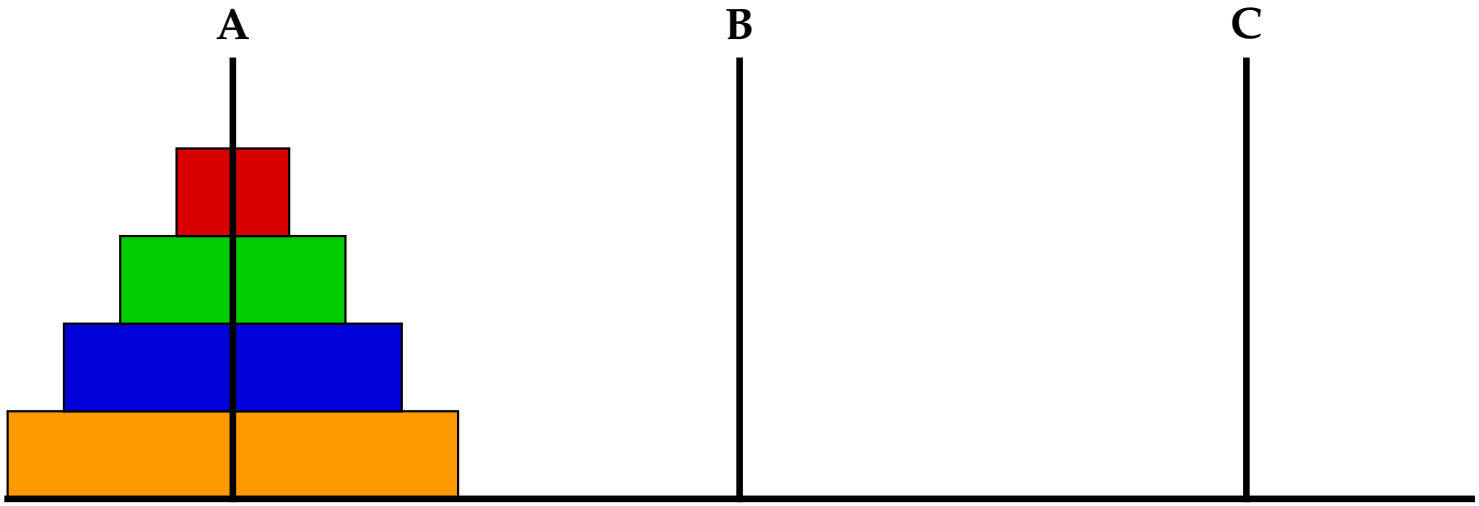
Example 4.5

If $n \in \mathbb{N}$ and $n \geq 4$ then $2^n \geq 4n$.

Towers of Hanoi

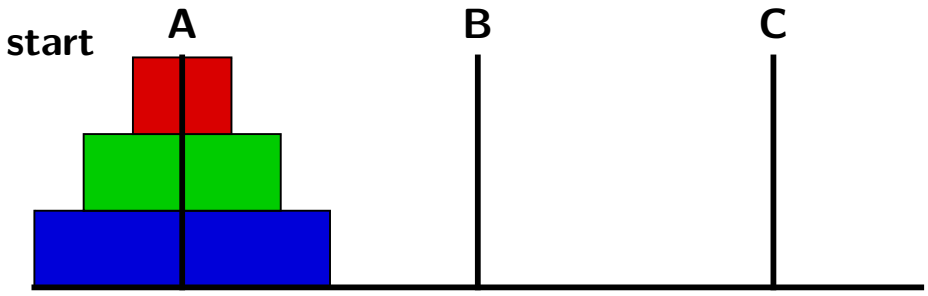
Problem 4.6 (Towers of Hanoi)

You are given a board with three pegs. On peg **A** there are n discs of strictly increasing radius. The starting position for a four disc game is shown below.

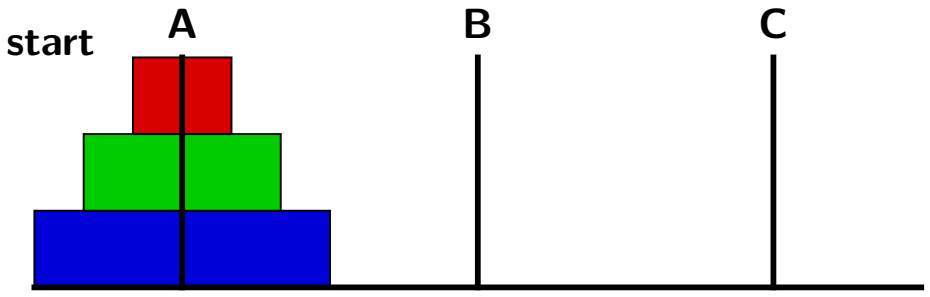


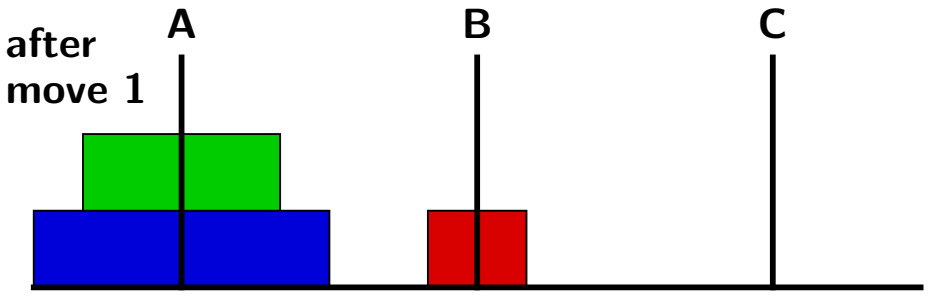
A *move* consists of taking a single disc at the top of the pile on one peg, and moving it to another peg. **At no point may a larger disc be placed on top of a smaller disc.** Your aim is to transfer all the discs from peg **A** to one of the other pegs. How many moves are required?

Towers of Hanoi: A Solution for Three Discs

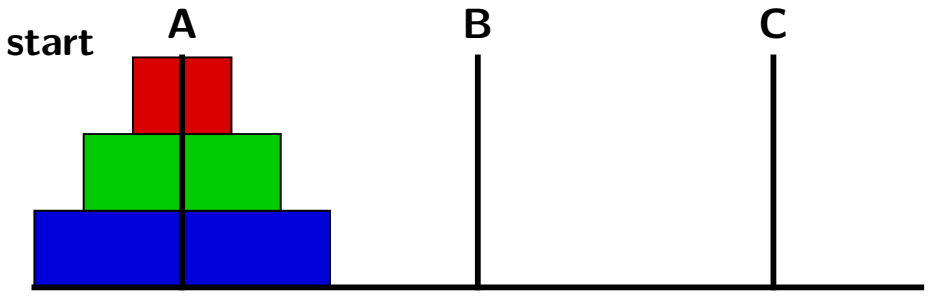


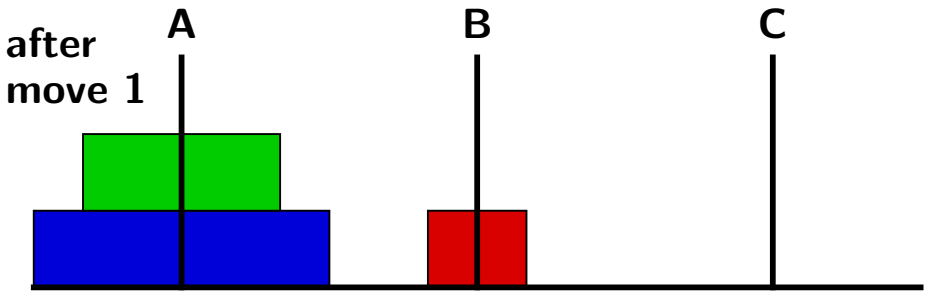
Towers of Hanoi: A Solution for Three Discs

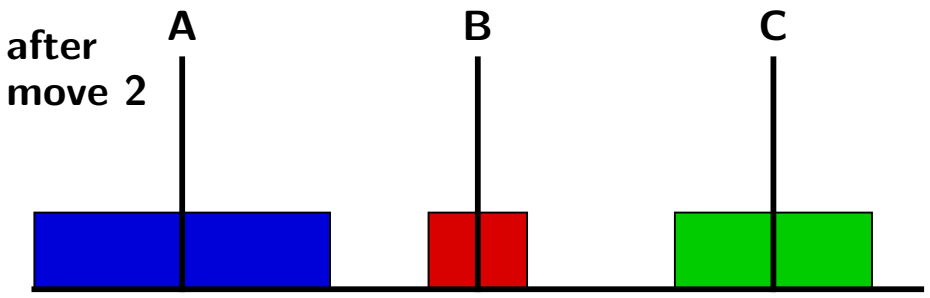




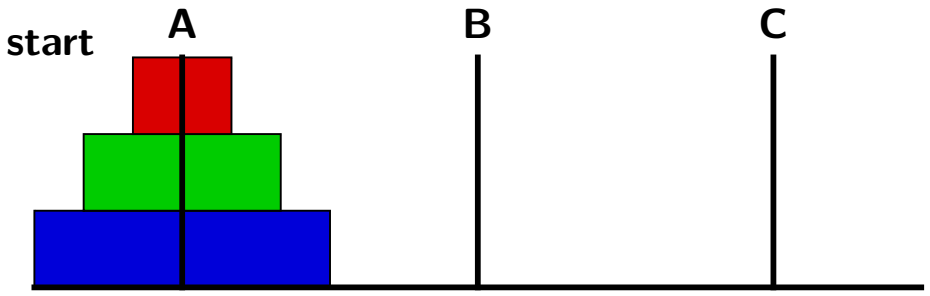
Towers of Hanoi: A Solution for Three Discs

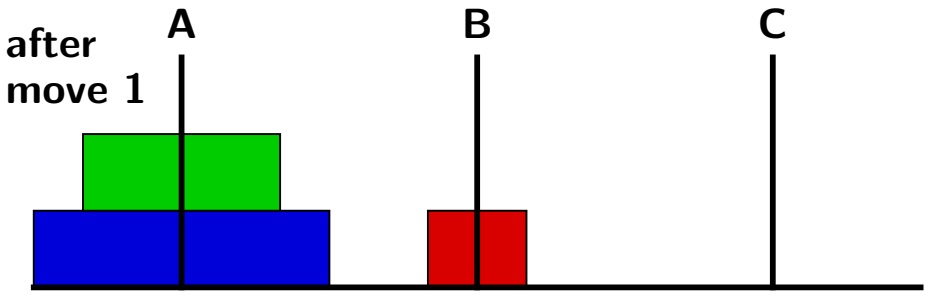


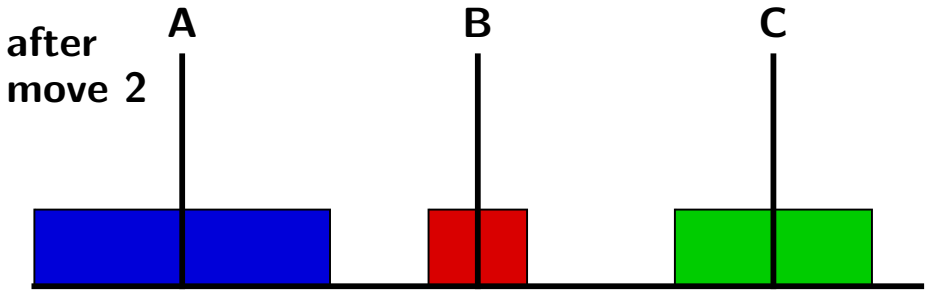


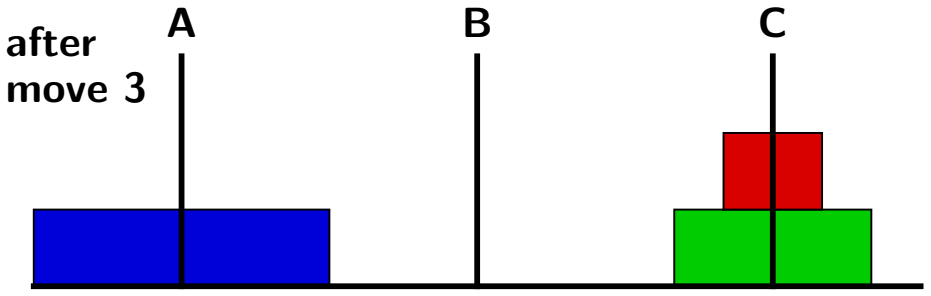


Towers of Hanoi: A Solution for Three Discs

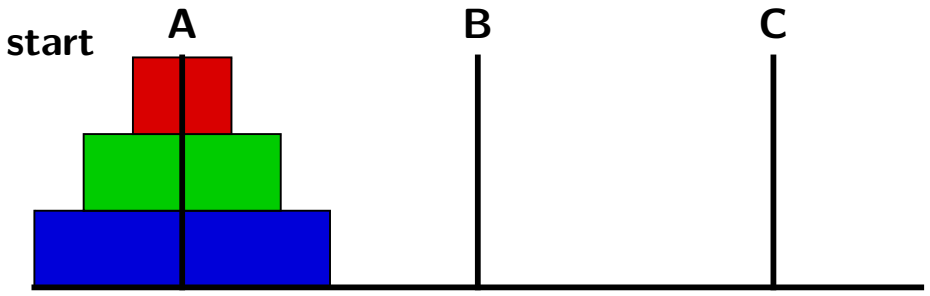


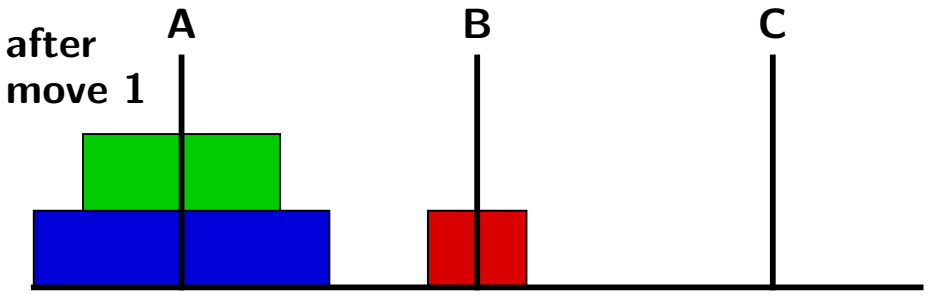


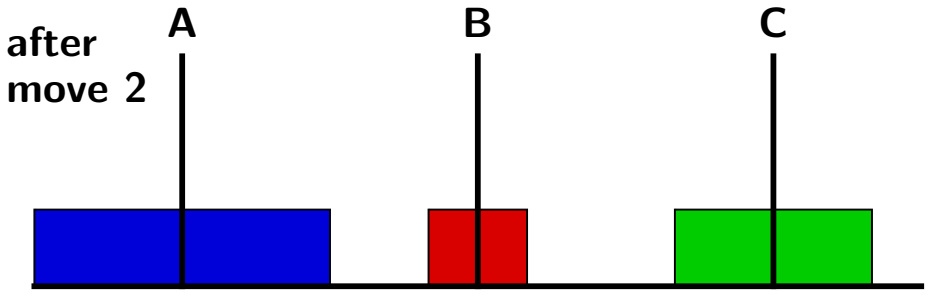


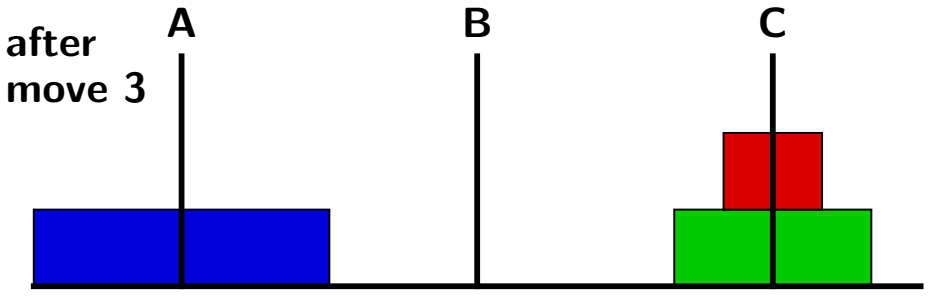


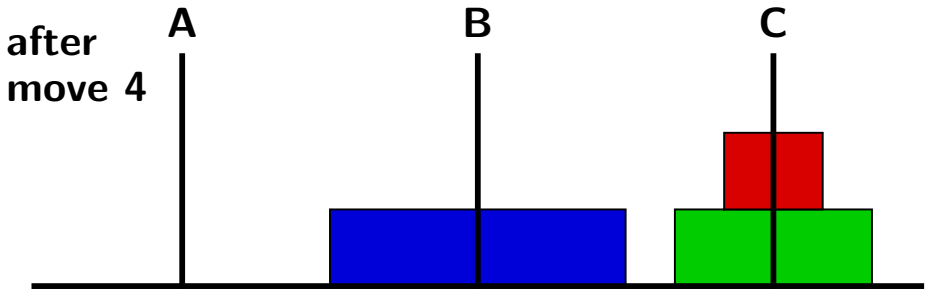
Towers of Hanoi: A Solution for Three Discs



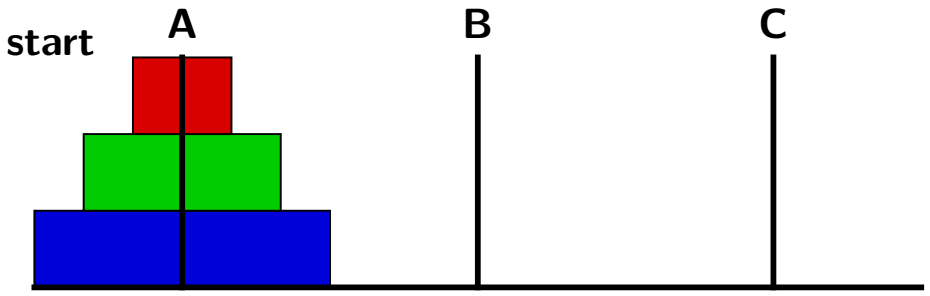


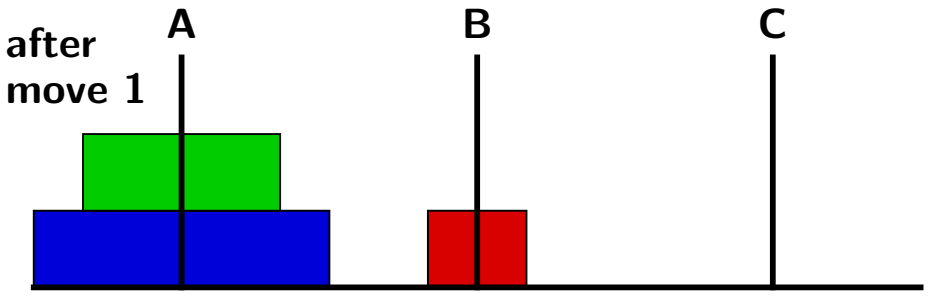


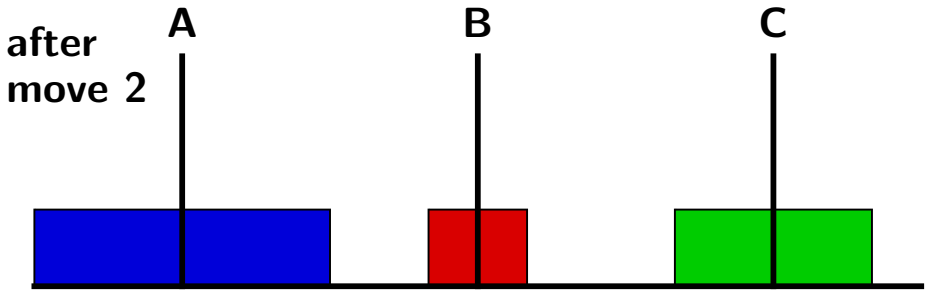


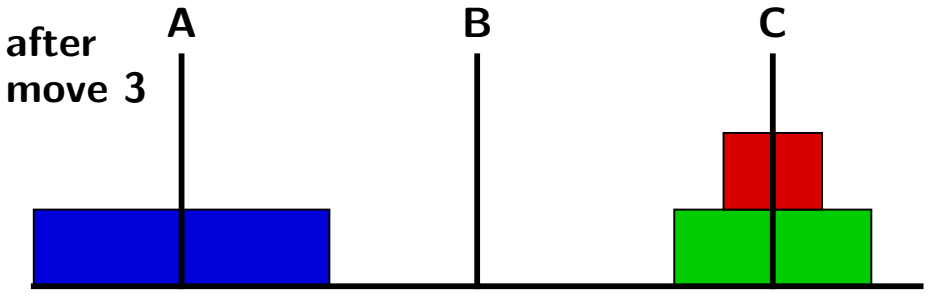


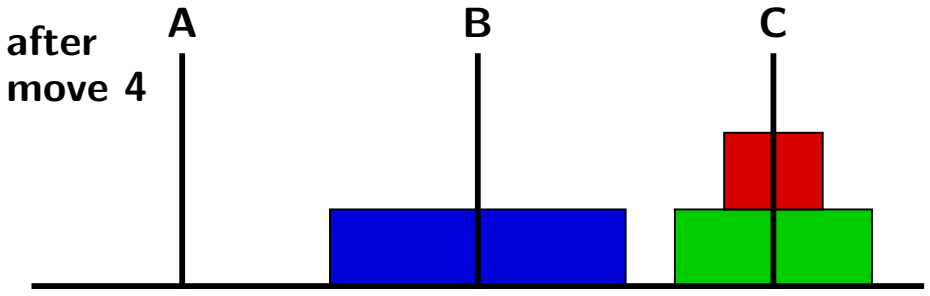
Towers of Hanoi: A Solution for Three Discs

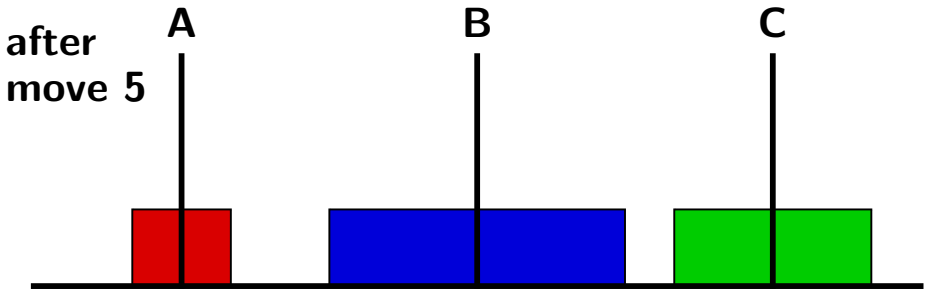




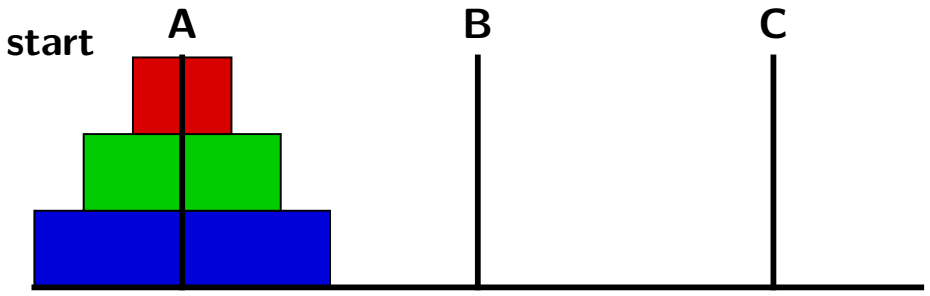


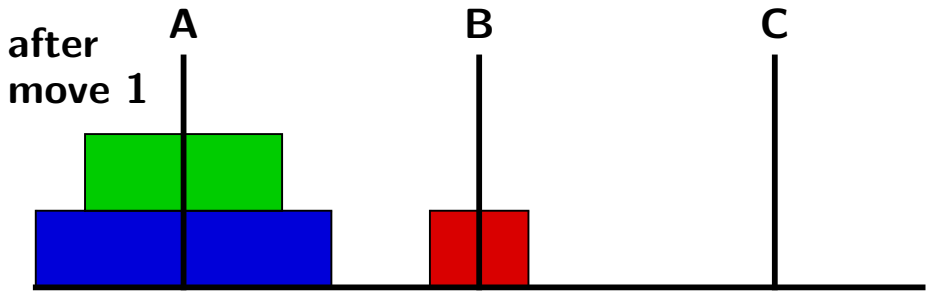


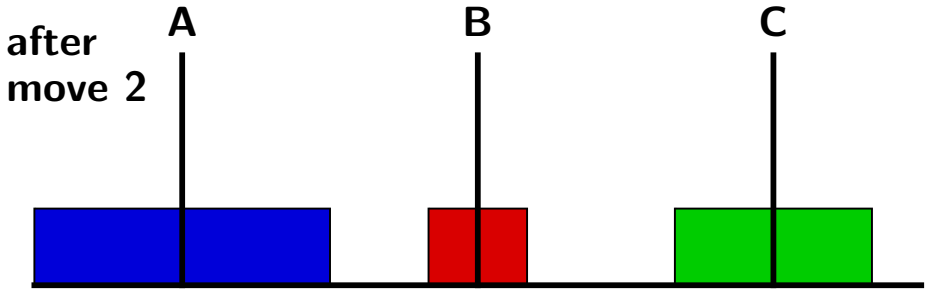


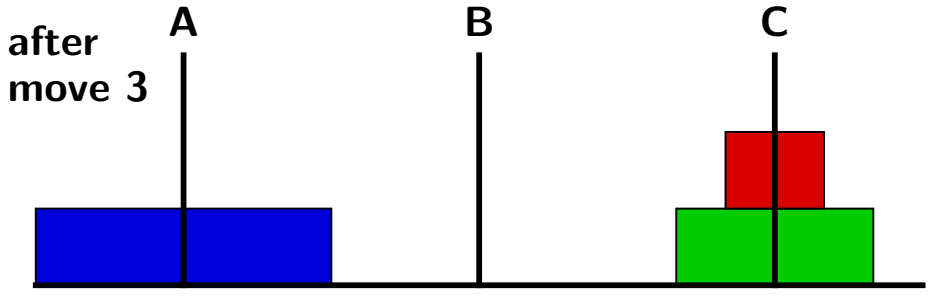


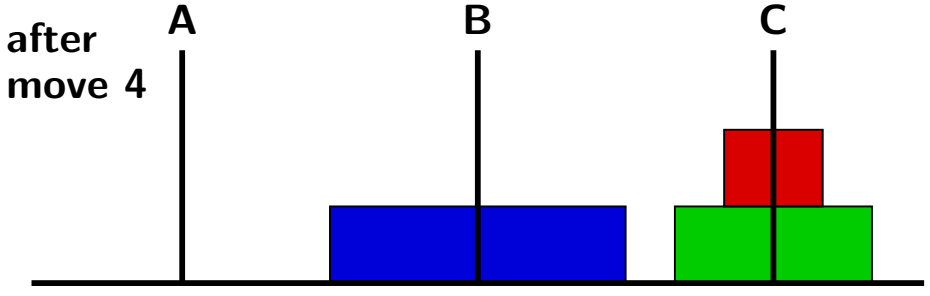
Towers of Hanoi: A Solution for Three Discs

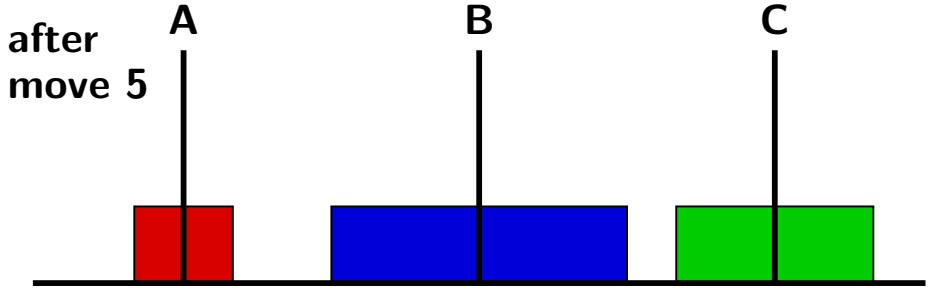


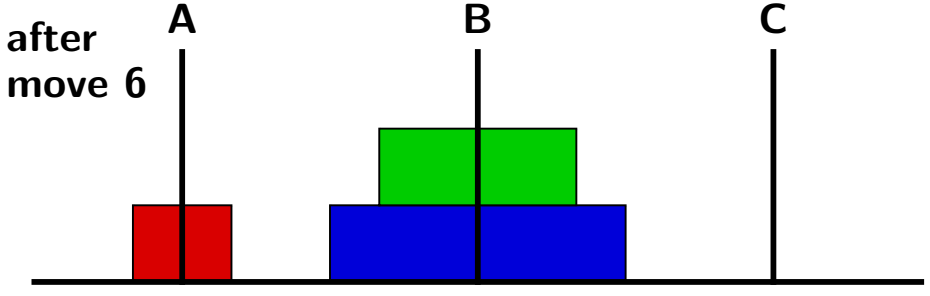




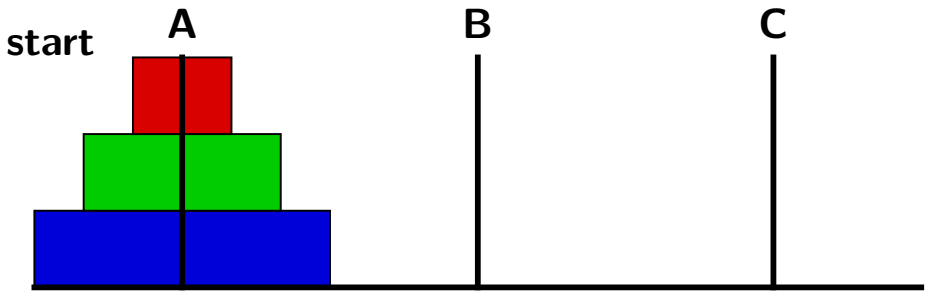


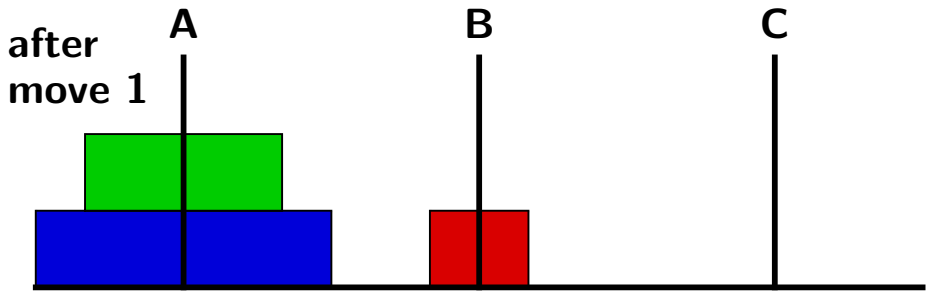


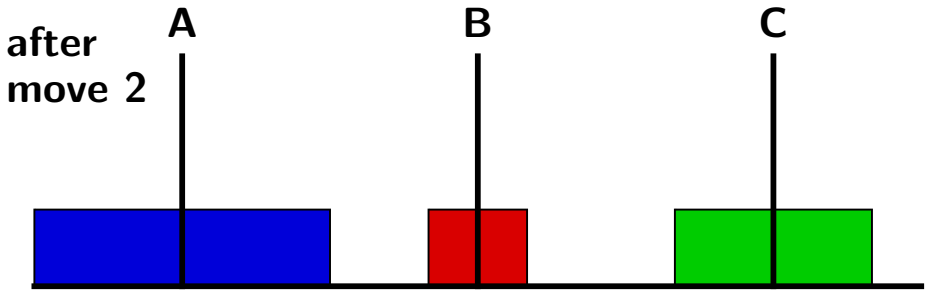


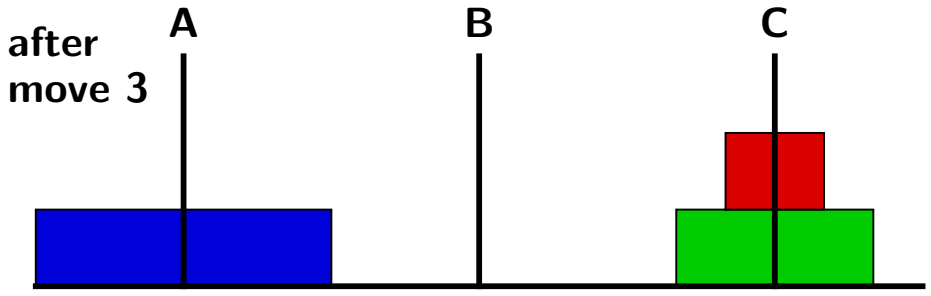


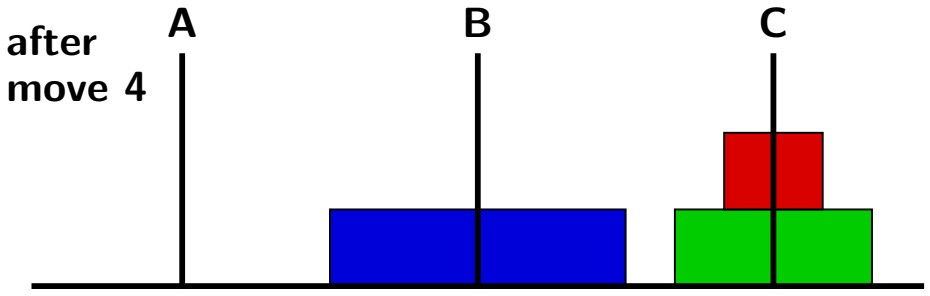
Towers of Hanoi: A Solution for Three Discs

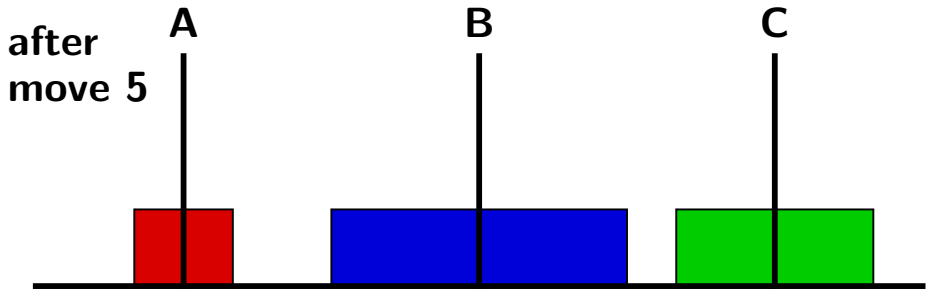


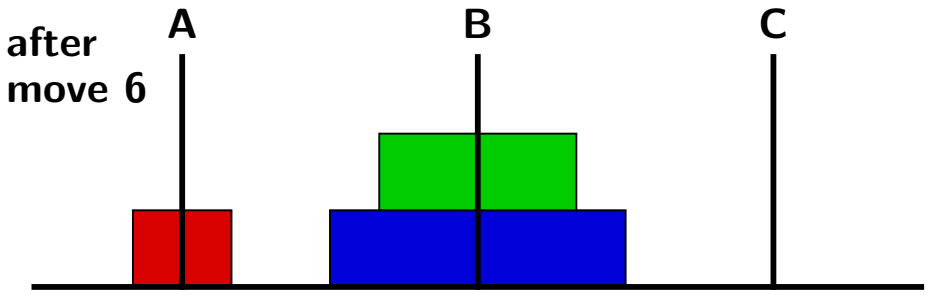


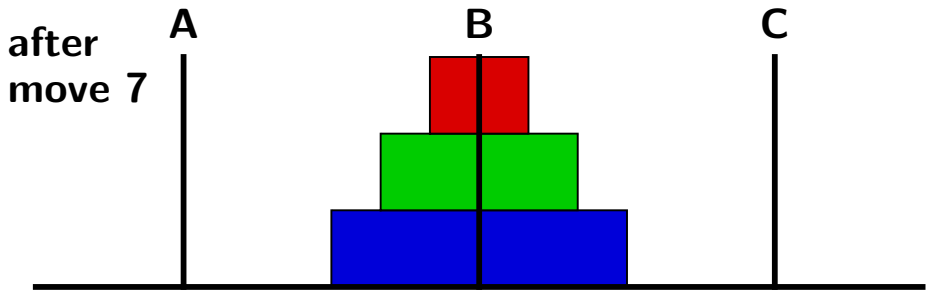




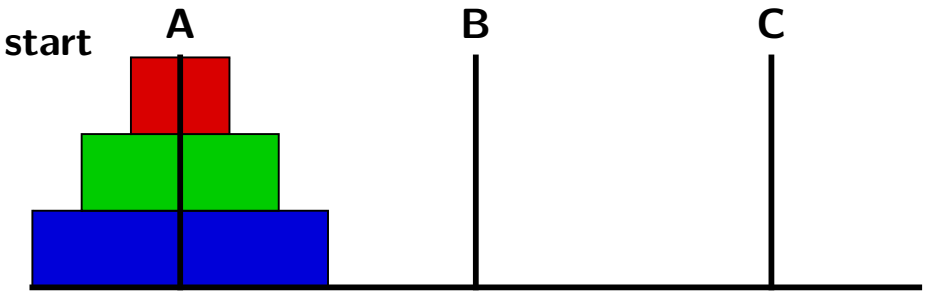


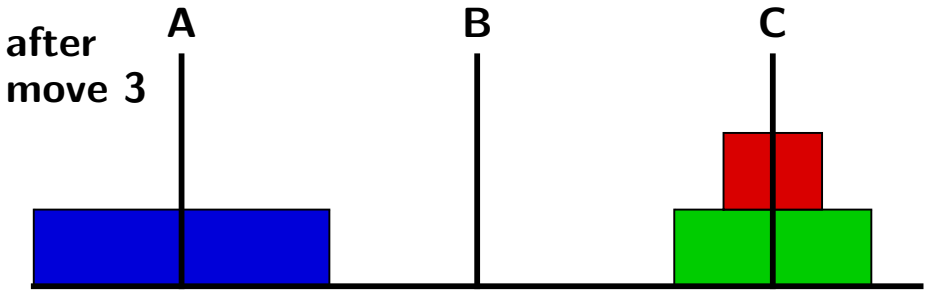


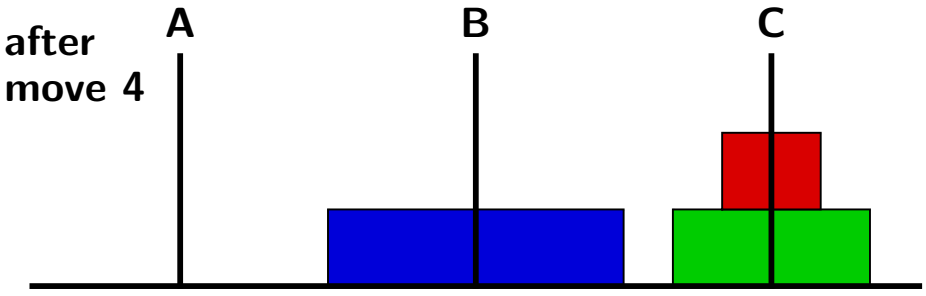


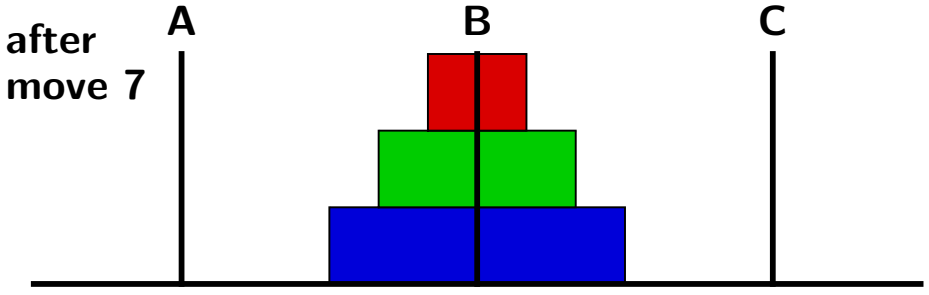


Towers of Hanoi: A Solution for Three Discs









- Please take Problem Sheet 6
- Please hand in Sheet 5 **promptly** at the end of this lecture, or leave in the box outside my office (McCrea 240) before 5pm.

Towers of Hanoi: an Unexpected Pattern

n	0	1	2	3	4	5
$2^n - 1$	0	1	3	7	15	31
$n^2 - (n-1)$	1	1	3	7	13	12

- Please take Problem Sheet 6
- Please hand in Sheet 5 **promptly** at the end of this lecture, or leave in the box outside my office (McCrea 240) before 5pm.

Towers of Hanoi: an Unexpected Pattern

n	0	1	2	3	4	5
$2^n - 1$	0	1	3	7	15	31
$n^2 - (n-1)$	1	1	3	7	13	12

- Please take Problem Sheet 6
- Please hand in Sheet 5 **promptly** at the end of this lecture, or leave in the box outside my office (McCrea 240) before 5pm.

Towers of Hanoi: an Unexpected Pattern

n	0	1	2	3	4	5
$2^n - 1$	0	1	3	7	15	31
$n^2 - (n-1)$	1	1	3	7	13	12

Question 2 on Sheet 6 asks you to complete the proof indicated on Friday that $2^n - 1$ moves are necessary to move n discs from one peg to another.

You can assume 'without loss of generality' that the aim is to move n discs from Peg 1 to Peg 2.

- Please take Problem Sheet 6
- Please hand in Sheet 5 **promptly** at the end of this lecture, or leave in the box outside my office (McCrea 240) before 5pm.

Towers of Hanoi: an Unexpected Pattern

n	0	1	2	3	4	5
$2^n - 1$	0	1	3	7	15	31
$n^2 - (n-1)$	1	1	3	7	13	12

Question 2 on Sheet 6 asks you to complete the proof indicated on Friday that $2^n - 1$ moves are necessary to move n discs from one peg to another.

You can assume 'without loss of generality' that the aim is to move n discs from Peg 1 to Peg 2.

Hint from Friday: to move n discs from Peg 1 to Peg 2, we must at some point move the largest disc from Peg 1 to Peg 2. This can only be done if all the other discs are on Peg 3.

Sigma Notation

Let m, $n \in \mathbb{Z}$ with $m \leq n$. If $a_m, a_{m+1}, \ldots, a_n$ are complex numbers then we write their sum $a_m + a_{m+1} + \cdots + a_n$ as

$$\sum_{k=m}^{n} a_k.$$

This is read as 'the sum of a_k for k from m to n', or 'sigma a_k for k from m to n'. We say that k is the *summation variable*, m is the *lower limit* and n is the *upper limit*.

Sigma Notation

Let m, $n \in \mathbb{Z}$ with $m \leq n$. If $a_m, a_{m+1}, \ldots, a_n$ are complex numbers then we write their sum $a_m + a_{m+1} + \cdots + a_n$ as

$$\sum_{k=m}^{n} a_k.$$

This is read as 'the sum of a_k for k from m to n', or 'sigma a_k for k from m to n'. We say that k is the *summation variable*, m is the *lower limit* and n is the *upper limit*.

Exercise 4.8

(i) Express the sums $1 + 3 + \cdots + (2n - 1)$ and $1 + 2 + 2^2 + \cdots + 2^n$ using Σ notation.

(ii) Calculate $\sum_{m=-2}^{3} m^2$.

More Examples of Sigma Notation

Example 4.9

Let z be a complex number. Then

(i) $\sum_{k=1}^{n} z =$

(ii) $\sum_{k=1}^{n} k =$

(iii) $\sum_{k=1}^{n} n =$

More Examples of Sigma Notation

Example 4.9

Let z be a complex number. Then

(i) $\sum_{k=1}^{n} z = nz$

(ii) $\sum_{k=1}^{n} k =$

(iii) $\sum_{k=1}^{n} n =$

More Examples of Sigma Notation

Example 4.9

Let z be a complex number. Then

(i) $\sum_{k=1}^{n} z = nz$

(ii) $\sum_{k=1}^{n} k = n(n+1)/2$

(iii) $\sum_{k=1}^{n} n =$

More Examples of Sigma Notation

Example 4.9

Let z be a complex number. Then

(i) $\sum_{k=1}^{n} z = nz$

(ii) $\sum_{k=1}^{n} k = n(n+1)/2$

(iii) $\sum_{k=1}^{n} n = n^2$.

More Examples of Sigma Notation

Example 4.9

Let z be a complex number. Then

(i) $\sum_{k=1}^{n} z = nz$

(ii) $\sum_{k=1}^{n} k = n(n+1)/2$

(iii) $\sum_{k=1}^{n} n = n^2$.

Quiz: (a) $\sum_{k=0}^{2} k^2 2^{k-1} =$

(A) 7 (B) 8 (C) 9 (D) something else

(b) If $n \in \mathbb{N}$ then $\sum_{j=1}^{n} 2^j - \sum_{k=2}^{n} 2^{k-1} =$

(A) 1 (B) 2 (C) 2^n (D) 2^{n-1}

Rules for Manipulating Sigma Notation

(1) The summation variable can be renamed:

$$\sum_{k=0}^{n} 2^k = \sum_{j=0}^{n} 2^j.$$

A similar renaming is possible for sets: $\{x \in \mathbb{R} : x^2 \geq 2\}$ is exactly the same set as $\{y \in \mathbb{R} : y^2 \geq 2\}$.

(2) In a product, expressions not involving the summation variable can be taken outside the sum:

$$\sum_{j=0}^{n} 5(j+1)^2 = 5\sum_{j=0}^{n}(j+1)^2$$

and

$$\sum_{j=0}^{n} 5m(j+m)^2 = 5m\sum_{j=0}^{n}(j+m)^2.$$

(3) Sums can be split up and terms taken out.

(4) The limits can be shifted.

Example 4.10

Define

$$P(n): \sum_{k=1}^{n} k^2 = \tfrac{1}{6} n(n+1)(2n+1).$$

Now consider $\sum_{k=1}^{n+1} k^2$. Split off the final summand using rule (3), and then use the inductive assumption $P(n)$ to get

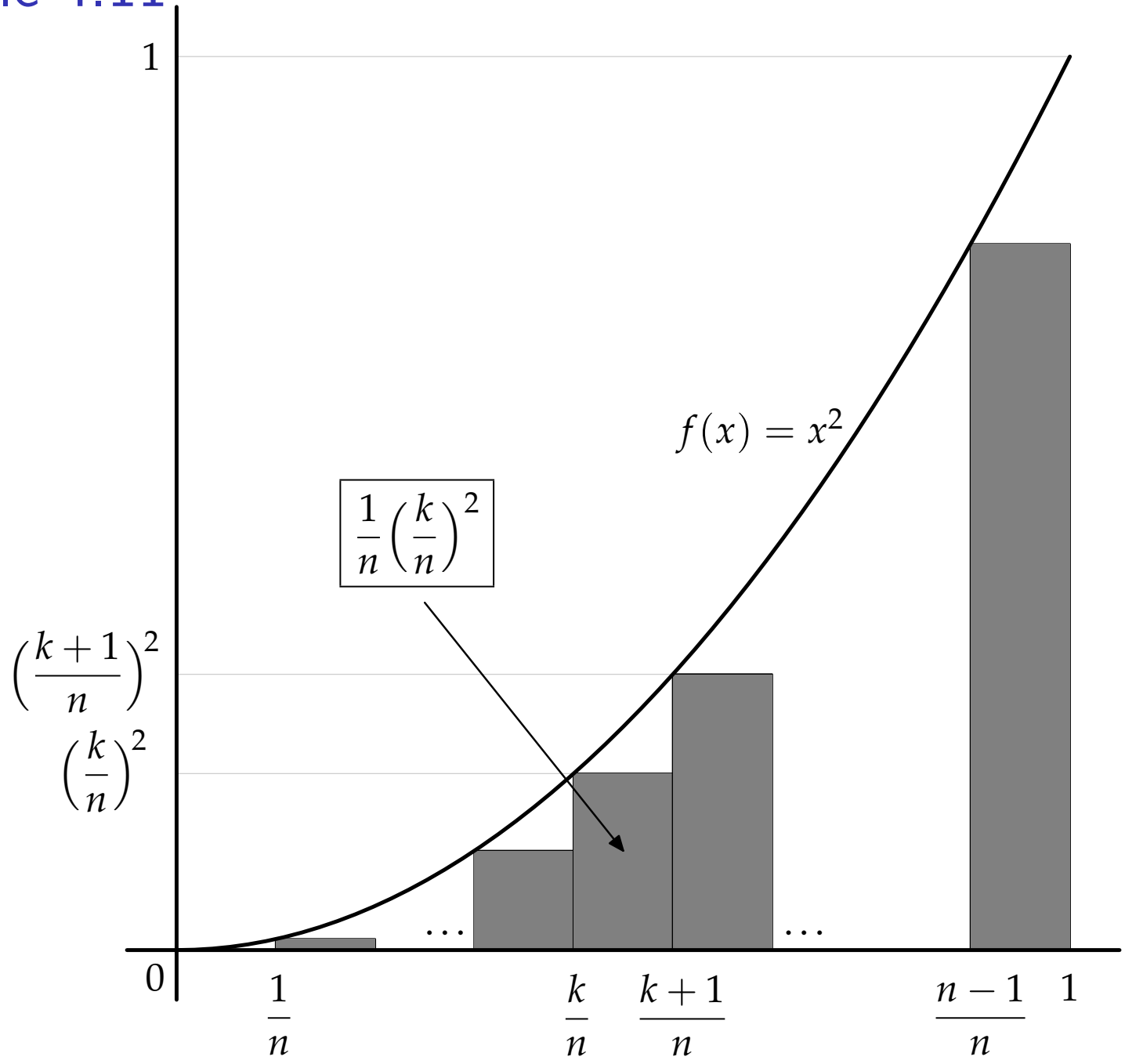
$$\sum_{k=1}^{n+1} k^2 = \sum_{k=1}^{n} k^2 + (n+1)^2 = \tfrac{1}{6} n(n+1)(2n+1) + (n+1)^2.$$

Routine algebraic manipulations give

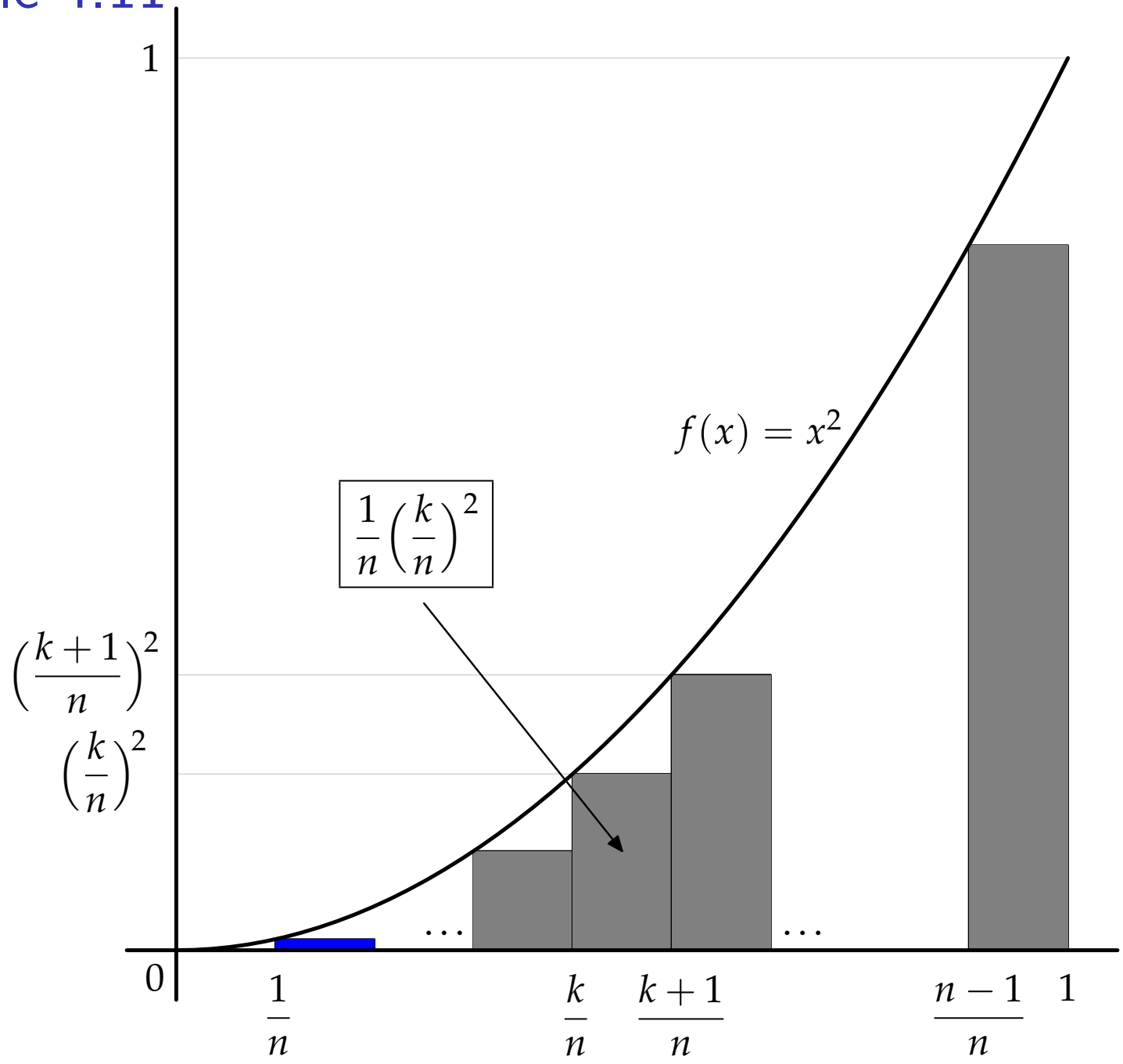
$$\sum_{k=1}^{n+1} k^2 = \ldots = \tfrac{1}{6}(n+1)(n+2)(2n+3)$$

Hence $P(n+1)$ is true. Therefore $P(n) \implies P(n+1)$. By induction $P(n)$ is true for all $n \in \mathbb{N}$.

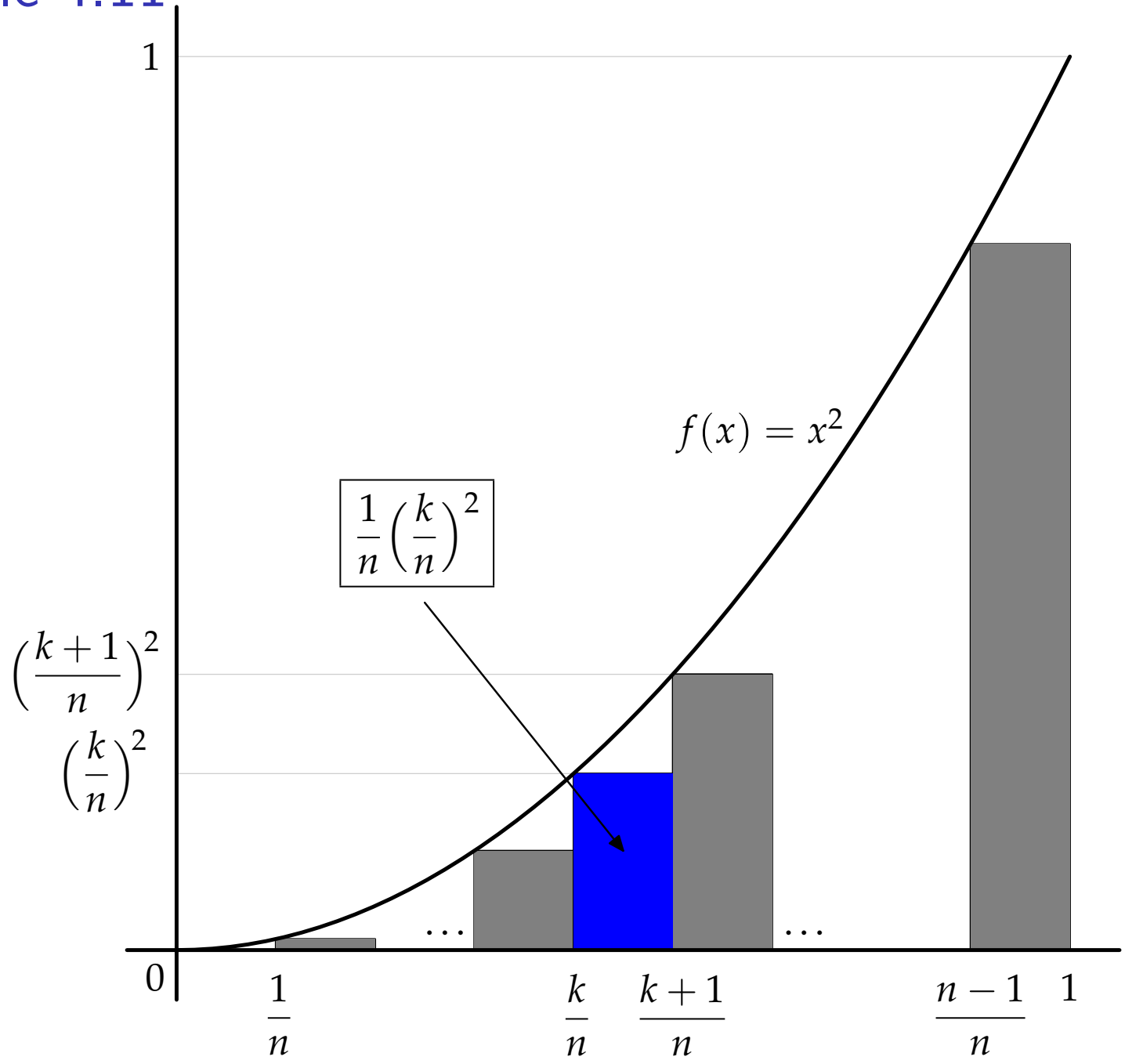
Example 4.11


1
$f(x) = x^2$
$\frac{1}{n}\left(\frac{k}{n}\right)^2$
$\left(\frac{k+1}{n}\right)^2$
$\left(\frac{k}{n}\right)^2$
0
$\frac{1}{n}$
$\frac{k}{n}$
$\frac{k+1}{n}$
$\frac{n-1}{n}$
1

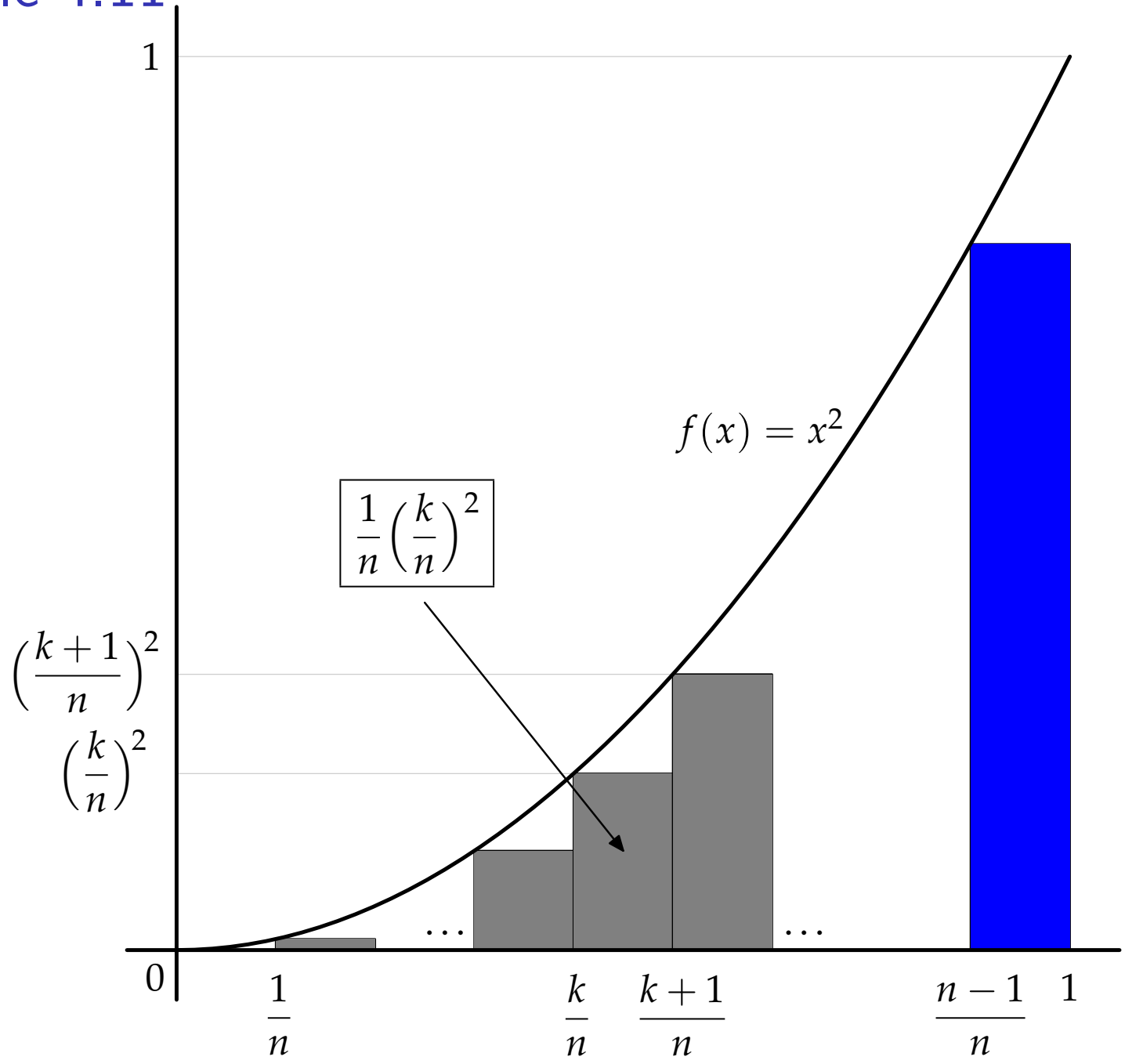
Example 4.11


1
$f(x) = x^2$
$\frac{1}{n}\left(\frac{k}{n}\right)^2$
$\left(\frac{k+1}{n}\right)^2$
$\left(\frac{k}{n}\right)^2$
0
$\frac{1}{n}$
$\frac{k}{n}$
$\frac{k+1}{n}$
$\frac{n-1}{n}$
1

Example 4.11


1
$f(x) = x^2$
$\frac{1}{n}\left(\frac{k}{n}\right)^2$
$\left(\frac{k+1}{n}\right)^2$
$\left(\frac{k}{n}\right)^2$
0
$\frac{1}{n}$
$\frac{k}{n}$
$\frac{k+1}{n}$
$\frac{n-1}{n}$
1

Example 4.11


1
$f(x) = x^2$
$\frac{1}{n}\left(\frac{k}{n}\right)^2$
$\left(\frac{k+1}{n}\right)^2$
$\left(\frac{k}{n}\right)^2$
...
...
0
$\frac{1}{n}$
$\frac{k}{n}$
$\frac{k+1}{n}$
$\frac{n-1}{n}$
1

Full Calculation of $\int_0^1 x^2\,\mathrm{d}x$

[On Tuesday: I wrote n rather than $n-1$ as the upper limit in the sum at least twice. This was pointed out, but I only changed it once.]

By Example 4.10 we have

$$\sum_{k=1}^{n-1} \frac{1}{n}\Big(\frac{k}{n}\Big)^2 = \frac{1}{n^3}\sum_{k=1}^{n-1} k^2 = \frac{(n-1)n(2n-1)}{6n^3} = \frac{1}{3}\Big(1-\frac{1}{n}\Big)\Big(1-\frac{1}{2n}\Big).$$

Hence

$$\frac{1}{3}\Big(1-\frac{1}{n}\Big)\Big(1-\frac{1}{2n}\Big) \le \int_0^1 x^2\,\mathrm{d}x \le \frac{1}{3}\Big(1-\frac{1}{n}\Big)\Big(1-\frac{1}{2n}\Big) + \frac{1}{n}.$$

Now $1/n$ converges to 0 as n tends to infinity, and so the left-hand side and right-hand side both converge to $1/3$. Hence $\int_0^1 x^2\,\mathrm{d}x$ is sandwiched between two sequences that converge to $1/3$.
Therefore

$$\int_0^1 x^2\,\mathrm{d}x = \frac{1}{3}.$$

§5 Prime Numbers

In this section we will look at prime numbers and prime factorizations.

Division with remainder should be familiar from school. It is stated formally in the next theorem.

Theorem 5.1 (Examinable)

Let $n \in \mathbb{Z}$ and let $m \in \mathbb{N}$. There exist unique integers q and r such that $n = qm + r$ and $0 \leq r < m$.

§5 Prime Numbers

In this section we will look at prime numbers and prime factorizations.

Division with remainder should be familiar from school. It is stated formally in the next theorem.

Theorem 5.1 (Examinable)

Let $n \in \mathbb{Z}$ and let $m \in \mathbb{N}$. There exist unique integers q and r such that $n = qm + r$ and $0 \leq r < m$.

The proof shows that $q = \lfloor n/m \rfloor$ where $\lfloor x \rfloor$ is the floor function, seen in Question 3 of Sheet 2. So the existence part of the proof gives an effective way to find q.

Integer Division

We say that q is the *quotient*, and r is the *remainder* when n is divided by m. If $r = 0$ then we say that m *divides* n, or that n is a *multiple* of m.

Example 5.2

(i) Let $n = 44$ and $m = 6$. Then $44/6 = 7\frac{2}{6}$ and so, when 44 is divided by 6, the quotient is 7 and the remainder is 2. Note that for this calculation it is better to leave the fractional part as $\frac{2}{6}$ than to simplify it to $\frac{1}{3}$.

(ii) Let $n = 63$ and $m = 7$. Then $63/7 = 9$ so 7 divides 63. The quotient is 9 and the remainder is 0.

(iii) Since $-13 = -3 \times 6 + 5$, when -13 is divided by 6 the quotient is -3 and the remainder is 5.

Integer Division Exercise

Exercise 5.3

Find the quotient q and the remainder r when n is divided by m in each of these cases:

(i) $n = 20$, $m = 7$, (ii) $n = 21$, $m = 7$, (iii) $n = 22$, $m = 7$

(iv) $n = 7$, $m = 22$, (v) $m = -10$, $m = 7$, (vi) $n = 0$, $m = 1$.

Integer Division Exercise

Exercise 5.3

Find the quotient q and the remainder r when n is divided by m in each of these cases:

(i) $n = 20,\ m = 7,$ (ii) $n = 21,\ m = 7,$ (iii) $n = 22,\ m = 7$

(iv) $n = 7,\ m = 22,$ (v) $m = -10,\ m = 7,$ (vi) $n = 0,\ m = 1.$

Answers:

(i) $q = 2,\ r = 6,$ (ii) $q = 3,\ r = 0,$ (iii) $q = 3,\ r = 1$

Integer Division Exercise

Exercise 5.3

Find the quotient q and the remainder r when n is divided by m in each of these cases:

(i) $n = 20,\ m = 7,$ (ii) $n = 21,\ m = 7,$ (iii) $n = 22,\ m = 7$

(iv) $n = 7,\ m = 22,$ (v) $m = -10,\ m = 7,$ (vi) $n = 0,\ m = 1.$

Answers:

(i) $q = 2,\ r = 6,$ (ii) $q = 3,\ r = 0,$ (iii) $q = 3,\ r = 1$

(iv) $q = 0,\ r = 0,$ (v) $q = -2,\ r = 4,$ (vi) $q = 0,\ r = 0.$

Factorization Into Primes

Definition 5.4

Let $n \in \mathbb{N}$ and suppose that $n > 1$.

(i) We say that n is *prime* if the only natural numbers that divide n are 1 and n.

(ii) We say that n is *composite* if it is not prime.

The first few prime numbers are

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47,\ \ldots.$$

By Definition 5.4, the number 1 is neither prime nor composite.

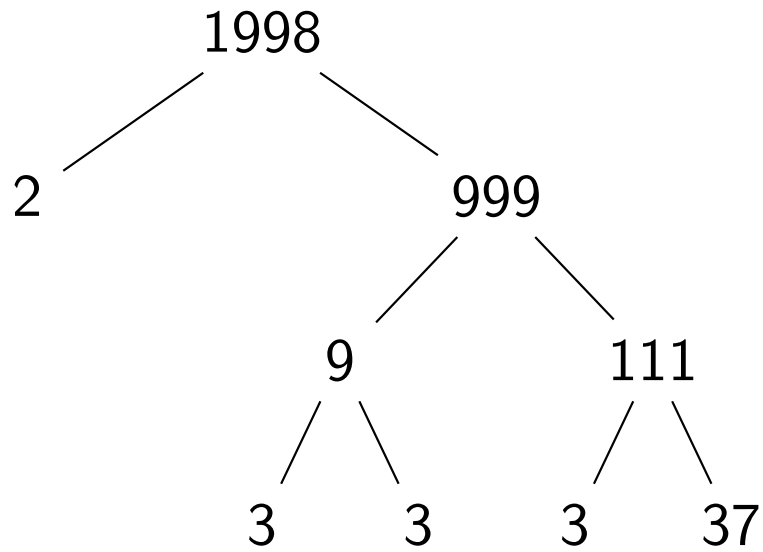
Prime Factorization Example

Example 5.5

Take $n = 1998$. We might spot that $n = 2 \times 999$ and that $999 = 9 \times 111$. Then $9 = 3 \times 3$, and $111 = 3 \times 37$, so

$$1998 = 2 \times 3 \times 3 \times 3 \times 37 = 2 \times 3^3 \times 37.$$

The tree below records these steps. (For some reason mathematical trees usually grow downwards.)



Infinitely Many Primes

The next theorem, due to Euclid, needs only the existence of prime factorizations, proved above.

Theorem 5.6 (Examinable)

There are infinitely many prime numbers.

Infinitely Many Primes

The next theorem, due to Euclid, needs only the existence of prime factorizations, proved above.

Theorem 5.6 (Examinable)

There are infinitely many prime numbers.

Exercise 5.7

The first five prime numbers are $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, $p_6 = 13$. Show that $p_1 + 1$, $p_1 p_2 + 1$, $p_1 p_2 p_3 + 1$, $p_1 p_2 p_3 p_4 + 1$ and $p_1 p_2 p_3 p_4 p_5 + 1$ are all prime, but

$$p_1 p_2 p_3 p_4 p_5 p_6 + 1 = 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 59 \times 509.$$

So the number N in Euclid's proof is not always prime.

Please Collect Work from Sheet 5

- A–K in green folder
- L–Z in red folder
- Older work: folders at front (please claim)

Questions 2, 4 and 5 were marked. Please see me if you have any queries. I have updated the model answers on Moodle with some feedback on common errors. Question 4 on $\exp : \mathbb{C} \to \mathbb{C}$:

(a) Not surjective since $\exp z = 0$ has no solution.

(b) Not injective since $\exp 0 = \exp(2\pi i) = 1$. (Or in Question 3 you should have found infinitely many z such that $\exp z = 1 + i$.)

(c) $L = \{2 + ib : b \in \mathbb{R}\} \implies$

$$\begin{aligned}\{\exp z : z \in L\} &= \{\mathrm{e}^2 \mathrm{e}^{ib} : b \in \mathbb{R}\} \\ &= \{\mathrm{e}^2(\cos b + i \sin b) : b \in \mathbb{R}\} \\ &= \text{circle of radius } \mathrm{e}^2.\end{aligned}$$

(d) See model answers: restrict imaginary part to a range of 2π.

Divisibility by 3

Let $n \in \mathbb{Z}$. You may have seen this rule before:

$$n \text{ is divisible by } 3 \iff \begin{array}{l}\text{the sum of the (decimal) digits} \\ \text{of } n \text{ is divisible by } 3.\end{array}$$

Divisibility by 3

Let $n \in \mathbb{Z}$. You may have seen this rule before:

$$n \text{ is divisible by } 3 \iff \begin{array}{l}\text{the sum of the (decimal) digits} \\ \text{of } n \text{ is divisible by } 3.\end{array}$$

Quiz:

(A) Is 123 divisible by 3?
(B) Is 1001 divisible by 3?
(C) Is 123456789123456789 divisible by 3?
(D) What is the remainder when 1267 is divided by 3?

Divisibility by 3

Let $n \in \mathbb{Z}$. You may have seen this rule before:

$$n \text{ is divisible by } 3 \iff \begin{array}{l}\text{the sum of the (decimal) digits} \\ \text{of } n \text{ is divisible by } 3.\end{array}$$

Quiz:

(A) Is 123 divisible by 3? Yes

(B) Is 1001 divisible by 3?

(C) Is 123456789123456789 divisible by 3?

(D) What is the remainder when 1267 is divided by 3?

Divisibility by 3

Let $n \in \mathbb{Z}$. You may have seen this rule before:

$$n \text{ is divisible by } 3 \iff \begin{array}{l}\text{the sum of the (decimal) digits} \\ \text{of } n \text{ is divisible by } 3.\end{array}$$

Quiz:

(A) Is 123 divisible by 3? Yes

(B) Is 1001 divisible by 3? No

(C) Is 123456789123456789 divisible by 3?

(D) What is the remainder when 1267 is divided by 3?

Divisibility by 3

Let $n \in \mathbb{Z}$. You may have seen this rule before:

$$n \text{ is divisible by } 3 \iff \begin{array}{l}\text{the sum of the (decimal) digits} \\ \text{of } n \text{ is divisible by } 3.\end{array}$$

Quiz:

(A) Is 123 divisible by 3? Yes

(B) Is 1001 divisible by 3? No

(C) Is 123456789123456789 divisible by 3? Yes

(D) What is the remainder when 1267 is divided by 3?

Divisibility by 3

Let $n \in \mathbb{Z}$. You may have seen this rule before:

$$n \text{ is divisible by } 3 \iff \begin{array}{l}\text{the sum of the (decimal) digits} \\ \text{of } n \text{ is divisible by } 3.\end{array}$$

Quiz:

(A) Is 123 divisible by 3? Yes

(B) Is 1001 divisible by 3? No

(C) Is 123456789123456789 divisible by 3? Yes

(D) What is the remainder when 1267 is divided by 3? 1

Divisibility by 3

Let $n \in \mathbb{Z}$. You may have seen this rule before:

$$n \text{ is divisible by } 3 \iff \begin{array}{l}\text{the sum of the (decimal) digits}\\ \text{of } n \text{ is divisible by } 3.\end{array}$$

Quiz:

(A) Is 123 divisible by 3? Yes

(B) Is 1001 divisible by 3? No

(C) Is 12345678912345678 9 divisible by 3? Yes

(D) What is the remainder when 1267 is divided by 3? 1

The point of proofs is to try to show *why* things are true. Without using the dread word 'proof', I will try to show you why the rule works. Example:

Divisibility by 3

Let $n \in \mathbb{Z}$. You may have seen this rule before:

$$n \text{ is divisible by } 3 \iff \begin{array}{l}\text{the sum of the (decimal) digits}\\ \text{of } n \text{ is divisible by } 3.\end{array}$$

Quiz:

(A) Is 123 divisible by 3? Yes

(B) Is 1001 divisible by 3? No

(C) Is 123456789123456789 divisible by 3? Yes

(D) What is the remainder when 1267 is divided by 3? 1

The point of proofs is to try to show *why* things are true. Without using the dread word 'proof', I will try to show you why the rule works. Example:

$$1267 = \mathbf{1} \times 1000 + \mathbf{2} \times 100 + \mathbf{6} \times 10 + \mathbf{7} \times 1$$

Divisibility by 3

Let $n \in \mathbb{Z}$. You may have seen this rule before:

$$n \text{ is divisible by } 3 \iff \begin{array}{l}\text{the sum of the (decimal) digits}\\ \text{of } n \text{ is divisible by } 3.\end{array}$$

Quiz:

(A) Is 123 divisible by 3? Yes

(B) Is 1001 divisible by 3? No

(C) Is 123456789123456789 divisible by 3? Yes

(D) What is the remainder when 1267 is divided by 3? 1

The point of proofs is to try to show *why* things are true. Without using the dread word 'proof', I will try to show you why the rule works. Example:

$$\begin{aligned}1267 &= \mathbf{1} \times 1000 + \mathbf{2} \times 100 + \mathbf{6} \times 10 + \mathbf{7} \times 1\\ &= \mathbf{1} \times (3 \times 333 + 1) + \mathbf{2} \times (3 \times 33 + 1) + \mathbf{6} \times (3 \times 3 + 1) + \mathbf{7} \times 1\end{aligned}$$

Divisibility by 3

Let $n \in \mathbb{Z}$. You may have seen this rule before:

$$n \text{ is divisible by } 3 \iff \begin{array}{l}\text{the sum of the (decimal) digits}\\ \text{of } n \text{ is divisible by } 3.\end{array}$$

Quiz:

(A) Is 123 divisible by 3? Yes

(B) Is 1001 divisible by 3? No

(C) Is 123456789123456789 divisible by 3? Yes

(D) What is the remainder when 1267 is divided by 3? 1

The point of proofs is to try to show *why* things are true. Without using the dread word 'proof', I will try to show you why the rule works. Example:

$$\begin{aligned}1267 &= \mathbf{1} \times 1000 + \mathbf{2} \times 100 + \mathbf{6} \times 10 + \mathbf{7} \times 1\\ &= \mathbf{1} \times (3 \times 333 + 1) + \mathbf{2} \times (3 \times 33 + 1) + \mathbf{6} \times (3 \times 3 + 1) + \mathbf{7} \times 1\\ &= 3 \times (\mathbf{1} \times 333 + \mathbf{2} \times 33 + \mathbf{6} \times 3) + \mathbf{1} \times 1 + \mathbf{2} \times 1 + \mathbf{6} \times 1 + \mathbf{7} \times 1\end{aligned}$$

Divisibility by 3

Let $n \in \mathbb{Z}$. You may have seen this rule before:

$$n \text{ is divisible by } 3 \iff \begin{array}{l}\text{the sum of the (decimal) digits}\\ \text{of } n \text{ is divisible by } 3.\end{array}$$

Quiz:

(A) Is 123 divisible by 3? Yes

(B) Is 1001 divisible by 3? No

(C) Is 12345678912345678 9 divisible by 3? Yes

(D) What is the remainder when 1267 is divided by 3? 1

The point of proofs is to try to show *why* things are true. Without using the dread word 'proof', I will try to show you why the rule works. Example:

$$\begin{aligned}1267 &= \mathbf{1}\times 1000 + \mathbf{2}\times 100 + \mathbf{6}\times 10 + \mathbf{7}\times 1\\ &= \mathbf{1}\times(3\times 333+1) + \mathbf{2}\times(3\times 33+1) + \mathbf{6}\times(3\times 3+1) + \mathbf{7}\times 1\\ &= 3\times(\mathbf{1}\times 333 + \mathbf{2}\times 33 + \mathbf{6}\times 3) + \mathbf{1}\times 1 + \mathbf{2}\times 1 + \mathbf{6}\times 1 + \mathbf{7}\times 1\\ &= 3\times(\mathbf{1}\times 333 + \mathbf{2}\times 33 + \mathbf{6}\times 3) + (\mathbf{1}+\mathbf{2}+\mathbf{6}+\mathbf{7})\end{aligned}$$

Unique factorization

Let $\mathbb{N}_0$ be the set $\{0, 1, 2, 3, \ldots\}$ of the natural numbers *together with* 0.

Theorem 5.8 (Fundamental Theorem of Arithmetic)

Let $n \in \mathbb{N}$. Let $p_1, p_2, p_3, \ldots$ be the primes in increasing order. There exists unique $e_i \in \mathbb{N}_0$ such that

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots.$$

Unique factorization

Let $\mathbb{N}_0$ be the set $\{0, 1, 2, 3, \ldots\}$ of the natural numbers *together with* 0.

Theorem 5.8 (Fundamental Theorem of Arithmetic)

Let $n \in \mathbb{N}$. Let $p_1, p_2, p_3, \ldots$ be the primes in increasing order. There exists unique $e_i \in \mathbb{N}_0$ such that

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots .$$

Writing out prime factorizations in the form in this theorem is a bit long-winded. For example

$$31460 = 2^2 \times 3^0 \times 5^1 \times 7^0 \times 11^2 \times 13^1 \times 17^0 \times 19^0 \ldots,$$

where all the exponents of the primes 17 or more are zero. But thinking about prime factorizations in this way is useful in proofs.

Irrational Numbers (Proved Using Unique Factorization)

Example 5.9

A manufacturer of cheap calculators claims to you that $\sqrt{3} = \frac{2148105}{1240209}$. Calculate the prime factorizations of 2148105 and 1240209 (in principle you could do this by repeated division, even using one of his cheapest calculators). Hence show that he is wrong.

Irrational Numbers (Proved Using Unique Factorization)

Example 5.9

A manufacturer of cheap calculators claims to you that $\sqrt{3} = \frac{2148105}{1240209}$. Calculate the prime factorizations of 2148105 and 1240209 (in principle you could do this by repeated division, even using one of his cheapest calculators). Hence show that he is wrong.

The prime factorizations are

$$2148105 = 3 \times 5 \times 71 \times 2017$$

$$1240209 = 3^2 \times 41 \times 3361.$$

Irrational Numbers (Proved Using Unique Factorization)

Example 5.9

A manufacturer of cheap calculators claims to you that $\sqrt{3} = \frac{2148105}{1240209}$. Calculate the prime factorizations of 2148105 and 1240209 (in principle you could do this by repeated division, even using one of his cheapest calculators). Hence show that he is wrong.

The prime factorizations are

$$2148105 = 3 \times 5 \times 71 \times 2017$$
$$1240209 = 3^2 \times 41 \times 3361.$$

Now

$$\begin{aligned} \sqrt{3} = \frac{2148105}{1240209} &\implies \sqrt{3} \times 1240209 = 2148105 \\ &\implies 3 \times 1240209^2 = 2148105^2 \\ &\implies 3 \times 3^4 \times 41^2 \times 3361^2 = 3^2 \times 5^2 \times 71^2 \times 2017^2. \end{aligned}$$

This contradicts unique factorization.

- Please hand in work for Sheet 6 promptly at the end of the lecture.
- If you miss me, please leave in the box outside my office by 5pm.

Claim 5.10

$\sqrt{3}$ is an irrational number.

We will prove Claim 5.10 using *proof by contradiction*. While related, this is not the same proof by contradiction you will have seen if you are doing 194 Numbers and Functions.

All we do in the proof is generalize the pattern from Example 5.9. Suppose someone claims to you that

$$\sqrt{3} = \frac{362}{209}.$$

This implies that

$$3 \times 209^2 = 362^2.$$

Take prime factorizations and get contradiction.

$$3 \times 11^2 \times 19^2 = 2^2 \times 181^2.$$

Binary and Other Bases

Example 5.11

To write 145 in base 3:

Divide 145 by 3:	$145 = 48 \times 3 + \mathbf{1}$
Divide the quotient 48 by 3:	$48 = 16 \times 3 + \mathbf{0}$
Divide the quotient 16 by 3:	$16 = 5 \times 3 + \mathbf{1}$
Divide the quotient 5 by 3:	$5 = 1 \times 3 + \mathbf{2}$
Divide the quotient 1 by 3:	$1 = 0 \times 3 + \mathbf{1}$

We now stop, because the last quotient was 0. Reading the list of remainders from bottom to top we get

$$145 = 1 \times 3^4 + 2 \times 3^3 + 1 \times 3^2 + 0 \times 3^1 + 1 \times 3^0.$$

Hence 145 is 12101 in base 3. We write this as $145 = 12101_3$.

Our usual way of writing numbers uses base 10. If no base is specified, as is usually the case, then base 10 is intended.

Writing a Number in Base b

The example above should suggest a general algorithm.

Algorithm 5.12

Let $n \in \mathbb{N}$ and let $b \in \mathbb{N}$. To write n in base b, divide n by b, then divide the quotient by b, and so on, until the quotient is 0. If $r_0, r_1, r_2, \ldots, r_k$ is the sequence of remainders then

$$n = r_k b^k + r_{k-1} b^{k-1} + \cdots + r_1 b + r_0$$

and $n = (r_k r_{k-1} \ldots r_1 r_0)_b$.

In Example 5.11, the base was 3 and the sequence of remainders was $r_0 = 1$, $r_1 = 0$, $r_2 = 1$, $r_3 = 2$ and $r_4 = 1$.

If time permits we will prove that the algorithm is correct by induction on k, taking as the base case $k = 0$.

Binary

Base 2 is known as *binary*. Binary is particularly important because computers store and process data as sequences of the *bi*nary digi*ts*, or *bits*, 0 and 1.

Exercise 5.13

Show that $21 = 10101_2$ and write 63, 64 and 65 in binary.

Exercise 5.14

Let $n = r_k r_{k-1} \dots r_1 r_0$ be a number written in binary. Describe, in terms of operations on the string of bits $r_k r_{k-1} \dots r_1 r_0$, how to

(i) Multiply n by 2,

(ii) Add 1 to n,

(iii) Subtract 1 from n,

(iv) Find the quotient and remainder when n is divided by 2.

[*Hint:* for base 10, you probably learned how to do these at school. The MATHEMATICA command `BaseForm[n,2]` will write $n \in \mathbb{N}_0$ in binary.]

Binary and Computers

In a modern computer, everything is stored as a lists of the **bits** (**bi**nary digi**ts**) 0 and 1.

Binary and Computers

In a modern computer, everything is stored as a lists of the **bits** (**bi**nary digi**ts**) 0 and 1. For example, the number 12 could be stored as 1100, corresponding to the sequence of answers 'Yes', 'No', 'Yes', 'Yes'.

Binary and Computers

In a modern computer, everything is stored as a lists of the **bits** (**bi**nary digi**ts**) 0 and 1. For example, the number 12 could be stored as 1100, corresponding to the sequence of answers 'Yes', 'No', 'Yes', 'Yes'.

Books, music, videos, computer programs, bitcoins . . . , are all stored as bits.

Binary and Computers

In a modern computer, everything is stored as a lists of the **bits** (**bi**nary digi**ts**) 0 and 1. For example, the number 12 could be stored as 1100, corresponding to the sequence of answers 'Yes', 'No', 'Yes', 'Yes'.

Books, music, videos, computer programs, bitcoins . . . , are all stored as bits.

01100010 00101011 11101010 00101111 00101110 10101100 11101011 10101010
00100000 10101101 00101111 11101011 00101011 10101011 00101001 10101100
00101110 00101111 11101011 00100000 10101010 11101011 00100000 10101101
10101111 11101011 10101100 10101100 00101001 00100000 00101010 11101010
00101001 00100000 10101101 10101011 11101010 01101001 01101010 10101101
00100000 00101011 01101000 00001110 11000000 10101100 00101011 10101010
10101010 00101111 10101101 00100000 11101011 00101110 00100000 00101010
11101010 01101001 01101011 00100000 00101011 01101000 00101110 00100000
11101010 01101001 00100000 10101100 00101011 01101010 10101000 11101011
11101010 00100000 10101101 01101001 00101110 10100011 00100000 10101100
00101011 01101000 00101110 00101011 01101000 10001111 11000000 11100100
11101010 11101011 01101001 00101110 10101101 00101011 00101111 00101101
00100000 00101011 01101000 00101110 00100000 10101101 01101001 00100000
00101110 00101001 01101000 00101110 00100000 11100100 00101011 10101000
00100000 11101011 00101110 00100000 00101110 11101011 11101010 00100000
10101100 11101011 00100000 01100010 00101011 10101000 00100000 11101011
00001110

William Shakespeare (approx 1600)

Binary and Computers

In a modern computer, everything is stored as a lists of the **bits** (**bi**nary digi**ts**) 0 and 1. For example, the number 12 could be stored as 1100, corresponding to the sequence of answers 'Yes', 'No', 'Yes', 'Yes'.

Books, music, videos, computer programs, bitcoins . . . , are all stored as bits.

01100010 00101011 11101010 00101111 00101110 10101100 11101011 10101010
00100000 10101101 00101111 11101011 00101011 10101011 00101001 10101100
00101110 00101111 11101011 00100000 10101010 11101011 00100000 10101101
10101111 11101011 10101100 10101100 00101001 00100000 00101010 11101010
00101001 00100000 10101101 10101011 11101010 01101001 01101010 10101101
00100000 00101011 01101000 00001110 11000000 10101100 00101011 10101010
10101010 00101111 10101101 00100000 11101011 00101110 00100000 00101010
11101010 01101001 01101011 00100000 00101011 01101000 00101110 00100000
11101010 01101001 00100000 10101100 00101011 01101010 10101000 11101011
11101010 00100000 10101101 01101001 00101110 10100011 00100000 10101100
00101011 01101000 00101110 00101011 01101000 10001111 11000000 11100100
11101010 11101011 01101001 00101110 10101101 00101011 00101111 00101101
00100000 00101011 01101000 00101110 00100000 10101101 01101001 00100000
00101110 00101001 01101000 00101110 00100000 11100100 00101011 10101000
00100000 11101011 00101110 00100000 00101110 11101011 11101010 00100000
10101100 11101011 00100000 01100010 00101011 10101000 00100000 11101011
00001110

William Shakespeare (approx 1600)

To be, or not to be: that is the question:
Whether 'tis nobler in the mind to suffer
The slings and arrows of outrageous fortune,

Binary and Computers

In a modern computer, everything is stored as a lists of the **bits** (**bi**nary digi**ts**) 0 and 1. For example, the number 12 could be stored as 1100, corresponding to the sequence of answers 'Yes', 'No', 'Yes', 'Yes'.

Books, music, videos, computer programs, bitcoins . . . , are all stored as bits.

00110000 01110111 01000110 10000000 00011000 00000001 01011101 00011110
10101100 00000000 10101110 00001011 10101100 00101011 01101011 01101001
00001110 00101110 10101100 00101001 00101110 10001101 00100100 00100101
10101100 00101011 01101011 01101001 00001110 00001111 10001000 01001011
01100100 11001010 11001100 11001111 11001111 00001000 00000101 00010100
00001100 00110000 01000000 01011010 00110000 11000010 00110000 00110000
10000000 00011010 00111010 00110000 10000110 10111101 00011010 10101100
00000000 00001011 00101110 10101001 00101011 11101000 10101000 11001011
10001001 10100111 10101001 10101010 11001011 10100101 11001010 01001001
00001110 11001100 11001111 11001111 00001000 00010100 10000001 01011010
00110000 01000101 00010001 01111010 00110000 10100101 01011010 10101100
00000000 00001011 11101010 11101011 01101001 00101110 00101100 00101011
10101001 01101100 00001011 10101111 11101011 01101010 10101010 10101100
00101011 10101110 11001011 10101100 00101011 10101011 00101011 00101110
11101010 01001001 10001001 00100111 10100100 10101001 10101010 11001011
10100101 11001010 01001001 00001110 11001100 11001111 11001111 00001000
00010100

Anonymous Microsoft Programmer (2010?)

Binary and Computers

In a modern computer, everything is stored as a lists of the **bits** (**bi**nary digi**ts**) 0 and 1. For example, the number 12 could be stored as 1100, corresponding to the sequence of answers 'Yes', 'No', 'Yes', 'Yes'.

Books, music, videos, computer programs, bitcoins . . . , are all stored as bits.

00110000 01110111 01000110 10000000 00011000 00000001 01011101 00011110
10101100 00000000 10101110 00001011 10101100 00101011 01101011 01101001
00001110 00101110 10101100 00101001 00101110 10001101 00100100 00100101
10101100 00101011 01101011 01101001 00001110 00001111 10001000 01001011
01100100 11001010 11001100 11001111 11001111 00001000 00000101 00010100
00001100 00110000 01000000 01011010 00110000 11000010 00110000 00110000
10000000 00011010 00111010 00110000 10000110 10111101 00011010 10101100
00000000 00001011 00101110 10101001 00101011 11101000 10101000 11001011
10001001 10100111 10101001 10101010 11001011 10100101 11001010 01001001
00001110 11001100 11001111 11001111 00001000 00010100 10000001 01011010
00110000 01000101 00010001 01111010 00110000 10100101 01011010 10101100
00000000 00001011 11101010 11101011 01101001 00101110 00101100 00101011
10101001 01101100 00001011 10101111 11101011 01101010 10101010 10101100
00101011 10101110 11001011 10101100 00101011 10101011 00101011 00101110
11101010 01001001 10001001 00100111 10100100 10101001 10101010 11001011
10100101 11001010 01001001 00001110 11001100 11001111 11001111 00001000
00010100

Anonymous Microsoft Programmer (2010?)

Part of the machine code for Microsoft Word 2011.

§6 Logic and proofs

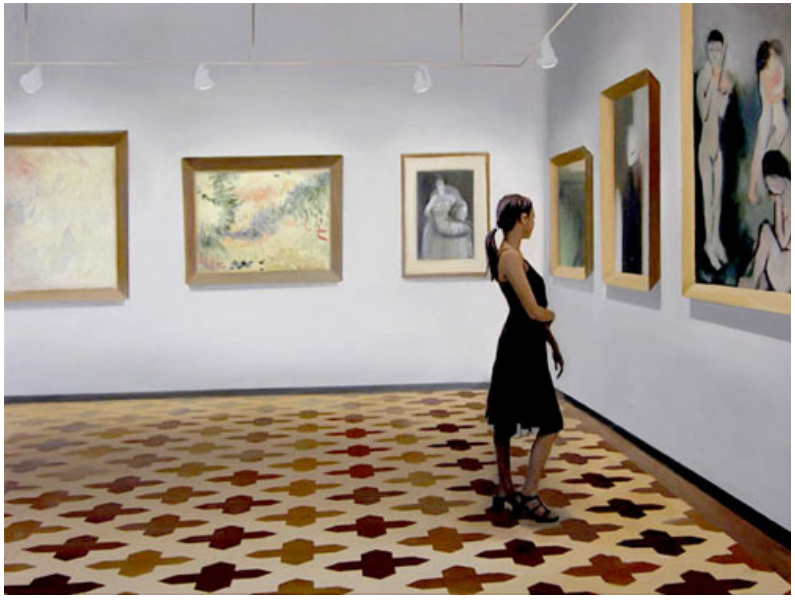
In pairs discuss the meaning of the following sentences. Each has two interpretations that are logically reasonable.

(1) The picture of the woman in the museum.
(2) The lady hit the man with an umbrella.
(3) Nurses help dog bite victim.
(4) Walk to Windsor or swim the Channel and climb the Matterhorn.

§6 Logic and proofs

In pairs discuss the meaning of the following sentences. Each has two interpretations that are logically reasonable.

(1) The picture of the woman in the museum.
(2) The lady hit the man with an umbrella.
(3) Nurses help dog bite victim.
(4) Walk to Windsor or swim the Channel and climb the Matterhorn.



§6 Logic and proofs

In pairs discuss the meaning of the following sentences. Each has two interpretations that are logically reasonable.

(1) The picture of the woman in the museum.
(2) The lady hit the man with an umbrella.
(3) Nurses help dog bite victim.
(4) Walk to Windsor or swim the Channel and climb the Matterhorn.

The ambiguities in everyday language are often resolved, either from the context, or because we are conditioned to expect one meaning. In mathematics we instead try to avoid ambiguity by careful use of mathematical language and symbols.

'And', 'or' and 'not'

One word that is used in mathematics in a way that may seem non-standard is 'or'. Let P and Q be propositions.

(i) P *or* Q, written $P \vee Q$, means at least one of P and Q is true.
(ii) P *and* Q, written $P \wedge Q$, means P and Q are both true.
(iii) *not* P, written $\neg P$, means that P is false.

There is a correspondence between the logical operations $\wedge$, $\vee$ and $\neg$ and the set operations $\cap$, $\cup$ and set complement.

Example 6.1

Consider the following propositions, depending on a natural number n.

$$P(n): \quad n \text{ is even}$$
$$Q(n): \quad n \text{ is a multiple of } 3$$
$$R(n): \quad n \text{ is prime}$$

Will discuss

(a) $\neg P(n) \wedge Q(n)$ (b) $P(n) \wedge Q(n)$ (c) $\neg P(n)$

and find $\{n \in \{1, 2, \ldots, 10\} : P(n) \wedge \big(Q(n) \vee R(n)\big)\}$.

Truth Tables and Implication

A concise way to specify a logical operation such as $\vee$, $\wedge$ or $\neg$ is by a *truth table*, such as the one below for $\vee$.

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

Recall that $P \Longrightarrow Q$ means 'if P is true then Q is true'. For the sake of argument, assume that $\Longrightarrow$ has a truth table. **Question:** what is it?

Truth Tables and Implication

A concise way to specify a logical operation such as $\vee$, $\wedge$ or $\neg$ is by a *truth table*, such as the one below for $\vee$.

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

Recall that $P \Longrightarrow Q$ means 'if P is true then Q is true'. For the sake of argument, assume that $\Longrightarrow$ has a truth table. **Question:** what is it?

Answer: Think of $P \Longrightarrow Q$ as a promise. The only time this promise is broken is if P is true and Q is false. So

> $P \Longrightarrow Q$ is false when P is true and Q is false, and true in all other cases

Please Collect Work from Sheet 6

- A–K in green folder
- L–Z in red folder
- Older work: folders at front (please claim)

Questions 4, 5 and 6 were marked and I looked briefly at Questions 2 and 7. Please see me if you have any queries. Will update model answers with feedback soon.

Question 2 on Towers of Hanoi. The point was to show that $2^n - 1$ moves are necessary to move n discs.

- Where are the discs? Many answers made no reference to the discs or pegs. Such an answer cannot be right.
- Why nothing faster? Many answers showed $2^n - 1$ moves suffice, but didn't show that there was no faster method.
- Several people wrote $P(n) = 2^n - 1$. But $P(n)$ should be a proposition: '$2^n - 1$ moves are necessary to move n discs', not a number.
- Some people assumed a recurrence relation $f(n) = 2f(n) + 1$, almost always without defining f. Not convincing.
- There were also a few excellent answers.

Exercise 6.2

Recall that $P \iff Q$ means that $P \implies Q$ and $Q \implies P$. Use the truth tables for $\implies$ and $\wedge$ to find the truth table for $\iff$.

Exercise 6.2

Recall that $P \iff Q$ means that $P \implies Q$ and $Q \implies P$. Use the truth tables for $\implies$ and $\wedge$ to find the truth table for $\iff$.

Exercise 6.3

Which of the following propositions are true for all $x \in \mathbb{R}$?

(a) $P(x)$: $x \geq 4 \implies x \geq 3$,

(b) $Q(x)$: $x \geq 3 \implies x \geq 4$,

(c) $R(x)$: $x^2 - 2x - 3 = 0 \implies x = -1$, $x = 3$ or $x = 37$,

(d) $S(x)$: $x \geq 0$ and $x^2 - 2x - 3 = 0 \implies x = 3$,

Which of the following propositions are true for all $x, y \in \mathbb{R}$?

(e) $T(x, y)$: $x^2 = y^2 \implies x = y$,

(f) $U(x, y)$: $x^3 = y^3 \implies x = y$.

In which of (c) and (d) can $\implies$ be replaced with $\iff$?

Exercise 6.2

Recall that $P \iff Q$ means that $P \implies Q$ and $Q \implies P$. Use the truth tables for $\implies$ and $\wedge$ to find the truth table for $\iff$.

Exercise 6.3

Which of the following propositions are true for all $x \in \mathbb{R}$?

(a) $P(x)$: $x \geq 4 \implies x \geq 3$, True

(b) $Q(x)$: $x \geq 3 \implies x \geq 4$,

(c) $R(x)$: $x^2 - 2x - 3 = 0 \implies x = -1$, $x = 3$ or $x = 37$,

(d) $S(x)$: $x \geq 0$ and $x^2 - 2x - 3 = 0 \implies x = 3$,

Which of the following propositions are true for all $x, y \in \mathbb{R}$?

(e) $T(x, y)$: $x^2 = y^2 \implies x = y$,

(f) $U(x, y)$: $x^3 = y^3 \implies x = y$.

In which of (c) and (d) can $\implies$ be replaced with $\iff$?

Exercise 6.2

Recall that $P \iff Q$ means that $P \implies Q$ and $Q \implies P$. Use the truth tables for $\implies$ and $\wedge$ to find the truth table for $\iff$.

Exercise 6.3

Which of the following propositions are true for all $x \in \mathbb{R}$?

(a) $P(x)$: $x \geq 4 \implies x \geq 3$, True

(b) $Q(x)$: $x \geq 3 \implies x \geq 4$, False

(c) $R(x)$: $x^2 - 2x - 3 = 0 \implies x = -1$, $x = 3$ or $x = 37$,

(d) $S(x)$: $x \geq 0$ and $x^2 - 2x - 3 = 0 \implies x = 3$,

Which of the following propositions are true for all $x, y \in \mathbb{R}$?

(e) $T(x, y)$: $x^2 = y^2 \implies x = y$,

(f) $U(x, y)$: $x^3 = y^3 \implies x = y$.

In which of (c) and (d) can $\implies$ be replaced with $\iff$?

Exercise 6.2

Recall that $P \iff Q$ means that $P \implies Q$ and $Q \implies P$. Use the truth tables for $\implies$ and $\wedge$ to find the truth table for $\iff$.

Exercise 6.3

Which of the following propositions are true for all $x \in \mathbb{R}$?

(a) $P(x)$: $x \geq 4 \implies x \geq 3$, True

(b) $Q(x)$: $x \geq 3 \implies x \geq 4$, False

(c) $R(x)$: $x^2 - 2x - 3 = 0 \implies x = -1$, $x = 3$ or $x = 37$, True

(d) $S(x)$: $x \geq 0$ and $x^2 - 2x - 3 = 0 \implies x = 3$,

Which of the following propositions are true for all $x, y \in \mathbb{R}$?

(e) $T(x, y)$: $x^2 = y^2 \implies x = y$,

(f) $U(x, y)$: $x^3 = y^3 \implies x = y$.

In which of (c) and (d) can $\implies$ be replaced with $\iff$?

Exercise 6.2

Recall that $P \iff Q$ means that $P \implies Q$ and $Q \implies P$. Use the truth tables for $\implies$ and $\wedge$ to find the truth table for $\iff$.

Exercise 6.3

Which of the following propositions are true for all $x \in \mathbb{R}$?

(a) $P(x)$: $x \geq 4 \implies x \geq 3$, True

(b) $Q(x)$: $x \geq 3 \implies x \geq 4$, False

(c) $R(x)$: $x^2 - 2x - 3 = 0 \implies x = -1$, $x = 3$ or $x = 37$, True

(d) $S(x)$: $x \geq 0$ and $x^2 - 2x - 3 = 0 \implies x = 3$, True

Which of the following propositions are true for all $x, y \in \mathbb{R}$?

(e) $T(x, y)$: $x^2 = y^2 \implies x = y$,

(f) $U(x, y)$: $x^3 = y^3 \implies x = y$.

In which of (c) and (d) can $\implies$ be replaced with $\iff$?

Exercise 6.2

Recall that $P \iff Q$ means that $P \implies Q$ and $Q \implies P$. Use the truth tables for $\implies$ and $\wedge$ to find the truth table for $\iff$.

Exercise 6.3

Which of the following propositions are true for all $x \in \mathbb{R}$?

(a) $P(x)$: $x \geq 4 \implies x \geq 3$, True

(b) $Q(x)$: $x \geq 3 \implies x \geq 4$, False

(c) $R(x)$: $x^2 - 2x - 3 = 0 \implies x = -1$, $x = 3$ or $x = 37$, True

(d) $S(x)$: $x \geq 0$ and $x^2 - 2x - 3 = 0 \implies x = 3$, True

Which of the following propositions are true for all $x, y \in \mathbb{R}$?

(e) $T(x, y)$: $x^2 = y^2 \implies x = y$, False

(f) $U(x, y)$: $x^3 = y^3 \implies x = y$.

In which of (c) and (d) can $\implies$ be replaced with $\iff$?

Exercise 6.2

Recall that $P \iff Q$ means that $P \implies Q$ and $Q \implies P$. Use the truth tables for $\implies$ and $\wedge$ to find the truth table for $\iff$.

Exercise 6.3

Which of the following propositions are true for all $x \in \mathbb{R}$?

(a) $P(x)$: $x \geq 4 \implies x \geq 3$, True

(b) $Q(x)$: $x \geq 3 \implies x \geq 4$, False

(c) $R(x)$: $x^2 - 2x - 3 = 0 \implies x = -1$, $x = 3$ or $x = 37$, True

(d) $S(x)$: $x \geq 0$ and $x^2 - 2x - 3 = 0 \implies x = 3$, True

Which of the following propositions are true for all $x, y \in \mathbb{R}$?

(e) $T(x, y)$: $x^2 = y^2 \implies x = y$, False

(f) $U(x, y)$: $x^3 = y^3 \implies x = y$. True

In which of (c) and (d) can $\implies$ be replaced with $\iff$?

Exercise 6.2

Recall that $P \iff Q$ means that $P \implies Q$ and $Q \implies P$. Use the truth tables for $\implies$ and $\wedge$ to find the truth table for $\iff$.

Exercise 6.3

Which of the following propositions are true for all $x \in \mathbb{R}$?

(a) $P(x)$: $x \geq 4 \implies x \geq 3$, True

(b) $Q(x)$: $x \geq 3 \implies x \geq 4$, False

(c) $R(x)$: $x^2 - 2x - 3 = 0 \implies x = -1$, $x = 3$ or $x = 37$, True

(d) $S(x)$: $x \geq 0$ and $x^2 - 2x - 3 = 0 \implies x = 3$, True

Which of the following propositions are true for all $x, y \in \mathbb{R}$?

(e) $T(x, y)$: $x^2 = y^2 \implies x = y$, False

(f) $U(x, y)$: $x^3 = y^3 \implies x = y$. True

In which of (c) and (d) can $\implies$ be replaced with $\iff$?

Logically $P \implies Q$ says nothing about $Q \implies P$. This was already seen in Example 1.6 and in (c) above.

Example 6.4

Suppose we want to find all $x \in \mathbb{R}$ such that

$$\sqrt{x+3} = x+1.$$

There is a correct chain of implications: $\sqrt{x+3} = x+1 \Longrightarrow x+3 = (x+1)^2 \Longrightarrow x^2+x-2 = 0 \Longrightarrow (x+2)(x-1) = 0$. But because the first implication sign is not reversible, it does not follow that both -2 and 1 are solutions.

Exercise 6.5

Each of Persons A, B, C is either a *Knight* who always tells the truth, or a *Knave*, who always lies.

(a) Person A says 'If I'm a Knight then I'll give you £1000'. What do you conclude?

(b) Person B says of Person C: 'If C is a Knight then I am a Knave'. Deduce the identities of B and C.

Logical equivalence and Tautologies

Definition 6.6

Let P and Q be propositions. If $P \iff Q$ is true then we say that P and Q are *logically equivalent*. If a proposition is always true, then it is said to be a *tautology*.

Claim 6.7 (De Morgan's Laws for propositions)

Let P and Q be propositions. Then the following are tautologies:

(i) $\neg(P \vee Q) \iff \neg P \wedge \neg Q$,

(ii) $\neg(P \wedge Q) \iff \neg P \vee \neg Q$.

The proof of (ii) is left to you in Question 2(c) on Sheet 7. It can be more illuminating not to use truth tables. Example: will show that

$$\big((P \implies Q) \wedge (Q \implies R)\big) \implies (P \implies R)$$

is a tautology. (This is Question 2(f) on Sheet 7.)

Proof by Contrapositive

The next claim can be proved easily using a truth table. But I am going to give you a direct proof since this seems best to explain *why* it is true.

Claim 6.8

Let P and Q be propositions. Then $P \implies Q$ and $\neg Q \implies \neg P$ are logically equivalent.

Switching to the contrapositive can be useful first step in a proof, particularly when statements appear in negated form.

Claim 6.9

Let $a \in \mathbb{Q}$ be non-zero and let $x \in \mathbb{R}$. If $x \notin \mathbb{Q}$ then $ax \notin \mathbb{Q}$.

Example 6.10 (See printed notes)

If $f : X \to Y$ and $g : Y \to Z$ are functions then

$$gf \text{ surjective} \implies g \text{ surjective.}$$

Quiz

(1) Cards. You are shown a number of cards. Each card has a letter printed on one side, and a number printed on the other. Four cards are put on a table. You can see:

(A) o (B) t (C) 5 (D) 6

Which cards would you turn over to test the conjecture: 'If a card has a vowel on one side then it has a prime on the other'? (Turn over all the cards that might disprove the conjecture.)

Quiz

(1) Cards. You are shown a number of cards. Each card has a letter printed on one side, and a number printed on the other. Four cards are put on a table. You can see:

(A) o (B) t (C) 5 (D) 6

Which cards would you turn over to test the conjecture: 'If a card has a vowel on one side then it has a prime on the other'? (Turn over all the cards that might disprove the conjecture.)

(2) Alcohol. In the far-off land of Erewhon, only people over the age of 18 are allowed to drink alcohol in public. If your job is to enforce this law, who of the following would you investigate?

(A) A person drinking a glass of wine

(B) A person drinking coke

(C) Someone clearly over 50 with an unidentifable drink

(D) Someone who looks about 16 with an unidentifiable drink

(Investigate all the people who might be committing an offence.)

Quiz (Wason Selection Task)

(1) Cards. You are shown a number of cards. Each card has a letter printed on one side, and a number printed on the other. Four cards are put on a table. You can see:

(A) o (B) t (C) 5 (D) 6

Which cards would you turn over to test the conjecture: 'If a card has a vowel on one side then it has a prime on the other'? (Turn over all the cards that might disprove the conjecture.)

(2) Alcohol. In the far-off land of Erewhon, only people over the age of 18 are allowed to drink alcohol in public. If your job is to enforce this law, who of the following would you investigate?

(A) A person drinking a glass of wine

(B) A person drinking coke

(C) Someone clearly over 50 with an unidentifable drink

(D) Someone who looks about 16 with an unidentifiable drink

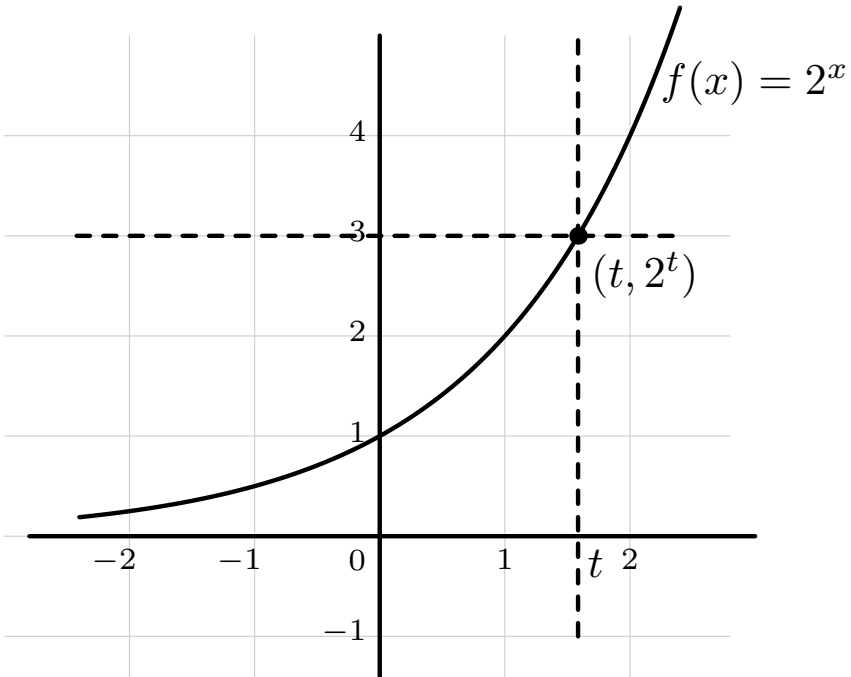
(Investigate all the people who might be committing an offence.)

Proof by Contradiction

Let P be a proposition. In a proof by contradiction, we suppose that P is false, so $\neg P$ is true. We then show that $\neg P \implies C$ where C is a false statement. Since a true statement does not imply a false statement, $\neg P$ must be false. So P is true.

Example 6.11

The function $f : \mathbb{R} \to \mathbb{R}_{>0}$ defined by $f(x) = 2^x$ is bijective, so there exists a unique $t \in \mathbb{R}$ such that $2^t = 3$. We will use proof by contradiction to show that t is irrational.



‘For all’ and ‘exists’

Let $P(x)$ be a propositions depending on an element x of a set X.

- If $P(x)$ is true for all $x \in X$, then we write $(\forall x \in X)\, P(x)$.
- If there exists an element $x \in X$ such that $P(x)$ is true, then we write $(\exists x \in X)\, P(x)$.

The negation of

- $(\forall x \in X)\, P(x)$ is $(\exists x \in X)\, \neg P(x)$.
- $(\exists x \in X)\, P(x)$ is $(\forall x \in X)\, \neg P(x)$.

'For all' and 'exists'

Let $P(x)$ be a propositions depending on an element x of a set X.

- If $P(x)$ is true for all $x \in X$, then we write $(\forall x \in X)\, P(x)$.
- If there exists an element $x \in X$ such that $P(x)$ is true, then we write $(\exists x \in X)\, P(x)$.

The negation of

- $(\forall x \in X)\, P(x)$ is $(\exists x \in X)\, \neg P(x)$.
- $(\exists x \in X)\, P(x)$ is $(\forall x \in X)\, \neg P(x)$.

Exercise 6.12

State the truth value of each of the propositions below. Justify your answers.

$$P\colon (\forall m \in \mathbb{Z})(4 \text{ divides } m^2)$$

$$Q\colon (\exists m \in \mathbb{Z})(4 \text{ divides } m^2)$$

$$R\colon (\forall m \in \mathbb{Z})(\exists n \in \mathbb{N})(m+n \text{ is even})$$

$$S\colon (\exists m \in \mathbb{Z})(\forall n \in \mathbb{N})(m+n \text{ is even})$$

[*Hint for S:* it may be easier to argue that $\neg S$ is true.]

'For all' and 'exists'

Let $P(x)$ be a propositions depending on an element x of a set X.

- If $P(x)$ is true for all $x \in X$, then we write $(\forall x \in X)\, P(x)$.
- If there exists an element $x \in X$ such that $P(x)$ is true, then we write $(\exists x \in X)\, P(x)$.

The negation of

- $(\forall x \in X)\, P(x)$ is $(\exists x \in X)\, \neg P(x)$.
- $(\exists x \in X)\, P(x)$ is $(\forall x \in X)\, \neg P(x)$.

Exercise 6.12

State the truth value of each of the propositions below. Justify your answers.

$$P\colon (\forall m \in \mathbb{Z})(4 \text{ divides } m^2)$$

$$Q\colon (\exists m \in \mathbb{Z})(4 \text{ divides } m^2)$$

$$R\colon (\forall m \in \mathbb{Z})(\exists n \in \mathbb{N})(m+n \text{ is even})$$

$$S\colon (\exists m \in \mathbb{Z})(\forall n \in \mathbb{N})(m+n \text{ is even})$$

[*Hint for S:* it may be easier to argue that $\neg S$ is true.]

More Quantifiers

Exercise 6.13

Sometimes the set X in $\forall x \in X$ is indicated by inequalities.

$(\forall \epsilon > 0)\, Q(\epsilon)$ means that $Q(\epsilon)$ is true for all ϵ in the set of positive real numbers,

$(\forall n > N)\, S(n)$ means that $S(n)$ is true for all $n \in \mathbb{N}$ such that $n > N$.

Let $a_1, a_2, a_3, \ldots$ be real numbers. Let $\ell \in \mathbb{R}$. Write down the negation of

$$(\forall \epsilon > 0)(\exists N \in \mathbb{N})(\forall n \geq N)\ |a_n - \ell| < \epsilon.$$

More Quantifiers

Exercise 6.13

Sometimes the set X in $\forall x \in X$ is indicated by inequalities.

$(\forall \epsilon > 0)\, Q(\epsilon)$ means that $Q(\epsilon)$ is true for all ϵ in the set of positive real numbers,

$(\forall n > N)\, S(n)$ means that $S(n)$ is true for all $n \in \mathbb{N}$ such that $n > N$.

Let $a_1, a_2, a_3, \ldots$ be real numbers. Let $\ell \in \mathbb{R}$. Write down the negation of

$$(\forall \epsilon > 0)(\exists N \in \mathbb{N})(\forall n \geq N)\ |a_n - \ell| < \epsilon.$$

Exercise 6.14

Let X be the set of people doing 181 and for $x \in X$ let $P(x)$ be the proposition 'x submitted answers to Sheet 6'. Show that

$$(\exists x \in X)\big(P(x) \Longrightarrow (\forall x \in X) P(x)\big).$$

Extras: Exercise 6.15. Assume P, Q, R.

P: If it is raining then the sky is cloudy.

Q: If it rains in the morning then Prof. X carries his umbrella all day.

R: People who carry umbrellas never get soaked.

Which of the following statements can be deduced from P, Q and R?

A: A cloudy sky is a necessary condition for rain.

B: A cloudy sky is a sufficient condition for rain.

C: It is raining only if the sky is cloudy.

D: Rain in the morning is a necessary condition for Prof. X to carry his umbrella.

E: Rain in the morning is a sufficient condition for Prof. X to carry his umbrella.

F: Rain falling implies that the sky is cloudy.

G: The sky is cloudy implies that rain is falling.

H: If Prof. X is soaked then it did not rain this morning.

Extras: Exercise 6.15. Assume P, Q, R.

P: If it is raining then the sky is cloudy.

$$\text{RAIN} \Longrightarrow \text{CLOUD}$$

Q: If it rains in the morning then Prof. X carries his umbrella all day.

$$\text{MORNING RAIN} \Longrightarrow \text{UMBRELLA}$$

R: People who carry umbrellas never get soaked.

$$\text{UMBRELLA} \Longrightarrow \text{NOT SOAKED}$$

Which of the following statements can be deduced from P, Q and R?

A: A cloudy sky is a necessary condition for rain.

B: A cloudy sky is a sufficient condition for rain.

C: It is raining only if the sky is cloudy.

D: Rain in the morning is a necessary condition for Prof. X to carry his umbrella.

E: Rain in the morning is a sufficient condition for Prof. X to carry his umbrella.

F: Rain falling implies that the sky is cloudy.

G: The sky is cloudy implies that rain is falling.

H: If Prof. X is soaked then it did not rain this morning.

Extras: Exercise 6.15. Assume P, Q, R.

P: If it is raining then the sky is cloudy.

$$\text{RAIN} \Longrightarrow \text{CLOUD}$$

Q: If it rains in the morning then Prof. X carries his umbrella all day.

$$\text{MORNING RAIN} \Longrightarrow \text{UMBRELLA}$$

R: People who carry umbrellas never get soaked.

$$\text{UMBRELLA} \Longrightarrow \text{NOT SOAKED}$$

Which of the following statements can be deduced from P, Q and R?

A: A cloudy sky is a necessary condition for rain. True

B: A cloudy sky is a sufficient condition for rain. False

C: It is raining only if the sky is cloudy. True

D: Rain in the morning is a necessary condition for Prof. X to carry his umbrella. False

E: Rain in the morning is a sufficient condition for Prof. X to carry his umbrella. True

F: Rain falling implies that the sky is cloudy. True

G: The sky is cloudy implies that rain is falling. False

H: If Prof. X is soaked then it did not rain this morning. True

§7 Sets and Counting

Definition 7.1

Let X be a set. We say that X is *finite* if it has finitely many elements, and *infinite* otherwise. The *size* of a finite set X is its number of elements. We denote the size of X by $|X|$,

Note that $|X|$ is read as 'mod X'.

Elements, Subsets and Sizes

Exercise 7.2

State the truth value (true or false) of each of these propositions.

(a) 1 is an element of $\mathbb{N}$.

(b) $\{1\}$ is an element of $\mathbb{N}$.

(c) $|\, x \in \mathbb{R} : x^3 = 1\}| = 1$.

(d) $|\{z \in \mathbb{C} : z^3 = 1\}| = 1$.

(e) The set of natural numbers is infinite.

(f) The empty set is a subset of every set.

(g) The empty set is an element of every set.

Proving that Two Sets are Equal

Claim 7.3

Let X, Y and Z be sets. Then

(i) $(X \cup Y) \cap Z = (X \cap Z) \cup (Y \cap Z)$,

(ii) $(X \cap Y) \cup Z = (X \cup Z) \cap (Y \cup Z)$.

Recall that, by the definition on page 7,

$$X \subseteq Y \iff (x \in X \Longrightarrow x \in Y).$$

We will also use the following fact:

$$X = Y \iff X \subseteq Y \text{ and } Y \subseteq X.$$

Feedback on Sheet 7 and Quiz and a **Correction**

- A–K in green folder (**unclaimed work is at front**)
- L–Z in red folder

Questions 3, 5 and 6 were used for the numerical mark. Please see me if you have any queries. Extensive feedback is on Moodle.

Question 2(e): Let A be $(P \implies Q) \implies R$ and B be $(Q \implies R)$. Is $A \implies B$ a tautology? **You need a truth table for $A \implies B$.**

- Many people compared the column for A and the column for B. These are not the same, but $A \implies B$ is still always true.
- The columns for A and B are the same if and only if $A \iff B$ is a tautology. This is a different question.

Correction. In Question 3 on Sheet 8, the hint should suggest $\exists n \in \mathbb{Z}$, not $\exists n \in \mathbb{N}$.

Feedback on Sheet 7 and Quiz and a **Correction**

- A–K in green folder (**unclaimed work is at front**)
- L–Z in red folder

Questions 3, 5 and 6 were used for the numerical mark. Please see me if you have any queries. Extensive feedback is on Moodle.

Question 2(e): Let A be $(P \implies Q) \implies R$ and B be $(Q \implies R)$. Is $A \implies B$ a tautology? **You need a truth table for $A \implies B$.**

- Many people compared the column for A and the column for B. These are not the same, but $A \implies B$ is still always true.
- The columns for A and B are the same if and only if $A \iff B$ is a tautology. This is a different question.

Correction. In Question 3 on Sheet 8, the hint should suggest $\exists n \in \mathbb{Z}$, not $\exists n \in \mathbb{N}$.

Quiz. Let $X = \{1, \{1, 6\}, 5, \mathbb{N}\}$. True or False?

- $\{1, 5\} \subseteq X$,
- $2 \in X$.
- $\{1, 5\} \in X$,

What is the size of X?

Feedback on Sheet 7 and Quiz and a **Correction**

- A–K in green folder (**unclaimed work is at front**)
- L–Z in red folder

Questions 3, 5 and 6 were used for the numerical mark. Please see me if you have any queries. Extensive feedback is on Moodle.

Question 2(e): Let A be $(P \implies Q) \implies R$ and B be $(Q \implies R)$. Is $A \implies B$ a tautology? **You need a truth table for $A \implies B$.**

- Many people compared the column for A and the column for B. These are not the same, but $A \implies B$ is still always true.
- The columns for A and B are the same if and only if $A \iff B$ is a tautology. This is a different question.

Correction. In Question 3 on Sheet 8, the hint should suggest $\exists n \in \mathbb{Z}$, not $\exists n \in \mathbb{N}$.

Quiz. Let $X = \{1, \{1, 6\}, 5, \mathbb{N}\}$. True or False?

- $\{1, 5\} \subseteq X$,
- $2 \in X$.
- $\{1, 5\} \in X$,

True: $1 \in X$ and $2 \in X$

False: $4 \notin X$ (but $2 \in \mathbb{N}$ and $\mathbb{N} \in X$)

What is the size of X?

Feedback on Sheet 7 and Quiz and a **Correction**

- A–K in green folder (**unclaimed work is at front**)
- L–Z in red folder

Questions 3, 5 and 6 were used for the numerical mark. Please see me if you have any queries. Extensive feedback is on Moodle.

Question 2(e): Let A be $(P \implies Q) \implies R$ and B be $(Q \implies R)$. Is $A \implies B$ a tautology? **You need a truth table for $A \implies B$.**

- Many people compared the column for A and the column for B. These are not the same, but $A \implies B$ is still always true.
- The columns for A and B are the same if and only if $A \iff B$ is a tautology. This is a different question.

Correction. In Question 3 on Sheet 8, the hint should suggest $\exists n \in \mathbb{Z}$, not $\exists n \in \mathbb{N}$.

Quiz. Let $X = \{1, \{1, 6\}, 5, \mathbb{N}\}$. True or False?

- $\{1, 5\} \subseteq X$,
- $2 \in X$.
- $\{1, 5\} \in X$,

True: $1 \in X$ and $2 \in X$

False: $4 \notin X$ (but $2 \in \mathbb{N}$ and $\mathbb{N} \in X$)

What is the size of X?

Feedback on Sheet 7 and Quiz and a **Correction**

- A–K in green folder (**unclaimed work is at front**)
- L–Z in red folder

Questions 3, 5 and 6 were used for the numerical mark. Please see me if you have any queries. Extensive feedback is on Moodle.

Question 2(e): Let A be $(P \implies Q) \implies R$ and B be $(Q \implies R)$. Is $A \implies B$ a tautology? **You need a truth table for $A \implies B$.**

- Many people compared the column for A and the column for B. These are not the same, but $A \implies B$ is still always true.
- The columns for A and B are the same if and only if $A \iff B$ is a tautology. This is a different question.

Correction. In Question 3 on Sheet 8, the hint should suggest $\exists n \in \mathbb{Z}$, not $\exists n \in \mathbb{N}$.

Quiz. Let $X = \{1, \{1, 6\}, 5, \mathbb{N}\}$. True or False?

- $\{1, 5\} \subseteq X$, True: $1 \in X$ and $2 \in X$
- $2 \in X$. False: $4 \notin X$ (but $2 \in \mathbb{N}$ and $\mathbb{N} \in X$)
- $\{1, 5\} \in X$, False: $\{1, 5\} \notin X$

What is the size of X?

Feedback on Sheet 7 and Quiz and a **Correction**

- A–K in green folder (**unclaimed work is at front**)
- L–Z in red folder

Questions 3, 5 and 6 were used for the numerical mark. Please see me if you have any queries. Extensive feedback is on Moodle.

Question 2(e): Let A be $(P \implies Q) \implies R$ and B be $(Q \implies R)$. Is $A \implies B$ a tautology? **You need a truth table for $A \implies B$.**

- Many people compared the column for A and the column for B. These are not the same, but $A \implies B$ is still always true.
- The columns for A and B are the same if and only if $A \iff B$ is a tautology. This is a different question.

Correction. In Question 3 on Sheet 8, the hint should suggest $\exists n \in \mathbb{Z}$, not $\exists n \in \mathbb{N}$.

Quiz. Let $X = \{1, \{1, 6\}, 5, \mathbb{N}\}$. True or False?

- $\{1, 5\} \subseteq X$, True: $1 \in X$ and $2 \in X$
- $2 \in X$. False: $4 \notin X$ (but $2 \in \mathbb{N}$ and $\mathbb{N} \in X$)
- $\{1, 5\} \in X$, False: $\{1, 5\} \notin X$

What is the size of X? $|X| = 4$

Principle of Inclusion and Exclusion

Let X and Y be finite sets. In the sum $|X| + |Y|$ we count each element of X once, and each element of Y once. So the elements of $X \cap Y$ are counted twice, once as elements of X, and once as elements of Y. If we subtract $|X \cap Y|$ to correct for this overcounting, we get

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$

Principle of Inclusion and Exclusion

Let X and Y be finite sets. In the sum $|X| + |Y|$ we count each element of X once, and each element of Y once. So the elements of $X \cap Y$ are counted twice, once as elements of X, and once as elements of Y. If we subtract $|X \cap Y|$ to correct for this overcounting, we get

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$

For example, if $z \in X \cap Y$ then z is counted in $|X|$, $|Y|$ and in $|X \cap Y|$, for a total contribution of $1 + 1 - 1 = 1$.

Principle of Inclusion and Exclusion

Let X and Y be finite sets. In the sum $|X| + |Y|$ we count each element of X once, and each element of Y once. So the elements of $X \cap Y$ are counted twice, once as elements of X, and once as elements of Y. If we subtract $|X \cap Y|$ to correct for this overcounting, we get

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$

For example, if $z \in X \cap Y$ then z is counted in $|X|$, $|Y|$ and in $|X \cap Y|$, for a total contribution of $1 + 1 - 1 = 1$.

If X and Y are contained in a universe set U then, since

$$|(X \cup Y)'| = |U| - |X \cup Y|$$

we have

$$|(X \cup Y)'| = |U| - |X| - |Y| + |X \cap Y|.$$

Exercise on Inclusion / Exclusion

Exercise 7.4

At the University of Erewhon, there are 100 students. At each algebra lecture there are 65 students and at each analysis lecture that are 70 students. Let b be the number of students doing both algebra and analysis.

(i) If $b = 50$, how many students are doing neither algebra nor analysis?

(ii) What is the greatest possible value of b?

(iii) What is the least possible value of b?

Principle of Inclusion and Exclusion for Three Sets

Claim 7.5

If X, Y and Z are finite sets then

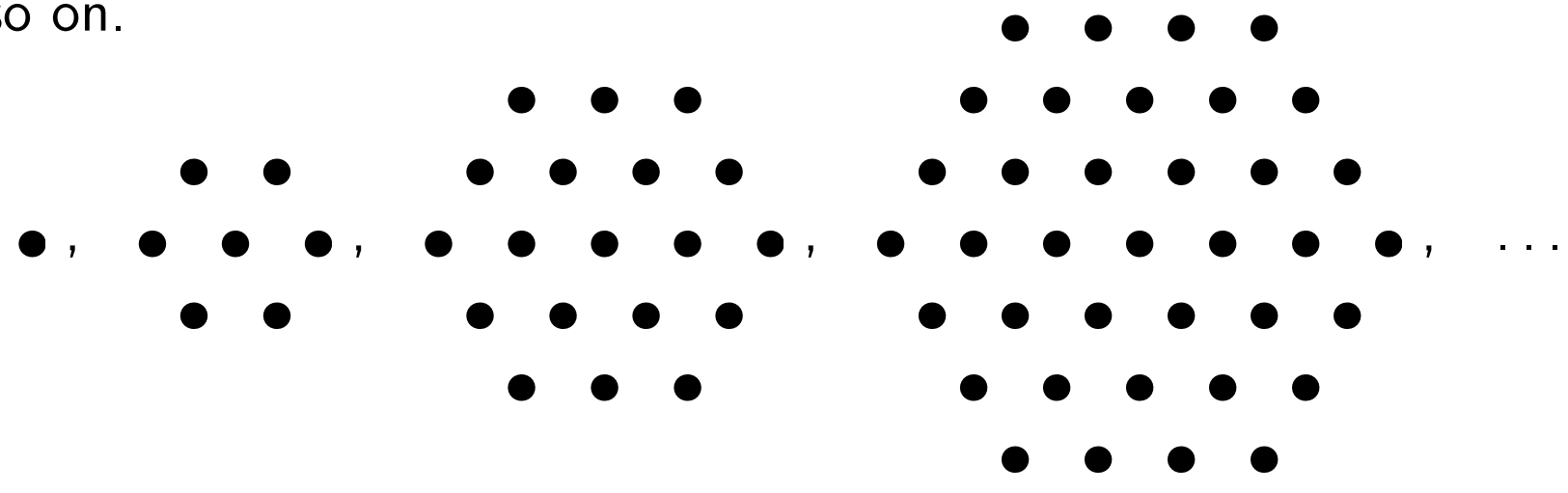
$$|X \cup Y \cup Z| = |X| + |Y| + |Z| - |X \cap Y| - |Y \cap Z| - |Z \cap X| + |X \cap Y \cap Z|.$$

Exercise 7.6

Suppose that X, Y, Z are subsets of a finite universe set U. Use Claim 7.5 to write down a formula for the size of $\left|(X \cup Y \cup Z)'\right|$.

Example 7.7

Define $f : \mathbb{N} \to \mathbb{N}$ so that $f(n)$ is the number of dots in the nth diagram below. So $f(1) = 1$, $f(2) = 7$, $f(3) = 19$, $f(4) = 37$, and so on.



Multiplying Choices

Suppose you have offers from RHUL, QMUL and UCL. In each case you can do either Maths or Physics. How many options do you have?

Multiplying Choices

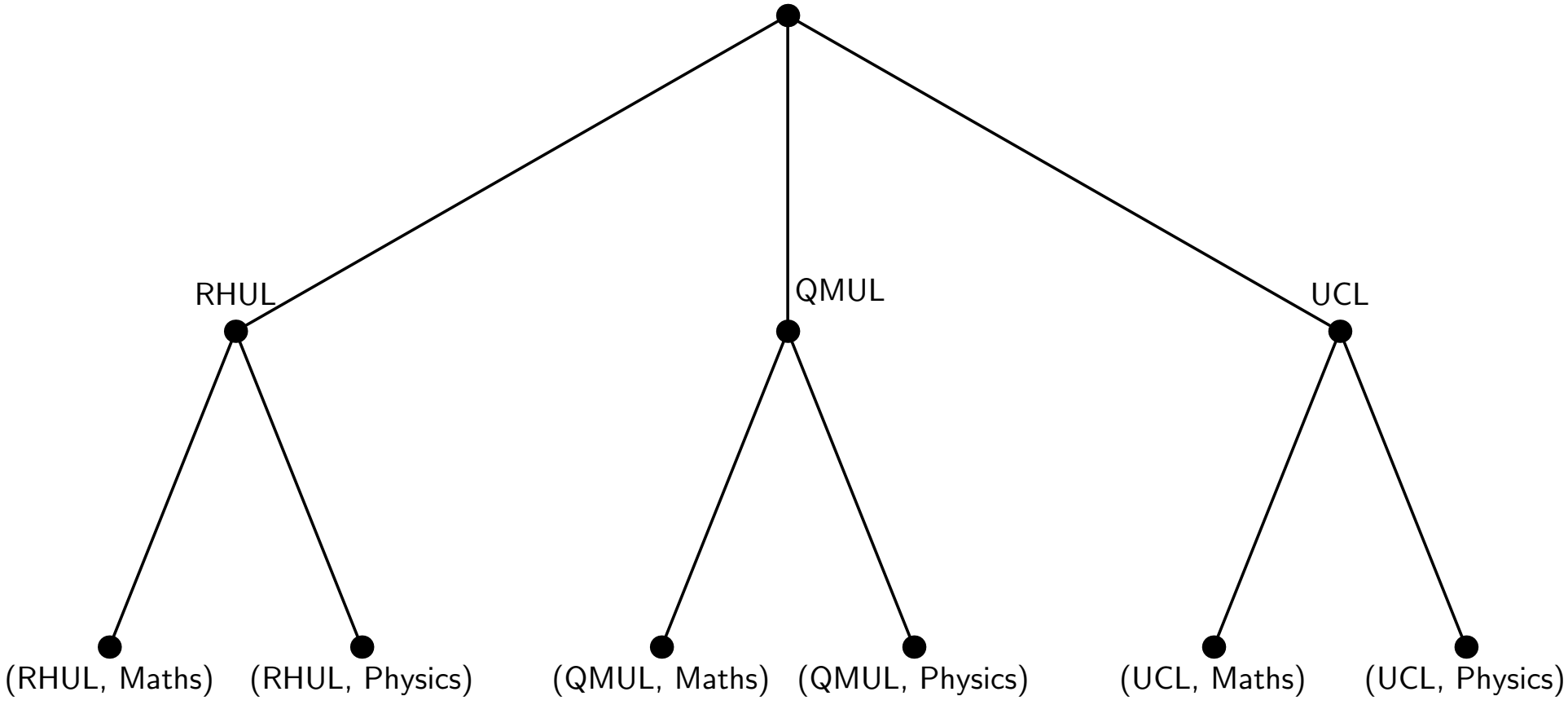
Suppose you have offers from RHUL, QMUL and UCL. In each case you can do either Maths or Physics. How many options do you have?

Answer: 6. There are 3 choices for university, 2 choices for the course, and $3 \times 2 = 6$.

Multiplying Choices

Suppose you have offers from RHUL, QMUL and UCL. In each case you can do either Maths or Physics. How many options do you have?

Answer: 6. There are 3 choices for university, 2 choices for the course, and $3 \times 2 = 6$.



Counting Subsets

There are four subsets of $\{1, 2\}$, namely $\varnothing, \{1\}, \{2\}, \{1, 2\}$.
Exercise: Write down all the subsets of $\{1\}$ and $\{1, 2, 3\}$. How many are there in each case?

Counting Subsets

There are four subsets of $\{1, 2\}$, namely $\varnothing, \{1\}, \{2\}, \{1, 2\}$.
Exercise: Write down all the subsets of $\{1\}$ and $\{1, 2, 3\}$. How many are there in each case?

The principle that numbers of independent choices can be multiplied to find the size of a set, is very useful when solving combinatorial problems.

Example 7.9

A menu has three starters, four main courses and six desserts.

(a) How many ways are there to choose a three course meal, having a starter, main course and dessert?

(b) How many two course meals, each having exactly one main course, can be chosen?

Example Menu

Starters

(1) Bruschetta
(2) Ravioli di granchio
(3) Zucchini fritti

Main courses

(1) Daube de boeuf
(2) Sole meunière
(3) Risotto des légumes et truffes noires
(4) Truite sauce vierge

Desserts

(1) Sticky toffee pudding
(2) Vanilla icecream
(3) Chocolate icecream
(4) Banana pancakes
(5) Cheeseboard
(6) Affogato

Cartesian Products

Exercise 7.10

Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

Decide on the truth value of the following propositions.

(a) $(1, 2) = (2, 1)$

(b) $\{1, 2\} = \{2, 1\}$

(c) $(5/2, 3/2) \in X \times Y$

(d) $(3/2, 5/2) \in X \times Y$

(e) $Y \times Y \subseteq X \times Y$

(f) $X \subseteq Y$

(g) $\varnothing \times X \subseteq \varnothing \times Y$

Cartesian Products

Exercise 7.10

Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

Decide on the truth value of the following propositions.

(a) $(1, 2) = (2, 1)$ False

(b) $\{1, 2\} = \{2, 1\}$

(c) $(5/2, 3/2) \in X \times Y$

(d) $(3/2, 5/2) \in X \times Y$

(e) $Y \times Y \subseteq X \times Y$

(f) $X \subseteq Y$

(g) $\varnothing \times X \subseteq \varnothing \times Y$

Cartesian Products

Exercise 7.10

Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

Decide on the truth value of the following propositions.

(a) $(1, 2) = (2, 1)$ False

(b) $\{1, 2\} = \{2, 1\}$ True

(c) $(5/2, 3/2) \in X \times Y$

(d) $(3/2, 5/2) \in X \times Y$

(e) $Y \times Y \subseteq X \times Y$

(f) $X \subseteq Y$

(g) $\varnothing \times X \subseteq \varnothing \times Y$

Cartesian Products

Exercise 7.10

Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

Decide on the truth value of the following propositions.

(a) $(1, 2) = (2, 1)$ — False

(b) $\{1, 2\} = \{2, 1\}$ — True

(c) $(5/2, 3/2) \in X \times Y$ — True

(d) $(3/2, 5/2) \in X \times Y$

(e) $Y \times Y \subseteq X \times Y$

(f) $X \subseteq Y$

(g) $\varnothing \times X \subseteq \varnothing \times Y$

Cartesian Products

Exercise 7.10

Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

Decide on the truth value of the following propositions.

(a) $(1, 2) = (2, 1)$ — False

(b) $\{1, 2\} = \{2, 1\}$ — True

(c) $(5/2, 3/2) \in X \times Y$ — True

(d) $(3/2, 5/2) \in X \times Y$ — False

(e) $Y \times Y \subseteq X \times Y$

(f) $X \subseteq Y$

(g) $\varnothing \times X \subseteq \varnothing \times Y$

Cartesian Products

Exercise 7.10

Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

Decide on the truth value of the following propositions.

(a) $(1, 2) = (2, 1)$ — False

(b) $\{1, 2\} = \{2, 1\}$ — True

(c) $(5/2, 3/2) \in X \times Y$ — True

(d) $(3/2, 5/2) \in X \times Y$ — False

(e) $Y \times Y \subseteq X \times Y$ — True

(f) $X \subseteq Y$

(g) $\varnothing \times X \subseteq \varnothing \times Y$

Cartesian Products

Exercise 7.10

Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

Decide on the truth value of the following propositions.

(a) $(1, 2) = (2, 1)$ — False

(b) $\{1, 2\} = \{2, 1\}$ — True

(c) $(5/2, 3/2) \in X \times Y$ — True

(d) $(3/2, 5/2) \in X \times Y$ — False

(e) $Y \times Y \subseteq X \times Y$ — True

(f) $X \subseteq Y$ — False

(g) $\varnothing \times X \subseteq \varnothing \times Y$

Cartesian Products

Exercise 7.10

Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

Decide on the truth value of the following propositions.

(a) $(1, 2) = (2, 1)$ — False

(b) $\{1, 2\} = \{2, 1\}$ — True

(c) $(5/2, 3/2) \in X \times Y$ — True

(d) $(3/2, 5/2) \in X \times Y$ — False

(e) $Y \times Y \subseteq X \times Y$ — True

(f) $X \subseteq Y$ — False

(g) $\varnothing \times X \subseteq \varnothing \times Y$ — True

Part D: Integers and rings

§8 Euclid's Algorithm and Congruences

Definition 8.1

Let $m, n \in \mathbb{N}$. We say that $d \in \mathbb{N}$ is the *greatest common divisor* of m and n, and write $\gcd(m, n) = d$, if d is the greatest natural number that divides both m and n.

Example 8.2′ See board

§8 Euclid's Algorithm and Congruences

Definition 8.1

Let $m, n \in \mathbb{N}$. We say that $d \in \mathbb{N}$ is the *greatest common divisor* of m and n, and write $\gcd(m, n) = d$, if d is the greatest natural number that divides both m and n.

Example 8.2′ See board

Exercise 8.3

Find $\gcd(m, n)$ in each of these cases:

(i) $m = 310$, $n = 42$,

(ii) $m = 23$, $n = 46$,

(iii) $m = 31460$, $n = 41\,991\,752$.

Hint: on page 38 we saw that $31460 = 2^2 \times 5 \times 11^2 \times 13$. You do not need to factor n completely to find the gcd. You can use

$$41\,991\,752 = 121 \times 347039 + 33 = 3230134 \times 13 + 10.$$

Sheet 8

Please take answers to Sheet 8:

- A–J in red folder
- K–Z in green folder

Mostly well done! Questions 4, 5 and 6 were marked. Model answers are on Moodle.

- Note that quantifiers should come before the thing they quantify. So

$$(\exists n \in \mathbb{Z})(b = \pi/2 + 2n\pi)$$

  is correct, and

$$(b = \pi/2 + 2n\pi)\exists n \in \mathbb{Z}$$

  is probably comprehensible, but is strictly speaking wrong.

If you have not yet completed a questionnaire please take one at end.

Euclid's Algorithm

Lemma 8.4 (Examinable)

Let $m, n \in \mathbb{N}$. If $n = qm + r$ where $q,\ r \in \mathbb{Z}$, then

$$\{d \in \mathbb{N} : d \text{ divides } n \text{ and } m\} = \{d \in \mathbb{N} : d \text{ divides } m \text{ and } r\}.$$

In particular, the greatest elements of these sets are equal, so

$$\gcd(n, m) = \gcd(m, r).$$

Euclid's Algorithm

Lemma 8.4 (Examinable)

Let $m, n \in \mathbb{N}$. If $n = qm + r$ where q, $r \in \mathbb{Z}$, then

$$\{d \in \mathbb{N} : d \text{ divides } n \text{ and } m\} = \{d \in \mathbb{N} : d \text{ divides } m \text{ and } r\}.$$

In particular, the greatest elements of these sets are equal, so

$$\gcd(n, m) = \gcd(m, r).$$

Algorithm 8.5 (Euclid's Algorithm)

Let n, $m \in \mathbb{N}$. Find the quotient q and the remainder r when n is divided by m.

- If $r = 0$ then m divides n and $\gcd(n, m) = m$.
- Otherwise repeat from the start with m and r.

Example 8.6

Let $n = 3933$ and let $m = 389$. The equations below show the quotient and remainder at each step of Euclid's Algorithm:

$$\begin{aligned} \mathbf{3933} &= 10 \times \mathbf{389} + \mathbf{43} \\ \mathbf{389} &= 9 \times \mathbf{43} + \mathbf{2} \\ \mathbf{43} &= 21 \times \mathbf{2} + \mathbf{1} \\ \mathbf{2} &= 2 \times \mathbf{1}. \end{aligned}$$

Hence $\gcd(3933, 389) = 1$.

Example 8.6

Let $n = 3933$ and let $m = 389$. The equations below show the quotient and remainder at each step of Euclid's Algorithm:

$$\begin{aligned} \mathbf{3933} &= 10 \times \mathbf{389} + \mathbf{43} \\ \mathbf{389} &= 9 \times \mathbf{43} + \mathbf{2} \\ \mathbf{43} &= 21 \times \mathbf{2} + \mathbf{1} \\ \mathbf{2} &= 2 \times \mathbf{1}. \end{aligned}$$

Hence $\gcd(3933, 389) = 1$.

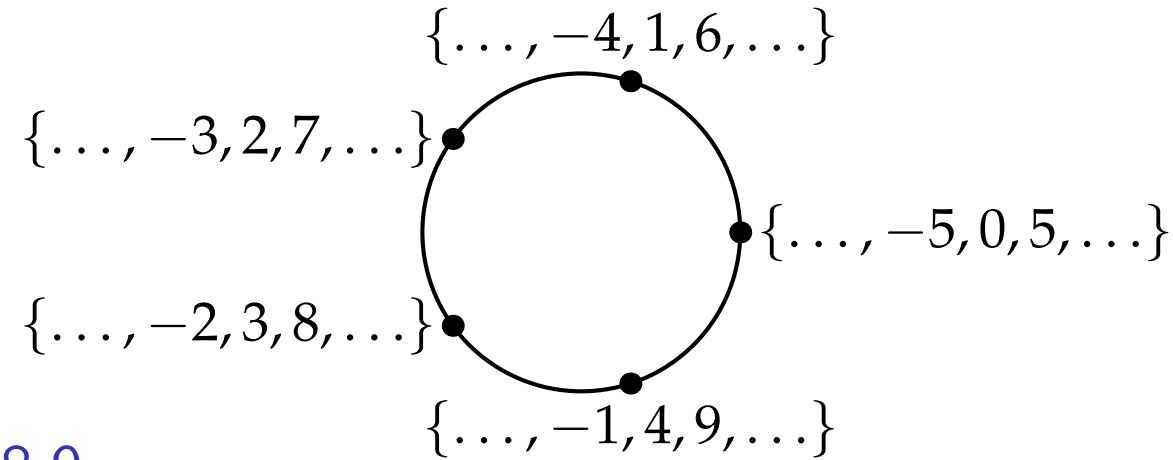
Example 8.7: Work backwards to get

$$\begin{aligned} 1 &= \mathbf{43} - 21 \times \mathbf{2} \\ &= \mathbf{43} - 21 \times (\mathbf{389} - 9 \times \mathbf{43}) \\ &= 190 \times \mathbf{43} - 21 \times \mathbf{389} \\ &= 190 \times (\mathbf{3933} - 10 \times \mathbf{389}) - 21 \times \mathbf{389} \\ &= 190 \times \mathbf{3933} - 1921 \times \mathbf{389}. \end{aligned}$$

Congruences

Definition 8.8

Let $m \in \mathbb{N}$. Let $n, n' \in \mathbb{N}$. If n and n' have the same remainder on division by m then we say that n is *congruent to* n' modulo m, and write $n \equiv n' \bmod m$.



Example 8.9

(a) Since 17 and -4 both have remainder 3 on division by 7, we have $17 \equiv -4 \bmod 7$.

(b) Since $19 - 12$ is divisible by 7, 19 and 12 have the same remainder on division by 7. Hence $19 \equiv 12 \bmod 7$.

(c) We have $0 + 0 \equiv 0 \bmod 2$, $0 + 1 \equiv 1 \bmod 2$, $1 + 0 \equiv 1 \bmod 2$ and $1 + 1 \equiv 0 \bmod 2$.

The Square Code

The *square code* is the set of all sequences

$$\{(u_1, u_2, u_3, u_4, u_1+u_2, u_3+u_4, u_1+u_3, u_2+u_4) : u_1, u_2, u_3, u_4 \in \{0, 1\}\}$$

where the addition is done mod 2, as in Example 8.9(c). The name comes from the representation of the sequences as a square of four message bits, (u_1, u_2, u_3, u_4), surrounded by four check bits.

u_1	u_2	$u_1 + u_2$
u_3	u_4	$u_3 + u_4$
$u_1 + u_3$	$u_2 + u_4$	

The elements of the square code are called *codewords*.

Example 8.10

Suppose we want to send 7. Since 7 is 111 in binary, we put in an initial 0 to get 0111, so $u_1 = 0$ and $u_2 = u_3 = u_4 = 1$. The sent codeword is 01111010.

Decoding using the Square Code

If at most one position in the sent codeword gets flipped (either from 0 to 1 or from 1 to 0) then the receiver will still be able to work out what number was sent.

Example 8.11

(i) Suppose you receive 01011100. What number was probably sent?

(ii) Suppose you receive 10000011. What number was probably sent?

Solving congruence equations

Observe that $27 \times 33 \equiv 7 \times 33 \equiv 7 \times 3 \equiv 1 \bmod 10$.

Exercise 8.12

What is $23427 \times 973249 \bmod 10$?

Solving congruence equations

Observe that $27 \times 33 \equiv 7 \times 33 \equiv 7 \times 3 \equiv 1 \bmod 10$.

Exercise 8.12

What is $23427 \times 973249 \bmod 10$?

Lemma 8.13 (Examinable)

Let $m \in \mathbb{N}$ and let $r, r', s, s' \in \mathbb{Z}$. If $r \equiv r' \bmod m$ and $s \equiv s' \bmod m$ then

(i) $r + s \equiv r' + s' \bmod m$,

(ii) $rs \equiv r's' \bmod m$.

Solving congruence equations

Observe that $27 \times 33 \equiv 7 \times 33 \equiv 7 \times 3 \equiv 1 \bmod 10$.

Exercise 8.12

What is $23427 \times 973249 \bmod 10$?

Lemma 8.13 (Examinable)

Let $m \in \mathbb{N}$ and let $r, r', s, s' \in \mathbb{Z}$. If $r \equiv r' \bmod m$ and $s \equiv s' \bmod m$ then

(i) $r + s \equiv r' + s' \bmod m$,

(ii) $rs \equiv r's' \bmod m$.

Lemma 8.12 justifies many other manipulations with congruences.

For example, $3^6 \equiv 9 \bmod 10 \implies 3^7 \equiv 9 \times 3 \equiv 7 \bmod 10$. The only calculation needed is $9 \times 3 = 27$: there is no need to calculate 3^7.

Exercise 8.14

Find $3^{2014} \bmod 10$.

Solving Congruences

Exercise 8.15

(a) Find $x \in \mathbb{Z}$ such that $0 \leq x < 11$ and $x + 9 \equiv 7 \bmod 12$.

(b) Find an $x \in \mathbb{Z}$ such that $3x \equiv 2 \bmod 5$.

(c) Find *all* $x \in \mathbb{Z}$ such that $3x \equiv 2 \bmod 5$.

Solving Congruences

Exercise 8.15

(a) Find $x \in \mathbb{Z}$ such that $0 \leq x < 11$ and $x + 9 \equiv 7 \bmod 12$.

$x = 10$ is the unique such x

(b) Find an $x \in \mathbb{Z}$ such that $3x \equiv 2 \bmod 5$.

(c) Find *all* $x \in \mathbb{Z}$ such that $3x \equiv 2 \bmod 5$.

Solving Congruences

Exercise 8.15

(a) Find $x \in \mathbb{Z}$ such that $0 \leq x < 11$ and $x + 9 \equiv 7 \bmod 12$.

$x = 10$ is the unique such x

(b) Find an $x \in \mathbb{Z}$ such that $3x \equiv 2 \bmod 5$.

$x = 4$, or $x = -1$, or $x = 9$ or ...

(c) Find *all* $x \in \mathbb{Z}$ such that $3x \equiv 2 \bmod 5$.

Solving Congruences

Exercise 8.15

(a) Find $x \in \mathbb{Z}$ such that $0 \leq x < 11$ and $x + 9 \equiv 7 \bmod 12$.

$x = 10$ is the unique such x

(b) Find an $x \in \mathbb{Z}$ such that $3x \equiv 2 \bmod 5$.

$x = 4$, or $x = -1$, or $x = 9$ or $\ldots$

(c) Find *all* $x \in \mathbb{Z}$ such that $3x \equiv 2 \bmod 5$.

$\{-1, 4, 9, \ldots\} = \{x \in \mathbb{Z} : x \equiv 4 \bmod 5\}$ **[corrected]**

Solving Congruences

Exercise 8.15

(a) Find $x \in \mathbb{Z}$ such that $0 \leq x < 11$ and $x + 9 \equiv 7 \bmod 12$.

$x = 10$ is the unique such x

(b) Find an $x \in \mathbb{Z}$ such that $3x \equiv 2 \bmod 5$.

$x = 4$, or $x = -1$, or $x = 9$ or $\ldots$

(c) Find *all* $x \in \mathbb{Z}$ such that $3x \equiv 2 \bmod 5$.

$\{-1, 4, 9, \ldots\} = \{x \in \mathbb{Z} : x \equiv 4 \bmod 5\}$ **[corrected]**

When the modulus m is larger, Euclid's algorithm can be used.

Example 8.16′ See board.

The printed notes have a similar example using larger numbers.

Not all congruences can be solved. For example $2x \equiv 3 \bmod 4$ has no solution, because $2x$ is always even, but any number congruent to 3 modulo 4 is odd.

The Square Code as a Party Trick

Question i can be stated more briefly as: is the ith position of the codeword for your number equal to 1?

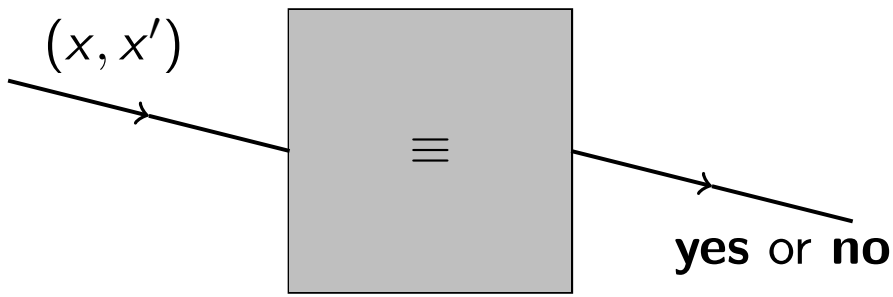
1	Is your number 8, 9, 10, 11, 12, 13, 14 or 15?
2	" " " 4, 5, 6, 7, 12, 13, 14 or 15?
3	" " " 2, 3, 6, 7, 10, 11, 14 or 15?
4	" " " 1, 3, 5, 7, 9, 11, 13 or 15?
5	" " " 4, 5, 6, 7, 8, 9, 10 or 11?
6	" " " 1, 2, 5, 6, 9, 10, 13 or 14?
7	" " " 2, 3, 6, 7, 8, 9, 12 or 13?
8	" " " 1, 3, 4, 6, 9, 11, 12 or 14?

§9 Relations and the Integers Modulo m

The following definition generalizes the congruence relation.

Definition 9.1

Let X be a set. A *relation* on X is a black box which, given an ordered pair (x, x') where x, $x' \in X$, outputs either **yes** or **no**. A **yes** means x is related to x', and a **no** means x is not related to x'.



Two relations on a set X are equal if they agree on all ordered pairs (x, x'). As for functions, it is irrelevant how the black box arrives at its answer.

Examples of Relations

Example 9.2

(i) Fix $m \in \mathbb{N}$. Let $n, n' \in \mathbb{Z}$. For the input (n, n'), let the black box output **yes** if $n \equiv n' \bmod m$ and **no** otherwise. This defines the congruence modulo m relation on $\mathbb{Z}$.

(ii) Let P be the set of all subsets of $\{1, 2, 3\}$. Given an ordered pair (X, Y) of elements of P, let the black box output **yes** if $X \subseteq Y$ and **no** otherwise.

Relations can be defined more briefly. For example, suppose that $X = \{1, 2, 3, 4, 5, 6\}$. Then

$$x \text{ relates to } y \iff x < y$$

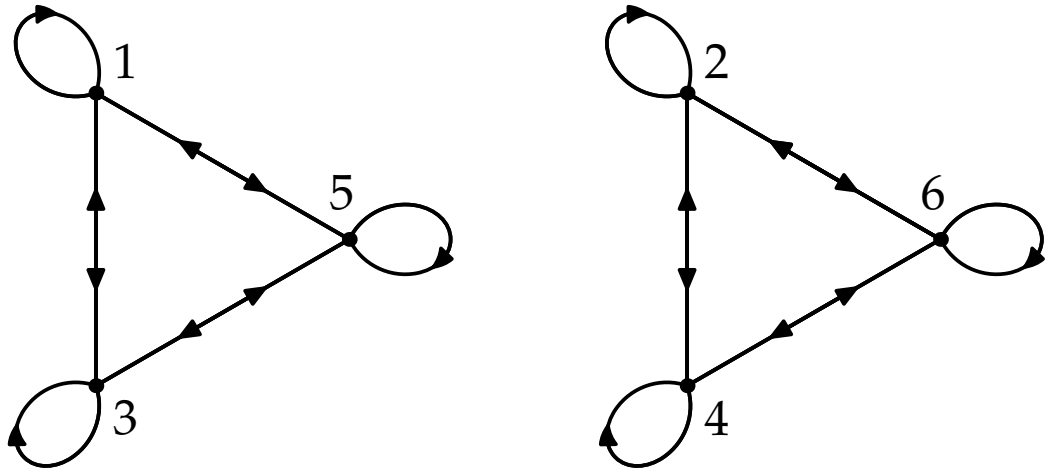
defines the relation 'strictly less than' on X. An analogous relation can be defined replacing X with any other subset of $\mathbb{R}$.

Diagrams

Let X be a set and let $\sim$ be a relation defined on X. To represent $\sim$ on a diagram, draw a dot for each element of X. Then for each $x, y \in X$ such that $x \sim y$, draw an arrow *from* x *to* y. If $x \sim x$ draw a loop from x to itself.

Example 9.3

Let $X = \{1, 2, 3, 4, 5, 6\}$. The relation $x \equiv y \bmod 2$ on X is:



Exercise: Draw a similar diagram for the relation on $\{1, 2, 3, 4, 5, 6\}$ defined by

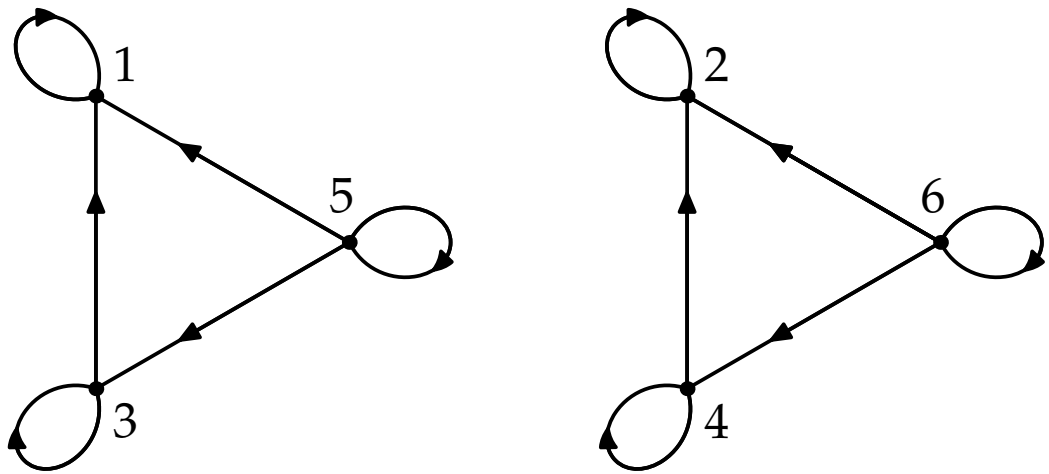
$$x \sim y \iff x - y \text{ is even and } x > y.$$

Diagrams

Let X be a set and let $\sim$ be a relation defined on X. To represent $\sim$ on a diagram, draw a dot for each element of X. Then for each $x, y \in X$ such that $x \sim y$, draw an arrow *from* x *to* y. If $x \sim x$ draw a loop from x to itself.

Example 9.3

Let $X = \{1, 2, 3, 4, 5, 6\}$. The relation $x \equiv y \bmod 2$ on X is:



Exercise: Draw a similar diagram for the relation on $\{1, 2, 3, 4, 5, 6\}$ defined by

$$x \sim y \iff x - y \text{ is even and } x > y.$$

Feedback on Sheet 9

Please take answers to Sheet 9:

- A–K in red folder
- L–Z in green folder

Questions 2, 4 and 5 were marked. Model answers are on Moodle. (Updated with missing answers to Question 2.)

Note there is no 0/1 or 1/1 mark: the first eight sheets will be used for the eight marks.

- Size of square code: there are 2 independent choices for each of u_1, u_2, u_3, u_4 so $2 \times 2 \times 2 \times 2 = 2^4$ codewords.

u_1	u_2	$u_1 + u_2$
u_3	u_4	$u_3 + u_4$
$u_1 + u_3$	$u_2 + u_4$	

- Congruences: mostly done well.
- Write a question on functions: some good efforts. Difficulty usually underestimated.

There are some revision questions on Moodle. Answers to come.

Properties of relations

Definition 9.4

Let $\sim$ be a relation on a set X. We say that $\sim$ is

(i) *reflexive* if $x \sim x$ for all $x \in X$;

(ii) *symmetric* if for all $x, y \in X$,

$$x \sim y \Longrightarrow y \sim x;$$

(iii) *transitive* if for all $x, y, z \in X$,

$$x \sim y \text{ and } y \sim z \Longrightarrow x \sim z.$$

A relation that is reflexive, symmetric and transitive is said to be an *equivalence relation*.

Example 9.5

Fix $m \in \mathbb{N}$. The congruence relation $n \equiv n' \bmod m$ is an equivalence relation on $\mathbb{Z}$.

More on Relations

In general a relation can have any combination of the properties reflexive, symmetric and transitive. See Question 2 of Sheet 10.

Exercise 9.7

Let X be the set of people sitting in a full lecture room. For each of the following relations, decide whether it is (i) reflexive, (ii) symmetric and (iii) transitive.

(a) $x \sim y$ if x and y are sitting in the same row,

(b) $x \sim y$ if x is sitting in a strictly higher row than y,

(c) $x \sim y$ if x and y are friends.

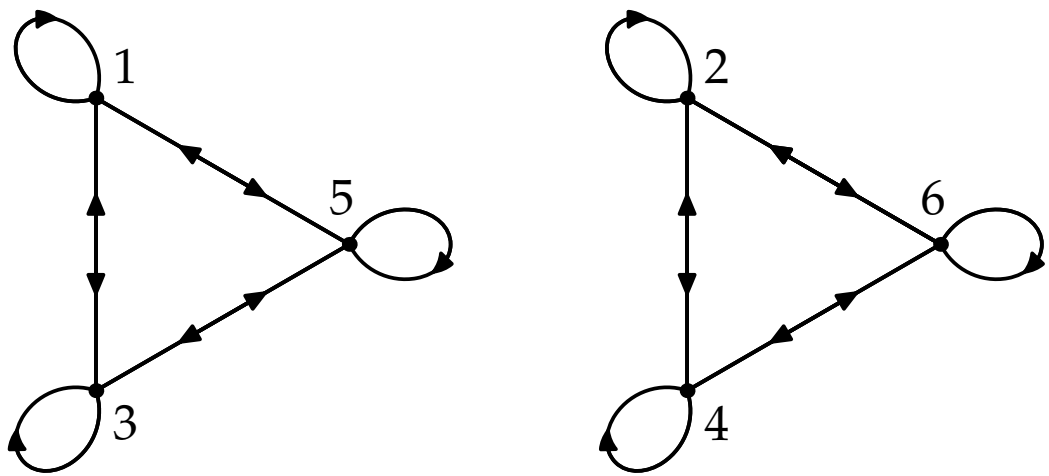
Equivalence relations and partitions

Suppose that $\sim$ is an equivalence relation on a set X. For $x \in X$, we define the *equivalence class of* x to be the set of all elements of X that relate to x. In symbols

$$[x] = \{z \in X : z \sim x\}.$$

For example, the equivalence classes for the relation $x \equiv y \bmod 2$ on the set $\{1, 2, 3, 4, 5, 6\}$ are

$$[0] = [2] = [4] = \{0, 2, 4\}$$
$$[1] = [3] = [5] = \{1, 3, 5\}$$



Main Theorem on Equivalence Classes

Theorem 9.8

Let $\sim$ be an equivalence relation on a set X. Let $x, y \in X$.

(i) $x \in [x]_\sim$,

(ii) $x \sim y \iff [x]_\sim = [y]_\sim$,

(ii) $x \not\sim y \iff [x]_\sim \cap [y]_\sim = \varnothing$.

Thus, by (i), every element of X lies in an equivalence class, and by (ii) and (iii), X is a disjoint union of the distinct equivalence classes.

The proof of Theorem 9.8 is non-examinable and will be skipped if time is pressing. See Theorem 31.13 in *How to think like a mathematician* for a careful (and exhaustively analysed) proof.

Administration

- Please take
  - Final installment of Part D handout
- Answers to Question 1 to 4 on Sheet 10 are now on Moodle.
- Answers to Questions 5 to 10 will be added on Friday.
- **You need not hand in answers to Sheet 10**: you should be able to check Questions 1 to 4 using the model answers. Or see lecturer after a lecture or in an office hour.
- Revision questions and answers are now on Moodle (top of page).

The Number System $\mathbb{Z}_m$ of Integers Modulo m.

Fix $m \in \mathbb{N}$. Let

$$\mathbb{Z}_m = \{[n] : n \in \mathbb{Z}\}$$

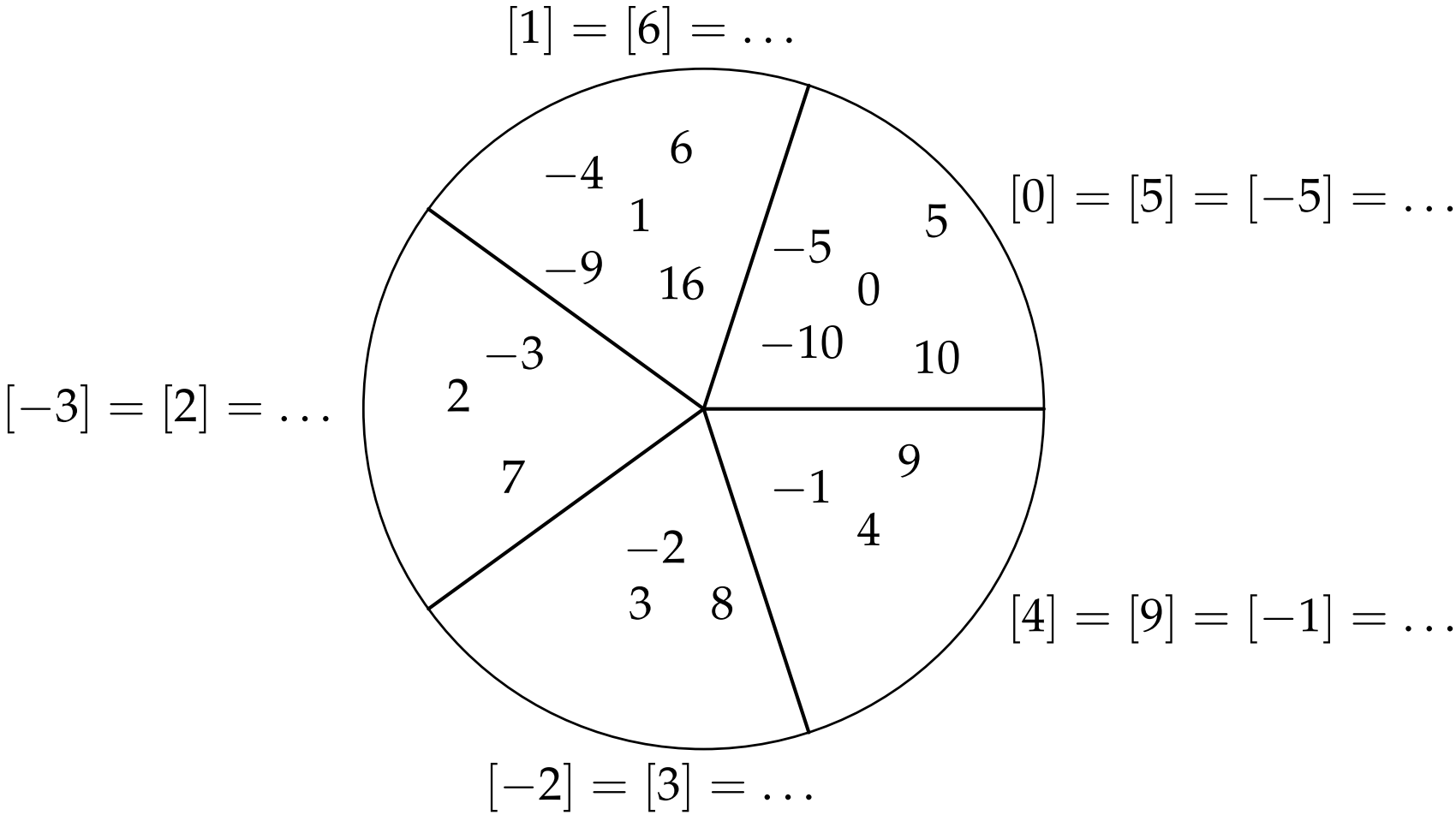
be the set of equivalence classes for congruence modulo m.

The Number System $\mathbb{Z}_m$ of Integers Modulo m.

Fix $m \in \mathbb{N}$. Let

$$\mathbb{Z}_m = \{[n] : n \in \mathbb{Z}\}$$

be the set of equivalence classes for congruence modulo m.
For example, $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$.



Addition and Multiplication in $\mathbb{Z}_m$

We turn the set $\mathbb{Z}_m$ of equivalence classes into a number system by defining addition and multiplication as follows.

Definition 9.9

Fix $m \in \mathbb{N}$. Given $[r], [s] \in \mathbb{Z}_m$ we define $[r] + [s] = [r + s]$ and $[r][s] = [rs]$.

Addition and Multiplication Tables

Example 9.10

The addition and multiplication tables for $\mathbb{Z}_5$ are shown below. For example, the entry in the addition table in the row for [4] and the column for [3] is

$$[4] + [3] = [2]$$

since $4 + 3 = 7$ and $7 \equiv 2 \bmod 5$.

$+$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

$\times$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

You may omit [0] from the multiplication table if you prefer.

Sums of squares

Exercise 9.11

Recall that a square number is a number of the form n^2 where $n \in \mathbb{N}$.

(i) Calculate $1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, \ldots$ modulo 4. State and prove a conjecture on the pattern you observe.

(ii) Is 2015 the sum of two square numbers?

§10 Rings

Definition 10.1

Suppose that R is a set on which addition and multiplication are defined, so that given any two elements $x, y \in R$, their sum $x + y$ and product xy are elements of R. Then R is a ring if

(1) (*Commutative law of addition*) $x + y = y + x$ for all $x, y \in R$,

(2) (*Existence of zero*) There is an element $0 \in R$ such that $0 + x = x$ for all $x \in R$,

(3) (*Existence of additive inverses*) For each $x \in R$ there exists an element $-x \in R$ such that $-x + x = 0$, where 0 is the element in property (2),

(4) (*Associative law of addition*) $(x + y) + z = x + (y + z)$ for all $x, y, z \in R$,

(5) (*Existence of one*) There exists an element $1 \in R$ such that $1x = x1 = x$ for all $x \in R$,

(6) (*Associative law of multiplication*) $(xy)z = x(yz)$ for all $x, y, z \in R$,

(7) (*Distributivity*) $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$ for all $x, y, z \in R$.

The number systems $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ and $\mathbb{Z}_m$ for $m \in \mathbb{N}$ are rings.

Fields

Definition 10.2

(i) A ring R is *commutative* if $xy = yx$ for all $x, y \in R$.

(ii) A commutative ring R is a *field* if for all non-zero $x \in R$ there exists an element $y \in R$ such that $xy = yx = 1$, where 1 is the one element in property (5). We say that y is the *multiplicative inverse* (or just *inverse*, for short) of x and write $y = x^{-1}$.

(iii) A commutative ring R is an *integral domain* if for all x, $y \in R$,

$$xy = 0 \implies x = 0 \text{ or } y = 0.$$

Some familiar examples of fields are $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. More interestingly, $\mathbb{Z}_5$ is a field.

Theorem 10.3 (Examinable [omitted from printed notes])

If p is prime then $\mathbb{Z}_p$ is a field.

Properties of Rings

See Question 8, Sheet 10 for (ii), (vii), (viii) and (ix).

Lemma 10.5

Let R be a ring.

(i) There is a unique zero element in R satisfying property *(2)*.

(ii) There is a unique one element in R satisfying property *(5)*.

(iii) For each $x \in R$ there exists a unique $y \in R$ such that $y + x = x + y = 0$.

(iv) If $x, z \in R$ and $x + z = x$ then $z = 0$.

(v) We have $0x = 0 = x0$ for all $x \in R$.

(vi) We have $-x = (-1)x = x(-1)$ for all $x \in R$.

(vii) For all $x \in R$ we have $-(-x) = x$.

(viii) For all $x, y \in R$ we have

$$-(xy) = (-x)y = y(-x) \text{ and } (-x)(-y) = xy.$$

(ix) $0 = 1$ if and only if $R = \{0\}$.

Fields and Integral Domains

Exercise 10.6

Show that if R is a field then R is an integral domain, making it clear which ring axioms you use.

Theorem 10.3 is a special case of the following result which gives a partial converse to the previous exercise.

Theorem 10.7

If R is a finite integral domain then R is a field.

Polynomial Rings

We define polynomial rings over an arbitrary field: the main examples to bear in mind are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_p$ for prime p.

Definition 10.8

Let F be a field. Let $F[x]$ denote the set of all polynomials

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$$

where $d \in \mathbb{N}_0$ and $a_0, a_1, a_2, \ldots, a_d \in F$. If $d = 0$, so $f(x) = a_0$, then $f(x)$ is a *constant polynomial*.

Polynomial Rings

We define polynomial rings over an arbitrary field: the main examples to bear in mind are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_p$ for prime p.

Definition 10.8

Let F be a field. Let $F[x]$ denote the set of all polynomials

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$$

where $d \in \mathbb{N}_0$ and $a_0, a_1, a_2, \ldots, a_d \in F$. If $d = 0$, so $f(x) = a_0$, then $f(x)$ is a *constant polynomial*.

When writing polynomials we usually omit coefficients of 1, and do not include powers of x whose coefficient is 0. For example, in $\mathbb{Z}_2[x]$, we write $x^2 + [1]$ rather than $[1]x^2 + [0]x + [1]$.

The x in $f(x)$ is called an *indeterminate*. You can think of it as standing for an unspecified element of F.

Ring Structure of $F[x]$

Polynomials are added and multiplied in the expected way.

Example 10.9

In $\mathbb{Z}_3[x]$, we have

$$\begin{aligned}
&(x^4 + [2]x^3 + [1]) + ([2]x^4 + x^2 + [1]) \\
&= ([1]x^4 + [2]x^3 + [1]) + ([2]x^4 + [1]x^2 + [1]) \\
&\qquad = ([1] + [2])x^4 + [2]x^3 + [1]x^2 + ([1] + [1]) \\
&\qquad = [0]x^4 + [2]x^3 + [1]x^2 + [2]
\end{aligned}$$

and

$$(x + [1])(x + [2]) = x^2 + ([1] + [2])x + [1][2] = x^2 + [2].$$

Ring Structure of $F[x]$

Polynomials are added and multiplied in the expected way.

Example 10.9

In $\mathbb{Z}_3[x]$, we have

$$\begin{aligned}
&(x^4 + [2]x^3 + [1]) + ([2]x^4 + x^2 + [1]) \\
&= ([1]x^4 + [2]x^3 + [1]) + ([2]x^4 + [1]x^2 + [1]) \\
&\qquad = ([1] + [2])x^4 + [2]x^3 + [1]x^2 + ([1] + [1]) \\
&\qquad = [0]x^4 + [2]x^3 + [1]x^2 + [2]
\end{aligned}$$

and

$$(x + [1])(x + [2]) = x^2 + ([1] + [2])x + [1][2] = x^2 + [2].$$

Ring Structure of $F[x]$

Polynomials are added and multiplied in the expected way.

Example 10.9

In $\mathbb{Z}_3[x]$, we have

$$\begin{aligned}
&(x^4 + [2]x^3 + [1]) + ([2]x^4 + x^2 + [1]) \\
&= ([1]x^4 + [2]x^3 + [1]) + ([2]x^4 + [1]x^2 + [1]) \\
&\qquad = ([1] + [2])x^4 + [2]x^3 + [1]x^2 + ([1] + [1]) \\
&\qquad = [0]x^4 + [2]x^3 + [1]x^2 + [2]
\end{aligned}$$

and

$$(x + [1])(x + [2]) = x^2 + ([1] + [2])x + [1][2] = x^2 + [2].$$

Ring Structure of $F[x]$

Polynomials are added and multiplied in the expected way.

Example 10.9

In $\mathbb{Z}_3[x]$, we have

$$\begin{aligned}
&(x^4 + [2]x^3 + [1]) + ([2]x^4 + x^2 + [1]) \\
&= ([1]x^4 + [2]x^3 + [1]) + ([2]x^4 + [1]x^2 + [1]) \\
&\qquad = ([1] + [2])x^4 + [2]x^3 + [1]x^2 + ([1] + [1]) \\
&\qquad = [0]x^4 + [2]x^3 + [1]x^2 + [2]
\end{aligned}$$

and

$$(x + [1])(x + [2]) = x^2 + ([1] + [2])x + [1][2] = x^2 + [2].$$

Ring Structure of $F[x]$

Polynomials are added and multiplied in the expected way.

Example 10.9

In $\mathbb{Z}_3[x]$, we have

$$\begin{aligned}
&(x^4 + [2]x^3 + [1]) + ([2]x^4 + x^2 + [1]) \\
&= ([1]x^4 + [2]x^3 + [1]) + ([2]x^4 + [1]x^2 + [1]) \\
&\qquad = ([1] + [2])x^4 + [2]x^3 + [1]x^2 + ([1] + [1]) \\
&\qquad = [0]x^4 + [2]x^3 + [1]x^2 + [2]
\end{aligned}$$

and

$$(x + [1])(x + [2]) = x^2 + ([1] + [2])x + [1][2] = x^2 + [2].$$

Ring Structure of $F[x]$

Polynomials are added and multiplied in the expected way.

Example 10.9

In $\mathbb{Z}_3[x]$, we have

$$\begin{aligned}
&(x^4 + [2]x^3 + [1]) + ([2]x^4 + x^2 + [1]) \\
&= ([1]x^4 + [2]x^3 + [1]) + ([2]x^4 + [1]x^2 + [1]) \\
&\qquad = ([1] + [2])x^4 + [2]x^3 + [1]x^2 + ([1] + [1]) \\
&\qquad = [0]x^4 + [2]x^3 + [1]x^2 + [2] \\
&\qquad = [2]x^3 + x^2 + [2]
\end{aligned}$$

and

$$(x + [1])(x + [2]) = x^2 + ([1] + [2])x + [1][2] = x^2 + [2].$$

Polynomial Division

Definition 10.10

Let F be a field and $f(x) = a_0 + a_1x + a_2 + \cdots + a_dx^d$ be a polynomial with $a_d \neq 0$.

(i) The *degree* of $f(x)$ is d. This is written $\deg f(x) = d$.

(ii) The *constant coefficient* of $f(x)$ is a_0.

(iii) The *leading coefficient* of $f(x)$ is a_d.

(iv) If $a_d = 1$ then we say that $f(x)$ is *monic*.

The degree of zero polynomial $f(x) = 0$ is undefined.

Polynomial Division

Definition 10.10

Let F be a field and $f(x) = a_0 + a_1x + a_2 + \cdots + a_dx^d$ be a polynomial with $a_d \neq 0$.

(i) The *degree* of $f(x)$ is d. This is written $\deg f(x) = d$.

(ii) The *constant coefficient* of $f(x)$ is a_0.

(iii) The *leading coefficient* of $f(x)$ is a_d.

(iv) If $a_d = 1$ then we say that $f(x)$ is *monic*.

The degree of zero polynomial $f(x) = 0$ is undefined.

Theorem 10.11

Let F be a field, let $f(x) \in F[x]$ be a non-zero polynomial and let $g(x) \in F[x]$. There exist polynomials $q(x), r(x) \in F[x]$ such that

$$g(x) = q(x)f(x) + r(x)$$

and either $r(x) = 0$ or $\deg r(x) < \deg f(x)$.

Examples of Polynomial Division

Example 10.12

(1) Working in $\mathbb{Q}[x]$, let $g(x) = 3x^2 + 2x - 1$ and let $f(x) = 2x + 1$. Then

$$g(x) = (\tfrac{3}{2}x + \tfrac{1}{4})f(x) - \tfrac{5}{4}$$

so the quotient is $q(x) = \frac{3}{2}x + \frac{1}{4}$ and the remainder is $r(x) = -\frac{5}{4}$. If instead we take $h(x) = x + 1$ then

$$g(x) = (3x - 1)h(x).$$

So when $g(x)$ is divided by $h(x)$ the quotient is $3x - 1$ and the remainder is 0.

(2) Working in $\mathbb{Z}_3[x]$, let $g(x) = x^4 + x^3 + [2]x^2 + x + 1$ and let $f(x) = x^2 + x$. Then

$$g(x) = (x^2 + [2]x)f(x) + 2[x] + 1.$$

Remainder Theorem

Theorem 10.13

Let F be a field and let $f(x) \in F[x]$ be a polynomial. Let $c \in F$. Then

$$f(x) = q(x)(x - c) + r$$

for some polynomial $q(x) \in F[x]$ and some $r \in \mathbb{F}$. Moreover $f(c) = 0$ if and only if $r = 0$.

Example of Remainder Theorem

Example 10.14

Working in $\mathbb{Z}_3[x]$, let $g(x) = x^4 + x^3 + [2]x^2 + x + [1]$ as in Example 10.10(2). Since

$$g([1]) = [1] + [1] + [2] + [1] + [1] = [6] = [0],$$

the Factor Theorem says that $x - [1]$ divides $g(x)$. Division gives

$$g(x) = (x - [1])(x^3 + [2]x^2 + x + [2]).$$

The cubic $x^3 + [2]x^2 + x + [2]$ also has $[1]$ as a root. Dividing it by $x - [1]$ gives

$$g(x) = (x - [1])^2(x^2 + [1]).$$

Therefore $g(x)$ has $[1]$ as a root with multiplicity 2, and no other roots in $\mathbb{Z}_3$.

Polynomials in $\mathbb{C}[x]$

We end with a corollary of Theorem 10.9 that gives a stronger version of the Fundamental Theorem of Algebra (Theorem 3.21).

Corollary 10.15

Let $g(x) \in \mathbb{C}[x]$ be a polynomial of degree d. There exist distinct $w_1, w_2, \ldots, w_r \in \mathbb{C}$ and $m_1, \ldots, m_r \in \mathbb{N}$ such that $m_1 + \cdots + m_r = d$ and

$$a_d z^d + a_{d-1} z^{d-1} + \cdots + a_1 z + a_0 = a_d (z - w_1)^{m_1} (z - w_2)^{m_2} \ldots (z - w_r)^{m_r}.$$