Why do we need Gauss — Kuz'min statistics?

Alexey Ustinov

Institute of Applied Mathematics (Khabarovsk)
Russian Academy of Sciences (Far Eastern Branch)

July 7, 2011

Why do we need Gauss — Kuz’min statistics?

Alexey Ustinov

Institute of Applied Mathematics (Khabarovsk)
Russian Academy of Sciences (Far Eastern Branch)

July 7, 2011

Let

$$\frac{a}{b} = [a_0; a_1, \ldots, a_s] = a_0 + \cfrac{1}{a_1 + \ddots + \cfrac{1}{a_s}},$$

be standard continued fraction expansion with $a_0 \in \mathbb{Z}$, $a_1, \ldots, a_s \in \mathbb{N}$. Standard assumption $a_s > 1$ (for $s > 0$) we replace by another one: $a_s = 1$.

Notations
Continued fractions

Let

$$\frac{a}{b} = [a_0; a_1, \ldots, a_s] = a_0 + \cfrac{1}{a_1 + \ddots + \cfrac{1}{a_s}},$$

be standard continued fraction expansion with $a_0 \in \mathbb{Z}$, $a_1, \ldots, a_s \in \mathbb{N}$.
Standard assumption $a_s > 1$ (for $s > 0$) we replace by another one: $a_s = 1$.
Length of continued fraction will be denoted by $s(a/b)$.

For $x \in [0,1]$ and rational number $a/b = [0; a_1, \dots, a_s]$ we define **Gauss — Kuz’min statistics** $s_x(a/b)$ as

$$s_x(a/b) = \left|\left\{j : 1 \le j \le s, [0; a_j, \dots, a_s] \le x\right\}\right|.$$

In particular $s_1(a/b) = s(a/b)$ is the length of continued fraction for a/b.

For $x \in [0,1]$ and rational number $a/b = [0; a_1, \ldots, a_s]$ we define **Gauss — Kuz'min statistics** $s_x(a/b)$ as

$$s_x(a/b) = \left|\{j : 1 \le j \le s, [0; a_j, \ldots, a_s] \le x\}\right|.$$

In particular $s_1(a/b) = s(a/b)$ is the length of continued fraction for a/b. Numbers

$$N_k(a/b) = \left|\{j : 1 \le j \le s, a_j = k\}\right|$$

(also known as Gauss — Kuz'min statistics) can be expressed in terms of $s_x(a/b)$:

$$N_k(a/b) = s_{1/k}(a/b) - s_{1/(k+1)}(a/b).$$

For $x \in [0,1]$ and rational number $a/b = [0; a_1, \ldots, a_s]$ we define **Gauss — Kuz'min statistics** $s_x(a/b)$ as

$$s_x(a/b) = \left|\left\{j : 1 \le j \le s, [0; a_j, \ldots, a_s] \le x\right\}\right|.$$

In particular $s_1(a/b) = s(a/b)$ is the length of continued fraction for a/b. Numbers

$$N_k(a/b) = \left|\left\{j : 1 \le j \le s, a_j = k\right\}\right|$$

(also known as Gauss — Kuz'min statistics) can be expressed in terms of $s_x(a/b)$:

$$N_k(a/b) = s_{1/k}(a/b) - s_{1/(k+1)}(a/b).$$

We prefer s_x instead of N_k because function $\log_2(1+x)$ is more comfortable than a set of probabilities

$$p_k = \log_2\left(1 + \frac{1}{k(k+2)}\right).$$

Continued fractions and Kloosterman sums

From geometrical point of view Gauss — Kuz'min statistics describe asymptotic behaviour of $\mathbb{Z}^2$ points in a given direction.

Continued fractions and Kloosterman sums

From geometrical point of view Gauss — Kuz'min statistics describe asymptotic behaviour of $\mathbb{Z}^2$ points in a given direction.
Nontrivial bounds for classical Kloosterman sums

$$K_q(1, m, n) = \sum_{\substack{x,y=1 \\ xy\equiv 1 \pmod{q}}}^{q} e^{2\pi i \frac{mx+ny}{q}}$$

explain isotropic properties of the lattice $\mathbb{Z}^2$.
These two observations give the possibility to study different problems living on $\mathbb{Z}^2$.

Continued fractions and Kloosterman sums

From geometrical point of view Gauss — Kuz'min statistics describe asymptotic behaviour of $\mathbb{Z}^2$ points in a given direction.
Nontrivial bounds for classical Kloosterman sums

$$K_q(1,m,n)=\sum_{\substack{x,y=1\\ xy\equiv 1 \pmod{q}}}^{q} e^{2\pi i\frac{mx+ny}{q}}$$

explain isotropic properties of the lattice $\mathbb{Z}^2$.
These two observations give the possibility to study different problems living on $\mathbb{Z}^2$.
More general Kloosterman sums

$$K_q(l,m,n)=\sum_{\substack{x,y=1\\ xy\equiv l \pmod{q}}}^{q} e^{2\pi i\frac{mx+ny}{q}}$$

explain isotropic properties of sublattices in $\mathbb{Z}^2$.

- (Trivial) Euclidean algorithm, calculation of $a^{-1} \pmod n$, lattice reduction, number recognition, parametrization of solution of the equation $ad - bc = N$, calculation of convex hull of non-zero lattice points from first quadrant etc.
- Decomposition of prime $p = 4n + 1$ to the sum of two squares.
- Calculation of goodness (dicrepancy or something similar) of 2-dimesional lattice rules for numerical integration.
- Analysis of Lehmer pseudo-random number generator ($x_{n+1} = ax_n + b \pmod m$).

Applications of finite continued fractions
Usual applications

- (Trivial) Euclidean algorithm, calculation of $a^{-1} \pmod{n}$, lattice reduction, number recognition, parametrization of solution of the equation $ad - bc = N$, calculation of convex hull of non-zero lattice points from first quadrant etc.
- Decomposition of prime $p = 4n + 1$ to the sum of two squares.
- Calculation of goodness (dicrepancy or something similar) of 2-dimesional lattice rules for numerical integration.
- Analysis of Lehmer pseudo-random number generator ($x_{n+1} = ax_n + b \pmod{m}$).

- (Trivial) Euclidean algorithm, calculation of $a^{-1} \pmod{n}$, lattice reduction, number recognition, parametrization of solution of the equation $ad - bc = N$, calculation of convex hull of non-zero lattice points from first quadrant etc.
- Decomposition of prime $p = 4n + 1$ to the sum of two squares.
- Calculation of goodness (dicrepancy or something similar) of 2-dimesional lattice rules for numerical integration.
- Analysis of Lehmer pseudo-random number generator ($x_{n+1} = ax_n + b \pmod{m}$).

- (Trivial) Euclidean algorithm, calculation of $a^{-1} \pmod{n}$, lattice reduction, number recognition, parametrization of solution of the equation $ad - bc = N$, calculation of convex hull of non-zero lattice points from first quadrant etc.
- Decomposition of prime $p = 4n + 1$ to the sum of two squares.
- Calculation of goodness (dicrepancy or something similar) of 2-dimesional lattice rules for numerical integration.
- Analysis of Lehmer pseudo-random number generator ($x_{n+1} = ax_n + b \pmod{m}$).

- Rödseth's formula for Frobenius numbers with three arguments (see below).
- Analysis of *Frieze Patterns* from *The Book of Numbers* (Conway and Guy)
- Calculation of Dedekind sums and Jacobi symbols.
- Algorithm for converting a segment into a nice-looking sequence of pixels. Another algorithms of integer linear programming: finding a "closest points" in a given halfplane.
- Calculation of the number of graded algebras (Arnold).

- Rödseth's formula for Frobenius numbers with three arguments (see below).
- Analysis of *Frieze Patterns* from *The Book of Numbers* (Conway and Guy)
- Calculation of Dedekind sums and Jacobi symbols.
- Algorithm for converting a segment into a nice-looking sequence of pixels. Another algorithms of integer linear programming: finding a "closest points" in a given halfplane.
- Calculation of the number of graded algebras (Arnold).

- Rödseth's formula for Frobenius numbers with three arguments (see below).
- Analysis of *Frieze Patterns* from *The Book of Numbers* (Conway and Guy)
- Calculation of Dedekind sums and Jacobi symbols.
- Algorithm for converting a segment into a nice-looking sequence of pixels. Another algorithms of integer linear programming: finding a "closest points" in a given halfplane.
- Calculation of the number of graded algebras (Arnold).

Applications of finite continued fractions

Not so usual elementary applications

- Rödseth's formula for Frobenius numbers with three arguments (see below).
- Analysis of *Frieze Patterns* from *The Book of Numbers* (Conway and Guy)
- Calculation of Dedekind sums and Jacobi symbols.
- Algorithm for converting a segment into a nice-looking sequence of pixels. Another algorithms of integer linear programming: finding a "closest points" in a given halfplane.
- Calculation of the number of graded algebras (Arnold).

- Rödseth's formula for Frobenius numbers with three arguments (see below).
- Analysis of *Frieze Patterns* from *The Book of Numbers* (Conway and Guy)
- Calculation of Dedekind sums and Jacobi symbols.
- Algorithm for converting a segment into a nice-looking sequence of pixels. Another algorithms of integer linear programming: finding a "closest points" in a given halfplane.
- Calculation of the number of graded algebras (Arnold).

- Classification of rational tangles in knot theory (Conway).
- A criterion for a rectangle to be tilable by rectangles of a similar shape. Construction of alternating-current circuits with given properties (Skopenkov).
- Asymptotic behavior of a curve in $\mathbb{R}^n$ with constant curvature k_1, constant second curvature $k_2, \ldots$ (till constant curvature k_{n-1}). (Arnold).
- Algorithm for converting a segment into a nice-looking sequence of pixels. Another algorithms of integer linear programming: finding a “closest points” in a given halfplane.

- Classification of rational tangles in knot theory (Conway).
- A criterion for a rectangle to be tilable by rectangles of a similar shape. Construction of alternating-current circuits with given properties (Skopenkov).
- Asymptotic behavior of a curve in $\mathbb{R}^n$ with constant curvature k_1, constant second curvature $k_2, \ldots$ (till constant curvature k_{n-1}). (Arnold).
- Algorithm for converting a segment into a nice-looking sequence of pixels. Another algorithms of integer linear programming: finding a "closest points" in a given halfplane.

- Classification of rational tangles in knot theory (Conway).
- A criterion for a rectangle to be tilable by rectangles of a similar shape. Construction of alternating-current circuits with given properties (Skopenkov).
- Asymptotic behavior of a curve in $\mathbb{R}^n$ with constant curvature k_1, constant second curvature $k_2, \ldots$ (till constant curvature k_{n-1}). (Arnold).
- Algorithm for converting a segment into a nice-looking sequence of pixels. Another algorithms of integer linear programming: finding a "closest points" in a given halfplane.

- Classification of rational tangles in knot theory (Conway).
- A criterion for a rectangle to be tilable by rectangles of a similar shape. Construction of alternating-current circuits with given properties (Skopenkov).
- Asymptotic behavior of a curve in $\mathbb{R}^n$ with constant curvature k_1, constant second curvature $k_2, \ldots$ (till constant curvature k_{n-1}). (Arnold).
- Algorithm for converting a segment into a nice-looking sequence of pixels. Another algorithms of integer linear programming: finding a “closest points” in a given halfplane.

Applications of finite continued fractions

The rest part

- The way to attack RSA public key crypto system with small private exponents (Wiener).
- Singularities resolution in toric surfaces. Slam dunking of rational surgery diagrams for a three-manifolds.

- The way to attack RSA public key crypto system with small private exponents (Wiener).
- Singularities resolution in toric surfaces. Slam dunking of rational surgery diagrams for a three-manifolds.

Let $s(a/b)$ be the **length** of standard continued fraction expansion (or the length of Euclidean algorithm) for

$$a/b = [0; a_1, \ldots, a_s] \in (0, 1] \quad \text{with} \quad a_s = 1.$$

Let $s(a/b)$ be the **length** of standard continued fraction expansion (or the length of Euclidean algorithm) for

$$a/b = [0; a_1, \ldots, a_s] \in (0, 1] \quad \text{with} \quad a_s = 1.$$

First result about average length of Euclidean algorithm belongs to Heilbronn (1968), who proved that

$$\frac{1}{\varphi(b)} \sum_{\substack{1 \le a \le b \\ (a,b)=1}} s(a/b) = \frac{2\log 2}{\zeta(2)} \log b + O(\log^4 \log b).$$

Let $s(a/b)$ be the **length** of standard continued fraction expansion (or the length of Euclidean algorithm) for

$$a/b = [0; a_1, \dots, a_s] \in (0,1] \quad \text{with} \quad a_s = 1.$$

First result about average length of Euclidean algorithm belongs to Heilbronn (1968), who proved that

$$\frac{1}{\varphi(b)} \sum_{\substack{1 \le a \le b \\ (a,b)=1}} s(a/b) = \frac{2\log 2}{\zeta(2)} \log b + O(\log^4 \log b).$$

Porter (1975) has shown that

$$\frac{1}{\varphi(b)} \sum_{\substack{1 \le a \le b \\ (a,b)=1}} s(a/b) = \frac{2\log 2}{\zeta(2)} \log b + C_P + O(b^{-1/6+\varepsilon}),$$

$$C_P = \frac{2\log 2}{\zeta(2)} \left(\frac{3\log 2}{2} + 2\gamma - 2\frac{\zeta'(2)}{\zeta(2)} - 1 \right) - \frac{1}{2}.$$

We can get a better estimate of the error term for the average value of $s(a/b)$ over a, b and by using elementary arguments.

Theorem (A.U., 2008)

Let $R \geq 2$. Then

$$E(R) = \frac{2}{R(R+1)} \sum_{b \leq R} \sum_{a \leq b} s(a/b) = \frac{2 \log 2}{\zeta(2)} \log R + \widetilde{C}_P + O(R^{-1+\varepsilon}),$$

where

$$\widetilde{C}_P = C_P + \frac{2 \log 2}{\zeta(2)} \left(\frac{\zeta'(2)}{\zeta(2)} - \frac{1}{2} \right)$$

Conjecture (Arnold, 1993)

Let $\Omega(R) = R \cdot \Omega$ $(R \to \infty)$ be extending region. Then elements of finite continued fractions for rational numbers a/b, $(a, b) \in \Omega(R)$ asymptotically satisfy the Gauss — Kuz'min statistic.

Conjecture (Arnold, 1993)

Let $\Omega(R) = R \cdot \Omega$ $(R \to \infty)$ be extending region. Then elements of finite continued fractions for rational numbers a/b, $(a, b) \in \Omega(R)$ asymptotically satisfy the Gauss — Kuz'min statistic.

Theorem (Avdeeva — Bykovskii, 2002–2004)

If $\Omega(R)$ *is a sector:*

$$\Omega(R) = \{(a, b) : a, b > 0, a^2 + b^2 \leq R^2\}$$

then

$$\frac{1}{\mathrm{Vol}(\Omega(R))} \sum_{(a,b)\in\Omega(R)} s_x(a/b) = \frac{2\log(x+1)}{\zeta(2)} \log R + O(1).$$

Theorem (A.U., 2005)

For any region Ω with "good" boundary

$$\frac{1}{\mathrm{Vol}(\Omega(R))}\sum_{(a,b)\in\Omega(R)} s_x(a/b) = \frac{2\log(x+1)}{\zeta(2)}\log R + C_\Omega(x) + O(R^{-1/5+\varepsilon}).$$

But Arnold's conjecture satisfies general...

Theorem (A.U., 2005)

For any region Ω with "good" boundary

$$\frac{1}{\mathrm{Vol}(\Omega(R))}\sum_{(a,b)\in\Omega(R)} s_x(a/b)=\frac{2\log(x+1)}{\zeta(2)}\log R+C_\Omega(x)+O(R^{-1/5+\varepsilon}).$$

But Arnold's conjecture satisfies general...

The Arnold Principle

If a notion bears a personal name, then this name is not the name of the discoverer.

even so general that...

Theorem (A.U., 2005)

For any region Ω with "good" boundary

$$\frac{1}{\mathrm{Vol}(\Omega(R))}\sum_{(a,b)\in\Omega(R)} s_x(a/b)=\frac{2\log(x+1)}{\zeta(2)}\log R+C_\Omega(x)+O(R^{-1/5+\varepsilon}).$$

But Arnold's conjecture satisfies general...

The Arnold Principle

If a notion bears a personal name, then this name is not the name of the discoverer.

even so general that...

The Berry Principle

The Arnold Principle is applicable to itself.

Particular case of Arnold's conjecture was proved by Lochs.

Theorem (Lochs, 1961 (32 years before Arnold's conjecture).)

For triangle region

$$\Omega(R)=\{(a,b):0<b<a\leq R\}$$

$$\frac{1}{\mathrm{Vol}(\Omega(R))}\sum_{(a,b)\in\Omega(R)} s_x(a/b)=\frac{2\log(x+1)}{\zeta(2)}\log R+C_\Omega(x)+O(R^{-1/2+\varepsilon}).$$

Gauss — Kuz'min statistics

Results on the average length of continued fractions can be generalized on Gauss — Kuz'min statistics.

Gauss — Kuz'min statistics

Results on the average length of continued fractions can be generalized on Gauss — Kuz'min statistics.

Theorem (A.U., 2008)

$$\frac{1}{\varphi(b)}\sum_{\substack{a=1\\(a,b)=1}}^{b} s_x(a/b) = \frac{2\log(1+x)}{\zeta(2)}\log b + C_P(x) + O(b^{-1/6+\varepsilon}),$$

$$\frac{2}{R(R+1)}\sum_{b\le R}\sum_{a=1}^{b} s_x(a/b) = \frac{2\log(1+x)}{\zeta(2)}\log R + \widetilde{C}_P(x) + O(R^{-1+\varepsilon}),$$

with complicate functions $C_P(x)$ and $\widetilde{C}_P(x)$.

Gauss — Kuz'min statistics

Results on the average length of continued fractions can be generalized on Gauss — Kuz'min statistics.

Theorem (A.U., 2008)

$$\frac{1}{\varphi(b)}\sum_{\substack{a=1\\(a,b)=1}}^{b} s_x(a/b) = \frac{2\log(1+x)}{\zeta(2)}\log b + C_P(x) + O(b^{-1/6+\varepsilon}),$$

$$\frac{2}{R(R+1)}\sum_{b\le R}\sum_{a=1}^{b} s_x(a/b) = \frac{2\log(1+x)}{\zeta(2)}\log R + \widetilde{C}_P(x) + O(R^{-1+\varepsilon}),$$

with complicate functions $C_P(x)$ and $\widetilde{C}_P(x)$.

Applications: fast Euclidean algorithms.

There are three main Euclidean algorithms: **standard**, **centered** and **odd**. They are based respectively on

There are three main Euclidean algorithms: **standard**, **centered** and **odd**. They are based respectively on
standard division:

$$a = bq + r, \quad q = \lfloor a/b \rfloor, \quad 0 \le r < b;$$

There are three main Euclidean algorithms: **standard**, **centered** and **odd**. They are based respectively on
standard division:

$$a = bq + r, \quad q = \lfloor a/b \rfloor, \quad 0 \leq r < b;$$

centered division:

$$a = bq + \varepsilon r, \quad \varepsilon = \pm 1, \quad q = \left\lceil \frac{a}{b} - \frac{1}{2} \right\rceil, \quad 0 \leq r \leq \frac{b}{2};$$

There are three main Euclidean algorithms: **standard**, **centered** and **odd**. They are based respectively on
standard division:

$$a = bq + r, \quad q = \lfloor a/b \rfloor, \quad 0 \le r < b;$$

centered division:

$$a = bq + \varepsilon r, \quad \varepsilon = \pm 1, \quad q = \left\lceil \frac{a}{b} - \frac{1}{2} \right\rceil, \quad 0 \le r \le \frac{b}{2};$$

and odd division:

$$a = bq + \varepsilon r, \quad \varepsilon = \pm 1, \quad q = 2\left\lceil \frac{a}{2b} \right\rceil - 1, \quad 0 \le r \le b.$$

There are three main Euclidean algorithms: **standard**, **centered** and **odd**. They are based respectively on
standard division:

$$a = bq + r, \quad q = \lfloor a/b \rfloor, \quad 0 \le r < b;$$

centered division:

$$a = bq + \varepsilon r, \quad \varepsilon = \pm 1, \quad q = \left\lceil \frac{a}{b} - \frac{1}{2} \right\rceil, \quad 0 \le r \le \frac{b}{2};$$

and odd division:

$$a = bq + \varepsilon r, \quad \varepsilon = \pm 1, \quad q = 2\left\lceil \frac{a}{2b} \right\rceil - 1, \quad 0 \le r \le b.$$

Let $s_{centered}(a/b)$ and $s_{odd}(a/b)$ be the lengths of centered and odd Euclidean algorithms. Elementary arguments allow to reduce both these algorithms to the classical one.

Theorem (A.U., 2009–2010)

Let $b \geq 1$, $1 \leq a < b$, $(a, b) = 1$, $\varphi = \frac{1+\sqrt{5}}{2}$. *Then*

$$s_{centered}(a/b) = s_{\varphi-1}(a/b).$$

Theorem (A.U., 2009–2010)

Let $b \geq 1$, $1 \leq a < b$, $(a, b) = 1$, $\varphi = \frac{1+\sqrt{5}}{2}$. *Then*

$$s_{centered}(a/b) = s_{\varphi-1}(a/b).$$

Moreover, if $b/2 \leq a$, $aa^\star \equiv 1 \pmod{b}$, $1 \leq a^\star < b$ *then*

$$s_{odd}\left(\frac{a^\star}{b}\right) + s_{odd}\left(\frac{b-a^\star}{b}\right) = s_\varphi\left(\frac{a}{b}\right) + s_{\varphi-1}\left(\frac{a}{b}\right).$$

Theorem (A.U., 2009–2010)

Let $b \geq 1$, $1 \leq a < b$, $(a, b) = 1$, $\varphi = \frac{1+\sqrt{5}}{2}$. *Then*

$$s_{centered}(a/b) = s_{\varphi-1}(a/b).$$

Moreover, if $b/2 \leq a$, $aa^\star \equiv 1 \pmod{b}$, $1 \leq a^\star < b$ *then*

$$s_{odd}\left(\frac{a^\star}{b}\right) + s_{odd}\left(\frac{b-a^\star}{b}\right) = s_\varphi\left(\frac{a}{b}\right) + s_{\varphi-1}\left(\frac{a}{b}\right).$$

Here we used "reasonable" extension of Gauss — Kuz'min statistics for arbitrary $x > 0$:

$$s_x(a/b) = \left|\{(j,t) : 0 \leq j \leq s, 0 \leq t < a_j, [t; a_{j+1}, \ldots, a_s, 1] \leq x\}\right|$$

$(a_0 = +\infty)$.

Last theorem allows to improve some results of Baladi and Vallée (2005) on the average value of $s_{centered}(a/b)$ and $s_{odd}(a/b)$.

Last theorem allows to improve some results of Baladi and Vallée (2005) on the average value of $s_{centered}(a/b)$ and $s_{odd}(a/b)$.

Corollary

We have

$$\frac{1}{\varphi(b)}\sum_{\substack{a=1\\(a,b)=1}}^{b} s_{centered}(a/b) = \frac{2\log\varphi}{\zeta(2)}\log b + C_1 + O(b^{-1/6+\varepsilon}),$$

$$\frac{2}{R(R+1)}\sum_{b\le R}\sum_{a=1}^{b} s_{centered}(a/b) = \frac{2\log\varphi}{\zeta(2)}\log R + \widetilde{C}_1 + O(R^{-1+\varepsilon}),$$

where constants C_1 and $\widetilde{C}_1$ can be written in terms of singular series.

Corollary

We have

$$\frac{1}{\varphi(b)}\sum_{\substack{a=1\\(a,b)=1}}^{b} s_{odd}(a/b) = \frac{3\log\varphi}{\zeta(2)}\log b + C_2 + O(b^{-1/6+\varepsilon}),$$

$$\frac{2}{R(R+1)}\sum_{b\le R}\sum_{a=1}^{b} s_{odd}(a/b) = \frac{3\log\varphi}{\zeta(2)}\log R + \widetilde{C}_2 + O(R^{-1+\varepsilon}),$$

where constants C_2 and $\widetilde{C}_2$ can be written in terms of singular series.

Let $a_1, \ldots, a_n$ be positive integers with $a_i \geq 2$ and $(a_1, \ldots, a_n) = 1$. The following naive questions is known as **"Diophantine Frobenius problem"** (or **"Coin exchange problem"**):

Let $a_1, \ldots, a_n$ be positive integers with $a_i \geq 2$ and $(a_1, \ldots, a_n) = 1$. The following naive questions is known as **"Diophantine Frobenius problem"** (or **"Coin exchange problem"**):
Determine the largest number which is not of the form

$$a_1 x_1 + \cdots + a_n x_n$$

where the coefficients x_i are non-negative integers. This number is denoted by $g(a_1, \ldots, a_n)$ and is called the **Frobenius number.**

Example

Let $a = 3$, $b = 5$. Then $g(a, b) =?$

Example

Let $a = 3$, $b = 5$. Then $g(a, b) =?$
Answer: $g(a, b) = 7$:

$$7 \neq 3x + 5y \qquad (x, y \geq 0),$$

but for every $m > 7$ there are some $x, y \geq 0$ such that

$$m = 3x + 5y.$$

Frobenius numbers

The Diophantine Frobenius problem

Example

Let $a = 3$, $b = 5$. Then $g(a, b) =?$
Answer: $g(a, b) = 7$:

$$7 \neq 3x + 5y \qquad (x, y \geq 0),$$

but for every $m > 7$ there are some $x, y \geq 0$ such that

$$m = 3x + 5y.$$

It is known that

$$g(a, b) = ab - a - a.$$

The challenge is to find g when $n \geq 3$.

The difficulty of the Diophantine Frobenius problem (**FP**) grows very fast with the number of arguments.

- For $n = 2$ problem is easy: $g(a, b) = ab - a - b$.
- For $n = 3$ problem is rather complicated (see Rödseth's formula below).
- For $n > 3$ general formula is unknown). We have only different algorithms for claculation Frobenius numbers.
- Kannan (1992) gave a polynomial time algorithm for **FP** for any fixed n.
- But there is no hope for a fast (polynomial time) algorithm that solves general **FP**, unless $\mathcal{P} = \mathcal{NP}$.

The difficulty of the Diophantine Frobenius problem (**FP**) grows very fast with the number of arguments.

- For $n = 2$ problem is easy: $g(a, b) = ab - a - b$.
- For $n = 3$ problem is rather complicated (see Rödseth's formula below).
- For $n > 3$ general formula is unknown). We have only different algorithms for claculation Frobenius numbers.
- Kannan (1992) gave a polynomial time algorithm for **FP** for any fixed n.
- But there is no hope for a fast (polynomial time) algorithm that solves general **FP**, unless $\mathcal{P} = \mathcal{NP}$.

The difficulty of the Diophantine Frobenius problem (**FP**) grows very fast with the number of arguments.

- For $n = 2$ problem is easy: $g(a, b) = ab - a - b$.
- For $n = 3$ problem is rather complicated (see Rödseth's formula below).
- For $n > 3$ general formula is unknown). We have only different algorithms for claculation Frobenius numbers.
- Kannan (1992) gave a polynomial time algorithm for **FP** for any fixed n.
- But there is no hope for a fast (polynomial time) algorithm that solves general **FP**, unless $\mathcal{P} = \mathcal{NP}$.

The difficulty of the Diophantine Frobenius problem (**FP**) grows very fast with the number of arguments.

- For $n = 2$ problem is easy: $g(a, b) = ab - a - b$.
- For $n = 3$ problem is rather complicated (see Rödseth's formula below).
- For $n > 3$ general formula is unknown). We have only different algorithms for claculation Frobenius numbers.
- Kannan (1992) gave a polynomial time algorithm for **FP** for any fixed n.
- But there is no hope for a fast (polynomial time) algorithm that solves general **FP**, unless $\mathcal{P} = \mathcal{NP}$.

The difficulty of the Diophantine Frobenius problem (**FP**) grows very fast with the number of arguments.

- For $n = 2$ problem is easy: $g(a, b) = ab - a - b$.
- For $n = 3$ problem is rather complicated (see Rödseth's formula below).
- For $n > 3$ general formula is unknown). We have only different algorithms for claculation Frobenius numbers.
- Kannan (1992) gave a polynomial time algorithm for **FP** for any fixed n.
- But there is no hope for a fast (polynomial time) algorithm that solves general **FP**, unless $\mathcal{P} = \mathcal{NP}$.

We shall consider

$$f(a,b,c) = g(a,b,c) + a + b + c,$$

the **positive Frobenius number** of a, b, c, defined to be the largest integer not representable as a **positive** linear combination of a, b, c

$$ax + by + cz, \qquad x, y, z \geq 1.$$

Positive Frobenius numbers are better because of Johnson's formula: for $d \mid a$, $d \mid b$

$$f(a,b,c) = d \cdot f\left(\frac{a}{d}, \frac{b}{d}, c\right).$$

Example

Let $a = 3$, $b = 5$, $c = 7$. Then $g(a, b, c) =?$

Example

Let $a = 3$, $b = 5$, $c = 7$. Then $g(a, b, c) = ?$
Answer: $g(3, 5, 7) = 4$:

$$4 \neq 3x + 5y + 7z \qquad (x, y, z \geq 0),$$

but for any $m > 4$ we can find $x, y, z \geq 0$ such that

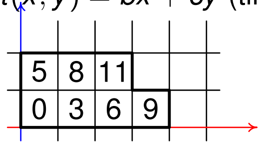
$$m \neq 3x + 5y + 7z.$$

Double loop network

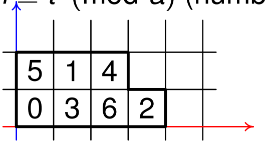
$b = 3$ (red step), $c = 5$ (blue step), $a = 7$ (number of vertices)

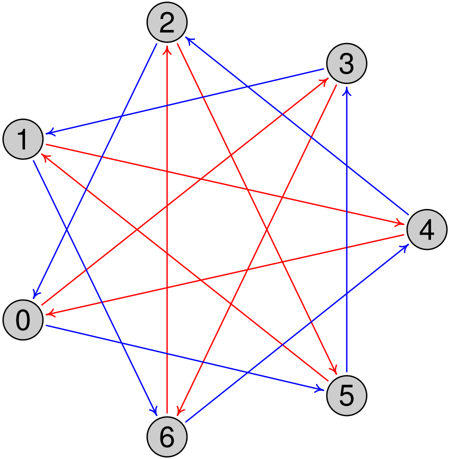
length($\color{red}{\uparrow}$)$= 3$, length($\color{blue}{\uparrow}$)$= 5$

$t(x, y) = bx + cy$ (time)



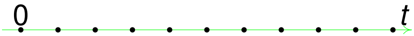
$n \equiv t \pmod{a}$ (number)



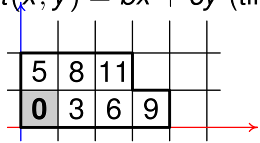


Double loop network

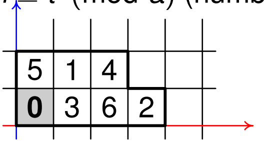
$b = 3$ (red step), $c = 5$ (blue step), $a = 7$ (number of vertices)

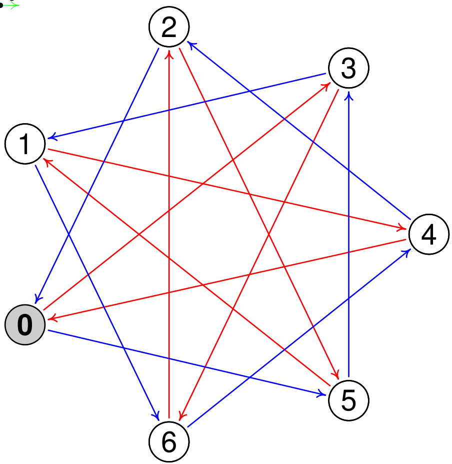


$t(x, y) = bx + cy$ (time)



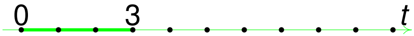
$n \equiv t \pmod{a}$ (number)



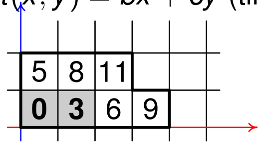


Double loop network

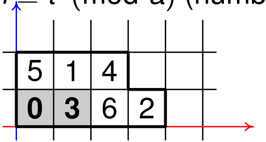
$b = 3$ (red step), $c = 5$ (blue step), $a = 7$ (number of vertices)

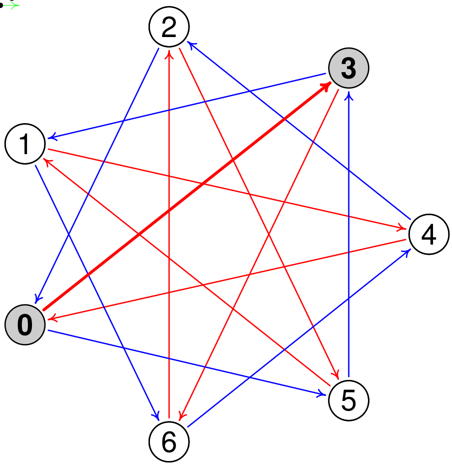


$t(x, y) = bx + cy$ (time)



$n \equiv t \pmod{a}$ (number)





Double loop network

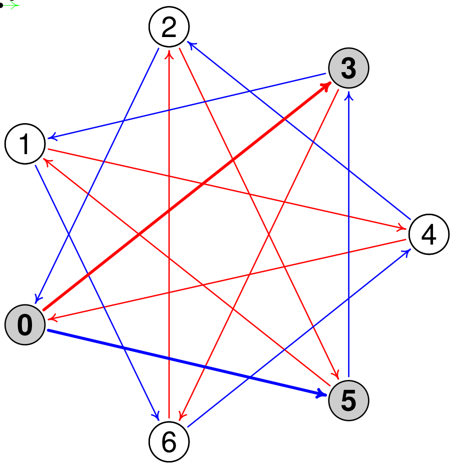
$b = 3$ (red step), $c = 5$ (blue step), $a = 7$ (number of vertices)

$t(x, y) = bx + cy$ (time)

5	8	11	
0	**3**	6	9

$n \equiv t \pmod{a}$ (number)

5	1	4	
0	**3**	6	2



Double loop network

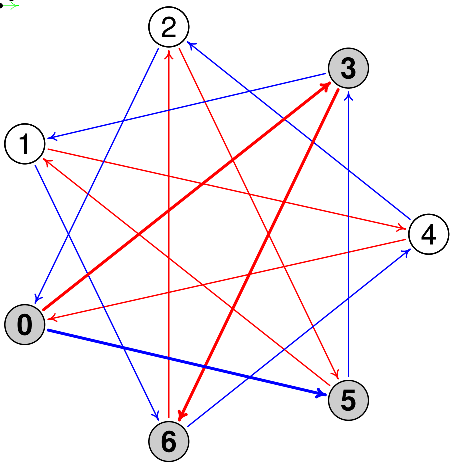
$b = 3$ (red step), $c = 5$ (blue step), $a = 7$ (number of vertices)

$t(x, y) = bx + cy$ (time)

5	8	11	
0	**3**	**6**	9

$n \equiv t \pmod{a}$ (number)

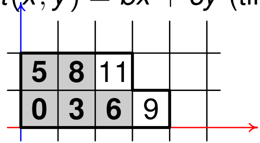
5	1	4	
0	**3**	**6**	2



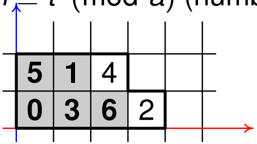
Double loop network

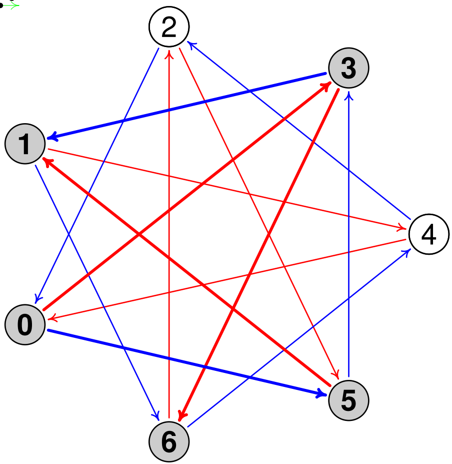
$b = 3$ (red step), $c = 5$ (blue step), $a = 7$ (number of vertices)

$t(x, y) = bx + cy$ (time)



$n \equiv t \pmod{a}$ (number)

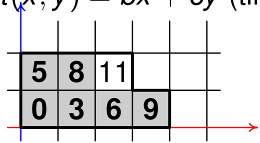




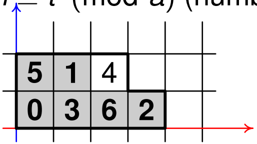
Double loop network

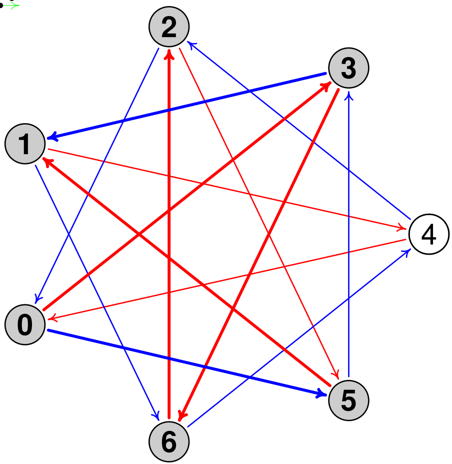
$b = 3$ (red step), $c = 5$ (blue step), $a = 7$ (number of vertices)

$t(x, y) = bx + cy$ (time)



$n \equiv t \pmod{a}$ (number)

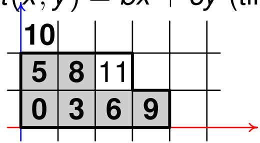




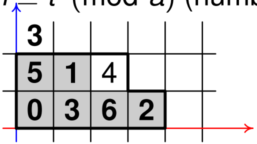
Double loop network

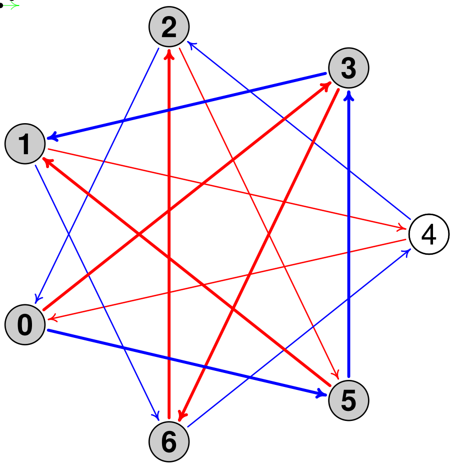
$b = 3$ (red step), $c = 5$ (blue step), $a = 7$ (number of vertices)

$t(x, y) = bx + cy$ (time)



$n \equiv t \pmod{a}$ (number)

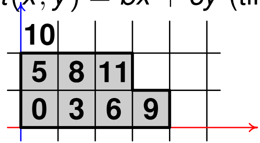




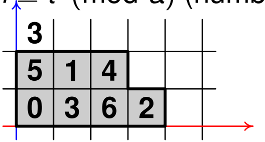
Double loop network

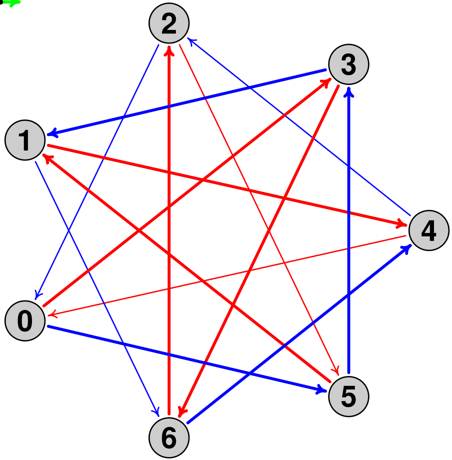
$b = 3$ (red step), $c = 5$ (blue step), $a = 7$ (number of vertices)

$t(x, y) = bx + cy$ (time)



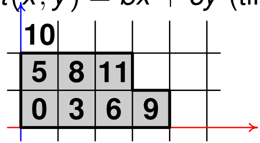
$n \equiv t \pmod{a}$ (number)



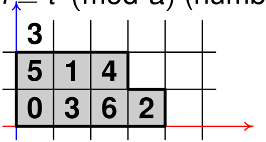


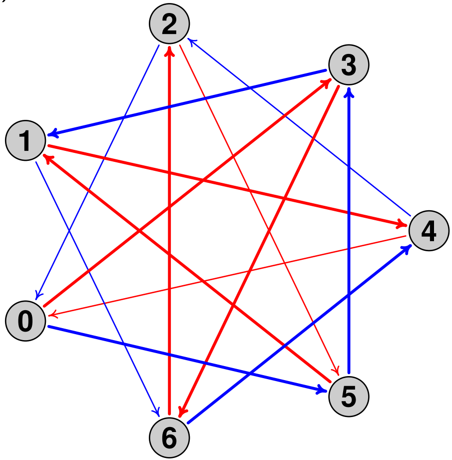
$$\mathrm{diam} = g(a, b, c) + a \quad (= 11)$$

$t(x, y) = bx + cy$ (time)



$n \equiv t \pmod{a}$ (number)





Double loop network
Properties

- Minimum distance diagram is always L-shaped (Wong, Coppersmith, 1974).
- L-shape always tessellates the plane.
- Form of L-shape depends on the properties of the lattice $\Lambda = \{(x, y) : bx + cy \equiv 0 \pmod{a}\}$.

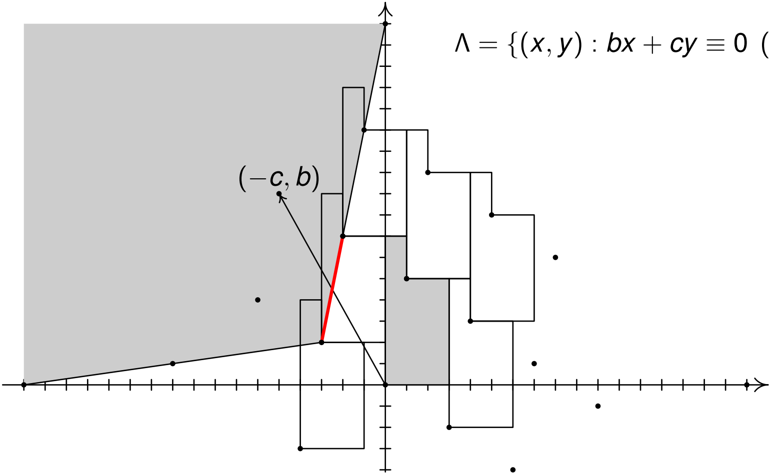
Double loop network
Properties

- Minimum distance diagram is always L-shaped (Wong, Coppersmith, 1974).
- L-shape always tessellates the plane.
- Form of L-shape depends on the properties of the lattice $\Lambda = \{(x, y) : bx + cy \equiv 0 \pmod{a}\}$.

- Minimum distance diagram is always L-shaped (Wong, Coppersmith, 1974).
- L-shape always tessellates the plane.
- Form of L-shape depends on the properties of the lattice $\Lambda = \{(x, y) : bx + cy \equiv 0 \pmod{a}\}$

Double loop network

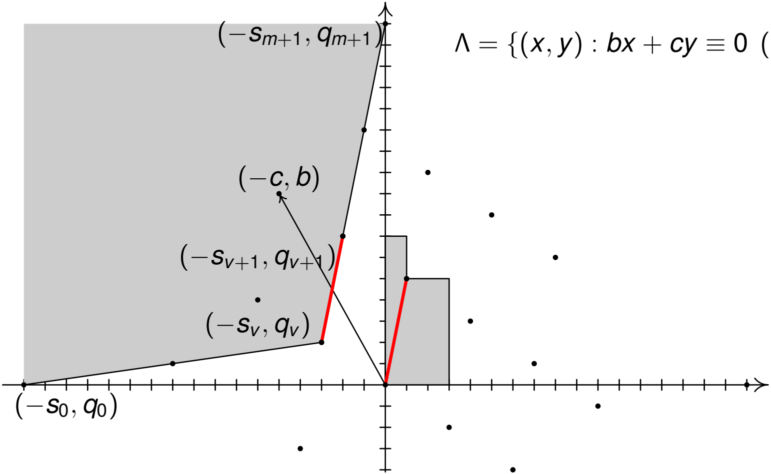
$b = 9$ (red step), $c = 5$ (blue step), $a = 17$ (number of vertices)



$$\Lambda = \{(x, y) : bx + cy \equiv 0 \pmod{a}\}$$

Double loop network

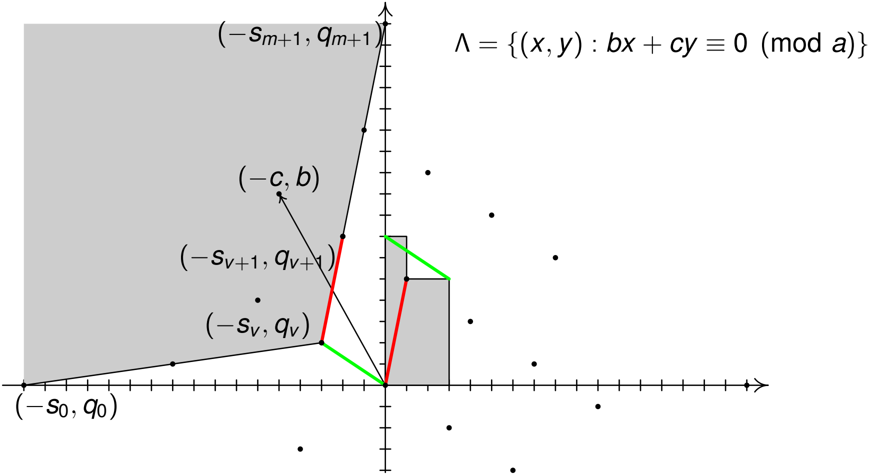
$b = 9$ (red step), $c = 5$ (blue step), $a = 17$ (number of vertices)



$$\Lambda = \{(x, y) : bx + cy \equiv 0 \pmod{a}\}$$

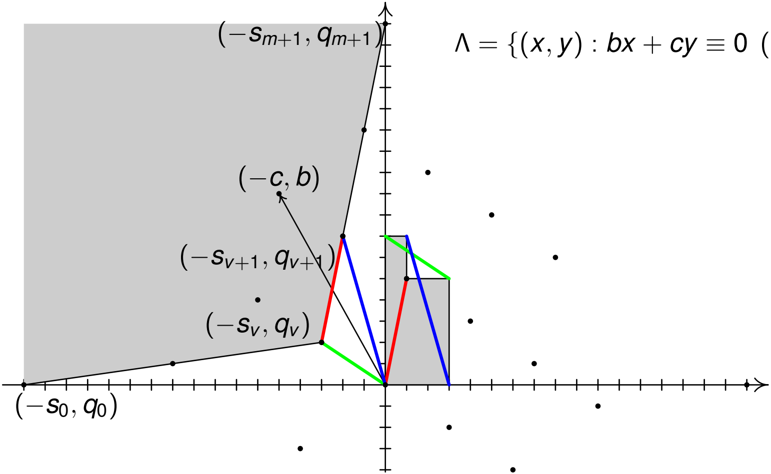
Double loop network

$b = 9$ (red step), $c = 5$ (blue step), $a = 17$ (number of vertices)



Double loop network

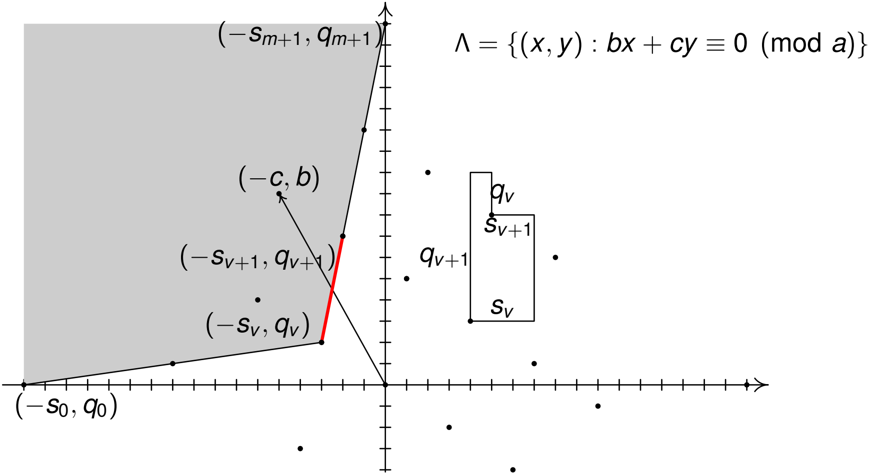
$b = 9$ (red step), $c = 5$ (blue step), $a = 17$ (number of vertices)



$$\Lambda = \{(x, y) : bx + cy \equiv 0 \pmod{a}\}$$

Double loop network

$b = 9$ (red step), $c = 5$ (blue step), $a = 17$ (number of vertices)



From obvious property

$$0 = \frac{s_{m+1}}{q_{m+1}} < \frac{s_{m-1}}{q_{m-1}} < \ldots < \frac{s_1}{q_1} < \frac{s_0}{q_0} = \infty$$

follows that for some n

$$\frac{s_n}{q_n} \leq \frac{c}{b} < \frac{s_{n-1}}{q_{n-1}}.$$

From obvious property

$$0 = \frac{s_{m+1}}{q_{m+1}} < \frac{s_{m-1}}{q_{m-1}} < \ldots < \frac{s_1}{q_1} < \frac{s_0}{q_0} = \infty$$

follows that for some n

$$\frac{s_n}{q_n} \le \frac{c}{b} < \frac{s_{n-1}}{q_{n-1}}.$$

Theorem (Ö. Rödseth, 1978)

$$f(a, b, c) = bs_{n-1} + cq_n - \min\{bs_n, cq_{n-1}\}.$$

Rödseth's formula can be written in terms of reduced regular continued fraction. We want to find $f(a,b,c)$ for $(a,b)=(a,c)=(b,c)=1$.
Let l is such that

$$bl \equiv c \pmod{a}, \qquad 1 \le l \le a.$$

Reduced regular continued fraction

$$\frac{a}{l} = \langle a_1, \dots, a_m \rangle = a_1 - \cfrac{1}{a_2 - \ddots - \cfrac{1}{a_m}},$$

where $a_1, \dots, a_m \geq 2$, defines sequences $\{s_j\}$, $\{q_j\}$ by

$$\frac{q_{j+1}}{q_j} = \langle a_j, \dots, a_1 \rangle, \qquad \frac{s_j}{s_{j+1}} = \langle a_{j+1}, \dots, a_m \rangle \qquad (0 \le j \le m).$$

Rödseth's formula can be written in terms of reduced regular continued fraction. We want to find $f(a,b,c)$ for $(a,b)=(a,c)=(b,c)=1$.
Let l is such that

$$bl \equiv c \pmod{a}, \qquad 1 \le l \le a.$$

Reduced regular continued fraction

$$\frac{a}{l} = \langle a_1, \ldots, a_m \rangle = a_1 - \cfrac{1}{a_2 - \ddots - \cfrac{1}{a_m}},$$

where $a_1, \ldots, a_m \ge 2$, defines sequences $\{s_j\}$, $\{q_j\}$ by

$$\frac{q_{j+1}}{q_j} = \langle a_j, \ldots, a_1 \rangle, \qquad \frac{s_j}{s_{j+1}} = \langle a_{j+1}, \ldots, a_m \rangle \qquad (0 \le j \le m).$$

Rödseth's formula can be written in terms of reduced regular continued fraction. We want to find $f(a, b, c)$ for $(a, b) = (a, c) = (b, c) = 1$.
Let l is such that

$$bl \equiv c \pmod{a}, \qquad 1 \le l \le a.$$

Reduced regular continued fraction

$$\frac{a}{l} = \langle a_1, \dots, a_m \rangle = a_1 - \cfrac{1}{a_2 - \ddots - \cfrac{1}{a_m}},$$

where $a_1, \dots, a_m \ge 2$, defines the same sequences $\{s_j\}$, $\{q_j\}$ by

$$\frac{q_{j+1}}{q_j} = \langle a_j, \dots, a_1 \rangle, \qquad \frac{s_j}{s_{j+1}} = \langle a_{j+1}, \dots, a_m \rangle \qquad (0 \le j \le m).$$

we have one-to-one correspondence between the set of quadruples $(q_n, s_n, q_{n-1}, s_{n-1})$ (taken for all lattices Λ_l) and the solutions of the equation

$$x_1 y_1 - x_2 y_2 = a$$

with $0 \le x_2 < x_1$, $0 \le y_2 < y_1$, $(x_1, x_2) = (y_1, y_2) = 1$:

$$(q_n, s_n, q_{n-1}, s_{n-1}) \longleftrightarrow (x_1, x_2, y_2, y_1).$$

From the equation

$$x_1 y_1 - x_2 y_2 = a$$

it follows that

$$x_1 y_1 \equiv a \pmod{x_2},$$

and **Kloosterman sums**

$$K_q(l, m, n) = \sum_{\substack{x,y=1 \\ xy \equiv l \pmod{q}}}^{q} e^{2\pi i \frac{mx+ny}{q}}$$

come into play. Solutions of the congruence $xy \equiv l \pmod{q}$ are uniformly distributed due to the bounds for Kloosterman sums.

This fact allows to calculate sums of the form

$$\sum_{xy\equiv l \pmod{q}} F(x,y)$$

and

$$\sum_{x_1y_1-x_2y_2=a} F(x_1,y_1,x_2,y_2).$$

In particular it allows to study distribution of Frobenius numbers $f(a,b,c)$.

Rödseth (1990) proved a lower bound for Frobenius numbers:

$$f(a_1, \ldots, a_n) \geq \sqrt[n-1]{(n-1)!a_1 \ldots a_n}.$$

Conjecture (Davison, 1994)

Average value of normalized Frobenius numbers $\frac{f(a,b,c)}{\sqrt{abc}}$ over cube $[1, N]^3$ tends to some constant as $N \to \infty$.

Rödseth (1990) proved a lower bound for Frobenius numbers:

$$f(a_1,\dots,a_n) \geq \sqrt[n-1]{(n-1)!a_1\dots a_n}.$$

Conjecture (Davison, 1994)

Average value of normalized Frobenius numbers $\frac{f(a,b,c)}{\sqrt{abc}}$ over cube $[1,N]^3$ tends to some constant as $N \to \infty$.

Conjecture (Arnold, 1999, 2005)

There is weak asymptotic for Frobenius numbers: for arbitrary n average value of $f(x_1,\dots,x_n)$ over small cube with a center in $(a_1,\dots,a_n)$ approximately equal to $c_n \sqrt[n-1]{a_1\dots a_n}$ for some constant $c_n > 0$.

Frobenius numbers

Bourgain and Sinaĭ in 2007 proved (with a little gap: they used one natural assumption which was proved later) that normalized Frobenius numbers $\frac{f(a,b,c)}{\sqrt{abc}}$ have limiting density function.

Frobenius numbers
Weak asymptotic

Let $x_1, x_2 > 0$ and
$M_a(x_1, x_2) = \{(b, c) : 1 \le b \le x_1 a, 1 \le c \le x_2 a, (a, b, c) = 1\}$.

Let $x_1, x_2 > 0$ and
$M_a(x_1, x_2) = \{(b, c) : 1 \le b \le x_1 a, 1 \le c \le x_2 a, (a, b, c) = 1\}$.

Theorem (A.U., 2009)

Frobenius numbers $f(a, b, c)$ have weak asymptotic $\frac{8}{\pi}\sqrt{abc}$:

$$\frac{1}{a^{3/2}|M_a(x_1, x_2)|} \sum_{(b,c)\in M_a(x_1,x_2)} \left(f(a, b, c) - \frac{8}{\pi}\sqrt{abc} \right) = O_{\varepsilon,x_1,x_2}(a^{-1/6+\varepsilon}).$$

Davison's conjecture holds in a stronger form:

$$\frac{1}{|M_a(x_1, x_2)|} \sum_{(b,c)\in M_a(x_1,x_2)} \frac{f(a, b, c)}{\sqrt{abc}} = \frac{8}{\pi} + O_{\varepsilon,x_1,x_2}(a^{-1/12+\varepsilon}).$$

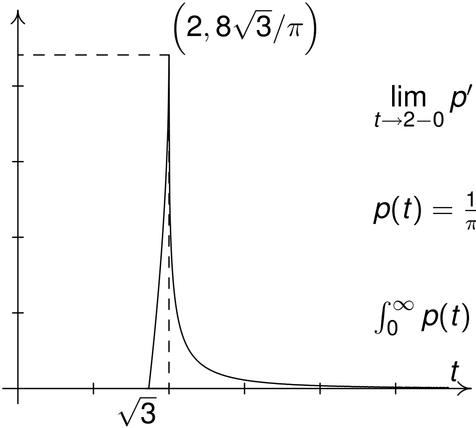
Theorem (A.U., 2010)

Normalized Frobenius numbers of three arguments have limiting density function:

$$\frac{1}{|M_a(x_1,x_2)|}\sum_{\substack{(b,c)\in M_a(x_1,x_2)\\ f(a,b,c)\le\tau\sqrt{abc}}} 1=\int_0^{\tau} p(t)\,dt+O_{\varepsilon,x_1,x_2,\tau}(a^{-1/6+\varepsilon}),$$

where

$$p(t)=\begin{cases}0, & \text{if } t\in[0,\sqrt{3}];\\ \frac{12}{\pi}\left(\frac{t}{\sqrt{3}}-\sqrt{4-t^2}\right), & \text{if } t\in[\sqrt{3},2];\\ \frac{12}{\pi^2}\left(t\sqrt{3}\arccos\frac{t+3\sqrt{t^2-4}}{4\sqrt{t^2-3}}+\frac{3}{2}\sqrt{t^2-4}\log\frac{t^2-4}{t^2-3}\right), & \text{if } t\in[2,+\infty).\end{cases}$$



$$\lim_{t \to 2-0} p'(t) = +\infty, \quad \lim_{t \to 2+0} p'(t) = -\infty$$

$$p(t) = \frac{18}{\pi^3} \cdot \frac{1}{t^3} + O\left(\frac{1}{t^5}\right) \qquad (t \to \infty)$$

$$\int_0^\infty p(t)\,dt = 1, \qquad \int_0^\infty tp(t)\,dt = \frac{8}{\pi}$$

Triples (α, β, r), where

$$\alpha = \frac{q_n}{\sqrt{a/\xi}}, \quad \beta = \frac{s_{n-1}}{\sqrt{a\xi}}, \quad r = \frac{s_n}{\sqrt{a\xi}} \qquad (\xi = c/b)$$

(normalized edges of L-shaped diagram) have joint limiting density function

$$p(\alpha, \beta, r) = \begin{cases} \dfrac{2}{\zeta(2)r}, & r \leq \min\{\alpha, \beta\}, 1 \leq \alpha\beta \leq 1 + r^2, \\ 0 & else. \end{cases}$$

It allows to study shortest cycles, average distances and another characteristics of L-shaped diagrams (double loop networks).

For usual Kloosterman sums

$$K_q(1,m,n) = \sum_{\substack{x,y=1 \\ xy\equiv 1 \pmod q}}^{q} e^{2\pi i \frac{mx+ny}{q}}$$

Estermann bound is known

$$|K_q(1,m,n)| \le \sigma_0(q) \cdot (m,n,q)^{1/2} \cdot q^{1/2}.$$

This bound can be generalized for the case of sums $K_q(l,m,n)$.

For usual Kloosterman sums

$$K_q(1,m,n) = \sum_{\substack{x,y=1 \\ xy\equiv 1 \pmod{q}}}^{q} e^{2\pi i \frac{mx+ny}{q}}$$

Estermann bound is known

$$|K_q(1,m,n)| \le \sigma_0(q)\cdot(m,n,q)^{1/2}\cdot q^{1/2}.$$

This bound can be generalized for the case of sums $K_q(l,m,n)$.

Theorem (A.U., 2008)

$$|K_q(l,m,n)| \le \sigma_0(q)\cdot\sigma_0((l,m,n,q))\cdot(lm,ln,mn,q)^{1/2}\cdot q^{1/2}.$$

This estimate allows to count solutions of the congruence $xy \equiv l \pmod{a}$ in different regions.

Corollary

Let $q \geq 1$, $0 \leq P_1, P_2 \leq q$. Then for any real Q_1, Q_2

$$\sum_{\substack{Q_1 < x \leq Q_1 + P_1 \\ Q_2 < y \leq Q_2 + P_2}} \delta_q(xy - 1) = \frac{\varphi(q)}{q^2} \cdot P_1 P_2 + O\left(\sigma_0(q) \log^2(q+1) q^{1/2}\right)$$

and

$$\sum_{\substack{Q_1 < x \leq Q_1 + P_1 \\ Q_2 < y \leq Q_2 + P_2}} \delta_q(xy - l) = \frac{K_q(0,0,l)}{q^2} \cdot P_1 P_2 + O\left(q^{1/2+\varepsilon} + (q,l) q^{\varepsilon}\right).$$

General idea
Kloosterman sums

A combination with **van der Corput's method** of exponential sums allows to count solutions under a graph of smooth function.

A combination with **van der Corput's method** of exponential sums allows to count solutions under a graph of smooth function.

Let $q \geq 1$, f be positive function and $T[f]$ be the number of solutions of the congruence $xy \equiv l \pmod q$ in the region $P_1 < x \leq P_2$, $0 < y \leq f(x)$:

$$T[f] = \sum_{P_1 < x \leq P_2} \sum_{0 < y \leq f(x)} \delta_q(xy - l).$$

A combination with **van der Corput's method** of exponential sums allows to count solutions under a graph of smooth function.
Let $q \geq 1$, f be positive function and $T[f]$ be the number of solutions of the congruence $xy \equiv l \pmod{q}$ in the region $P_1 < x \leq P_2$, $0 < y \leq f(x)$:

$$T[f] = \sum_{P_1 < x \leq P_2} \sum_{0 < y \leq f(x)} \delta_q(xy - l).$$

Let

$$S[f] = \sum_{P_1 < x \leq P_2} \frac{\mu_{q,l}(x)}{q} f(x),$$

where $\mu_{q,l}(x)$ is the number of solutions of the congruence $xy \equiv l \pmod{q}$ over y such that $1 \leq y \leq q$.

Theorem (A.U., 2008)

Let P_1, P_2 be reals, $P = P_2 - P_1 \geq 2$ and for some $A > 0$, $w \geq 1$ function $f(x)$ satisfies conditions

$$\frac{1}{A} \leq |f''(x)| \leq \frac{w}{A}.$$

Then

$$T[f] = S[f] - \frac{P}{2} \cdot \delta_q(l) + R[f],$$

where

$$R[f] \ll_w (PA^{-1/3} + A^{1/2}(l,q)^{1/2} + q^{1/2})P^{\varepsilon}.$$

Recent results

- The existence of limiting distribution for normalized Frobenius numbers of arbitrary number of arguments was proved by J. Marklof (2010).
- Distribution of diameters and distribution of shortest cycles in *circulant graphs* (often also called multi-loop networks) were studied by J. Marklof and A. Strömbergsson (2011). They proved existence of these distributions for arbitrary n and made some interesting numerical computations.
- For $n = 3$ Davison's conjecture in a stronger form was proved by D. Frolenkov (2011).

Recent results

- The existence of limiting distribution for normalized Frobenius numbers of arbitrary number of arguments was proved by J. Marklof (2010).
- Distribution of diameters and distribution of shortest cycles in *circulant graphs* (often also called multi-loop networks) were studied by J. Marklof and A. Strömbergsson (2011). They proved existence of these distributions for arbitrary n and made some interesting numerical computations.
- For $n = 3$ Davison's conjecture in a stronger form was proved by D. Frolenkov (2011).

Recent results

- The existence of limiting distribution for normalized Frobenius numbers of arbitrary number of arguments was proved by J. Marklof (2010).
- Distribution of diameters and distribution of shortest cycles in *circulant graphs* (often also called multi-loop networks) were studied by J. Marklof and A. Strömbergsson (2011). They proved existence of these distributions for arbitrary n and made some interesting numerical computations.
- For $n = 3$ Davison's conjecture in a stronger form was proved by D. Frolenkov (2011).

Sinai problem

Let $0 < h < \frac{1}{8}$, $T > 0$ and $\Omega_h(T)$ is the set of angles $\varphi \in [0, 2\pi)$ such that the ray

$$\{(t\cos\varphi, t\sin\varphi) : t \geq 0\}$$

intersects h-neighborhood of some integer point $(m, n) \neq (0, 0)$ from the circle

$$\left\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq T^2\right\}.$$

Denote by $G_h(T)$ normalized measure of $\Omega_h(T)$:

$$G_h(T) = \frac{1}{2\pi} \operatorname{mes} \Omega_h(T) \in [0, 1].$$

In 1918 Polya proved that

$$G_h(T) = 1$$

for all $T \geq h^{-1}$.

Sinai problem

Boca, Gologan and Zaharescu (2003) proved that for all $\varepsilon > 0$ uniformly over $T \in [0, h^{-1}]$

$$G_h(T) = \int_0^{h \cdot T} \sigma(t)\, dt + O_\varepsilon(h^{1/8-\varepsilon}),$$

where

$$\sigma(t) = \begin{cases} \frac{12}{\pi^2}, & \text{if } 0 \le t \le \frac{1}{2}; \\ \frac{12}{\pi^2}\left(\frac{1}{t} - 1\right)\left(1 - \log\left(\frac{1}{t} - 1\right)\right), & \text{if } \frac{1}{2} < t \le 1. \end{cases}$$

From physical point of view $G_h(T)$ is the density function for free path lengths in 2-dimensional Lorentz gas.

Sinai problem

We considered more general situation when trajectories start from h-neighborhood of the origin. Let $v \in (-1, 1)$ be the fixed number and the particle moves along the ray

$$\left\{(-hv\sin\varphi + t\cos\varphi, hv\cos\varphi + t\sin\varphi) \in \mathbb{R}^2 : t \geq 0\right\}. \tag{1}$$

Let $(m(\varphi), n(\varphi))$ be the center of the first h-neighborhood intersected by the ray.

Sinai problem

In other words $(m(\varphi), n(\varphi))$ is the nearest to the origin point such that

$$R(m,n) > 0 \quad \text{and} \quad |U(m,n)| < h$$

where

$$R(x,y) = x\cos\varphi + y\sin\varphi,$$
$$U(x,y) = x\sin\varphi - y\cos\varphi + hv.$$

We denote by

$$r(\varphi) = h \cdot R\,(m(\varphi), n(\varphi))\,, \quad u(\varphi) = h^{-1} \cdot U\,(m(\varphi), n(\varphi))\,.$$

normalized free path length and normalized sighting (aiming?) parameter.

Sinai problem

Suppose

$$0 < r_0 < \frac{1}{1-|v|} \quad \text{and} \quad -1 < u_- < u_+ < 1.$$

Theorem (Bykovskii, A.U., 2007–2008)

Let $|v| < c < 1$. *Then for all* $\varepsilon > 0$ *for the distribution function*

$$\Phi_v(h) = \Phi_v(h; \varphi_0, r_0, u_-, u_+) = \\ = \int_0^{\varphi_0} \chi_{[0,r_0]}\left(r(\varphi)\right) \chi_{[u_-,u_+]}\left(u(\varphi)\right)\, d\varphi$$

following asymptotic formula holds $(h \to 0)$

$$\Phi_v(h) = \int_0^{\varphi_0} \int_0^{r_0} \int_{u_-}^{u_+} \rho(\varphi, r, v, u)\, d\varphi\, dr\, du + O_{\varepsilon,c}\left(h^{\frac{1}{2}-\varepsilon}\right).$$

Sinai problem

Density function has following symmetries

$$\rho(\varphi, r, v, u) = \rho(r, v, u) = \rho(r, u, v) = \rho(r, -u, -v),$$

for $u \geq |v|$ is equal to

$$\rho(r, u, v) = \begin{cases} \frac{6}{\pi^2}, & \text{if } \ 0 \leq r \leq \frac{1}{u+1}; \\ \frac{6}{\pi^2} \cdot \frac{1}{u-v} \left(\frac{1}{r} - 1 - v \right), & \text{if } \ \frac{1}{u+1} \leq r \leq \frac{1}{1+v}; \\ 0, & \text{if } \ \frac{1}{1+v} \leq r. \end{cases}$$

From physical point of view $\frac{1}{2\pi}\rho(\varphi, r, v, u)$ is the density of the particles moving along the ray (1), with unit speed after first reflection in h-neighborhood of the origin and passing distance $R = h^{-1} \cdot r$ before next reflection with sighting parameter $h \cdot u$.

Reduced bases in two-dimensional lattices

Reduced (2-dimensional) bases are important in different number theory algorithms:

- fast point multiplication on elliptic curves;
- prediction of pseudo random generators, numerical integration;
- combinatorial optimization. . .

Reduced bases in two-dimensional lattices

Reduced (2-dimensional) bases are important in different number theory algorithms:

- fast point multiplication on elliptic curves;
- prediction of pseudo random generators, numerical integration;
- combinatorial optimization...

Reduced bases in two-dimensional lattices

Reduced (2-dimensional) bases are important in different number theory algorithms:

- fast point multiplication on elliptic curves;
- prediction of pseudo random generators, numerical integration;
- combinatorial optimization...

Work of these algorithms depends on properties of reduced basis (shorter vectors are better).

Reduced bases in two-dimensional lattices

Let $1 \le l \le a$, $(l, a) = 1$ and e_1 be the shortest vector of the lattice $\Lambda_l = \{(x, y) : lx \equiv y \pmod{a}\}$.

Reduced bases in two-dimensional lattices

Let $1 \leq l \leq a$, $(l, a) = 1$ and e_1 be the shortest vector of the lattice $\Lambda_l = \{(x, y) : lx \equiv y \pmod{a}\}$. Basis (e_1, e_2) is reduced iff $e_2 \in \Omega(e_1)$ where $\Omega(e_1)$ is the plane region defined by inequalities

$$\|e_2\| \geq \|e_1\| \quad \text{and} \quad \|e_2 \pm e_1\| \geq \|e_2\|.$$

Reduced bases in two-dimensional lattices

Let $1 \leq l \leq a$, $(l, a) = 1$ and e_1 be the shortest vector of the lattice $\Lambda_l = \{(x, y) : lx \equiv y \pmod{a}\}$. Basis (e_1, e_2) is reduced iff $e_2 \in \Omega(e_1)$ where $\Omega(e_1)$ is the plane region defined by inequalities

$$\|e_2\| \geq \|e_1\| \quad \text{and} \quad \|e_2 \pm e_1\| \geq \|e_2\|.$$

Moreover vector e_2 must lie on the line $l(e_1)$ defined by equation $\det(e_1, e_2) = a$.

Reduced bases in two-dimensional lattices

Let $1 \leq l \leq a$, $(l, a) = 1$ and e_1 be the shortest vector of the lattice $\Lambda_l = \{(x, y) : lx \equiv y \pmod{a}\}$. Basis (e_1, e_2) is reduced iff $e_2 \in \Omega(e_1)$ where $\Omega(e_1)$ is the plane region defined by inequalities

$$\|e_2\| \geq \|e_1\| \quad \text{and} \quad \|e_2 \pm e_1\| \geq \|e_2\|.$$

Moreover vector e_2 must lie on the line $l(e_1)$ defined by equation $\det(e_1, e_2) = a$. By averaging over l we can get that vectors e_2 distributed uniformly on $\Omega(e_1) \cap l(e_1)$ with weight $\|e_2\|_2^{-1}$. Suppose $e_1 = \sqrt{a}(\alpha, \beta)$, $e_2 = \sqrt{a}(\gamma, \delta)$.

Reduced bases in two-dimensional lattices

For example in the case of the most popular $\|\cdot\|_\infty$-norm integration over e_2 lead to the density function for e_1:

Reduced bases in two-dimensional lattices

For example in the case of the most popular $\|\cdot\|_\infty$-norm integration over e_2 lead to the density function for e_1:

$$p(\alpha,\beta)=p(\pm\alpha,\pm\beta)=p(\beta,\alpha);$$

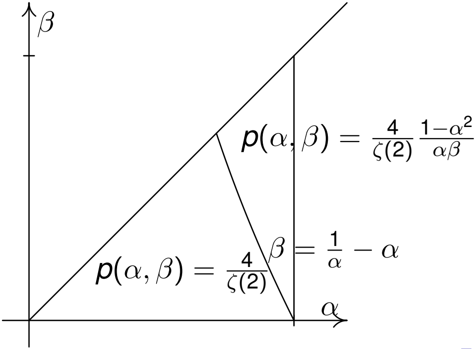
$$p(\alpha,\beta)=\frac{4}{\zeta(2)}\min\left\{1,\frac{1-\alpha^2}{\alpha\beta}\right\}\qquad(0\le\beta\le\alpha\le1).$$

Reduced bases in two-dimensional lattices

For example in the case of the most popular $\|\cdot\|_\infty$-norm integration over e_2 lead to the density function for e_1:

$$p(\alpha,\beta)=p(\pm\alpha,\pm\beta)=p(\beta,\alpha);$$

$$p(\alpha,\beta)=\frac{4}{\zeta(2)}\min\left\{1,\frac{1-\alpha^2}{\alpha\beta}\right\}\qquad(0\le\beta\le\alpha\le1).$$



Reduced bases in two-dimensional lattices

By integrating over e_1 we can get density function for $t = \|e_2\|/\sqrt{a}$:

Reduced bases in two-dimensional lattices

By integrating over e_1 we can get density function for $t = \|e_2\|/\sqrt{a}$:

$$p(t) = \begin{cases} 0, & \text{if } t \in \left[0, 1/\sqrt{2}\right]; \\ \frac{4}{\zeta(2)}\left(2t - \frac{1}{t} + \left(\frac{1}{t} - t\right)\log\left(\frac{1}{t^2} - 1\right)\right), & \text{if } t \in \left[1/\sqrt{2}, 1\right]; \\ \frac{4}{\zeta(2)}\left(\frac{1}{t} + \left(t - \frac{1}{t}\right)\log\left(1 - \frac{1}{t^2}\right)\right), & \text{if } t \in [1, \infty]. \end{cases}$$

By integrating over e_1 we can get density function for $t = \|e_2\|/\sqrt{a}$:

$$p(t) = \begin{cases} 0, & \text{if } t \in \left[0, 1/\sqrt{2}\right]; \\ \frac{4}{\zeta(2)}\left(2t - \frac{1}{t} + \left(\frac{1}{t} - t\right)\log\left(\frac{1}{t^2} - 1\right)\right), & \text{if } t \in \left[1/\sqrt{2}, 1\right]; \\ \frac{4}{\zeta(2)}\left(\frac{1}{t} + \left(t - \frac{1}{t}\right)\log\left(1 - \frac{1}{t^2}\right)\right), & \text{if } t \in [1, \infty]. \end{cases}$$