Kloosterman Sums and Continued Fractions

Alexey Ustinov
Russian Academy of Sciences
Institute of Applied Mathematics, Khabarovsk

General idea

Let $1 \leqslant l \leqslant a$, $(l,a)=1$, and $\Lambda_l = \{(x,y) : lx \equiv y \pmod a\}$. Reduced regular continued fraction

$$\frac{a}{l} = \langle a_0; a_1, \dots, a_m\rangle = a_1 - \cfrac{1}{a_2 - \cfrac{}{\ddots - \cfrac{1}{a_m}}},$$

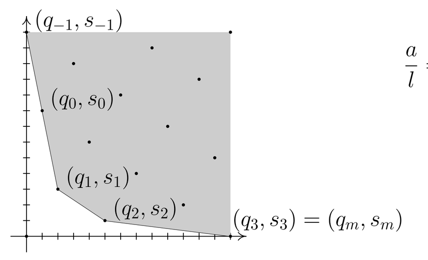
where $a_1 = \lceil a/l \rceil = -\lfloor -a/l \rfloor$, $a_2, \dots, a_m \geqslant 2$, defines sequences $\{s_j\}$, $\{q_j\}$ by

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

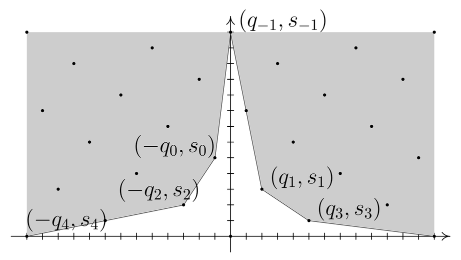
1°. Vectors $e_m = (q_m, s_m)$ and $e_{m-1} = (q_{m-1}, s_{m-1})$ form a basis of the lattice Λ_l.
2°. Points (q_n, s_n) are vertices of a convex hull of the set $\{(x,y) \in \Lambda_l \setminus \{0\} : x, y \geqslant 0\}$ (left picture).
3°. There is one-to-one correspondence between the set of quadruples $(q_n, s_n, q_{n-1}, s_{n-1})$ (taken for all lattices Λ_l) and the solutions of the equation $x_1y_1 - x_2y_2 = a$ with $0 \leqslant x_2 < x_1$, $0 \leqslant y_2 < y_1$, $(x_1, x_2) = (y_1, y_2) = 1$: $(q_n, s_n, q_{n-1}, s_{n-1}) \longleftrightarrow (x_1, x_2, y_2, y_1)$.
This observation allows to transform different problems concerned with continued fractions or integer lattices to the investigation of solutions of $x_1y_1 - x_2y_2 = a$ with additional restrictions.

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

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



$$\frac{a}{l} = \frac{13}{5} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}}$$



The same arguments lead from classical continued fractions to the equation $x_1y_1 + x_2y_2 = a$ (right picture).
From equation $x_1y_1 \pm x_2y_2 = a$ it follows that $x_1y_1 \equiv a \pmod{x_2}$, and Kloosterman sums

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

come into play. Solutions of the congruence $xy \equiv l \pmod q$ are uniformly distributed due to the generalized Estermann bound (see [4])

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

A combination of this estimate with van der Corput's method of exponential sums leads to the following results.

Classical Euclidean algorithm

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

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

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

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

Later (1975) Porter has shown that

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

where

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

now is known as Porter's constant. 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 1 (see [1]) *Let $R \geqslant 2$. Then*

$$E(R) = \frac{2}{R(R+1)} \sum_{b \leqslant R} \sum_{a \leqslant b} s(a/b) = \frac{2\log 2}{\zeta(2)} \log R + \widetilde{C}_P + O(R^{-1+\varepsilon}), \tag{3}$$

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

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

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 and new formula for Hensley's constant.

Theorem 2 (see [1]) *For $R \geqslant 2$*

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

Both constants D_1 and D_0 can be written in terms of complicated singular series.

Theorem 3 (see [2])

$$\frac{1}{\varphi(b)} \sum_{\substack{1 \leqslant a \leqslant b\\ (a,b)=1}} s(a/b) = \frac{2\log 2}{\zeta(2)} \log b + C_P + O(b^{-5/24+\varepsilon}).$$

[1] USTINOV A. V. Asymptotic behavior of the first and second moments for the number of steps in the Euclidean algorithm — *Izv. Ross. Akad. Nauk Ser. Mat.*, **72** (2008), 189–224.
[2] BYKOVSKII V. A., USTINOV A. V. An improvement of Porter's result on average length of finite continued fraction (in preparation).

Gauss — Kuz'min statistics

Conjecture 1 (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 (1) Gauss — Kuz'min statistics $s_x(a/b)$ can be defined in the following way: $s_x(a/b) = |\{j : 1 \leqslant j \leqslant s, [0; a_j, \dots, a_s] \leqslant x\}|$. In particular $s_1(a/b) = s(a/b)$ is the length of continued fraction (1).

Theorem 4 (see [3]) *For a region Ω with "good" boundary*

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

Moreover formulae (2)–(3) can be generalized to the case of Gauss — Kuz'min statistics.

Theorem 5 (see [4])

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

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

where

$$C_P(x) = \frac{2\log(1+x)}{\zeta(2)} \left(2\gamma - 2\frac{\zeta'(2)}{\zeta(2)} - \frac{\log(1+x)}{2} + \log x - 1 \right) + \frac{2}{\zeta(2)}(h_1(x) + h_2(x)) + \frac{x^2}{x+1}, \tag{4}$$

$$\widetilde{C}_P(x) = C_P(x) + \frac{2\log(1+x)}{\zeta(2)} \left(\frac{\zeta'(2)}{\zeta(2)} - \frac{1}{2} \right), \tag{5}$$

and $h_1(x)$, $h_2(x)$ are defined by singular series

$$h_1(x) = \sum_{n=1}^{\infty} \frac{1}{n} \left(\sum_{m=1}^{n} \frac{x}{n+mx} - \log(1+x) \right), \qquad h_2(x) = \sum_{n=1}^{\infty} \frac{1}{n} \left(\sum_{\frac{n}{x} \leqslant m < \frac{n}{x}+n} \frac{1}{m} - \log(1+x) \right).$$

[3] USTINOV A. V. On the Gauss-Kuz'min statistics for finite continued fractions — *Fundam. Prikl. Mat.*, 11 (2005), 195–208.
[4] USTINOV A. V. On the number of solutions of the congruence $xy \equiv l \pmod q$ under the graph of a twice continuously differentiable function — *Algebra i Analiz*, **20** (2008), 186–216.

Fast Euclidean algorithms

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

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

centered division

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

and odd division

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

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

Theorem 6 (see [5,6]) *Let $b \geqslant 1$, $1 \leqslant a < b$, $(a,b) = 1$, $\varphi = \frac{1+\sqrt{5}}{2}$. Then*

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

Moreover, if $b/2 \leqslant a$, $aa^\star \equiv 1 \pmod b$, $1 \leqslant a^\star < b$ then

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

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

$$s_x(a/b) = |\{(j,t) : 0 \leqslant j \leqslant s, 0 \leqslant t < a_j, [t; a_{j+1}, \dots, a_s, 1] \leqslant x\}| \qquad (a_0 = +\infty).$$

Theorem 6 implies theorems 7, 8. They improve result of Baladi and Vallée (2005) on the average value of $l(a/b)$ and $h(a/b)$.

Theorem 7 (see [5]) *We have*

$$\frac{1}{\varphi(b)} \sum_{\substack{a=1\\ (a,b)=1}}^{b} l(a/b) = \frac{2\log\varphi}{\zeta(2)} \log b + C_l + O(b^{-1/6+\varepsilon}), \qquad \frac{2}{R(R+1)} \sum_{b \leqslant R} \sum_{a=1}^{b} l(a/b) = \frac{2\log\varphi}{\zeta(2)} \log R + \widetilde{C}_l + O(R^{-1+\varepsilon}),$$

where $C_l = C_P(\varphi - 1)$, $\widetilde{C}_l = \widetilde{C}_P(\varphi - 1)$, and function $C_P(x)$, $\widetilde{C}_P(x)$ are defined by (4) *and* (5).

Theorem 8 (see [6]) *We have*

$$\frac{1}{\varphi(b)} \sum_{\substack{a=1\\ (a,b)=1}}^{b} h(a/b) = \frac{3\log\varphi}{\zeta(2)} \log b + C_h + O(b^{-1/6+\varepsilon}), \qquad \frac{2}{R(R+1)} \sum_{b \leqslant R} \sum_{a=1}^{b} h(a/b) = \frac{3\log\varphi}{\zeta(2)} \log R + \widetilde{C}_h + O(R^{-1+\varepsilon}),$$

where $C_h = \frac{1}{2}(C_P(\varphi) + C_P(\varphi - 1))$, $\widetilde{C}_h = \frac{1}{2}(\widetilde{C}_P(\varphi) + \widetilde{C}_P(\varphi - 1))$, and function $C_P(x)$, $\widetilde{C}_P(x)$ are defined by (4) *and* (5).

[5] USTINOV A. V. On the average number of steps in the least-remainder Euclidean algorithm — *Mat. Zametki*, 85 (2009), 153–156.
[6] USTINOV A. V. On the average number of steps in the Euclidean algorithm with odd partial quotients — *Mat. Zametki*, (to appear).

Frobenius numbers

Let a, b, c be three positive integers with $(a,b,c) = 1$. It is well-known that all sufficiently large integers are representable as positive linear combinations of a, b, c. Consider $f(a,b,c)$, 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. Then $g(a,b,c) = f(a,b,c) - a - b - c$ is the usual *Frobenius number*, that is, the largest integer not representable as a non-negative linear combination a, b, c.
Conjecture 2 (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 3 (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 $c_n > 0$.
Let x_1, $x_2 > 0$ and $M_a(x_1, x_2) = \{(b,c) : 1 \leqslant b \leqslant x_1 a, 1 \leqslant c \leqslant x_2 a, (a,b,c) = 1\}$.

Theorem 9 (see [7]) *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 10 (see [8]) *Normalized Frobenius numbers of three arguments have limiting density function:*

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

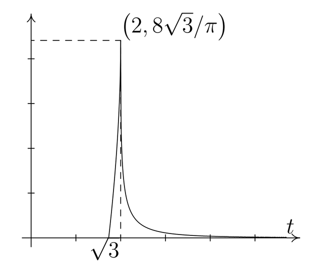
where

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

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

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

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



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

[7] USTINOV A. V. Solution of the Arnol'd problem on weak asymptotics for Frobenius numbers with three arguments — *Mat. Sb.*, **200** (2009) 131–160.
[8] USTINOV A. V. On the distribution of Frobenius numbers — *Izvestiya: Mathematics*, **74**: 5 (2010) 145–170.

Reduced bases in two-dimensional lattices

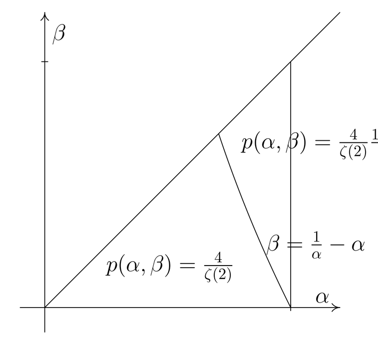
Reduced bases are important in different number theory algorithms (fast point multiplication on elliptic curves, prediction of pseudo random generators, numerical integration, ...). Work of these algorithms depends on properties of reduced basis (shorter vectors are better).
Let $1 \leqslant l \leqslant a$, $(l,a) = 1$ 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

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

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 $e_1 = \sqrt{a}(\alpha, \beta)$, $e_2 = \sqrt{a}(\gamma, \delta)$.
For example in the case of the most popular $\|\cdot\|_\infty$-norm integration over e_2 lead to the density function for e_1:

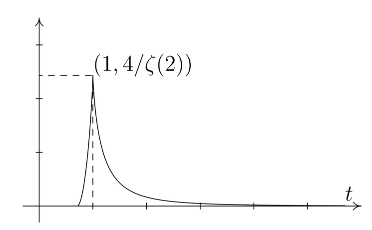
$$p(\alpha, \beta) = p(\pm\alpha, \pm\beta) = p(\beta, \alpha)$$

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



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

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



[9] USTINOV A. V. Distribution of reduced bases in two-dimensional integer lattices — (in preparation).

Conclusions

This approach combines elementary observations, methods from geometry of numbers and analytic number theory. It gives an effective tool for studying continued fractions and lattice point problems. More applications can be found in the following articles.

[10] BYKOVSKII V. A., USTINOV A. V. The statistics of particle trajectories in the inhomogeneous Sinai problem for a two-dimensional lattice — *Izv. RAN. Ser. Mat.*, **73**: 4 (2009) 17–36.
[11] SHCHUR V., SINAI, Y., USTINOV A. Limiting distribution of Frobenius numbers for $n = 3$ — *Journal of Number Theory*, **129** (2009), 2778–2789.
[12] USTINOV A. V. On the distribution of integer points — *Far Eastern Mathematical Journal*, **9**:1–2 (2009) 176–181.

http://iam.khv.ru/staff/Ustinov.htm
ustinov@iam.khv.ru