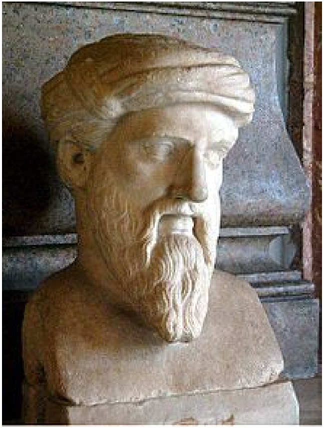
Diophantine equations, Diophantine approximation, and geometry of numbers

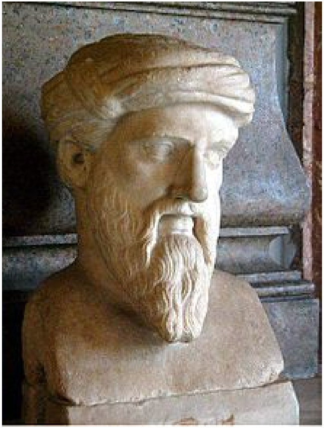
Damien Roy

University of Ottawa

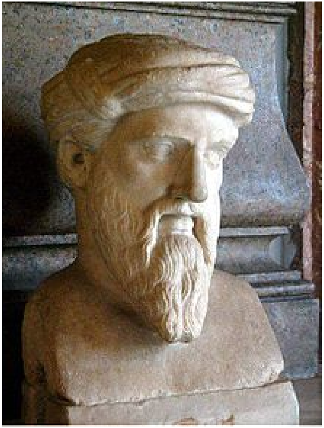
Ottawa Mathematics Conference

May 17-18, 2013



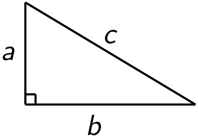


Pythagoras
(-570BC to -495BC)



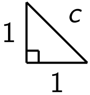
Pythagoras
(-570BC to -495BC)

Pythagorean theorem:



$$a^2 + b^2 = c^2$$

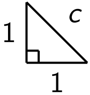
Two problems

1. The triangle 

has $c = \sqrt{2} \notin \mathbb{Q}$.

How to handle such numbers?

Two problems

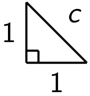
1. The triangle 

has $c = \sqrt{2} \notin \mathbb{Q}$.

How to handle such numbers?

2. Find integer right-angle triangles.

Two problems

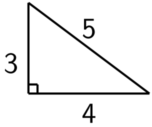
1. The triangle 

has $c = \sqrt{2} \notin \mathbb{Q}$.

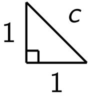
How to handle such numbers?

2. Find integer right-angle triangles.

Example: $3^2 + 4^2 = 5^2$:



Two problems

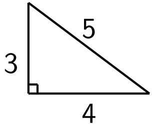
1. The triangle 

has $c = \sqrt{2} \notin \mathbb{Q}$.

How to handle such numbers?

2. Find integer right-angle triangles.

Example: $3^2 + 4^2 = 5^2$:



$$5^2 + 12^2 = 13^2, \ \ldots$$

Diophantine equation

= an equation to be solved in integers

Diophantine equation

= an equation to be solved in integers

1. $\boxed{a^2 + b^2 = c^2}$ $\quad a, b, c \in \mathbb{Z}$

Diophantine equation

= an equation to be solved in integers

1. $\boxed{a^2 + b^2 = c^2}$ $\quad a, b, c \in \mathbb{Z}$

$$\iff \quad (a, b, c) \text{ or } (b, a, c) = d(u^2 - v^2, 2uv, u^2 + v^2)$$

with $d, u, v \in \mathbb{Z}$, $\gcd(u, v) = 1$, $u \not\equiv v \mod 2$.

Diophantine equation

$= $ an equation to be solved in integers

1. $\boxed{a^2 + b^2 = c^2}$ $\quad a, b, c \in \mathbb{Z}$

$$\iff \quad (a,b,c) \text{ or } (b,a,c) = d(u^2 - v^2, 2uv, u^2 + v^2)$$
$$\text{with } d, u, v \in \mathbb{Z},\ \gcd(u,v) = 1,\ u \not\equiv v \mod 2.$$

Example: $d = 1$, $u = 2$, $v = 1$ yields $a = 3$, $b = 4$, $c = 5$

Diophantine equation

= an equation to be solved in integers

1. $\boxed{a^2 + b^2 = c^2}$ $\quad a, b, c \in \mathbb{Z}$

$$\iff \quad (a, b, c) \text{ or } (b, a, c) = d(u^2 - v^2, 2uv, u^2 + v^2)$$
$$\text{with } d, u, v \in \mathbb{Z},\ \gcd(u, v) = 1,\ u \not\equiv v \mod 2.$$

Example: $d = 1,\ u = 2,\ v = 1$ yields $a = 3,\ b = 4,\ c = 5$

2. $\boxed{a^n + b^n = c^n}$ $\quad a, b, c \geq 1,\ n \geq 3$ (Fermat, 1601-1665)

Diophantine equation

= an equation to be solved in integers

1. $\boxed{a^2 + b^2 = c^2}$ $\quad a, b, c \in \mathbb{Z}$

   $$\iff \quad (a, b, c) \text{ or } (b, a, c) = d(u^2 - v^2, 2uv, u^2 + v^2)$$
   with $d, u, v \in \mathbb{Z}$, $\gcd(u, v) = 1$, $u \not\equiv v \mod 2$.

   Example: $d = 1$, $u = 2$, $v = 1$ yields $a = 3$, $b = 4$, $c = 5$

2. $\boxed{a^n + b^n = c^n}$ $\quad a, b, c \geq 1$, $n \geq 3$ (Fermat, 1601-1665)

   no solution: Wiles 1993, Taylor-Wiles 1994

Diophantine equation

= an equation to be solved in integers

1. $\boxed{a^2 + b^2 = c^2}$ $\quad a, b, c \in \mathbb{Z}$

   $\iff$ (a, b, c) or $(b, a, c) = d(u^2 - v^2, 2uv, u^2 + v^2)$
   with $d, u, v \in \mathbb{Z}$, $\gcd(u, v) = 1$, $u \not\equiv v \mod 2$.

   Example: $d = 1$, $u = 2$, $v = 1$ yields $a = 3$, $b = 4$, $c = 5$

2. $\boxed{a^n + b^n = c^n}$ $\quad a, b, c \geq 1$, $n \geq 3$ (Fermat, 1601-1665)

   no solution: Wiles 1993, Taylor-Wiles 1994

3. $\boxed{a^m = b^n + 1}$ $\quad a, b, m, n \geq 2$ (Catalan, 1844)

Diophantine equation

$= \text{an equation to be solved in integers}$

1. $\boxed{a^2 + b^2 = c^2}$ $\quad a, b, c \in \mathbb{Z}$

   $\iff \quad (a, b, c)$ or $(b, a, c) = d(u^2 - v^2, 2uv, u^2 + v^2)$
   with $d, u, v \in \mathbb{Z}$, $\gcd(u, v) = 1$, $u \not\equiv v \mod 2$.

   Example: $d = 1$, $u = 2$, $v = 1$ yields $a = 3$, $b = 4$, $c = 5$

2. $\boxed{a^n + b^n = c^n}$ $\quad a, b, c \geq 1$, $n \geq 3$ (Fermat, 1601-1665)

   no solution: Wiles 1993, Taylor-Wiles 1994

3. $\boxed{a^m = b^n + 1}$ $\quad a, b, m, n \geq 2$ (Catalan, 1844)

   only solution: $3^2 = 2^3 + 1$: Mihăilescu 2002

Diophantine equation

= an equation to be solved in integers

1. $\boxed{a^2 + b^2 = c^2}$ $\quad a, b, c \in \mathbb{Z}$

   $\iff$ (a, b, c) or $(b, a, c) = d(u^2 - v^2, 2uv, u^2 + v^2)$
   with $d, u, v \in \mathbb{Z}$, $\gcd(u, v) = 1$, $u \not\equiv v \mod 2$.

   Example: $d = 1$, $u = 2$, $v = 1$ yields $a = 3$, $b = 4$, $c = 5$

2. $\boxed{a^n + b^n = c^n}$ $\quad a, b, c \geq 1$, $n \geq 3$ (Fermat, 1601-1665)

   no solution: Wiles 1993, Taylor-Wiles 1994

3. $\boxed{a^m = b^n + 1}$ $\quad a, b, m, n \geq 2$ (Catalan, 1844)

   only solution: $3^2 = 2^3 + 1$: Mihăilescu 2002

4. $\boxed{a^2 = db^2 + 1}$ $\quad d$ not a square ("Pell's equation")

Diophantine equation

= an equation to be solved in integers

1. $\boxed{a^2 + b^2 = c^2}$ $\quad a, b, c \in \mathbb{Z}$

   $\iff$ (a, b, c) or $(b, a, c) = d(u^2 - v^2, 2uv, u^2 + v^2)$
   with $d, u, v \in \mathbb{Z}$, $\gcd(u, v) = 1$, $u \not\equiv v \mod 2$.

   Example: $d = 1$, $u = 2$, $v = 1$ yields $a = 3$, $b = 4$, $c = 5$

2. $\boxed{a^n + b^n = c^n}$ $\quad a, b, c \geq 1$, $n \geq 3$ (Fermat, 1601-1665)

   no solution: Wiles 1993, Taylor-Wiles 1994

3. $\boxed{a^m = b^n + 1}$ $\quad a, b, m, n \geq 2$ (Catalan, 1844)

   only solution: $3^2 = 2^3 + 1$: Mihăilescu 2002

4. $\boxed{a^2 = db^2 + 1}$ $\quad d$ not a square ("Pell's equation")

   has infinitely many solutions for each d: Lagrange (1768)

A particular Pell equation: $a^2 = 2b^2 + 1 \ \ (a, b \geq 1)$

Solutions: $(a, b) = (3, 2), (17, 12), \ldots$

A particular Pell equation: $a^2 = 2b^2 + 1 \ \ (a, b \geq 1)$

Solutions: $(a, b) = (3, 2), (17, 12), \ldots$

$a^2 = 2b^2 + 1$

A particular Pell equation: $a^2 = 2b^2 + 1 \ \ (a, b \geq 1)$

Solutions: $(a, b) = (3, 2), (17, 12), \ldots$

$a^2 = 2b^2 + 1$

$\Leftrightarrow a^2 - 2b^2 = 1$

A particular Pell equation: $a^2 = 2b^2 + 1 \ \ (a, b \geq 1)$

Solutions: $(a, b) = (3, 2), (17, 12), \ldots$

$$a^2 = 2b^2 + 1$$

$$\Leftrightarrow a^2 - 2b^2 = 1$$

$$\Leftrightarrow (a - b\sqrt{2})(a + b\sqrt{2}) = 1$$

A particular Pell equation: $a^2 = 2b^2 + 1 \ \ (a, b \geq 1)$

Solutions: $(a, b) = (3, 2), (17, 12), \ldots$

$$
\begin{aligned}
& a^2 = 2b^2 + 1 \\
& \qquad \Leftrightarrow a^2 - 2b^2 = 1 \\
& \qquad \Leftrightarrow (a - b\sqrt{2})(a + b\sqrt{2}) = 1 \\
& \qquad \Rightarrow 0 \leq a - b\sqrt{2} = \frac{1}{a + b\sqrt{2}} \leq \frac{1}{2b\sqrt{2}} \qquad (\text{since } a \geq b\sqrt{2})
\end{aligned}
$$

A particular Pell equation: $a^2 = 2b^2 + 1 \;\; (a, b \geq 1)$

Solutions: $(a, b) = (3, 2), (17, 12), \ldots$

$$\begin{aligned}
a^2 &= 2b^2 + 1 \\
&\Leftrightarrow a^2 - 2b^2 = 1 \\
&\Leftrightarrow (a - b\sqrt{2})(a + b\sqrt{2}) = 1 \\
&\Rightarrow 0 \leq a - b\sqrt{2} = \frac{1}{a + b\sqrt{2}} \leq \frac{1}{2b\sqrt{2}} \qquad (\text{since } a \geq b\sqrt{2}) \\
&\Rightarrow \left| \frac{a}{b} - \sqrt{2} \right| \leq \frac{1}{2b^2\sqrt{2}} \leq \frac{1}{2b^2}
\end{aligned}$$

A particular Pell equation: $a^2 = 2b^2 + 1 \;\; (a, b \geq 1)$

Solutions: $(a, b) = (3, 2), (17, 12), \ldots$

$$
\begin{aligned}
a^2 &= 2b^2 + 1 \\
&\Leftrightarrow a^2 - 2b^2 = 1 \\
&\Leftrightarrow (a - b\sqrt{2})(a + b\sqrt{2}) = 1 \\
&\Rightarrow 0 \leq a - b\sqrt{2} = \frac{1}{a + b\sqrt{2}} \leq \frac{1}{2b\sqrt{2}} \qquad (\text{since } a \geq b\sqrt{2}) \\
&\Rightarrow \left| \frac{a}{b} - \sqrt{2} \right| \leq \frac{1}{2b^2\sqrt{2}} \leq \frac{1}{2b^2}
\end{aligned}
$$

i.e. $\dfrac{a}{b}$ is a very good rational approximation to $\sqrt{2}$.

Continued fractions

$$\frac{31}{22}$$

Continued fractions

$$\frac{31}{22} = 1 + \frac{9}{22}$$

Continued fractions

$$\frac{31}{22} = 1 + \frac{9}{22} = 1 + \frac{1}{\frac{22}{9}}$$

Continued fractions

$$\frac{31}{22} = 1 + \frac{9}{22} = 1 + \cfrac{1}{\frac{22}{9}} = 1 + \cfrac{1}{2 + \frac{4}{9}}$$

Continued fractions

$$\frac{31}{22} = 1 + \frac{9}{22} = 1 + \frac{1}{\frac{22}{9}} = 1 + \frac{1}{2 + \frac{4}{9}} = 1 + \frac{1}{2 + \frac{1}{\frac{9}{4}}}$$

Continued fractions

$$\frac{31}{22} = 1 + \frac{9}{22} = 1 + \cfrac{1}{\frac{22}{9}} = 1 + \cfrac{1}{2 + \frac{4}{9}} = 1 + \cfrac{1}{2 + \cfrac{1}{\frac{9}{4}}} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \frac{1}{4}}}$$

Continued fractions

$$\frac{31}{22} = 1 + \frac{9}{22} = 1 + \frac{1}{\frac{22}{9}} = 1 + \frac{1}{2 + \frac{4}{9}} = 1 + \frac{1}{2 + \frac{1}{\frac{9}{4}}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{4}}}$$

$$= (1, 2, 2, 4)$$

Continued fractions

$$\frac{31}{22} = 1 + \frac{9}{22} = 1 + \frac{1}{\frac{22}{9}} = 1 + \frac{1}{2 + \frac{4}{9}} = 1 + \frac{1}{2 + \frac{1}{\frac{9}{4}}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{4}}}$$

$$= (1, 2, 2, 4)$$

$\sqrt{2}$

Continued fractions

$$\frac{31}{22} = 1 + \frac{9}{22} = 1 + \frac{1}{\frac{22}{9}} = 1 + \frac{1}{2 + \frac{4}{9}} = 1 + \frac{1}{2 + \frac{1}{\frac{9}{4}}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{4}}}$$

$$= (1, 2, 2, 4)$$

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

Continued fractions

$$\frac{31}{22} = 1 + \frac{9}{22} = 1 + \frac{1}{\frac{22}{9}} = 1 + \frac{1}{2 + \frac{4}{9}} = 1 + \frac{1}{2 + \frac{1}{\frac{9}{4}}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{4}}}$$

$$= (1, 2, 2, 4)$$

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

Continued fractions

$$\frac{31}{22} = 1 + \frac{9}{22} = 1 + \frac{1}{\frac{22}{9}} = 1 + \frac{1}{2 + \frac{4}{9}} = 1 + \frac{1}{2 + \frac{1}{\frac{9}{4}}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{4}}}$$

$$= (1, 2, 2, 4)$$

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

Continued fractions

$$\frac{31}{22} = 1 + \frac{9}{22} = 1 + \frac{1}{\frac{22}{9}} = 1 + \frac{1}{2 + \frac{4}{9}} = 1 + \frac{1}{2 + \frac{1}{\frac{9}{4}}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{4}}}$$

$$= (1, 2, 2, 4)$$

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

$$= 1 + \frac{1}{2 + \frac{1}{\sqrt{2} + 1}}$$

Continued fractions

$$\frac{31}{22} = 1 + \frac{9}{22} = 1 + \frac{1}{\frac{22}{9}} = 1 + \frac{1}{2 + \frac{4}{9}} = 1 + \frac{1}{2 + \frac{1}{\frac{9}{4}}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{4}}}$$

$$= (1, 2, 2, 4)$$

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

$$= 1 + \frac{1}{2 + \frac{1}{\sqrt{2} + 1}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\ddots}}}}$$

Continued fractions

$$\frac{31}{22} = 1 + \frac{9}{22} = 1 + \frac{1}{\frac{22}{9}} = 1 + \frac{1}{2 + \frac{4}{9}} = 1 + \frac{1}{2 + \frac{1}{\frac{9}{4}}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{4}}}$$

$$= (1, 2, 2, 4)$$

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

$$= 1 + \frac{1}{2 + \frac{1}{\sqrt{2} + 1}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\ddots}}}} = (1, 2, 2, 2, \dots)$$

Convergents

The continued fraction expansion of $\xi \in \mathbb{R}$ is

Convergents

The continued fraction expansion of $\xi \in \mathbb{R}$ is

- finite $\iff \xi \in \mathbb{Q}$

Convergents

The continued fraction expansion of $\xi \in \mathbb{R}$ is

- finite $\Longleftrightarrow \xi \in \mathbb{Q}$
- ultimately periodic $\Longleftrightarrow \xi$ is quadratic over $\mathbb{Q}$

Convergents

The continued fraction expansion of $\xi \in \mathbb{R}$ is

- finite $\iff \xi \in \mathbb{Q}$
- ultimately periodic $\iff \xi$ is quadratic over $\mathbb{Q}$

The convergents of $\xi = (a_0, a_1, a_2, \ldots) = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$

Convergents

The continued fraction expansion of $\xi \in \mathbb{R}$ is

- finite $\iff \xi \in \mathbb{Q}$
- ultimately periodic $\iff \xi$ is quadratic over $\mathbb{Q}$

The convergents of $\xi = (a_0, a_1, a_2, \dots) = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$

are $\dfrac{p_n}{q_n} = (a_0, a_1, \dots, a_n) = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{\ddots}{+\cfrac{1}{a_n}}}} \in \mathbb{Q}$.

Application to Pell equation

Theorem (Legendre)

$$\left|\frac{a}{b} - \xi\right| \leq \frac{1}{2b^2} \implies \frac{a}{b} \textit{ is a convergent of } \xi$$

Application to Pell equation

Theorem (Legendre)

$$\left|\frac{a}{b} - \xi\right| \leq \frac{1}{2b^2} \implies \frac{a}{b} \text{ is a convergent of } \xi$$

$\implies$ The solutions of a Pell equation $a^2 = db^2 + 1$ come from convergents $\dfrac{a}{b}$ of $\sqrt{d}$.

Application to Pell equation

Theorem (Legendre)

$$\left|\frac{a}{b} - \xi\right| \leq \frac{1}{2b^2} \implies \frac{a}{b} \text{ is a convergent of } \xi$$

$\implies$ The solutions of a Pell equation $a^2 = db^2 + 1$ come from convergents $\frac{a}{b}$ of $\sqrt{d}$.

Example: $a^2 = 2b^2 + 1$

Application to Pell equation

Theorem (Legendre)

$$\left|\frac{a}{b} - \xi\right| \leq \frac{1}{2b^2} \implies \frac{a}{b} \textit{ is a convergent of } \xi$$

$\implies$ The solutions of a Pell equation $a^2 = db^2 + 1$ come from convergents $\dfrac{a}{b}$ of $\sqrt{d}$.

Example: $a^2 = 2b^2 + 1 \rightsquigarrow \sqrt{2} = (1, 2, 2, 2, \dots)$

Application to Pell equation

Theorem (Legendre)

$$\left|\frac{a}{b} - \xi\right| \leq \frac{1}{2b^2} \implies \frac{a}{b} \textit{ is a convergent of } \xi$$

$\implies$ The solutions of a Pell equation $a^2 = db^2 + 1$ come from convergents $\dfrac{a}{b}$ of $\sqrt{d}$.

Example: $a^2 = 2b^2 + 1 \rightsquigarrow \sqrt{2} = (1, 2, 2, 2, \ldots)$

- $(1, 2) = 1 + \dfrac{1}{2} = \dfrac{3}{2}$ is a convergent of $\sqrt{2}$:

Application to Pell equation

Theorem (Legendre)

$$\left|\frac{a}{b}-\xi\right| \leq \frac{1}{2b^2} \implies \frac{a}{b} \textit{ is a convergent of } \xi$$

$\implies$ The solutions of a Pell equation $a^2 = db^2 + 1$ come from convergents $\dfrac{a}{b}$ of $\sqrt{d}$.

Example: $a^2 = 2b^2 + 1 \quad \rightsquigarrow \quad \sqrt{2} = (1, 2, 2, 2, \dots)$

- $(1, 2) = 1 + \dfrac{1}{2} = \dfrac{3}{2}$ is a convergent of $\sqrt{2}$: $\quad \boxed{3^2 = 2 \times 2^2 + 1}$

Application to Pell equation

Theorem (Legendre)

$$\left|\frac{a}{b} - \xi\right| \leq \frac{1}{2b^2} \implies \frac{a}{b} \textit{ is a convergent of } \xi$$

$\implies$ The solutions of a Pell equation $a^2 = db^2 + 1$ come from convergents $\frac{a}{b}$ of $\sqrt{d}$.

Example: $a^2 = 2b^2 + 1 \rightsquigarrow \sqrt{2} = (1, 2, 2, 2, \dots)$

- $(1, 2) = 1 + \frac{1}{2} = \frac{3}{2}$ is a convergent of $\sqrt{2}$: $\boxed{3^2 = 2 \times 2^2 + 1}$
- $(1, 2, 2) = 1 + \cfrac{1}{2 + \cfrac{1}{2}} = \frac{7}{5}$ is a convergent of $\sqrt{2}$:

Application to Pell equation

Theorem (Legendre)

$$\left|\frac{a}{b} - \xi\right| \leq \frac{1}{2b^2} \implies \frac{a}{b} \text{ is a convergent of } \xi$$

$\implies$ The solutions of a Pell equation $a^2 = db^2 + 1$ come from convergents $\frac{a}{b}$ of $\sqrt{d}$.

Example: $a^2 = 2b^2 + 1 \rightsquigarrow \sqrt{2} = (1, 2, 2, 2, \dots)$

- $(1, 2) = 1 + \frac{1}{2} = \frac{3}{2}$ is a convergent of $\sqrt{2}$: $\boxed{3^2 = 2 \times 2^2 + 1}$
- $(1, 2, 2) = 1 + \cfrac{1}{2 + \cfrac{1}{2}} = \frac{7}{5}$ is a convergent of $\sqrt{2}$: $\boxed{7^2 = 2 \times 5^2 - 1}$

Application to Pell equation

Theorem (Legendre)

$$\left|\frac{a}{b} - \xi\right| \le \frac{1}{2b^2} \implies \frac{a}{b} \textit{ is a convergent of } \xi$$

$\implies$ The solutions of a Pell equation $a^2 = db^2 + 1$ come from convergents $\dfrac{a}{b}$ of $\sqrt{d}$.

Example: $a^2 = 2b^2 + 1 \leadsto \sqrt{2} = (1, 2, 2, 2, \dots)$

- $(1,2) = 1 + \dfrac{1}{2} = \dfrac{3}{2}$ is a convergent of $\sqrt{2}$: $\boxed{3^2 = 2 \times 2^2 + 1}$
- $(1,2,2) = 1 + \dfrac{1}{2 + \dfrac{1}{2}} = \dfrac{7}{5}$ is a convergent of $\sqrt{2}$: $\boxed{7^2 = 2 \times 5^2 - 1}$
- $(1,2,2,2) = \dfrac{17}{12}$ is a convergent of $\sqrt{2}$:

Application to Pell equation

Theorem (Legendre)

$$\left|\frac{a}{b} - \xi\right| \leq \frac{1}{2b^2} \implies \frac{a}{b} \textit{ is a convergent of } \xi$$

$\implies$ The solutions of a Pell equation $a^2 = db^2 + 1$ come from convergents $\frac{a}{b}$ of $\sqrt{d}$.

Example: $a^2 = 2b^2 + 1 \rightsquigarrow \sqrt{2} = (1, 2, 2, 2, \dots)$

- $(1,2) = 1 + \frac{1}{2} = \frac{3}{2}$ is a convergent of $\sqrt{2}$: $\boxed{3^2 = 2 \times 2^2 + 1}$
- $(1,2,2) = 1 + \cfrac{1}{2 + \cfrac{1}{2}} = \frac{7}{5}$ is a convergent of $\sqrt{2}$: $\boxed{7^2 = 2 \times 5^2 - 1}$
- $(1,2,2,2) = \frac{17}{12}$ is a convergent of $\sqrt{2}$: $\boxed{17^2 = 2 \times 12^2 + 1}$

Axel Thue
(Norway, 1863-1922)

Thue equation

Axel Thue
(Norway, 1863-1922)

A Thue equation is an equation of the form

$$p(x, y) = m$$

where $p(x, y) \in \mathbb{Z}[x, y]$ is an irreducible homogeneous polynomial of degree ≥ 3, and where $m \in \mathbb{Z}$.

Thue equation

Axel Thue
(Norway, 1863-1922)

A Thue equation is an equation of the form

$$p(x, y) = m$$

where $p(x, y) \in \mathbb{Z}[x, y]$ is an irreducible homogeneous polynomial of degree ≥ 3, and where $m \in \mathbb{Z}$.

We search for solutions $(x, y) \in \mathbb{Z}^2$.

Example of a Thue equation

$$x^3 - 2y^3 = 1, \qquad x, y \in \mathbb{Z} \quad (x > y > 0)$$

Example of a Thue equation

$$x^3 - 2y^3 = 1, \qquad x, y \in \mathbb{Z} \quad (x > y > 0)$$

$$\iff \left(x - \sqrt[3]{2}y\right)\left(x^2 + \sqrt[3]{2}xy + \sqrt[3]{2}^2 y^2\right) = 1$$

Example of a Thue equation

$$x^3 - 2y^3 = 1, \qquad x, y \in \mathbb{Z} \quad (x > y > 0)$$

$$\iff \left(x - \sqrt[3]{2}y\right)\left(x^2 + \sqrt[3]{2}xy + \sqrt[3]{2}^2 y^2\right) = 1$$

$$\implies \left|x - \sqrt[3]{2}y\right| = \frac{1}{x^2 + \sqrt[3]{2}xy + \sqrt[3]{2}^2 y^2} \leq \frac{1}{3y^2} \ \text{ since } x \geq \sqrt[3]{2}y \geq y$$

Example of a Thue equation

$$x^3 - 2y^3 = 1, \qquad x, y \in \mathbb{Z} \quad (x > y > 0)$$

$$\iff \left(x - \sqrt[3]{2}y\right)\left(x^2 + \sqrt[3]{2}xy + \sqrt[3]{2}^2 y^2\right) = 1$$

$$\implies \left|x - \sqrt[3]{2}y\right| = \frac{1}{x^2 + \sqrt[3]{2}xy + \sqrt[3]{2}^2 y^2} \leq \frac{1}{3y^2} \;\; \text{since } x \geq \sqrt[3]{2}y \geq y$$

$$\implies \boxed{\left|\frac{x}{y} - \sqrt[3]{2}\right| \leq \frac{1}{3y^3}}$$

Example of a Thue equation

$$x^3 - 2y^3 = 1, \qquad x, y \in \mathbb{Z} \quad (x > y > 0)$$

$$\iff \left(x - \sqrt[3]{2}y\right)\left(x^2 + \sqrt[3]{2}xy + \sqrt[3]{2}^2 y^2\right) = 1$$

$$\implies \left|x - \sqrt[3]{2}y\right| = \frac{1}{x^2 + \sqrt[3]{2}xy + \sqrt[3]{2}^2 y^2} \leq \frac{1}{3y^2} \quad \text{since } x \geq \sqrt[3]{2}y \geq y$$

$$\implies \boxed{\left|\frac{x}{y} - \sqrt[3]{2}\right| \leq \frac{1}{3y^3}}$$

Does there exist such good approximations to $\sqrt[3]{2}$? How many are they ?

Thue's theorem (1909)

Let α be an algebraic number of degree $d \geq 3$. For each $\mu > 1 + \frac{d}{2}$, there exists a constant $C > 0$ such that

$$\left| \frac{x}{y} - \alpha \right| \geq \frac{C}{y^{\mu}}$$

for any $x, y \in \mathbb{Z}$ with $y > 0$.

Thue's theorem (1909)

Let α be an algebraic number of degree $d \geq 3$. For each $\mu > 1 + \frac{d}{2}$, there exists a constant $C > 0$ such that

$$\left| \frac{x}{y} - \alpha \right| \geq \frac{C}{y^{\mu}}$$

for any $x, y \in \mathbb{Z}$ with $y > 0$.

$\Longrightarrow$ Any Thue equation has at most finitely many solutions.

Thue's theorem (1909)

Let α be an algebraic number of degree $d \geq 3$. For each $\mu > 1 + \frac{d}{2}$, there exists a constant $C > 0$ such that

$$\left| \frac{x}{y} - \alpha \right| \geq \frac{C}{y^\mu}$$

for any $x, y \in \mathbb{Z}$ with $y > 0$.

$\Longrightarrow$ Any Thue equation has at most finitely many solutions.

Example: $x^3 - 2y^3 = 1$

Thue's theorem (1909)

Let α be an algebraic number of degree $d \geq 3$. For each $\mu > 1 + \frac{d}{2}$, there exists a constant $C > 0$ such that

$$\left| \frac{x}{y} - \alpha \right| \geq \frac{C}{y^\mu}$$

for any $x, y \in \mathbb{Z}$ with $y > 0$.

$\implies$ Any Thue equation has at most finitely many solutions.

Example: $x^3 - 2y^3 = 1 \ \rightsquigarrow \ d = 3$

Thue's theorem (1909)

Let α be an algebraic number of degree $d \geq 3$. For each $\mu > 1 + \frac{d}{2}$, there exists a constant $C > 0$ such that

$$\left| \frac{x}{y} - \alpha \right| \geq \frac{C}{y^{\mu}}$$

for any $x, y \in \mathbb{Z}$ with $y > 0$.

$\Longrightarrow$ Any Thue equation has at most finitely many solutions.

Example: $x^3 - 2y^3 = 1 \rightsquigarrow d = 3 \rightsquigarrow$ take $\mu = \frac{8}{3} > \frac{5}{2} = 1 + \frac{d}{2}$

Thue's theorem (1909)

Let α be an algebraic number of degree $d \geq 3$. For each $\mu > 1 + \frac{d}{2}$, there exists a constant $C > 0$ such that

$$\left| \frac{x}{y} - \alpha \right| \geq \frac{C}{y^{\mu}}$$

for any $x, y \in \mathbb{Z}$ with $y > 0$.

$\Longrightarrow$ Any Thue equation has at most finitely many solutions.

Example: $x^3 - 2y^3 = 1 \ \rightsquigarrow \ d = 3 \ \rightsquigarrow$ take $\mu = \frac{8}{3} > \frac{5}{2} = 1 + \frac{d}{2}$

$$\Longrightarrow \ \frac{1}{3y^3} \geq \left| \frac{x}{y} - \sqrt[3]{2} \right|$$

Thue's theorem (1909)

Let α be an algebraic number of degree $d \geq 3$. For each $\mu > 1 + \frac{d}{2}$, there exists a constant $C > 0$ such that

$$\left| \frac{x}{y} - \alpha \right| \geq \frac{C}{y^{\mu}}$$

for any $x, y \in \mathbb{Z}$ with $y > 0$.

$\Longrightarrow$ Any Thue equation has at most finitely many solutions.

Example: $x^3 - 2y^3 = 1 \ \rightsquigarrow \ d = 3 \ \rightsquigarrow$ take $\mu = \frac{8}{3} > \frac{5}{2} = 1 + \frac{d}{2}$

$$\Longrightarrow \quad \frac{1}{3y^3} \geq \left| \frac{x}{y} - \sqrt[3]{2} \right| \geq \frac{C}{y^{8/3}}$$

Thue's theorem (1909)

Let α be an algebraic number of degree $d \geq 3$. For each $\mu > 1 + \frac{d}{2}$, there exists a constant $C > 0$ such that

$$\left| \frac{x}{y} - \alpha \right| \geq \frac{C}{y^{\mu}}$$

for any $x, y \in \mathbb{Z}$ with $y > 0$.

$\Longrightarrow$ Any Thue equation has at most finitely many solutions.

Example: $x^3 - 2y^3 = 1 \rightsquigarrow d = 3 \rightsquigarrow$ take $\mu = \frac{8}{3} > \frac{5}{2} = 1 + \frac{d}{2}$

$$\Longrightarrow \frac{1}{3y^3} \geq \left| \frac{x}{y} - \sqrt[3]{2} \right| \geq \frac{C}{y^{8/3}} \qquad \Longrightarrow y \leq \left(\frac{1}{3C} \right)^3$$

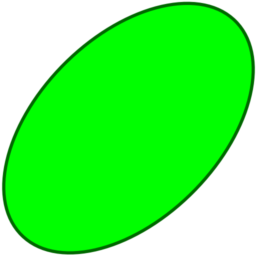
Geometry of numbers (Minkowski, 1889)

A *(Minkowski) convex body* in $\mathbb{R}^n$ is a subset of $\mathbb{R}^n$ which is

Geometry of numbers (Minkowski, 1889)

A *(Minkowski) convex body* in $\mathbb{R}^n$ is a subset of $\mathbb{R}^n$ which is

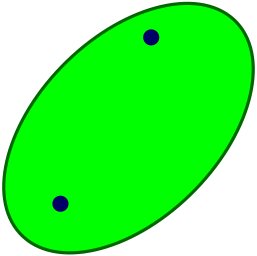
- compact,



Geometry of numbers (Minkowski, 1889)

A *(Minkowski) convex body* in $\mathbb{R}^n$ is a subset of $\mathbb{R}^n$ which is

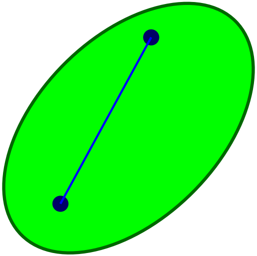
- compact,
- convex,



Geometry of numbers (Minkowski, 1889)

A *(Minkowski) convex body* in $\mathbb{R}^n$ is a subset of $\mathbb{R}^n$ which is

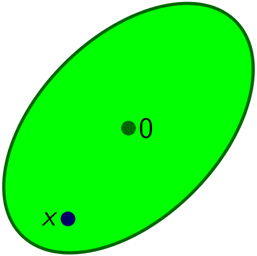
- compact,
- convex,



Geometry of numbers (Minkowski, 1889)

A *(Minkowski) convex body* in $\mathbb{R}^n$ is a subset of $\mathbb{R}^n$ which is

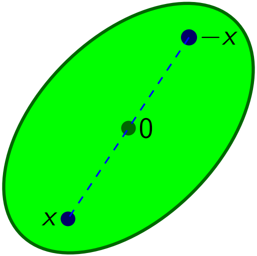
- compact,
- convex,
- symmetric with respect to 0,



Geometry of numbers (Minkowski, 1889)

A *(Minkowski) convex body* in $\mathbb{R}^n$ is a subset of $\mathbb{R}^n$ which is

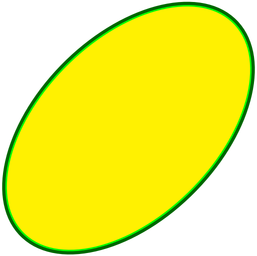
- compact,
- convex,
- symmetric with respect to 0,



Geometry of numbers (Minkowski, 1889)

A *(Minkowski) convex body* in $\mathbb{R}^n$ is a subset of $\mathbb{R}^n$ which is

- compact,
- convex,
- symmetric with respect to 0,
- and has non-empty interior.



Fact: The image of a convex body $\mathcal{C}$ of $\mathbb{R}^n$ by an invertible linear map $T\colon \mathbb{R}^n \to \mathbb{R}^n$ is a convex body $T(\mathcal{C})$ of $\mathbb{R}^n$ with

$$\mathrm{vol}(T(\mathcal{C})) = |\det(T)|\mathrm{vol}(\mathcal{C}).$$

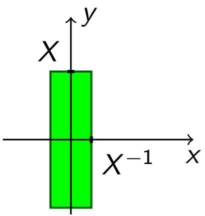
Fact: The image of a convex body $\mathcal{C}$ of $\mathbb{R}^n$ by an invertible linear map $T\colon \mathbb{R}^n \to \mathbb{R}^n$ is a convex body $T(\mathcal{C})$ of $\mathbb{R}^n$ with

$$\mathrm{vol}(T(\mathcal{C})) = |\det(T)|\mathrm{vol}(\mathcal{C}).$$

Example: Let $X \geq 1$. The rectangle

$$\mathcal{C}\colon \begin{cases} |x| \leq X^{-1} \\ |y| \leq X \end{cases}$$

is a convex body $\mathcal{C}$ of $\mathbb{R}^2$ of volume (area) 4.

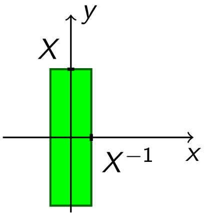


Fact: The image of a convex body $\mathcal{C}$ of $\mathbb{R}^n$ by an invertible linear map $T\colon \mathbb{R}^n \to \mathbb{R}^n$ is a convex body $T(\mathcal{C})$ of $\mathbb{R}^n$ with

$$\mathrm{vol}(T(\mathcal{C})) = |\det(T)|\mathrm{vol}(\mathcal{C}).$$

Example: Let $X \geq 1$. The rectangle

$$\mathcal{C}\colon \begin{cases} |x| \leq X^{-1} \\ |y| \leq X \end{cases}$$



is a convex body $\mathcal{C}$ of $\mathbb{R}^2$ of volume (area) 4. Given $\xi \in \mathbb{R}$, the inverse image of $\mathcal{C}$ under the linear map $T(x, y) = (x - \xi y, y)$ is the parallelogram

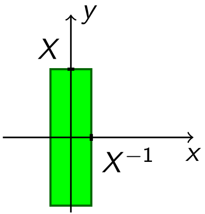
$$T^{-1}(\mathcal{C})\colon \begin{cases} |x - \xi y| \leq X^{-1} \\ \qquad |y| \leq X \end{cases}$$

Fact: The image of a convex body $\mathcal{C}$ of $\mathbb{R}^n$ by an invertible linear map $T\colon \mathbb{R}^n \to \mathbb{R}^n$ is a convex body $T(\mathcal{C})$ of $\mathbb{R}^n$ with

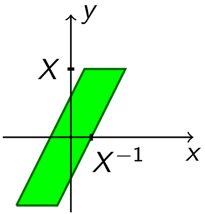
$$\mathrm{vol}(T(\mathcal{C})) = |\det(T)|\mathrm{vol}(\mathcal{C}).$$

Example: Let $X \geq 1$. The rectangle

$$\mathcal{C}\colon \begin{cases} |x| \leq X^{-1} \\ |y| \leq X \end{cases}$$



is a convex body $\mathcal{C}$ of $\mathbb{R}^2$ of volume (area) 4. Given $\xi \in \mathbb{R}$, the inverse image of $\mathcal{C}$ under the linear map $T(x, y) = (x - \xi y, y)$ is the parallelogram



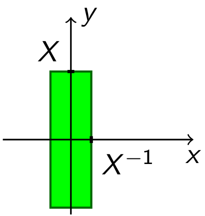
$$T^{-1}(\mathcal{C})\colon \begin{cases} |x - \xi y| \leq X^{-1} \\ |y| \leq X \end{cases}$$

Fact: The image of a convex body $\mathcal{C}$ of $\mathbb{R}^n$ by an invertible linear map $T\colon \mathbb{R}^n \to \mathbb{R}^n$ is a convex body $T(\mathcal{C})$ of $\mathbb{R}^n$ with

$$\mathrm{vol}(T(\mathcal{C})) = |\det(T)|\mathrm{vol}(\mathcal{C}).$$

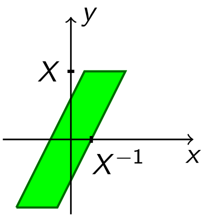
Example: Let $X \geq 1$. The rectangle

$$\mathcal{C}\colon \begin{cases} |x| \leq X^{-1} \\ |y| \leq X \end{cases}$$



is a convex body $\mathcal{C}$ of $\mathbb{R}^2$ of volume (area) 4. Given $\xi \in \mathbb{R}$, the inverse image of $\mathcal{C}$ under the linear map $T(x,y) = (x - \xi y, y)$ is the parallelogram

$$T^{-1}(\mathcal{C})\colon \begin{cases} |x - \xi y| \leq X^{-1} \\ |y| \leq X \end{cases}$$



Since $\det(T) = 1$, its volume is also 4.

Minkowski's first convex body theorem

Let $\mathcal{C}$ be a convex body of $\mathbb{R}^n$. If $\mathrm{vol}(\mathcal{C}) \geq 2^n$, then $\mathcal{C}$ contains a non-zero integer point.

Minkowski's first convex body theorem

Let $\mathcal{C}$ be a convex body of $\mathbb{R}^n$. If $\mathrm{vol}(\mathcal{C}) \geq 2^n$, then $\mathcal{C}$ contains a non-zero integer point.

Corollary (Dirichlet, 1842)

Let $\xi \in \mathbb{R}$. For each $X > 1$, there exists a non-zero point $(x, y) \in \mathbb{Z}^2$ such that

$$|x - \xi y| \leq X^{-1} \quad \textit{and} \quad |y| \leq X.$$

Minkowski's first convex body theorem

Let $\mathcal{C}$ be a convex body of $\mathbb{R}^n$. If $\mathrm{vol}(\mathcal{C}) \geq 2^n$, then $\mathcal{C}$ contains a non-zero integer point.

Corollary (Dirichlet, 1842)

Let $\xi \in \mathbb{R}$. For each $X > 1$, there exists a non-zero point $(x, y) \in \mathbb{Z}^2$ such that

$$|x - \xi y| \leq X^{-1} \quad \textit{and} \quad |y| \leq X.$$

$$\Longrightarrow \left|\frac{x}{y} - \xi\right| \leq \frac{X^{-1}}{|y|} \leq \frac{1}{y^2}.$$

Minkowski's first convex body theorem

Let $\mathcal{C}$ be a convex body of $\mathbb{R}^n$. If $\mathrm{vol}(\mathcal{C}) \geq 2^n$, then $\mathcal{C}$ contains a non-zero integer point.

Corollary (Dirichlet, 1842)

Let $\xi \in \mathbb{R}$. For each $X > 1$, there exists a non-zero point $(x, y) \in \mathbb{Z}^2$ such that

$$|x - \xi y| \leq X^{-1} \quad \textit{and} \quad |y| \leq X.$$

$$\Longrightarrow \left| \frac{x}{y} - \xi \right| \leq \frac{X^{-1}}{|y|} \leq \frac{1}{y^2}.$$

$\Longrightarrow$ If $\xi \notin \mathbb{Q}$, there are infinitely many rational numbers $\dfrac{x}{y} \in \mathbb{Q}$ with

$$\left| \frac{x}{y} - \xi \right| \leq \frac{1}{y^2}$$

Thue-Siegel-Roth theorem (1909, 1921, 1955)

Let α be an algebraic number of degree $d \geq 3$. For each $\epsilon > 0$, there exists a constant $C > 0$ such that

$$\left| \frac{x}{y} - \alpha \right| \geq \frac{C}{y^{2+\epsilon}}$$

for any $x, y \in \mathbb{Z}$ with $y > 0$.

Thue-Siegel-Roth theorem (1909, 1921, 1955)

Let α be an algebraic number of degree $d \geq 3$. For each $\epsilon > 0$, there exists a constant $C > 0$ such that

$$\left| \frac{x}{y} - \alpha \right| \geq \frac{C}{y^{2+\epsilon}}$$

for any $x, y \in \mathbb{Z}$ with $y > 0$.

"One cannot do much better than Dirichlet in approximating algebraic numbers by rational numbers."

Thue-Siegel-Roth theorem (1909, 1921, 1955)

Let α be an algebraic number of degree $d \geq 3$. For each $\epsilon > 0$, there exists a constant $C > 0$ such that

$$\left| \frac{x}{y} - \alpha \right| \geq \frac{C}{y^{2+\epsilon}}$$

for any $x, y \in \mathbb{Z}$ with $y > 0$.

"One cannot do much better than Dirichlet in approximating algebraic numbers by rational numbers."

Open problem: Can the product $|y(x - y\sqrt[3]{2})|$ be made arbitrarily small for positive integers x, y?

A more general construction

Let $\xi_1, \dots, \xi_n \in \mathbb{R}$. For each $X > 0$, the convex body of $\mathbb{R}^{n+1}$ defined by

$$|x_0 + x_1\xi_1 + \cdots + x_n\xi_n| \leq X^{-n},\ |x_1| \leq X,\ \dots,\ |x_n| \leq X \tag{1}$$

has volume 2^{n+1}.

A more general construction

Let $\xi_1, \ldots, \xi_n \in \mathbb{R}$. For each $X > 0$, the convex body of $\mathbb{R}^{n+1}$ defined by

$$|x_0 + x_1\xi_1 + \cdots + x_n\xi_n| \leq X^{-n}, \ |x_1| \leq X, \ \ldots, \ |x_n| \leq X \qquad (1)$$

has volume 2^{n+1}.

Corollary (Dirichlet, 1842)

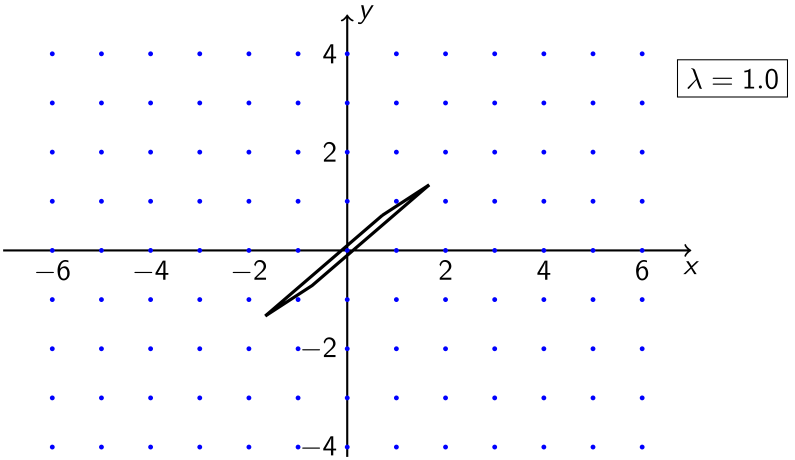
For each $X > 0$, the equations (1) have a solution in integers $x_0, \ldots, x_n$ not all 0.

Minkowski's successive minima

Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. For $i = 1, \ldots, n$, the *i-th minimum* of $\mathcal{C}$, denoted $\lambda_i(\mathcal{C})$, is the smallest λ such that $\lambda\mathcal{C}$ contains at least i linearly independent points of $\mathbb{Z}^n$.

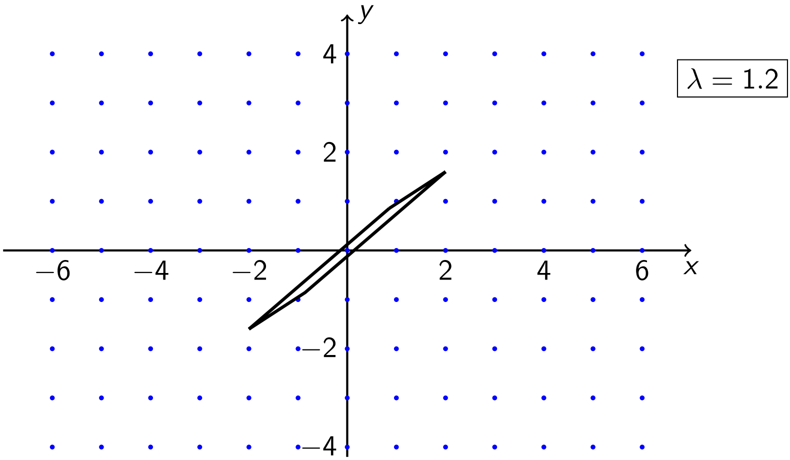
Minkowski's successive minima

Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. For $i = 1, \ldots, n$, the *i-th minimum* of $\mathcal{C}$, denoted $\lambda_i(\mathcal{C})$, is the smallest λ such that $\lambda\mathcal{C}$ contains at least i linearly independent points of $\mathbb{Z}^n$.



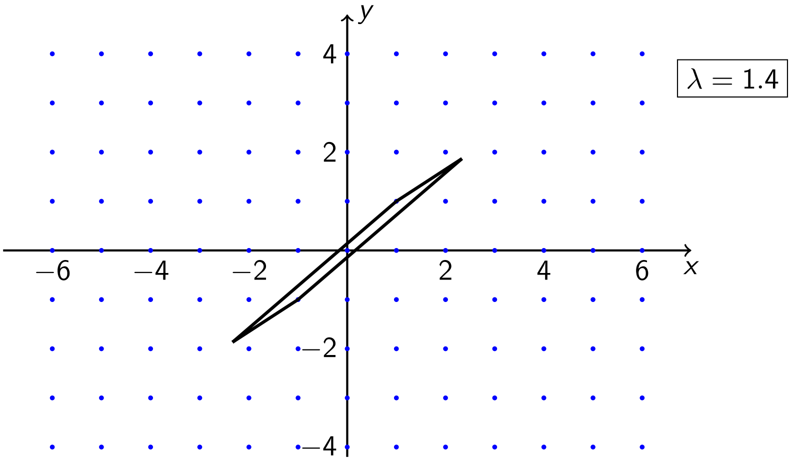
Minkowski's successive minima

Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. For $i = 1, \ldots, n$, the *i-th minimum* of $\mathcal{C}$, denoted $\lambda_i(\mathcal{C})$, is the smallest λ such that $\lambda\mathcal{C}$ contains at least i linearly independent points of $\mathbb{Z}^n$.



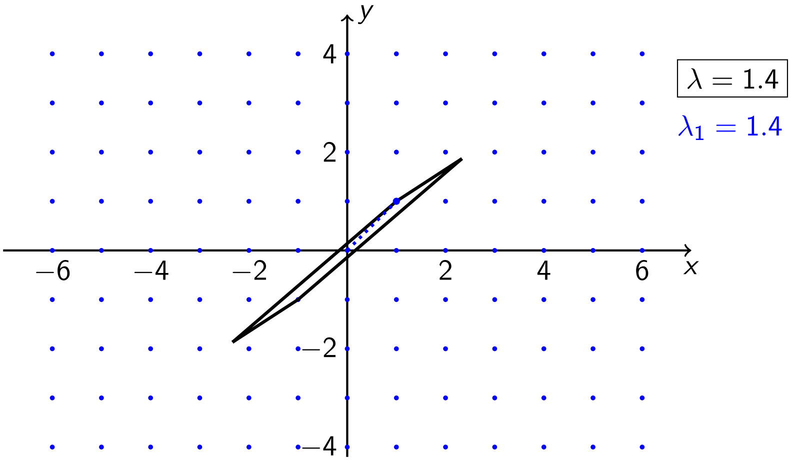
Minkowski's successive minima

Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. For $i = 1, \ldots, n$, the *i-th minimum* of $\mathcal{C}$, denoted $\lambda_i(\mathcal{C})$, is the smallest λ such that $\lambda\mathcal{C}$ contains at least i linearly independent points of $\mathbb{Z}^n$.



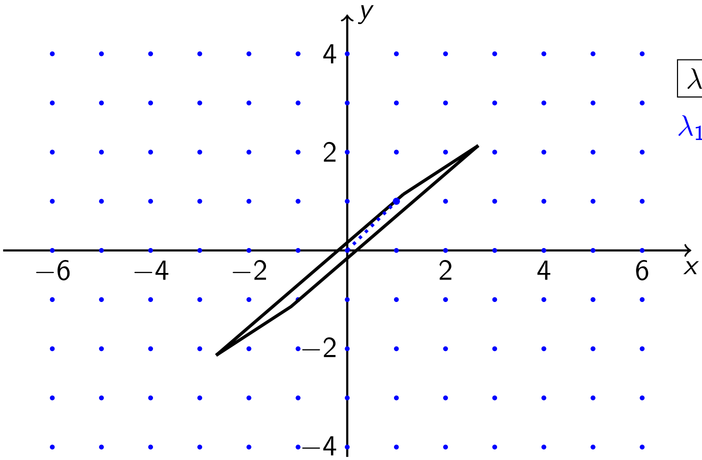
Minkowski's successive minima

Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. For $i = 1, \ldots, n$, the *i-th minimum* of $\mathcal{C}$, denoted $\lambda_i(\mathcal{C})$, is the smallest λ such that $\lambda\mathcal{C}$ contains at least i linearly independent points of $\mathbb{Z}^n$.



Minkowski's successive minima

Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. For $i = 1, \ldots, n$, the *i-th minimum* of $\mathcal{C}$, denoted $\lambda_i(\mathcal{C})$, is the smallest λ such that $\lambda\mathcal{C}$ contains at least i linearly independent points of $\mathbb{Z}^n$.

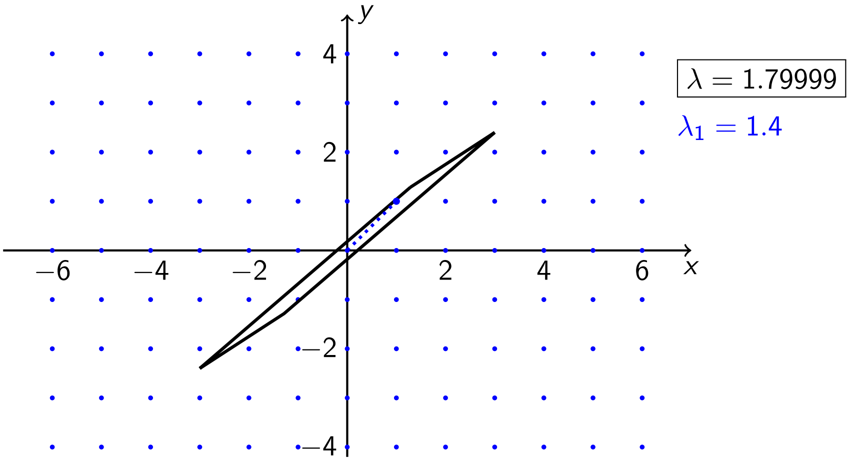


$\boxed{\lambda = 1.59999}$

$\lambda_1 = 1.4$

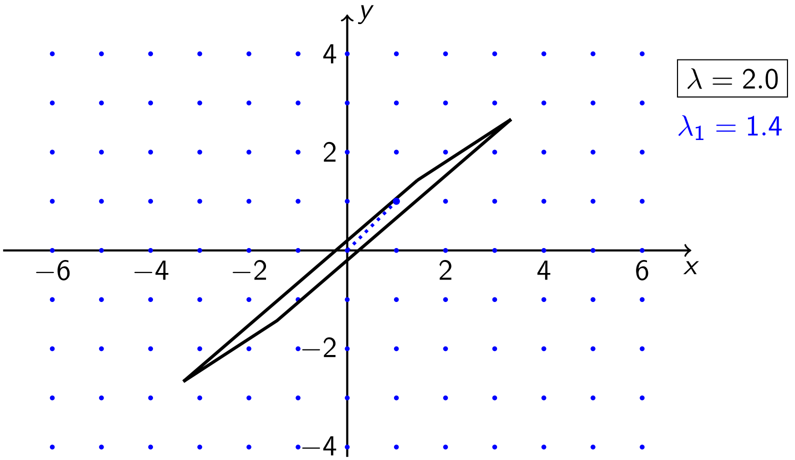
Minkowski's successive minima

Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. For $i = 1, \ldots, n$, the *i-th minimum* of $\mathcal{C}$, denoted $\lambda_i(\mathcal{C})$, is the smallest λ such that $\lambda\mathcal{C}$ contains at least i linearly independent points of $\mathbb{Z}^n$.



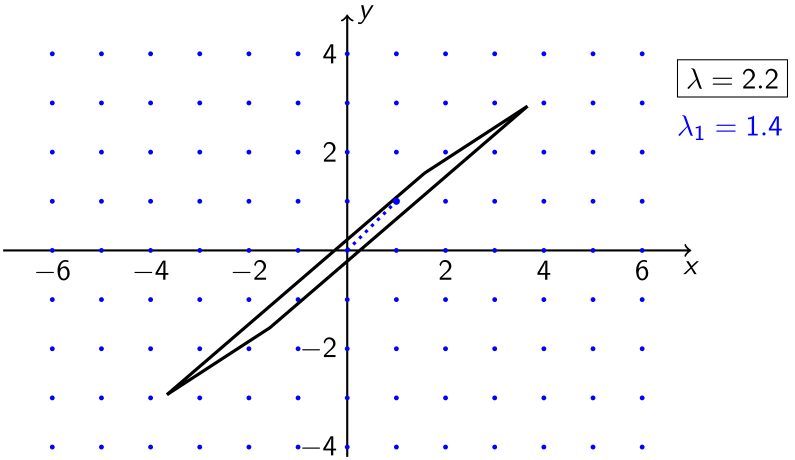
Minkowski's successive minima

Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. For $i = 1, \ldots, n$, the *i-th minimum* of $\mathcal{C}$, denoted $\lambda_i(\mathcal{C})$, is the smallest λ such that $\lambda\mathcal{C}$ contains at least i linearly independent points of $\mathbb{Z}^n$.



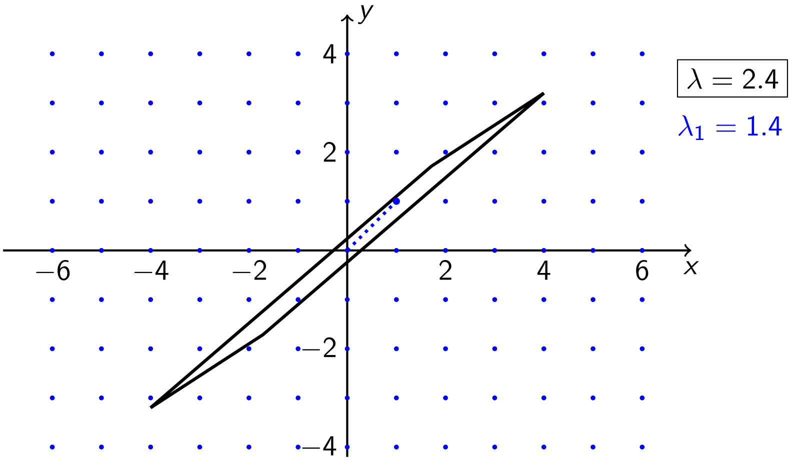
Minkowski's successive minima

Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. For $i = 1, \ldots, n$, the *i-th minimum* of $\mathcal{C}$, denoted $\lambda_i(\mathcal{C})$, is the smallest λ such that $\lambda\mathcal{C}$ contains at least i linearly independent points of $\mathbb{Z}^n$.



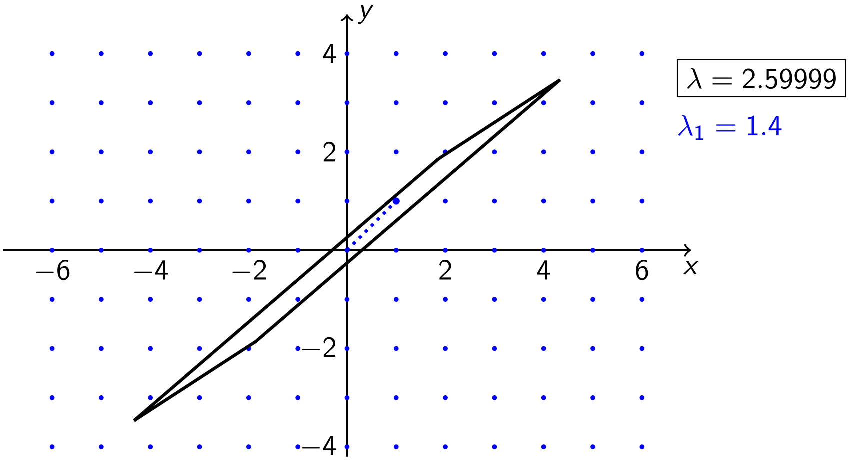
Minkowski's successive minima

Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. For $i = 1, \ldots, n$, the *i-th minimum* of $\mathcal{C}$, denoted $\lambda_i(\mathcal{C})$, is the smallest λ such that $\lambda\mathcal{C}$ contains at least i linearly independent points of $\mathbb{Z}^n$.



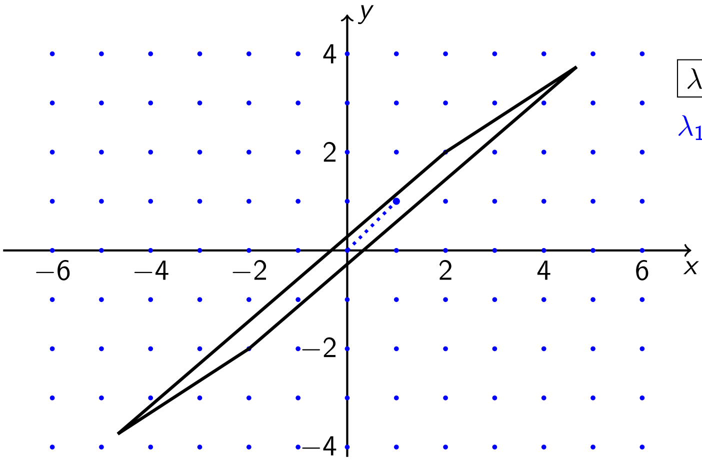
Minkowski's successive minima

Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. For $i = 1, \ldots, n$, the *i-th minimum* of $\mathcal{C}$, denoted $\lambda_i(\mathcal{C})$, is the smallest λ such that $\lambda\mathcal{C}$ contains at least i linearly independent points of $\mathbb{Z}^n$.



Minkowski's successive minima

Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. For $i = 1, \ldots, n$, the *i-th minimum* of $\mathcal{C}$, denoted $\lambda_i(\mathcal{C})$, is the smallest λ such that $\lambda\mathcal{C}$ contains at least i linearly independent points of $\mathbb{Z}^n$.

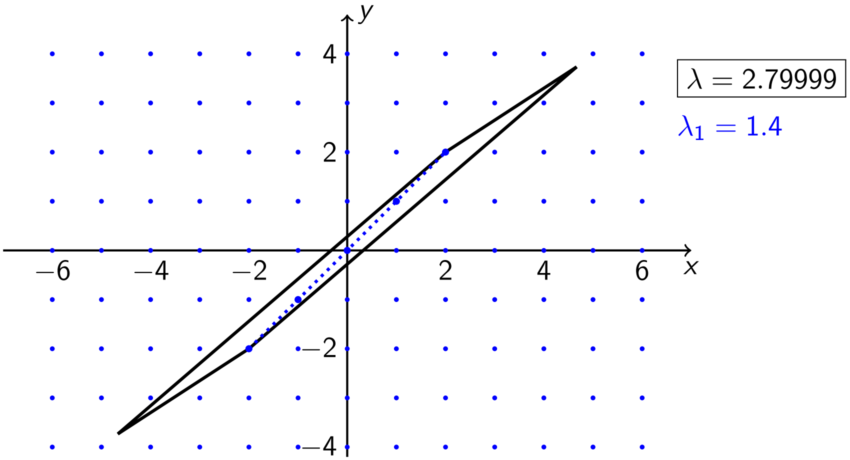


$\boxed{\lambda = 2.79999}$

$\lambda_1 = 1.4$

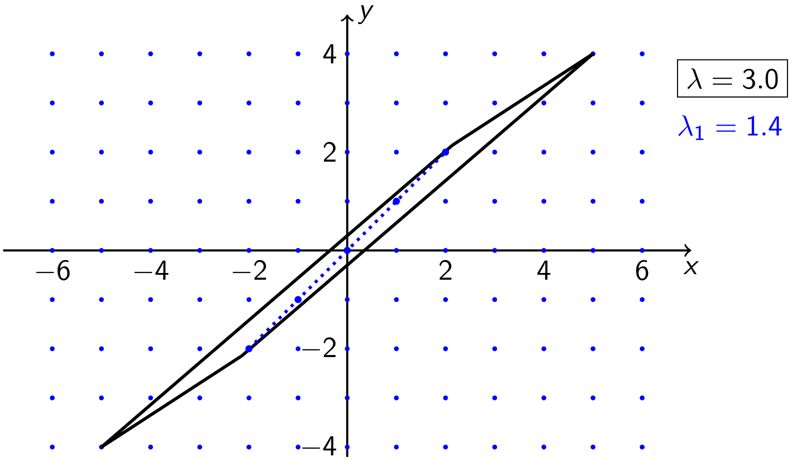
Minkowski's successive minima

Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. For $i = 1, \ldots, n$, the *i-th minimum* of $\mathcal{C}$, denoted $\lambda_i(\mathcal{C})$, is the smallest λ such that $\lambda\mathcal{C}$ contains at least i linearly independent points of $\mathbb{Z}^n$.



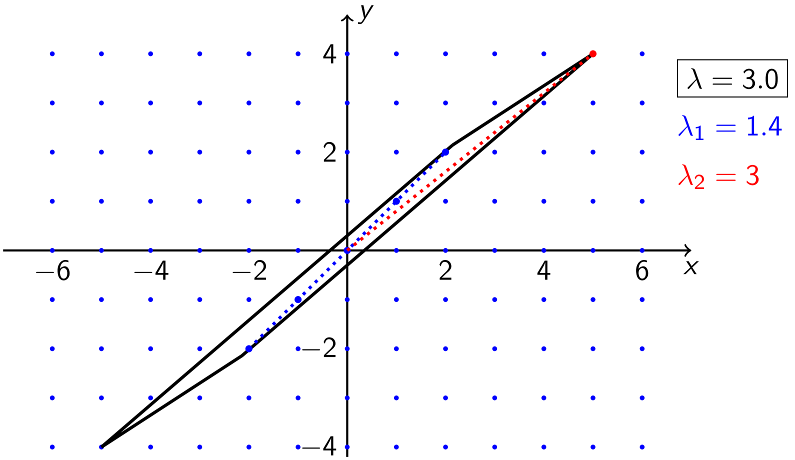
Minkowski's successive minima

Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. For $i = 1, \dots, n$, the *i-th minimum* of $\mathcal{C}$, denoted $\lambda_i(\mathcal{C})$, is the smallest λ such that $\lambda\mathcal{C}$ contains at least i linearly independent points of $\mathbb{Z}^n$.



Minkowski's successive minima

Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. For $i = 1, \ldots, n$, the *i-th minimum* of $\mathcal{C}$, denoted $\lambda_i(\mathcal{C})$, is the smallest λ such that $\lambda\mathcal{C}$ contains at least i linearly independent points of $\mathbb{Z}^n$.



Minkowski's second convex body theorem

Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. Then

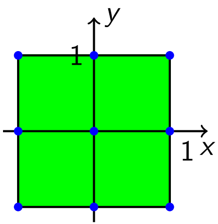
$$\frac{2^n}{n!} \leq \lambda_1(\mathcal{C}) \cdots \lambda_n(\mathcal{C}) \mathrm{vol}(\mathcal{C}) \leq 2^n.$$

Minkowski's second convex body theorem

Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. Then

$$\frac{2^n}{n!} \le \lambda_1(\mathcal{C}) \cdots \lambda_n(\mathcal{C}) \mathrm{vol}(\mathcal{C}) \le 2^n.$$

Examples ($n = 2$):

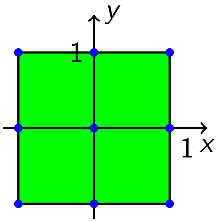


Minkowski's second convex body theorem

Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. Then

$$\frac{2^n}{n!} \leq \lambda_1(\mathcal{C}) \cdots \lambda_n(\mathcal{C})\mathrm{vol}(\mathcal{C}) \leq 2^n.$$

Examples ($n = 2$):



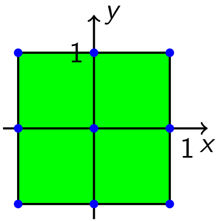
$\lambda_1 = \lambda_2 = 1$, $\mathrm{vol}(\mathcal{C}) = 4$

Minkowski's second convex body theorem

Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. Then

$$\frac{2^n}{n!} \leq \lambda_1(\mathcal{C}) \cdots \lambda_n(\mathcal{C}) \mathrm{vol}(\mathcal{C}) \leq 2^n.$$

Examples ($n = 2$):



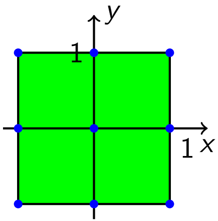
$\lambda_1 = \lambda_2 = 1$, $\mathrm{vol}(\mathcal{C}) = 4$
Here $\lambda_1 \lambda_2 \mathrm{vol}(\mathcal{C}) = 2^n$

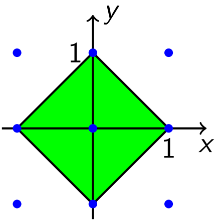
Minkowski's second convex body theorem

Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. Then

$$\frac{2^n}{n!} \leq \lambda_1(\mathcal{C}) \cdots \lambda_n(\mathcal{C}) \mathrm{vol}(\mathcal{C}) \leq 2^n.$$

Examples ($n = 2$):





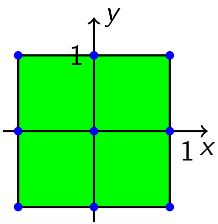
$\lambda_1 = \lambda_2 = 1$, $\mathrm{vol}(\mathcal{C}) = 4$
Here $\lambda_1 \lambda_2 \mathrm{vol}(\mathcal{C}) = 2^n$

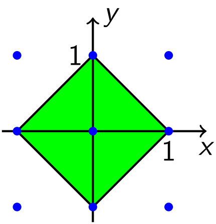
Minkowski's second convex body theorem

Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. Then

$$\frac{2^n}{n!} \leq \lambda_1(\mathcal{C}) \cdots \lambda_n(\mathcal{C}) \mathrm{vol}(\mathcal{C}) \leq 2^n.$$

Examples ($n = 2$):





$\lambda_1 = \lambda_2 = 1$, $\mathrm{vol}(\mathcal{C}) = 4$
Here $\lambda_1 \lambda_2 \mathrm{vol}(\mathcal{C}) = 2^n$

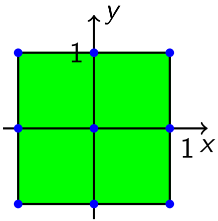
$\lambda_1 = \lambda_2 = 1$, $\mathrm{vol}(\mathcal{C}) = 2$

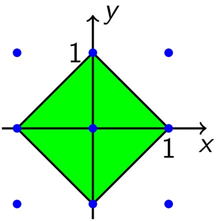
Minkowski's second convex body theorem

Let $\mathcal{C}$ be a convex body in $\mathbb{R}^n$. Then

$$\frac{2^n}{n!} \leq \lambda_1(\mathcal{C}) \cdots \lambda_n(\mathcal{C}) \mathrm{vol}(\mathcal{C}) \leq 2^n.$$

Examples ($n = 2$):





$\lambda_1 = \lambda_2 = 1$, $\mathrm{vol}(\mathcal{C}) = 4$
Here $\lambda_1 \lambda_2 \mathrm{vol}(\mathcal{C}) = 2^n$

$\lambda_1 = \lambda_2 = 1$, $\mathrm{vol}(\mathcal{C}) = 2$
Here $\lambda_1 \lambda_2 \mathrm{vol}(\mathcal{C}) = 2^n / n!$

Second theorem implies first

Let $\mathcal{C}$ be a convex body of $\mathbb{R}^n$ with $\text{vol}(\mathcal{C}) \geq 2^n$.

Second theorem implies first

Let $\mathcal{C}$ be a convex body of $\mathbb{R}^n$ with $\mathrm{vol}(\mathcal{C}) \geq 2^n$.

We have

$$\lambda_1(\mathcal{C}) \cdots \lambda_n(\mathcal{C}) \mathrm{vol}(\mathcal{C}) \leq 2^n.$$

Second theorem implies first

Let $\mathcal{C}$ be a convex body of $\mathbb{R}^n$ with $\mathrm{vol}(\mathcal{C}) \geq 2^n$.

We have

$$\lambda_1(\mathcal{C}) \cdots \lambda_n(\mathcal{C}) \mathrm{vol}(\mathcal{C}) \leq 2^n.$$

But

$$\lambda_1(\mathcal{C}) \leq \cdots \leq \lambda_n(\mathcal{C}),$$

Second theorem implies first

Let $\mathcal{C}$ be a convex body of $\mathbb{R}^n$ with $\mathrm{vol}(\mathcal{C}) \geq 2^n$.

We have

$$\lambda_1(\mathcal{C}) \cdots \lambda_n(\mathcal{C}) \mathrm{vol}(\mathcal{C}) \leq 2^n.$$

But

$$\lambda_1(\mathcal{C}) \leq \cdots \leq \lambda_n(\mathcal{C}),$$

so

$$\lambda_1(\mathcal{C})^n \mathrm{vol}(\mathcal{C}) \leq 2^n,$$

Second theorem implies first

Let $\mathcal{C}$ be a convex body of $\mathbb{R}^n$ with $\mathrm{vol}(\mathcal{C}) \geq 2^n$.

We have

$$\lambda_1(\mathcal{C}) \cdots \lambda_n(\mathcal{C}) \mathrm{vol}(\mathcal{C}) \leq 2^n.$$

But

$$\lambda_1(\mathcal{C}) \leq \cdots \leq \lambda_n(\mathcal{C}),$$

so

$$\lambda_1(\mathcal{C})^n \mathrm{vol}(\mathcal{C}) \leq 2^n,$$

and thus

$$\lambda_1(\mathcal{C}) \leq 1,$$

Second theorem implies first

Let $\mathcal{C}$ be a convex body of $\mathbb{R}^n$ with $\mathrm{vol}(\mathcal{C}) \geq 2^n$.

We have

$$\lambda_1(\mathcal{C}) \cdots \lambda_n(\mathcal{C}) \mathrm{vol}(\mathcal{C}) \leq 2^n.$$

But

$$\lambda_1(\mathcal{C}) \leq \cdots \leq \lambda_n(\mathcal{C}),$$

so

$$\lambda_1(\mathcal{C})^n \mathrm{vol}(\mathcal{C}) \leq 2^n,$$

and thus

$$\lambda_1(\mathcal{C}) \leq 1,$$

i.e. $\mathcal{C}$ contains a non-zero point of $\mathbb{Z}^n$.

Parametric geometry of numbers

Let $\xi_1, \dots, \xi_n \in \mathbb{R}$. For each $X > 0$, let $\mathcal{C}(X)$ denote the convex body of $\mathbb{R}^{n+1}$ defined by

$$|x_0 + x_1\xi_1 + \cdots + x_n\xi_n| \leq X^{-n},\ |x_1| \leq X,\ \dots,\ |x_n| \leq X$$

For $i = 1, \dots, n$, denote by $\lambda_i(X) = \lambda_i(\mathcal{C}(X))$ the i-th minimum of $\mathcal{C}(X)$.

Parametric geometry of numbers

Let $\xi_1, \ldots, \xi_n \in \mathbb{R}$. For each $X > 0$, let $\mathcal{C}(X)$ denote the convex body of $\mathbb{R}^{n+1}$ defined by

$$|x_0 + x_1\xi_1 + \cdots + x_n\xi_n| \leq X^{-n},\ |x_1| \leq X,\ \ldots,\ |x_n| \leq X$$

For $i = 1, \ldots, n$, denote by $\lambda_i(X) = \lambda_i(\mathcal{C}(X))$ the i-th minimum of $\mathcal{C}(X)$.

$$\mathrm{vol}(\mathcal{C}(X)) = 2^{n+1}$$

Parametric geometry of numbers

Let $\xi_1, \dots, \xi_n \in \mathbb{R}$. For each $X > 0$, let $\mathcal{C}(X)$ denote the convex body of $\mathbb{R}^{n+1}$ defined by

$$|x_0 + x_1\xi_1 + \cdots + x_n\xi_n| \le X^{-n},\ |x_1| \le X,\ \dots\ ,\ |x_n| \le X$$

For $i = 1, \dots, n$, denote by $\lambda_i(X) = \lambda_i(\mathcal{C}(X))$ the i-th minimum of $\mathcal{C}(X)$.

$$\mathrm{vol}(\mathcal{C}(X)) = 2^{n+1} \Longrightarrow \frac{1}{(n+1)!} \le \lambda_1(X) \cdots \lambda_{n+1}(X) \le 1$$

Parametric geometry of numbers

Let $\xi_1, \ldots, \xi_n \in \mathbb{R}$. For each $X > 0$, let $\mathcal{C}(X)$ denote the convex body of $\mathbb{R}^{n+1}$ defined by

$$|x_0 + x_1\xi_1 + \cdots + x_n\xi_n| \leq X^{-n}, \ |x_1| \leq X, \ \ldots, \ |x_n| \leq X$$

For $i = 1, \ldots, n$, denote by $\lambda_i(X) = \lambda_i(\mathcal{C}(X))$ the i-th minimum of $\mathcal{C}(X)$.

$$\mathrm{vol}(\mathcal{C}(X)) = 2^{n+1} \Longrightarrow \frac{1}{(n+1)!} \leq \lambda_1(X) \cdots \lambda_{n+1}(X) \leq 1$$

$$\Longrightarrow \sum_{i=1}^{n+1} \log(\lambda_i(X)) = \mathcal{O}(1).$$

Parametric geometry of numbers

Let $\xi_1, \dots, \xi_n \in \mathbb{R}$. For each $X > 0$, let $\mathcal{C}(X)$ denote the convex body of $\mathbb{R}^{n+1}$ defined by

$$|x_0 + x_1\xi_1 + \cdots + x_n\xi_n| \leq X^{-n}, \ |x_1| \leq X, \ \dots, \ |x_n| \leq X$$

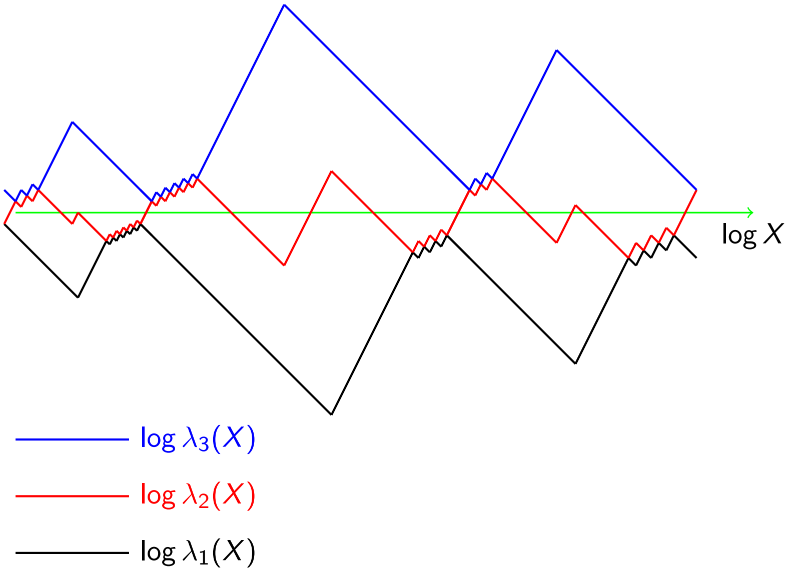
For $i = 1, \dots, n$, denote by $\lambda_i(X) = \lambda_i(\mathcal{C}(X))$ the i-th minimum of $\mathcal{C}(X)$.

$$\mathrm{vol}(\mathcal{C}(X)) = 2^{n+1} \Longrightarrow \frac{1}{(n+1)!} \leq \lambda_1(X) \cdots \lambda_{n+1}(X) \leq 1$$

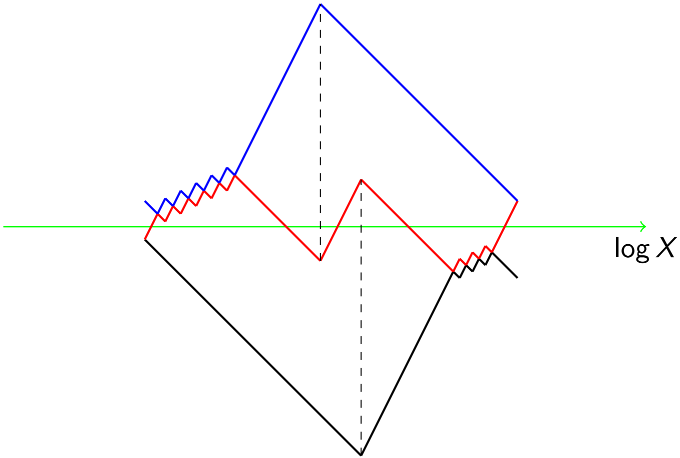
$$\Longrightarrow \sum_{i=1}^{n+1} \log(\lambda_i(X)) = \mathcal{O}(1).$$

$$\text{Ideally: } \boxed{\sum_{i=1}^{n+1} \log(\lambda_i(X)) = 0}$$

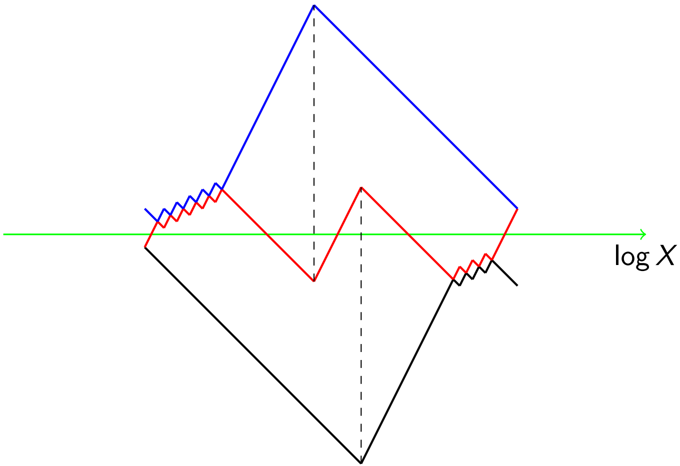
The ideal model of Schmidt and Summerer (2013)



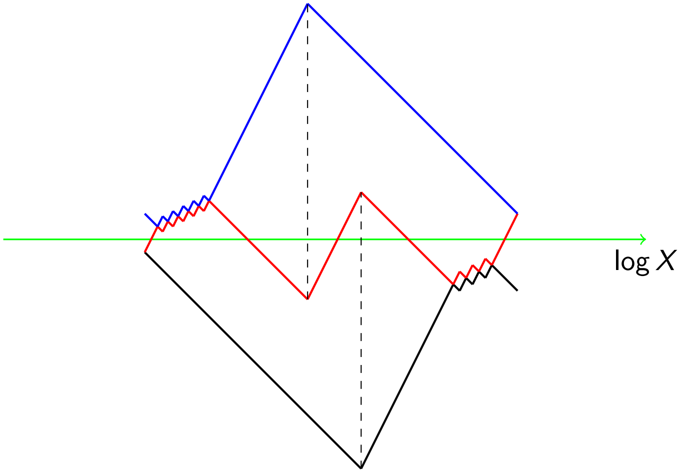
The basic mesh



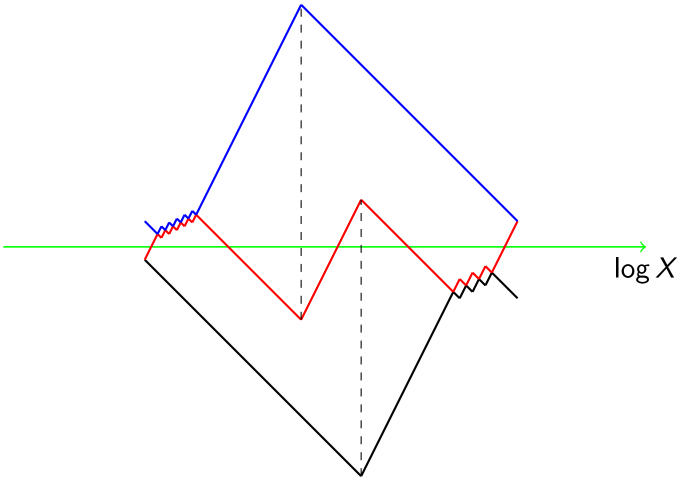
The basic mesh



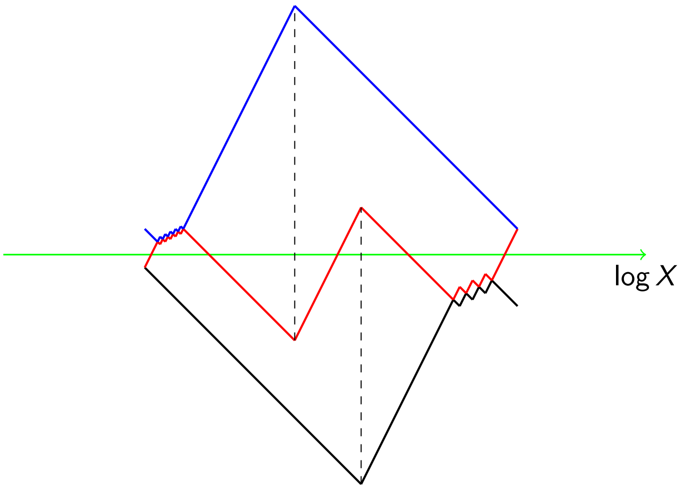
The basic mesh



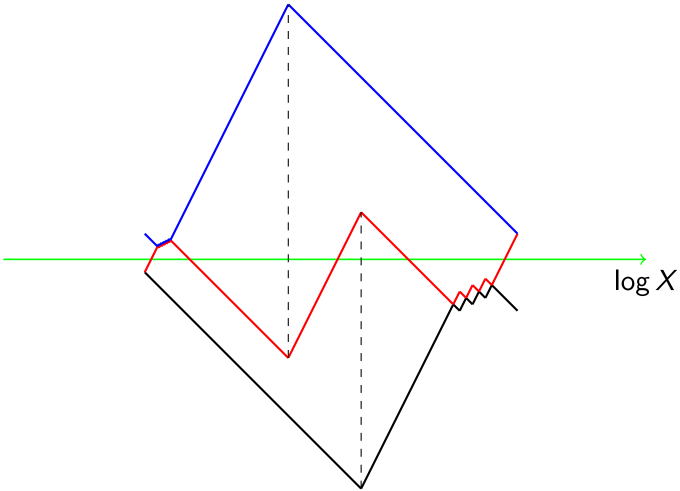
The basic mesh



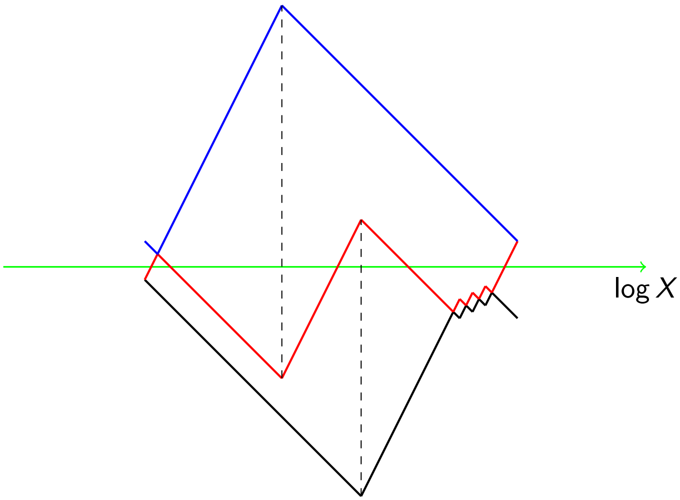
The basic mesh



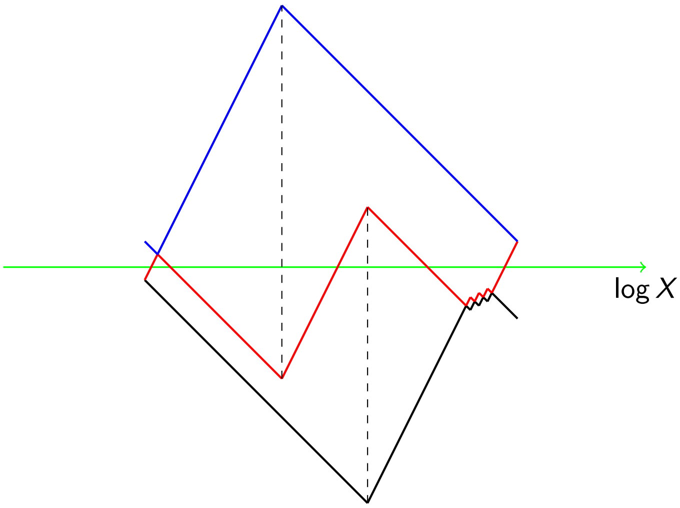
The basic mesh



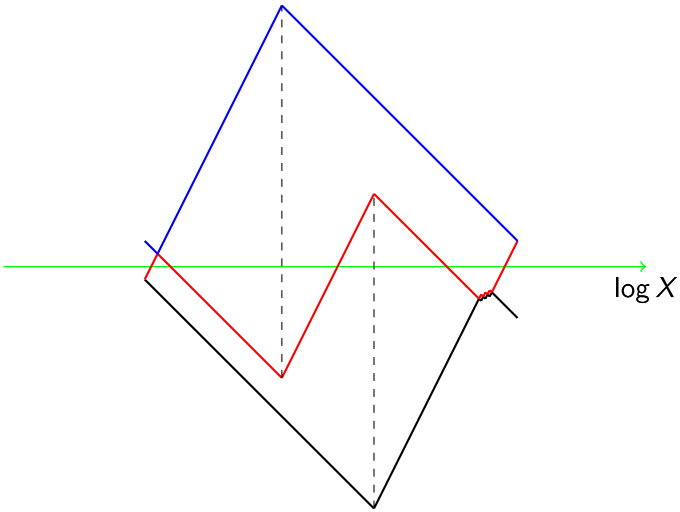
The basic mesh



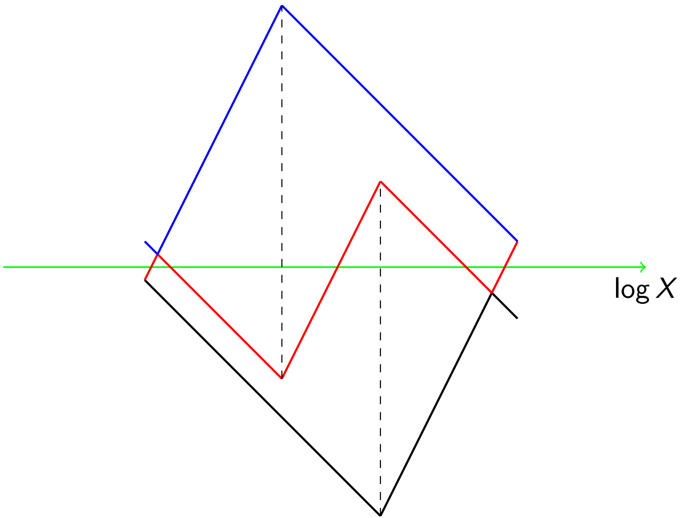
The basic mesh



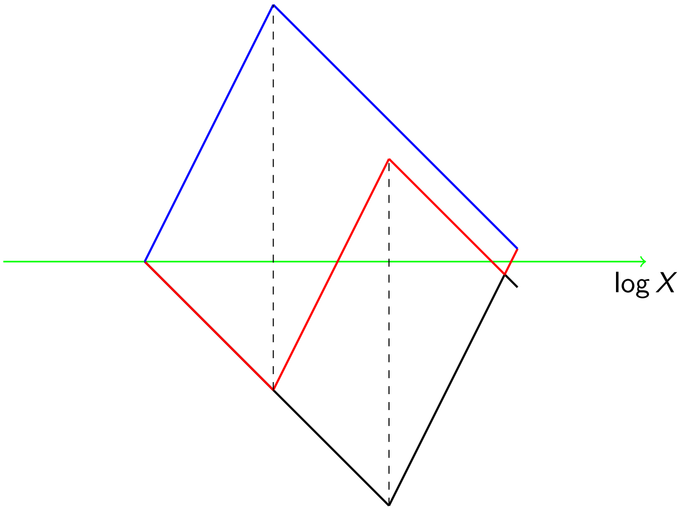
The basic mesh



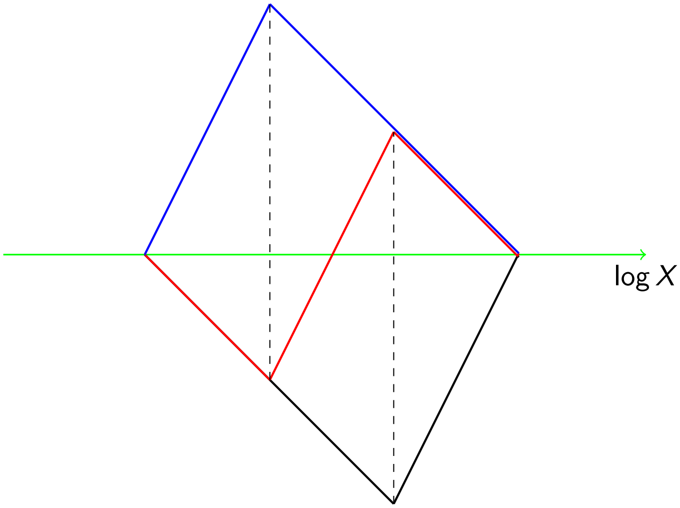
The basic mesh



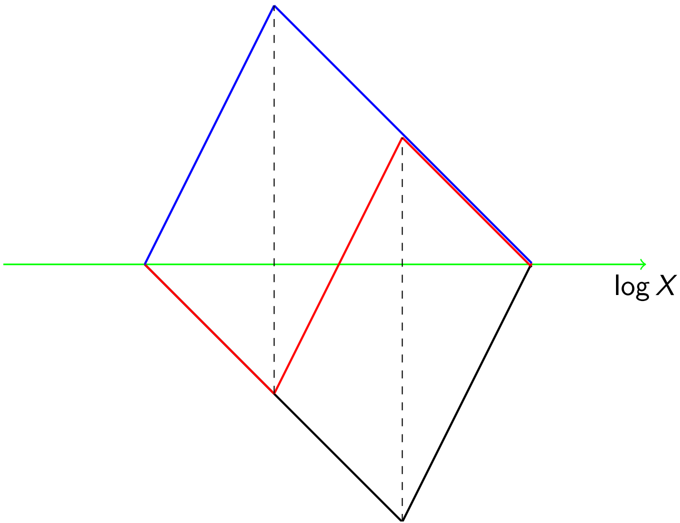
The basic mesh



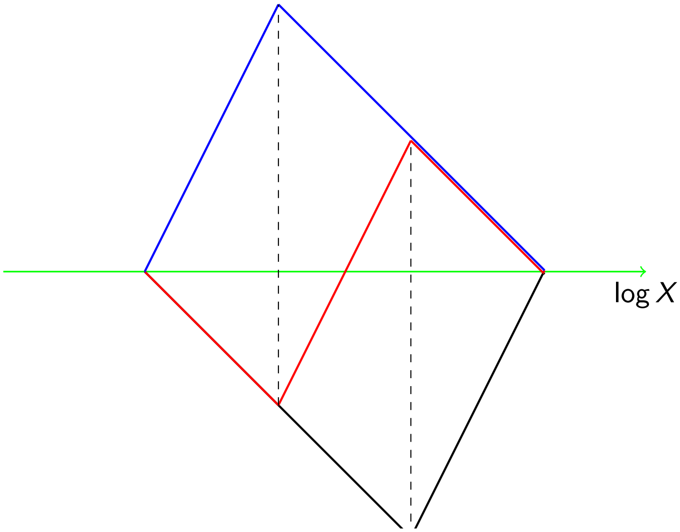
The basic mesh



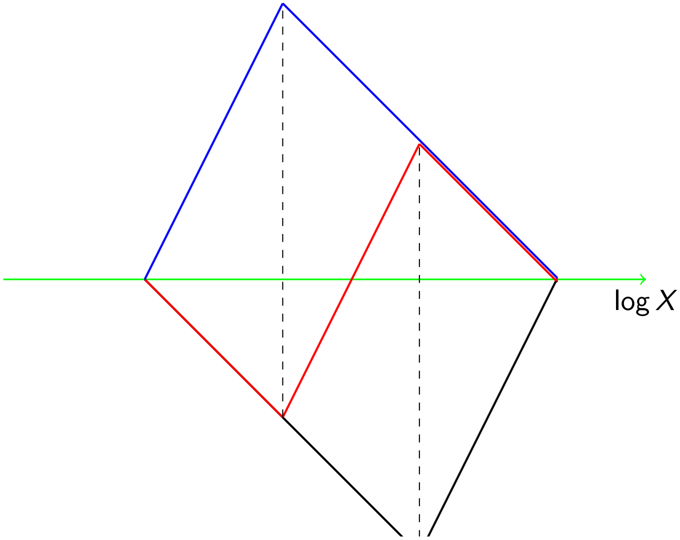
The basic mesh



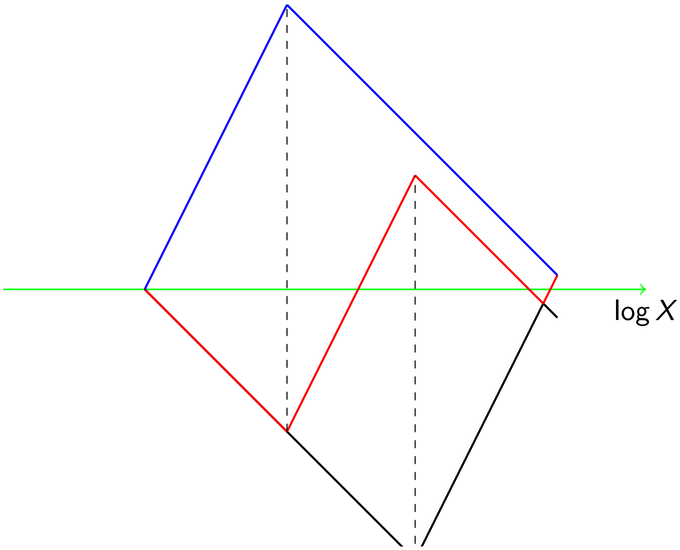
The basic mesh



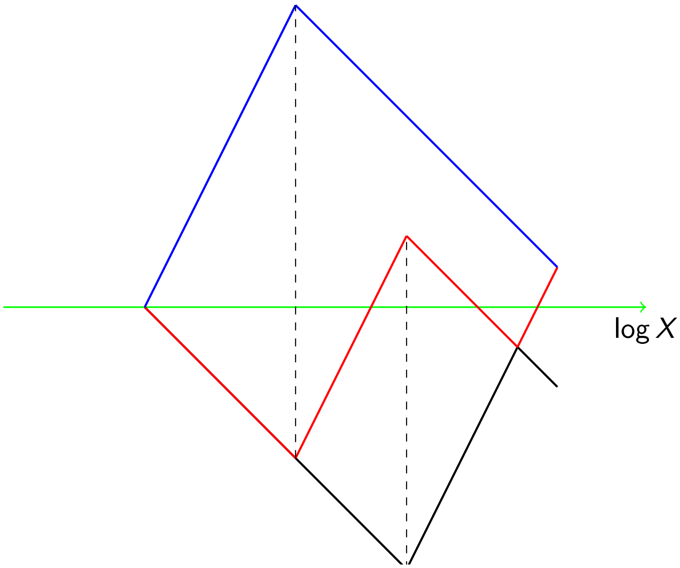
The basic mesh



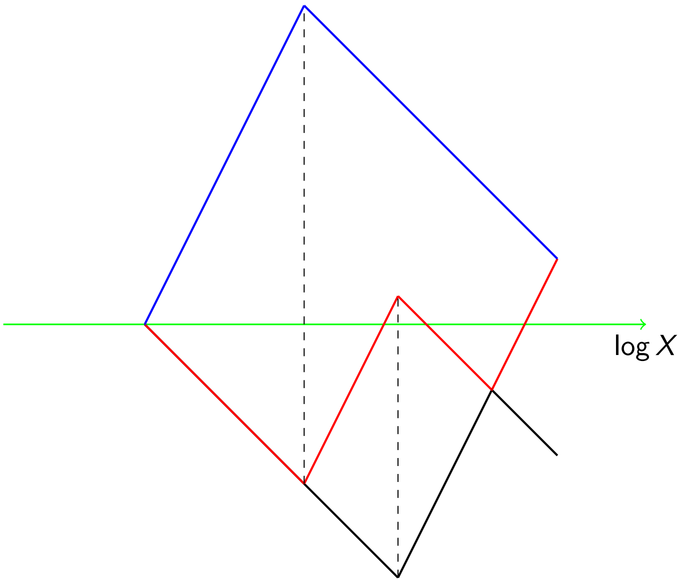
The basic mesh



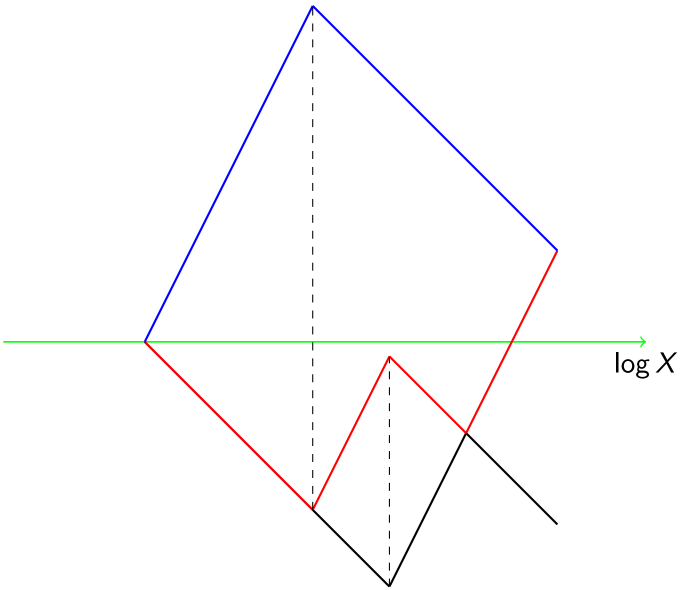
The basic mesh



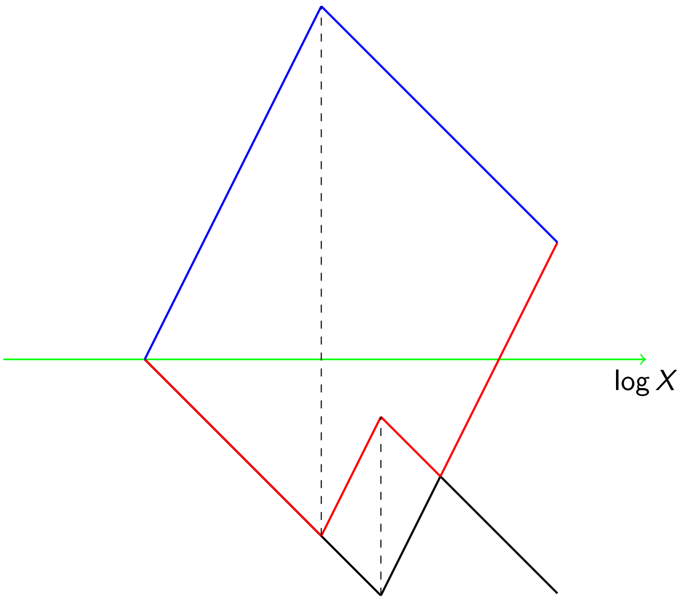
The basic mesh



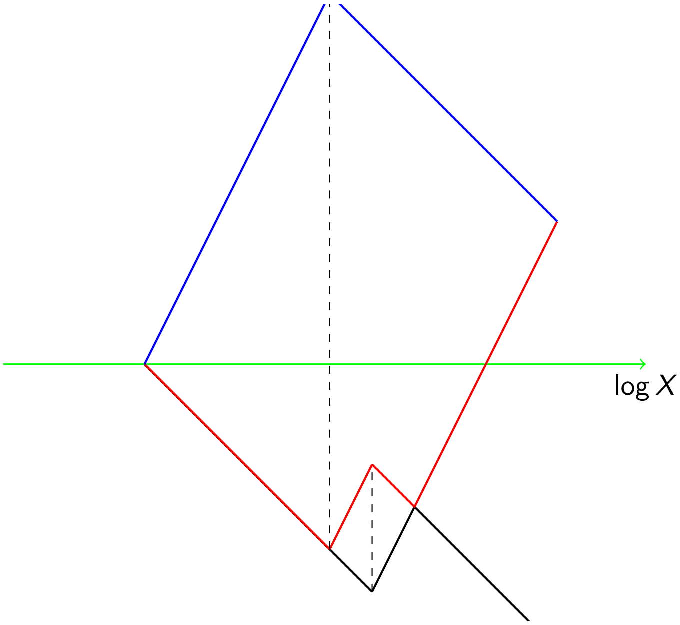
The basic mesh



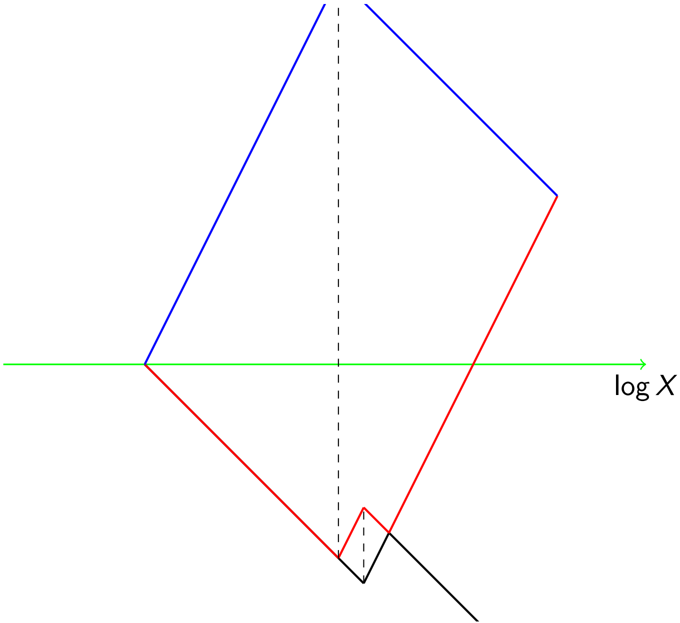
The basic mesh



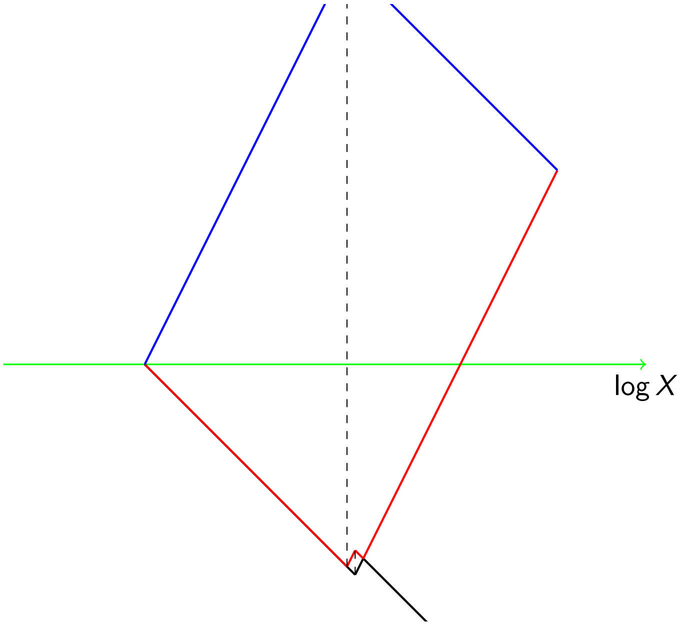
The basic mesh



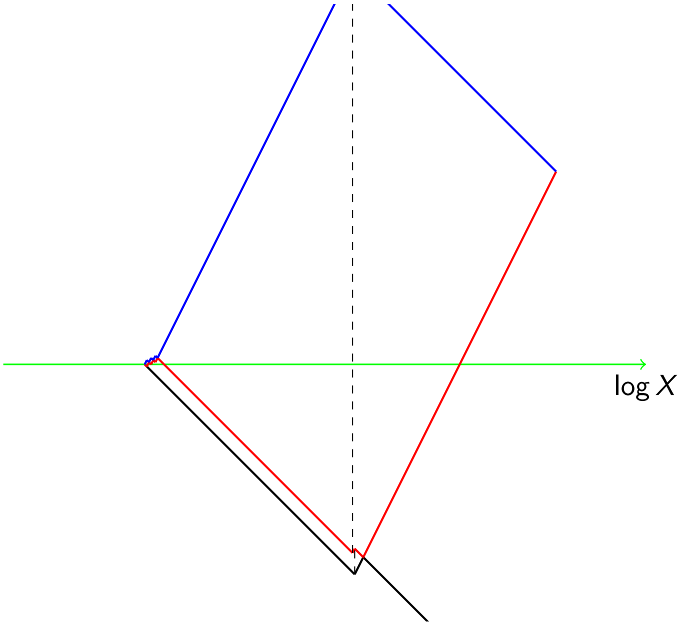
The basic mesh



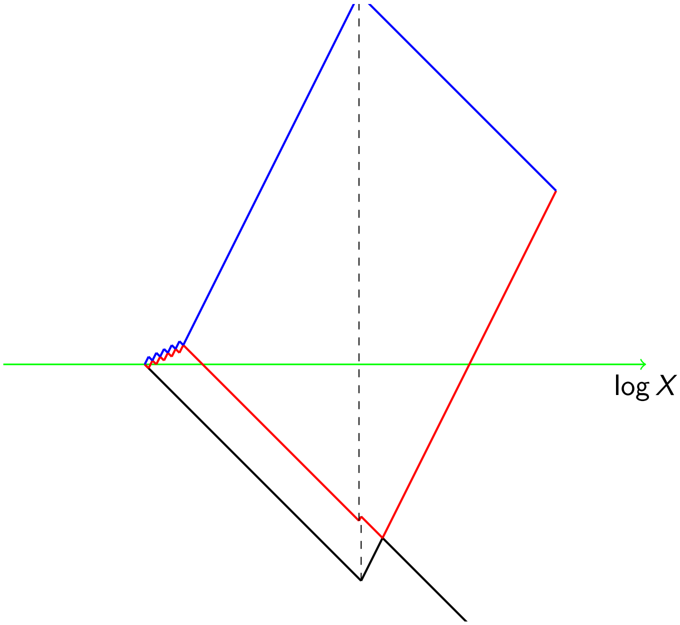
The basic mesh



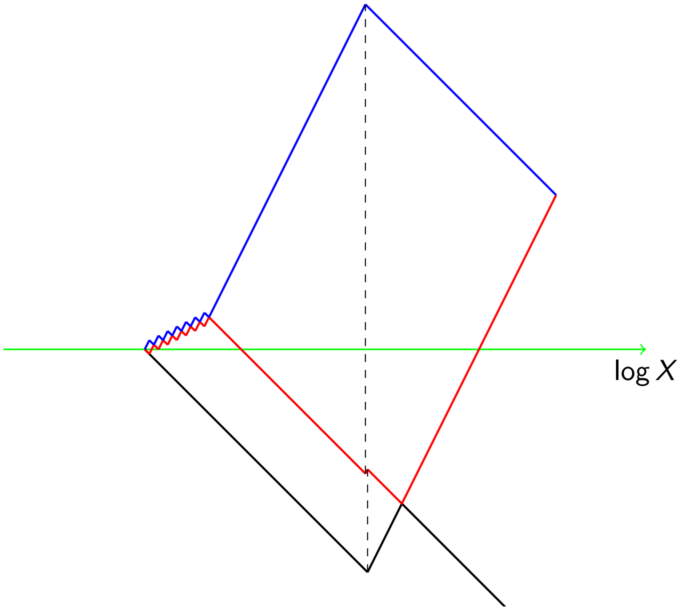
The basic mesh



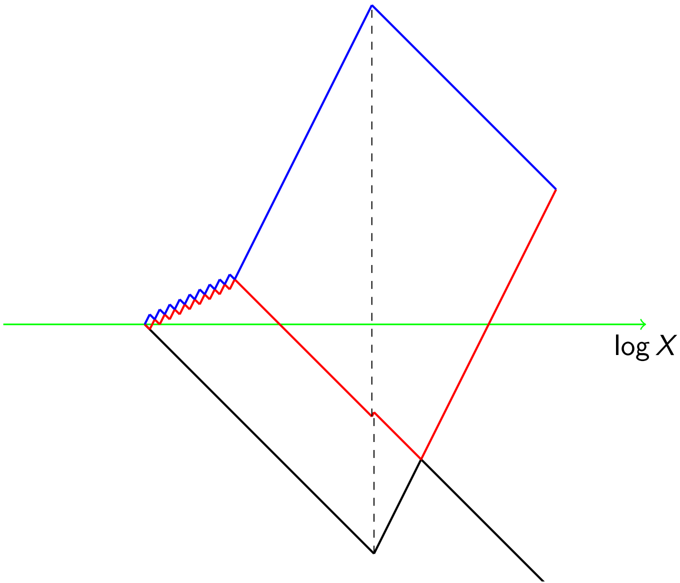
The basic mesh



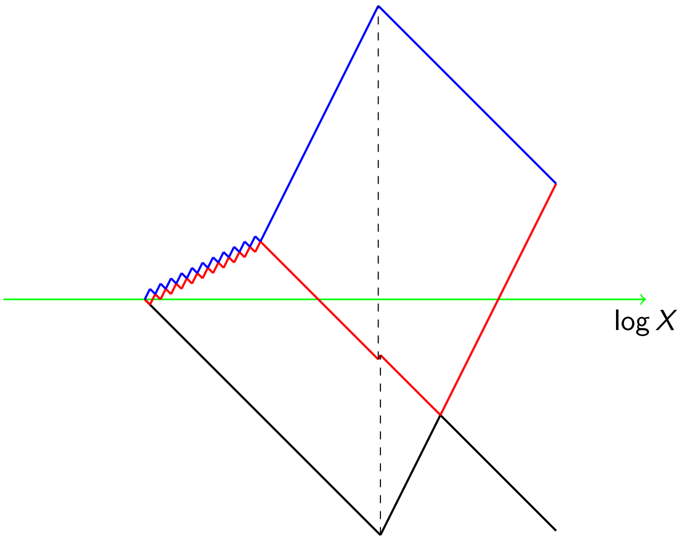
The basic mesh



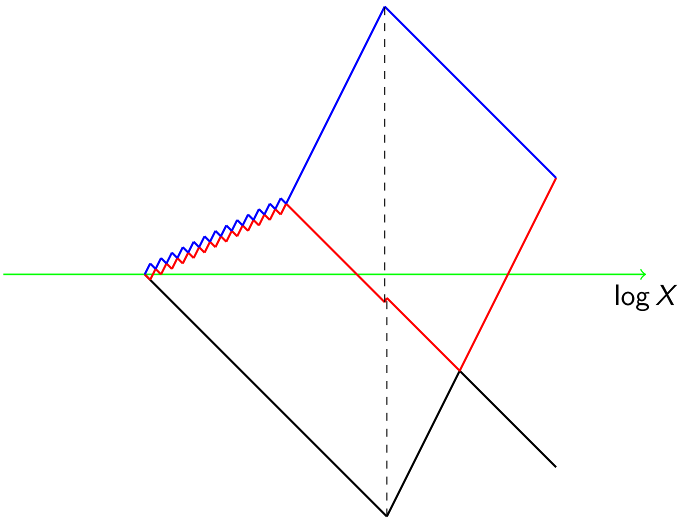
The basic mesh



The basic mesh



The basic mesh



The basic mesh