# The linear Diophantine problem of Frobenius

**Matthias Beck**

**SUNY Binghamton**

www.math.binghamton.edu/matthias

Joint work with

- Ricardo Diaz, University of Northern Colorado
- Ira Gessel, Brandeis University
- Takao Komatsu, Mie University (Japan)
- Sinai Robins, Temple University
- Shelemyahu Zacks, SUNY Binghamton

"If you think it's simple, then you have misunderstood the problem"

Bjarne Strustrup
(lecture at Temple University, 11/25/97)

Frobenius problem: Given relatively prime positive integers $a_1, \ldots, a_d$ , we call an integer $n$ representable if there exist nonnegative integers $m_1, \ldots, m_d$ such that

$$n = m_1 a_1 + \cdots + m_d a_d \ .$$

Find the largest integer (the Frobenius number $g(a_1, \ldots, a_d)$ ) which is not representable.

We study the (restricted) partition function

$$p_{\{a_1,\ldots,a_d\}}(n) = \# \left\{ \begin{array}{l} (m_1, \ldots, m_d) \in \mathbb{Z}^d_{\geq 0} \ : \\ m_1 a_1 + \cdots + m_d a_d = n \end{array} \right\}$$

Frobenius problem: find the largest value for $n$ such that $p_{\{a_1,\ldots,a_d\}}(n) = 0$.

- (Sylvester, 1884)

$$g(a_1, a_2) = a_1 a_2 - a_1 - a_2$$

- (Pólya–Szegő, 1925, ...)

$$p_{\{a_1,\ldots,a_d\}}(n) = \frac{n^{d-1}}{a_1 \cdots a_d (d-1)!} + O\left(n^{d-2}\right)$$

- (Erdős–Graham, 1972)

$$g(a_1, \ldots, a_n) \leq 2a_n \left\lfloor \frac{a_1}{n} \right\rfloor - a_1$$

- (Vitek, 1975)

$$g(a_1, \ldots, a_n) \leq \left\lfloor \frac{1}{2}(a_2 - 1)(a_n - 2) \right\rfloor - 1$$

- (Selmer, 1977)

$$g(a_1, \ldots, a_n) \leq 2a_{n-1} \left\lfloor \frac{a_n}{n} \right\rfloor - a_n$$

- (Kannan, 1992) $g(a_1, \ldots, a_n)$ is polynomial-time computable in the input length of $a_1, \ldots, a_n$.

Theorem (Sertöz, Tripathi, Robins–B)
If $a_1$ and $a_2$ are relatively prime then

$$p_{\{a_1,a_2\}}(n) = \frac{n}{a_1 a_2} - \left\{ \frac{a_2^{-1} n}{a_1} \right\} - \left\{ \frac{a_1^{-1} n}{a_2} \right\} + 1 \, .$$

Here $\{x\} = x - \lfloor x \rfloor$ denotes the fractional part of $x$,

$$a_1^{-1} a_1 \equiv 1 \pmod{a_2} \, ,$$

and

$$a_2^{-1} a_2 \equiv 1 \pmod{a_1} \, .$$

Corollary (Sylvester?)
$g(a_1, a_2) = a_1 a_2 - a_1 - a_2$

Corollary (Sylvester)
Exactly half of the integers between 1 and $(a_1 - 1)(a_2 - 1)$ are representable.

Extension: $n$ is called $k$-representable if

$$p_{\{a_1,\dots,a_d\}}(n) = k\ ,$$

that is, $n$ can be represented in exactly $k$ ways. Define $g_k(a_1,\dots,a_d)$ to be the largest $k$-representable integer.

Theorem (Robins–B)
$g_k(a_1,a_2) = (k+1)a_1a_2 - a_1 - a_2$

This follows directly from

$$p_{\{a_1,a_2\}}(n + a_1a_2) = p_{\{a_1,a_2\}}(n) + 1\ .$$

Dilate the rational polytope $\mathcal{P} \subset \mathbb{R}^d$ by a positive integer $n$:

$$n\mathcal{P} = \{nx : x \in \mathcal{P}\}$$

and count the number of integer points ("lattice points") in $n\mathcal{P}$ :

$$L_{\mathcal{P}}(n) = \# \left( n\mathcal{P} \cap \mathbb{Z}^d \right) .$$

A quasipolynomial is an expression

$$c_m(n)\, n^m + \cdots + c_1(n)\, n + c_0(n) ,$$

where $c_0, \dots, c_m$ are periodic functions in $n$

Theorem (Ehrhart, 1960's)
$L_{\mathcal{P}}(n)$ is a quasipolynomial in $n$ whose degree is the dimension of $\mathcal{P}$. The period of this quasipolynomial divides any common multiple of the denominators of the vertices of $\mathcal{P}$.

$$L^{\star}_{\mathcal{P}}(n) = \#\left(n\mathcal{P}^{\mathrm{int}} \cap \mathbb{Z}^d\right)$$

Theorem (Ehrhart, Macdonald, ∼1970)
If $\mathcal{P}$ is homeomorphic to a $d$-sphere then

$$L_{\mathcal{P}}(-n) = (-1)^d L^{\star}_{\mathcal{P}}(n)\ .$$

Let $A = \{a_1, \ldots, a_d\}$, then $p_A(n) = L_{\mathcal{P}}(n)$ where

$$\mathcal{P} = \left\{ \begin{array}{l} (x_1, \ldots, x_d) \in \mathbb{R}^d : \\ x_j \geq 0, \ x_1 a_1 + \cdots + x_d a_d = 1 \end{array} \right\} .$$

Hence $p_A(n)$ is a quasipolynomial in $n$ of degree $n-1$ and period $\operatorname{lcm}(a_1, \ldots, a_d)$.

$$\mathcal{P}^{\text{int}} = \left\{ \begin{array}{l} (x_1, \ldots, x_d) \in \mathbb{R}^d : \\ x_j > 0, \ x_1 a_1 + \cdots + x_d a_d = 1 \end{array} \right\} .$$

Note that

$$L^{\star}_{\mathcal{P}}(n) = 0$$

for $n = 1, \ldots, a_1 + \cdots + a_d - 1$ and

$$L^{\star}_{\mathcal{P}}(n) = L_{\mathcal{P}}(n - (a_1 + \cdots + a_d)) .$$

Corollary

$$p_A(n) = 0$$

for $n = -1, \ldots, -(a_1 + \cdots + a_d) + 1$.

$$p_A(-n) = (-1)^{d-1} p_A(n - (a_1 + \cdots + a_d))$$

$p_A(n)$ is the coefficient of $z^n$ in

$$\frac{1}{(1-z^{a_1})(1-z^{a_2})\cdots(1-z^{a_n})}\,,$$

equivalently,

$$p_A(n) = \operatorname{Res}_{z=0}\left(\frac{z^{-n-1}}{(1-z^{a_1})(1-z^{a_2})\cdots(1-z^{a_n})}\right)\,.$$

Write $p_A(n) = P_A(n) + Q_A(n)$, where $P_A(n)$ is a polynomial in $n$.

Define the Bernoulli numbers $B_j$ by

$$\frac{z}{e^z-1} = \sum_{j\geq 0} B_j\,\frac{z^j}{j!}$$

(so $B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_4 = -\frac{1}{30}$, and $B_j = 0$ if $j$ is odd and greater than 1.)
Let $s_j = a_1^j + \cdots + a_d^j$ .

Theorem (Gessel–Komatsu–B)

$$P_A(n) = \text{const}\left(-\frac{ze^{-nz}}{(1-e^{a_1 z})\cdots(1-e^{a_d z})}\right)$$

$$= \frac{1}{a_1\cdots a_d}\sum_{m=0}^{d-1}\frac{(-1)^m}{(d-1-m)!}$$

$$\times \sum_{k_1+\cdots+k_d=m} a_1^{k_1}\cdots a_d^{k_d}\frac{B_{k_1}\cdots B_{k_d}}{k_1!\cdots k_d!}n^{d-1-m}$$

For $c_1, \ldots, c_d \in \mathbb{Z}$ relatively prime to $c \in \mathbb{Z}$ and $n \in \mathbb{Z}$, define the Fourier-Dedekind sum

$$\sigma_n(c_1, \ldots, c_d; c) = \frac{1}{c} \sum_{\lambda^c = 1 \neq \lambda} \frac{\lambda^n}{(1-\lambda^{c_1}) \cdots (1-\lambda^{c_d})} .$$

Theorem (Diaz–Robins–B) If $a_1, \ldots, a_d$ are pairwise relatively prime then

$$p_A(n) = P_A(n) + \sum_{j=1}^{d} \sigma_{-n}(a_1, \ldots, \hat{a}_j, \ldots, a_d; a_j) .$$

Examples:

$$\sigma_n(1; c) = \left(\left(\frac{-n}{c}\right)\right) + \frac{1}{2c} ,$$

where $((x)) = x - \lfloor x \rfloor - 1/2$.

$$\sigma_n(a, b; c) = \sum_{m=0}^{c-1} \left(\left(\frac{-a^{-1}(bm+n)}{c}\right)\right) \left(\left(\frac{m}{c}\right)\right) - \frac{1}{4c} ,$$

a special case of the Dedekind-Rademacher sum.

Corollary

For pairwise relatively prime integers $a_1, \ldots, a_d$

$$\sum_{j=1}^{d} \sigma_0(a_1, \ldots, \hat{a}_j, \ldots, a_d; a_j) = 1 - P_A(0)$$

This statement is equivalent to Zagier's reciprocity law for his higher dimensional Dedekind sums

Corollary

Let $a_1, \ldots, a_n$ be pairwise relatively prime integers and $0 < n \le a_1 + \cdots + a_n$. Then

$$\sum_{j=1}^{d} \sigma_n(a_1, \ldots, \hat{a}_j, \ldots, a_d; a_j) = -P_A(n) \ .$$

Corollary

For pairwise relatively prime integers $a_1, \ldots, a_d$ $g(a_1, \ldots, a_d)$ is bounded from above by

$$\frac{1}{2}\left(\sqrt{a_1 a_2 a_3 (a_1 + a_2 + a_3)} - a_1 - a_2 - a_3\right) \ .$$

An admissible triple $(a, b, c)$ is a triple of pairwise relatively prime integers for which none of $a, b, c$ can be represented by the other two, and which do not form an almost arithmetic sequences.

Conjectures (Zachs–B)
There exists an upper bound for $g(a, b, c)$ proportional to $\sqrt{abc}^{p}$ where $p < \frac{4}{3}$, valid for all admissible triplets $(a, b, c)$.

For all admissible triplets $(a, b, c)$,

$$g(a, b, c) \leq \sqrt{abc}^{5/4} - a - b - c \; .$$

## Open problems

- Find a formula (?) for $g(a, b, c)$
- Find a polynomial-time algorithm for $g(a_1, \ldots, a_d)$
- Find formulas for $g_k(a_1, \ldots, a_d)$ for special cases of $a_1, \ldots, a_d$
- Find a formula (?) for $g_k(a, b, c)$