1

The Coin-Exchange Problem of Frobenius

The full beauty of the subject of generating functions emerges only from tuning in on both channels: the discrete and the continuous.

Herbert Wilf [186]

Suppose we're interested in an infinite sequence of numbers $(a_k)_{k=0}^{\infty}$ that arises geometrically or recursively. Is there a "good formula" for a_k as a function of k? Are there identities involving various a_k's? Embedding this sequence into the **generating function**

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

allows us to retrieve answers to the questions above in a surprisingly quick and elegant way. We can think of $F(z)$ as lifting our sequence a_k from its discrete setting into the continuous world of functions.

1.1 Why Use Generating Functions?

To illustrate these concepts, we warm up with the classic example of the **Fibonacci sequence** f_k, named after Leonardo Pisano Fibonacci (1170–1250?)[1] and defined by the recursion

$$f_0 = 0, \;\; f_1 = 1, \;\; \text{and} \;\; f_{k+2} = f_{k+1} + f_k \;\; \text{for} \;\; k \geq 0 \, .$$

This gives the sequence $(f_k)_{k=0}^{\infty} = (0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \dots)$ (see also [164, Sequence A000045]). Now let's see what generating functions can do for us. Let

[1] For more information about Fibonacci, see
`http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Fibonacci.html`.

$$F(z) = \sum_{k\geq 0} f_k\, z^k.$$

We embed both sides of the recursion identity into their generating functions:

$$\sum_{k\geq 0} f_{k+2}\, z^k = \sum_{k\geq 0} (f_{k+1} + f_k)\, z^k = \sum_{k\geq 0} f_{k+1}\, z^k + \sum_{k\geq 0} f_k\, z^k. \tag{1.1}$$

The left–hand side of (1.1) is

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

while the right–hand side of (1.1) is

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

So (1.1) can be restated as

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

or

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

It's fun to check (e.g., with a computer) that when we expand the function F into a power series, we indeed obtain the Fibonacci numbers as coefficients:

$$\frac{z}{1 - z - z^2} = z + z^2 + 2\,z^3 + 3\,z^4 + 5\,z^5 + 8\,z^6 + 13\,z^7 + 21\,z^8 + 34\,z^9 + \cdots\,.$$

Now we use our favorite method of handling rational functions: the partial fraction expansion. In our case, the denominator factors as $1 - z - z^2 = \left(1 - \frac{1+\sqrt{5}}{2}\, z\right)\left(1 - \frac{1-\sqrt{5}}{2}\, z\right)$, and the partial fraction expansion is (see Exercise 1.1)

$$F(z) = \frac{z}{1 - z - z^2} = \frac{1/\sqrt{5}}{1 - \frac{1+\sqrt{5}}{2}\, z} - \frac{1/\sqrt{5}}{1 - \frac{1-\sqrt{5}}{2}\, z}\,. \tag{1.2}$$

The two terms suggest the use of the **geometric series**

$$\sum_{k\geq 0} x^k = \frac{1}{1 - x} \tag{1.3}$$

(see Exercise 1.2) with $x = \frac{1+\sqrt{5}}{2}\, z$ and $x = \frac{1-\sqrt{5}}{2}\, z$, respectively:

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

Comparing the coefficients of z^k in the definition of $F(z) = \sum_{k\geq 0} f_k\, z^k$ and the new expression above for $F(z)$, we discover the closed form expression for the Fibonacci sequence

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

This method of decomposing a rational generating function into partial fractions is one of our key tools. Because we will use partial fractions time and again throughout this book, we record the result on which this method is based.

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.

One possible proof of this theorem is based on the fact that the polynomials form a Euclidean domain. For readers who are acquainted with this notion, we outline this proof in Exercise 1.35.

1.2 Two Coins

Let's imagine that we introduce a new coin system. Instead of using pennies, nickels, dimes, and quarters, let's say we agree on using 4-cent, 7-cent, 9-cent, and 34-cent coins. The reader might point out the following flaw of this new system: certain amounts cannot be changed (that is, created with the available coins), for example, 2 or 5 cents. On the other hand, this deficiency makes our new coin system more interesting than the old one, because we can ask the question, "which amounts can be changed?" In fact, we will prove in Exercise 1.20 that there are only finitely many integer amounts that *cannot* be changed using our new coin system. A natural question, first tackled by Ferdinand Georg Frobenius (1849–1917),[2] and James Joseph Sylvester (1814–1897)[3] is,

[2] For more information about Frobenius, see `http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Frobenius.html`.

[3] For more information about Sylvester, see `http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Sylvester.html`.

"what is the *largest* amount that cannot be changed?" As mathematicians, we like to keep questions as general as possible, and so we ask, given coins of denominations $a_1, a_2, \ldots, a_d$, which are positive integers without any common factor, can you give a formula for the largest amount that cannot be changed using the coins $a_1, a_2, \ldots, a_d$? This problem is known as the *Frobenius coin-exchange problem*.

To be precise, suppose we're given a set of positive integers

$$A = \{a_1, a_2, \ldots, a_d\}$$

with $\gcd(a_1, a_2, \ldots, a_d) = 1$ and we call an integer n **representable** if there exist nonnegative integers $m_1, m_2, \ldots, m_d$ such that

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

In the language of coins, this means that we can change the amount n using the coins $a_1, a_2, \ldots, a_d$. The Frobenius problem (often called the *linear Diophantine problem of Frobenius*) asks us to find the largest integer that is not representable. We call this largest integer the **Frobenius number** and denote it by $g(a_1, \ldots, a_d)$. The following theorem gives us a pretty formula for $d = 2$.

Theorem 1.2. *If a_1 and a_2 are relatively prime positive integers, then*

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

This simple-looking formula for g inspired a great deal of research into formulas for $g(a_1, a_2, \ldots, a_d)$ with only limited success; see the notes at the end of this chapter. For $d = 2$, Sylvester gave the following result.

Theorem 1.3 (Sylvester's theorem). *Let a_1 and a_2 be relatively prime positive integers. Exactly half of the integers between 1 and $(a_1 - 1)(a_2 - 1)$ are representable.*

Our goal in this chapter is to prove these two theorems (and a little more) using the machinery of partial fractions. We approach the Frobenius problem through the study of the **restricted partition function**

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

the number of partitions of n using only the elements of A as parts.[4] In view of this partition function, $g(a_1, \ldots, a_d)$ is the largest integer n for which $p_A(n) = 0$.

There is a beautiful geometric interpretation of the restricted partition function. The geometric description begins with the set

[4] A **partition** of a positive integer n is a multiset (i.e., a set in which we allow repetition) $\{n_1, n_2, \ldots, n_k\}$ of positive integers such that $n = n_1 + n_2 + \cdots + n_k$. The numbers $n_1, n_2, \ldots, n_k$ are called the **parts** of the partition.

$$\mathcal{P} = \left\{(x_1, \ldots, x_d) \in \mathbb{R}^d : \quad \text{all } x_j \geq 0,\ x_1 a_1 + \cdots + x_d a_d = 1\right\}. \tag{1.4}$$

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

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

The function $p_A(n)$ counts precisely those integer points that lie in the n^{th} integer dilate of the body $\mathcal{P}$. The dilation process in this context is tantamount to replacing $x_1a_1+\cdots+x_da_d = 1$ in the definition of $\mathcal{P}$ by $x_1a_1+\cdots+x_da_d = n$. The set $\mathcal{P}$ turns out to be a *polytope*. We can easily picture $\mathcal{P}$ and its dilates for dimension $d \leq 3$; Figure 1.1 shows the three-dimensional case.

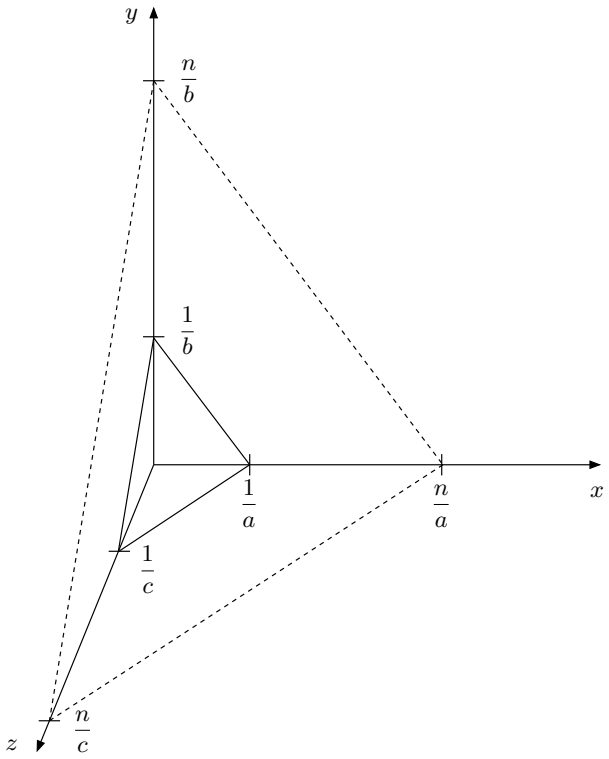

Fig. 1.1. $d = 3$.

1.3 Partial Fractions and a Surprising Formula

We first concentrate on the case $d = 2$ and study

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

Recall that we require a and b to be relatively prime. To begin our discussion, we start playing with generating functions. Consider the product of the following two geometric series:

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

(see Exercise 1.2). If we multiply out all the terms we'll get a power series all of whose exponents are linear combinations of a and b. In fact, the coefficient of z^n in this power series counts the number of ways that n can be written as a nonnegative linear combination of a and b. In other words, these coefficients are precisely evaluations of our counting function $p_{\{a,b\}}$:

$$\left(\frac{1}{1-z^a}\right)\left(\frac{1}{1-z^b}\right) = \sum_{k\geq 0}\sum_{l\geq 0} z^{ak} z^{bl} = \sum_{n\geq 0} p_{\{a,b\}}(n)\, z^n.$$

So this function is the generating function for the sequence of integers $\left(p_{\{a,b\}}(n)\right)_{n=0}^{\infty}$. The idea is now to study the compact function on the left.

We would like to uncover an interesting formula for $p_{\{a,b\}}(n)$ by looking at the generating function on the left more closely. To make our computational life easier, we study the *constant term* of a related series; namely, $p_{\{a,b\}}(n)$ is the constant term of

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

The latter series is not quite a power series, since it includes terms with negative exponents. These series are called *Laurent series*, after Pierre Alphonse Laurent (1813–1854). For a power series (centered at 0), we could simply evaluate the corresponding function at $z = 0$ to obtain the constant term; once we have negative exponents, such an evaluation is not possible. However, if we first subtract all terms with negative exponents, we'll get a power series whose constant term (which remains unchanged) can now be computed by evaluating this remaining function at $z = 0$.

To be able to compute this constant term, we will expand f into partial fractions. As a warm-up to partial fraction decompositions, we first work out a one-dimensional example. Let's denote the first a^{th} root of unity by

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

then all the a^{th} roots of unity are $1, \xi_a, \xi_a^2, \xi_a^3, \ldots, \xi_a^{a-1}$.

Example 1.4. Let's find the partial fraction expansion of $\frac{1}{1-z^a}$. The poles of this function are located at all a^{th} roots of unity ξ_a^k for $k = 0, 1, \ldots, a-1$. So we expand

$$\frac{1}{1-z^a} = \sum_{k=0}^{a-1} \frac{C_k}{z-\xi_a^k}\,.$$

How do we find the coefficients C_k? Well,

$$C_k = \lim_{z\to\xi_a^k} \left(z-\xi_a^k\right)\left(\frac{1}{1-z^a}\right) = \lim_{z\to\xi_a^k} \frac{1}{-a\,z^{a-1}} = -\frac{\xi_a^k}{a}\,,$$

where we have used L'Hôpital's rule in the penultimate equality. Therefore, we arrive at the expansion

$$\frac{1}{1-z^a} = -\frac{1}{a}\sum_{k=0}^{a-1} \frac{\xi_a^k}{z-\xi_a^k}\,. \qquad \square$$

Returning to restricted partitions, the poles of f are located at $z=0$ with multiplicity n, at $z=1$ with multiplicity 2, and at all the other a^{th} and b^{th} roots of unity with multiplicity 1 because a and b are relatively prime. Hence our partial fraction expansion looks like

$$f(z) = \frac{A_1}{z}+\frac{A_2}{z^2}+\cdots+\frac{A_n}{z^n}+\frac{B_1}{z-1}+\frac{B_2}{(z-1)^2}+\sum_{k=1}^{a-1}\frac{C_k}{z-\xi_a^k}+\sum_{j=1}^{b-1}\frac{D_j}{z-\xi_b^j}\,. \quad (1.5)$$

We invite the reader to compute the coefficients (Exercise 1.21)

$$\begin{aligned} C_k &= -\frac{1}{a\left(1-\xi_a^{kb}\right)\xi_a^{k(n-1)}}\,, \\ D_j &= -\frac{1}{b\left(1-\xi_b^{ja}\right)\xi_b^{j(n-1)}}\,. \end{aligned} \quad (1.6)$$

To compute B_2, we multiply both sides of (1.5) by $(z-1)^2$ and take the limit as $z\to 1$ to obtain

$$B_2 = \lim_{z\to 1}\frac{(z-1)^2}{\left(1-z^a\right)\left(1-z^b\right)z^n} = \frac{1}{ab}\,,$$

by applying L'Hôpital's rule twice, for example. For the more interesting constant B_1, we compute

$$B_1 = \lim_{z\to 1}(z-1)\left(\frac{1}{\left(1-z^a\right)\left(1-z^b\right)z^n} - \frac{\frac{1}{ab}}{(z-1)^2}\right) = \frac{1}{ab}-\frac{1}{2a}-\frac{1}{2b}-\frac{n}{ab}\,,$$

again by applying L'Hôpital's rule.

We don't need to compute the coefficients $A_1,\ldots,A_n$, since they contribute only to the terms with negative exponents, which we can safely neglect; these terms do not contribute to the constant term of f. Once we have

the other coefficients, the constant term of the Laurent series of f is—as we said above—the following function evaluated at 0:

$$\begin{aligned} p_{\{a,b\}}(n) &= \left(\frac{B_1}{z-1} + \frac{B_2}{(z-1)^2} + \sum_{k=1}^{a-1} \frac{C_k}{z-\xi_a^k} + \sum_{j=1}^{b-1} \frac{D_j}{z-\xi_b^j} \right) \Bigg|_{z=0} \\ &= -B_1 + B_2 - \sum_{k=1}^{a-1} \frac{C_k}{\xi_a^k} - \sum_{j=1}^{b-1} \frac{D_j}{\xi_b^j} \,. \end{aligned}$$

With (1.6) in hand, this simplifies to

$$p_{\{a,b\}}(n) = \frac{1}{2a} + \frac{1}{2b} + \frac{n}{ab} + \frac{1}{a} \sum_{k=1}^{a-1} \frac{1}{(1-\xi_a^{kb})\,\xi_a^{kn}} + \frac{1}{b} \sum_{j=1}^{b-1} \frac{1}{\left(1-\xi_b^{ja}\right)\xi_b^{jn}} \,. \quad (1.7)$$

Encouraged by this initial success, we now proceed to analyze each sum in (1.7) with the hope of recognizing them as more familiar objects.

For the next step we need to define the **greatest-integer function** $\lfloor x \rfloor$, which denotes the greatest integer less than or equal to x. A close sibling to this function is the **fractional-part function** $\{x\} = x - \lfloor x \rfloor$. To readers not familiar with the functions $\lfloor x \rfloor$ and $\{x\}$ we recommend working through Exercises 1.3–1.5.

What we'll do next is study a special case, namely $b = 1$. This is appealing because $p_{\{a,1\}}(n)$ simply counts integer points in an interval:

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

(See Exercise 1.3.) On the other hand, in (1.7) we just computed a different expression for this function, so that

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

With the help of the fractional-part function $\{x\} = x - \lfloor x \rfloor$, we have derived a formula for the following sum over a^{th} roots of unity:

$$\frac{1}{a} \sum_{k=1}^{a-1} \frac{1}{(1-\xi_a^k)\,\xi_a^{kn}} = -\left\{\frac{n}{a}\right\} + \frac{1}{2} - \frac{1}{2a} \,. \quad (1.8)$$

We're almost there: we invite the reader (Exercise 1.22) to show that

$$\frac{1}{a}\sum_{k=1}^{a-1}\frac{1}{(1-\xi_a^{bk})\,\xi_a^{kn}}=\frac{1}{a}\sum_{k=1}^{a-1}\frac{1}{(1-\xi_a^{k})\,\xi_a^{b^{-1}kn}}\,, \tag{1.9}$$

where b^{-1} is an integer such that $b^{-1}b\equiv 1 \bmod a$, and to conclude that

$$\frac{1}{a}\sum_{k=1}^{a-1}\frac{1}{(1-\xi_a^{bk})\,\xi_a^{kn}}=-\left\{\frac{b^{-1}n}{a}\right\}+\frac{1}{2}-\frac{1}{2a}\,. \tag{1.10}$$

Now all that's left to do is to substitute this expression back into (1.7), which yields the following beautiful formula due to Tiberiu Popoviciu (1906–1975).

Theorem 1.5 (Popoviciu's theorem). *If a and b are relatively prime, then*

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

where $b^{-1}b\equiv 1 \bmod a$ and $a^{-1}a\equiv 1 \bmod b$. □

1.4 Sylvester's Result

Before we apply Theorem 1.5 to obtain the classical Theorems 1.2 and 1.3, we return for a moment to the geometry behind the restricted partition function $p_{\{a,b\}}(n)$. In the two-dimensional case (which is the setting of Theorem 1.5), we are counting integer points $(x,y)\in\mathbb{Z}^2$ on the line segments defined by the constraints

$$ax+by=n\,,\qquad x,y\geq 0\,.$$

As n increases, the line segment gets dilated. It is not too far-fetched (although Exercise 1.13 teaches us to be careful with such statements) to expect that the likelihood for an integer point to lie on the line segment increases with n. In fact, one might even guess that the number of points on the line segment increases linearly with n, since the line segment is a one-dimensional object. Theorem 1.5 quantifies the previous statement in a very precise form: $p_{\{a,b\}}(n)$ has the "leading term" n/ab, and the remaining terms are bounded as functions in n. Figure 1.2 shows the geometry behind the counting function $p_{\{4,7\}}(n)$ for the first few values of n. Note that the thick line segment for $n=17=4\cdot 7-4-7$ is the last one that does not contain any integer point.

Lemma 1.6. *If a and b are relatively prime positive integers and $n\in[1,ab-1]$ is not a multiple of a or b, then*

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

In other words, for n between 1 and $ab-1$ and not divisible by a or b, exactly one of the two integers n and $ab-n$ is representable in terms of a and b.

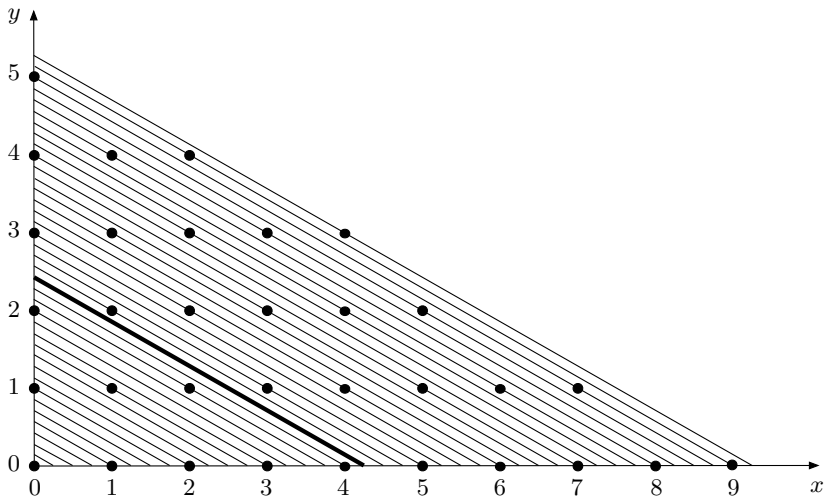

Fig. 1.2. $4x + 7y = n,\ n = 1, 2, \ldots$

Proof. This identity follows directly from Theorem 1.5:

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

Here, $(\star)$ follows from the fact that $\{-x\} = 1 - \{x\}$ if $x \notin \mathbb{Z}$ (see Exercise 1.5). □

Proof of Theorem 1.2. We have to show that $p_{\{a,b\}}(ab-a-b) = 0$ and that $p_{\{a,b\}}(n) > 0$ for every $n > ab-a-b$. The first assertion follows with Exercise 1.24, which states that $p_{\{a,b\}}(a+b) = 1$, and Lemma 1.6. To prove the second assertion, we note that for any integer m, $\left\{\frac{m}{a}\right\} \le 1 - \frac{1}{a}$. Hence for any positive integer n,

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

□

Proof of Theorem 1.3. Recall that Lemma 1.6 states that for n between 1 and $ab-1$ and not divisible by a or b, exactly one of n and $ab-n$ is representable. There are

$$ab - a - b + 1 = (a-1)(b-1)$$

integers between 1 and $ab-1$ that are not divisible by a or b. Finally, we note that $p_{\{a,b\}}(n) > 0$ if n is a multiple of a or b, by the very definition of $p_{\{a,b\}}(n)$. Hence the number of nonrepresentable integers is $\frac{1}{2}(a-1)(b-1)$. □

Note that we have proved even more. Essentially by Lemma 1.6, every positive integer less than ab has at most one representation. Hence, the representable integers less than ab are *uniquely* representable (see also Exercise 1.25).

1.5 Three and More Coins

What happens to the complexity of the Frobenius problem if we have more than two coins? Let's go back to our restricted partition function

$$p_A(n) = \#\left\{(m_1,\dots,m_d)\in\mathbb{Z}^d:\ \text{ all } m_j\ge 0,\ m_1a_1+\cdots+m_da_d=n\right\},$$

where $A=\{a_1,\dots,a_d\}$. By the very same reasoning as in Section 1.3, we can easily write down the generating function for $p_A(n)$:

$$\sum_{n\ge 0} p_A(n)\,z^n = \left(\frac{1}{1-z^{a_1}}\right)\left(\frac{1}{1-z^{a_2}}\right)\cdots\left(\frac{1}{1-z^{a_d}}\right).$$

We use the same methods that were exploited in Section 1.3 to recover our function $p_A(n)$ as the constant term of a useful generating function. Namely,

$$p_A(n) = \operatorname{const}\left(\frac{1}{(1-z^{a_1})\,(1-z^{a_2})\cdots(1-z^{a_d})\,z^n}\right).$$

We now expand the function on the right into partial fractions. For reasons of simplicity we assume in the following that $a_1,\dots,a_d$ are *pairwise* relatively prime; that is, no two of the integers $a_1,a_2,\dots,a_d$ have a common factor. Then our partial fraction expansion looks like

$$\begin{aligned} f(z) &= \frac{1}{(1-z^{a_1})\cdots(1-z^{a_d})\,z^n} \\ &= \frac{A_1}{z}+\frac{A_2}{z^2}+\cdots+\frac{A_n}{z^n}+\frac{B_1}{z-1}+\frac{B_2}{(z-1)^2}+\cdots+\frac{B_d}{(z-1)^d} \\ &\quad+\sum_{k=1}^{a_1-1}\frac{C_{1k}}{z-\xi_{a_1}^k}+\sum_{k=1}^{a_2-1}\frac{C_{2k}}{z-\xi_{a_2}^k}+\cdots+\sum_{k=1}^{a_d-1}\frac{C_{dk}}{z-\xi_{a_d}^k}. \end{aligned} \tag{1.11}$$

By now we're experienced in computing partial fraction coefficients, so that the reader will easily verify that (Exercise 1.29)

$$C_{1k} = -\frac{1}{a_1\left(1-\xi_{a_1}^{ka_2}\right)\left(1-\xi_{a_1}^{ka_3}\right)\cdots\left(1-\xi_{a_1}^{ka_d}\right)\xi_{a_1}^{k(n-1)}}. \tag{1.12}$$

As before, we don't have to compute the coefficients $A_1, \ldots, A_n$, because they don't contribute to the constant term of f. For the computation of $B_1, \ldots, B_d$, we may use a symbolic manipulation program such as `Maple` or `Mathematica`. Again, once we have calculated these coefficients, we can compute the constant term of f by dropping all negative exponents and evaluating the remaining function at 0:

$$\begin{aligned} p_A(n) &= \left(\frac{B_1}{z-1} + \cdots + \frac{B_d}{(z-1)^d} + \sum_{k=1}^{a_1-1} \frac{C_{1k}}{z-\xi_{a_1}^k} + \cdots + \sum_{k=1}^{a_d-1} \frac{C_{dk}}{z-\xi_{a_d}^k} \right) \Bigg|_{z=0} \\ &= -B_1 + B_2 - \cdots + (-1)^d B_d - \sum_{k=1}^{a_1-1} \frac{C_{1k}}{\xi_{a_1}^k} - \sum_{k=1}^{a_2-1} \frac{C_{2k}}{\xi_{a_2}^k} - \cdots - \sum_{k=1}^{a_d-1} \frac{C_{dk}}{\xi_{a_d}^k}. \end{aligned}$$

Substituting the expression we found for C_{1k} into the latter sum over the nontrivial a_1^{th} roots of unity, for example, gives rise to

$$\frac{1}{a_1} \sum_{k=1}^{a_1-1} \frac{1}{\left(1-\xi_{a_1}^{ka_2}\right)\left(1-\xi_{a_1}^{ka_3}\right)\cdots\left(1-\xi_{a_1}^{ka_d}\right)\xi_{a_1}^{kn}}.$$

This motivates the definition of the **Fourier–Dedekind sum**

$$s_n\left(a_1, a_2, \ldots, a_m; b\right) := \frac{1}{b} \sum_{k=1}^{b-1} \frac{\xi_b^{kn}}{\left(1-\xi_b^{ka_1}\right)\left(1-\xi_b^{ka_2}\right)\cdots\left(1-\xi_b^{ka_m}\right)}. \quad (1.13)$$

We will study these sums in detail in Chapter 8. With this definition, we have arrived at the following result.

Theorem 1.7. *The restricted partition function for $A = \{a_1, a_2, \ldots, a_d\}$, where the a_k's are pairwise relatively prime, can be computed as*

$$\begin{aligned} p_A(n) = -B_1 + B_2 - \cdots + (-1)^d B_d &+ s_{-n}\left(a_2, a_3, \ldots, a_d; a_1\right) \\ &+ s_{-n}\left(a_1, a_3, a_4, \ldots, a_d; a_2\right) + \cdots + s_{-n}\left(a_1, a_2, \ldots, a_{d-1}; a_d\right). \end{aligned}$$

Here $B_1, B_2, \ldots, B_d$ are the partial fraction coefficients in the expansion (1.11). □

Example 1.8. We give the restricted partition functions for $d = 3$ and 4. These closed-form formulas have proven useful in the refined analysis of the periodicity that is inherent in the restricted partition function $p_A(n)$. For example, one can visualize the graph of $p_{\{a,b,c\}}(n)$ as a "wavy parabola," as its formula plainly shows.

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

$$p_{\{a,b,c,d\}}(n) = \frac{n^3}{6abcd} + \frac{n^2}{4}\left(\frac{1}{abc}+\frac{1}{abd}+\frac{1}{acd}+\frac{1}{bcd}\right)$$
$$+ \frac{n}{12}\left(\frac{3}{ab}+\frac{3}{ac}+\frac{3}{ad}+\frac{3}{bc}+\frac{3}{bd}+\frac{3}{cd}+\frac{a}{bcd}+\frac{b}{acd}+\frac{c}{abd}+\frac{d}{abc}\right)$$
$$+ \frac{1}{24}\left(\frac{a}{bc}+\frac{a}{bd}+\frac{a}{cd}+\frac{b}{ad}+\frac{b}{ac}+\frac{b}{cd}+\frac{c}{ab}+\frac{c}{ad}+\frac{c}{bd}\right.$$
$$\left.+\frac{d}{ab}+\frac{d}{ac}+\frac{d}{bc}\right) - \frac{1}{8}\left(\frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\frac{1}{d}\right)$$
$$+ \frac{1}{a}\sum_{k=1}^{a-1}\frac{1}{(1-\xi_a^{kb})(1-\xi_a^{kc})(1-\xi_a^{kd})\xi_a^{kn}}$$
$$+ \frac{1}{b}\sum_{k=1}^{b-1}\frac{1}{(1-\xi_b^{kc})(1-\xi_b^{kd})(1-\xi_b^{ka})\xi_b^{kn}}$$
$$+ \frac{1}{c}\sum_{k=1}^{c-1}\frac{1}{(1-\xi_c^{kd})(1-\xi_c^{ka})(1-\xi_c^{kb})\xi_c^{kn}}$$
$$+ \frac{1}{d}\sum_{k=1}^{d-1}\frac{1}{(1-\xi_d^{ka})(1-\xi_d^{kb})(1-\xi_d^{kc})\xi_d^{kn}}. \qquad \square$$

Notes

1. The theory of generating functions has a long and powerful tradition. We only touch on its utility. For those readers who would like to dig a little deeper into the vast generating-function garden, we strongly recommend Herb Wilf's *generatingfunctionology* [186] and László Lovász's *Combinatorial Problems and Exercises* [121]. The reader might wonder why we do not stress convergence aspects of the generating functions we play with. Almost all of our series are geometric series and have trivial convergence properties. In the spirit of not muddying the waters of lucid mathematical exposition, we omit such convergence details.

2. The Frobenius problem is named after Georg Frobenius, who apparently liked to raise this problem in his lectures [40]. Theorem 1.2 is one of the

famous folklore results and might be one of the most misquoted theorems in all of mathematics. People usually cite James J. Sylvester's problem in [176], but his paper contains Theorem 1.3 rather than 1.2. In fact, Sylvester's problem had previously appeared as a theorem in [175]. It is not known who first discovered or proved Theorem 1.2. It is very conceivable that Sylvester knew about it when he came up with Theorem 1.3.

3. The linear Diophantine problem of Frobenius should not be confused with the *postage-stamp problem*. The latter problem asks for a similar determination, but adds an additional independent bound on the size of the integer solutions to the linear equation.

4. Theorem 1.5 has an interesting history. The earliest appearance of this result that we are aware of is in a paper by Tiberiu Popoviciu [147]. Popoviciu's formula has since been resurrected at least twice [160, 182].

5. Fourier–Dedekind sums first surfaced implicitly in Sylvester's work (see, e.g., [174]) and explicitly in connection with restricted partition functions in [103]. They were rediscovered in [25], in connection with the Frobenius problem. The papers [156, 82] contain interesting connections to Bernoulli and Euler polynomials. We will resume the study of the Fourier–Dedekind sums in Chapter 8.

6. As we already mentioned above, the Frobenius problem for $d \geq 3$ is much harder than the case $d = 2$ that we have discussed. Certainly beyond $d = 3$, the Frobenius problem is wide open, though much effort has been put into its study. The literature on the Frobenius problem is vast, and there is still much room for improvement. The interested reader might consult the comprehensive monograph [152], which surveys the references to almost all articles dealing with the Frobenius problem and gives about 40 open problems and conjectures related to the Frobenius problem. To give a flavor, we mention two landmark results that go beyond $d = 2$.

The first one concerns the generating function $r(z) := \sum_{k \in R} z^k$, where R is the set of all integers representable by a given set of relatively prime positive integers $a_1, a_2, \ldots, a_d$. It is not hard to see (Exercise 1.34) that $r(z) = p(z)/\left(1 - z^{a_1}\right)\left(1 - z^{a_2}\right)\cdots\left(1 - z^{a_d}\right)$ for some polynomial p. This rational generating function contains all the information about the Frobenius problem; for example, the Frobenius number is the total degree of the function $\frac{1}{1-z} - r(z)$. Hence the Frobenius problem reduces to finding the polynomial p, the numerator of r. Marcel Morales [133, 134] and Graham Denham [72] discovered the remarkable fact that for $d = 3$, the polynomial p has either 4 or 6 terms. Moreover, they gave semi-explicit formulas for p. The Morales–Denham theorem implies that the Frobenius number in the case $d = 3$ is quickly computable, a result that is originally due, in various disguises, to Jürgen Herzog [94], Harold Greenberg [88], and J. Leslie Davison [64]. As

much as there seems to be a well-defined border between the cases $d = 2$ and $d = 3$, there also seems to be such a border between the cases $d = 3$ and $d = 4$: Henrik Bresinsky [42] proved that for $d \geq 4$, there is no absolute bound for the number of terms in the numerator p, in sharp contrast to the Morales–Denham theorem.

On the other hand, Alexander Barvinok and Kevin Woods [14] proved that for fixed d, the rational generating function $r(z)$ can be written as a "short" sum of rational functions; in particular, r can be efficiently computed when d is fixed. A corollary of this fact is that the Frobenius number can be efficiently computed when d is fixed; this theorem is due to Ravi Kannan [104]. On the other hand, Jorge Ramírez-Alfonsín [151] proved that trying to efficiently compute the Frobenius number is hopeless if d is left as a variable.

While the above results settle the theoretical complexity of the computation of the Frobenius number, practical algorithms are a completely different matter. Both Kannan's and Barvinok–Woods's ideas seem complex enough that nobody has yet tried to implement them. Currently, the fastest algorithm is presented in [32].

Exercises

1.1. ♣ Check the partial fraction expansion (1.2):

$$\frac{z}{1-z-z^2} = \frac{1/\sqrt{5}}{1-\frac{1+\sqrt{5}}{2}\,z} - \frac{1/\sqrt{5}}{1-\frac{1-\sqrt{5}}{2}\,z}\,.$$

1.2. ♣ Suppose z is a complex number, and n is a positive integer. Show that

$$(1-z)\left(1+z+z^2+\cdots+z^n\right) = 1-z^{n+1},$$

and use this to prove that if $|z| < 1$,

$$\sum_{k\geq 0} z^k = \frac{1}{1-z}\,.$$

1.3. ♣ Find a formula for the number of lattice points in $[a, b]$ for arbitrary real numbers a and b.

1.4. Prove the following. Unless stated differently, $n \in \mathbb{Z}$ and $x, y \in \mathbb{R}$.

(a) $\lfloor x+n \rfloor = \lfloor x \rfloor + n$.
(b) $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x+y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$.
(c) $\lfloor x \rfloor + \lfloor -x \rfloor = \begin{cases} 0 & \text{if } x \in \mathbb{Z}, \\ -1 & \text{otherwise.} \end{cases}$
(d) For $n \in \mathbb{Z}_{>0}$, $\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor$.
(e) $-\lfloor -x \rfloor$ is the least integer greater than or equal to x, denoted by $\lceil x \rceil$.

(f) $\lfloor x + 1/2 \rfloor$ is the nearest integer to x (and if two integers are equally near to x, it is the larger of the two).
(g) $\lfloor x \rfloor + \lfloor x + 1/2 \rfloor = \lfloor 2x \rfloor$.
(h) If m and n are positive integers, $\left\lfloor \frac{m}{n} \right\rfloor$ is the number of integers among $1, \ldots, m$ that are divisible by n.
(i) ♣ If $m \in \mathbb{Z}_{>0}, n \in \mathbb{Z}$, then $\left\lfloor \frac{n-1}{m} \right\rfloor = -\left\lfloor \frac{-n}{m} \right\rfloor - 1$.
(j) ♣ If $m \in \mathbb{Z}_{>0}, n \in \mathbb{Z}$, then $\left\lfloor \frac{n-1}{m} \right\rfloor + 1$ is the least integer greater than or equal to n/m.

1.5. Rewrite in terms of the fractional-part function as many of the above identities as you can make sense of.

1.6. Suppose m and n are relatively prime positive integers. Prove that

$$\sum_{k=0}^{m-1} \left\lfloor \frac{kn}{m} \right\rfloor = \sum_{j=0}^{n-1} \left\lfloor \frac{jm}{n} \right\rfloor = \frac{1}{2}(m-1)(n-1)\,.$$

1.7. Prove the following identities. They will become handy at least twice: when we study partial fractions, and when we discuss finite Fourier series. For $\phi, \psi \in \mathbb{R}, n \in \mathbb{Z}_{>0}, m \in \mathbb{Z}$,

(a) $e^{i0} = 1$,
(b) $e^{i\phi}\, e^{i\psi} = e^{i(\phi+\psi)}$,
(c) $1/e^{i\phi} = e^{-i\phi}$,
(d) $e^{i(\phi+2\pi)} = e^{i\phi}$,
(e) $e^{2\pi i} = 1$,
(f) $\left|e^{i\phi}\right| = 1$,
(g) $\frac{d}{d\phi}\, e^{i\phi} = i\, e^{i\phi}$,
(h) $\sum_{k=0}^{n-1} e^{2\pi i k m/n} = \begin{cases} n & \text{if } n|m, \\ 0 & \text{otherwise,} \end{cases}$
(i) $\sum_{k=1}^{n-1} k\, e^{2\pi i k/n} = \frac{n}{e^{2\pi i/n}-1}$.

1.8. Suppose $m, n \in \mathbb{Z}$ and $n > 0$. Find a closed form for $\sum_{k=0}^{n-1} \left\{ \frac{k}{n} \right\} e^{2\pi i k m/n}$ (as a function of m and n).

1.9. ♣ Suppose m and n are relatively prime integers, and n is positive. Show that

$$\left\{ e^{2\pi i m k/n} :\ 0 \le k < n \right\} = \left\{ e^{2\pi i j/n} :\ 0 \le j < n \right\}$$

and

$$\left\{ e^{2\pi i m k/n} :\ 0 < k < n \right\} = \left\{ e^{2\pi i j/n} :\ 0 < j < n \right\}.$$

Conclude that if f is any complex-valued function, then

$$\sum_{k=0}^{n-1} f\left(e^{2\pi i m k/n}\right) = \sum_{j=0}^{n-1} f\left(e^{2\pi i j/n}\right)$$

and

$$\sum_{k=1}^{n-1} f\left(e^{2\pi imk/n}\right) = \sum_{j=1}^{n-1} f\left(e^{2\pi ij/n}\right).$$

1.10. Suppose n is a positive integer. If you know what a *group* is, prove that the set $\left\{e^{2\pi ik/n} : \ 0 \le k < n\right\}$ forms a cyclic group of order n (under multiplication in $\mathbb{C}$).

1.11. Fix $n \in \mathbb{Z}_{>0}$. For an integer m, let $(m \bmod n)$ denote the least nonnegative integer in $G_1 := \mathbb{Z}_n$ to which m is congruent. Let's denote by $\star$ addition modulo n, and by $\circ$ the following composition:

$$\left\{\frac{m_1}{n}\right\} \circ \left\{\frac{m_2}{n}\right\} = \left\{\frac{m_1 + m_2}{n}\right\},$$

defined on the set $G_2 := \left\{\left\{\frac{m}{n}\right\} : \ m \in \mathbb{Z}\right\}$. Define the following functions:

$$\begin{aligned} \phi\left((m \bmod n)\right) &= e^{2\pi im/n}, \\ \psi\left(e^{2\pi im/n}\right) &= \left\{\frac{m}{n}\right\}, \\ \chi\left(\left\{\frac{m}{n}\right\}\right) &= (m \bmod n). \end{aligned}$$

Prove the following:

$$\begin{aligned} \phi\left((m_1 \bmod n) \star (m_2 \bmod n)\right) &= \phi\left((m_1 \bmod n)\right) \phi\left((m_2 \bmod n)\right), \\ \psi\left(e^{2\pi im_1/n} e^{2\pi im_2/n}\right) &= \psi\left(e^{2\pi im_1/n}\right) \circ \psi\left(e^{2\pi im_2/n}\right), \\ \chi\left(\left\{\frac{m_1}{n}\right\} \circ \left\{\frac{m_2}{n}\right\}\right) &= \chi\left(\left\{\frac{m_1}{n}\right\}\right) \star \chi\left(\left\{\frac{m_2}{n}\right\}\right). \end{aligned}$$

Prove that the three maps defined above, namely ϕ, ψ, and χ, are one-to-one. Again, for the reader who is familiar with the notion of a *group*, let G_3 be the group of n^{th} roots of unity. What we have shown is that the three groups G_1, G_2, and G_3 are all isomorphic. It is very useful to cycle among these three isomorphic groups.

1.12. ♣ Given integers a, b, c, d, form the line segment in $\mathbb{R}^2$ joining the point (a, b) to (c, d). Show that the number of integer points on this line segment is $\gcd(a - c, b - d) + 1$.

1.13. Give an example of a line with

(a) no lattice point;
(b) one lattice point;
(c) an infinite number of lattice points.

In each case, state—if appropriate—necessary conditions about the (ir)rationality of the slope.

1.14. Suppose a line $y = mx + b$ passes through the lattice points (p_1, q_1) and (p_2, q_2). Prove that it also passes through the lattice points

$$\big(p_1 + k(p_2 - p_1), q_1 + k(q_2 - q_1)\big),\ k \in \mathbb{Z}\,.$$

1.15. Given positive irrational numbers p and q with $\frac{1}{p} + \frac{1}{q} = 1$, show that $\mathbb{Z}_{>0}$ is the disjoint union of the two integer sequences $\{\lfloor pn \rfloor :\ n \in \mathbb{Z}_{>0}\}$ and $\{\lfloor qn \rfloor :\ n \in \mathbb{Z}_{>0}\}$. This theorem from 1894 is due to Lord Rayleigh and was rediscovered in 1926 by Sam Beatty. Sequences of the form $\{\lfloor pn \rfloor :\ n \in \mathbb{Z}_{>0}\}$ are often called *Beatty sequences*.

1.16. Let $a, b, c, d \in \mathbb{Z}$. We say that $\{(a, b), (c, d)\}$ is a *lattice basis* of $\mathbb{Z}^2$ if any lattice point $(m, n) \in \mathbb{Z}^2$ can be written as

$$(m, n) = p\,(a, b) + q\,(c, d)$$

for some $p, q \in \mathbb{Z}$. Prove that if $\{(a, b), (c, d)\}$ and $\{(e, f), (g, h)\}$ are lattice bases of $\mathbb{Z}^2$ then there exists an integer matrix M with determinant ± 1 such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = M \begin{pmatrix} e & f \\ g & h \end{pmatrix}.$$

Conclude that the determinant of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is ± 1.

1.17. ♣ Prove that a triangle with vertices on the integer lattice has no other interior/boundary lattice points if and only if it has area $\frac{1}{2}$. (*Hint:* You may begin by "doubling" the triangle to form a parallelogram.)

1.18. Let's define a *northeast lattice path* as a path through lattice points that uses only the steps $(1, 0)$ and $(0, 1)$. Let L_n be the line defined by $x + 2y = n$. Prove that the number of northeast lattice paths from the origin to a lattice point on L_n is the $(n+1)^{\text{th}}$ Fibonacci number f_{n+1}.

1.19. Compute the coefficients of the Taylor series of $1/(1 - z)^2$ expanded at $z = 0$

(a) by a counting argument,
(b) by differentiating the geometric series.

Generalize.

1.20. ♣ Prove that if $a_1, a_2, \ldots, a_d \in \mathbb{Z}_{>0}$ do not have a common factor then the Frobenius number $g(a_1, \ldots, a_d)$ is well defined.

1.21. ♣ Compute the partial fraction coefficients (1.6).

1.22. ♣ Prove (1.9): For relatively prime positive integers a and b,

$$\frac{1}{a}\sum_{k=1}^{a-1}\frac{1}{(1-\xi_a^{bk})\,\xi_a^{kn}}=\frac{1}{a}\sum_{k=1}^{a-1}\frac{1}{(1-\xi_a^{k})\,\xi_a^{b^{-1}kn}}\,,$$

where $b^{-1}b\equiv 1 \bmod a$, and deduce from this (1.10), namely,

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

(*Hint:* Use Exercise 1.9.)

1.23. Prove that for relatively prime positive integers a and b,

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

1.24. ♣ Show that if a and b are relatively prime positive integers, then

$$p_{\{a,b\}}(a+b)=1\,.$$

1.25. To extend the Frobenius problem, let us call an integer n *k-representable* if $p_A(n)=k$; that is, n can be represented in exactly k ways using the integers in the set A. Define $g_k=g_k(a_1,\ldots,a_d)$ to be the largest k-representable integer. Prove:

(a) Let $d=2$. For any $k\in\mathbb{Z}_{\geq 0}$ there is an N such that all integers larger than N have at least k representations (and hence $g_k(a,b)$ is well defined).
(b) $g_k(a,b)=(k+1)ab-a-b$.
(c) Given $k\geq 2$, the smallest k-representable integer is $ab(k-1)$.
(d) The smallest interval containing all uniquely representable integers is $[\min(a,b),g_1(a,b)]$.
(e) Given $k\geq 2$, the smallest interval containing all k-representable integers is $[g_{k-2}(a,b)+a+b,g_k(a,b)]$.
(f) There are exactly $ab-1$ integers that are uniquely representable. Given $k\geq 2$, there are exactly ab k-representable integers.
(g) Extend all of this to $d\geq 3$ (see open problems).

1.26. Find a formula for $p_{\{a\}}(n)$.

1.27. Prove the following recursion formula:

$$p_{\{a_1,\ldots,a_d\}}(n)=\sum_{m\geq 0}p_{\{a_1,\ldots,a_{d-1}\}}(n-ma_d)\,.$$

(Here we use the convention that $p_A(n)=0$ if $n<0$.) Use it in the case $d=2$ to give an alternative proof of Theorem 1.2.

1.28. Prove the following extension of Theorem 1.5: Suppose $\gcd(a,b) = d$. Then

$$p_{\{a,b\}}(n) = \begin{cases} \frac{nd}{ab} - \left\{\frac{\beta n}{a}\right\} - \left\{\frac{\alpha n}{b}\right\} + 1 & \text{if } d|n, \\ 0 & \text{otherwise,} \end{cases}$$

where $\beta \frac{b}{d} \equiv 1 \bmod \frac{a}{d}$, and $\alpha \frac{a}{d} \equiv 1 \bmod \frac{b}{d}$.

1.29. ♣ Compute the partial fraction coefficient (1.12).

1.30. Find a formula for $p_{\{a,b,c\}}(n)$ for the case $\gcd(a,b,c) \neq 1$.

1.31. ♣ With $A = \{a_1, a_2, \ldots, a_d\} \subset \mathbb{Z}_{>0}$, let

$$p_A^\circ(n) := \#\left\{(m_1, \ldots, m_d) \in \mathbb{Z}^d : \text{ all } m_j > 0,\ m_1 a_1 + \cdots + m_d a_d = n\right\};$$

that is, $p_A^\circ(n)$ counts the number of partitions of n using only the elements of A as parts, *where each part is used at least once*. Find formulas for p_A° for $A = \{a\}, A = \{a,b\}, A = \{a,b,c\}, A = \{a,b,c,d\}$, where a, b, c, d are pairwise relatively prime positive integers. Observe that in all examples, the counting functions p_A and p_A° satisfy the algebraic relation

$$p_A^\circ(-n) = (-1)^{d-1} p_A(n).$$

1.32. Prove that $p_A^\circ(n) = p_A(n - a_1 - a_2 - \cdots - a_d)$. (Here, as usual, $A = \{a_1, a_2, \ldots, a_d\}$.) Conclude that in the examples of Exercise 1.31 the algebraic relation

$$p_A(-t) = (-1)^{d-1} p_A(t - a_1 - a_2 - \cdots - a_d)$$

holds.

1.33. For relatively prime positive integers a, b, let

$$R := \{am + bn : \ m, n \in \mathbb{Z}_{\geq 0}\},$$

the set of all integers representable by a and b. Prove that

$$\sum_{k \in R} z^k = \frac{1 - z^{ab}}{(1 - z^a)(1 - z^b)}.$$

Use this rational generating function to give alternative proofs of Theorems 1.2 and 1.3.

1.34. For relatively prime positive integers $a_1, a_2, \ldots, a_d$, let

$$R := \{m_1 a_1 + m_2 a_2 + \cdots + m_d a_d : \ m_1, m_2, \ldots, m_d \in \mathbb{Z}_{\geq 0}\},$$

the set of all integers representable by $a_1, a_2, \ldots, a_d$. Prove that

$$r(z) := \sum_{k \in R} z^k = \frac{p(z)}{(1 - z^{a_1})(1 - z^{a_2}) \cdots (1 - z^{a_d})}$$

for some polynomial p.

1.35. Prove Theorem 1.1: Given any rational function $\frac{p(z)}{\prod_{k=1}^{m}(z-a_k)^{e_k}}$, 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

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

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

Here is an outline of one possible proof. Recall that the set of polynomials (over $\mathbb{R}$ or $\mathbb{C}$) forms a *Euclidean domain*, that is, given any two polynomials $a(z), b(z)$, there exist polynomials $q(z), r(z)$ with $\deg(r)<\deg(b)$, such that

$$a(z)=b(z)q(z)+r(z)\,.$$

Applying this procedure repeatedly (the *Euclidean algorithm*) gives the greatest common divisor of $a(z)$ and $b(z)$ as a linear combination of them, that is, there exist polynomials $c(z)$ and $d(z)$ such that $a(z)c(z)+b(z)d(z)=\gcd\left(a(z),b(z)\right)$.

Step 1: Apply the Euclidean algorithm to show that there exist polynomials u_1, u_2 such that

$$u_1(z)\left(z-a_1\right)^{e_1}+u_2(z)\left(z-a_2\right)^{e_2}=1\,.$$

Step 2: Deduce that there exist polynomials v_1, v_2 with $\deg\left(v_k\right)<e_k$ such that

$$\frac{p(z)}{\left(z-a_1\right)^{e_1}\left(z-a_2\right)^{e_2}}=\frac{v_1(z)}{\left(z-a_1\right)^{e_1}}+\frac{v_2(z)}{\left(z-a_2\right)^{e_2}}\,.$$

(*Hint:* Long division.)

Step 3: Repeat this procedure to obtain a partial fraction decomposition for

$$\frac{p(z)}{\left(z-a_1\right)^{e_1}\left(z-a_2\right)^{e_2}\left(z-a_3\right)^{e_3}}\,.$$

Open Problems

1.36. Come up with a new approach or a new algorithm for the Frobenius problem in the $d=4$ case.

1.37. There are a very good lower [64] and several upper bounds [152, Chapter 3] for the Frobenius number. Come up with improved upper bounds.

1.38. Solve Vladimir I. Arnold's Problems 1999-8 through 1999-11 [7]. To give a flavor, we mention two of the problems explicitly:

(a) Explore the statistics of $g(a_1, a_2, \ldots, a_d)$ for typical large $a_1, a_2, \ldots, a_d$. It is conjectured that $g(a_1, a_2, \ldots, a_d)$ grows asymptotically like a constant times $\sqrt[d-1]{a_1 a_2 \cdots a_d}$.
(b) Determine what fraction of the integers in the interval $[0, g(a_1, a_2, \ldots, a_d)]$ is representable, for typical large $a_1, a_2, \ldots, a_d$. It is conjectured that this fraction is asymptotically equal to $\frac{1}{d}$. (Theorem 1.3 implies that this conjecture is true in the case $d = 2$.)

1.39. Study vector generalizations of the Frobenius problem [154, 163].

1.40. There are several special cases of $A = \{a_1, a_2, \ldots, a_d\}$ for which the Frobenius problem is solved, for example, arithmetic sequences [152, Chapter 3]. Study these special cases in light of the generating function $r(x)$, defined in the Notes and in Exercise 1.34.

1.41. Study the generalized Frobenius number g_k (defined in Exercise 1.25), e.g., in light of the Morales–Denham theorem mentioned in the Notes. Derive formulas for special cases, e.g., arithmetic sequences.

1.42. For which $0 \leq n \leq b-1$ is $s_n(a_1, a_2, \ldots, a_d; b) = 0$?

Springer

http://www.springer.com/978-0-387-29139-0

Computing the Continuous Discretely
Integer-point Enumeration in Polyhedra
Beck, M.; Robins, S.
2007, XVIII, 227 p., Hardcover
ISBN: 978-0-387-29139-0