Oakland/East Bay Teacher's Circle – Coins, M&M's, and generating functions

August 2007

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 only 4-cent and 7-cent coins. One might point out the following flaw of this new system: certain amounts cannot be exchanged, for example, 1, 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?" We will see shortly that there are only finitely many integer amounts that *cannot* be exchanged using our new coin system. A natural question, first tackled by Ferdinand Georg Frobenius and James Joseph Sylvester in the 19'th century, is: "what is the *largest* amount that cannot be exchanged?" As mathematicians, we like to keep questions as general as possible, and so we ask: given coins of denominations a and b—positive integers without a common factor—can you give a formula $g(a,b)$ for the largest amount that cannot be exchanged using the coins a and b? This problem and its generalization for coins $a_1, a_2, \ldots, a_n$ is known as the *Frobenius coin-exchange problem.*

To study the Frobenius number $g(a,b)$, we use the *Euclidean Algorithm.* For integers a and b that have no common factor, this algorithm yields integers x and y such that $ax + by = 1$.

(1) Find $g(4,7)$.

(2) Show that $g(5,11) = 39$.

(3) Find x and y such that $4x + 7y = 1$.

(4) Find another x and y such that $4x + 7y = 1$.

(5) Find x and y such that $5x + 11y = 1$.

(6) Find x and y such that $5x + 11y = 39$.

(7) Show that, if t is a given integer, we can always find integers x and y such that $4x + 7y = t$. Generalize to two coins a and b with no common factor.

(8) Show that, if t is a given integer, we can always find integers x and y such that $4x + 7y = t$ and $0 \le x \le 6$. Generalize to two coins a and b with no common factor.

(9) Show that the following recipe for determining whether or not a given amount t can be changed (using the coins 4 and 7) works: Given t, find integers x and y such that $4x + 7y = t$ and $0 \le x \le 6$. Then t can be changed precisely if $y \ge 0$. Generalize to two coins a and b with no common factor.

(10) Use the previous argument to re-compute $g(4,7)$. Generalize your argument to compute $g(a,b)$, for any two coins a and b with no common factor.

(11) Prove that exactly half of the amounts between 1 and $(a-1)(b-1)$ can be changed.

Now it's time for something new. Every infinite sequence $(a_0, a_1, a_2, \dots)$ comes with a handy analytic gadget, namely its *generating function*, which is defined as

$$g(x) = \sum_{k=0}^{\infty} a_k \, x^k .$$

If you know some Analysis (and you don't have to know any Analysis for these exercises), this looks like a power series, however, we don't have to worry about convergence of this series, but rather treat it as a *formal power series*. In the course of the exercises, you will get a feeling for what this means.

(1) Show that $1+x+x^2+x^3+\cdots+x^n = \frac{1-x^{n+1}}{1-x}$ for any number x. Conclude that the *infinite* sum $1+x+x^2+x^3+\cdots = \frac{1}{1-x}$ (if we worry about convergence, we should demand that $|x|<1$). We just computed the generating function for the sequence a_k consisting of all 1's:

$$\sum_{k\ge 0} x^k = \frac{1}{1-x} .$$

Compute the sequence (a_k) that gives rise to the generating function $\sum_{k\ge 0} a_k \, x^k = \left(\frac{1}{1-x}\right)^2$, by looking at the product $\left(1+x+x^2+x^3+\cdots\right)\left(1+x+x^2+x^3+\cdots\right)$. If you look at the result, can you think of a different way to compute (a_k)?

(2) Now we define a sequence recursively. Namely, we set $a_0 = 0$ and $a_{n+1} = 2a_n + 1$ for $n \ge 0$.

(a) Conjecture a formula for a_k by experimenting.

(b) Now put the sequence (a_k) into a generating function $g(x)$ and find a formula for $g(x)$ by utilizing the recursive definition of a_k.

(c) Expand your formula for $g(x)$ into partial fractions, and use the result to prove your conjectured formula for a_k.

(3) We define a second recursive sequence by setting $a_0 = 1$ and $a_{n+1} = 2a_n + n$ for $n \ge 0$. Find a formula for a_k.

It's time to go back to the Frobenius problem. Let us introduce the counting sequence

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

In words, r_k counts the representations of $k \in \mathbb{Z}_{\ge 0}$ as nonnegative linear combinations of a and b. Thus, $r_{ab-a-b} = 0$, and $ab-a-b$ is the largest integer k for which $r_k = 0$.

(1) Prove that $r_{k+ab} = r_k + 1$.

(2) Compute the generating function for the sequence

$$a_k = \begin{cases} 1 & \text{if } k \text{ is a multiple of 7,} \\ 0 & \text{otherwise.} \end{cases}$$

(3) Prove that, for $r_k = \# \left\{ (m,n) \in \mathbb{Z}^2 : \ m,n \geq 0, \ ma + nb = k \right\}$,

$$\sum_{k \geq 0} r_k \, x^k = \left(\frac{1}{1-x^a} \right) \left(\frac{1}{1-x^b} \right) .$$

(4) Now let $s_k = \begin{cases} 1 & \text{if } k \text{ can be changed,} \\ 0 & \text{otherwise.} \end{cases}$ Prove that

$$\sum_{k \geq 0} s_k \, x^k = \frac{1 - x^{ab}}{(1-x^a)(1-x^b)} .$$

A few remarks

The simple-looking formula for $g(a,b)$ that you have found inspired a great deal of research into formulas for the general Frobenius number $g\left(a_1, a_2, \dots, a_d\right)$, with limited success: While it is safe to assume that the formula for $g(a,b)$ has been known for more than a century, no analogous formula exists for $d \geq 3$. The case $d = 3$ is solved algorithmically, i.e., there are efficient algorithms to compute $g(a,b,c)$, and in form of a semi-explicit formula. The Frobenius problem for fixed $d \geq 4$ has been proved to be computationally feasible, but no efficient practical algorithm for $d = 4$ is known.

A second classic theorem for the case $d = 2$, which you have proved and Sylvester published as a math problem in the *Educational Times* more than a century ago [2], says that exactly half of the amounts between 1 and $(a-1)(b-1)$ cannot be changed using the coins a and b.

For more, we refer to a research monograph on the Frobenius problem [1]; it includes more than 400 references to articles written about the Frobenius problem.

References

[1] Jorge L. Ramírez-Alfonsín, *The Diophantine Frobenius problem*, Oxford University Press, Oxford, 2006.

[2] James J. Sylvester, *Mathematical questions with their solutions*, Educational Times **41** (1884), 171–178.