

A REMARK RELATED TO THE FROBENIUS PROBLEM

Tom C. Brown

Simon Fraser University, Burnaby, B.C., Canada V5A 1S6

Peter Jau-shyong Shiue

University of Nevada, Las Vegas, NV 89154-4020

(Submitted March 1991)

The Frobenius problem [2; 3] is to find, for a given set a_1, \dots, a_m of relatively prime integers, the largest number which is **not** a linear combination of a_1, \dots, a_m with nonnegative integer coefficients.

Given a set a_1, \dots, a_m of relatively prime positive integers, let us agree to call a number *representable* if it is a linear combination of a_1, \dots, a_m with nonnegative integer coefficients; otherwise, we call it *nonrepresentable*.

The fact that every sufficiently large positive integer is representable (given relatively prime a_1, \dots, a_m) has been rediscovered many times, and makes a good exercise in a course in elementary number theory.

The Frobenius problem has a long history. (See [7] for a list of references.) In 1884, J. J. Sylvester [8] completely solved the problem for $m = 2$. He found that if a and b are positive integers such that $(a, b) = 1$, then every $n \geq (a-1)(b-1)$ can be expressed in the form $n = xa + by$ where x, y are nonnegative integers, and $ab - a - b$ cannot be so expressed. That is, the largest nonrepresentable number in this case is $ab - a - b$. Sylvester also found that among the $(a-1)(b-1)$ numbers $0, 1, 2, \dots, ab - a - b$, exactly half are representable and half are nonrepresentable.

When $m = 3$, no closed-form expression for the largest nonrepresentable number is known (except in some special cases), although there do exist explicit algorithms for calculating it.

In the general case, various upper bounds are known for the largest nonrepresentable number, and closed-form expressions are known in a few special cases, for example, in the case that a_1, \dots, a_m are in arithmetic progression [1; 6].

In this note we consider an aspect of the case $m = 2$ which seems not to have been examined previously. We start by defining two notations.

For given a, b with $(a, b) = 1$, let $\text{NR}(a, b)$ denote the *set* of numbers nonrepresentable in terms of a, b . Thus, $\text{NR}(a, b)$ is the set of all those nonnegative integers n which *cannot* be expressed in the form $n = xa + by$, where x, y are nonnegative integers. Let

$$S(a, b) = \sum \{n : n \in \text{NR}(a, b)\}$$

equal the *sum* of the numbers nonrepresentable in terms of a and b .

Although Sylvester showed that exactly $\frac{1}{2}(a-1)(b-1)$ of the numbers $0, 1, 2, \dots, ab - a - b$ are nonrepresentable, that is that

$$|\text{NR}(a, b)| = \frac{1}{2}(a-1)(b-1),$$

additional information about the nonrepresentable numbers would be provided by an estimate of their sum $S(a, b) = \sum\{n : n \in \text{NR}(a, b)\}$.

A crude upper bound for $S(a, b)$ is obtained by taking the sum of the $\frac{1}{2}(a-1)(b-1)$ largest integers in the interval $[0, ab-a-b]$. Similarly, a crude lower bound is obtained by taking the sum of the $\frac{1}{2}(a-1)(b-1)$ smallest integers in the interval $[0, ab-a-b]$. This gives

$$\frac{1}{8}(a-1)^2(b-1)^2 - \frac{1}{4}(a-1)(b-1) \leq S(a, b) \leq \frac{3}{8}(a-1)^2(b-1)^2 - \frac{1}{4}(a-1)(b-1),$$

an upper bound of order $\frac{3}{8}(ab)^2$ and a lower bound of order $\frac{1}{8}(ab)^2$.

C. W. Ho, J. L. Parish, & P. J. Shiue [4] found that if A is any finite set of nonnegative integers such that the complement of A (in the set of nonnegative integers) is closed under addition, then $\sum\{n : n \in A\} \leq |A|^2$. Since the sum of two representable numbers is certainly a representable number, we can take $\text{NR}(a, b)$ in the place of A , and obtain

$$S(a, b) = \sum\{n : n \in \text{NR}(a, b)\} \leq |\text{NR}(a, b)|^2 = \frac{1}{4}(a-1)^2(b-1)^2$$

an upper bound for $S(a, b)$ of order $\frac{1}{4}(ab)^2$, which considerably improves the previous upper bound.

In this note we find that, in fact,

$$S(a, b) = \frac{1}{12}(a-1)(b-1)(2ab-a-b-1),$$

so that the exact order of $S(a, b)$ is $\frac{1}{6}(ab)^2$.

For example, when $a = 4$, $b = 7$, the nonrepresentable numbers are 1, 2, 3, 5, 6, 9, 10, 13, and 17, which sum to

$$S(4, 7) = 66 = \frac{1}{12}(4-1)(7-1)(56-4-7-1).$$

For the remainder of the paper, a, b are fixed positive integers with $(a, b) = 1$.

To calculate $S(a, b)$, we use the following idea:

For each $n \geq 0$, let $r(n)$ be the number of representations of n in the form $n = sa + tb$, where s, t are nonnegative integers. That is, $r(n)$ is the number of ordered pairs (s, t) such that $n = sa + tb$.

For example, $r(ab) = 2$, since if $ab = sa + tb$, then $(a, b) = 1$ implies that a divides t and b divides s , so that the only possibilities for (s, t) are $(b, 0)$ and $(0, a)$.

It is not hard to see that if $0 \leq n \leq ab-1$, then either $r(n) = 0$ or $r(n) = 1$. For suppose that $r(n) \geq 2$ and that $n = s_1a + t_1b = s_2a + t_2b$ where (without loss of generality) $s_1 > s_2$. Then $0 = (s_1 - s_2)a + (t_1 - t_2)b$. Therefore, b divides $s_1 - s_2$, so $s_1 \geq b$ and $n \geq ab$.

Now, we define

$$f(x) = \sum_{n=0}^{ab-a-b} [1 - r(n)]x^n.$$

Using the fact that $r(n) = 0$ or $r(n) = 1$ for $0 \leq n \leq ab-1$, we obtain

$$\begin{aligned} f'(1) &= \sum_{n=1}^{ab-a-b} n[1-r(n)] = \sum\{n : 1 \leq n \leq ab-a-b \text{ and } r(n) = 0\} \\ &= \sum\{n : n \in \text{NR}(a,b)\} = S(a,b). \end{aligned}$$

Thus, the problem of finding $S(a,b)$ has been reduced to calculating $f'(1)$. It will turn out that

$$f(x) = \frac{P(x)-1}{x-1}, \text{ where } P(x) = \frac{(x^{ab}-1)(x-1)}{(x^a-1)(x^b-1)}.$$

This remarkably simple formula for $f(x)$ was discovered by Ali Ozluk, and appears in a more general setting (using a_1, \dots, a_m instead of a, b) in a paper by Ozluk & Sertoz [5]. For our case of $m = 2$, the calculations can be done as follows.

Let

$$A(x) = 1/(1-x^a)(1-x^b) = \left(\sum_{n=0}^{\infty} x^{an} \right) \left(\sum_{n=0}^{\infty} x^{bn} \right) = \sum_{n=0}^{\infty} r(n)x^n.$$

Now, since $(a,b) = 1$, it follows that

$$P(x) = \frac{(x^{ab}-1)(x-1)}{(x^a-1)(x^b-1)}$$

is a polynomial, with leading coefficient 1. (This can be seen by factoring both the numerator and denominator into complex linear factors. Since $(a,b) = 1$, there are integers s, t such that $as+bt = 1$. Let ζ be any complex number such that both $\zeta^a = 1$ and $\zeta^b = 1$; then $\zeta = \zeta^1 = \zeta^{as+bt} = (\zeta^a)^s (\zeta^b)^t = 1$. In other words, no linear factor [except for $(x-1)$] appears twice in the denominator of $P(x)$; hence, every linear factor in the denominator cancels against a linear factor in the numerator.)

Since $P(1) = 1$ by L'Hospital's rule, we have that $\frac{P(x)-1}{x-1}$ is also a polynomial, of degree $ab-a-b$, with leading coefficient 1.

Now we write,

$$\begin{aligned} \frac{P(x)-1}{x-1} &= \frac{P(x)}{x-1} + \frac{1}{1-x} = (x^{ab}-1)A(x) + \frac{1}{1-x} \\ &= \sum_{n=0}^{\infty} r(n)x^{ab+n} + \sum_{n=0}^{\infty} [1-r(n)]x^n \\ &= \sum_{n=ab}^{\infty} [r(n-ab)+1-r(n)]x^n + \sum_{n=0}^{ab-1} [1-r(n)]x^n. \end{aligned}$$

Since we know that this power series is really a polynomial of degree $ab-a-b$ with leading coefficient 1, we can deduce that the power series coefficient of the $(ab-a-b)^{\text{th}}$ term is 1, and all later power series coefficients are zero. [Therefore, in particular, $r(ab-a-b) = 0$, $r(n) = 1$ for $ab-a-b < n \leq ab-1$, and $r(n) = r(n-ab) + 1$ for $n \geq ab$, although we do not use these facts in what follows.]

Thus, we now have

$$\frac{P(x)-1}{x-1} = \sum_{n=0}^{ab-a-b} [1-r(n)]x^n = f(x)$$

We now proceed to calculate $f'(1)$. Let $y = x^a$. Then

$$P(x) = \frac{(x^{ab}-1)(x-1)}{(x^a-1)(x^b-1)} = \sum_{k=0}^{b-1} y^k / \sum_{k=0}^{b-1} x^k$$

and

$$f(x) = \frac{P(x)-1}{x-1} = \frac{\sum_{k=0}^{b-1} y^k - \sum_{k=0}^{b-1} x^k}{(x-1)\sum_{k=0}^{b-1} x^k} = \frac{\sum_{k=1}^{b-1} \frac{y^k - x^k}{x-1}}{\sum_{k=0}^{b-1} x^k} = \frac{g(x)}{h(x)},$$

where

$$g(x) = \sum_{k=1}^{b-1} \frac{y^k - x^k}{x-1}, \quad h(x) = \sum_{k=0}^{b-1} x^k.$$

Now we use

$$\frac{y^k - x^k}{x-1} = \frac{x^{ak} - x^k}{x-1} = (x^k + x^{k+1} + \dots + x^{ak-1})$$

to get

$$g(x) = \sum_{k=1}^{b-1} (x^k + x^{k+1} + \dots + x^{ak-1}).$$

Then,

$$g(1) = \sum_{k=1}^{b-1} (a-1)k = \frac{1}{2}(a-1)(b-1)b, \quad h(1) = b, \quad h'(1) = \frac{1}{2}b(b-1).$$

Using the fact that

$$k + (k+1) + \dots + (ka-1) = \frac{1}{2}ka(ka-1) - \frac{1}{2}k(k-1) = \frac{1}{2}(k^2(a^2-1) - k(a-1)),$$

we get that

$$\begin{aligned} g'(1) &= \sum_{k=1}^{b-1} (k + (k+1) + \dots + (ka-1)) = \sum_{k=1}^{b-1} \frac{1}{2}(k^2(a^2-1) - k(a-1)) \\ &= \frac{1}{2}(a^2-1) \sum_{k=1}^{b-1} k^2 - \frac{1}{2}(a-1) \sum_{k=1}^{b-1} k = \frac{1}{2}(a^2-1) \frac{1}{6}(b-1)b(2b-1) - \frac{1}{2}(a-1) \frac{1}{2}(b-1)b \\ &= b(a-1)(b-1) \left(\frac{(a+1)(2b-1)}{12} - \frac{1}{4} \right). \end{aligned}$$

Finally, we get

$$S(a,b) = f'(1) = \frac{h(1)g'(1) - g(1)h'(1)}{(h(1))^2} = \frac{1}{12}(a-1)(b-1)(2ab - a - b - 1).$$

REFERENCES

1. P. T. Bateman. "Remark on a Recent Note on Linear Forms." *Amer Math. Monthly* **65** (1958):517-18.
2. A. Brauer. "On a Problem of Partitions." *Amer. J. Math.* **64** (1942):299-312.
3. G. Frobenius. "Über Matrizen aus nicht negative Elementen." *S.B. Preuss. Akad. Wiss. Berlin* (1912):456-77.
4. C. W. Ho, J. L. Parish, & P. J. Shiue. "On the Sizes of Elements in the Complement of a Submonoid of Integers." *Proceedings of the Fourth International Conference on Fibonacci Numbers and Their Applications*, 1991, pp. 139-44.
5. A. Ozluk & S. Sertoz. "On a Diophantine Problem of Frobenius." *Bull. Tech. Univ. Istanbul*. (To appear.)
6. J. B. Roberts. "On a Diophantine Problem." *Canad. J. Math.* **9** (1957):219-22.
7. E. S. Selmer. "On the Linear Diophantine Problem of Frobenius." *J. Reine Angew. Math.* **293/4** (1977):1-17.
8. J. J. Sylvester. "Mathematical Questions with Their Solutions." *Educational Times* **41** (1884):21.

AMS Classification Numbers: 10B55, 10A99

