Distribution of Frobenius Numbers

Alexey Ustinov

Pacific National University,
Institute of Applied Mathematics (Khabarovsk),
Russian Academy of Sciences

July 5, 2016

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 $g(a_1, \ldots, a_n)$ when $n \geq 3$.

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 $g(a_1, \dots, a_n)$ when $n \geq 3$.

Example

$g(3, 5, 7) = 4$:

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

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

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

Double loop network

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

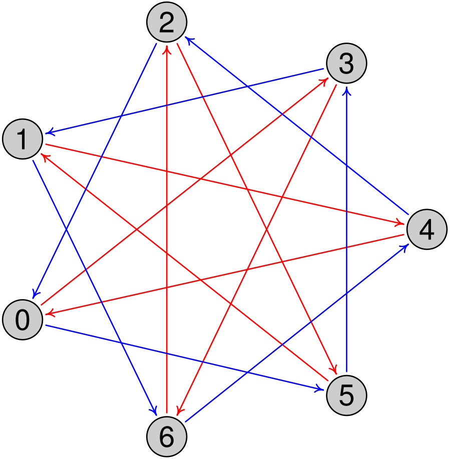
length(↑)$= 3$,   length(↑)$= 5$

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

5	8	11	
0	3	6	9

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

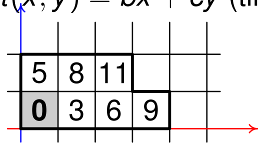
5	1	4	
0	3	6	2



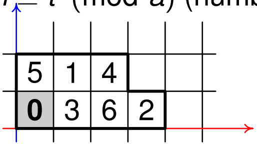
Double loop network

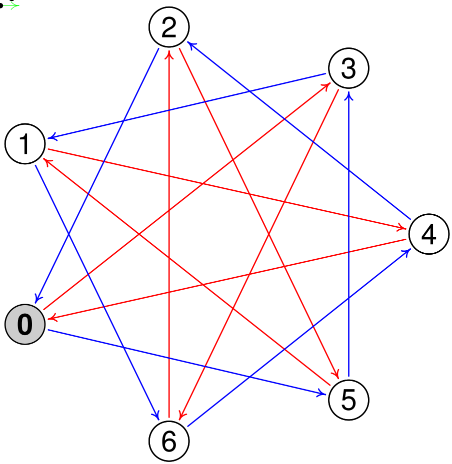
$b = 3$ (red step), $c = 5$ (blue step), $a = 7$ (number of vertices)

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



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

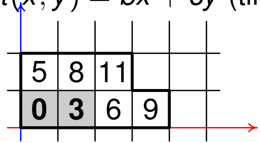




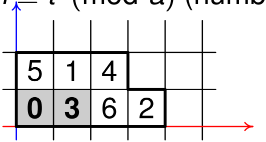
Double loop network

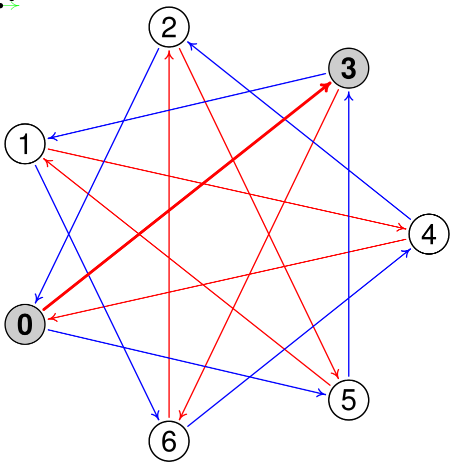
$b = 3$ (red step), $c = 5$ (blue step), $a = 7$ (number of vertices)

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



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





Double loop network

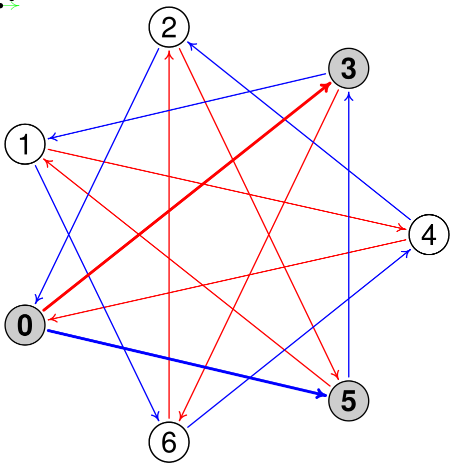
$b = 3$ (red step), $c = 5$ (blue step), $a = 7$ (number of vertices)

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

5	8	11	
0	**3**	6	9

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

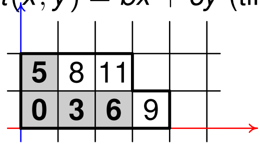
5	1	4	
0	**3**	6	2



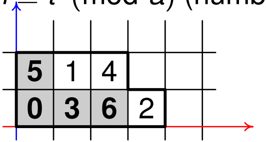
Double loop network

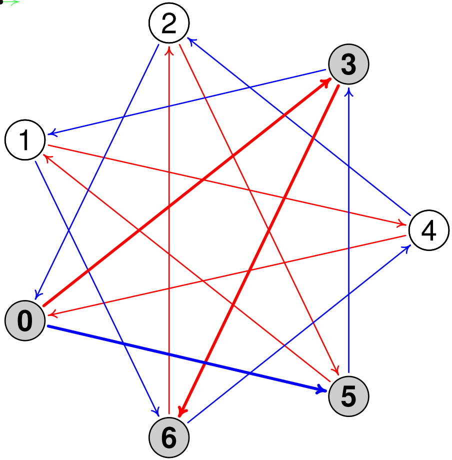
$b = 3$ (red step), $c = 5$ (blue step), $a = 7$ (number of vertices)

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



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

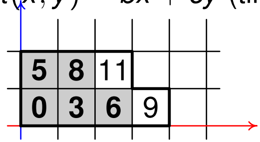




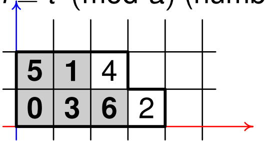
Double loop network

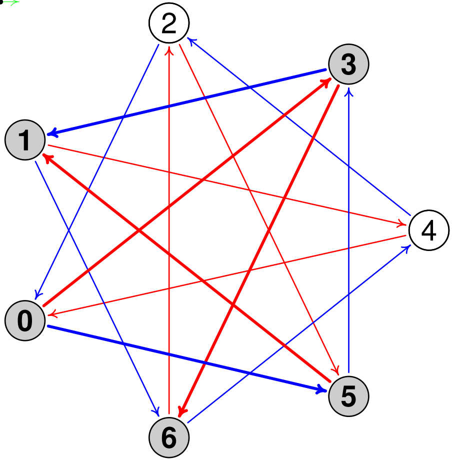
$b = 3$ (red step), $c = 5$ (blue step), $a = 7$ (number of vertices)

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



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

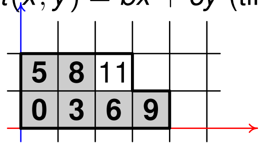




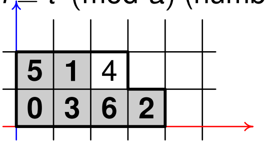
Double loop network

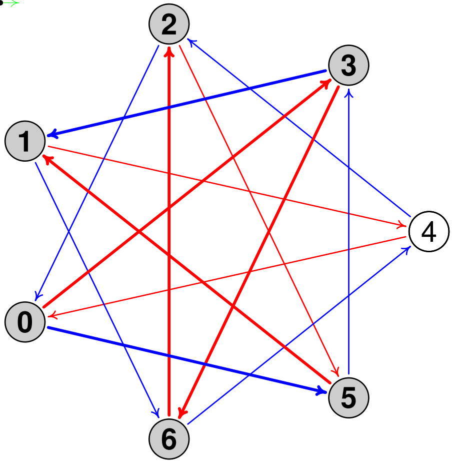
$b = 3$ (red step), $c = 5$ (blue step), $a = 7$ (number of vertices)

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



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

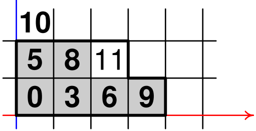




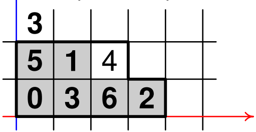
Double loop network

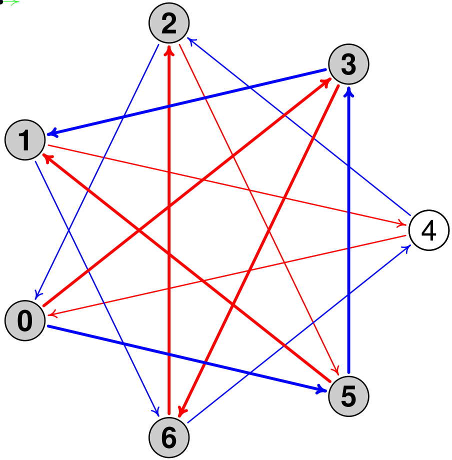
$b = 3$ (red step), $c = 5$ (blue step), $a = 7$ (number of vertices)

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



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

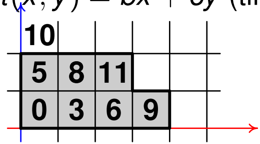




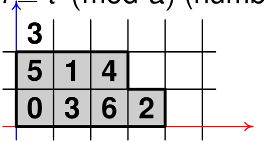
Double loop network

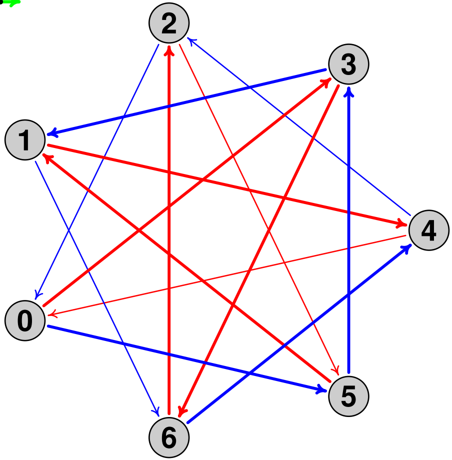
$b = 3$ (red step), $c = 5$ (blue step), $a = 7$ (number of vertices)

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



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



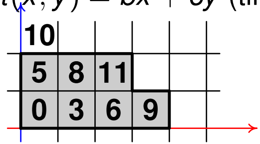


Double loop network

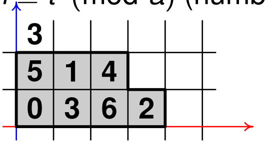
$b = 3$ (red step), $c = 5$ (blue step), $a = 7$ (number of vertices)

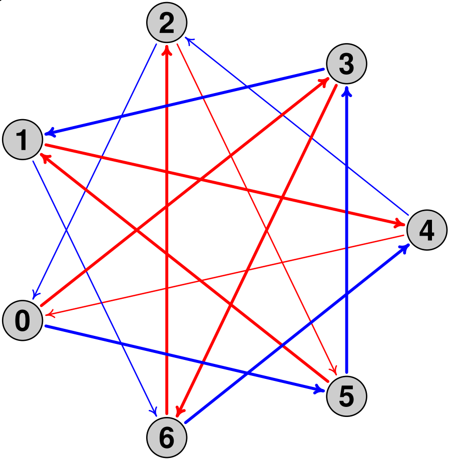
$$\mathrm{diam} = g(a, b, c) + a \quad (= 11)$$

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



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

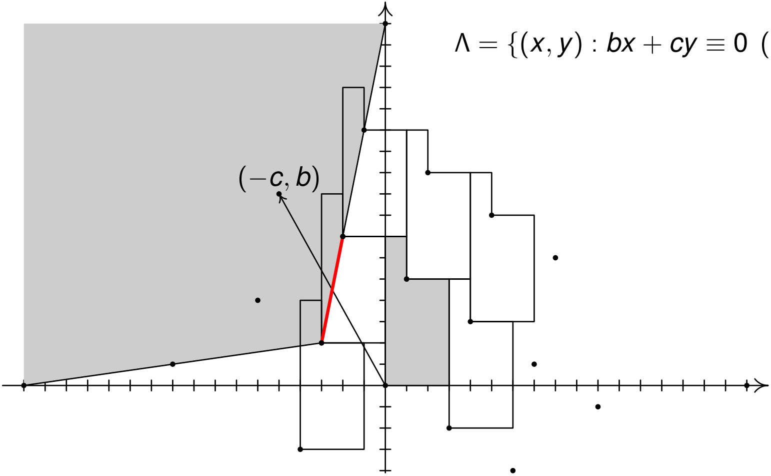




Double loop network

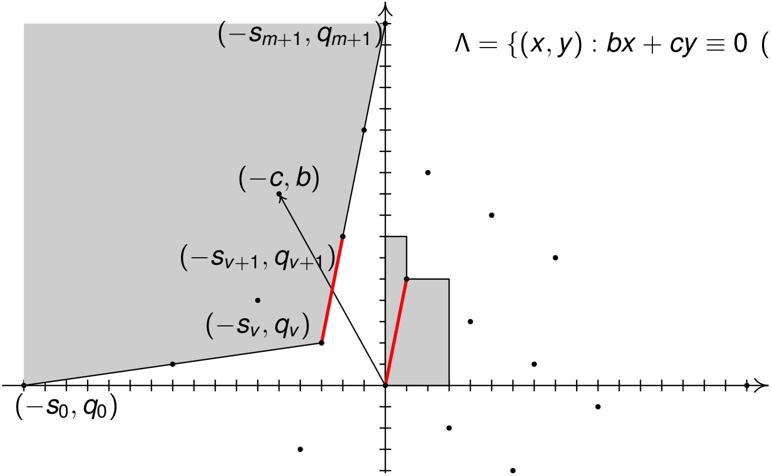
$b = 9$ (red step), $c = 5$ (blue step), $a = 17$ (number of vertices)

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



Double loop network

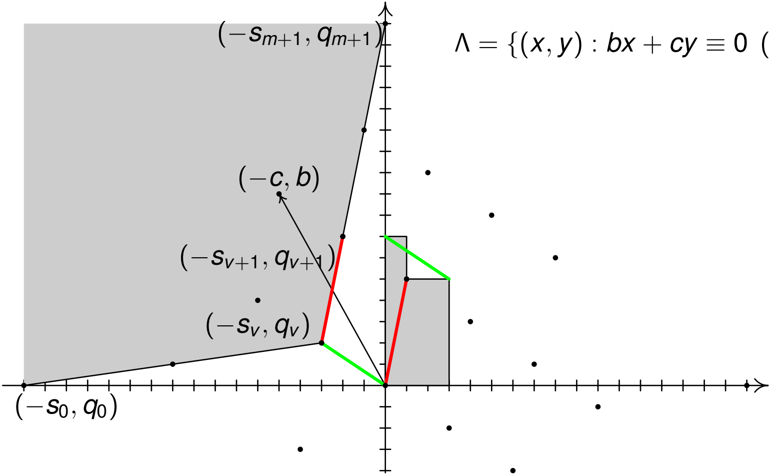
$b = 9$ (red step), $c = 5$ (blue step), $a = 17$ (number of vertices)



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

Double loop network

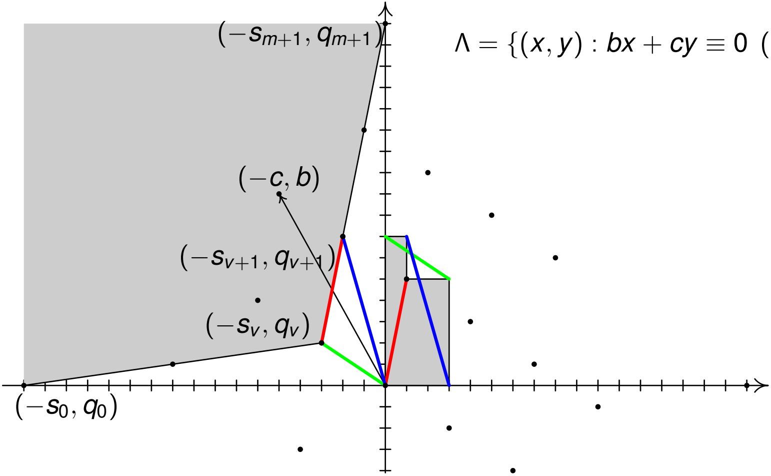
$b = 9$ (red step), $c = 5$ (blue step), $a = 17$ (number of vertices)



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

Double loop network

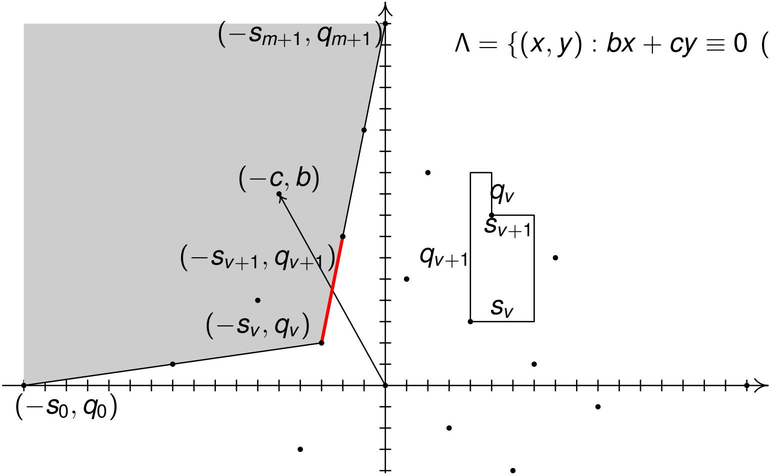
$b = 9$ (red step), $c = 5$ (blue step), $a = 17$ (number of vertices)



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

Double loop network

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



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

Rödseth's formula

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

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

Rödseth's formula

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

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

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

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 sequences $\{s_j\}$, $\{q_j\}$ by

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

General idea

Reduced regular continued fraction

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 $f(a,b,c)$.

Conjectures

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 $N \to \infty$.

Conjectures

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 $c_n > 0$.

Limiting density function

Theorem (Bourgain and Sinaĭ, 2007)

Normalized Frobenius numbers $\frac{f(a,b,c)}{\sqrt{abc}}$ *(under some natural assumption) have limiting density function.*

Weak asymptotic

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

Weak asymptotic

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

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:

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

Density function

Theorem (A.U., 2010)

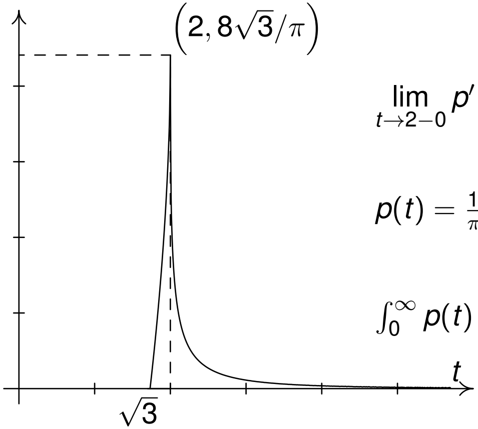
Normalized Frobenius numbers of three arguments have limiting density function:

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

where

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

Density function



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

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

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

Density function

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

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

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

Weak asymptotic for genus

Let

$$n(a,b,c) = \#(\mathbb{N} \setminus \langle a,b,c\rangle)$$

be a genus of numerical semigroup $\langle a,b,c\rangle$ and let $N(a,b,c)$ let be modified genus:

$$N(a,b,c) = n(a,b,c) + \frac{a}{2} + \frac{b}{2} + \frac{c}{2} - \frac{1}{2}.$$

It is more convenient because for $d \mid a$, $d \mid b$ we have

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

Theorem (Vorob'ev, 2016)

$$N(a,b,c) \approx \frac{64}{5\pi^2}\sqrt{abc}.$$

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 $K_q(l,m,n)$.

General idea

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

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

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

Theorem (A.U., 2008)

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

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).
- Aliev, Henk, Hinrichs (2011) and Strömbergsson(2012) studied the properties of limiting distribution for normalized Frobenius numbers of arbitrary number of arguments.

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).
- Aliev, Henk, Hinrichs (2011) and Strömbergsson(2012) studied the properties of limiting distribution for normalized Frobenius numbers of arbitrary number of arguments.

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).
- Aliev, Henk, Hinrichs (2011) and Strömbergsson(2012) studied the properties of limiting distribution for normalized Frobenius numbers of arbitrary number of arguments.

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).
- Aliev, Henk, Hinrichs (2011) and Strömbergsson(2012) studied the properties of limiting distribution for normalized Frobenius numbers of arbitrary number of arguments.

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 $1 \le l \le a$, $(l, a) = 1$ 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 $\det(e_1, e_2) = a$.

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 $\|e_2\|^{-1}$. Suppose $e_1 = \sqrt{a}(\alpha, \beta)$, $e_2 = \sqrt{a}(\gamma, \delta)$.

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

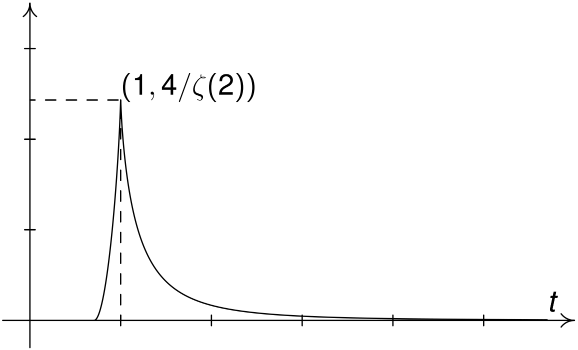
By integrating over e_1 we can get density function for $t = \|e_2\|/\sqrt{a}$:

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

Reduced bases in two-dimensional lattices

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

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



Aliev I., Henk M., Hinrichs A., “Expected Frobenius numbers” — Journal of Combinatorial Theory, Series A 118 (2), 525-531.

Bourgain J., Sinai Ya. G. “Limit behaviour of large Frobenius numbers.” — Uspekhi Mat. Nauk, 62:4(376) (2007), 7790.

Marklof J. “The asymptotic distribution of Frobenius numbers.” — Invent. Math., 2010, 181, 179-207.

Marklof J., Strömbergsson A. “Diameters of random circulant graphs.” — Combinatorica, 33: 4 (2013), 429-466.

Strömbergsson A. On the limit distribution of Frobenius numbers. Acta Arith., Polish Academy of Sciences (Polska Akademia Nauk - PAN), Institute of Mathematics (Instytut Matematyczny), Warsaw, 2012, 152, 81-107

Ustinov A. V. “Solution of the Arnolrime d problem on weak asymptotics for Frobenius numbers with three arguments.” — Mat. Sb., 2009, 200, 131-160.

Ustinov A. V. “On the distribution of Frobenius numbers with three arguments.” — Izvestiya: Mathematics, 2010, 74, 1023-1049.

Vorob’ev I. S. “On the Frobenius problem in case of three arguments.” — Mat. Sb., 207:6 (2016), 5378.

Questione?