Frobenius Coin-Exchange Generating Functions

Leonardo Bardomero
Notre Dame Belmont

Matthias Beck
San Francisco State
Freie Universität Berlin

Amer. Math. Monthly
127 (2020), 308–315

Team SFSU Math @ R4R

The Frobenius Coin-Exchange Problem

The Frobenius Coin-Exchange Problem

Given coins of denominations $a_1, a_2, \ldots, a_d$ (with no common factor), what is the largest amount that cannot be changed?

Current state of affairs:

- $d = 2$ solved (probably by Sylvester in 1880's)
- $d = 3$ solved algorithmically (Herzog 1970, Greenberg 1980, Davison 1994) and in not-quite-explicit form (Denham 2003, Ramirez-Alfonsin 2005)
- $d \geq 4$ computationally feasible (Kannan 1992, Barvinok-Woods 2003), otherwise: completely open

Just a Pinch of Algebra

Given two positive integers a and b with no common factor, we can write any integer t as an integral linear combination

$$t = ma + nb \ .$$

In fact, $\{ma + nb : \ m, n \in \mathbb{Z}\}$ is a group (it's called $\mathbb{Z}$).

Just a Pinch of Algebra

Given two positive integers a and b with no common factor, we can write any integer t as an integral linear combination

$$t = ma + nb \, .$$

In fact, $\{ma + nb : \, m, n \in \mathbb{Z}\}$ is a group (it's called $\mathbb{Z}$).

Slight Variation $S_0(a,b) := \{ma + nb : \, m, n \in \mathbb{Z}_{\geq 0}\}$ is a semigroup.

Frobenius Problem Find $\max\left(\mathbb{Z}_{\geq 0} \setminus S_0(a,b)\right)$.

The Frobenius Coin-Exchange Problem

Given two positive integers a and b with no common factor, let

$$S_0(a,b) \; := \; \{ma + nb : \, m, n \in \mathbb{Z}_{\geq 0}\}$$

and

$$R_0(a,b) \; := \; \mathbb{Z}_{\geq 0} \setminus S_0(a,b)$$

The Frobenius Coin-Exchange Problem

Given two positive integers a and b with no common factor, let

$$S_0(a,b) \ := \ \{ma + nb : \ m,n \in \mathbb{Z}_{\geq 0}\}$$

and
$$R_0(a,b) \ := \ \mathbb{Z}_{\geq 0} \setminus S_0(a,b)$$

Natural problems: find

- $\max R_0(a,b)$ ($\longleftarrow$ Frobenius problem)
- $|R_0(a,b)|$
- $\sum R_0(a,b)$

The Frobenius Coin-Exchange Problem

Given two positive integers a and b with no common factor, let

$$S_0(a,b) \ := \ \{ma + nb : \ m,n \in \mathbb{Z}_{\geq 0}\}$$

and

$$R_0(a,b) \ := \ \mathbb{Z}_{\geq 0} \setminus S_0(a,b)$$

... and the winners are:

- $\max R_0(a,b) \ = \ ab - a - b$ [$\sim$ Sylvester 1884]
- $|R_0(a,b)| \ = \ \frac{1}{2}(a-1)(b-1)$ [Sylvester 1884]
- $\sum R_0(a,b) \ = \ \frac{1}{12}(a-1)(b-1)(2ab-a-b-1)$ [Brown–Shiue 1993]

The Frobenius Coin-Exchange Problem

Given two positive integers a and b with no common factor, let

$$S_0(a,b) \ := \ \{ma + nb : \ m, n \in \mathbb{Z}_{\geq 0}\}$$

and

$$R_0(a,b) \ := \ \mathbb{Z}_{\geq 0} \setminus S_0(a,b)$$

... and the winners are:

- $\max R_0(a,b) \ = \ ab - a - b$ [$\sim$ Sylvester 1884]
- $|R_0(a,b)| \ = \ \frac{1}{2}(a-1)(b-1)$ [Sylvester 1884]
- $\sum R_0(a,b) \ = \ \frac{1}{12}(a-1)(b-1)(2ab-a-b-1)$ [Brown–Shiue 1993]

(All of this can be asked for $d > 2$ parameters...)

Frobenius Generating Functions

Given two positive integers a and b with no common factor, let

$$S_0(a,b) := \{ma + nb : \ m, n \in \mathbb{Z}_{\geq 0}\} \qquad \text{and} \qquad R_0(a,b) := \mathbb{Z}_{\geq 0} \setminus S_0(a,b)$$

Theorem [Székely–Wormald 1986, Sertöz–Özlük 1991]

$$\sum_{j \in S_0(a,b)} z^j \ = \ \frac{1 - z^{ab}}{(1 - z^a)(1 - z^b)}$$

Frobenius Generating Functions

Given two positive integers a and b with no common factor, let

$S_0(a,b) := \{ma + nb : \, m, n \in \mathbb{Z}_{\geq 0}\}$ and $R_0(a,b) := \mathbb{Z}_{\geq 0} \setminus S_0(a,b)$

Theorem [Székely–Wormald 1986, Sertöz–Özlük 1991]

$$\sum_{j \in S_0(a,b)} z^j \; = \; \frac{1 - z^{ab}}{(1 - z^a)(1 - z^b)}$$

Why this is cool $p_0\,(a,b;z) \; := \sum_{j \in R_0(a,b)} z^j \; = \; \frac{1}{1-z} - \frac{1 - z^{ab}}{(1 - z^a)(1 - z^b)}$

Frobenius Generating Functions

Given two positive integers a and b with no common factor, let

$$S_0(a,b) := \{ma + nb : \, m,n \in \mathbb{Z}_{\geq 0}\} \qquad \text{and} \qquad R_0(a,b) := \mathbb{Z}_{\geq 0} \setminus S_0(a,b)$$

Theorem [Székely–Wormald 1986, Sertöz–Özlük 1991]

$$\sum_{j \in S_0(a,b)} z^j \;=\; \frac{1 - z^{ab}}{(1-z^a)(1-z^b)}$$

Why this is cool $\; p_0\,(a,b;z) \;:=\; \sum_{j \in R_0(a,b)} z^j \;=\; \frac{1}{1-z} - \frac{1-z^{ab}}{(1-z^a)(1-z^b)}$

- $\max R_0(a,b)$ equals the degree of $p_0\,(a,b;z)$
- $|R_0(a,b)| \;=\; \lim_{z \to 1} p_0\,(a,b;z)$
- $\sum R_0(a,b) \;=\; \lim_{z \to 1} p_0'\,(a,b;z)$

The k-Frobenius Problem

Given two positive integers a and b with no common factor, let $R_k(a,b)$ consist of all integers with exactly k representations of the form

$$ma + nb \qquad \text{with} \qquad m, n \in \mathbb{Z}_{\geq 0}$$

Natural problems: find

- $\max R_k(a,b)$
- $|R_k(a,b)|$
- $\sum R_k(a,b)$

The k-Frobenius Problem

Given two positive integers a and b with no common factor, let $R_k(a,b)$ consist of all integers with exactly k representations of the form

$$ma + nb \qquad \text{with} \qquad m, n \in \mathbb{Z}_{\geq 0}$$

Natural problems: find

- $\max R_k(a,b) \ = \ (k+1)ab - a - b$ [MB–Robins 2004]
- $|R_k(a,b)| \ = \ ab$ [MB–Robins 2004]
- $\sum R_k(a,b)$

(All of this can be asked for $d > 2$ parameters...)

More Frobenius Generating Functions

Given two positive integers a and b with no common factor, let $R_k(a,b)$ consist of all integers with exactly k representations of the form

$$ma + nb \qquad \text{with} \qquad m, n \in \mathbb{Z}_{\geq 0}$$

and let $S_k(a,b)$ consist of all integers with more than k representations of this form.

Theorem [Bardomero–MB 2020] $$\sum_{j \in S_k(a,b)} z^j \;=\; \frac{z^{abk}(1 - z^{ab})}{(1 - z^a)(1 - z^b)}$$

More Frobenius Generating Functions

Given two positive integers a and b with no common factor, let $R_k(a,b)$ consist of all integers with exactly k representations of the form

$$ma + nb \qquad \text{with} \qquad m, n \in \mathbb{Z}_{\ge 0}$$

and let $S_k(a,b)$ consist of all integers with more than k representations of this form.

Theorem [Bardomero–MB 2020] $$\sum_{j \in S_k(a,b)} z^j = \frac{z^{abk}(1-z^{ab})}{(1-z^a)(1-z^b)}$$

Corollary $$\sum_{j \in R_k(a,b)} z^j = \frac{z^{ab(k-1)}(1-z^{ab})^2}{(1-z^a)(1-z^b)}$$ where $k \ge 1$

More Frobenius Generating Functions

Given two positive integers a and b with no common factor, let $R_k(a,b)$ consist of all integers with exactly k representations of the form

$$ma + nb \qquad \text{with} \qquad m, n \in \mathbb{Z}_{\geq 0}$$

and let $S_k(a,b)$ consist of all integers with more than k representations of this form.

Theorem [Bardomero–MB 2020] $\displaystyle\sum_{j \in S_k(a,b)} z^j \ = \ \frac{z^{abk}(1 - z^{ab})}{(1 - z^a)(1 - z^b)}$

Corollary $\displaystyle\sum_{j \in R_k(a,b)} z^j \ = \ \frac{z^{ab(k-1)}(1 - z^{ab})^2}{(1 - z^a)(1 - z^b)}$ where $k \geq 1$

Corollary^2 $\sum R_k(a,b) \ = \ \frac{1}{2}\, ab\,(2abk - a - b)$ where $k \geq 1$

Frobenius Generating Function Subtleties

Given two positive integers a and b with no common factor, let $R_k(a,b)$ consist of all integers with exactly k representations of the form

$$ma + nb \qquad \text{with} \qquad m, n \in \mathbb{Z}_{\geq 0}$$

We have seen
$$\sum_{j \in R_0(a,b)} z^j = \frac{1}{1-z} - \frac{1-z^{ab}}{(1-z^a)(1-z^b)}$$

whereas for $k \geq 1$

$$\begin{aligned}\sum_{j \in R_k(a,b)} z^j &= \frac{z^{ab(k-1)}(1-z^{ab})^2}{(1-z^a)(1-z^b)} \\ &= z^{ab(k-1)}\left(1 + z^a + \cdots + z^{(b-1)a}\right)\left(1 + z^b + \cdots + z^{(a-1)b}\right)\end{aligned}$$

Frobenius generatingfunctionology

Given (relatively prime) positive integers a and b, consider

$$\frac{1}{(1-z^a)(1-z^b)} = \left(\sum_{m \ge 0} z^{ma}\right)\left(\sum_{n \ge 0} z^{nb}\right).$$

A typical term looks like z^{ma+nb} for some $m, n \ge 0$

Frobenius generatingfunctionology

Given (relatively prime) positive integers a and b, consider

$$\frac{1}{(1-z^a)\,(1-z^b)} \;=\; \left(\sum_{m\ge 0} z^{ma}\right)\left(\sum_{n\ge 0} z^{nb}\right).$$

A typical term looks like z^{ma+nb} for some $m,n \ge 0$, and so

$$\frac{1}{(1-z^a)\,(1-z^b)} \;=\; \sum_{t\ge 0} N(t)\, z^t$$

where $N(t) \;:=\; \#\left\{(m,n)\in\mathbb{Z}^2 :\; m,n\ge 0,\; ma+nb=t\right\}.$

Frobenius generatingfunctionology

Given (relatively prime) positive integers a and b, consider

$$\frac{1}{(1-z^a)\,(1-z^b)} \;=\; \left(\sum_{m\ge 0} z^{ma}\right)\left(\sum_{n\ge 0} z^{nb}\right).$$

A typical term looks like z^{ma+nb} for some $m, n \ge 0$, and so

$$\frac{1}{(1-z^a)\,(1-z^b)} \;=\; \sum_{t\ge 0} N(t)\, z^t$$

where $N(t) \;:=\; \#\left\{(m,n)\in\mathbb{Z}^2 :\; m,n\ge 0,\; ma+nb=t\right\}.$

Homework 1 $N(t+ab) = N(t)+1$

Frobenius generatingfunctionology

Homework 1 $N(t+ab) = N(t) + 1$

$$\begin{aligned}
\sum_{t \ge 0} N(t+ab)\, z^t &= \sum_{t \ge 0} (N(t)+1)\, z^t \\
\frac{1}{z^{ab}} \sum_{t \ge ab} N(t)\, z^t &= \sum_{t \ge 0} N(t)\, z^t + \sum_{t \ge 0} z^t \\
\frac{1}{z^{ab}} \left(\frac{1}{(1-z^a)\,(1-z^b)} - \sum_{t=0}^{ab-1} N(t)\, z^t \right) &= \frac{1}{(1-z^a)\,(1-z^b)} + \frac{1}{1-z}
\end{aligned}$$

Frobenius generatingfunctionology

Homework 1 $N(t+ab) = N(t) + 1$

$$\begin{aligned} \sum_{t \ge 0} N(t+ab)\, z^t &= \sum_{t \ge 0} (N(t)+1)\, z^t \\ \frac{1}{z^{ab}} \sum_{t \ge ab} N(t)\, z^t &= \sum_{t \ge 0} N(t)\, z^t + \sum_{t \ge 0} z^t \\ \frac{1}{z^{ab}} \left(\frac{1}{(1-z^a)\,(1-z^b)} - \sum_{t=0}^{ab-1} N(t)\, z^t \right) &= \frac{1}{(1-z^a)\,(1-z^b)} + \frac{1}{1-z} \end{aligned}$$

Homework 2 For $0 \le t \le ab-1$, $N(t)$ is 0 or 1.

$$\sum_{j \in S_0(a,b)} z^j = \frac{1-z^{ab}}{(1-z^a)(1-z^b)}$$

Beyond d=2

Given integers $a_1, a_2, \ldots, a_d$ with no common factor, let

$$F(z) \;=\; \sum_{j \in S_0(a_1,\ldots,a_d)} z^j \;=\; \frac{p(z)}{(1-z^{a_1})\,(1-z^{a_2})\cdots(1-z^{a_d})}\,.$$

- (Denham 2003) For $d=3$, the polynomial $p(z)$ has either 4 or 6 terms, given in semi-explicit form.
- (Bresinsky 1975) For $d \ge 4$, there is no absolute bound for the number of terms in $p(z)$.
- (Barvinok-Woods 2003) For fixed d, the rational generating function $F(z)$ can be written as a short sum of rational functions.

What else is (not yet) known

- Frobenius number and number of non-representable integers in special cases: arithmetic progressions and variations, extension cases
- Upper and lower bounds for the Frobenius number
- Algorithms
- Computational complexity
- k-Frobenius problem variants