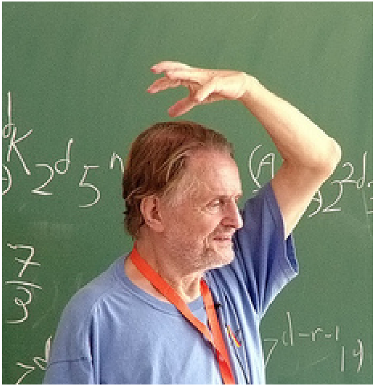
Conway river and Arnold sail

A.P. Veselov, Loughborough, UK and MSU, Russia

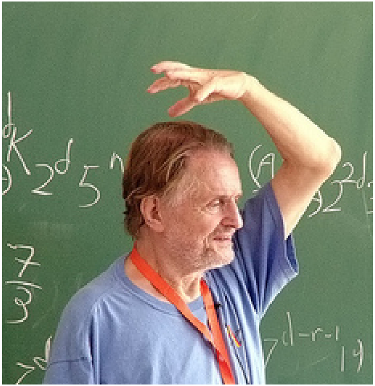
Summer School "Modern Mathematics", July 2018

Carl F. Gauss (1777-1855), Felix Klein (1849-1925) and Andrei A. Markov (1856-1918)

Modern variations



Modern variations



Vladimir I. Arnold (1937-2010) and John H. Conway (1937-)

Prehistory: Farey sequences

John Farey (1816): "On a Curious Property of Vulgar Fractions":

Farey sequence F_n: ordered fractions between 0 and 1 with denominators $\leq n$

$$F_4 = \{\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}\}$$

$$F_5 = \{\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}\}$$

Prehistory: Farey sequences

John Farey (1816): "On a Curious Property of Vulgar Fractions":

Farey sequence F_n: ordered fractions between 0 and 1 with denominators $\leq n$

$$F_4 = \{\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}\}$$
$$F_5 = \{\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}\}$$

"Farey addition" (mediant): $\frac{a}{b} * \frac{c}{d} = \frac{a+c}{b+d}$. Observation: $ad - bc = -1.$

Farey: *"I am not acquainted, whether this curious property of vulgar fractions has been before pointed out?"*

Prehistory: Farey sequences

John Farey (1816): "On a Curious Property of Vulgar Fractions":

Farey sequence F_n: ordered fractions between 0 and 1 with denominators $\leq n$

$$F_4 = \{\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}\}$$

$$F_5 = \{\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}\}$$

"Farey addition" (mediant): $\frac{a}{b} * \frac{c}{d} = \frac{a+c}{b+d}$. Observation: $ad - bc = -1.$

Farey: *"I am not acquainted, whether this curious property of vulgar fractions has been before pointed out?"*

The answer is yes, by French mathematician **Charles Haros (1802)**, but this was not known at the time even to **Cauchy**, who attributed this to Farey.

Prehistory: Farey sequences

John Farey (1816): "On a Curious Property of Vulgar Fractions":

Farey sequence F_n: ordered fractions between 0 and 1 with denominators $\leq n$

$$F_4 = \{\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}\}$$

$$F_5 = \{\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}\}$$

"Farey addition" (mediant): $\frac{a}{b} * \frac{c}{d} = \frac{a+c}{b+d}$. Observation: $ad - bc = -1$.

Farey: *"I am not acquainted, whether this curious property of vulgar fractions has been before pointed out?"*

The answer is yes, by French mathematician **Charles Haros (1802)**, but this was not known at the time even to **Cauchy**, who attributed this to Farey.

Jèrome Franel (1924): Riemann Hypothesis is equivalent to the claim that

$$\sum_{k=1}^{|F_n|} \left(\frac{p_k}{q_k} - \frac{k}{|F_n|} \right)^2 = O(n^r), \quad \forall r > -1.$$

Ford circles and Farey tree

Ford circles are centred at $(\frac{p}{q}, \frac{1}{2q^2})$ with radius $R = \frac{1}{2q^2}$.

Lester Ford (1938): Ford circles of two Farey neighbours are tangent to each other **(Check!)**

Ford circles and Farey tree

Ford circles are centred at $\left(\frac{p}{q}, \frac{1}{2q^2}\right)$ with radius $R = \frac{1}{2q^2}$.

Lester Ford (1938): Ford circles of two Farey neighbours are tangent to each other **(Check!)**

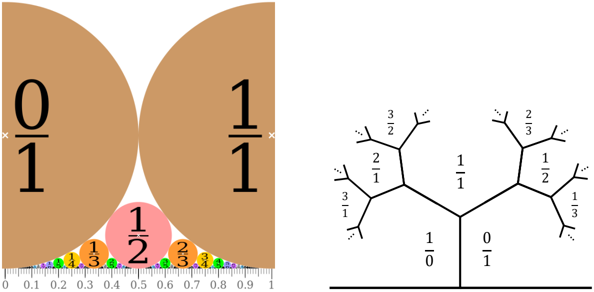


Figure: Ford circles and Farey tree

Conway's superbases

Following Conway define the **lax vector** as a pair $(\pm v), v \in \mathbb{Z}^2$, and of the **superbase** of the integer lattice $\mathbb{Z}^2$ as a triple of lax vectors $(\pm e_1, \pm e_2, \pm e_3)$ such that (e_1, e_2) is a basis of the lattice and

$$e_1 + e_2 + e_3 = 0.$$

Every basis gives rise to exactly two superbases, which form a binary tree.

Conway's superbases

Following Conway define the **lax vector** as a pair $(\pm v)$, $v \in \mathbb{Z}^2$, and of the **superbase** of the integer lattice $\mathbb{Z}^2$ as a triple of lax vectors $(\pm e_1, \pm e_2, \pm e_3)$ such that (e_1, e_2) is a basis of the lattice and

$$e_1 + e_2 + e_3 = 0.$$

Every basis gives rise to exactly two superbases, which form a binary tree.

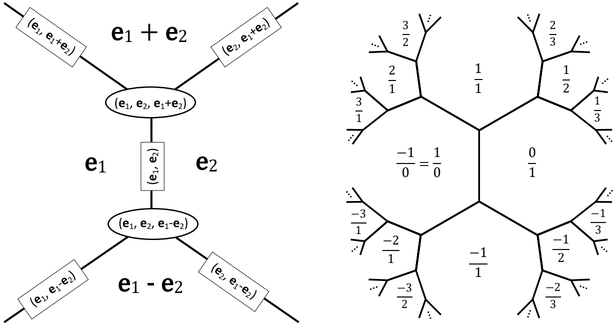


Figure: The superbase and full Farey trees.

Conway (1997): "topographic" way to "vizualise" the values of a binary quadratic form

$$Q(x, y) = ax^2 + hxy + by^2, \quad (x, y) \in \mathbb{Z}^2$$

by taking values of Q on the vectors of the superbase. In particular,

$$Q(e_1) = a, Q(e_2) = b, Q(e_1 + e_2) = c = a + h + b, Q(e_1 - e_2) = a - h + b.$$

Conway (1997): "topographic" way to "vizualise" the values of a binary quadratic form

$$Q(x,y) = ax^2 + hxy + by^2, \quad (x,y) \in \mathbb{Z}^2$$

by taking values of Q on the vectors of the superbase. In particular,

$$Q(e_1) = a, Q(e_2) = b, Q(e_1+e_2) = c = a+h+b, Q(e_1-e_2) = a-h+b.$$

One can construct the *topograph* of Q using the *Arithmetic progression (parallelogram) rule*:

$$Q(\mathbf{u}+\mathbf{v}) + Q(\mathbf{u}-\mathbf{v}) = 2(Q(\mathbf{u}) + Q(\mathbf{v})), \quad \mathbf{u},\mathbf{v} \in \mathbb{R}^2.$$

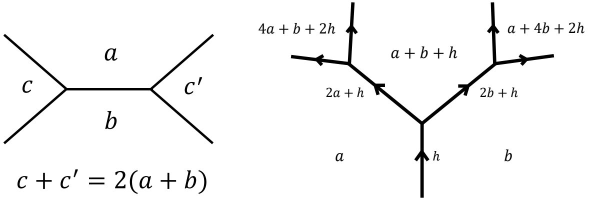


Figure: Arithmetic progression rule and Conway's Climbing Lemma.

Euclidean example

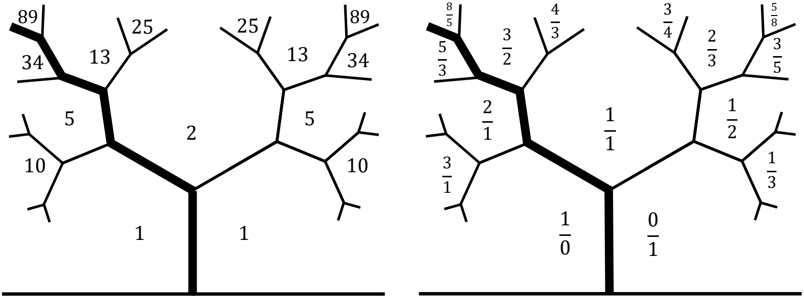


Figure: Topograph of $Q = x^2 + y^2$ and Farey tree with marked "golden" path.

Conway river

For indefinite binary quadratic form $Q(x, y)$ the situation is more interesting: positive and negative values of Q are separated by the path on the topograph called **Conway river**. For integer form Q the Conway river is periodic.

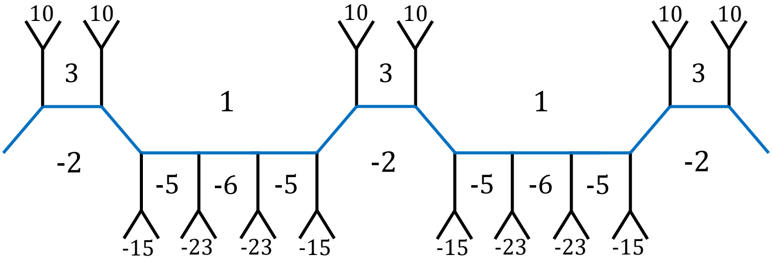


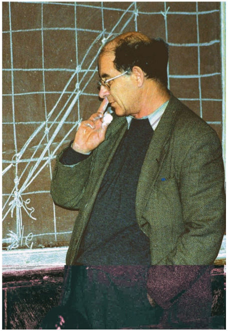
Figure: Conway river for the quadratic form $Q = x^2 - 2xy - 5y^2$.

Arnold sails

For indefinite form the equation $Q(x, y) = 0$ determines a pair of lines. Assume that $(0, 0)$ is the only integer point on them.

For indefinite form the equation $Q(x, y) = 0$ determines a pair of lines. Assume that $(0, 0)$ is the only integer point on them.

The convex hulls of integer points inside each angle are **Klein polygons** with boundaries known as **Arnold sails**.



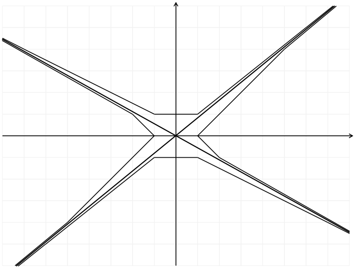


Figure: Vladimir I. Arnold and the sails for a pair of lines.

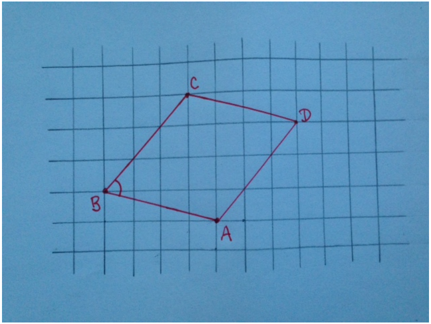
Elements of lattice geometry

Define the *lattice length* $l(AB)$ of a lattice segment AB as the number of lattice points in AB minus one and the *lattice sine* of the angle $\angle ABC$ as

$$l\sin\angle ABC = \frac{lS(ABCD)}{l(AB)l(BC)} = \frac{|\det(BA, BC)|}{l(AB)l(BC)}.$$

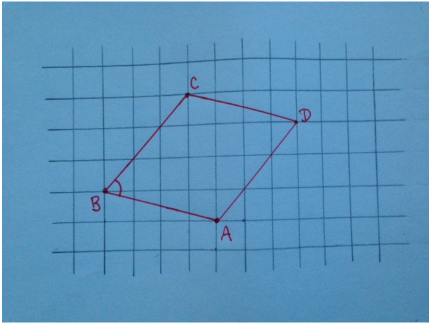
Define the *lattice length* $l(AB)$ of a lattice segment AB as the number of lattice points in AB minus one and the *lattice sine* of the angle $\angle ABC$ as

$$l\sin\angle ABC = \frac{lS(ABCD)}{l(AB)l(BC)} = \frac{|\det(BA, BC)|}{l(AB)l(BC)}.$$



Define the *lattice length* $l(AB)$ of a lattice segment AB as the number of lattice points in AB minus one and the *lattice sine* of the angle $\angle ABC$ as

$$l\sin\angle ABC = \frac{lS(ABCD)}{l(AB)l(BC)} = \frac{|\det(BA, BC)|}{l(AB)l(BC)}.$$



Here $l\sin\angle ABC = |\det\begin{pmatrix} 4 & 3 \\ -1 & 3 \end{pmatrix}|/1\times 3 = 5.$

LLS sequence of Arnold sails

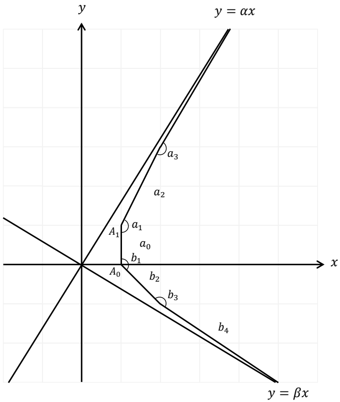
Following **Karpenkov** introduce the *LLS (lattice length sine) sequence* (a_i), $i \in \mathbb{Z}$ of a broken lattice line (A_k), $k \in \mathbb{Z}$ as

$$a_{2k} = l(A_k A_{k+1}), \quad a_{2k-1} = l\sin\left(\angle A_{k-1} A_k A_{k+1}\right).$$

LLS sequence of Arnold sails

Following **Karpenkov** introduce the *LLS (lattice length sine) sequence* (a_i), $i \in \mathbb{Z}$ of a broken lattice line (A_k), $k \in \mathbb{Z}$ as

$$a_{2k} = l(A_k A_{k+1}), \quad a_{2k-1} = l \sin\left(\angle A_{k-1} A_k A_{k+1}\right).$$



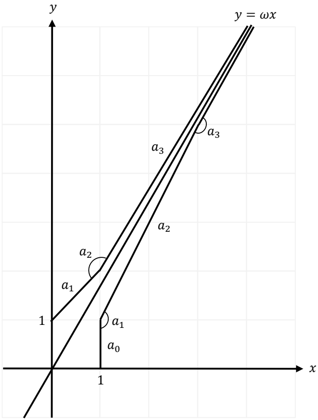


Figure: Arnold sail and Edge-Angle duality.

K. Spalding, AV (2017):

Let $Q(x, y)$ be a real indefinite binary quadratic form and consider the Arnold sail of the pair of lines given by $Q(x, y) = 0$.
The LLS sequence $(\dots, a_0, a_1, a_2, a_3, \dots)$ of Arnold sail coincides with the sequence of the left- and right-turns of the Conway river on topograph of Q :

$$\dots L^{a_0} R^{a_1} L^{a_2} R^{a_3} \dots$$

This determines the river uniquely up to the action of the group $PGL(2, \mathbb{Z})$ on the topograph and a change of direction.

K. Spalding, AV (2017):

Let $Q(x,y)$ be a real indefinite binary quadratic form and consider the Arnold sail of the pair of lines given by $Q(x,y)=0$.
The LLS sequence $(\dots, a_0, a_1, a_2, a_3, \dots)$ of Arnold sail coincides with the sequence of the left- and right-turns of the Conway river on topograph of Q :

$$\dots L^{a_0} R^{a_1} L^{a_2} R^{a_3} \dots$$

This determines the river uniquely up to the action of the group $PGL(2,\mathbb{Z})$ on the topograph and a change of direction.

For example, for $Q = x^2 - 2xy - 5y^2$ the corresponding LLS sequence is $\dots 4, 2, 4, 2, 4, 2, \dots$, which is exactly the sequence of left-right turns $\dots LLLLRRLLLLRR \dots$ of the (properly oriented) Conway river:

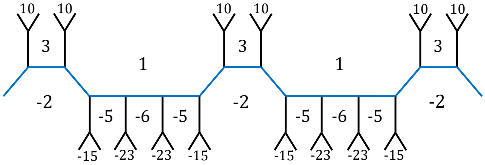


Figure: Conway river for $Q = x^2 - 2xy - 5y^2$.

Felix Klein (1895):

Imagine pegs or needles affixed at all the integral points, and wrap a tightly drawn string about the sets of pegs to the right and to the left of the ω-ray, then the vertices of the two convex strong-polygons which bound our two point sets will be precisely the points (p_ν, q_ν) whose coordinates are the numerators and denominators of the successive convergents to ω, the left polygon having the even convergents, the right one the odd.

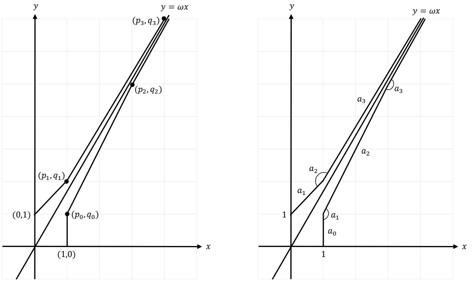


Figure: Klein's construction and Karpenkov's LLS sequence

Continued fractions: crush course

Let $\alpha = \alpha_0$ be a real number. Consider its integer part $a_0 = [\alpha_0]$ and the difference $\alpha_0 - a_0$. If it is zero then we stop. Otherwise consider $\alpha_1 = \frac{1}{\alpha_0 - a_0}$, $a_1 = [\alpha_1]$ and continue in the same way:

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k}, \; a_{k+1} = [\alpha_{k+1}].$$

As a result we have the representation of α as a **continued fraction**:

$$\phi(\alpha) = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}} := [a_0; a_1, a_2, \dots].$$

Here $a_0 \in \mathbb{Z}, a_1, a_2, \dots \in \mathbb{N}$ are called **partial quotients** of continued fraction.

Continued fractions: crush course

Let $\alpha = \alpha_0$ be a real number. Consider its integer part $a_0 = [\alpha_0]$ and the difference $\alpha_0 - a_0$. If it is zero then we stop. Otherwise consider $\alpha_1 = \frac{1}{\alpha_0 - a_0}$, $a_1 = [\alpha_1]$ and continue in the same way:

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k}, \ a_{k+1} = [\alpha_{k+1}].$$

As a result we have the representation of α as a **continued fraction**:

$$\phi(\alpha) = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}} := [a_0; a_1, a_2, \dots].$$

Here $a_0 \in \mathbb{Z}, a_1, a_2, \dots \in \mathbb{N}$ are called **partial quotients** of continued fraction.

The numbers

$$C_k = [a_0; a_1, a_2, \dots, a_k] = \frac{p_k}{q_k}$$

are called **convergents** and known to be **best rational approximations** of α. They can be computed recursively using

$$p_k = a_k p_{k-1} + p_{k-2}, \ q_k = a_k q_{k-1} + q_{k-2}$$

with the convention that $p_{-2} = 0, p_{-1} = 1$ and $q_{-2} = 1, q_{-1} = 0$.

A continued fraction $[a_0; a_1, \ldots]$ is called **periodic** if $a_{n+k} = a_n$ for some $k \in \mathbb{N}$ and all $n \geq N$ with some $N \in \mathbb{N}$. We will write in that case

$$[a_0; a_1, \ldots, a_{N-1}, \overline{a_N, \ldots, a_{N+k-1}}].$$

A continued fraction $[a_0; a_1, \dots]$ is called **periodic** if $a_{n+k} = a_n$ for some $k \in \mathbb{N}$ and all $n \geq N$ with some $N \in \mathbb{N}$. We will write in that case

$$[a_0; a_1, \dots, a_{N-1}, \overline{a_N, \dots, a_{N+k-1}}].$$

Example. The simplest periodic continued fraction $\phi = [1, 1, 1, \dots] = \frac{1+\sqrt{5}}{2}$ corresponds to the **Golden Ratio**. Indeed, we have

$$\phi = 1 + \frac{1}{\phi}, \quad \phi^2 - \phi - 1 = 0.$$

Note that the corresponding p_k, q_k are the **Fibonacci numbers**:

$$p_{k+1} = p_k + p_{k-1}, \ q_{k+1} = q_k + q_{k-1} :$$

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \dots.$$

Lagrange (1770):
Every periodic continued fraction represents a quadratic irrational, and every quadratic irrational has a periodic continued fraction expansion.

For example,

$$\alpha = 1+\sqrt{6} = [3; 2, 4, 2, 4, \dots] = [3; \overline{2, 4}], \;\; \beta = 2+\sqrt{6} = [4; 2, 4, 2, \dots] = [\overline{4, 2}].$$

Lagrange (1770):
Every periodic continued fraction represents a quadratic irrational, and every quadratic irrational has a periodic continued fraction expansion.

For example,

$$\alpha = 1+\sqrt{6} = [3; 2, 4, 2, 4, \ldots] = [3; \overline{2, 4}], \;\; \beta = 2+\sqrt{6} = [4; 2, 4, 2, \ldots] = [\overline{4, 2}].$$

Galois (1829):
A quadratic irrational $\alpha = \frac{A+\sqrt{D}}{B}$ has a pure periodic continued fraction expansion $\alpha = [\overline{b_1, \ldots, b_l}]$ if and only if its conjugate $\bar{\alpha} = \frac{A-\sqrt{D}}{B}$ satisfies the inequality

$$-1 < \bar{\alpha} < 0.$$

Moreover, in that case

$$\bar{\alpha} = -[0, \overline{b_l, \ldots, b_1}].$$

For example, $-1 < \bar{\beta} = 2 - \sqrt{6} < 0$ and $-\bar{\beta} = \sqrt{6} - 2 = [0, \overline{4, 2}]$.

For the form $Q(x, y) = ax^2 + hxy + by^2$ consider the corresponding roots

$$Q(\alpha, 1) = a\alpha^2 + h\alpha + b = 0.$$

Then the period $b_1, \dots, b_l$ of the continued fraction expansion

$$\alpha = [a_0, a_1, \dots, a_k, \overline{b_1, \dots, b_l}]$$

describes the sequence of the left/right-turns of the Conway river. The pre-period $a_0, a_1, \dots, a_k$ determines the path to the Conway river.

For the form $Q(x, y) = ax^2 + hxy + by^2$ consider the corresponding roots

$$Q(\alpha, 1) = a\alpha^2 + h\alpha + b = 0.$$

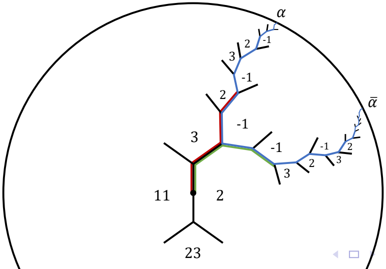
Then the period $b_1, \ldots, b_l$ of the continued fraction expansion

$$\alpha = [a_0, a_1, \ldots, a_k, \overline{b_1, \ldots, b_l}]$$

describes the sequence of the left/right-turns of the Conway river. The pre-period $a_0, a_1, \ldots, a_k$ determines the path to the Conway river.

Example. For $Q = 11x^2 - 10xy + 2y^2$ we have quadratic irrationals

$$\alpha = \frac{5 + \sqrt{3}}{11} = [0; 1, 1, 1, \overline{1, 2}], \quad \bar{\alpha} = \frac{5 - \sqrt{3}}{11} = [0; 3, \overline{2, 1}].$$



LLS sequences of Arnold sail

Key observation (cf. Markov (1880), Klein (1895), Karpenkov (2013))
The LLS sequence of the Arnold sail of a pair of lines $y = \alpha x$ and $y = \beta x$ with $\alpha > 1$ and $0 > \beta > -1$ is

$$\ldots, b_4, b_3, b_2, b_1, a_0, a_1, a_2, a_3, \ldots,$$

where a_i and b_j are given by the continued fraction expansions

$$\alpha = [a_0, a_1, a_2, a_3, \ldots], \quad -\beta = [0, b_1, b_2, b_3, b_4, \ldots].$$

Key observation (cf. Markov (1880), Klein (1895), Karpenkov (2013))
The LLS sequence of the Arnold sail of a pair of lines $y = \alpha x$ and $y = \beta x$ with $\alpha > 1$ and $0 > \beta > -1$ is

$$\ldots, b_4, b_3, b_2, b_1, a_0, a_1, a_2, a_3, \ldots,$$

where a_i and b_j are given by the continued fraction expansions

$$\alpha = [a_0, a_1, a_2, a_3, \ldots], \quad -\beta = [0, b_1, b_2, b_3, b_4, \ldots].$$

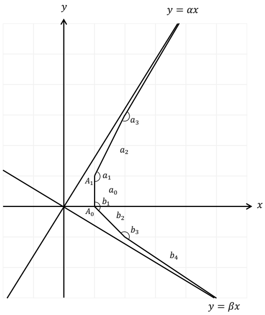


Figure: Arnold sail in a special basis.

Key background: group $SL(2, \mathbb{Z})$

The group

$$SL(2,\mathbb{Z}) = \{A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \ a, b, c, d \in \mathbb{Z}, \ \det A = ad - bc = 1\}$$

is one of the most important in mathematics. It acts on the upper half plane $z = x + iy \in \mathbb{C}, y > 0$ by

$$z \to \frac{az + b}{cz + d},$$

leaving invariant Farey tesselation, and thus the corresponding dual tree $\mathcal{T}$.

Key background: group $SL(2,\mathbb{Z})$

The group

$$SL(2,\mathbb{Z}) = \{A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \; a,b,c,d \in \mathbb{Z}, \; \det A = ad - bc = 1\}$$

is one of the most important in mathematics. It acts on the upper half plane $z = x + iy \in \mathbb{C}, y > 0$ by

$$z \to \frac{az+b}{cz+d},$$

leaving invariant Farey tesselation, and thus the corresponding dual tree $\mathcal{T}$.

Its quotient $PSL(2,\mathbb{Z}) = SL(2,\mathbb{Z})/\pm I = \mathbb{Z}_2 * \mathbb{Z}_3$ is freely generated by its elements of order 2 and 3

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$$

acting by rotations on trivalent tree $\mathcal{T}$.

Positive part of $SL(2,\mathbb{Z})$ is monoid

$$SL(2,\mathbb{N}) = \{A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \ a,b,c,d \in \mathbb{Z}_{\geq 0}, \ \det A = ad - bc = 1\}$$

Monoid $SL(2,\mathbb{N})$ and the Farey tree

Positive part of $SL(2,\mathbb{Z})$ is monoid

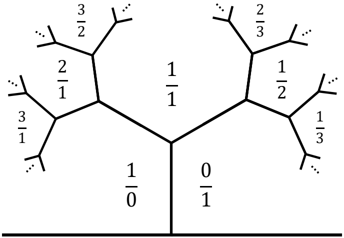
$$SL(2,\mathbb{N}) = \{A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \ a,b,c,d \in \mathbb{Z}_{\geq 0}, \ \det A = ad - bc = 1\}$$

It is freely generated by the triangular matrices

$$L = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

The positive Farey tree gives a nice parametrisation of this monoid: for every edge E of $\mathcal{T}$ we have two adjacent fractions $\frac{a}{c}, \frac{b}{d}$ defining the matrix

$$A_E = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{N}).$$



Continued fractions and paths on Farey tree

A finite path γ on the Farey tree is the sequence of left/right turns $LLL...LRR...RL...L\ldots RR = L^{a_0}R^{a_1}L^{a_2}\ldots R^{a_k}$ leads to the matrix

$$A = L^{a_0}R^{a_1}L^{a_2}\ldots R^{a_k} = \begin{pmatrix}1 & a_0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ a_1 & 1\end{pmatrix}\begin{pmatrix}1 & a_2\\ 0 & 1\end{pmatrix}\cdots\begin{pmatrix}1 & 0\\ a_k & 1\end{pmatrix} \in SL(2,\mathbb{N}).$$

Going down the Farey tree is nothing other but **Euclidean algorithm!**

Continued fractions and paths on Farey tree

A finite path γ on the Farey tree is the sequence of left/right turns $LLL...LRR...RL...L\dots RR = L^{a_0}R^{a_1}L^{a_2}\dots R^{a_k}$ leads to the matrix

$$A = L^{a_0}R^{a_1}L^{a_2}\dots R^{a_k} = \begin{pmatrix} 1 & a_0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ a_1 & 1 \end{pmatrix}\begin{pmatrix} 1 & a_2 \\ 0 & 1 \end{pmatrix}\dots\begin{pmatrix} 1 & 0 \\ a_k & 1 \end{pmatrix} \in SL(2,\mathbb{N}).$$

Going down the Farey tree is nothing other but **Euclidean algorithm!**

An infinite path $L^{a_0}R^{a_1}L^{a_2}\dots$ goes to an irrational number $[a_0, a_1, a_2, \dots]$ on the boundary of unit disk considered as **Poincare model of hyperbolic plane.**

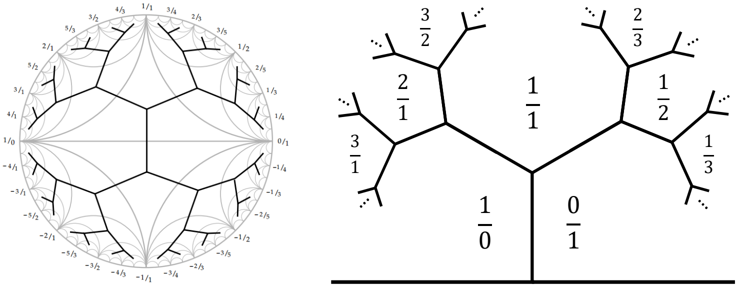
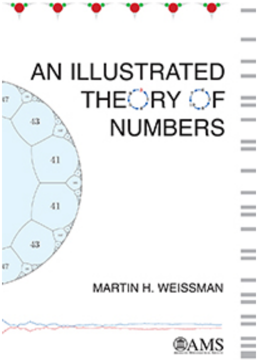
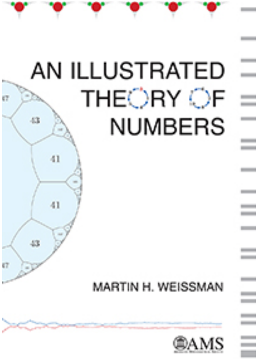


Figure: Dual tree for Farey tessellation and positive Farey tree

Good reading



Good reading



More special:

O. Karpenkov *Geometry of Continued Fractions*. Springer-Verlag, 2013.

K. Spalding, A.P. Veselov *Conway river and Arnold sail.*
https://arxiv.org/pdf/1801.10072.pdf

PART II: APPLICATIONS TO PELL'S EQUATION

Pell's equation

is the Diophantine equation

$$x^2 - dy^2 = 1$$

where d is not total square.

Pell's equation

is the Diophantine equation

$$x^2 - dy^2 = 1$$

where d is not total square.

History

- **Diophantus (200-284AD)**: first examples inspired by Archimedes

Pell's equation

is the Diophantine equation

$$x^2 - dy^2 = 1$$

where d is not total square.

History

- **Diophantus (200-284AD)**: first examples inspired by Archimedes
- **Brahmagupta (628AD), Bhaskara (1114-85)**: general method of finding integer solutions

Pell's equation

is the Diophantine equation

$$x^2 - dy^2 = 1$$

where d is not total square.

History

- **Diophantus (200-284AD)**: first examples inspired by Archimedes
- **Brahmagupta (628AD), Bhaskara (1114-85)**: general method of finding integer solutions
- **Pierre Fermat (1657)**: $x^2 - 61y^2 = 1$
  "We await these solutions, which, if England or Belgic or Celtic Gaul do not produce, then Narbonese Gaul will."

is the Diophantine equation

$$x^2 - dy^2 = 1$$

where d is not total square.

History

- **Diophantus (200-284AD)**: first examples inspired by Archimedes
- **Brahmagupta (628AD), Bhaskara (1114-85)**: general method of finding integer solutions
- **Pierre Fermat (1657)**: $x^2 - 61y^2 = 1$
  "We await these solutions, which, if England or Belgic or Celtic Gaul do not produce, then Narbonese Gaul will."
- **William Brouncker, PRS (1620-1684)**: continued fraction method

Pell's equation

is the Diophantine equation

$$x^2 - dy^2 = 1$$

where d is not total square.

History

- **Diophantus (200-284AD)**: first examples inspired by Archimedes
- **Brahmagupta (628AD), Bhaskara (1114-85)**: general method of finding integer solutions
- **Pierre Fermat (1657)**: $x^2 - 61y^2 = 1$
  "We await these solutions, which, if England or Belgic or Celtic Gaul do not produce, then Narbonese Gaul will."
- **William Brouncker, PRS (1620-1684)**: continued fraction method
- **Leonhard Euler (1733)**: ascribed the equation wrongly to **John Pell (1611-85)**. Example: $x^2 - 31y^2 = 1$.

Continued fraction approach

Fact 1. *For any positive integer* d *not a total square* $\sqrt{d}$ *has continued fraction expansion of the form*

$$\sqrt{d} = [a_0; \overline{a_1, a_2, \ldots, a_{n-1}, 2a_0}]$$

with "palindromic" set $a_1, \ldots, a_{n-1}$: $a_1 = a_{n-1},\ a_2 = a_{n-2}, \ldots$.

Continued fraction approach

Fact 1. *For any positive integer d not a total square $\sqrt{d}$ has continued fraction expansion of the form*

$$\sqrt{d} = [a_0; \overline{a_1, a_2, \ldots, a_{n-1}, 2a_0}]$$

with "palindromic" set $a_1, \ldots, a_{n-1} : a_1 = a_{n-1},\ a_2 = a_{n-2}, \ldots$.

Consider now two Pell's equations $Pell_\pm : x^2 - dy^2 = \pm 1$. The least positive solutions (if exist) are called **fundamental solutions**.

Continued fraction approach

Fact 1. *For any positive integer d not a total square $\sqrt{d}$ has continued fraction expansion of the form*

$$\sqrt{d} = [a_0; \overline{a_1, a_2, \ldots, a_{n-1}, 2a_0}]$$

with "palindromic" set $a_1, \ldots, a_{n-1} : a_1 = a_{n-1},\ a_2 = a_{n-2}, \ldots.$

Consider now two Pell's equations $Pell_{\pm} : x^2 - dy^2 = \pm 1.$ The least positive solutions (if exist) are called **fundamental solutions**.

To find them consider the $(n-1)$-th convergent of $\sqrt{d}$:

$$\frac{p_{n-1}}{q_{n-1}} = [a_0; a_1, a_2, \ldots, a_{n-1}].$$

Fact 2. *If the period n of the continued fraction expansion of $\sqrt{d}$ is even then $x_1 = p_{n-1},\ y_1 = q_{n-1}$ is the fundamental solution of $Pell_+$ and $Pell_-$ has no solutions. If the period n is odd then $x_0 = p_{n-1},\ y_0 = q_{n-1}$ is the fundamental solution of $Pell_-$ and the one of $Pell_+$ is $x_1 = p_{2n-1},\ y_1 = q_{2n-1}$.*

General solution

Brahmagupta's Lemma. *If* (x, y) *is a solution of* $x^2 - dy^2 = 1$ *then* (X, Y) *defined by*

$$X + Y\sqrt{d} = (x + y\sqrt{d})^k$$

is a solution too for any $k \in \mathbb{N}$.

Brahmagupta's Lemma. *If* (x, y) *is a solution of* $x^2 - dy^2 = 1$ *then* (X, Y) *defined by*

$$X + Y\sqrt{d} = (x + y\sqrt{d})^k$$

is a solution too for any $k \in \mathbb{N}$*.*

Proof. Define the **conjugate** $\bar{z}$ of the number $x + y\sqrt{d}$ as $\bar{z} = x - y\sqrt{d}$. Then one can check that

$$\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2, \quad z\bar{z} = x^2 - dy^2.$$

General solution

Brahmagupta's Lemma. *If (x, y) is a solution of $x^2 - dy^2 = 1$ then (X, Y) defined by*

$$X + Y\sqrt{d} = (x + y\sqrt{d})^k$$

is a solution too for any $k \in \mathbb{N}$.

Proof. Define the **conjugate** $\bar{z}$ of the number $x + y\sqrt{d}$ as $\bar{z} = x - y\sqrt{d}$. Then one can check that

$$\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2, \quad z\bar{z} = x^2 - dy^2.$$

If (x, y) is a solution of Pell's equation then for the $z = x + y\sqrt{d}$

$$z\bar{z} = x^2 - dy^2 = 1,$$

so for $Z = X + Y\sqrt{d}$ we have

$$X^2 - dY^2 = Z\bar{Z} = z^k \bar{z}^k = (z\bar{z})^k = 1^k = 1.$$

Brahmagupta's Lemma. *If* (x, y) *is a solution of* $x^2 - dy^2 = 1$ *then* (X, Y) *defined by*

$$X + Y\sqrt{d} = (x + y\sqrt{d})^k$$

is a solution too for any $k \in \mathbb{N}$.

Proof. Define the **conjugate** $\bar{z}$ of the number $x + y\sqrt{d}$ as $\bar{z} = x - y\sqrt{d}$. Then one can check that

$$\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2, \quad z\bar{z} = x^2 - dy^2.$$

If (x, y) is a solution of Pell's equation then for the $z = x + y\sqrt{d}$

$$z\bar{z} = x^2 - dy^2 = 1,$$

so for $Z = X + Y\sqrt{d}$ we have

$$X^2 - dY^2 = Z\bar{Z} = z^k \bar{z}^k = (z\bar{z})^k = 1^k = 1.$$

Fact 3. *All positive solutions of Pell's equation can be found from the fundamental solution* (x_1, y_1) *in this way.*

Euler's example

$$x^2 - 31y^2 = 1$$

Euler's example

$$x^2 - 31y^2 = 1$$

Continued fraction expansion

$$\sqrt{31} = [5; \overline{1, 1, 3, 5, 3, 1, 1, 10}]$$

Euler's example

$$x^2 - 31y^2 = 1$$

Continued fraction expansion

$$\sqrt{31} = [5; \overline{1, 1, 3, 5, 3, 1, 1, 10}]$$

$$\frac{p_7}{q_7} = [5; 1, 1, 3, 5, 3, 1, 1] = \frac{1520}{273},$$

so $x_1 = 1520,\ y_1 = 273$ is the fundamental solution.

Euler's example

$$x^2 - 31y^2 = 1$$

Continued fraction expansion

$$\sqrt{31} = [5; \overline{1, 1, 3, 5, 3, 1, 1, 10}]$$

$$\frac{p_7}{q_7} = [5; 1, 1, 3, 5, 3, 1, 1] = \frac{1520}{273},$$

so $x_1 = 1520,\ y_1 = 273$ is the fundamental solution.

$$(1520 + 273\sqrt{31})^2 = 4620799 + 829920\sqrt{31},$$

so next solution is $x_2 = 4620799,\ y_2 = 829920.$

Euler's example

$$x^2 - 31y^2 = 1$$

Continued fraction expansion

$$\sqrt{31} = [5; \overline{1, 1, 3, 5, 3, 1, 1, 10}]$$

$$\frac{p_7}{q_7} = [5; 1, 1, 3, 5, 3, 1, 1] = \frac{1520}{273},$$

so $x_1 = 1520,\ y_1 = 273$ is the fundamental solution.

$$(1520 + 273\sqrt{31})^2 = 4620799 + 829920\sqrt{31},$$

so next solution is $x_2 = 4620799,\ y_2 = 829920.$

Exercise. Answer Fermat's question: find the smallest positive solution of

$$x^2 - 61y^2 = 1.$$