The Frobenius Number

Exploring The World Of Non-representable Integers

Péter Suhajda

Bachelor's thesis
2024:K3

Lund University

Faculty of Science
Centre for Mathematical Sciences
Mathematics

Centrum Scientiarum Mathematicarum

Abstract

We call a number *representable* by some given integers $a_1, \ldots, a_n$, if the number can be expressed as a linear combination of $a_1, \ldots, a_n$ with non-negative coefficients. This thesis explores the properties of *non-representable* numbers, with the main focus on the greatest such number called the Frobenius number, denoted by $g(a_1, \ldots, a_n)$. We derive a simple formula when $n = 2$ for the Frobenius number, and for the number and sum of non-representable numbers. Furthermore, for $n = 3$, we give exact formulae for some generalizations, and discuss the author's proposed corrected version of Tripathi's formula for the arbitrary case $g(a, b, c)$.

Popular Summary

Imagine that you and your friends decided to go to a local fast food restaurant. After some discussion, you arrive at the conclusion that together you would like to order and eat 43 chicken nuggets. The nuggets come in 3 sizes: a box of 6, 9 and 20 pieces. Since you are the mathematician of the group, you are given the great honor to do the math and place the order in the self-service machine. After some thought, you can get $42 = 1 \cdot 6 + 4 \cdot 9$ and $44 = 4 \cdot 6 + 1 \cdot 20$, but nothing seems to work for 43... Can it really be so? It turns out that 43 is the largest number that cannot be constructed with any multiples of 6, 9 and 20, which is what we call the Frobenius number (for $6, 9$ and 20). You start to think: Is this unique? Does this always happen? Is there always a largest number? Is there a formula for calculating this largest number?

This and other questions are explored in this thesis, with a surprising twist at the end. At first glance, this knowledge does not seem to be more than just a way to mess with a fast food restaurant employee, however, looking more deeply into the nature of this simple first-grade addition problem, many interesting patterns pop up. We explore not only the existence of the Frobenius number, but also the way we can easily calculate it for two chosen numbers, and not so easily calculate it for three. What about the other numbers that cannot be represented? Good question, look no further than Chapter 3, where we derive the formula for the amount of such numbers, and the formula for their sum.

Interestingly, we could approach this problem from the other way around as well: let us say you choose your favourite number, is there a double or triple for which your chosen number is the Frobenius number? The answer is yes! This and other interesting formulae are presented in Chapter 4, but unchartered territory awaits us at the end...

The Frobenius Formula for Three Numbers! In the final chapter, we discuss this with our focus on Tripathi's 2017 paper. However, the twist that I mentioned earlier is that computational evidence indicates that some of his proposed solutions are incorrect. We end this chapter with some computer-based predictions for corrected versions of Tripathi's results. Additionally, an algorithm is also presented at the end in order to enable one to double check their calculations.

And now, dear reader, you can go ahead and tell your friends more about why they should maybe consider getting more Chicken Nuggets the next time you are hungry...

Acknowledgements

I hereby would like to express my utmost and profound gratitude towards all the people that have helped me during the creation of my thesis, but in particular:

I would like to thank my boyfriend, Arlen, for his patient assistance in helping me manage my time effectively and constantly encouraging me to reach my full potential. I would like to thank my supervisor, Anitha, for her incredible diligence, amiable attitude and passion for Mathematics that has definitely flowed over to me, strengthening my motivation and joy in scientific writing. I would like to thank my close friends for always being there for me through thick and thin, and for relentlessly providing a sound basis for rationale and logic. I must also thank my mother, whom I left in her home country to pursue my dreams in Sweden, yet she never stopped supporting me during both emotionally and financially daring times.

Contents

1. Introduction

1.1 Overview

In this thesis, we are going to discuss the Frobenius Number Problem for a varying number of arbitrary integers and also explore some related concepts regarding non-representable numbers. Chapter 1 introduces the problem with a concrete example, gives the definition of the Frobenius number and then a quick overview of the history of the Frobenius Number Problem.

In Chapter 2, we are going to make sure that the Frobenius number is actually well defined for all integers. This is going to be achieved by giving two proofs, one by Kifer [7] and one by the author. This chapter also features an alternative definition, which we are going to rely on throughout this whole thesis. We also give three separate proofs of the Frobenius number of two arbitrary integers, once again featuring a proof from the author. The other two proofs by Ramírez Alfonsín [9] are included, since they tackle the problem from different perspectives and use clever ideas that are worth exploring, such as Pick's Theorem.

Chapter 3 features two natural continuations of studying the Frobenius numbers after finding the formula for two variables. One of them is about how many non-representable numbers there are for any chosen two integers, and the other one is what their sum is. These questions are going to be presented with the help of Kifer [7] and Brown & Shiue [3] respectively, with the addition of Tripathi's [18] alternative definition of the sum of non-representable numbers.

Chapter 4 goes further by considering the Frobenius problem with three integers. It introduces Johnson's theorem [6] that simplifies the number of triplets one needs to consider from being coprime to being pairwise coprime. This chapter also gives the theorem of Rosales, García-Sánchez and García-García [12], which states that for any number N, there exists an integer triple for which N is the Frobenius number. In other words, if the Frobenius problem is thought of as a map from a triple to an integer, then this mapping is surjective. Moreover, this chapter also covers formulae for some important generalizations subject to certain conditions, namely when the integers follow an arithmetic sequence, the formula for the triple (a^2, a^2+1, a^2+a) for some $a > 2$, and the formula for the case when a divides $b+c$ for some coprimes $a, b, c > 1$.

There has been a recent development in 2017, provided by Tripathi [19], where he proved that there are several formulae based on certain conditions that actually cover all possible triples. This is covered in Chapter 5, together with the fact that unfortunately, computational data seems to indicate a discrepancy in Tripathi's results. We provide an account of Tripathi's ideas, and we highlight the place where the first discrepancy occurs by showcasing an example, for which Tripathi's proposed formula fails, but the author's amendments show potential to give the correct result.

1.2 Definition and brief history of the Frobenius number

Let us consider the following situation: You and your friends decided to go to a local fast food restaurant. After some discussion, you have arrived at the conclusion that together you would like to order and eat 43 chicken nuggets. The nuggets come in 3 sizes: a box of 6, 9 and 20 pieces. Since you are the mathematician of the group, they ask you to do the math and place the order in the self-service machine. After some thought, it seems like this is not possible. Can it really be so? You can get $42 = 1 \cdot 6 + 4 \cdot 9$ and $44 = 4 \cdot 6 + 1 \cdot 20$, but nothing seems to work for 43 ... It turns out that 43 is the largest number that cannot be constructed with any multiples of 6, 9 and 20. You start to think: Is this unique? Does this always happen? Is there always a largest number? Is there a formula for calculating this largest number?

These questions and more came up to me personally after being introduced to this problem even before starting university. The original video that grabbed my attention was a YouTube video uploaded

in 2012 by the channel Numberphile titled *How to order 43 Chicken McNuggets - Numberphile* [8].

A similar famous problem is the money-changing problem, which asks the question:

> "Given n coins of denomination $(a_1, \ldots, a_n)$ with $\gcd(a_1, \ldots, a_n) = 1$, what is the largest integer amount of money for which change cannot be made with these coins?"

The answer to this and the previous question is called the Frobenius number. More formally,

Definition 1.1. Let $a_1, \ldots, a_n$ be positive integers with $\gcd(a_1, \ldots, a_n) = 1$. The *Frobenius number* $g(a_1, \ldots, a_n)$ is the largest integer N such that the equation

$$\sum_{i=1}^{n} a_i x_i = N \tag{1.1}$$

has no solutions for $x_1, \ldots, x_n$ non-negative integers.

Remark 1.2. Without loss of generality, from now on we are going to assume that $a < b < c < \cdots$ for when we write $g(a, b, c, \ldots)$.

It is essential that all numbers are coprime because if $\gcd(a_1, \ldots, a_n) = d$, then every positive integer $d \nmid N$ will be impossible to be represented as an integer combination of $a_1, \ldots, a_n$, and as such, the Frobenius number does not exist since there is no largest integer N to satisfy the definition. For a simple example, take the numbers 2,4 and 6. Clearly, one cannot construct any odd number using only these three numbers.

This problem originally came from J.J. Sylvester (1814–1897), who first published this problem in 1884 [15]. The paper tackles the case when $n = 2$ and gives an explicit formula for it, which we will discuss in the coming chapter. Although it was Sylvester that first wrote about this restricted Diophantine problem (*Note: The Frobenius Problem is essentially a Diophantine equation where the coefficients are restricted to being only non-negative numbers*), its name is, however, associated to Ferdinant Georg Frobenius (1849–1917). Even though Frobenius has contributed numerous times to the theory of elliptic functions, differential equations, number theory and group theory, this problem was named after him merely because he popularised this problem during his lectures, not because he made any significant advances in the topic.

Ever since the topic was introduced, nobody succeeded in finding a way to calculate the Frobenius number for any arbitrary 3 numbers. It has been proven by Curtis [4] that the Frobenius number cannot be given by "closed" formulae of a certain type. Brauer [1] found the Frobenius number for consecutive integers, Roberts [10] extended this result to numbers in arithmetic progression, and Selmer [13] further generalized this to the determination of $g(a, ha + d, ha + 2d, \ldots, ha + nd)$. As a result of its complexity, research was mostly focused on finding efficient algorithms to find the Frobenius numbers, alongside with finding lower and upper bounds. The most notable early exploration of an algorithm for the Frobenius problem for three variables was given by Rødseth [11] in 1978. In 2017, Tripathi [19] published a paper where he presents several exact formulae for $g(a, b, c)$ for all choices of the variables, however, in this thesis it is going to be shown that there are some formulae that do not work.

Current research also concerns itself with the number of non-representable numbers, which is denoted by $n(a_1, \ldots, a_n)$, and by looking at special cases of the Frobenius number for 4 variables.

2. Frobenius number when $n = 2$

This chapter is dedicated to investigating the Frobenius Number Problem for the least amount of integers that it makes sense for. Trivially, $g(a)$ cannot be defined since there are infinitely many integers that do not equal a multiple of a. Therefore the smallest n we can start with is $n = 2$. In Section 2.1, we are going to make sure that the Frobenius number is actually well defined for all integers. This is going to be achieved by giving two proofs, one by Kifer [7] and one by the author. This section also features an alternative definition, which we are going to rely on throughout this whole thesis. In Section 2.2, we give three separate proofs of the Frobenius number for two integers, once again featuring a proof from the author. The other two proofs are included since they tackle the problem from different perspectives and use clever ideas that are worth exploring.

2.1 Proof of existence

To start off, let us define what it means for an integer to be representable.

Definition 2.1. We say that a number N is *representable* by $a_1, \ldots, a_n$ if there exists some representation of N such that $N = a_1x_1 + a_2x_2 + \cdots + a_nx_n$ for some non-negative integers $x_1, \ldots, x_n$.

Theorem 2.2. *For all $n \geq 2$, the Frobenius number $g(a_1, \ldots, a_n)$ is well defined.*

First proof of Theorem 2.2. Given $a_1, \ldots, a_n$ with $\gcd(a_1, \ldots, a_n) = 1$, the extended Euclidean algorithm gives that there exist integers $k_1, \ldots, k_n \in \mathbb{Z}$, such that

$$a_1k_1 + a_2k_2 + \cdots + a_nk_n = 1.$$

We collect the negative and non-negative coefficients on the left and right side respectively. Then we get

$$a_{i_1}k_{i_1} + a_{i_2}k_{i_2} + \cdots + a_{i_\alpha}k_{i_\alpha} + a_{i_{\alpha+1}}k_{i_{\alpha+1}} + \cdots + a_{i_n}k_{i_n} = 1, \tag{2.1}$$

where $i_1, \ldots, i_\alpha$ are the indices of the negative coefficients and $i_{\alpha+1}, \ldots, i_n$ are the indices of the positive and zero coefficients. It is worth noting that if α is 0, then this means that there are no negative coefficients, which can only happen if one of the a_i's and its coefficient is 1 and every other coefficient is 0 since all a_i are non-negative then. Now let

$$x = -(a_{i_1} - 1)(a_{i_1}k_{i_1} + \cdots + a_{i_\alpha}k_{i_\alpha}).$$

Note that x is representable since $k_{i_1}, \ldots, k_{i_\alpha}$ are all negative coefficients and the whole expression is multiplied by a negative number, thus satisfying Definition 2.1. Also note that a_{i_1} being 1 is not an issue since $x = 0$ is trivially representable with coefficients of 0. Now we can create a list of other representable numbers in the following way: Take x and add Equation (2.1) to it, yielding $x + 1$. We can repeat this process $a_{i_1} - 1$ times, producing the list $x, x+1, \ldots, x+a_{i_1}-2, x+a_{i_1}-1$. However, we cannot continue this process to get $x + a_{i_1}$. To understand why, we can see that

$$\begin{aligned} x + a_{i_1} - 1 &= -(a_{i_1} - 1)(a_{i_1}k_{i_1} + \cdots + a_{i_\alpha}k_{i_\alpha}) \\ &\quad + (a_{i_1} - 1)(a_{i_1}k_{i_1} + \cdots + a_{i_\alpha}k_{i_\alpha} + a_{i_{\alpha+1}}k_{i_{\alpha+1}} + \cdots + a_{i_n}k_{i_n}) \\ &= (a_{i_1} - 1)(a_{i_{\alpha+1}}k_{i_{\alpha+1}} + \cdots + a_{i_n}k_{i_n}), \end{aligned}$$

however, by adding Equation (2.1) to $x + a_{i_1} - 1$ we would obtain an expression for $x + a_{i_1}$ that has both negative and non-negative terms, which does not yield that $x + a_{i_1}$ is representable. To overcome this issue, we simply add a_{i_1} to x instead of adding 1 to $x + a_{i_1} - 1$, which results in $x + a_{i_1}$ being representable

again. After this, we can continue generating our list by the same procedure as before (adding ones until a multiple of a_{i_1}, at which point add a_{i_1} itself instead of the ones). Hence we have proven that every integer greater than or equal to x is representable. □

Now I am going to present my own proof for Theorem 2.2, which I have not seen in other literature so far. Before that, however, it will be useful to state and prove a lemma related to multiples of b and residues modulo a.

Lemma 2.3. *[7, Lemma 2.1] For positive integers a, b with $\gcd(a, b) = 1$, the integers $0b, 1b, 2b, \ldots, (a-1)b$ form a complete set of residues modulo a.*

Proof. Let $i \neq j$ and $i, j \in \{0, 1, 2, \ldots, a-1\}$. Then

$$\begin{aligned} ib \equiv jb \mod a &\implies a \mid (ib - jb) \\ &\implies a \mid b(i-j) \\ &\implies a \mid (i-j) \text{ since } \gcd(a,b) = 1 \\ &\implies i \equiv j \mod a, \end{aligned}$$

but this is a contradiction because of our initial conditions $i \neq j$ and $i, j \in \{0, 1, 2, \ldots, a-1\}$. Thus the multiples of b form a complete set of residues modulo a since the set is composed of exactly a distinct integers modulo a. □

Now we are ready to begin the second proof of existence. Lemma 2.3 will be used later in this thesis as well.

Second proof of Theorem 2.2. In order to prove that $g(a_1, \ldots, a_n)$ is well defined, i.e. there always exists some integer $N < \infty$ after which all integers are representable by $a_1, \ldots, a_n$, it suffices to only show that it is well defined for $g(a, b)$.

Consider the set of congruence classes modulo a, with addition defined as $[m] + [n] = [m + n]$ and standard multiplication defined as $[m] \cdot [n] = [m \cdot n]$.

Let us take all positive integers and write them out in increasing order, grouped into a columns as shown in Figure 1.

1	2	$\ldots$	$a-1$	a
$a+1$	$a+2$	$\ldots$	$2a-1$	$2a$
$2a+1$	$2a+2$	$\ldots$	$3a-1$	$3a$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Figure 1: All positive integers divided into a columns.

Firstly, we will proceed by marking every number that can be represented by a with a cross. Right now this is trivially all numbers $a, 2a, 3a, \ldots$; or the ath column in our figure. Next, mark integer b and all following positive integers that satisfy $b + k \cdot a$, $k \in \mathbb{N}$. In Figure 1, this coincides with the $(b \mod a)$th column starting from b and going downwards. We continue doing the previous procedure with $2b, 3b, \ldots$ until all columns have been marked. Once this is done, we can observe that after a certain row, all integers can be represented by some linear combination of a, b, showing that there exists a largest non-representable number $N = g(a, b)$. See Figure 2 for an example of this method with the integers $5, 7$.

Note that this will necessarily happen for all choices of a, b because of Lemma 2.3 and because, by definition, $\gcd(a, b) = 1$. This results in the fact that our method described above "touches" every

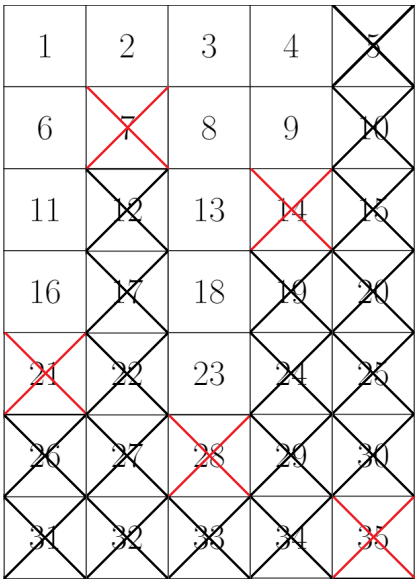

Figure 2: Example of the method for $g(5,7)$. Multiples of b's are marked with red crosses, and added multiples of a's with black. This also gives us $g(5,7) = 23$.

column once after $a-1$ steps, and on the ath step it reaches the rightmost column, which has already been marked, terminating the process.

This proves the existence not only for two variables, but due to the nature of the equivalence classes, any further number added to the list of variables will not change the fact that after some number N, all columns are accounted for. To illustrate this, it is enough to state that if we consider $g(a,b,c)$, then c will fall into the $(c \mod a)$th column. This can happen in two cases. Case 1 is when it falls "above" one of the red-marked numbers of the $(k \cdot b \mod a)$th column (meaning $c = kb - ha$ for some $k \in \{1,2,\ldots,a-1\}, h \in \mathbb{N}$), then it just further restricts the value of $g(a,b,c) \leq g(a,b)$. Case 2 is when it falls "below" a red-crossed integer, but then it has no restrictive effect, so $g(a,b,c) = g(a,b)$.

This is not unique to three variables either, as any further addition of numbers will result in it falling into one of the columns, either above or below an already red-marked number, hence the existence of $g(a_1,\ldots,a_n)$ is proven. Furthermore, by induction, we get an additional fact that $g(a_1,a_2) \geq g(a_1,a_2,a_3) \geq \cdots \geq g(a_1,\ldots,a_n)$. □

Lemma 2.3 and the above proof guarantees that every residue class of a_1 will have at least one representative that is a linear combination of $a_2,\ldots,a_n$. This observation warrants the following alternative definition of the Frobenius number, initially given by Brauer & Shockley [2], which will help us to prove the upcoming theorems much more easily.

Lemma 2.4. *[16, Lemma 1] Let $a_1,\ldots,a_n$ be such that $\gcd(a_1,\ldots,a_n) = 1$. For $1 \leq i \leq a_1 - 1$, let $\mathbf{m}(i)$ denote the least positive integer that is congruent to $i \pmod{a_1}$ such that Equation (1.1) has a solution in non-negative integers. Then*

$$g(a_1,\ldots,a_n) = \left(\max_{1\leq i\leq a_1-1} \mathbf{m}(i)\right) - a_1.$$

Proof. Since $\mathbf{m}(i)$ is the least positive integer that is representable by $a_1,\ldots,a_n$, it follows immediately that $\mathbf{m}(i) - a_1$ is *not* representable by non-negative integers for each $1 \leq i \leq a_1 - 1$. On the other hand, any N greater than each $\mathbf{m}(i) - a_1$ and congruent to $j \pmod{a_1}$ must be at least $\mathbf{m}(j)$, hence representable by $a_1, a_2, \ldots, a_n$ in non-negative integers. This shows that the largest value of $\mathbf{m}(i) - a_1$ is indeed the Frobenius number for $a_1,\ldots,a_n$. □

To illustrate an example of this with 2 variables, notice that in Figure 2, the $\mathbf{m}(i)$'s are the integers marked with a red cross, since they are the least positive integers representable by a, b in their respective

columns. In particular, $\mathbf{m}(1) = 21$, $\mathbf{m}(2) = 7$, $\mathbf{m}(3) = 28$ and $\mathbf{m}(4) = 14$. Therefore, by this definition, $g(5,7) = \max\limits_{1\le i\le 4} \mathbf{m}(i) - 5 = \max\{21, 7, 28, 14\} - 5 = 28 - 5 = 23$.

2.2 The formula

It takes barely any effort to calculate the Frobenius number for two chosen variables, as there is a very simple and straight-forward formula for it. In this section we are going to state this formula, and give three proofs for it: two given by Ramírez Alfonsín [9] and one by the author.

Theorem 2.5. *Let a, b be two positive coprime integers with $a < b$. Then the formula for the Frobenius number is given by*

$$g(a,b) = ab - a - b.$$

My proof. Looking back at Figure 2, we can visually see what Lemma 2.3 has stated, namely that every multiple of $b < ab$ belongs to a unique column, i.e. a unique residue class modulo a. To find the largest one, we just need to look at the last multiple of b, which is $(a-1)b$, then we "go up one row", which is equivalent to subtracting a, giving the formula $g(a,b) = (a-1)b - a = ab - a - b$.

An alternative, more rigorous approach can be achieved by using Definition 2.4, which states that $g(a,b) = (\max\limits_{1\le i\le a-1} \mathbf{m}(i)) - a$. Calculating $\max\limits_{i} \mathbf{m}(i)$ is very easy, since $\{\mathbf{m}(i)\} = \{1b, 2b, \dots, (a-1)b\}$, whose largest element is trivially $(a-1)b$, hence $g(a,b) = (a-1)b - a = ab - a - b$, proving the theorem. □

Now I am going to present two more proofs given by Ramírez Alfonsín. The one below already assumes that the formula is $g(a,b) = ab - a - b$, and uses contradiction to prove it. This approach differs from my proof, since my proof arrived at the formula in a constructive way, hence my decision to include it.

Second proof of Theorem 2.5. [9, Section 2.1] For $a, b \in \mathbb{N}$, let $\mathcal{R} = a\mathbb{N} + b\mathbb{N} = \{xa + yb \mid x, y \in \mathbb{N}\}$. $\mathcal{R}$ here is simply the set of all integers that can be represented by a, b.

Suppose that $ab - a - b = r_1 a + r_2 b$ with $r_1, r_2 \in \mathbb{N}$. Collecting all the a's on the left side and b's on the right, we get

$$a(b - r_1 - 1) = b(r_2 + 1).$$

Since $\gcd(a,b) = 1$, then this means b has to divide $b - r_1 - 1$, i.e. $b - r_1 - 1 = sb \ge b$, but this is impossible. Therefore $ab - a - b \notin \mathcal{R}$.

The next step is to show that $ab - a - b$ is the largest such number. In other words, we need to show that, if we let $\gamma = ab - a - b$, then $\gamma + i \in \mathcal{R}$ for any integer $i \ge 1$. By Bézout's identity, there always exist integers r_1 and r_2 with $0 \le r_1 < b$ such that $ar_1 + br_2 = 1$. This gives us the possibility to rewrite the integer i as $i = air_1 + bir_1$. Then

$$\gamma + i = ab - a - b + air_1 + bir_2 = (b - 1 + ir_1)a + (ir_2 - 1)b.$$

We may rewrite this equation as $\gamma + i = v_1 a + v_2 b$ with $0 \le v_2 < a$. If we rearrange this equation, we get

$$-i = \gamma - v_1 a - v_2 b = ab - a - b - v_1 a - v_2 b = (-v_1 - 1)a + (a - 1 - v_2)b.$$

Since $-i \notin \mathcal{R}$ because it is a negative integer, we must have that one of the coefficients of a or b must be negative. Note that $a - 1 - v_2 \ge 0$ by construction, so then we must have $-v_1 - 1 < 0$. This implies that $v_1 > -1 \implies v_1 \ge 0$. Since both v_1, v_2 are non-negative, and $\gamma + i = v_1 a + v_2 b$, we can conclude that $\gamma + i \in \mathcal{R}$. This proves that indeed $g(a,b) = ab - a - b$ is the largest number that cannot be represented. □

The last proof is going to approach this formula from a lattice point of view. It is going to utilize the well-known Pick's Theorem that relates the area of a simple lattice polygon to its boundary and internal lattice points. A simple lattice polygon is any polygon whose vertices lie on the lattice grid (or, equivalently, their coordinates are integers) and no sides cross each other. We are going to prove this now as a lemma with a direct, intuitive proof given by Varberg [20].

Lemma 2.6 (Pick's Theorem)**.** *Let S be a simple lattice polygon and write $A(S)$ for the area of S. Then*

$$A(S) = i + \frac{1}{2}b - 1,$$

where i and b are the number of lattice points in the interior of S and in the boundary of S respectively.

Proof. To every lattice point P_k of S, let us associate a weight $w_k = \theta_k/2\pi$, where θ_k measures P_k's "visibility" angle into S. For example, in Figure 3, the weight of the interior lattice point A is 1, the weight of the lattice point B on the boundary, which is not a vertex, is $\frac{1}{2}$ and the weight of C, a right-angled vertex, is $\frac{1}{4}$ etc.

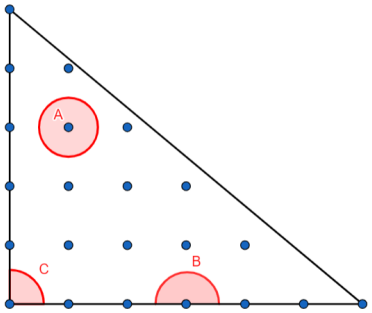

Figure 3: Interior points A, B, C with their inner visibility

It helps to think of w_k as the contribution that the lattice point makes to the area of S. Let

$$W(S) = \sum_{P_k \in S} w_k$$

denote the sum of these weights. To show that $W(S) = A(S)$, we note first that W is additive. This means that if $S = S_1 \cup S_2$, then $W(S) = W(S_1) + W(S_2)$. This fact is easy to see, since the inner visibility angles of the common lattice points get added up when adding two polygons.

Next, if we consider a lattice rectangle S_r with sides parallel to the lattice (Figure 4) and a lattice right-angle triangle S_t (Figure 5) it is immediately obvious that $W(S_r) = A(S_r)$ and $W(S_t) = A(S_t)$ because of W's additivity. One can deduce this inductively from the fact that the unit lattice square S_u has area 1, and has four right-angles whose weight are all $\frac{1}{4}$, and no other lattice points are inside or on the boundary. Therefore

$$A(S_u) = W(S_u) = \sum_{k=1}^{4} \frac{\pi/2}{2\pi} = 1,$$

after which adding the appropriate amount of unit squares will give us our initial lattice rectangle S_r. Upon division by 2, the right-angle lattice triangle's area immediately follows as well.

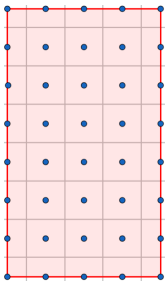

Figure 4: Rectangle S_r

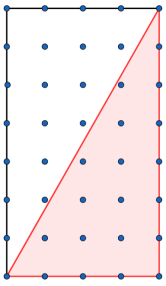

Figure 5: Right-angle triangle S_t

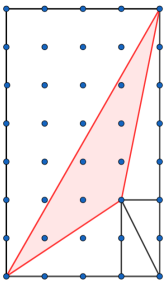

Figure 6: Arbitrary triangle S_a

Furthermore, if we look at an arbitrary lattice triangle S_a (Figure 6)[1], then we can see that, once again with the help of additivity, $A(S_a) = W(S_a)$ since the area of S_a consists of the big rectangle

[1] Figures 4,5,6 were made with GeoGebra in the style of [20, Figure 2, 3, 4]

that includes it, minus the union of some right-angle triangles. Thus we can conclude that we are able to decompose an arbitrary lattice polygon as a union of some lattice triangles, proving the claim that $W(S) = A(S)$ for any arbitrary lattice polygon.

To finish the proof, we notice that a simple polygon with n vertices has angle sum $(n-2)\pi$. Let us divide the boundary points into b_v vertices and b_s points on the sides. Then the sum of the visibility angles given by these points is $(b_v - 2)\pi + b_s\pi$ because every point on the side has π angles of visibility. Therefore it follows that the sum of all visibility angles at the boundary points is $(b_v - 2)\pi + b_s\pi = (b_v + b_s - 2)\pi = (b-2)\pi$. Thus, if I and B denote the set of interior and boundary points of S, then

$$A(S) = W(S) = \sum_{P_k \in I} w_k + \sum_{P_k \in B} w_k = i + \frac{(b-2)\pi}{2\pi} = i + \frac{1}{2}b - 1. \qquad \square$$

Now we can proceed with the second proof of Theorem 2.5.

Second proof of Theorem 2.5. [9, Section 2.1] Let a, b be as stated in the theorem and let P be the lattice polygon with vertices $A = (b-1, -1)$, $B = (-1, a-1)$, $C = (b, 0)$ and $D = (0, a)$, as shown in Figure 7[2]. Notice that there are no other lattice points on the boundary of P other than the 4 vertices since a, b are coprime. Note also that the set of lattice points inside P are all in the first quadrant.

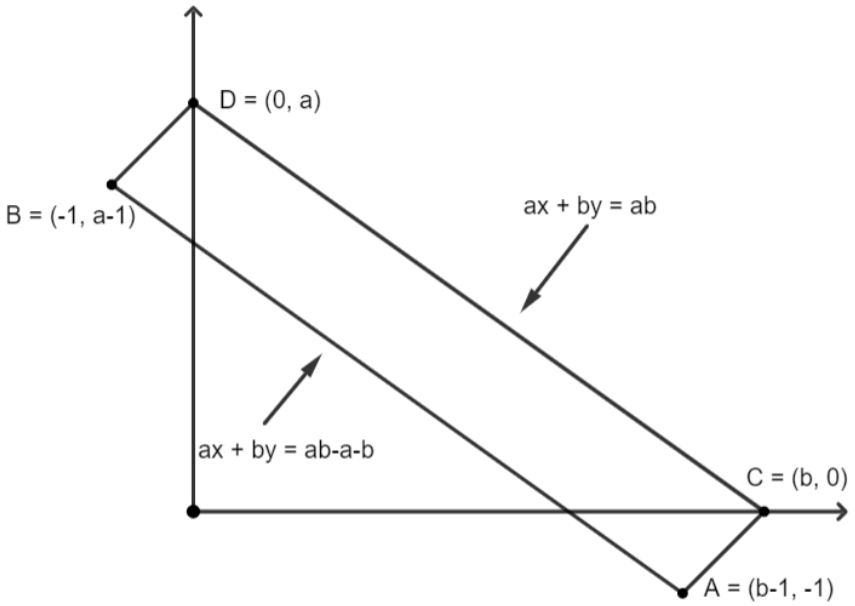

Figure 7: Polygon P as described above

The standard line equation with gradient m and y-intercept k of the line connecting A and B is given by

$$y = mx + k = \frac{-1-(a-1)}{(b-1)-(-1)}x + k = -\frac{a}{b}x + k \implies ax + by = c, \quad c \text{ a constant.}$$

Substituting in point B to get c, we arrive at

$$c = ax + by = a(-1) + b(a-1) = ab - a - b,$$

therefore the lower line's equation is $ax + by = ab - a - b$, as shown in the figure. A similar calculation yields $ax + by = ab$ for the line connecting the points C and D.

Let $I(P)$ and $B(P)$ denote the set of interior and boundary points of P respectively, and let P_1, P_2 be the triangles formed by the vertices CDB and BAC respectively. We can calculate the area of these two triangles by putting the coordinates of the vertices into a matrix and calculating their determinants:

[2]Figure 7 was made with GeoGebra in the style of [9, Figure 2.1]

$$A(P_1) = \frac{1}{2}\begin{vmatrix} b & 0 & 1 \\ 0 & a & 1 \\ -1 & a-1 & 1 \end{vmatrix} = \frac{1}{2}(b(a-(a-1))+a) = \frac{1}{2}(a+b),$$

$$A(P_2) = \frac{1}{2}\begin{vmatrix} -1 & a-1 & 1 \\ b-1 & -1 & 1 \\ b & 0 & 1 \end{vmatrix} = \frac{1}{2}(b((a-1)-(-1))+(1-(a-1)(b-1)))$$

$$= \frac{1}{2}(ab+1-(ab-a-b+1)) = \frac{1}{2}(a+b).$$

From this we can see that $A(P) = A(P_1) + A(P_2) = a + b$. With the help of the slightly relabeled Lemma 2.6, we are able to calculate the number of interior points, which is

$$I(P) = A(P) - \frac{1}{2}B(P) + 1 = a + b - \frac{4}{2} + 1 = a + b - 1.$$

We claim that the line $ax + by = ab - a - b + i$ contains exactly one point in $I(P)$ for each $i = 1, \ldots, a+b-1$. Suppose that there exists $1 \leq j \leq a+b-1$, such that $ax+by = ab-a-b+j$ has two points in $I(P)$, namely $J_1 = (x_1, y_1)$ and $J_2 = (x_2, y_2)$, that satisfy $ax_1+by_1 = ax_2+by_2 = ab-a-b+j$ for some $0 \leq x_1, x_2, y_1, y_2 < b$, $x_1 \neq x_2$, $y_1 \neq y_2$. Then we can rearrange the first equation to get $(x_1 - x_2)a = (y_2 - y_1)b$, and since $(a, b) = 1$, we must have that b divides $(x_1 - x_2)$, but this is impossible since both x_1, x_2 were chosen to be less than b. Therefore we have shown that each line $ax + by = ab - a - b + i$ contains at most one interior point of P.

Next up, we want to show that there is no line that does not hit any of the interior points. Assume that there exists a $1 \leq j \leq a + b - 1$ such that $ax_1 + by_1 = ab - a - b + j$ does not contain any points of $I(P)$. This means then that each of the $a + b - 1$ points of $I(P)$ belongs to at least one of the $a + b - 2$ lines $ax + by = ab - a - b + i$, $1 \leq i \neq j \leq a + b - 1$. Since there are more points than lines available, by the pigeon-hole principle, one of the lines must contain at least two of the interior points, but this is a contradiction.

Since all lines $ax+by = c \leq ab$ contain exactly one lattice point in the first quadrant, that means all those c's are representable by some arbitrary a, b. We conclude that $c = ab - a - b$ is the largest number where $ax + by = c$ has no non-negative solutions, therefore proving that indeed $g(a, b) = ab - a - b$. $\square$

3. Other related formulae when $n = 2$

One natural continuation of studying the Frobenius numbers after finding the formula for two variables is to go further; is there a formula for three variables, or perhaps more? We are going to tackle this immensely more difficult problem in the next chapter, however before that, this chapter is going to follow another natural path of mathematical exploration: What can we say about the number and sum of the other non-representable integers, out of which the Frobenius number just happens to be the largest? Are there also convenient formulae for these with two arbitrary integers as well? Section 3.1 and 3.2 are going to cover these respectively.

3.1 Number of non-representable integers

Concerning the question of how many non-representable integers there are, Sylvester [14] tackled this problem already in 1882, two years before his paper about the Frobenius number problem, where he proved the following:

Theorem 3.1. *[14] Let a, b be positive integers such that $\gcd(a, b) = 1$ and let $N(a, b)$ denote the number of integers without non-negative integer representations by a, b. Then*

$$N(a, b) = \frac{1}{2}(a - 1)(b - 1).$$

The experienced reader might notice that the amount of non-representable numbers is exactly half of the numbers from 0 to $g(a, b)$, which is quite similar to the relationship between primes and quadratic residues. There are many ways to prove this formula, but I will present a proof that utilizes a lattice point counting approach that I find quite satisfying and is also used for proving the quadratic reciprocity law. Before proving Theorem 3.1, however, we will need the help of a lemma by Kifer:

Lemma 3.2. *[7, Lemma 2.3] Let a, b be such that $\gcd(a, b) = 1$ with $a, b > 1$ and let $\lfloor \cdot \rfloor$ denote the greatest integer (floor) function. Then*

$$\sum_{i=1}^{a-1} \left\lfloor \frac{ib}{a} \right\rfloor = \frac{1}{2}(a - 1)(b - 1).$$

Proof. Consider the line $y = \frac{b}{a}x$ in the first quadrant between $x = 1$ and $x = a - 1$. We now count the number of positive-valued lattice points below the line for all such x. When $x = i$ with $1 \leq i \leq a-1$, then $y = \frac{ib}{a}$, which means that there are exactly $\lfloor \frac{ib}{a} \rfloor$ lattice points below the line (see Figure 8). Summing over all x gives the left-hand side of the stated equation, namely $\sum_{i=1}^{a-1} \lfloor \frac{ib}{a} \rfloor$.

The next step is showing that this sum is equal to the right-hand side. Consider now the same line $y = \frac{b}{a}x$, but this time, mark the rectangle defined by this line as the diagonal from the lattice point $(0, 0)$ to (a, b), and afterwards shrink this rectangle symmetrically to the $(a-2)$-by-$(b-2)$ rectangle with coordinates $(1, 1)$, $(a - 1, 1)$, $(1, b - 1)$ and $(a - 1, b - 1)$. There are a couple important things to note in this new rectangle:

- As a result of shrinking the rectangle symmetrically, the line $y = \frac{b}{a}x$ is still cutting the new rectangle in half.
- The new rectangle contains $(a - 1)(b - 1)$ lattice points.
- The $\sum_{i=1}^{a-1} \lfloor \frac{ib}{a} \rfloor$ positive-valued lattice points are all part of the new rectangle.

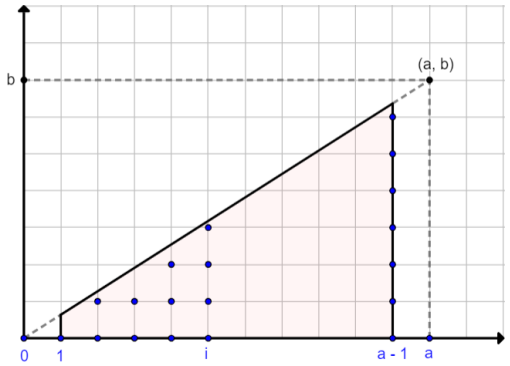

Figure 8: Counting lattice points between 1 and $a-1$.

- The line $y = \frac{b}{a}x$ does not contain any lattice points because $\gcd(a,b) = 1$ by definition. In order for a lattice point to be included, it would have to be an integer multiple of a, but the new triangle reaches only until $a-1$.

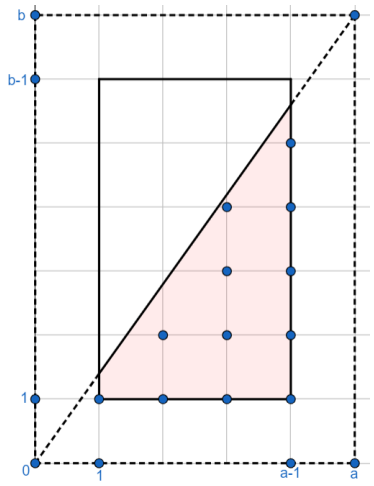

Figure 9: Counting the lattice points inside the shrunk rectangle, below the line $y = \frac{b}{a}x$.

Combining all of these above shows that, since the line divides the new rectangle in half and the new rectangle has $(a-1)(b-1)$ lattice points, the number of positive lattice points lying beneath the line in this new rectangle is $\frac{1}{2}(a-1)(b-1)$, proving the lemma. □

Now we can prove Theorem 3.1.

Proof of Theorem 3.1. To count the number of non-representable integers by a, b, it is enough to look at the interval $[1, ab-b-a]$ by Theorem 2.5. We start by proving a claim.

Claim: For each $k \in \{1, 2, \ldots, a-1\}$, there exists an integer t_k such that the list of non-negative integers $ab-kb-a, ab-kb-2a, \ldots, ab-kb-t_k a$ are all non-representable by a, b, where t_k is maximal so that no integer in that list becomes negative.

Proof of Claim: This is proven by contradiction. Assume that for some $k \in \{1, 2, \ldots, a-1\}$, there exist non-negative integers x, y and $q \in \{1, 2, \ldots, t_k\}$ such that $xa + yb = ab - kb - qa$. Then

$$xa + yb = ab - kb - qa \implies yb = (a-k)b - (q+x)a.$$

Since q, x, a are non-negative, this implies that $yb < (a-k)b$, so y is equal to exactly one of $0, 1, \ldots, a-k-1$. Furthermore, $yb \equiv (a-k)b \pmod{a}$, however none of the possible values of y are congruent to $a-k$ modulo a since they are all less than $a-k$. Thus no such y, $q \in \{1, 2, \ldots, t_k\}$ can exist.

The actual size of t_k for the different k's is yet to be determined. Note that $ab - kb - t_k a = (a-k)b - t_k a$ will stay non-negative if we subtract the number of a's that fit into $(a-k)b$. This number is the non-negative integer $\left\lfloor \frac{(a-k)b}{a} \right\rfloor$, therefore for each $k \in \{1, 2, \ldots, a-1\}$, the list of non-representable integers has $\left\lfloor \frac{(a-k)b}{a} \right\rfloor$ elements. Thus the number of non-representable integers is at least

$$\begin{aligned} N(a,b) &\geq \left\lfloor \frac{(a-1)b}{a} \right\rfloor + \left\lfloor \frac{(a-2)b}{a} \right\rfloor + \cdots + \left\lfloor \frac{(a-(a-1))b}{a} \right\rfloor \\ &= \left\lfloor \frac{b}{a} \right\rfloor + \left\lfloor \frac{2b}{a} \right\rfloor + \cdots + \left\lfloor \frac{(a-1)b}{a} \right\rfloor \\ &= \sum_{i=1}^{a-1} \left\lfloor \frac{ib}{a} \right\rfloor = \frac{1}{2}(a-1)(b-1) \text{ by Lemma 3.2.} \end{aligned}$$

We now show equality. To this end, it is important to realize that we have looked at all non-representable integers $1b, 2b, \ldots, (a-1)b \pmod a$ because we counted $ab - kb - qa = (a-k)b - qa \equiv (a-k)b \pmod a$ for each $k \in \{1, 2, \ldots, a-1\}$ and $q \in \{1, 2, \ldots, t_k\}$ (t_k maximal). By Lemma 2.3, $1b, 2b, \ldots, (a-1)b \pmod a$ form a complete set of residues modulo a, so we have not missed any other non-representable numbers, proving the theorem. □

Another, arguably easier way to prove the formula $N(a,b) = \frac{1}{2}(a-1)(b-1)$ uses a definition of $N(a_1, \ldots, a_n)$ that is extremely similar to that of Lemma 2.4, whose proof is again given by Tripathi [16].

Lemma 3.3. *[16, Lemma 1] Let $a_1, \ldots, a_n$ be positive integers such that $\gcd(a_1, \ldots, a_n) = 1$ and $1 \leq i \leq a_1 - 1$. Let $\mathbf{m}(i)$ denote the least positive integer that is congruent to $i \pmod{a_1}$ such that Equation (1.1) has a solution in non-negative integers. Then*

$$N(a_1, \ldots, a_n) = \frac{1}{a_1} \sum_{i=1}^{a_1 - 1} (\mathbf{m}(i) - i).$$

Proof. The non-representable numbers that are congruent to $i \pmod{a_1}$ form an arithmetic progression, where the first element is i and the last element is $\mathbf{m}(i) - a_1$ with common difference a_1. The number of that is therefore $(\mathbf{m}(i) - i)/a_1$, and since $i \in \{1, \ldots, a_1 - 1\}$, the second part of the definition easily follows. □

Now, with this definition, we are able to prove Theorem 3.1 in a more concise way.

Second proof of Theorem 3.1. As mentioned at the end of Section 2.1, the integers marked with a red cross in Figure 2 are the $\mathbf{m}(i)$'s for $1 \leq i \leq a-1$. Furthermore, in the first proof of Theorem 2.5, it is stated that $\{\mathbf{m}(i)\} = \{1b, 2b, \ldots, (a-1)b\}$, therefore we have that

$$\begin{aligned} N(a,b) &= \frac{1}{a} \sum_{i=1}^{a-1} (\mathbf{m}(i) - i) = \frac{1}{a} \sum_{i=1}^{a-1} (ib - i) \\ &= \frac{1}{a} \sum_{i=1}^{a-1} ((b-1)i) = \frac{b-1}{a} \sum_{i=1}^{a-1} i \\ &= \frac{b-1}{a} \cdot \frac{a(a-1)}{2} = \frac{1}{2}(a-1)(b-1). \end{aligned}$$

□

3.2 Sum of non-representable integers

In the previous section we were able to show that exactly half of the integers between 0 and $g(a,b)$ are non-representable, which might have come as a pleasant surprise. One natural step further would be to pose the question whether there are any patterns for the sum of these integers? For example, as we have seen before in Figure 2, $g(5,7) = 23$ with the uncrossed numbers showing the non-representable integers, of which there are indeed $N(5,7) = \frac{1}{2} \cdot 4 \cdot 6 = 12$ numbers, namely $A = \{1, 2, 3, 4, 6, 8, 9, 11, 13, 16, 18, 23\}$.

The sum of these numbers is $\sum_{a\in A} a = 114$, but is there an explicit formula for this sum? As we are going to find out later, there is! Before that, let us introduce the notation of this function.

Let a, b be positive integers with $\gcd(a, b) = 1$. Let $NR(a, b)$ denote the *set* of numbers *not* representable by a, b. Then denote the *sum* of these numbers as

$$S(a, b) = \sum_{n\in NR(a,b)} n. \tag{3.1}$$

Now we can state the general formula for the sum of non-representable numbers by two integers, and afterwards present the ingenious proof given by Brown & Shiue [3], which gives us even more than what we bargained for (see Remark 3.10 below).

Theorem 3.4. *Let a, b be positive integers with $\gcd(a, b) = 1$. Then*

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

To set up the proof, we need to define two auxiliary functions and prove some lemmas. The first function is $r(n)$, which for each $n \geq 0$, is going to denote the *number* of representations of n in the form $n = sa + tb$, where s, t are non-negative integers. For example, if we take $a = 5$ and $b = 7$, then $r(35) = 2$, since $35 = 7 \cdot 5 + 0 \cdot 7 = 0 \cdot 5 + 5 \cdot 7$, or in other words, the ordered pairs $(7, 0)$ and $(0, 5)$ are the two possible representations of 35 by 5 and 7.

Lemma 3.5. *Let a, b be positive integers with $\gcd(a, b) = 1$. If $0 \leq n \leq ab-1$, then $r(n) = 0$ or $r(n) = 1$.*

Proof. Suppose that $r(n) \geq 2$ and that $n = s_1a + t_1b = s_2a + t_2b$, where we assume without loss of generality that $s_1 > s_2$. Then $0 = (s_1 - s_2)a + (t_1 - t_2)b \implies 0 \equiv (s_1 - s_2)a \pmod{b}$. Since $\gcd(a, b) = 1$, $b \mid (s_1 - s_2)$, so $s_1 \geq b$ and $n \geq ba + t_1b \geq ab$. □

Now we define the second function in the following way:

$$f(x) = \sum_{n=0}^{ab-a-b} (1 - r(n))x^n. \tag{3.2}$$

This is a very useful function, because if we differentiate it, apply the above claim and evaluate it at $x = 1$, we obtain

$$f'(1) = \sum_{n=1}^{ab-a-b} n(1 - r(n)) = \sum_{\substack{n=1 \\ r(n)=0}}^{ab-a-b} n = \sum_{n\in NR(a,b)} n \overset{(3.1)}{=} S(a, b). \tag{3.3}$$

Thus the question of finding a formula for $S(a, b)$ has been reduced to evaluating $f'(1)$, but that can still pose a big issue. How do we know whether there even exists a differentiable function that would be equivalent? We have the possibility of exploring this question with the help of generating functions, since $f(x)$ is of a similar form already.

Lemma 3.6. *Let a, b be positive integers with $\gcd(a, b) = 1$ and let $A(x) = \frac{1}{(1-x^a)(1-x^b)}$. Then*

$$A(x) = \sum_{n=0}^{\infty} r(n)x^n.$$

Proof. We have that

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

The second equation is the standard power series expansion of $A(x)$, and the last equation follows since upon multiplication of x^{as} and x^{bt} for some $s, t \in \mathbb{N}$, the coefficient of x^n "counts" the number of ways n can be represented by the different s, t from $sa + tb$. This is the exact definition of $r(n)$. □

Lemma 3.7. *The polynomial*

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

has a leading coefficient 1*.*

Proof. We can see this by factoring both the numerator and denominator into complex linear factors. Since $\gcd(a,b) = 1$, 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 factor in the denominator cancels against a linear factor in the numerator. □

Lemma 3.8. *Let* $P(x) = \frac{(x^{ab}-1)(x-1)}{(x^a-1)(x^b-1)}$ *as stated above. Then* $P(1) = 1$*.*

Proof. Since $\lim_{x\to 1} P(1) = \frac{0}{0}$, we can apply L'Hôpital's rule, which yields

$$\begin{aligned}\lim_{x\to 1} P(x) &= \lim_{x\to 1} \frac{(x^{ab}-1)(x-1)}{(x^a-1)(x^b-1)} = \lim_{x\to 1} \frac{x^{ab+1} - x^{ab} - x + 1}{x^{a+b} - x^a - x^b + 1} \\ &= \lim_{x\to 1} \frac{(ab+1)x^{ab} - abx^{ab-1} - 1}{(a+b)x^{a+b-1} - ax^{a-1} - bx^{b-1}} = \frac{ab+1-ab-1}{a+b-a-b} = \frac{0}{0}.\end{aligned}$$

Applying it a second time yields

$$\begin{aligned}\lim_{x\to 1} P(x) &= \lim_{x\to 1} \frac{(ab+1)x^{ab} - abx^{ab-1} - 1}{(a+b)x^{a+b-1} - ax^{a-1} - bx^{b-1}} \\ &= \lim_{x\to 1} \frac{ab(ab+1)x^{ab-1} - (ab-1)abx^{ab-2}}{(a+b-1)(a+b)x^{a+b-2} - (a-1)ax^{a-2} - (b-1)bx^{b-2}} \\ &= \frac{ab(ab+1) - (ab-1)ab}{(a+b)(a+b-1) - a(a-1) - b(b-1)} \\ &= \frac{a^2b^2 + ab - a^2b^2 + ab}{a^2 + 2ab + b^2 - a - b - a^2 + a - b^2 + b} = \frac{2ab}{2ab} = 1,\end{aligned}$$

therefore we have shown that indeed $P(1) = 1$. □

Lemma 3.9. *For* $P(x)$ *as defined above and* a, b *positive integers with* $\gcd(a,b) = 1$*, we have that*

$$\frac{P(x)-1}{x-1} = \sum_{n=ab}^{\infty} (r(n-ab) + 1 - r(n))x^n + \sum_{n=0}^{ab-1} (1 - r(n))x^n.$$

Proof. Since $P(1) = 1$ by Lemma 3.8, we have that $\frac{P(x)-1}{x-1}$ is also a polynomial, of degree $ab - a - b$, similarly with leading coefficient 1. Now we can write

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

□

Remark 3.10. Using the previous observations, we are able to deduce a lot of extra information as a by-product of Lemma (3.9). Since this power series is actually a polynomial of degree $ab - a - b$ with leading coefficient 1, we can deduce the following corollaries:

- All the coefficients of the powers greater than $ab-a-b$ are 0.
- The coefficient of x^{ab-a-b} is 1, therefore $1-r(ab-a-b)=1 \implies r(ab-a-b)=0$.
- For all $ab-a-b<n\leq ab-1$, it follows that $r(n)=1$. (Second part of Lemma 3.9)
- For $n\geq ab$, $r(n)=r(n-ab)+1$ (First part of Lemma 3.9)

Incidentally, combining these facts also constitutes yet another proof for the Frobenius number formula for two integers!

We now have all the necessary pieces and are able to prove Theorem 3.4.

Proof of Theorem 3.4. Recall that we have a polynomial expression for the above function $f(x)$, namely

$$\frac{P(x)-1}{x-1}=\sum_{n=0}^{ab-a-b}(1-r(n))x^n \overset{(3.2)}{=} f(x).$$

The next step is, of course, to calculate $f'(1)$ and then we are finished. Let $y=x^a$ and

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

Then

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

For ease of notation, let us call the numerator $g(x)$ and denominator $h(x)$, which will make calculating $f'(x)$ easier by applying the division rule for derivatives later on. So let $f(x)=\frac{g(x)}{h(x)}$ where

$$\begin{aligned}g(x)&=\sum_{k=1}^{b-1}\frac{y^k-x^k}{x-1}=\sum_{k=1}^{b-1}\frac{x^{ak}-x^k}{x-1}=\sum_{k=1}^{b-1}(x^k+x^{k+1}+\cdots+x^{ak-1}),\\ h(x)&=\sum_{k=0}^{b-1}x^k.\end{aligned}$$

Now, in order to calculate $f'(1)$, we will need the values of $g(1), g'(1), h(1)$ and $h'(1)$. Out of these, $g'(1)$ will require the most attention and good confidence in algebraic gymnastics. The values are as follows:

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

Finally, substituting all these components yields

$$\begin{aligned}
S(a,b) \overset{(3.3)}{=} f'(1) &= \frac{h(1)g'(1) - g(1)h'(1)}{(h(1))^2} \\
&= \frac{b^2(a-1)(b-1)\left(\frac{(a+1)(2b-1)}{12} - \frac{1}{4}\right) - [\frac{1}{2}(a-1)(b-1)b][\frac{1}{2}b(b-1)]}{b^2} \\
&= (a-1)(b-1)\left(\frac{(a+1)(2b-1)}{12} - \frac{1}{4}\right) - \frac{1}{4}(a-1)(b-1)^2. \\
&= \frac{1}{12}(a-1)(b-1)(2ab-a-b-1). \qquad \square
\end{aligned}$$

4. Explicit formulae for specific cases when $n = 3$

In the previous chapter we have derived two formulae regarding integers that could be constructed by a linear combination of two arbitrary integers. The current chapter would present a simple formula for the Frobenius number with three variables – if such a formula existed. Unfortunately, Curtis [4] has shown that there is no general explicit formula for $g(a, b, c)$ (or for any higher dimension) that is of a certain type. However, there exist some general formulae that simplify the number of triplets one needs to consider. We will also prove that for any number N, there exists an integer triple for which $g(a, b, c) = N$. Beyond this, this chapter is going to cover formulae for some important generalizations subject to certain conditions, namely when the integers follow an arithmetic sequence, or when a divides $b + c$.

Note: Recall Remark 1.2. We are still assuming, without loss of generality, that $a < b < c$ holds throughout this whole thesis.

Let us begin with the fact that there is no explicit formula for $g(a, b, c)$ in the form of a polynomial.

Theorem 4.1. *[4] Let $A = \{(a, b, c) \in \mathbb{N}^3 \mid a < b < c$, where a and b are prime and $a, b \nmid c\}$. Then there is no non-zero polynomial $H \in \mathbb{C}[X_1, X_2, X_3, Y]$ such that $H(a, b, c, g(a, b, c)) = 0$ for all $(a, b, c) \in A$.*

The proof of this theorem is beyond the scope of this thesis, however, the keen and curious reader interested in infinite semigroups, Farey sequences and projective curves is more than welcome to explore the proof at their own leisure. However, a useful corollary to this theorem can be stated as the following:

Corollary 4.2. *[4] There is no finite set of polynomials $\{h_1, \ldots, h_n\}$ such that for each choice of a, b, c there is some i such that $h_i(a, b, c) = g(a, b, c)$.*

Proof. Assume the contrary: There exists a finite set of polynomials as described above. Then construct the polynomial $H = \prod_{i=i}^{n}(h_i(X_1, X_2, X_3) - Y)$. Clearly $H \in \mathbb{C}[X_1, X_2, X_3, Y]$, but by assumption, for any choice of a, b, c there exists a polynomial h_i such that $h_i(a, b, c) = g(a, b, c) = Y$, which results in the fact that H would vanish for all values of a, b, c while being a non-zero polynomial, which is prohibited by Theorem 4.1. □

Even though there is no single polynomial formula, one can view this problem from the opposite perspective. We can view g as a function that maps three coprime integers a, b, c to a non-negative integer $g(a, b, c)$, and then deduce some results. One of these results is given by Rosales, García-Sánchez and García-García [12] who have proven that this Frobenius number function is surjective. We record this result without a full proof, but record the proofs of some of the lemmas as the whole proof is slightly more involved.

Definition 4.3. Let $R := R(a_1, \ldots, a_n)$ denote the set of all non-negative integers representable by $a_1, \ldots, a_n$, or in other words, $R = \{a_1x_1 + \cdots + a_nx_n \mid x_1, \ldots, x_n \geq 0\}$. For $a \in R \setminus \{0\}$, the *Apéry set* of a in R is the set

$$Ap(R, a) = \{r \in R \mid r - a \notin R\}.$$

Clearly $Ap(R, a) = \{0, \mathbf{m}(1), \ldots, \mathbf{m}(a - 1)\}$, where for $1 \leq i \leq a - 1$, $\mathbf{m}(i)$ denotes the least representable integer congruent to $i \pmod a$, and by applying Lemma 2.4, we can also see that $g(a_1, \ldots, a_n) = (\max Ap(R, a)) - a$.

Lemma 4.4. *[12, Lemma 1.1] Let N be a positive integer.*

i) If N is odd, then $g(2, N + 2) = N$.

ii) If $3 \nmid N$, then $g(3, a, b) = N$, where $\{a, b\} = \{k \in \{N + 1, N + 2, N + 3\} : 3 \nmid k\}$.

iii) If N is even and $4 \nmid N$, then $g(4, \frac{N}{2}+2, \frac{N}{2}+4) = N$.

Proof. i) Follows immediately by applying the formula for two integers:

$$g(2, N+2) = 2(N+2) - 2 - (N+2) = N.$$

ii) Clearly the numbers representable by $3, a, b$ are also representable by $3, N+1, N+2, N+3$ for some N. Thus

$$g(3, a, b) = g(3, N+1, N+2, N+3) = N.$$

iii) Let R be generated by $\{4, \frac{N}{2}+2, \frac{N}{2}+4\}$. If we show that $Ap(R,4) = \{0, \frac{N}{2}+2, \frac{N}{2}+4, N+4\}$, then we are done since $g(4, \frac{N}{2}+2, \frac{N}{2}+4) = (\max Ap(R,4)) - 4$. As all of $\frac{N}{2}+2$, $\frac{N}{2}+4$ and $N+4$ belong to R, it is enough to demonstrate that none of the integers $\frac{N}{2}+2-4, \frac{N}{2}+4-4, N+4-4$ is in R.

- If $\frac{N}{2} - 2 \in R$, then it must be a multiple of 4 since the second and third term are both larger than $\frac{N}{2} - 2$. Thus $\frac{N}{2}$ is a multiple of 2, which means that N is a multiple of 4, contradicting the hypothesis.
- If $\frac{N}{2} \in R$, then arguing as the above, we arrive at the same contradiction.
- If $N \in R$, then $N = x_1 4 + x_2(\frac{N}{2}+2) + x_3(\frac{N}{2}+4)$ for some non-negative integers x_1, x_2, x_3. Observe that this implies that $0 < x_2 + x_3$ (N is not a multiple of 4) and $x_2 + x_3 \leq 1$, because otherwise $N \geq N+4$, which is impossible. Hence either $N = x_1 4 + (\frac{N}{2}+2)$ or $N = x_1 4 + (\frac{N}{2}+4)$. In both cases we get that $\frac{N}{2}$ is even, once more contradicting the fact that N is not a multiple of 4. □

Lemma 4.5. *[12, Proposition 1.2] If there exists a positive integer $d > 1$ such that $\gcd(d, N) = 1, (d-1) \mid N$ and $d(d-1)(d-3) < N$, then there exist a, b, c such that $g(a, b, c) = N$.*

Proof. Let R be generated by $\left\{d, \frac{N}{d-1} + d, N + d\right\}$. We need to prove that

$$Ap(R, d) = \left\{0, \frac{N}{d-1} + d, \ldots, (d-2)\left(\frac{N}{d-1} + d\right), N + d\right\},$$

because then $\max Ap(R,d) = N + d$, and therefore $g(a,b,c) = N + d - d = N$. It is clear that if R' denotes the set of integers representable by a, b, where $\gcd(a,b) = 1$, then

$$Ap(R', a) = \{0, b, 2b, \ldots, (a-1)b\},$$

as we have already seen before in Lemma 2.3. If we set $a = d$ and $b = \frac{N}{d-1} + d$, we have that

$$Ap\left(R', d\right) = \left\{0, \frac{N}{d-1} + d, \ldots, (d-1)\left(\frac{N}{d-1} + d\right)\right\}.$$

Since $(d-2)(\frac{N}{d-1} + d) < N + d$ whenever $d(d-1)(d-3) < N$, we have that

$$\left\{0, \frac{N}{d-1} + d, \ldots, (d-2)\left(\frac{N}{d-1} + d\right)\right\} \subset Ap(R, d).$$

Note that $(d-1)(\frac{N}{d-1} + d) = N + (d-1)d \equiv N \equiv N + d \pmod{d}$ and that $(d-1)(\frac{N}{d-1} + d) \geq N + d$, which means that $N + d$ must be in $Ap(R,d)$. This is true because from $Ap(R', d)$, we had that $(d-1)(\frac{N}{d-1} + d)$ is the smallest representable number for its congruence class modulo d, but $N + d$ is also in the same congruence class while also being smaller, essentially overriding it. Therefore

$$Ap(R, d) = \left\{0, \frac{N}{d-1} + d, \ldots, (d-2)\left(\frac{N}{d-1} + d\right), N + d\right\}.$$

Since $(d-2)(\frac{N}{d-1} + d) < N + d$, we have that $(\max Ap(R,d)) - d = N + d - d = N$. □

Corollary 4.6. *[12, Corollary 1.3] Let N be a positive integer such that it is not a multiple of $5, 7$ or 11. Then there exist positive integers a, b, c such that $g(a, b, c) = N$.*

Proof. Assume that $5 \nmid N$. We can also assume that $4 \mid N$, since otherwise either Lemma 4.4 (i) or (iii) would apply depending on whether N is even or odd. By applying Lemma 4.5 it suffices to prove the statement for $N \leq 5 \cdot 4 \cdot 2 = 40$. In view of Lemma 4.4 we can also assume that $3 \mid N$. Thus the only possible values left for N are multiples of 12 less than or equal to 40, that is, $N \in \{12, 24, 36\}$. Since $g(5, 8, 9) = 12$, $g(5, 11, 18) = 24$ and $g(5, 14, 27) = 36$, we are done.

Now we study the case $7 \nmid N$ and $5 \mid N$. By using Lemma 4.4, we can assume that $3 \cdot 4 \cdot 5 = 60 \mid N$. In particular, $6 \mid N$, which allows us to apply Lemma 4.5, whence arguing as above, it suffices to prove the statement for $N \leq 7 \cdot 6 \cdot 4 = 168$. As N is a multiple of 60, the only possible values left for N are $N = 60$ and $N = 120$. Since $g(7, 17, 33) = 60$, and $g(7, 27, 73) = 120$, these two cases are also covered.

Finally, suppose that $11 \nmid N$, and that 5 and 7 divide N. By using this together with Lemma 4.4, we can assume that $3 \cdot 4 \cdot 5 \cdot 7 = 420 \mid N$, whence $10 \mid N$. By Lemma 4.5 we can restrict ourselves to $N \leq 11 \cdot 10 \cdot 8 = 880$. Since N is a multiple of 420, it suffices to check that the cases $N \in \{420, 840\}$. We conclude the proof by pointing out that $g(8, 107, 109) = 420$ and $g(9, 143, 353) = 840$. □

Lemma 4.7. *[12, Proposition 1.4] If N is a positive integer such that $N < 4620$, then there exist positive integers a, b, c such that $g(a, b, c) = N$.*

Proof. Note that $3 \cdot 4 \cdot 5 \cdot 7 \cdot 11 = 4620$. Hence if $N < 4620$, then there exists $k \in \{3, 4, 5, 7, 11\}$ such that $k \nmid N$. According to the value of k, by applying one of the results presented so far we conclude in any case that there exist a, b, c such that $g(a, b, c) = N$. □

The following lemma is just of interest.

Lemma 4.8. *[12, Lemma 1.5] Let N be a positive integer and let d be the least positive integer such that $d \nmid N$. Then d is a prime power.*

Proof. If d is not a prime power, then $d = pq$, with $\gcd(p, q) = 1$ and $p \neq 1 \neq q$. As $p, q < d$ we have that both p and q divide N, but then $d = pq$ also divides N, contradicting the hypothesis. □

The proof of the following result relies on the above lemmas, but also on other propositions and further lemmas present in the original paper that are not mentioned here, therefore no proof is given.

Theorem 4.9. *[12, Theorem 1.11] Let N be a positive integer. Then there exist positive integers a, b, c such that*

$$g(a, b, c) = N.$$

I have collected both the results of some of the lemmas and propositions mentioned in the paper together with the ones proven here into a single corollary, which is stated below.

Corollary 4.10. *[12, Proofs of Proposition 1.9 and Corollary 1.3] Let N be a positive integer and d be the least positive integer such that $d \nmid N$, and set $k = \gcd(d, N)$. Then*

$$N = \begin{cases} g\left(d, \frac{N+d}{k}, \left\lceil \frac{N+d}{k(d-k)} \right\rceil d - \frac{N+d}{k}\right) & \text{if } d < 5 \text{ or } d(d-1)(d-2) < N; \\ \text{Specific values (see A.1)} & \text{if } 5 \leq d < 13 \text{ and } d(d-1)(d-2) \geq N. \end{cases}$$

Remark 4.11. In the original paper it is proven that $d \geq 13$ implies that $d(d-1)(d-2) < N$, hence the restriction.

It is important to note that when we are dealing with the linear combination of three positive integers, the restriction is that $\gcd(a, b, c) = 1$, or in other words, they cannot share a common divisor. We have already met this fact in the introduction to this thesis, namely the fact that the Frobenius number existed for the numbers $\{6, 9, 20\}$ even though $\gcd(6, 9) = 3$ and $\gcd(6, 20) = 2$. The following result by Johnson, however, is vital in order to significantly restrict the number of triples to be investigated only to pairwise coprime triples.

Theorem 4.12. *[6] Let $a_1, a_2 \ldots, a_n$ be positive integers. If $\gcd(a_2, \ldots, a_n) = d$ and $a_i = da_i'$ for each $i > 1$, then*

$$g(a_1, a_2 \ldots, a_n) = dg(a_1, a_2', \ldots, a_n') + a_1(d-1).$$

Proof. Just like in Lemma 2.4, let $\mathbf{m}(i)$ and $\mathbf{m}'(i)$ denote the *least* positive integers congruent to $i \pmod{a_1}$ representable by $a_1, a_2, \ldots, a_n$ and $a_1, a_2', \ldots, a_n'$ respectively. Notice that since we are reducing them by $\pmod{a_1}$, $\mathbf{m}(i)$ and $\mathbf{m}'(i)$ can be represented by $a_2, \ldots, a_n$ and $a_2', \ldots, a_n'$ respectively, which gives

$$\mathbf{m}(i) = a_2x_2 + \cdots + a_nx_n = da_2'x_2 + \cdots + da_n'x_n = d(a_2'x_n + \cdots + a_n'x_n) = d\mathbf{m}'(i).$$

Now we can use Lemma 2.4 and get

$$\begin{aligned} g(a_1, a_2, \ldots, a_n) &= \max_{1 \le i \le a_1 - 1} \mathbf{m}(i) - a_1 = \max_{1 \le i \le a_1 - 1} d\mathbf{m}'(i) - a_1 \\ &= d\left(\max_{1 \le i \le a_1 - 1} \mathbf{m}'(i) - a_1\right) + a_1(d-1) \\ &= dg(a_1, a_2', \ldots, a_n') + a_1(d-1). \end{aligned}$$

□

Remark 4.13. This reduction works for any combination of the integers, as demonstrated later in Example 5.2. If any of the a_i are reduced to 1, the reduction still works if we define $g(1, a_2, \ldots, a_n) = -1$. This extension still makes sense, because all non-negative numbers can be represented by 1, so the "largest" non-representable number is indeed -1.

Since Curtis' proof discouraged looking for a formula for the three integer case, there were important developments in finding explicit formulae for other cases instead. One of the most important such solutions for a specific case is the formula for arithmetic progressions. The most generic version for a kind of arithmetic sequence was given by Selmer [13], for $g(a, ha + d, ha + 2d, \ldots, ha + kd)$ with $\gcd(a, d) = 1$ and $h, k \ge 1$. We give a proof of this by Tripathi [18], using the same useful notation as in Lemma 2.4.

Firstly, recall that $g(a, ha + d, ha + 2d, \ldots, ha + kd)$ denotes the largest N such that the equation

$$ax_0 + (ha + d)x_1 + (ha + 2d)x_2 + \cdots + (ha + kd)x_k = a\Big(x_0 + h\sum_{i=1}^{k} x_i\Big) + d\Big(\sum_{i=1}^{k} ix_i\Big) = N \tag{4.1}$$

does not have a solution in non-negative integers. We will now prove a lemma that is necessary for the proof of the formula later.

Lemma 4.14. *[18, Lemma 3] For each $1 \le x \le a - 1$, the least positive integer of the form given in Equation (4.1) in the class $[dx]$ modulo a is given by $ha\big(1 + \lfloor \frac{x-1}{k} \rfloor\big) + dx$.*

Proof. Let $\mathbf{m}(dx)$ denote the least positive integer in the class $[dx]$ modulo a. Then $\mathbf{m}(dx)$ is the minimum value attained by the expression on the left in Equation (4.1), subject to $x = \sum_{i=1}^{k} ix_i$ and each $x_i \ge 0$. If we set $x = qk + r$ with $0 \le r \le k - 1$, then we claim that $x_0 + h\sum_{i=1}^{k} x_i$ is minimized by choosing $x_k = q$ and then either choose $x_r = 1$ and $x_i = 0$ for all other i when $r > 0$, or choose $x_r = 0$ when $r = 0$. Indeed, if $x = \sum_{i=1}^{k} ix_i = x_1 + 2x_2 + \cdots + kx_k$, then minimizing $x_0 + h\sum_{i=1}^{k} x_i$ corresponds to finding a partition of x by the integers $1, \ldots, k$ that has the least amount of parts. This is achieved by choosing the largest integer k as many times as possible (in our case that's q times), plus one copy of the remainder $r < k$. If we choose $x_k < q$, then we need to make up the missing k from $x_1 + 2x_2 + \cdots + (k-1)x_{k-1}$, but no such choice of the form $x_i = 1, x_j = 0$ exists where $i, j \in \{1, \ldots, k-1\}, i \ne j$. In the case when $1 \le x \le k$, then $r = x$. Thus the minimum value for $x_0 + h\sum_{i=1}^{k} x_i$ is then $h(q+1)$ if $r \ne 0$ and hq if $r = 0$. This can be expressed in one expression by combining these conditions as $h\big(1 + \lfloor \frac{x-1}{k} \rfloor\big)$. Therefore $\mathbf{m}(dx) = ha\big(1 + \lfloor \frac{x-1}{k} \rfloor\big) + dx$. □

Theorem 4.15. *[18, Theorem 4] Let a, d, h, k be positive integers, with $\gcd(a, d) = 1$. Then*

$$g(a, ha + d, ha + 2d, \ldots, ha + kd) = ha\left\lfloor \frac{a-2}{k} \right\rfloor + (h-1)a + d(a-1).$$

Proof. By Lemma 2.4 and Lemma 4.14, we have that

$$\begin{aligned} g(a, ha+d, ha+2d, \ldots, ha+kd) &= \max_{1\le x\le a-1} \mathbf{m}(dx) - a \\ &= \max_{1\le x\le a-1} \Big(ha\big(1 + \lfloor \tfrac{x-1}{k} \rfloor\big) + dx \Big) - a \\ &= ha\big(1 + \lfloor \tfrac{a-2}{k} \rfloor\big) + d(a-1) - a \\ &= ha \lfloor \tfrac{a-2}{k} \rfloor + (h-1)a + d(a-1). \end{aligned}$$

□

There are a number of immediate consequences one can draw from the above theorem.

Corollary 4.16. *Let $a, a+d, a+2d, \ldots, a+kd$ be an arithmetic sequence with $\gcd(a,d) = 1$. Then*

$$g(a, a+d, a+2d, \ldots, a+kd) = a \lfloor \tfrac{a-2}{k} \rfloor + d(a-1).$$

Proof. Follows immediately from Theorem 4.15 by setting $h = 1$. □

Corollary 4.17. *Let $a > 1, d > 0$ be positive integers with $\gcd(a,d) = 1$. Then*

$$g(a, a+d, a+2d) = \begin{cases} \frac{a(a-2)}{2} + d(a-1) & \text{if } a \text{ is even.} \\ \frac{a(a-3)}{2} + d(a-1) & \text{if } a \text{ is odd.} \end{cases}$$

Proof. Follows immediately from Corollary 4.16 by setting $k = 2$ and noticing that if a is even, then $\lfloor \frac{a}{2} \rfloor = \frac{a}{2}$, and if a is odd, then $\lfloor \frac{a}{2} \rfloor = \frac{a-1}{2}$. □

Corollary 4.18. *Let $a > 1$ be a positive integer. Then*

$$g(a, a+1, a+2) = \begin{cases} \frac{a^2}{2} - 1 & \text{if } a \text{ is even.} \\ \frac{(a+1)(a-2)}{2} & \text{if } a \text{ is odd.} \end{cases}$$

Proof. If we set $d = 1$ and a is even, from Corollary 4.17 then we have

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

and if a is odd, then we have

$$\frac{a(a-3)}{2} + (a-1) = \frac{a^2 - 3a + 2a - 2}{2} = \frac{(a+1)(a-2)}{2}.$$

□

Hujter has given the following specific formula in [5], however the proof is given by me because I could not find the reference mentioned in Ramírez Alfonsín's book [9].

Theorem 4.19. *[9, Equation (2.4)] Let $a > 2$ be an integer. Then*

$$g(a^2, a^2+1, a^2+a) = 2a^3 - 2a^2 - 1.$$

Proof. If we investigate the triple (a^2, a^2+1, a^2+a) modulo a^2, we see immediately that the second term is $1 \pmod{a^2}$ and the third term is $a \pmod{a^2}$. Note that with these terms, there are two ways of reaching $[i]$: either $i(a^2+1) \in i \cdot [1]$ which corresponds to the second term, or $\lfloor \frac{i}{a} \rfloor (a^2+a) + (i \bmod a)(a^2+1) \in \lfloor \frac{i}{a} \rfloor \cdot [a] + (i \bmod a) \cdot [1]$ with $0 \le i \bmod a \le a-1$, which corresponds to a combination of the second and third term. Note that for all $a \le i \le a^2 - 1$, the first approach is always greater than the second approach, and for $i < a$ it is the same value. Recall that for this case, $\mathbf{m}(i)$ is the least positive integer congruent to $i \pmod{a^2}$ that is representable by the triple (a^2, a^2+1, a^2+a). As a result of the above observations, we can set $\mathbf{m}(i) = \lfloor \frac{i}{a} \rfloor \cdot [a] + (i \bmod a) \cdot [1]$. Then $\mathbf{m}(i)$ is maximal when $i = a^2 - 1$ and

$$[a^2 - 1] = (a-1) \cdot [a] + (a-1) \cdot [1] = (a-1)(a^2+a) + (a-1)(a^2+1),$$

so we can apply this and Lemma 2.4, which results in

$$\begin{aligned} g(a^2, a^2+1, a^2+a) &= \max_{1\le i\le a^2-1} \mathbf{m}(i) - a^2 \\ &= (a-1)(a^2+a) + (a-1)(a^2+1) - a^2 \\ &= (a^3+a^2-a^2-a) + (a^3+a-a^2-1) - a^2 \\ &= 2a^3 - 2a^2 - 1. \end{aligned}$$

□

Theorem 4.20. *[2] Let a, b, c be pairwise coprime integers such that $a \mid (b+c)$. Then*

$$g(a,b,c) + a = \begin{cases} b\lfloor \frac{ac}{b+c} \rfloor & \text{if } \lfloor \frac{ac}{b+c} \rfloor \ge \frac{(a-1)c}{b+c}; \\ c\lfloor \frac{ab}{b+c} \rfloor & \text{if } \lfloor \frac{ac}{b+c} \rfloor \le \frac{(a-1)c}{b+c}. \end{cases}$$

Proof. [17, Theorem 1 (i)] Since $a \mid (b+c)$, then $\mathbf{m}(i)$ is either of the form bx or cy. Assume otherwise, without loss of generality, that $\mathbf{m}(i) = bx' + cy'$ with $x' > y'$, then

$$bx' + cy' \equiv b(x'-y') + (b+c)y' \equiv b(x'-y') \equiv bx'' \pmod{a}$$

for some $0 < x'' < x'$. Additionally, since $b \equiv -c \pmod{a}$, then $bx \equiv -cx \equiv ca - cx \equiv c(a-x) \pmod{a}$, therefore $\mathbf{m}(bx) = \min\{bx, c(a-x)\}$. Note that

$$bx \le c(a-x) \iff (b+c)x \le ac \iff x \le \frac{ac}{b+c}. \tag{4.2}$$

Observe that also since $\gcd(b,c) = 1$, then $b+c$ divides neither ab nor ac. Then

$$\left\lfloor \frac{ab}{b+c} \right\rfloor + \left\lfloor \frac{ac}{b+c} \right\rfloor = \frac{ab}{b+c} - \frac{s}{b+c} + \frac{ac}{b+c} - \frac{t}{b+c} = a - \frac{(s+t)}{b+c},$$

where $s = ab \pmod{(b+c)}$ and $t = ac \pmod{(b+c)}$, with $0 \le s, t \le b+c-1$. Then we can see that $s+t \equiv ab+ac \equiv a(b+c) \equiv 0 \pmod{(b+c)}$, therefore $(b+c) \mid (s+t)$, but $s+t < 2(b+c)$, which results in the fact that $s+t = b+c$, and

$$\left\lfloor \frac{ab}{b+c} \right\rfloor + \left\lfloor \frac{ac}{b+c} \right\rfloor = a - 1. \tag{4.3}$$

Then, if we apply Lemma 2.4, and notice from Equation (4.2) that the biggest x for which $\mathbf{m}(x) = bx$ is $\lfloor \frac{ac}{b+c} \rfloor$ and consequently the biggest x for which $\mathbf{m}(x) = c(a-x)$ is $\lfloor \frac{ac}{b+c} \rfloor + 1$, we get that

$$\begin{aligned} g(a,b,c) + a &= \max_{1\le x\le a-1} \mathbf{m}(x) \\ &= \max\left\{ b\left\lfloor \frac{ac}{b+c} \right\rfloor, c\Big(a - \Big(1 + \left\lfloor \frac{ac}{b+c} \right\rfloor\Big)\Big) \right\} \\ &= \max\left\{ b\left\lfloor \frac{ac}{b+c} \right\rfloor, c\left\lfloor \frac{ab}{b+c} \right\rfloor \right\}, \end{aligned}$$

where the last equation follows by Equation (4.3). To complete the proof, note that

$$b\left\lfloor \frac{ac}{b+c} \right\rfloor \ge c\left\lfloor \frac{ab}{b+c} \right\rfloor = c\Big(a - 1 - \left\lfloor \frac{ac}{b+c} \right\rfloor\Big) \iff \left\lfloor \frac{ac}{b+c} \right\rfloor \ge \frac{(a-1)c}{b+c},$$

where the opposite holds true as well, with equality when $a = 1$. □

More such formulae for specific cases can be found in Chapter 2 of Ramírez Alfonsín's book [9].

5. Explicit formulae for exact cases when $n = 3$

Ever since Sylvester introduced this problem to the public, nobody has been able to tackle the Frobenius problem for $n = 3$ in a way that would not require some kind of generalization. However, there has been a recent development in 2017, provided by Tripathi [19], where he proved that there are several formulae based on certain conditions that actually cover all possible triples for $g(a, b, c)$. Unfortunately, computational data seems to indicate a discrepancy in Tripathi's results. However, the ideas of the proofs are still worth exploring. In this chapter we provide an account of Tripathi's ideas, and we highlight the places where the discrepancies occur. Our computational evidence implies that perhaps only a small change needs to be made to Tripathi's last two formulae. The preliminary lemmas and definitions are going to be set up and presented in Section 5.1, then Section 5.2 will showcase the main theorem together with the author's modifications, also illustrated by an example.

5.1 Preliminary results and definitions

Recall that we have already seen a notation for the set of *non-representable* numbers in Section 3.2, and a notation for the set of *representable* numbers in Definition 4.3. To reiterate, denote the set of *representable* numbers with respect to $a_1, \ldots, a_n$ by

$$R(a_1, \ldots, a_n) = \{a_1x_1 + \cdots + a_nx_n : x_1, \ldots, x_n \geq 0\}.$$

We also record the facts that

$$NR(a_1, \ldots, a_n) = \mathbb{N} \setminus R(a_1, \ldots, a_n), \text{ and } g(a_1, \ldots, a_n) := \max NR(a_1, \ldots, a_n).$$

We know from Lemma 2.4 that $g(a, b, c)$ is of the form $bx + cy - a$ with some $x, y \geq 0$, so our goal is to find a pair of non-negative integers (x_0, y_0) for which $g(a, b, c) = bx_0 + cy_0 - a$. We also know by the same theorem that $g(a, b, c)$ is the maximum among the largest integers in $NR(a, b, c) \cap [i]$ taken over all non-zero residue classes $[i] \pmod a$. Note that since this chapter deals with the Frobenius number $g(a_1, \ldots, a_n)$ when $n = 3$, then by Lemma 2.4, $\mathbf{m}(i)$ denotes the least positive integer that is representable by a, b, c congruent to $i \pmod a$. We can now introduce a lemma that further restricts the number of triplets that needs to be considered.

Lemma 5.1. *[19, Lemma 1] Let* $\gcd(a, b) = 1$ *and* $a < b$. *Then*

$$g(a, b, c) = \begin{cases} g(a, b) & \text{if } c \in R(a, b); \\ g(a, b) - a & \text{if } c = g(a, b). \end{cases}$$

Proof. If $c \in R(a, b)$, then c is representable by definition, therefore

$$NR(a, b, c) = NR(a, b) \implies g(a, b, c) = \max NR(a, b, c) = \max NR(a, b) = g(a, b).$$

If $c = g(a, b)$ and $n < g(a, b)$, then $n \in R(a, b, c) \iff n \in R(a, b)$. If $\mathbf{m}^*(x)$ and $\mathbf{m}(x)$ denote the least positive integer in $R(a, b) \cap [x]$ and $R(a, b, c) \cap [x]$ respectively, then we have that $\mathbf{m}^*(x) = \mathbf{m}(x)$, except for $[x] = [c]$ by the previous observation. Since $\mathbf{m}(c) = c = g(a, b)$, it follows from Lemma 2.4 that

$$g(a, b, c) = \max_{1 \leq x \leq a-1} \mathbf{m}(x) - a = \mathbf{m}(c) - a = c - a = g(a, b) - a. \qquad \square$$

We can therefore restrict our attention to $c < g(a,b) = ab - a - b$, since by Definition 1.1, all $c > g(a,b)$ are representable by a, b.

Example 5.2. To see these theorems in action, let us take the Chicken Nugget example from before. We have then

$$g(6,9,20) = 3 \cdot g(2,3,20) + 20 \cdot (3-1) = 3 \cdot g(2,3) + 40 = 3 + 40 = 43,$$

which is exactly what we got before as well. Alternatively we could have also reduced 6 and 20, also resulting in

$$g(6,9,20) = 2 \cdot g(3,9,10) + 9 \cdot (2-1) = 2 \cdot g(3,10) + 9 = 2 \cdot 17 + 9 = 43.$$

Alternatively, as mentioned in Remark 4.13, we can reduce it twice by setting $g(1,b,c) = -1$ in the following way:

$$\begin{aligned} g(6,9,20) &= 3 \cdot g(2,3,20) + 20 \cdot (3-1) \\ &= 3 \cdot \big(2 \cdot g(1,3,10) + 3 \cdot (2-1)\big) + 40 = 3 \cdot \big((-2)+3\big) + 40 = 43. \end{aligned}$$

This has already proven to be very useful, but we can do even better with the help of defining two new variables k and ℓ in the following way:

$$k := \left\lfloor \frac{c}{b} \right\rfloor, \qquad \ell := cb^{-1} \pmod{a}. \tag{5.1}$$

Remark 5.3. Here ℓ is the least positive representative in its congruence class. Furthermore, in light of Theorem 4.12, we are assuming that the necessary reductions have already been made, so the inverse b^{-1} exists.

With these, we can further restrict ourselves to $\ell > k$ as a result of the following lemma.

Lemma 5.4. *[19, Lemma 2] Let $a < b < c$ and $\gcd(a,b) = 1$. If $\ell \leq k$, then $g(a,b,c) = g(a,b)$.*

Proof. Since $c \equiv b\ell \pmod{a}$, we can write $c = am + b\ell$ for some $m \in \mathbb{Z}$. Then, since $\ell \leq k = \lfloor \frac{c}{b} \rfloor \leq \frac{c}{b}$ and $a, b, k, \ell > 0$, we have that

$$m = \frac{c - b\ell}{a} \geq \frac{c - b(\frac{c}{b})}{a} \geq 0.$$

This means that c is representable by a, b with non-negative integers m, ℓ, so therefore $g(a,b,c) = g(a,b)$ by Lemma 5.1. □

As noted earlier, we want to find a pair (x_0, y_0) such that $g(a,b,c) = bx_0 + cy_0 - a$ with $x_0, y_0 \geq 0$. To this end, we are going to use the notation $\mathbf{v}(x,y) := bx + cy$ and call this the $\mathbf{v}$-*value* of (x,y).

Lemma 5.5. *[19, Lemma 3] Let a, b, c be pairwise coprime positive integers. Then*

$$g(a,b,c) = \max_{1 \leq x \leq a-1} \left\{ \min_{0 \leq t \leq a-1} \mathbf{v}\big((x + (a-\ell)t) \bmod a, t\big) \right\} - a.$$

Proof. Since $\gcd(a,b) = 1$, by Lemma 2.4 and Lemma 2.3 we have that

$$g(a,b,c) = \left(\max_{1 \leq i \leq a_1 - 1} \mathbf{m}(i) \right) - a = \left(\max_{1 \leq x \leq a_1 - 1} \mathbf{m}(bx) \right) - a.$$

For a fixed x_0 with $1 \leq x_0 \leq a-1$, we have that

$$bx + cy \equiv bx_0 \pmod{a} \iff b(x - x_0) \equiv -cy \equiv -b\ell y \pmod{a} \iff x \equiv x_0 - \ell y \pmod{a}.$$

Hence for $0 \leq t \leq a-1$, the integers $b\big((x_0 - \ell t) \bmod a\big) + ct$ all belong to the class $[bx_0]$. To ensure that we are working with positive numbers, note that $(x_0 - \ell t) \equiv (x_0 - \ell t + at) \equiv \big(x_0 + (a-\ell)t\big) \pmod{a}$.

Minimizing $b\big((x_0-\ell t) \bmod a\big)+ct$ over all t gives the least representable integer congruent to bx_0 modulo a, and then maximizing over all $1 \le x \le a-1$ gives the equation stated in the lemma. □

Since we are trying to minimize over all t to find the smallest representative of the congruence class $[bx_0] \pmod a$, it makes sense to define a local minimum.

Definition 5.6. Let $1 \le x_0 \le a-1$. For $1 \le y_0 \le a-2$, the integer $\mathbf{v}(x_0, y_0)$ is said to be a *local minimum* if

$$\mathbf{v}(x_0, y_0) \le \min\left\{\mathbf{v}\big((x_0-\ell) \bmod a, y_0+1\big), \mathbf{v}\big((x_0+\ell) \bmod a, y_0-1\big)\right\}.$$

If $y_0 = 0$, then $\mathbf{v}(x_0, 0)$ is said to be a *local minimum* if $\mathbf{v}(x_0, 0) \le \mathbf{v}\big((x_0-\ell) \bmod a, 1\big)$.
If $y_0 = a-1$, then $\mathbf{v}(x_0, a-1)$ is said to be a *local minimum* if $\mathbf{v}(x_0, a-1) \le \mathbf{v}\big((x_0+\ell) \bmod a, a-2\big)$.
We say that two local minima, $\mathbf{v}(x_0, y_0)$ and $\mathbf{v}(x_0', y_0')$, are *consecutive* if there is no local minimum $\mathbf{v}(x, y)$ with $y_0 < y < y_0'$.

We are able to speed up the process of finding the minimum $\mathbf{v}$-value of each congruence class by restricting ourselves to the $\mathbf{v}$-values at local minima. To illustrate how this process works, we give a quick example.

Example 5.7. Let $a = 5, b = 13$, and $c = 19$. Then

$$\ell \equiv 19 \cdot 13^{-1} \equiv (-1) \cdot 3^{-1} \equiv (-1) \cdot 2 \equiv 3 \pmod 5.$$

Our process is to run through all $0 \le t \le a-1$ for the $\mathbf{v}$-values given in Lemma 5.5. Set $x_0 = 1$ and $t = 0$, and let us check for local minima starting from $\mathbf{v}(1, 0)$. Then the next step $t = 1$ is

$$\mathbf{v}(1 + (5-3) \bmod 5, 0+1) = \mathbf{v}(3, 1) = 3 \cdot 13 + 1 \cdot 19 > 1 \cdot 13 + 0 \cdot 19 = \mathbf{v}(1, 0).$$

Continuing these steps, we are able to set up the following inequalities:

$$\mathbf{v}(1, 0) < \mathbf{v}(3, 1) > \mathbf{v}(0, 2) < \mathbf{v}(2, 3) < \mathbf{v}(4, 4).$$

From this we can immediately see that there are two local minima, $\mathbf{v}(1, 0)$ and $\mathbf{v}(0, 2)$, which also are consecutive local minima.

Lemma 5.8. *[19, Lemma 4] For each $0 \le t \le a-1$, the difference between two consecutive $\mathbf{v}$-values for the congruence class $[bx]$ is either $b(a-\ell)+c$ or $c-b\ell$.*

Proof. Recall that from Lemma 5.5, the $\mathbf{v}$-values for $[bx]$ are given by $\mathbf{v}\big((x+(a-\ell)t) \bmod a, t\big)$. Then checking the difference of two consecutive $\mathbf{v}$-values gives

$$\begin{aligned}
&\mathbf{v}\Big(\big(x+(a-\ell)(t+1)\big) \bmod a, t+1\Big) - \mathbf{v}\Big(\big(x+(a-\ell)t\big) \bmod a, t\Big) = \\
&= b\Big(\big(x+(a-\ell)(t+1)\big) \bmod a\Big) + c(t+1) - b\Big(\big(x+(a-\ell)t\big) \bmod a\Big) - ct = \\
&= b\big((a-\ell) \bmod a\big) + c = b(a-\ell)+c \text{ or } c-b\ell
\end{aligned}$$

□

In order to compare the $\mathbf{v}$-values at local minima in the congruence class $[bx]$, we see from the above lemma that the list of these integers can be generated in two ways. First option is *increasing* the left component by $a-\ell$ while incrementing the right component by 1, the other one is *decreasing* the left component by ℓ while incrementing the right component by 1. The result will be the same because of the modular reduction, but this gives us two approaches, "Approach 1" and "Approach 2" respectively. Let us call each such operation a *step*. We are going to mainly focus on Approach 1, that is given by the mapping $(x, y) \to \big((x+a-\ell) \bmod a, y+1\big)$.

From Example 5.7, we have seen that a potential local minimum may happen when the x component reduces in value modulo a, i.e. when its value reaches or surpasses a. Since we are adding $a-\ell$ to it, we will be able to utilize their ratio in order to faster identify the other local minima.

Definition 5.9. Let q, r be non-negative integers defined as

$$q := \left\lfloor \frac{a}{a-\ell} \right\rfloor, \quad r := a - q(a-\ell).$$

In other words, q and r are the quotient and remainder of the division $\frac{a}{a-\ell}$ respectively. Thus $a = q(a-\ell) + r$ with $q \geq 1$ and $0 \leq r < a - \ell$.

Remark 5.10. It is true that $r \neq 0$, except for $\ell = a - 1$. This can be seen from the fact that if $r = 0$, then $(a-\ell) \mid a$, and $(a-\ell) \mid c$ because $a \mid \big(c + b(a-\ell)\big)$. Since by assumption $\gcd(a, c) = 1$, the only way for $(a-\ell)$ to divide both a and c is when $\ell = a - 1$. The case when $\ell = a - 1$ is a special case of Theorem 5.14, but it has also already been covered in Theorem 4.20.

We have tackled so far the challenge of finding out the difference between consecutive $\mathbf{v}$-values. The next lemma will go one step further, stating the difference between *consecutive* local minima, which is crucial in order to determine $\mathbf{m}(bx)$. The following lemma gives the said difference, albeit it substantially differs from Tripathi's lemma, which I have found to be incorrect (c.f. Remark 5.12 and Example 5.13). The corrected version is presented below.

Lemma 5.11. *[19, Lemma 5, corrected] Let $\mathbf{v}(x_0, y_0)$ and $\mathbf{v}(x_0', y_0')$ be consecutive local minima with $0 \leq x_0, x_0' < \ell$, and let r_{x_0} denote $a - x_0 \pmod{a-\ell}$. Then*

$$\mathbf{v}(x_0', y_0') - \mathbf{v}(x_0, y_0) = \mathbf{v}\Big((a - r_{x_0} \bmod \ell) - x_0,\ \left\lfloor \frac{a - x_0}{a-\ell} \right\rfloor + \left\lfloor \frac{a - r_{x_0}}{\ell} \right\rfloor\Big).$$

Proof. Since we are deploying Approach 1, we are increasing the x-component by $(a-\ell)$ and the y-component by 1. In practice, if we think inside a modular grid, the values can only increase until we reach $a - (a-\ell) = \ell$, since afterwards we wrap around to the bottom. This wrapping around is the same as *decreasing* the x value by ℓ, which is our Approach 2. This essentially cuts our grid into two sections, where the consecutive x values either only increase or only decrease. In Figure 10, the dashed red line at $\ell = 4$ divides the grid into these sections. The lower red section is where the x value is only increasing and the upper section, where the x value is only decreasing. As a result of this, the only x values for which $\mathbf{v}(x, y)$ can be a local minimum are $0 \leq x < \ell$, because if the x value is in the upper (decreasing) section, at the next step it has to decrease, therefore it cannot be a local minimum by Definition 5.6.

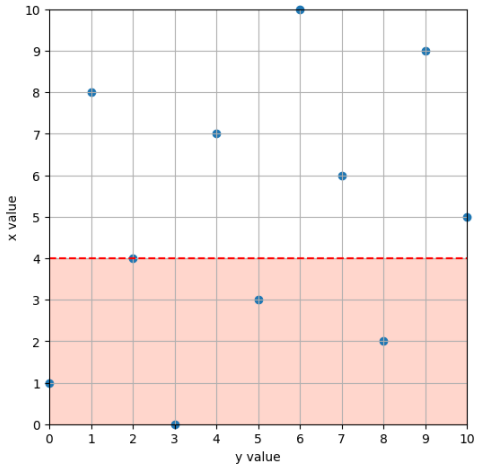

Figure 10: The modular grid for $g(11, 15, 16)$ when $x = 1$. Note the axis labels.

Therefore, for a starting value x_0, for the number of increases, we need to find how many copies of $(a-\ell)$ fit into $(a - x_0)$, and then similarly, for the number of decreases, how many copies of ℓ fit into $(a - r_{x_0})$. The former is clearly $\lfloor \frac{a-x_0}{a-\ell} \rfloor$ and the latter is $\lfloor \frac{a-r_{x_0}}{\ell} \rfloor$, the sum of which is the difference between the initial y_0 value and the consecutive y_0' value.

To calculate the change from x_0, recall that we add $(a-\ell)$ and subtract ℓ as many times as mentioned above, respectively. Observe also that

$$a - x_0 = \left\lfloor \frac{a-x_0}{a-\ell} \right\rfloor (a-\ell) + (a - x_0 \bmod a-\ell) \quad \Longrightarrow \quad \left\lfloor \frac{a-x_0}{a-\ell} \right\rfloor (a-\ell) = a - r_{x_0} - x_0,$$
$$a - r_{x_0} = \left\lfloor \frac{a-r_{x_0}}{\ell} \right\rfloor \ell + (a - r_{x_0} \bmod \ell) \quad \Longrightarrow \quad -\left\lfloor \frac{a-r_{x_0}}{\ell} \right\rfloor \ell = r_{x_0} - a + (a - r_{x_0} \bmod \ell).$$

Now, if we add the two expressions on the right side above, we get that

$$\begin{aligned} x_0' - x_0 &= \left\lfloor \frac{a-x_0}{a-\ell} \right\rfloor (a-\ell) - \left\lfloor \frac{a-r_{x_0}}{\ell} \right\rfloor \ell = a - r_{x_0} - x_0 + r_{x_0} - a + (a - r_{x_0} \bmod \ell) \\ &= (a - r_{x_0} \bmod \ell) - x_0. \end{aligned}$$

Inserting these results into $\mathbf{v}(x_0', y_0') - \mathbf{v}(x_0, y_0)$ yields the statement of the theorem. □

Remark 5.12. Tripathi's original formulation is the following:

"Let $\mathbf{v}(x_0, y_0)$ and $\mathbf{v}(x_0', y_0')$ be consecutive local minima, with $0 \le x_0, x_0' < a - \ell$. Then

$$\mathbf{v}(x_0', y_0') - \mathbf{v}(x_0, y_0) = \begin{cases} \mathbf{v}(a - \ell - r, q+1) & \text{if } 0 \le x_0 < r; \\ \mathbf{v}(-r, q) & \text{if } r \le x_0 < a - \ell. \text{"} \end{cases}$$

Example 5.13. One can easily check that this does not work, for example, for the triple $(11, 15, 16)$, the same triple that was used in Figure 10. For this triple, $a = 11, q = 1$ and $\ell = r = 4$. By Tripathi's lemma, we should expect the next local minimum from $\mathbf{v}(1,0)$ to be $\mathbf{v}(1,0) + \mathbf{v}(11-4-4, 2) = \mathbf{v}(4,2)$, since $x_0 = 1 < 4 = r$. However, we can clearly see from Figure 10 that $(4,2)$ is *not* a local minimum, but rather the next one, namely $\mathbf{v}(0,3)$. The author's correction, however, yields the correct difference between the above mentioned local minima. If we set $(x_0, y_0) = (1,0)$, then $r_{x_0} = 11 - 1 \pmod 7 = 3$, and

$$\begin{aligned} \mathbf{v}(0,3) - \mathbf{v}(1,0) &= \mathbf{v}\Big((a - r_{x_0} \bmod \ell) - x_0,\ \left\lfloor \frac{a-x_0}{a-\ell} \right\rfloor + \left\lfloor \frac{a-r_{x_0}}{\ell} \right\rfloor \Big) \\ &= \mathbf{v}\Big((11 - 3 \bmod 4) - 1, \left\lfloor \frac{11-1}{11-4} \right\rfloor + \left\lfloor \frac{11-3}{4} \right\rfloor \Big) \\ &= \mathbf{v}\Big((8 \bmod 4) - 1, \left\lfloor \frac{10}{7} \right\rfloor + \left\lfloor \frac{8}{4} \right\rfloor \Big) = \mathbf{v}(-1, 3), \end{aligned}$$

which is indeed the correct solution.

Unfortunately, since Tripathi's Lemma 5 has turned out to be incorrect, anything based on this cannot be justified without further investigation. At this point I suspect that with my corrected version, the subsequent Lemma 7 in Tripathi's [19] paper would also hold, but this assumption could not be verified due to time constraints. This and the validity of the other results could be verified in a future paper.

5.2 The explicit formulae for $g(a, b, c)$

For completeness' sake, we are going to state Tripathi's formulae, however, as a result of personal investigations, it has come to light that unfortunately some of the preceding lemmas are incorrect, therefore the validity of these theorems cannot be fully justified. Furthermore, after a substantial checking of the last two theorems during the personal investigations, it is clear that the last two formulae given by Tripathi are incorrect. For these reasons, no proofs are going to be presented in this section.

A potential fix for these shortcomings is proposed by the author, which are going to be highlighted in blue and explained in the remark afterwards. These conjectured fixes rely on the author's computer-

assisted analysis after testing several different ideas. An example is also going to be provided to showcase the discrepancies at the end of this section.

Theorem 5.14. *[19, Theorem 3] If $\ell > k$ and $br < cq$, then*

$$g(a,b,c)+a=\begin{cases} b\big((\lambda+1)(a-\ell)+r-1\big) & \text{if } \lambda \geq \frac{c(q-1)-br}{b(a-\ell)+c};\\ b(a-\ell-1)+c(q-\lambda-1) & \text{if } \lambda \leq \frac{c(q-1)-br}{b(a-\ell)+c}, \end{cases}$$

where $\lambda := \left\lfloor \frac{cq-br}{b(a-\ell)+c} \right\rfloor$.

Definition 5.15. Set $A := br - cq, B := b(a-\ell-r)+c(q+1)$. Then define

$$\Lambda := \left\lfloor \frac{r}{a-\ell-r} \right\rfloor, \quad \Delta := \left\lfloor \frac{A}{B} \right\rfloor; \qquad \Lambda' := \left\lfloor \frac{a-\ell-r}{r} \right\rfloor, \quad \Delta' := \left\lfloor \frac{B}{A} \right\rfloor.$$

Now we can state the main theorem, amended by the author's suggested corrections in blue text.

Theorem 5.16. *[19, Theorem 5] Let $\ell > k$ and $br > cq$. Let $u \equiv a-\ell \pmod r$, and let μ' be the smallest non-negative integer m for which $\lfloor \frac{mB}{A} \rfloor = \lfloor \frac{m(a-\ell-r)}{r} \rfloor$, but $\lfloor \frac{(m+1)B}{A} \rfloor \neq \lfloor \frac{(m+1)(a-\ell-r)}{r} \rfloor$.*

a) If $\mu' < \lfloor \frac{r}{u} \rfloor$,

$$\begin{aligned} g(a,b,c)+a =& \max\Big\{b(r-\mu' u-1),\ b(u-1)+c\big(\mu'(q+1)+(\lfloor \tfrac{(a-\ell-r)\mu'}{r} \rfloor+1)q\big)\Big\}\\ &+cq\left\lfloor \tfrac{(a-\ell-1)}{r} \right\rfloor. \end{aligned}$$

In particular,

i) if $\Lambda > \Delta$,

$$\begin{aligned} g(a,b,c)+a =& \max\Big\{b\big(r-\Delta(a-\ell-r)-1\big),\ b(a-\ell-r-1)+c\big(\Delta(q+1)+q\big)\Big\}\\ &+cq, \end{aligned}$$

ii) if $\Delta' > \Lambda'$,

$$\begin{aligned} g(a,b,c)+a =& \max\Big\{b(r-1),\ b\big((a-\ell-1) \bmod r\big)+cq\Big\}\\ &+cq\left\lfloor \tfrac{(a-\ell-1)}{r} \right\rfloor. \end{aligned}$$

b) If $\mu' > \lfloor \frac{r}{u} \rfloor$, then let $\mathbb{X} = \{x_i : 0 \leq i \leq \mu'\}$, where

$$x_i = r\big(\lfloor \tfrac{(a-\ell-r)i}{r} \rfloor + 1\big) - (a-\ell-r)i.$$

Set $y_i = q\big(\lfloor \frac{(a-\ell-r)i}{r} \rfloor + 1\big) + (q+1)i$ for $0 \leq i \leq \mu'$. Let $x_m = \min \mathbb{X}$ for some $0 \leq m \leq \mu'$, and let d be the largest positive integer such that $x_d + x_m \in \mathbb{X}$. Then

$$g(a,b,c)+a = \max\Big\{b(x_m-1)+cy_d,\ b(x_{m-1}-x_{\mu'}-1)+cy_{\mu'}\Big\} + cq\lfloor \tfrac{a-\ell-1}{r} \rfloor.$$

Remark 5.17. In the statement of the theorem, the first blue amendment was originally

"*and let μ' be the largest non-negative integer m for which $\lfloor \frac{mB}{A} \rfloor = \lfloor \frac{m(a-\ell-r)}{r} \rfloor$*",

and the second blue statement was

"*Let $d_1 = \lceil \frac{r}{u} \rceil u - r$, and $d_2 = \min \mathbb{X}$. Let p_i be the largest positive integer such that $x_{p_i} + d_i \in \mathbb{X}$ for $i = 1, 2$. Then*

$$g(a,b,c)+a = \max\big\{b(d_1-1)+cy_{p_1},\ b(d_2-1)+cy_{p_2}\big\} + cq\lfloor \tfrac{a-\ell-1}{r} \rfloor.$$"

Example 5.18. To illustrate the differences between Tripathi's theorem and the author's corrections, let us take the triple $(100, 103, 111)$. In this case $A = 3700, B = 2900, a = 100, \ell = r = 37$. If we write out the values of $\lfloor \frac{mB}{A} \rfloor$ and $\lfloor \frac{m(a-\ell-r)}{r} \rfloor$ respectively for $0 \leq m \leq 20$, and mark with red text the m values for which the two expressions equal, then the difference in the formulation becomes evident:

$$\left\lfloor \frac{mB}{A} \right\rfloor = \{0, 0, 1, 2, 3, 3, 4, 5, 6, 7, 7, 8, 9, 10, 10, 11, 12, 13, 14, 14, 15\},$$
$$\left\lfloor \frac{m(a-\ell-r)}{r} \right\rfloor = \{0, 0, 1, 2, 2, 3, 4, 4, 5, 6, 7, 7, 8, \ \ 9, \ \ 9, 10, 11, 11, 12, 13, 14\}.$$

In Tripathi's formulation, $\mu' = 10$ since the 10th number is the largest value of m for which the two expression are equal. However, it grossly overestimates the Frobenius number as a result, therefore I assumed that Tripathi meant to stop after the first time they are unequal. My correction is therefore to achieve just that, giving $\mu' = 3$. Continuing, since all conditions are satisfied for part b) of Theorem 5.14, let us write out all necessary variables. Let us first consider Tripathi's original way of defining these variables:

$$\begin{aligned}
\mathbb{X} &= \{37, 11, 22, 33\}, \\
\mathbb{Y} &= \{1, 3, 6, 9\}, \\
d_1 = 15, p_1 = 2 &\implies y_{p_1} = 6, \\
d_2 = 11, p_2 = 2 &\implies y_{p_2} = 6.
\end{aligned}$$

These values can be easily verified, which then lead to the following result:

$$\begin{aligned}
g(a, b, c) &= \max\left\{b(d_1 - 1) + cy_{p_1}, \ b(d_2 - 1) + cy_{p_2}\right\} + cq\lfloor \tfrac{a-\ell-1}{r} \rfloor - a \\
&= \max\left\{103 \cdot 14 + 111 \cdot 6, 103 \cdot 10 + 111 \cdot 6\right\} + 111 - 100 \\
&= 103 \cdot 14 + 111 \cdot 7 - 100 = 2119,
\end{aligned}$$

however, unfortunately, the correct value of $g(100, 103, 111) = 1707$. This overshooting becomes more and more egregious as larger numbers are considered. Now let us calculate the same with my corrections:

$$\begin{aligned}
\mathbb{X} &= \{37, 11, 22, 33\}, \\
\mathbb{Y} &= \{1, 3, 6, 9\}, \\
x_m = 11, d = 2 &\implies y_d = 6, \\
x_{m-1} = 37, x_{\mu'} &= 33, y_{\mu'} = 9.
\end{aligned}$$

These values then lead to the following result:

$$\begin{aligned}
g(a, b, c) &= \max\left\{b(x_m - 1) + cy_d, \ b(x_{m-1} - x_{\mu'} - 1) + cy_{\mu'}\right\} + cq\lfloor \tfrac{a-\ell-1}{r} \rfloor - a \\
&= \max\left\{103 \cdot 10 + 111 \cdot 6, 103 \cdot 3 + 111 \cdot 9\right\} + 111 - 100 \\
&= 103 \cdot 10 + 111 \cdot 7 - 100 = 1707,
\end{aligned}$$

which is indeed the correct result, which can be easily verified by Rødseth's algorithm [11], or any other suitable algorithm.

The author came across the first discrepancy after trying to find a triple to demonstrate part b) of the above theorem. After failing doing it by hand, the theorem was implemented in python to check it against Rødseth's algorithm. Computational evidence suggested that out of the integers triples for which Theorem 5.20 b) can be applied, about 23% is incorrect. The same computational comparison was run for 27 million triples with the author's correction against Rødseth's algorithm with a perfect result, i.e. for all tested numbers, the values matched up. For the implementation of Rødseth's algorithm please refer to Appendix B.

A. Appendix

A.1 Specific values for $d < 13$

N	d	$g(a,b,c)$
12	5	$g(5,8,9)$
24	5	$g(5,11,18)$
36	5	$g(5,14,27)$
48	5	$g(5,17,53)$
60	7	$g(7,17,33)$
120	7	$g(7,27,73)$
180	7	$g(7,37,187)$
420	11	$g(8,107,109)$
840	11	$g(9,143,353)$

Table A.1: Suggested Frobenius number triples for a given N such that $g(a,b,c) = N$.

A.2 Results for Approach 2

In this section, I am going to give an account of all the theorem and lemmas of Tripathi's [19] paper that concern Approach 2, that is when our main approach is decreasing the x component of $\mathbf{v}(x,y)$ by ℓ, as opposed to Approach 1, where we were adding $(a-\ell)$.

Definition A.1. Let $\overline{q}, \overline{r}$ be non-negative integers defined as

$$\overline{q} := \left\lfloor \frac{a}{\ell} \right\rfloor, \quad \overline{r} := a - \overline{q}\ell.$$

In other words, $\overline{q}$ and $\overline{r}$ are the quotient and remainder of the division $\frac{a}{\ell}$ respectively. Thus $a = \overline{q}\ell + \overline{r}$, with $\overline{q} \geq 1$ and $0 \leq \overline{r} < \ell$.

Remark A.2. It is true that $\overline{r} \neq 0$ unless $\ell = 1$. This can be seen from the fact that if $\overline{r} = 0$, then $\ell \mid a$, and $\ell \mid c$ because $a \mid c - b\ell$. Since by assumption $\gcd(a,c) = 1$, the only way for ℓ to divide both a and c is when $\ell = 1$. The case $\ell = 1$ implies that $\ell \leq k$, which Lemma 5.4 has already covered.

Lemma A.3. *[19, Lemma 6] Let $\mathbf{v}(x_0,y_0)$ and $\mathbf{v}(x_0',y_0')$ be consecutive local minima, with $0 \leq x_0, x_0' < \ell$. Then*

$$\mathbf{v}(x_0',y_0') - \mathbf{v}(x_0,y_0) = \begin{cases} \mathbf{v}(\overline{r},\overline{q}) & \text{if } 0 \leq x_0 < \ell - \overline{r}; \\ \mathbf{v}\big(-(\ell-\overline{r}), \overline{q}+1\big) & \text{if } \ell - \overline{r} \leq x_0 < \ell. \end{cases}$$

Theorem A.4. *[19, Theorem 4] If $\ell > k$ and $b(\ell - \overline{r}) < c(\overline{q}+1)$, then*

$$g(a,b,c) + a = \begin{cases} b(\ell-1) + c(\overline{q}-1) & \text{if } 0 \leq \overline{r} < \ell - k; \\ b(\overline{r}-1) + c\overline{q} & \text{if } \ell - k \leq \overline{r} < \ell. \end{cases}$$

For Approach 2, we state the following parallel definitions with the corresponding suggested corrections for Tripathi's results, written in blue text as well.

Definition A.5. Set $\overline{A} := b(\ell - \overline{r}) - c(\overline{q}+1), \overline{B} := b\overline{r} + c\overline{q}$. Then define

$$\overline{\Lambda} := \left\lfloor \frac{\ell - \overline{r}}{\overline{r}} \right\rfloor, \quad \overline{\Delta} := \left\lfloor \frac{\overline{A}}{\overline{B}} \right\rfloor; \qquad \overline{\Lambda}' := \left\lfloor \frac{\overline{r}}{\ell - \overline{r}} \right\rfloor, \quad \overline{\Delta}' := \left\lfloor \frac{\overline{B}}{\overline{A}} \right\rfloor.$$

Theorem A.6. *[19, Theorem 6] Let $\ell > k$ and $b(\ell - \overline{r}) > c(\overline{q}+1)$. Let $\overline{u} \equiv \overline{r} (\mathrm{mod}\ \ell - \overline{r})$, and let $\overline{\mu}'$ be the smallest non-negative integer m for which $\lfloor \frac{m\overline{B}}{\overline{A}} \rfloor = \lfloor \frac{m\overline{r}}{\ell - \overline{r}} \rfloor$, but $\lfloor \frac{(m+1)\overline{B}}{\overline{A}} \rfloor \neq \lfloor \frac{(m+1)\overline{r}}{\ell - \overline{r}} \rfloor$.*

a) If $\overline{\mu}' \leq \lfloor \frac{\ell - \overline{r}}{\overline{u}} \rfloor$,

$$g(a,b,c) + a = \max\Big\{ b(\ell - \overline{r} - \overline{\mu}'\overline{u} - 1),\ b(\overline{u} - 1) + c\big(\overline{\mu}'\overline{q} + (\lfloor \tfrac{\overline{r}\overline{\mu}'}{\ell - \overline{r}} \rfloor + 1)(\overline{q}+1)\big) \Big\} + c\big((\overline{q}+1)\lfloor \tfrac{\ell - 1}{\ell - \overline{r}} \rfloor - 2\big).$$

In particular,

i) if $\overline{\Lambda} > \overline{\Delta}$,

$$g(a,b,c) + a = \max\Big\{ b(\overline{r} - 1) + c\overline{q}(\overline{\Delta} + 2),\ b\big(\ell - (\overline{\Delta}+1)\overline{r} - 1\big) + c(\overline{q} - 1) \Big\},$$

ii) if $\overline{\Delta}' > \overline{\Lambda}'$,

$$g(a,b,c) + a = \max\Big\{ b\big(\overline{r} - 1 \bmod (\ell - \overline{r})\big) + c(\overline{q}+1),\ b(\ell - \overline{r} - 1) \Big\} + c\big((\overline{q}+1)\lfloor \tfrac{\ell - 1}{\ell - \overline{r}} \rfloor - 2\big).$$

b) If $\overline{\mu}' > \lfloor \frac{\ell - \overline{r}}{\overline{u}} \rfloor$, then let $\overline{\mathbb{X}} = \{x_i : 0 \leq i \leq \overline{\mu}'\}$, where

$$x_i = (\ell - \overline{r})\big(\lfloor \tfrac{\overline{r}i}{\ell - \overline{r}} \rfloor + 1\big) - \overline{r}i.$$

Set $y_i = (\overline{q}+1)\big(\lfloor \frac{\overline{r}i}{\ell - \overline{r}} \rfloor + 1\big) + \overline{q}i$ for $0 \leq i \leq \overline{\mu}'$. Let $x_m = \min \overline{\mathbb{X}}$ for some $0 \leq m \leq \overline{\mu}'$, and let d be the largest positive integer such that $x_d + x_m \in \overline{\mathbb{X}}$. Then

$$g(a,b,c) + a = \max\Big\{ b(x_m - 1) + cy_d,\ b(x_{m-1} - x_{\overline{\mu}'} - 1) + cy_{\overline{\mu}'} \Big\} + c\big((\overline{q}+1)\lfloor \tfrac{\ell - 1}{\ell - \overline{r}} \rfloor - 2\big).$$

Remark A.7. The original statement for the first blue line is

"and let $\overline{\mu}'$ be the largest non-negative integer m such that $\lfloor \frac{m\overline{B}}{\overline{A}} \rfloor = \lfloor \frac{m\overline{r}}{\ell - \overline{r}} \rfloor$",

and the second blue text was written in the following way:

"Let $d_1 = \lceil \frac{\ell - \overline{r}}{\overline{u}} \rceil \overline{u} - (\ell - \overline{r})$, and $d_2 = \min \overline{\mathbb{X}}$. Let p_i be the largest positive integer such that $x_{p_i} + d_i \in \overline{\mathbb{X}}$ for $i = 1, 2$. Then

$$g(a,b,c) + a = \max\Big\{ b(d_1 - 1) + cy_{p_1},\ b(d_2 - 1) + cy_{p_2} \Big\} + c\big((\overline{q}+1)\lfloor \tfrac{\ell - 1}{\ell - \overline{r}} \rfloor - 2\big)."$$

Just as previously, these corrections are also based on computer-assisted investigation, where these parallel theorems also failed to the same extent as Approach 1 with a 23% failure rate.

B. Python code for Rødseth's algorithm

Rødseth's algorithm for finding the Frobenius number is restricted to three pairwise coprime positive integers, however, this is not an issue considering the fact that Johnson's formula (Theorem 4.12) allows all valid triples to be reduced to pairwise coprime integers. The algorithm that I implemented in Python is the one mentioned in Ramírez Alfonsín's [9] book in Section 1.1.1.

```
def rodseth(A,B,C):

    # Check if triple is relatively prime
    if gcd(A,gcd(B,C))==1:

        # Reduce the numbers to pairwise coprime
        d_ab, d_bc, d_ac = gcd(A,B), gcd(B,C), gcd(A,C)
        a, b, c = int(A/d_ab/d_ac), int(B/d_ab/d_bc), int(C/d_bc/d_ac)

        # Perform Rodseth's main algorithm
        b_mod=b % a
        c_mod=c % a
        s_0 = (pow(b_mod,-1,a)*c_mod) % a

        s_list=[a,s_0] #s_0 = index 1
        q_list=[0]     #q_1 = index 1
        p_list=[0,1]   #p_0 = index 1

        while b*s_list[-1]-c*p_list[-1] > 0:
            q_list.append(ceil(s_list[-2]/s_list[-1])) #q_1 = ceil(s_{-1}/s_0)
            s_list.append(q_list[-1]*s_list[-1]-s_list[-2]) # s_1 = q_1 * s_0 - s_{-1}
            p_list.append(q_list[-1]*p_list[-1]-p_list[-2]) #p_1 = q_1 * p_0 - p_{-1}

        pairwise_coprime_result = -a + b*(s_list[-2]-1)+c*(p_list[-1]-1)-min(b*s_list
    [-1],c*p_list[-2])

        # Use Johnson's reduction formula to get the result
        frobenius_number = d_ab*d_bc*d_ac*pairwise_coprime_result + A*(d_bc-1) + B*(d_ac
    -1) + C*(d_ab-1)

        return int(frobenius_number)

    else:
        return f"The Frobenius number does not exist for the numbers {A,B,C} as they
    share a common divisor of {gcd(A,gcd(B,C))}."
```

Bibliography

[1] A. Brauer. "On a problem of partitions". In: *Amer. J. Math.* **64** (1942), pp. 299–312.

[2] A. Brauer and J.E. Shockley. "On a problem of Frobenius." In: *J. Reine Angew. Math.* **211** (1962), pp. 215–220.

[3] T.C. Brown and P.J.-S. Shiue. "A remark related to the Frobenius problem". In: *Fib. Quart.* **31** (1993), pp. 32–36.

[4] F. Curtis. "On formulas for the Frobenius number of a numerical semigroup". In: *Math. Scand.* **67**.2 (1990), pp. 190–192.

[5] M. Hujter. *On the lowest value of the Frobenius number*. Tech. rep. **MN/31** Computer and Automation Inst., Hungarian Academy of Sciences, 1987.

[6] S.M. Johnson. "A Linear Diophantine Problem". In: *Canad. J. Math.* **12** (1960), pp. 390–398.

[7] C. Kifer. *Extending the Linear Diophantine Problem of Frobenius*. 2010. URL: `https://matthbeck.github.io/teach/masters/curtis.pdf`. (accessed: 12.06.2023).

[8] Numberphile. *How to order 43 Chicken McNuggets - Numberphile*. URL: `https://www.youtube.com/watch?v=vNTSugyS038`. (accessed: 04.06.2023).

[9] J.L. Ramírez Alfonsín. *The Diophantine Frobenius problem*. Vol. 30. Oxford Lecture Series in Mathematics and its Applications. Oxford University Press, Oxford, 2005, pp. xvi+243.

[10] J.B. Roberts. "Note on linear forms". In: *Proc. Amer. Math. Soc.* **7** (1956), pp. 465–469.

[11] Ø. J. Rödseth. "On a linear Diophantine problem of Frobenius." In: *J. Reine Angew. Math.* **301** (1978), pp. 171–178.

[12] J.C. Rosales, P.A. García-Sánchez, and J.I. García-García. "Every positive integer is the Frobenius number of a numerical semigroup with three generators". In: *Math. Scand.* **94** (2004), pp. 5–12.

[13] E.S. Selmer. "On the linear Diophantine problem of Frobenius". In: *J. Reine Angew. Math.* **293/294** (1977), pp. 1–17.

[14] J.J. Sylvester. "On Subvariants, i.e. Semi-Invariants to Binary Quantics of an Unlimited Order". In: *Amer. J. Math.* **5**.1 (1882), pp. 79–136.

[15] J.J. Sylvester. "Mathematical questions with their solutions". In: *Educational Times* **41** (1884), p. 21.

[16] A. Tripathi. *On a Linear Diophentine Problem of Frobenius*. Indian Institute of Technology Delhi. 2006. URL: `https://web.iitd.ac.in/~atripath/publications/FP.pdf`. (accessed: 21.12.2023).

[17] A. Tripathi. "A Note on a Special Case of the Frobenius Problem". In: *Indian J. Pure Appl. Math.* **44**.3 (2013), pp. 375–381.

[18] A. Tripathi. "The Frobenius problem for modified arithmetic progressions". In: *J. Integer Seq.* **16**.7 (2013), p. 13.7.4.

[19] A. Tripathi. "Formulae for the Frobenius number in three variables". In: *J. Number Theory* **170** (2017), pp. 368–389.

[20] D.E. Varberg. "Pick's Theorem Revisited". In: *Am. Math. Monthly* **92**.8 (1985), pp. 584–587.

Bachelor's Theses in Mathematical Sciences 2024:K3
ISSN 1654-6229

LUNFMA-4161-2024

Mathematics
Centre for Mathematical Sciences
Lund University
Box 118, SE-221 00 Lund, Sweden

http://www.maths.lu.se/