Kloosterman Sums and Continued Fractions

Alexey Ustinov

Russian Academy of Sciences
Institute of Applied Mathematics (Khabarovsk)

July 8, 2010

Let $1 \leq l \leq a$, $(l, a) = 1$. 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 $a_1, \ldots, a_m \geq 2$, defines sequences $\{s_j\}$, $\{q_j\}$ by

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

Let $1 \leq l \leq a$, $(l, a) = 1$. 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 $a_1, \ldots, a_m \geq 2$, defines sequences $\{s_j\}$, $\{q_j\}$ by

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

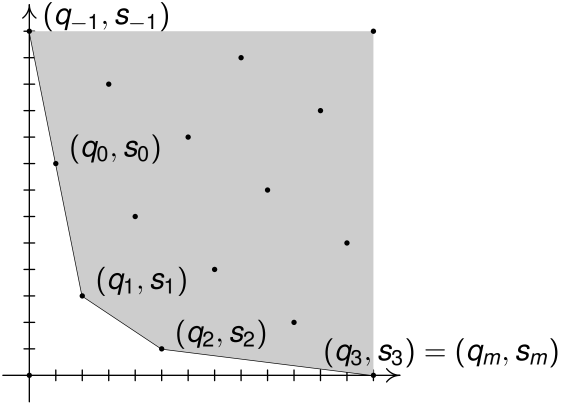
These sequences are closely connected with the lattice

$$\Lambda_l = \{(x, y) : lx \equiv y \pmod{a}\}.$$

General idea
Reduced regular continued fraction

$$\Lambda_l = \{(b, c) : 8b \equiv c \pmod{13}\}$$

$$\frac{a}{l} = \frac{13}{8} = 2 - \cfrac{1}{3 - \cfrac{1}{3}}$$



General idea

Reduced regular continued fraction

- Vectors $e_n = (q_n, s_n)$ and $e_{n-1} = (q_{n-1}, s_{n-1})$ form a basis of the lattice Λ_l.
- Points (q_n, s_n) are vertices of a convex hull of the set $\{(x, y) \in \Lambda_l \setminus \{0\} : x, y \geq 0\}$.
- $$\det\begin{pmatrix} q_n & s_n \\ q_{n-1} & s_{n-1} \end{pmatrix} = a$$

  and 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 $0 \leq x_2 < x_1$, $0 \leq y_2 < y_1$, $(x_1, x_2) = (y_1, y_2) = 1$:

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

General idea

Reduced regular continued fraction

- Vectors $e_n = (q_n, s_n)$ and $e_{n-1} = (q_{n-1}, s_{n-1})$ form a basis of the lattice Λ_l.
- Points (q_n, s_n) are vertices of a convex hull of the set $\{(x, y) \in \Lambda_l \setminus \{0\} : x, y \geq 0\}$.
- $$\det\begin{pmatrix} q_n & s_n \\ q_{n-1} & s_{n-1} \end{pmatrix} = a$$

  and 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 $0 \leq x_2 < x_1$, $0 \leq y_2 < y_1$, $(x_1, x_2) = (y_1, y_2) = 1$:

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

- Vectors $e_n = (q_n, s_n)$ and $e_{n-1} = (q_{n-1}, s_{n-1})$ form a basis of the lattice Λ_l.
- Points (q_n, s_n) are vertices of a convex hull of the set $\{(x, y) \in \Lambda_l \setminus \{0\} : x, y \geq 0\}$.
- $$\det\begin{pmatrix} q_n & s_n \\ q_{n-1} & s_{n-1} \end{pmatrix} = a$$

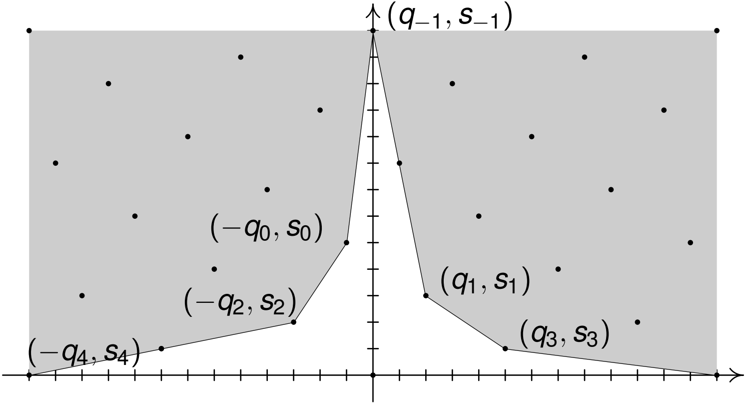
  and we have one-to-one correspondence between the set of quadruples $(q_n, s_n, q_{n-1}, s_{n-1})$ (taken for all lattices Λ_l) and the solutions of the equation

  $$x_1 y_1 - x_2 y_2 = a$$

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

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

$$\Lambda_l = \{(b,c) : 8b \equiv c \pmod{13}\},\ \frac{a}{l} = \frac{13}{5} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{2}}}$$



General idea
Kloosterman sums

The sequences arising from classical continued fractions give parameterization for the equation $x_1 y_1 + x_2 y_2 = a$.

The sequences arising from classical continued fractions give parameterization for the equation $x_1y_1 + x_2y_2 = a$.
From both equations

$$x_1y_1 \pm x_2y_2 = a$$

it follows that

$$x_1y_1 \equiv a \pmod{x_2},$$

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.

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

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

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 $P_1 < x \leq P_2$, $0 < y \leq f(x)$:

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

General idea

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

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

and $a = (l, q)$.

Classical Euclidean algorithm
Expectation

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

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

Classical Euclidean algorithm
Expectation

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

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

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

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

Asymptotic formula for the variance

$$D(R) = \frac{2}{R(R+1)} \sum_{b \le R} \sum_{a \le b} (s(c/d) - E(R))^2 .$$

is also known (Hensley 1994, Baladi and Vallée 2005)

$$D(R) = D_1 \cdot \log R + D_0 + O(R^{-\beta}),$$

where $\beta > 0$ and D_1 is Hensley's constant.
Application of Kloosterman sums lead to the better error term.

Asymptotic formula for the variance

$$D(R) = \frac{2}{R(R+1)} \sum_{b \le R} \sum_{a \le b} (s(c/d) - E(R))^2 .$$

is also known (Hensley 1994, Baladi and Vallée 2005)

$$D(R) = D_1 \cdot \log R + D_0 + O(R^{-\beta}),$$

where $\beta > 0$ and D_1 is Hensley's constant.
Application of Kloosterman sums lead to the better error term.

Theorem (A.U., 2008)

For $R \geq 2$

$$D(R) = D_1 \cdot \log R + D_0 + O(R^{-1/4+\varepsilon}).$$

This result gives new formulae for D_1 and D_0 in terms of complicated singular series.

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.

For $x \in [0, 1]$ and rational number $a/b = [0; a_1, \ldots, a_s]$ **Gauss — Kuz'min statistics** $s_x(a/b)$ can be defined in the following way: $s_x(a/b) = \left|\{j : 1 \le j \le s, [0; a_j, \ldots, a_s] \le x\}\right|$. In particular $s_1(a/b) = s(a/b)$ is the length of continued fraction for a/b.

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.

For $x \in [0, 1]$ and rational number $a/b = [0; a_1, \ldots, a_s]$ **Gauss — Kuz'min statistics** $s_x(a/b)$ can be defined in the following way: $s_x(a/b) = \left|\{j : 1 \leq j \leq s, [0; a_j, \ldots, a_s] \leq x\}\right|$. In particular $s_1(a/b) = s(a/b)$ is the length of continued fraction for a/b.

Theorem (A.U., 2005)

For any region Ω with "good" boundary

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

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:

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

centered division:

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

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 $g(a, b) = 7$:

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

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

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

Example

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

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

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 $n \geq 3$.

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 $d \mid a$, $d \mid b$

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

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 $N \to \infty$.

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 $N\to\infty$.

Conjecture (Arnold, 1999, 2005)

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

Frobenius numbers

Burgeĭn 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.

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:

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

Frobenius numbers
Density function

Theorem (A.U., 2010)

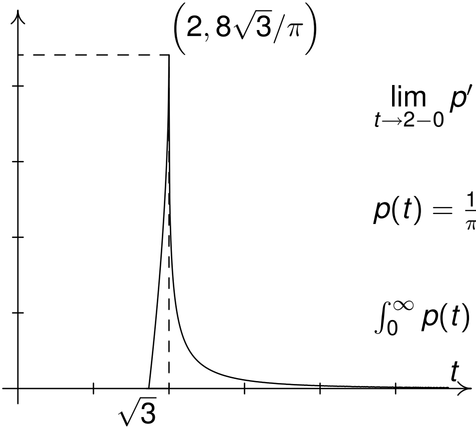
Normalized Frobenius numbers of three arguments have limiting density function:

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

where

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

Frobenius numbers
Density function



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

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

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

These results are based on Rödseth formula for positive Frobenius numbers (1978).
We want to find $f(a, b, c)$ for $(a, b) = (a, c) = (b, c) = 1$.

These results are based on Rödseth formula for positive Frobenius numbers (1978).

We want to find $f(a, b, c)$ for $(a, b) = (a, c) = (b, c) = 1$. Let l is such that

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

These results are based on Rödseth formula for positive Frobenius numbers (1978).
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

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

From obvious property

$$0 = \frac{s_m}{q_m} < \frac{s_{m-1}}{q_{m-1}} < \ldots < \frac{s_0}{q_0} < \frac{s_{-1}}{q_{-1}} = \infty$$

follows that for some n

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

From obvious property

$$0 = \frac{s_m}{q_m} < \frac{s_{m-1}}{q_{m-1}} < \ldots < \frac{s_0}{q_0} < \frac{s_{-1}}{q_{-1}} = \infty$$

follows that for some n

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

Then we have Rödseth formula for positive Frobenius numbers:

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

From obvious property

$$0 = \frac{s_m}{q_m} < \frac{s_{m-1}}{q_{m-1}} < \ldots < \frac{s_0}{q_0} < \frac{s_{-1}}{q_{-1}} = \infty$$

follows that for some n

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

Then we have Rödseth formula for positive Frobenius numbers:

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

The existence of limiting distribution for normalized Frobenius numbers of arbitrary number of arguments was proved by Marklof (2010).

Reduced bases in two-dimensional lattices

Reduced bases are important in different number theory algorithms (fast point multiplication on elliptic curves, prediction of pseudo random generators, numerical integration, ...). Work of these algorithms depends on properties of reduced basis (shorter vectors are better).

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 $\Lambda_l = \{(x, y) : lx \equiv y \pmod{a}\}$.

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

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

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:

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

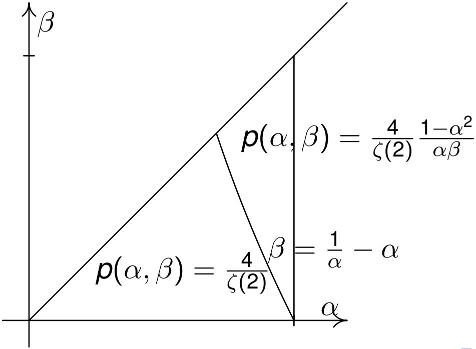
$$p(\alpha,\beta) = \frac{4}{\zeta(2)} \min\left\{1, \frac{1-\alpha^2}{\alpha\beta}\right\} \qquad (0 \le \beta \le \alpha \le 1).$$

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

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 $t = \|e_2\|/\sqrt{a}$:

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

Reduced bases in two-dimensional lattices

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

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