Discrete Mathematics & Computational Structures
Lattice-Point Counting in Convex Polytopes
(1) Frobenius' Coin-Exchange Problem

Yoshio Okamoto

Tokyo Institute of Technology

April 16, 2009

"Last updated: 2009/04/16 13:10"

Textbook

We follow the book:

- Matthias Beck and Sinai Robins, *Computing the Continuous Discretely. Integer-Point Enumeration in Polyhedra*. Undergraduate Texts in Mathematics. New York, Springer. 2007.
    - The updated version is available at http://math.sfsu.edu/beck/ccd.html
    - Japanese translation will be available soon

Lecture Style

- Language
  - Spoken: in English or Japanese
  - Slides: in English
  - Report submission: in Japanese/English (up to you)
- Feedback
  - Submission of a piece of paper at the end of each lecture
  - Can be anonymous
  - There might be a survey at the term end

Goal

This is a course on mathematics and/or theory of computation

Goal of the course

- Study an example of mathematical thoughts that are benefitial for algorithms design
- In this course, such an example = lattice-point counting in convex polytopes

Prerequisites

- Nothing in particular
- Other than a moderate familiarity with freshmen math (Calculus, Linear Algebra, Discrete Math)
- And eagerness to learn

Evaluation

How to get a credit

Submission of exercise solutions

- Each lecture is accompanied with several exercises in the textbook
- Students should assign themselves to different exercises
- Assignment should be done at the wiki page of the course in the first-come-first-serve way
- Submission due: next lecture

Wiki: http://www.is.titech.ac.jp/˜okamoto/cgi-bin/pukiwiki/index.php?DMCS09

Administration

- Course Webpage
  - http://www.is.titech.ac.jp/~okamoto/lect/2009/dmcs/
  - Reachable from the CompView website (http://compview.titech.ac.jp/)
- This is in the Education Program for CompView
- Lecturer: Yoshio Okamoto
  - Email: okamoto at is.titech.ac.jp
  - Office: W904 in West 8th Bldg.
  - Int. Phone: 3871
  - Office hours: by appointment, or you can try your luck any time
- Remark: This lattice-point counting course will not be given next year; Could be discrete geometry, data structures, graph theory, extremal combinatorics, ..., I'm thinking

1. Introduction
2. Frobenius' coin-exchange problem
   - Why use generating functions?
   - Two coins
   - Partial fractions and a surprising formula
   - Sylvester's result
   - Three and more coins
3. Concluding remarks

The basic computational problems

When a finite set Ω is given implicitly...,

- Decide whether $\Omega = \varnothing$ (decision)
- Find an element of Ω if it exists (search)
- Count $|\Omega|$ (counting)
- List all elements of Ω (listing)
- Sample an element of Ω uniformly at random (sampling)

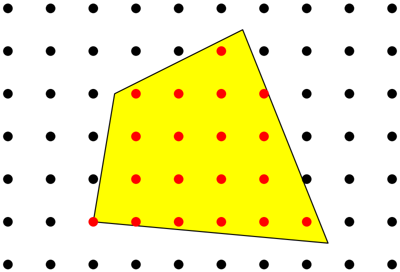
- They have some relationship
- Counting is the most difficult in a certain sense

A kind of the most general setting

One setting

$\Omega = P \cap \mathbb{Z}^d$ where

- P a d-dimensional convex polyhedron (in the H-representation) (the terminology will be defined through the course)
- $\mathbb{Z}$ is the set of integers



A theoretical development

$\Omega = P \cap \mathbb{Z}^d$

Theorem (Barvinok, Math of OR '94)

P is rational, d is constant $\Rightarrow$
$|P \cap \mathbb{Z}^d|$ can be computed in polynomial time

Implementations are also available

- LattE (Project led by De Loera)
  http://www.math.ucdavis.edu/~latte/
- LattE macchiato (Köppe)
  http://www.math.ucdavis.edu/~mkoppe/latte/
- barvinok (Verdoolaege)
  http://www.kotnet.org/~skimo/barvinok/

More formally speaking...

$\Omega = P \cap \mathbb{Z}^d$

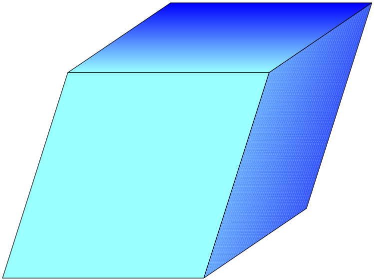
Theorem (Barvinok, Math of OR '94)

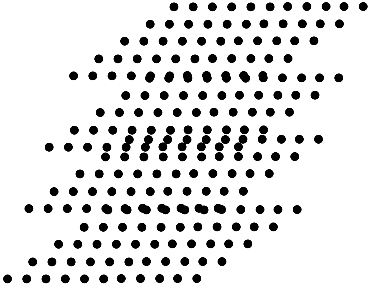
P is rational, d is constant $\Rightarrow$
The Ehrhart quasi-polynomial of P can be computed in poly time

So, in this course we look at

- lattice points in convex polyhedra
- Ehrhart (quasi-)polynomials
- and relationship with other subarea of mathematics

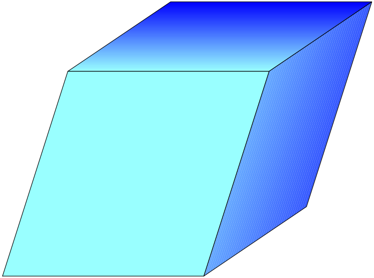
What's discrete volume?

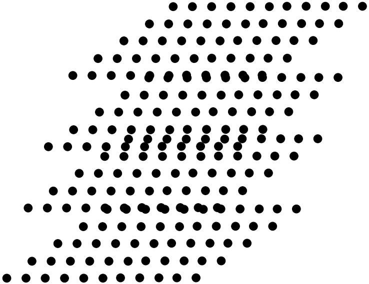




$\mathrm{vol}\,\mathcal{P}$ $\qquad$ $\#\left(\mathcal{P} \cap \mathbb{Z}^d\right)$

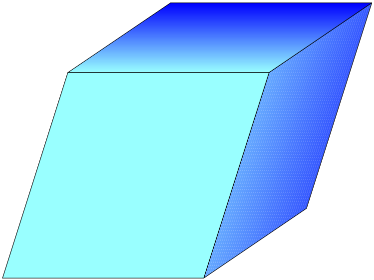
What's discrete volume?

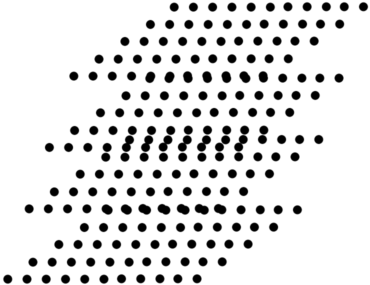




$$\mathrm{vol}\,\mathcal{P} \quad = \quad \lim_{k\to\infty} \#\left(\mathcal{P} \cap \frac{1}{k}\mathbb{Z}^d\right)\frac{1}{k^d}$$

What's discrete volume?

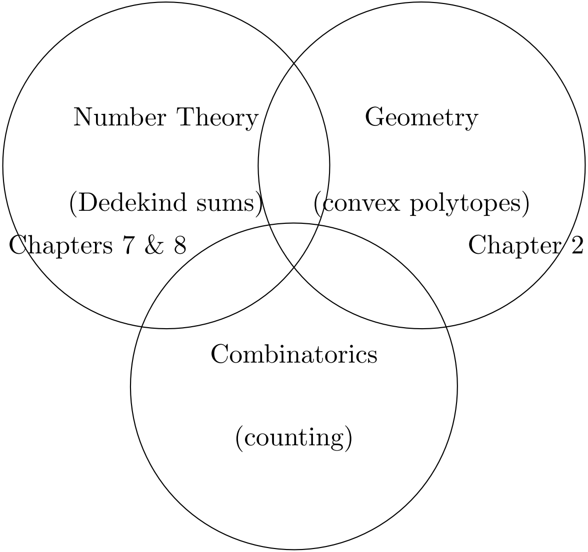




$$\mathrm{vol}\,\mathcal{P} \quad = \quad \lim_{k\to\infty} \#\left(\mathcal{P} \cap \frac{1}{k}\mathbb{Z}^d\right)\frac{1}{k^d}$$

integration (analysis) | counting (combinatorics)

Lattice-point counting in convex polytopes



A generating function of a sequence

Definition (Generating function)

Given a sequence $\{a_k\}$, define its generating function as

$$F(z) = \sum_{k \geq 0} a_k z^k$$

$F(z)$ is a power series, but let's forget about the convergence for the moment

- Generating functions are quite useful for many reasons
- Generating functions are main objects we deal with in this course

Example: Fibonacci sequence

Definition (Fibonacci sequence)

The Fibonacci sequence $\{f_k\}$ is defined as follows

- $f_0 = 0,\ f_1 = 1$
- $f_{k+2} = f_{k+1} + f_k$ for all $k \geq 0$

The first few numbers in the sequence are:

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987

See http://www.research.att.com/~njas/sequences/

- Excellent source of integer sequences

Discovery through the generating function

- $F(z)$ the generating function for the Fibonacci sequence

Discovery through the generating function

- $F(z)$ the generating function for the Fibonacci sequence
- Then, by the recursion

$$\sum_{k\geq 0} f_{k+2}\, z^k \tag{1}$$

Discovery through the generating function

- $F(z)$ the generating function for the Fibonacci sequence
- Then, by the recursion

$$\sum_{k\geq 0} f_{k+2}\, z^k = \sum_{k\geq 0} (f_{k+1} + f_k)\, z^k \tag{1}$$

Discovery through the generating function

- $F(z)$ the generating function for the Fibonacci sequence
- Then, by the recursion

$$\sum_{k\geq 0} f_{k+2}\, z^k = \sum_{k\geq 0} (f_{k+1} + f_k)\, z^k = \sum_{k\geq 0} f_{k+1}\, z^k + \sum_{k\geq 0} f_k\, z^k \quad (1)$$

Discovery through the generating function

- $F(z)$ the generating function for the Fibonacci sequence
- Then, by the recursion

$$\sum_{k\geq 0} f_{k+2}\, z^k = \sum_{k\geq 0} (f_{k+1} + f_k)\, z^k = \sum_{k\geq 0} f_{k+1}\, z^k + \sum_{k\geq 0} f_k\, z^k \quad (1)$$

- The LHS of (1) is

$$\sum_{k\geq 0} f_{k+2}\, z^k$$

Discovery through the generating function

- $F(z)$ the generating function for the Fibonacci sequence
- Then, by the recursion

$$\sum_{k\geq 0} f_{k+2}\, z^k = \sum_{k\geq 0} (f_{k+1} + f_k)\, z^k = \sum_{k\geq 0} f_{k+1}\, z^k + \sum_{k\geq 0} f_k\, z^k \quad (1)$$

- The LHS of (1) is

$$\sum_{k\geq 0} f_{k+2}\, z^k = \frac{1}{z^2} \sum_{k\geq 0} f_{k+2}\, z^{k+2}$$

Discovery through the generating function

- $F(z)$ the generating function for the Fibonacci sequence
- Then, by the recursion

$$\sum_{k\geq 0} f_{k+2}\, z^k = \sum_{k\geq 0} (f_{k+1} + f_k)\, z^k = \sum_{k\geq 0} f_{k+1}\, z^k + \sum_{k\geq 0} f_k\, z^k \quad (1)$$

- The LHS of (1) is

$$\sum_{k\geq 0} f_{k+2}\, z^k = \frac{1}{z^2} \sum_{k\geq 0} f_{k+2}\, z^{k+2} = \frac{1}{z^2} \sum_{k\geq 2} f_k\, z^k$$

Discovery through the generating function

- $F(z)$ the generating function for the Fibonacci sequence
- Then, by the recursion

$$\sum_{k\geq 0} f_{k+2}\, z^k = \sum_{k\geq 0} (f_{k+1} + f_k)\, z^k = \sum_{k\geq 0} f_{k+1}\, z^k + \sum_{k\geq 0} f_k\, z^k \quad (1)$$

- The LHS of (1) is

$$\sum_{k\geq 0} f_{k+2}\, z^k = \frac{1}{z^2} \sum_{k\geq 0} f_{k+2}\, z^{k+2} = \frac{1}{z^2} \sum_{k\geq 2} f_k\, z^k = \frac{1}{z^2} (F(z) - z)$$

Discovery through the generating function

- $F(z)$ the generating function for the Fibonacci sequence
- Then, by the recursion

$$\sum_{k\geq 0} f_{k+2}\, z^k = \sum_{k\geq 0} (f_{k+1} + f_k)\, z^k = \sum_{k\geq 0} f_{k+1}\, z^k + \sum_{k\geq 0} f_k\, z^k \quad (1)$$

- The LHS of (1) is

$$\sum_{k\geq 0} f_{k+2}\, z^k = \frac{1}{z^2} \sum_{k\geq 0} f_{k+2}\, z^{k+2} = \frac{1}{z^2} \sum_{k\geq 2} f_k\, z^k = \frac{1}{z^2} (F(z) - z)$$

- The RHS of (1) is

$$\sum_{k\geq 0} f_{k+1}\, z^k + \sum_{k\geq 0} f_k\, z^k$$

Discovery through the generating function

- $F(z)$ the generating function for the Fibonacci sequence
- Then, by the recursion

$$\sum_{k\geq 0} f_{k+2}\, z^k = \sum_{k\geq 0} (f_{k+1} + f_k)\, z^k = \sum_{k\geq 0} f_{k+1}\, z^k + \sum_{k\geq 0} f_k\, z^k \quad (1)$$

- The LHS of (1) is

$$\sum_{k\geq 0} f_{k+2}\, z^k = \frac{1}{z^2} \sum_{k\geq 0} f_{k+2}\, z^{k+2} = \frac{1}{z^2} \sum_{k\geq 2} f_k\, z^k = \frac{1}{z^2} (F(z) - z)$$

- The RHS of (1) is

$$\sum_{k\geq 0} f_{k+1}\, z^k + \sum_{k\geq 0} f_k\, z^k = \frac{1}{z} \sum_{k\geq 0} f_{k+1}\, z^{k+1} + \sum_{k\geq 0} f_k\, z^k$$

Discovery through the generating function

- $F(z)$ the generating function for the Fibonacci sequence
- Then, by the recursion

$$\sum_{k\geq 0} f_{k+2}\, z^k = \sum_{k\geq 0} (f_{k+1} + f_k)\, z^k = \sum_{k\geq 0} f_{k+1}\, z^k + \sum_{k\geq 0} f_k\, z^k \quad (1)$$

- The LHS of (1) is

$$\sum_{k\geq 0} f_{k+2}\, z^k = \frac{1}{z^2}\sum_{k\geq 0} f_{k+2}\, z^{k+2} = \frac{1}{z^2}\sum_{k\geq 2} f_k\, z^k = \frac{1}{z^2}(F(z) - z)$$

- The RHS of (1) is

$$\sum_{k\geq 0} f_{k+1}\, z^k + \sum_{k\geq 0} f_k\, z^k = \frac{1}{z}\sum_{k\geq 0} f_{k+1}\, z^{k+1} + \sum_{k\geq 0} f_k\, z^k = \frac{1}{z}F(z) + F(z)$$

Discovery through the generating function (cont'd)

- $\therefore$ (1) is rewritten as

$$\frac{1}{z^2}(F(z) - z) = \frac{1}{z}F(z) + F(z)$$

Discovery through the generating function (cont'd)

- $\therefore$ (1) is rewritten as

$$\frac{1}{z^2}(F(z) - z) = \frac{1}{z}F(z) + F(z)$$

- Equivalently,

$$F(z) = \frac{z}{1 - z - z^2}$$

Discovery through the generating function (cont'd)

- $\therefore$ (1) is rewritten as

$$\frac{1}{z^2}(F(z) - z) = \frac{1}{z}F(z) + F(z)$$

- Equivalently,

$$F(z) = \frac{z}{1 - z - z^2}$$

- A fun to check (by a computer)

$$\frac{z}{1 - z - z^2} = z + z^2 + 2\,z^3 + 3\,z^4 + 5\,z^5 + 8\,z^6 + 13\,z^7 + \cdots$$

Discovery through the generating function (cont'd)

- A partial fraction expansion gives us

$$F(z) = \frac{z}{1 - z - z^2} = \frac{1/\sqrt{5}}{1 - \frac{1+\sqrt{5}}{2} z} - \frac{1/\sqrt{5}}{1 - \frac{1-\sqrt{5}}{2} z} \tag{2}$$

Discovery through the generating function (cont'd)

- A partial fraction expansion gives us

$$F(z) = \frac{z}{1-z-z^2} = \frac{1/\sqrt{5}}{1-\frac{1+\sqrt{5}}{2}z} - \frac{1/\sqrt{5}}{1-\frac{1-\sqrt{5}}{2}z} \tag{2}$$

- Remember the geometric series

$$\sum_{k\geq 0} x^k = \frac{1}{1-x} \tag{3}$$

Discovery through the generating function (cont'd)

- A partial fraction expansion gives us

$$F(z) = \frac{z}{1-z-z^2} = \frac{1/\sqrt{5}}{1-\frac{1+\sqrt{5}}{2}z} - \frac{1/\sqrt{5}}{1-\frac{1-\sqrt{5}}{2}z} \tag{2}$$

- Remember the geometric series

$$\sum_{k\geq 0} x^k = \frac{1}{1-x} \tag{3}$$

- Then, by setting $x = \frac{1+\sqrt{5}}{2}z$ and $x = \frac{1-\sqrt{5}}{2}z$ we have

$$\begin{aligned} F(z) &= \frac{z}{1-z-z^2} \\ &= \frac{1}{\sqrt{5}}\sum_{k\geq 0}\left(\frac{1+\sqrt{5}}{2}z\right)^k - \frac{1}{\sqrt{5}}\sum_{k\geq 0}\left(\frac{1-\sqrt{5}}{2}z\right)^k \end{aligned}$$

Discovery through the generating function (cont'd)

- We have

$$F(z) = \frac{1}{\sqrt{5}} \sum_{k \geq 0} \left(\frac{1+\sqrt{5}}{2} z \right)^k - \frac{1}{\sqrt{5}} \sum_{k \geq 0} \left(\frac{1-\sqrt{5}}{2} z \right)^k$$

Discovery through the generating function (cont'd)

- We have

$$F(z) = \frac{1}{\sqrt{5}} \sum_{k \geq 0} \left(\frac{1+\sqrt{5}}{2} z \right)^k - \frac{1}{\sqrt{5}} \sum_{k \geq 0} \left(\frac{1-\sqrt{5}}{2} z \right)^k$$

$$= \sum_{k \geq 0} \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^k - \left(\frac{1-\sqrt{5}}{2} \right)^k \right) z^k$$

Discovery through the generating function (cont'd)

- We have

$$F(z) = \frac{1}{\sqrt{5}} \sum_{k \geq 0} \left(\frac{1+\sqrt{5}}{2} z \right)^k - \frac{1}{\sqrt{5}} \sum_{k \geq 0} \left(\frac{1-\sqrt{5}}{2} z \right)^k$$
$$= \sum_{k \geq 0} \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^k - \left(\frac{1-\sqrt{5}}{2} \right)^k \right) z^k$$

- Thus, we obtain a closed formula for the Fibonacci sequence

$$f_k = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^k - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^k$$

Usefulness of a generating function

- It gives a closed formula of a sequence

$$f_k = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^k - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^k$$

- It gives a short description of a sequence as a rational function

$$F(z) = \frac{z}{1-z-z^2}$$

Partial fraction expansion (in case you've never heard of that)

Theorem 1.1 (Partial fraction expansion)

Given any rational function

$$F(z) := \frac{p(z)}{\prod_{k=1}^{m} (z - a_k)^{e_k}},$$

where p is a polynomial of degree less than $e_1 + e_2 + \cdots + e_m$ and the a_k's are distinct, there exists a decomposition

$$F(z) = \sum_{k=1}^{m} \left(\frac{c_{k,1}}{z - a_k} + \frac{c_{k,2}}{(z - a_k)^2} + \cdots + \frac{c_{k,e_k}}{(z - a_k)^{e_k}} \right),$$

where $c_{k,j} \in \mathbb{C}$ are unique.

Proof: Exercise 1.35 □

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	6	11	16	21
2	7	12	17	22
3	8	13	18	23
4	9	14	19	24
5	10	15	20	25

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1 $\times$	6	11	16	21
2	7	12	17	22
3	8	13	18	23
4	9	14	19	24
5	10	15	20	25

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	$\times$	6	11	16	21
2	$\times$	7	12	17	22
3		8	13	18	23
4		9	14	19	24
5		10	15	20	25

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	$\times$	6	11	16	21
2	$\times$	7	12	17	22
3	$\times$	8	13	18	23
4		9	14	19	24
5		10	15	20	25

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	$\times$	6	11	16	21
2	$\times$	7	12	17	22
3	$\times$	8	13	18	23
4	$\surd$	9	14	19	24
5		10	15	20	25

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	$\times$	6	11	16	21
2	$\times$	7	12	17	22
3	$\times$	8	13	18	23
4	$\surd$	9	14	19	24
5	$\times$	10	15	20	25

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	$\times$	6	$\times$	11		16		21	
2	$\times$	7		12		17		22	
3	$\times$	8		13		18		23	
4	$\surd$	9		14		19		24	
5	$\times$	10		15		20		25	

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	$\times$	6	$\times$	11	16	21
2	$\times$	7	$\surd$	12	17	22
3	$\times$	8		13	18	23
4	$\surd$	9		14	19	24
5	$\times$	10		15	20	25

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	$\times$	6	$\times$	11		16		21	
2	$\times$	7	$\surd$	12		17		22	
3	$\times$	8	$\surd$	13		18		23	
4	$\surd$	9		14		19		24	
5	$\times$	10		15		20		25	

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	$\times$	6	$\times$	11	16	21
2	$\times$	7	$\surd$	12	17	22
3	$\times$	8	$\surd$	13	18	23
4	$\surd$	9	$\surd$	14	19	24
5	$\times$	10		15	20	25

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	$\times$	6	$\times$	11	16	21
2	$\times$	7	$\surd$	12	17	22
3	$\times$	8	$\surd$	13	18	23
4	$\surd$	9	$\surd$	14	19	24
5	$\times$	10	$\times$	15	20	25

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	$\times$	6	$\times$	11	$\surd$	16		21	
2	$\times$	7	$\surd$	12		17		22	
3	$\times$	8	$\surd$	13		18		23	
4	$\surd$	9	$\surd$	14		19		24	
5	$\times$	10	$\times$	15		20		25	

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	$\times$	6	$\times$	11	$\surd$	16		21	
2	$\times$	7	$\surd$	12	$\surd$	17		22	
3	$\times$	8	$\surd$	13		18		23	
4	$\surd$	9	$\surd$	14		19		24	
5	$\times$	10	$\times$	15		20		25	

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	$\times$	6	$\times$	11	$\surd$	16		21	
2	$\times$	7	$\surd$	12	$\surd$	17		22	
3	$\times$	8	$\surd$	13	$\surd$	18		23	
4	$\surd$	9	$\surd$	14		19		24	
5	$\times$	10	$\times$	15		20		25	

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	$\times$	6	$\times$	11	$\surd$	16		21	
2	$\times$	7	$\surd$	12	$\surd$	17		22	
3	$\times$	8	$\surd$	13	$\surd$	18		23	
4	$\surd$	9	$\surd$	14	$\surd$	19		24	
5	$\times$	10	$\times$	15		20		25	

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	$\times$	6	$\times$	11	$\surd$	16		21	
2	$\times$	7	$\surd$	12	$\surd$	17		22	
3	$\times$	8	$\surd$	13	$\surd$	18		23	
4	$\surd$	9	$\surd$	14	$\surd$	19		24	
5	$\times$	10	$\times$	15	$\surd$	20		25	

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	$\times$	6	$\times$	11	$\surd$	16	$\surd$	21	
2	$\times$	7	$\surd$	12	$\surd$	17		22	
3	$\times$	8	$\surd$	13	$\surd$	18		23	
4	$\surd$	9	$\surd$	14	$\surd$	19		24	
5	$\times$	10	$\times$	15	$\surd$	20		25	

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	$\times$	6	$\times$	11	$\surd$	16	$\surd$	21	
2	$\times$	7	$\surd$	12	$\surd$	17	$\surd$	22	
3	$\times$	8	$\surd$	13	$\surd$	18		23	
4	$\surd$	9	$\surd$	14	$\surd$	19		24	
5	$\times$	10	$\times$	15	$\surd$	20		25	

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	$\times$	6	$\times$	11	$\surd$	16	$\surd$	21	
2	$\times$	7	$\surd$	12	$\surd$	17	$\surd$	22	
3	$\times$	8	$\surd$	13	$\surd$	18	$\surd$	23	
4	$\surd$	9	$\surd$	14	$\surd$	19		24	
5	$\times$	10	$\times$	15	$\surd$	20		25	

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	$\times$	6	$\times$	11	$\surd$	16	$\surd$	21	
2	$\times$	7	$\surd$	12	$\surd$	17	$\surd$	22	
3	$\times$	8	$\surd$	13	$\surd$	18	$\surd$	23	
4	$\surd$	9	$\surd$	14	$\surd$	19	$\surd$	24	
5	$\times$	10	$\times$	15	$\surd$	20		25	

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	$\times$	6	$\times$	11	$\surd$	16	$\surd$	21	
2	$\times$	7	$\surd$	12	$\surd$	17	$\surd$	22	
3	$\times$	8	$\surd$	13	$\surd$	18	$\surd$	23	
4	$\surd$	9	$\surd$	14	$\surd$	19	$\surd$	24	
5	$\times$	10	$\times$	15	$\surd$	20	$\surd$	25	

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	$\times$	6	$\times$	11	$\surd$	16	$\surd$	21	$\surd$
2	$\times$	7	$\surd$	12	$\surd$	17	$\surd$	22	$\surd$
3	$\times$	8	$\surd$	13	$\surd$	18	$\surd$	23	$\surd$
4	$\surd$	9	$\surd$	14	$\surd$	19	$\surd$	24	$\surd$
5	$\times$	10	$\times$	15	$\surd$	20	$\surd$	25	$\surd$

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	$\times$	6	$\times$	11	$\surd$	16	$\surd$	21	$\surd$
2	$\times$	7	$\surd$	12	$\surd$	17	$\surd$	22	$\surd$
3	$\times$	8	$\surd$	13	$\surd$	18	$\surd$	23	$\surd$
4	$\surd$	9	$\surd$	14	$\surd$	19	$\surd$	24	$\surd$
5	$\times$	10	$\times$	15	$\surd$	20	$\surd$	25	$\surd$

Exercise 1.20

The coins are coprime $\Rightarrow$ Only finitely many prices cannot be paid

What if the new coin system is introduced

Imagine we only have 4-yen, 7-yen, 9-yen, and 34-yen coins

Which price can be paid without making any change?

1	$\times$	6	$\times$	11	$\surd$	16	$\surd$	21	$\surd$
2	$\times$	7	$\surd$	12	$\surd$	17	$\surd$	22	$\surd$
3	$\times$	8	$\surd$	13	$\surd$	18	$\surd$	23	$\surd$
4	$\surd$	9	$\surd$	14	$\surd$	19	$\surd$	24	$\surd$
5	$\times$	10	$\times$	15	$\surd$	20	$\surd$	25	$\surd$

Exercise 1.20

The coins are coprime $\Rightarrow$ Only finitely many prices cannot be paid

Frobenius' coin-exchange problem, informally

Find the largest price that the coin system cannot allow us to pay

Frobenius' coin-exchange problem

$A = \{a_1, a_2, \ldots, a_d\}$ a set of coprime positive integers

Definition (Representable integer)

An integer n is representable by A if $\exists$ non-negative integers $m_1, m_2, \ldots, m_d$ s.t. $n = m_1 a_1 + \cdots + m_d a_d$

Definition (Frobenius number)

$$g(A) = \text{max number that's not representable by } A$$

Frobenius' coin-exchange problem

Determine $g(A)$

Two coins

When $d = 2$ the situation is well studied

Theorem 1.2

a_1, a_2 coprime $\Rightarrow g(a_1, a_2) = a_1 a_2 - a_1 - a_2$

- Quite simple
- But such a simple formula cannot be expected for larger d

We prove it in the next subsection

Sylvester's theorem

More is known when $d = 2$

Theorem 1.3 (Sylvester's theorem, 1884)

a_1, a_2 coprime $\Rightarrow$ exactly $\dfrac{(a_1-1)(a_2-1)}{2}$ integers are not representable

Example: $a_1 = 3, a_2 = 7$ ($\rightsquigarrow a_1 a_2 - a_1 - a_2 = 11$)

1	$\times$	6	$\surd$	11	$\times$	16	$\surd$	21	$\surd$
2	$\times$	7	$\surd$	12	$\surd$	17	$\surd$	22	$\surd$
3	$\surd$	8	$\times$	13	$\surd$	18	$\surd$	23	$\surd$
4	$\times$	9	$\surd$	14	$\surd$	19	$\surd$	24	$\surd$
5	$\times$	10	$\surd$	15	$\surd$	20	$\surd$	25	$\surd$

A tool: restricted partition function

$A = \{a_1, \ldots, a_d\}$ a set of coprime positive integer

Definition (Restricted partition function)

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

In words

$p_A(n) = \#$ representations of n by A

Note

$g(A) = \max\{n \mid p_A(n) = 0\}$

Restricted partition functions and polytopes

Definition (Dilate)

The n-th dilate of any set $S \subseteq \mathbb{R}^d$ is

$$nS = \{(nx_1, nx_2, \ldots, nx_d) : (x_1, \ldots, x_d) \in S\}$$

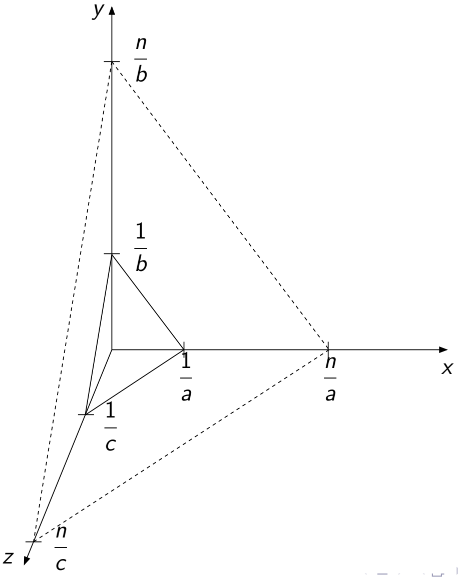
If we define

$$\mathcal{P} = \left\{(x_1, \ldots, x_d) \in \mathbb{R}^d : \text{ all } x_j \geq 0,\ x_1 a_1 + \cdots + x_d a_d = 1\right\} \tag{4}$$

then we see that

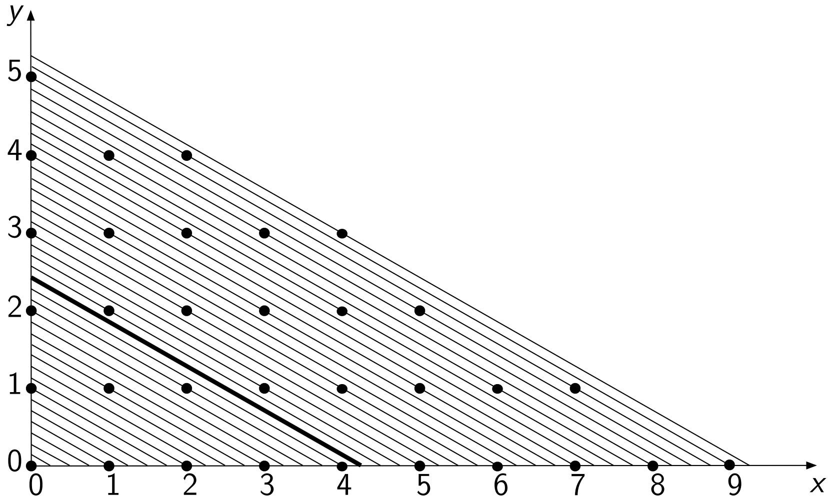
- $\mathcal{P}$ is a polytope (defined in the next lecture), and
- $p_A(n) = \#(n\mathcal{P} \cap \mathbb{Z}^d)$

Schematic geometric picture for three coins



Geometric picture for two coins

$A = \{4, 7\}$, the lines $4x + 7y = n$, $n = 1, 2, \ldots$



Generating function for the restricted partition function

Concentrate on the case $d = 2$, so let $A = \{a, b\}$ where a, b coprime

- Consider $p_{\{a,b\}}(n) = \#\{(k, l) \in \mathbb{Z}^2 : \ k, l \geq 0, \ ak + bl = n\}$

Generating function for the restricted partition function

Concentrate on the case $d = 2$, so let $A = \{a, b\}$ where a, b coprime

- Consider $p_{\{a,b\}}(n) = \#\{(k, l) \in \mathbb{Z}^2 : \ k, l \geq 0, \ ak + bl = n\}$
- Consider the product of the following two geometric series:

$$\left(\frac{1}{1 - z^a}\right)\left(\frac{1}{1 - z^b}\right)$$

Generating function for the restricted partition function

Concentrate on the case $d = 2$, so let $A = \{a, b\}$ where a, b coprime

- Consider $p_{\{a,b\}}(n) = \#\{(k, l) \in \mathbb{Z}^2 : \ k, l \geq 0, \ ak + bl = n\}$
- Consider the product of the following two geometric series:

$$\left(\frac{1}{1 - z^a}\right)\left(\frac{1}{1 - z^b}\right) = \left(1 + z^a + z^{2a} + \cdots\right)\left(1 + z^b + z^{2b} + \cdots\right)$$

Generating function for the restricted partition function

Concentrate on the case $d = 2$, so let $A = \{a, b\}$ where a, b coprime

- Consider $p_{\{a,b\}}(n) = \#\{(k, l) \in \mathbb{Z}^2 : \ k, l \geq 0, \ ak + bl = n\}$
- Consider the product of the following two geometric series:

$$\begin{aligned} \left(\frac{1}{1-z^a}\right)\left(\frac{1}{1-z^b}\right) &= \left(1 + z^a + z^{2a} + \cdots\right)\left(1 + z^b + z^{2b} + \cdots\right) \\ &= \sum_{k \geq 0} \sum_{l \geq 0} z^{ak} z^{bl} \end{aligned}$$

Generating function for the restricted partition function

Concentrate on the case $d = 2$, so let $A = \{a, b\}$ where a, b coprime

- Consider $p_{\{a,b\}}(n) = \#\{(k, l) \in \mathbb{Z}^2 : \ k, l \geq 0, \ ak + bl = n\}$
- Consider the product of the following two geometric series:

$$\begin{aligned}\left(\frac{1}{1-z^a}\right)\left(\frac{1}{1-z^b}\right) &= \left(1 + z^a + z^{2a} + \cdots\right)\left(1 + z^b + z^{2b} + \cdots\right) \\ &= \sum_{k \geq 0} \sum_{l \geq 0} z^{ak} z^{bl} \\ &= \sum_{n \geq 0} p_{\{a,b\}}(n)\, z^n\end{aligned}$$

Generating function for the restricted partition function

Concentrate on the case $d = 2$, so let $A = \{a, b\}$ where a, b coprime

- Consider $p_{\{a,b\}}(n) = \#\{(k,l) \in \mathbb{Z}^2 : \ k,l \geq 0, \ ak + bl = n\}$
- Consider the product of the following two geometric series:

$$\begin{aligned} \left(\frac{1}{1-z^a}\right)\left(\frac{1}{1-z^b}\right) &= \left(1 + z^a + z^{2a} + \cdots\right)\left(1 + z^b + z^{2b} + \cdots\right) \\ &= \sum_{k\geq 0}\sum_{l\geq 0} z^{ak} z^{bl} \\ &= \sum_{n\geq 0} p_{\{a,b\}}(n)\, z^n \end{aligned}$$

- $\therefore$ this fn is the generating fn for the seq $\left(p_{\{a,b\}}(n)\right)_{n=0}^{\infty}$

Generating function for the restricted partition function

Concentrate on the case $d = 2$, so let $A = \{a, b\}$ where a, b coprime

- Consider $p_{\{a,b\}}(n) = \#\{(k, l) \in \mathbb{Z}^2 : \ k, l \geq 0, \ ak + bl = n\}$
- Consider the product of the following two geometric series:

$$\begin{aligned} \left(\frac{1}{1 - z^a}\right)\left(\frac{1}{1 - z^b}\right) &= \left(1 + z^a + z^{2a} + \cdots\right)\left(1 + z^b + z^{2b} + \cdots\right) \\ &= \sum_{k \geq 0} \sum_{l \geq 0} z^{ak} z^{bl} \\ &= \sum_{n \geq 0} p_{\{a,b\}}(n)\, z^n \end{aligned}$$

- $\therefore$ this fn is the generating fn for the seq $\left(p_{\{a,b\}}(n)\right)_{n=0}^{\infty}$

The idea is to study the compact function on the LHS!

Looking at the constant term by shifting

More convenient if we can look at the constant term after shifting

- Namely, $p_A(n)$ is the constant term of

$$f(z) := \frac{1}{(1-z^a)(1-z^b)\,z^n} = \sum_{k\geq 0} p_{\{a,b\}}(k)\, z^{k-n}$$

This is a Laurent series

Looking at the constant term by shifting

More convenient if we can look at the constant term after shifting

- Namely, $p_A(n)$ is the constant term of

$$f(z) := \frac{1}{(1-z^a)(1-z^b)\,z^n} = \sum_{k\geq 0} p_{\{a,b\}}(k)\,z^{k-n}$$

  This is a Laurent series

- To obtain $p_A(n)$ we only need to "evaluate" $f(z)$ at $z=0$, but this is impossible since $f(z)$ has terms with negative exponents

Looking at the constant term by shifting

More convenient if we can look at the constant term after shifting

- Namely, $p_A(n)$ is the constant term of

$$f(z) := \frac{1}{(1-z^a)(1-z^b)\,z^n} = \sum_{k\geq 0} p_{\{a,b\}}(k)\, z^{k-n}$$

  This is a Laurent series

- To obtain $p_A(n)$ we only need to "evaluate" $f(z)$ at $z=0$, but this is impossible since $f(z)$ has terms with negative exponents
- We just need a contant term, so we subtract the terms with negative exponents from $f(z)$ and evaluate it at $z=0$
- (Or, we may use the residue theorem from complex analysis)

After a few minutes of computation...

We get

$$p_{\{a,b\}}(n) = \frac{1}{2a} + \frac{1}{2b} + \frac{n}{ab} + \frac{1}{a}\sum_{k=1}^{a-1}\frac{1}{(1-\xi_a^{kb})\xi_a^{kn}} + \frac{1}{b}\sum_{j=1}^{b-1}\frac{1}{(1-\xi_b^{ja})\xi_b^{jn}} \tag{7}$$

where

$$\xi_a := e^{2\pi i/a} = \cos\frac{2\pi}{a} + i\sin\frac{2\pi}{a}$$

is the a-th root of unity

After a few minutes of computation...

We get

$$p_{\{a,b\}}(n) = \frac{1}{2a} + \frac{1}{2b} + \frac{n}{ab} + \frac{1}{a}\sum_{k=1}^{a-1} \frac{1}{(1-\xi_a^{kb})\xi_a^{kn}} + \frac{1}{b}\sum_{j=1}^{b-1} \frac{1}{(1-\xi_b^{ja})\xi_b^{jn}} \tag{7}$$

where

$$\xi_a := e^{2\pi i/a} = \cos\frac{2\pi}{a} + i\sin\frac{2\pi}{a}$$

is the a-th root of unity

- Let's make it simpler and more understandable

Greatest-integer functions and fractional-part functions

Let $x \in \mathbb{R}$

Definition (Greatest-integer function)

$\lfloor x \rfloor = \max\{n \in \mathbb{Z} \mid n \leq x\}$

Definition (Fractional-part function)

$\{x\} = x - \lfloor x \rfloor$

Example:

x	$\lfloor x \rfloor$	$\{x\}$
4.2	4	0.2
-3.7	-4	0.3
7	7	0

With help of this notation

- When $b = 1$, the problem gets one-dimensional

$$p_{\{a,1\}}(n) = \#\left\{(k, l) \in \mathbb{Z}^2 : \ k, l \geq 0, \ ak + l = n\right\}$$

With help of this notation

- When $b = 1$, the problem gets one-dimensional

$$\begin{aligned} p_{\{a,1\}}(n) &= \#\left\{(k,l) \in \mathbb{Z}^2 : \ k,l \geq 0, \ ak + l = n\right\} \\ &= \#\left\{k \in \mathbb{Z} : \ k \geq 0, \ ak \leq n\right\} \end{aligned}$$

With help of this notation

- When $b = 1$, the problem gets one-dimensional

$$
\begin{aligned}
p_{\{a,1\}}(n) &= \#\left\{(k,l) \in \mathbb{Z}^2 :\ k,l \geq 0,\ ak + l = n\right\} \\
&= \#\left\{k \in \mathbb{Z} :\ k \geq 0,\ ak \leq n\right\} \\
&= \#\left\{k \in \mathbb{Z} :\ 0 \leq k \leq \frac{n}{a}\right\}
\end{aligned}
$$

With help of this notation

- When $b = 1$, the problem gets one-dimensional

$$
\begin{aligned}
p_{\{a,1\}}(n) &= \#\left\{(k,l) \in \mathbb{Z}^2 : \ k, l \geq 0, \ ak + l = n\right\} \\
&= \#\left\{k \in \mathbb{Z} : \ k \geq 0, \ ak \leq n\right\} \\
&= \#\left\{k \in \mathbb{Z} : \ 0 \leq k \leq \frac{n}{a}\right\} = \left\lfloor \frac{n}{a} \right\rfloor + 1
\end{aligned}
$$

With help of this notation

- When $b = 1$, the problem gets one-dimensional

$$\begin{aligned} p_{\{a,1\}}(n) &= \#\left\{(k,l) \in \mathbb{Z}^2 : \ k,l \geq 0,\ ak + l = n\right\} \\ &= \#\left\{k \in \mathbb{Z} : \ k \geq 0,\ ak \leq n\right\} \\ &= \#\left\{k \in \mathbb{Z} : \ 0 \leq k \leq \frac{n}{a}\right\} = \left\lfloor \frac{n}{a} \right\rfloor + 1 \end{aligned}$$

- Therefore,

$$\frac{1}{2a} + \frac{1}{2} + \frac{n}{a} + \frac{1}{a}\sum_{k=1}^{a-1} \frac{1}{\left(1 - \xi_a^k\right)\xi_a^{kn}} = \left\lfloor \frac{n}{a} \right\rfloor + 1 \tag{8}$$

With help of this notation

- When $b = 1$, the problem gets one-dimensional

$$\begin{aligned} p_{\{a,1\}}(n) &= \#\left\{(k,l) \in \mathbb{Z}^2 : \ k,l \geq 0,\ ak + l = n\right\} \\ &= \#\left\{k \in \mathbb{Z} : \ k \geq 0,\ ak \leq n\right\} \\ &= \#\left\{k \in \mathbb{Z} : \ 0 \leq k \leq \frac{n}{a}\right\} = \left\lfloor \frac{n}{a} \right\rfloor + 1 \end{aligned}$$

- Therefore,

$$\frac{1}{2a} + \frac{1}{2} + \frac{n}{a} + \frac{1}{a}\sum_{k=1}^{a-1} \frac{1}{\left(1 - \xi_a^k\right)\xi_a^{kn}} = \left\lfloor \frac{n}{a} \right\rfloor + 1$$

$$\frac{1}{a}\sum_{k=1}^{a-1} \frac{1}{\left(1 - \xi_a^k\right)\xi_a^{kn}} = -\left\{\frac{n}{a}\right\} + \frac{1}{2} - \frac{1}{2a} \tag{8}$$

Popoviciu's theorem

- Exercise 1.22

$$\frac{1}{a}\sum_{k=1}^{a-1}\frac{1}{\left(1-\xi_a^{bk}\right)\xi_a^{kn}}=\frac{1}{a}\sum_{k=1}^{a-1}\frac{1}{\left(1-\xi_a^{k}\right)\xi_a^{b^{-1}kn}} \tag{9}$$

where b^{-1} is an integer s.t. $b^{-1}b \equiv 1 \bmod a$

Popoviciu's theorem

- Exercise 1.22

$$\frac{1}{a}\sum_{k=1}^{a-1}\frac{1}{\left(1-\xi_a^{bk}\right)\xi_a^{kn}} = \frac{1}{a}\sum_{k=1}^{a-1}\frac{1}{\left(1-\xi_a^{k}\right)\xi_a^{b^{-1}kn}} \tag{9}$$

where b^{-1} is an integer s.t. $b^{-1}b \equiv 1 \bmod a$

- Therefore

$$\frac{1}{a}\sum_{k=1}^{a-1}\frac{1}{\left(1-\xi_a^{bk}\right)\xi_a^{kn}} = -\left\{\frac{b^{-1}n}{a}\right\} + \frac{1}{2} - \frac{1}{2a} \tag{10}$$

Popoviciu's theorem

- Exercise 1.22

$$\frac{1}{a}\sum_{k=1}^{a-1}\frac{1}{\left(1-\xi_a^{bk}\right)\xi_a^{kn}}=\frac{1}{a}\sum_{k=1}^{a-1}\frac{1}{\left(1-\xi_a^{k}\right)\xi_a^{b^{-1}kn}} \tag{9}$$

where b^{-1} is an integer s.t. $b^{-1}b \equiv 1 \bmod a$

- Therefore

$$\frac{1}{a}\sum_{k=1}^{a-1}\frac{1}{\left(1-\xi_a^{bk}\right)\xi_a^{kn}}=-\left\{\frac{b^{-1}n}{a}\right\}+\frac{1}{2}-\frac{1}{2a} \tag{10}$$

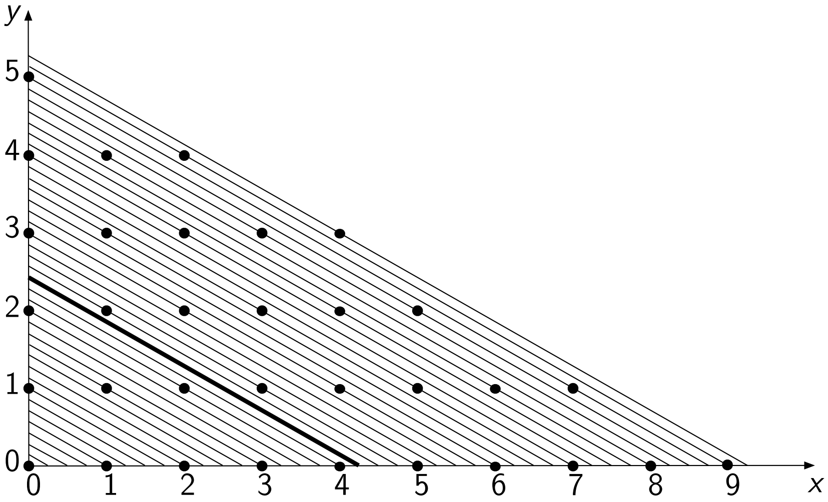
- Combining this with (7) gives the following theorem

Theorem 1.5 (Popoviciu's theorem, 1953)

a, b coprime $\Rightarrow$ $$p_{\{a,b\}}(n)=\frac{n}{ab}-\left\{\frac{b^{-1}n}{a}\right\}-\left\{\frac{a^{-1}n}{b}\right\}+1$$
where $b^{-1}b \equiv 1 \bmod a$, $a^{-1}a \equiv 1 \bmod b$ $\square$

Geometric picture for two coins, again

$A = \{4, 7\}$, the lines $4x + 7y = n$, $n = 1, 2, \ldots$



What we're going to do now

Prove Theorems 1.2 and 1.3 from Theorem 1.5

Theorem 1.2

a_1, a_2 coprime $\Rightarrow g(a_1, a_2) = a_1 a_2 - a_1 - a_2$

Theorem 1.3 (Sylvester's theorem, 1884)

a_1, a_2 coprime $\Rightarrow$ exactly $\dfrac{(a_1-1)(a_2-1)}{2}$ integers are not representable

Theorem 1.5 (Popoviciu's theorem, 1953)

a, b coprime $\Rightarrow$ $p_{\{a,b\}}(n) = \dfrac{n}{ab} - \left\{\dfrac{b^{-1}n}{a}\right\} - \left\{\dfrac{a^{-1}n}{b}\right\} + 1$
where $b^{-1}b \equiv 1 \bmod a$, $a^{-1}a \equiv 1 \bmod b$

We use a lemma

Lemma 1.6

a, b coprime, $n \in [1, ab-1]$, $a \nmid n$, $b \nmid n \Rightarrow$

$$p_{\{a,b\}}(n) + p_{\{a,b\}}(ab-n) = 1$$

We use a lemma

Lemma 1.6

a, b coprime, $n \in [1, ab-1]$, $a \nmid n$, $b \nmid n \Rightarrow$

$$p_{\{a,b\}}(n) + p_{\{a,b\}}(ab-n) = 1$$

Proof: Use Theorem 5

$$p_{\{a,b\}}(ab-n) = \frac{ab-n}{ab} - \left\{ \frac{b^{-1}(ab-n)}{a} \right\} - \left\{ \frac{a^{-1}(ab-n)}{b} \right\} + 1$$

We use a lemma

Lemma 1.6

a, b coprime, $n \in [1, ab-1]$, $a \nmid n$, $b \nmid n \Rightarrow$

$$p_{\{a,b\}}(n) + p_{\{a,b\}}(ab-n) = 1$$

Proof: Use Theorem 5

$$\begin{aligned} p_{\{a,b\}}(ab-n) &= \frac{ab-n}{ab} - \left\{ \frac{b^{-1}(ab-n)}{a} \right\} - \left\{ \frac{a^{-1}(ab-n)}{b} \right\} + 1 \\ &= 2 - \frac{n}{ab} - \left\{ \frac{-b^{-1}n}{a} \right\} - \left\{ \frac{-a^{-1}n}{b} \right\} \end{aligned}$$

We use a lemma

Lemma 1.6

a, b coprime, $n \in [1, ab-1]$, $a \nmid n$, $b \nmid n \Rightarrow$

$$p_{\{a,b\}}(n) + p_{\{a,b\}}(ab-n) = 1$$

<u>Proof</u>: Use Theorem 5

$$\begin{aligned}
p_{\{a,b\}}(ab-n) &= \frac{ab-n}{ab} - \left\{\frac{b^{-1}(ab-n)}{a}\right\} - \left\{\frac{a^{-1}(ab-n)}{b}\right\} + 1 \\
&= 2 - \frac{n}{ab} - \left\{\frac{-b^{-1}n}{a}\right\} - \left\{\frac{-a^{-1}n}{b}\right\} \\
&\overset{(\star)}{=} -\frac{n}{ab} + \left\{\frac{b^{-1}n}{a}\right\} + \left\{\frac{a^{-1}n}{b}\right\}
\end{aligned}$$

$(\star)$ follows by $\{-x\} = 1 - \{x\}$ for $x \notin \mathbb{Z}$

We use a lemma

Lemma 1.6

a, b coprime, $n \in [1, ab-1]$, $a \nmid n$, $b \nmid n \Rightarrow$

$$p_{\{a,b\}}(n) + p_{\{a,b\}}(ab-n) = 1$$

Proof: Use Theorem 5

$$\begin{aligned}
p_{\{a,b\}}(ab-n) &= \frac{ab-n}{ab} - \left\{\frac{b^{-1}(ab-n)}{a}\right\} - \left\{\frac{a^{-1}(ab-n)}{b}\right\} + 1 \\
&= 2 - \frac{n}{ab} - \left\{\frac{-b^{-1}n}{a}\right\} - \left\{\frac{-a^{-1}n}{b}\right\} \\
&\overset{(\star)}{=} -\frac{n}{ab} + \left\{\frac{b^{-1}n}{a}\right\} + \left\{\frac{a^{-1}n}{b}\right\} \\
&= 1 - p_{\{a,b\}}(n)
\end{aligned}$$

$(\star)$ follows by $\{-x\} = 1 - \{x\}$ for $x \notin \mathbb{Z}$

Proof of Theorem 1.2

It suffices to prove the following two

1. $p_{\{a,b\}}(ab-a-b) = 0$ (Exer 1.24 and Lem 1.6)
2. $p_{\{a,b\}}(ab-a-b+n) > 0$ for all $n > 0$

Proof of Theorem 1.2

It suffices to prove the following two

1. $p_{\{a,b\}}(ab-a-b) = 0$ (Exer 1.24 and Lem 1.6)
2. $p_{\{a,b\}}(ab-a-b+n) > 0$ for all $n > 0$

Proof of (2):

- Note $\left\{\frac{m}{a}\right\} \leq 1 - \frac{1}{a}$ for all $m \in \mathbb{Z}$

Proof of Theorem 1.2

It suffices to prove the following two

1. $p_{\{a,b\}}(ab-a-b) = 0$ (Exer 1.24 and Lem 1.6)
2. $p_{\{a,b\}}(ab-a-b+n) > 0$ for all $n > 0$

Proof of (2):

- Note $\left\{\frac{m}{a}\right\} \leq 1 - \frac{1}{a}$ for all $m \in \mathbb{Z}$
- Then

$$p_{\{a,b\}}(ab-a-b+n) \geq \frac{ab-a-b+n}{ab} - \left(1-\frac{1}{a}\right) - \left(1-\frac{1}{b}\right) + 1$$

Proof of Theorem 1.2

It suffices to prove the following two

1. $p_{\{a,b\}}(ab-a-b) = 0$ (Exer 1.24 and Lem 1.6)
2. $p_{\{a,b\}}(ab-a-b+n) > 0$ for all $n > 0$

Proof of (2):

- Note $\left\{\frac{m}{a}\right\} \leq 1 - \frac{1}{a}$ for all $m \in \mathbb{Z}$
- Then

$$p_{\{a,b\}}(ab-a-b+n) \geq \frac{ab-a-b+n}{ab} - \left(1-\frac{1}{a}\right) - \left(1-\frac{1}{b}\right) + 1$$
$$= \frac{n}{ab}$$

Proof of Theorem 1.2

It suffices to prove the following two

1. $p_{\{a,b\}}(ab-a-b) = 0$ (Exer 1.24 and Lem 1.6)
2. $p_{\{a,b\}}(ab-a-b+n) > 0$ for all $n > 0$

Proof of (2):

- Note $\left\{\frac{m}{a}\right\} \leq 1 - \frac{1}{a}$ for all $m \in \mathbb{Z}$
- Then

$$p_{\{a,b\}}(ab-a-b+n) \geq \frac{ab-a-b+n}{ab} - \left(1-\frac{1}{a}\right) - \left(1-\frac{1}{b}\right) + 1$$
$$= \frac{n}{ab} > 0 \quad \square$$

Proof of Theorem 1.3

- Non-representable numbers all in $[1, ab-1]$ (by Thm 1.2)

Proof of Theorem 1.3

- Non-representable numbers all in $[1, ab-1]$ (by Thm 1.2)
- $a|n$ or $b|n \Rightarrow n$ representable

Proof of Theorem 1.3

- Non-representable numbers all in $[1, ab-1]$ (by Thm 1.2)
- $a|n$ or $b|n \Rightarrow n$ representable
- Otherwise, exactly one of n and $ab-n$ is representable (Lem 1.6)

Proof of Theorem 1.3

- Non-representable numbers all in $[1, ab-1]$ (by Thm 1.2)
- $a|n$ or $b|n \Rightarrow n$ representable
- Otherwise, exactly one of n and $ab-n$ is representable (Lem 1.6)
- $\therefore$

$$\#\ \text{non-representable numbers} = \frac{(ab-1)-(b-1)-(a-1)+0}{2}$$

Proof of Theorem 1.3

- Non-representable numbers all in $[1, ab-1]$ (by Thm 1.2)
- $a|n$ or $b|n \Rightarrow n$ representable
- Otherwise, exactly one of n and $ab-n$ is representable (Lem 1.6)
- $\therefore$

$$\begin{aligned}\#\text{ non-representable numbers} &= \frac{(ab-1)-(b-1)-(a-1)+0}{2} \\ &= \frac{(a-1)(b-1)}{2} \quad \square\end{aligned}$$

Three coins

a, b, c coprime (Reminder: $\xi_b = e^{2\pi i/b}$)

$$
\begin{aligned}
p_{\{a,b,c\}}(n) &= \frac{n^2}{2abc} + \frac{n}{2}\left(\frac{1}{ab} + \frac{1}{ac} + \frac{1}{bc}\right) \\
&\quad + \frac{1}{12}\left(\frac{3}{a} + \frac{3}{b} + \frac{3}{c} + \frac{a}{bc} + \frac{b}{ac} + \frac{c}{ab}\right) \\
&\quad + \frac{1}{a}\sum_{k=1}^{a-1} \frac{1}{\left(1-\xi_a^{kb}\right)\left(1-\xi_a^{kc}\right)\xi_a^{kn}} \\
&\quad + \frac{1}{b}\sum_{k=1}^{b-1} \frac{1}{\left(1-\xi_b^{kc}\right)\left(1-\xi_b^{ka}\right)\xi_b^{kn}} \\
&\quad + \frac{1}{c}\sum_{k=1}^{c-1} \frac{1}{\left(1-\xi_c^{ka}\right)\left(1-\xi_c^{kb}\right)\xi_c^{kn}}
\end{aligned}
$$

Fourier–Dedekind sums

Reminder: $\xi_b = e^{2\pi i/b}$

Definition (Fourier–Dedekind sum)

$$s_n(a_1, a_2, \dots, a_m; b) := \frac{1}{b} \sum_{k=1}^{b-1} \frac{\xi_b^{kn}}{\left(1 - \xi_b^{ka_1}\right)\left(1 - \xi_b^{ka_2}\right) \cdots \left(1 - \xi_b^{ka_m}\right)} \tag{13}$$

- Generalizes Dedekind sums (defined in Chapter 7)
- Studied thoroughly (in Chapter 8)

Three coins, rewritten

a, b, c coprime

$$\begin{aligned} p_{\{a,b,c\}}(n) &= \frac{n^2}{2abc} + \frac{n}{2}\left(\frac{1}{ab} + \frac{1}{ac} + \frac{1}{bc}\right) \\ &\quad + \frac{1}{12}\left(\frac{3}{a} + \frac{3}{b} + \frac{3}{c} + \frac{a}{bc} + \frac{b}{ac} + \frac{c}{ab}\right) \\ &\quad + s_{-n}(b, c; a) + s_{-n}(a, c; b) + s_{-n}(a, b; c) \end{aligned}$$

For the derivation, and the extension to more coins, see the textbook

Two coins, revisited

Eq. (7) for two coins

$$\begin{aligned} p_{\{a,b\}}(n) &= \frac{1}{2a} + \frac{1}{2b} + \frac{n}{ab} \\ &\quad + \frac{1}{a}\sum_{k=1}^{a-1} \frac{1}{(1-\xi_a^{kb})\xi_a^{kn}} + \frac{1}{b}\sum_{j=1}^{b-1} \frac{1}{(1-\xi_b^{ja})\xi_b^{jn}} \\ &= \frac{1}{2a} + \frac{1}{2b} + \frac{n}{ab} + s_{-n}(b;a) + s_{-n}(a;b) \end{aligned}$$

Concluding remarks

- Frobenius' coin-exchange problem to see the relation of
  - Combinatorics (generating functions)
  - Geometry (convex polytopes)
  - Number theory (Dedekind sums)
- Lots of problems still remain unsolved

Literature

- J.L. Ramírez-Alfonsín. *The Diophantine Frobenius Problem*. Oxford University Press, 2006.