THE FROBENIUS PROBLEM

by

Sambandam Ekambaram

M.Sc., Simon Fraser University, 1987

THESIS SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

in the Department

of

MATHEMATICS AND STATISTICS

SIMON FRASER UNIVERSITY

January 1991

APPROVAL

Name: Sambandam Ekambaram

Degree: Ph.D. (Mathematics)

Title of Thesis: The Frobenius Problem

Examining Committee:

Chairman: Prof. A. H. Lachlan

Dr. T. C. Brown, Professor
Senior Supervisor

Dr. A. R. Freedman, Professor

Dr. K. Heinrich, Professor

Dr. S. K. Thomason, Professor

Dr. William Yslas Vélez, Professor
Department of Mathematics
University of Arizona
External Examiner

Date Approved: January 8, 1991

PARTIAL COPYRIGHT LICENSE

I hereby grant to Simon Fraser University the right to lend my thesis, project or extended essay (the title of which is shown below) to users of the Simon Fraser University Library, and to make partial or single copies only for such users or in response to a request from the library of any other university, or other educational institution, on its own behalf or for one of its users. I further agree that permission for multiple copying of this work for scholarly purposes may be granted by me or the Dean of Graduate Studies. It is understood that copying or publication of this work for financial gain shall not be allowed without my written permission.

Title of Thesis/Project/Extended Essay

THE FROBENIUS PROBLEM

Author:

(signature)

S. EKAMBARAM

(name)

Jan 8, '91

(date)

ABSTRACT

The purpose of this thesis is to investigate the partition problem of Frobenius. Given relatively prime positive integers $a_0, a_1, \ldots, a_s$, the problem of Frobenius is to find the largest positive integer $g(a_0, a_1, \ldots, a_s)$ which cannot be represented as a linear combination of $a_0, a_1, \ldots, a_s$ with non-negative integer coefficients. For s =1, the exact value of $g(a_0, a_1)$ was found by J. J. Sylvester back in 1884 . I. Shur was the first to give an upper bound for the number $g(a_0, a_1, \ldots, a_s)$ for any $s \geq 1$.

In this thesis we find upper bounds for $g(a_0, a_1, \ldots, a_s)$ for any s in specific cases using additive number theory and show that these bounds are better than the best known upper bounds. We also study the greatest common divisor d of $a_0, a_1, \ldots, a_{s-1}$ and using this we prove that Lewin's conjecture

$$(*) \qquad g(a_0, a_1, \ldots, a_s) \leq \left[\frac{(a_s - 2)\,(a_s - s)}{s}\right] - 1$$

holds good in the special case when $\frac{a_i}{i} \leq \frac{a_{i+1}}{i+1}$, where $[x]$ denotes the largest integer $\leq x$. We also obtain a better upper bound for the case s=3 when $d \geq 2$. For $s = 2$, we find the exact value of $g(a, b, c)$ where $b + c \equiv 0 (\mathrm{mod}\ a)$. An algorithm to find an upper bound for $g(a_0, a_1, \ldots, a_s)$ for any $s \geq 3$ is given. We also investigate a related problem of the representation of positive integers by trees and give a different proof for finding the *conductor* $\kappa(g_0, g_1, g_2, \ldots, g_k)$ of a $(g_0, g_1, g_2, \ldots, g_k)$-tree.

In Chapter 1 we prove the existence of the number theoretic function $g(a_0, a_1, \ldots, a_s)$ and study two related functions that arise naturally in connection with $g(a_0, a_1, \ldots, a_s)$. We conclude this Chapter by presenting the exact solution to the problem for $s = 1$.

In Chapter 2 we determine the exact value of $g(a, b, c)$ of relatively prime integers a, b, c when $b + c \equiv 0 (\text{mod } a)$. While the case $s = 1$ is easy, it appears that all the difficulties of the problem in the general case are contained in the case $s = 2$. So we study the effect of extending $\{a, b\}$ of relatively prime integers to $\{a, b, c\}$ where c is non-representable by a, b, and prove that $g(a, b, c) \leq g(a, b) - a$. Also, we show that this bound is sharp.

In Chapter 3 we use addition theorems in Number Theory and deduce upper bounds in special cases which are better than the best known upper bounds. We also prove that the conjecture (*) holds for any s when $\frac{a_i}{i} \leq \frac{a_{i+1}}{i+1}$ for $i = 2, 3, \ldots, s - 1$. If the g.c.d$(a_0, a_1, a_2) = d$, $d \geq 2$, then we find an upper bound for $g(a_0, a_1, a_2, a_3)$ which is better than the known bounds. An algorithm to find an upper bound for $g(a_0, a_1, \ldots, a_s)$, when a_0 is relatively prime to each a_i, is also described.

In Chapter 4 we study the related problem of finding the *conductor* of a $(g_0, g_1, g_2, \ldots, g_k)$-tree. We give a proof for finding the exact value of the conductor of $\kappa(a, a + 1)$ and deduce the exact value of $\kappa(a, a+1, \ldots, a+s)$ for any s, $s \geq 1$.

DEDICATION

To my father Shri. Tulasi Sambandam.

Swamiyé Saranam Iyappà

ACKNOWLEDGEMENTS

I cannot find words within me strong enough to adequately express my sincerest gratitude to Dr. Tom Brown for suggesting the problem, for his continued guidance, for his smiling readiness to help at all times, for his wisdom in dealing with my trying times, for his critical comments while reading the written work and for his financial support.

I would like to thank the Department of Mathematics and Simon Fraser University for the financial support throughout my graduate work . Many thanks to Maggie Fankboner for her help in functioning efficiently as a graduate assistant and also to Sylvia Holmes especially for informing me of regulations and deadlines. It is a pleasure to thank Mr. Rod Lapsley with whom I had several enjoyable discussions in Mathematics.

As for my family, I am ever grateful to my mother who has dedicated her life for the education of her sons, and today her wish is fulfilled. Though far from home, it is my brother Shri. S. Amirthalingam whose love, support and total commitment towards all my endeavours made me to complete my Ph.D program. May God bless you both for ever! Also, I would like to thank my sister-in-law Mrs. Sumathi Amirthalingam for taking good care of my mother. I appreciate my wife Malarvizhi who assumed full family-responsibility, leaving me entirely for my studies.

TABLE OF C0NTENTS

CHAPTER 3

CHAPTER 4

LIST OF FIGURES

CHAPTER 1

1.1 ***Introduction.*** Let $S = \{a_0, a_1, \ldots, a_s\}$ be a set of relatively prime positive integers where $a_i > 1$ for all i. Define

$$Sp(S) = \left\{ \sum_{i=0}^{s} x_i a_i : x_i \text{ is a non-negative integer for } i = 0, 1, \ldots, s \right\}.$$

It is shown in section 1.2 that $Sp(S)$ contains all but finitely many non-negative integers. We denote the largest integer not in $Sp(S)$ by $g(a_0, a_1, \ldots, a_s)$ or by $g(S)$. Given $S = \{a_0, a_1, \ldots, a_s\}$, we say a non-negative integer n is *representable* by $a_0, a_1, \ldots, a_s$, if and only if $n \in Sp(S)$. Otherwise we say n is *non-representable*.

We note that $g(a_0, a_1, \ldots, a_s)$ is precisely the largest integer N which cannot be expressed by $a_0, a_1, \ldots, a_s$ in the form

$$N = \sum_{i=0}^{s} a_i x_i,$$

with non-negative integral coefficients x_i.

The problem of Frobenius consists of finding $g(S)$ or at least obtaining non-trivial upper bounds for $g(S)$ for any given set $S = \{a_0, a_1, \ldots, a_s\}$ of relatively prime positive integers. For $s = 1$, with g.c.d.$(a_0, a_1) = 1$,

$$g(a_0, a_1) = a_0 a_1 - a_0 - a_1 \tag{1}$$

has been known [21] for over a hundred years.

A concrete algorithm ([3], [18]) is known for finding the exact value of $g(a_0, a_1, a_2)$ for integers a_0, a_1, a_2, $1 < a_0 < a_1 < a_2$ with g.c.d.$(a_0, a_1, a_2) = 1$. However for $s \geq 3$, the exact value of $g(a_0, a_1, \ldots, a_s)$ as a closed formula in $a_0, a_1, \ldots, a_s$ is <u>not</u> known except in special cases, for example, when $a_0, a_1, \ldots, a_s$ are consecutive integers [2], or when $a_0, a_1, \ldots, a_s$ are in arithmetic progression [1,17].

We say a set $S = \{a_0, a_1, \ldots, a_s\}$, $1 < a_0 < a_1 < \ldots < a_s$, of integers is *independent* if $a_i \notin Sp(a_0, a_1, \ldots, a_{i-1})$ for $i = 1, 2, \ldots, s$.

The set

$$\{x : a \leq x \leq b \text{ and } x \text{ is an integer}\}$$

of integers between two integers a and b, $a < b$, including a and b is denoted by $[a, b]$. If a divides b, we write $a \mid b$.

In this chapter, the next section begins with the proof of the basic fact that $g(a_0, a_1, \ldots, a_s)$ exists. Then we make some observations on the two best known functions that arise naturally in connection with $g(a_0, a_1, \ldots, a_s)$. We conclude Chapter 1 by presenting the complete solution to the Frobenius problem for $s = 1$.

In Chapter 2 we are concerned with the study of the Frobenius problem for three variables a, b, c. Let g.c.d. $(a, b) = 1$. Let $\{a, b\}$ be extended to an independent set $\{a, b, c\}$. We prove that $g(a, b, c) \leq g(a, b) - a$. In the special case when $c + b \equiv 0 \pmod{a}$, we obtain the exact solution for $g(a, b, c)$. In general we prove that

$$g(a, b, c) \leq g(a, b) - a.$$

We also show that if $c = g(a, b)$, then equality holds. Conversely, if equality holds we show that $b|(a + c)$.

In Chapter 3 we study the best known upper bounds for any $s \geq 2$. We obtain new upper bounds in special cases and show that they are better than the best known upper bounds. We prove that the conjecture of M. Lewin [14]

$$g(S) \leq \left[\frac{(a_s - 2)(a_s - s)}{s}\right] - 1$$

is valid in the special case of $S = \{a_0, a_1, \ldots, a_s\}$ which satisfies

$$\frac{a_i}{i} \leq \frac{a_{i+1}}{i+1}, \; i = 2, 3, \ldots, s - 1.$$

We also give examples to show that this bound is better than the best known upper bounds. A computational method is also studied to obtain a non-trivial upper bound for $s = 3$ and the method is generalized to $s \geq 3$.

In Chapter 4 we study the problem of finding the *conductor* of a $(g_0, g_1, \ldots, g_k)$–tree, which is related the Frobenius problem. We give a different proof for finding the exact value of the conductor $\kappa(a, a+1, \ldots, a+s)$ for any $s \geq 1$.

1.2 ***The existence of*** $g(a_0, a_1, \ldots, a_s)$. In the beginning of this chapter we mentioned that $Sp(S)$ contains all but finitely many non-negative integers for any given $S = \{a_0, a_1, \ldots, a_s\}$ of relatively prime positive integers. We will prove this fundamental fact.

1.2.1 ***Theorem.*** Let $S = \{a_0, a_1, \ldots, a_s\}$ and g.c.d.$(a_0, a_1, \ldots, a_s) = 1$. Then there exists an n_0 such that $n \in Sp(S)$ for all $n \geq n_0$.

Proof. Since g.c.d.$(a_0, a_1, \ldots, a_s) = 1$, there exist integers x_i such that

$$\sum_{i=0}^{s} x_i a_i = 1.$$

Let $$N = a_0 \sum_{i=0}^{s} |x_i| a_i$$

Then, $$N + m = a_0 \sum_{i=0}^{s} |x_i| a_i + m \sum_{i=0}^{s} x_i a_i,$$

(2) $$N + m = \sum_{i=0}^{s} (a_0 |x_i| + m x_i) a_i.$$

Now,

$a_0|x_i| + mx_i = x_i(a_0 + m)$, if $x_i \geq 0$, and

$a_0|x_i| + mx_i = -x_i(a_0 - m)$ if $x_i < 0$.

Therefore if $m \in [0, a_0 - 1]$, then $a_0|x_i| + mx_i \geq 0$ for each $i = 0, 1, \ldots, s$.

Hence (2) implies that for each m in $[0, a_0 - 1]$

$$N + m \in Sp(S).$$

If $m \geq a_0$, then

$$m = p\,a_0 + q,\ 0 \le q \le a_0 - 1 \text{ and } N + m = p\,a_0 + (N + q)$$

so that $(N + m) \in Sp(S)$. Hence $Sp(S)$ contains all $n \ge N$. This completes the proof of the theorem.

1.3 *Related functions.*

1.3.1 ***Definition.*** For integers $1 < a_0 < a_1 < \ldots < a_s$, with g.c.d.$(a_0, a_1, \ldots, a_s) = 1$, we define $f(a_0, a_1, \ldots, a_s)$ to be the largest integer N which can not be expressed in the form

$$N = \sum_{i=0}^{s} x_i\, a_i$$

with integral coefficients $x_i \ge 1$.

From the definition of the two numbers $f(a_0, a_1, \ldots, a_s)$ and $g(a_0, a_1, \ldots, a_s)$ it immediately follows that

$$f(a_0, a_1, \ldots, a_s) = g(a_0, a_1, \ldots, a_s) + \sum_{i=0}^{s} a_i. \tag{3}$$

1.3.2 ***Definition.*** Given a set $S = \{a_0, a_1, \ldots, a_s\}$ of relatively prime positive integers, the number of integers x, $0 \le x \le g(S)$, such that $x \notin Sp(S)$ is denoted by $n(a_0, a_1, \ldots, a_s)$.

Remark. If $0 \le x \le g(S)$, then x and $g(S) - x$ can not both belong to $Sp(S)$. For, writing

$$g(S) = (g(S) - x) + x,$$

we observe that if both x and $g(S) - x$ belong to $Sp(S)$, then $g(S) \in Sp(S)$, a contradiction. Since $|\{0, 1, 2, \ldots, g(S)\}| = g(S) + 1$, we deduce that at least half of the elements in this set are are non-representable. That is,

$$\frac{g(S) + 1}{2} \leq n(S) \leq g(S). \tag{4}$$

In fact as we will see below in theorem 1.5.1 the bounds for $n(S)$ given above are sharp. For $s = 1$,

$$\frac{g(S) + 1}{2} = n(S)$$

and when $S = \{k, k+1, \ldots, 2k-1\}$, it is easy to see that

$$g(S) = k - 1, \qquad n(S) = k - 1.$$

Moreover we note that this is the only case in which $g(S) = n(S)$.

1.3.3 ***Definition.*** Given integers $n \geq 2$ and $t \geq 3$ we define

$$G(n, t) = max\ g(S),$$

where the maximum is taken over all sets $S = \{a_0, a_1, \ldots, a_{n-1}\}$ of relatively prime integers with $2 \leq a_0 < \ldots < a_{n-1} \leq t$.

1.3.4 ***Bounds for G(n, t).*** We easily see from (1) that

$$G(2, t) = g(t-1, t) = (t-2)(t-1) - 1. \tag{5}$$

Y.Vitek [22] has shown that

$g(a, b, c) \leq \left[\frac{a}{2}\right](c - 2) - 1$, for any integers $1 < a < b < c$ which are relatively prime.

For $c = t$, we have

$$\left[\frac{a}{2}\right] \leq \left[\frac{t-2}{2}\right] \text{ and } c - 2 \leq t - 2$$

so that

$$G(3, t) \leq \left[\frac{t-2}{2}\right](t-2) - 1.$$

Since then $t-2, t-1, t$ are in arithmetic progression, using [17] we obtain

$$g(t-2, t-1, t) = \left(\left[\frac{t-4}{2}\right]+1\right)(t-2) - 1,$$

$$= \left[\frac{t-2}{2}\right](t-2) - 1.$$

Hence we conclude that

$$G(3, t) = \left[\frac{t-2}{2}\right](t-2) - 1.$$

For any $n \geq 2$, using the bound

$$g(a_0, \ldots, a_{n-1}) \leq 2\left[\frac{a_{n-1}}{n}\right] a_{n-2} - a_{n-1},$$

which was proved by P. Erdös and R. L. Graham [7], we deduce that

$$G(n, t) < \frac{2\,t^2}{n}$$

We can improve this further by using the bound

$$g(a_0, \ldots, a_{n-1}) \leq \frac{a_{n-1}^2}{n-1}$$

obtained by Y.Vitek [23] so that

$$G(n, t) \leq \frac{t^2}{n-1}.$$

We now find a lower bound. It is easy to see that for the set

$$\{x, 2x, \ldots, (n-1)x, x^*\},\ x = \left[\frac{t}{n-1}\right] \text{ and } x^* = (n-1)\,x - 1,$$

$$G(n, t) \geq g(x, 2x, \ldots, x^*) = g(x, x^*) \geq \frac{t^2}{n-1} - 3\,t.$$

Therefore for any $n \geq 2$, we have

$$\frac{t^2}{n-1} - 3t \le G(n,t) \le \frac{t^2}{n-1}.$$

Very recently Jacques Dixmier [6] improved the upper bound for $G(n, t)$ and showed that for $t > n \ge 2$,

$$G(n,t) = t\left(\left\lceil \frac{t-1}{n-1} \right\rceil - 1\right) - 1.$$

1.4. ***An analytical form of the Frobenius problem.*** Define the rational function $f(z)$ by

$$f(z) = \frac{1}{(1-z^{a_0})(1-z^{a_1})\ldots(1-z^{a_s})},$$

for any complex number z. Then $f(z)$ is the generating function for the number $r_S(n)$ of representations of n of the form

$$n = \sum_{i=0}^{s} a_i x_i$$

with integral coefficients $x_i \ge 0$. So we may write

$$f(z) = \sum_{n=0}^{\infty} r_S(n)\, z^n.$$

Now it is easy to see that $g(a_0, a_1, \ldots, a_s)$ is precisely the largest integer k for which $f^{(k)}(0) = 0$.

1.5. *The Exact Solution for s = 1.*

1.5.1. ***Theorem.*** For relatively prime integers a, b, $2 \le a < b$, we have

$$(i)\ g(a, b) = ab - a - b,$$

$$(ii)\ n(a, b) = \frac{g(a, b) + 1}{2}.$$

Proof of (*i*). We first observe that the condition that g.c.d.$(a, b) = 1$ implies that

$$\{bt : t = 1, 2, \ldots, a - 1\}$$

forms a system of all non-zero residues modulo a.

Now we claim that in each non-zero residue class *r(mod a)*, the largest non-representable number has the form $bt - a$, $1 \le t \le a - 1$. Suppose $bt - a = xa + yb$, where $1 \le t \le a - 1$, $x \ge 0$, $y \ge 0$. Then $b(t - y) = (x+1)a$. Since g.c.d.$(a,b) = 1$, it follows that $a \mid (t - y)$. Since $0 \le y < t$, we must have $a \le t$, a contradiction.

Therefore by definition,

$$g(a, b) = max\{bt - a : t = 0, 1, 2, \ldots, a - 1\},$$

$$= b(a - 1) - a.$$

This proves (*i*).

Now we show (*ii*). We need a Lemma.

1.5.2 ***Lemma.*** Let g.c.d.$(a, b) = 1$. Then exactly one of the integers x and $g(a, b) - x$ belongs to $Sp(a,b)$, for each x, $0 \le x \le g(a, b)$.

Proof of the Lemma. We note that for any $x \le g(a, b)$, both x and $g(a, b) - x$ can not be representable by a, b. Otherwise,

$$g(a, b) = (g(a, b) - x) + x$$

would be representable by a, b. In other words,

(6) $x \in Sp(a, b)$ implies that $g(a, b) - x \notin Sp(a, b)$.

On the other hand, suppose $x \notin Sp(a, b)$. As g.c.d.$(a, b) = 1$, we can find non-negative integers m, n such that

$$x = m\,a - n\,b.$$

If $m \geq b$, then write $m = j\,b + k$, $0 \leq k \leq b - 1$ and $j \geq 1$.

Now, $x = jba + ka - nb$, and therefore $x = ka - (n - ja)b$, $0 \leq k \leq b - 1$. Since x is non-representable by a, b, $n - j\,a \geq 1$. So we can write x in the form

$$x = m\,a - n\,b$$

where $0 \leq m \leq b - 1$ and $n \geq 1$. Now

$$g(a, b) - x = ab - a - b - (ma - nb) = (b - m - 1)a + (n - 1)b.$$

Since $m \leq b - 1$ and $n \geq 1$, the coefficients $b - m - 1$ and $n - 1$ are both non-negative. This shows that

(7) $x \notin Sp(a, b)$ implies that $g(a, b) - x \in Sp(a, b)$.

From (6) and (7) it follows that exactly one of the numbers

$$g(a, b) - x \text{ and } x$$

is representable for all $0 \leq x \leq g(a, b)$.

Proof of (ii). From the above Lemma it follows that exactly half of the members in the set $\{0, 1, \ldots, g(a, b)\}$ belong to $Sp(a, b)$. This proves (*ii*).

CHAPTER 2

2.1 *Basic results.*

2.1.1 Given a set $S = \{a_0, a_1, \ldots, a_s\}$ of relatively prime integers, $1 < a_0 < a_1 < \ldots < a_s$, suppose some a_i is representable by $a_0, a_1, \ldots, a_{i-1}$. Then it is easy to see that any integer n is representable by $a_0, a_1, \ldots, a_s$ if and only if n is representable by $\{a_0, a_1, \ldots, a_s\} \setminus \{a_i\}$. Hence

$$Sp(S) = Sp(S - \{a_i\})$$

This implies that we can delete a_i from the given set S without affecting the value of $g(S)$. Hence we may assume that no a_i is representable by the preceding ones.

2.1.2 ***Definition***. We say that a set of integers $S = \{a_0, a_1, \ldots, a_s\}$, $1 < a_0 < a_1 < \ldots < a_s$, is *independent* if no a_i is representable by $a_0, a_1, \ldots, a_{i-1}$ for $i = 1, 2, \ldots, s$.

Remark. Note that any given set S of positive integers always contains a maximal independent set S'. By 2.1.1 $g(S) = g(S')$. Therefore it is no restriction to assume that S is independent.

2.1.3 ***Definition.***. Given a set $S = \{a_0, a_1, \ldots, a_s\}$ of relatively prime integers, we denote by $t_r = t_r(a_0, a_1, \ldots, a_s)$ the smallest integer $\equiv r \pmod{a_0}$ such that

$$t_r = \sum_{i=1}^{s} a_i x_i, \tag{1}$$

for non-negative integers x_i.

It is trivial that for $r = 0$, $t_r = 0$. By the definition of t_r, it follows that $t_r - a_0$ is the largest integer $\equiv r \pmod{a_0}$ which can not be expressed in the form

$$t_r = \sum_{i=1}^{s} a_i x_i \tag{2}$$

for any non-negative integral coefficients x_i. From this we obtain

2.1.4 ***Proposition*** [3]. Let g.c.d. $(a_0, a_1, \ldots, a_s) = 1$. Then

$$g(a_0, a_1, \ldots, a_s) = \max\{t_r : r = 0, 1, \ldots, a_0 - 1\} - a_0. \tag{3}$$

2.1.5 ***Remark.*** We may use any a_i instead of a_0 in the above Proposition.

The number of positive integers which can not be represented by $a_0, a_1, \ldots, a_s$ is easily determined by considering the positive integers $\leq t_r$ in the residue class $r \pmod{a_0}$, say,

$$\{r, r + a_0, r + 2a_0, \ldots, r + ma_0 = t_r\}$$

where $1 \leq r \leq a_0 - 1$. All integers in this set $< t_r$ are non-representable by the definition of t_r. Now

$$\frac{t_r - r}{a_0} = m,$$

which is precisely the number of positive integers non-representable by $a_0, a_1, \ldots, a_s$ in the residue class r (mod a_0). Thus, using the notation

$$R(a_0) = \{1,2, \ldots, a_0 - 1\}$$

we obtain

$$n(a_0, a_1, \ldots, a_s) = \sum_{r=1}^{a_0 - 1} \frac{t_r - r}{a_0}$$

which we state as follows.

2.1.6 ***Proposition.*** Let $R(a_0) = \{1, 2, \ldots, a_0 - 1\}$ and let $a_0, a_1, \ldots, a_s$ be relatively prime positive integers. Then

$$n(a_0, a_1, \ldots, a_s) = \left(\frac{1}{a_0} \sum_{r \in R(a)} t_r\right) - \frac{a_0 - 1}{2}. \tag{4}$$

Let d = g.c.d.$(a_1, \ldots, a_s)$ so that $a_i = d\, b_i$, for $i = 1, 2, \ldots, s$. Since g.c.d. $(a_0, a_1, \ldots, a_s) = 1$, we have g.c.d.$(a_0, d) = 1$. For any residue r (mod a_0) we define as in 2.1.3

$$u_r = t_r\,(a_0, b_1, \ldots, b_s).$$

Then there exist non-negative integers y_i such that

$$u_r = \sum_{i=1}^{s} b_i\, y_i, \tag{5}$$

so that $du_r = \sum_{i=1}^{s} d\ b_i\ y_i,$

(6) $du_r = \sum_{i=1}^{s} a_i\ y_i.$

Clearly the last sum is $\equiv dr \pmod{a_0}$ and it is the smallest integer $\equiv dr \pmod{a_0}$ which is representable by $a_0, a_1, \ldots, a_s$. If this is not the smallest, then the right hand side of (5) will not be the smallest integer representable by $a_0, b_1, \ldots, b_s$ and $\equiv r \pmod{a_0}$. Hence by the definition of $t_{dr} = t_{dr}(a_0, a_1, \ldots, a_s)$, we must have

$$t_{dr} = \sum_{i=1}^{s} a_i\ y_i\ .$$

Thus we get from (6)

(7) $t_{dr} = d\ u_r$

for any residue $r \pmod{a_0}$. Since d and r are relatively prime,

$$\{r : r = 0, 1, \ldots, a_0 - 1\} = \{d\ r : r = 0, 1, \ldots, a_0 - 1\ \}.$$

By 2.1.4 we have now from (7)

$$g(a_0, a_1, \ldots, a_s) + a_0 = d \cdot \{g(a_0, b_1, \ldots, b_s) + a_0\}$$

which yields

2.1.7 ***Lemma*** [3]. Let g.c.d. $(a_0, a_1, \ldots, a_s) = 1$. Let d = g.c.d.$(a_1, \ldots, a_s)$. Then

(8) $$g(a_0, a_1, \ldots, a_s) = d \cdot g\left(a_0\ ,\ \frac{a_1}{d}\ ,\ \ldots\ ,\ \frac{a_s}{d}\right) + a_0(d-1).$$

This is a very useful *reduction formula* which we we will be using very often throughout our work. For $s = 2$, this result was first proved [9] by S. M. Johnson.

We use (4) and (7) to deduce a similar reduction formula for the number of non-representable integers.

From (4) we have

$$n(a_0, a_1, \ldots, a_s) = \frac{1}{a_0} \sum_{r \in R(a)} t_{dr} - \frac{a_0 - 1}{2}$$

$$= \frac{1}{a_0} \sum_{r \in R(a)} d u_r - \frac{a_0 - 1}{2}$$

$$= \frac{1}{a_0} \sum_{r \in R(a)} d(u_r - r) + \frac{1}{a_0} \sum_{r \in R(a)} dr - \frac{a_0 - 1}{2}$$

$$= \frac{d}{a_0} \sum_{r \in R(a)} (u_r - r) + d\left(\frac{a_0 - 1}{2}\right) - \frac{a_0 - 1}{2}$$

$$= d\, n\left(a_0, \frac{a_1}{d}, \ldots, \frac{a_s}{d}\right) + \frac{1}{2}(d - 1)(a_0 - 1).$$

We give below a combinatorial proof of the above result.

2.1.8 ***Lemma.*** Let g.c.d. $(a_0, a_1, \ldots, a_s) = 1$. Let d = g.c.d.$(a_1, \ldots, a_s)$. Then

$$n(a_0, a_1, \ldots, a_s) = d\, n\left(a_0, \frac{a_1}{d}, \ldots, \frac{a_s}{d}\right) + n(a_0, d).$$

Proof. Define the sets

$$A = \{x : x \notin Sp(a_0, a_1, \ldots, a_s)\},$$

$$B = \{x : x \notin Sp(a_0, b_1, \ldots, b_s)\},$$

$$C = \{x : x \notin Sp(a_0, d)\},$$

$$D_i = \{ia_0 + d\,y : y \in B\}, \text{ for } i = 1, 2, \ldots, d-1,$$

$$d\,B = \{dx : x \in B\} \text{ and } D = D_1 \cup D_2 \cup \ldots \cup D_{d-1}.$$

We will show that

$$A = (dB) \cup C \cup D.$$

First we show that $(dB) \cup C \cup D \subseteq A$. If $x \in dB$, then $x = dy$ where $y \in B$. If $dy \notin A$, then

$$dy = a_0 x_0 + \sum_{i=1}^{s} a_i x_i.$$

Consequently d divides $a_0 x_0$. Since g.c.d.$(d, a_0) = 1$, d divides x_0. But then

$$y = a_0 \left(\frac{x_0}{d}\right) + \sum_{i=1}^{s} b_i x_i$$

which implies that $y \notin B$, a contradiction. This shows that $dB \subseteq A$. It is easy to see that $C \subseteq A$. We now show that $D_i \subseteq A$ for each i. Let $x \in D_i$. Then $x = ia_0 + dy$, $y \in B$. We have to show that $x \in A$. Suppose $x \notin A$. Then

$$x = ma_0 + d \sum_{i=1}^{s} b_i x_i,\ m, x_i \geq 0, \text{ being integers.}$$

We may write $m = pd + r$, $p \geq 0$, $0 \leq r \leq d-1$ so that

$$x = ra_0 + d\left(x_0 a_0 + \sum_{i=1}^{s} b_i x_i\right).$$

Since $x \in D_i$, we have

$$ia_0 + dy = ra_0 + d\left(x_0 a_0 + \sum_{i=1}^{s} b_i x_i\right),$$

so that

$$(i-r)a_0 + dy = d\left(x_0 a_0 + \sum_{i=1}^{s} b_i x_i\right).$$

Clearly $d \mid (i - r)$, say $i - r = qd$, q an integer.

Case 1. Let $q = 0$. Then $y \notin B$, a contradiction.

Case 2. Let $q \geq 1$. Then $r + qd = i$. But $i \leq d-1$. As $r \geq 0$, this is impossible.

Case 3. Let $q \leq -1$. Then $r = i - qd \geq i + d \geq d + 1$, a contradiction.

Therefore $x \in D_i$ implies that $x \in A$, for each $i=1, 2, \ldots, d-1$. Hence we have

(9) $$(dB) \cup C \cup D \subseteq A.$$

Next we show that $A \subseteq (dB) \cup C \cup D$.

Suppose that $x \notin (dB) \cup C \cup D$. Then $x \notin dB$ and $x \notin C$ and $x \notin D$. Since $x \notin C$, $x = ma_0 + nd$ where we can assume that $0 \leq m \leq d - 1$ and $n \geq 0$. Since $x \notin D$, we must have $m = 0$ or $n \notin B$.

If $m = 0$, then $x = nd$. If $n \in B$, then $x \in dB$, a contradiction. If $n \notin B$, then $n = x_0a_0 + x_1b_1 + x_2b_2 + \ldots + x_sb_s$ so that

$$nd = x_0da_0 + d(x_1b_1 + x_2b_2 + \ldots + x_sb_s).$$

That is, $x = nd = x_0da_0 + x_1a_1 + x_2a_2 + \ldots + x_sa_s$ which implies that $x \notin A$.

On the other hand if $n \notin B$, then n is representable by $a_0, b_1, \ldots, b_s$ in which case $x = ma_0 + nd$ is representable by $a_0, a_1, \ldots, a_s$. Therefore $x \notin A$. Hence

(10) $$A \subseteq (dB) \cup C \cup D.$$

From (9) and (10) it follows that $A = (dB) \cup C \cup D$.

By definition of the sets B, C, D, we easily see that

$$|dB| = |B| = |D_i| = n\left(a_0, \frac{a_1}{d}, \ldots, \frac{a_s}{d}\right)$$

for each $i = 1, 2, \ldots, d - 1$ and $|C| = n(a_0, d)$.

We now show that the sets dB, C, D_i are pairwise disjoint.

If $x \in D$ then $x \in D_i$ for some i. By definition of D_i we see that $x \in Sp(a_0, d)$ so that $x \notin C$. Therefore $C \cap D = \emptyset$.

If $x \in dB$ then $x = dy, y \in B$. That is, $x = 0 \bullet a_0 + dy, y \in B$ so that $x \notin D_i$ for any i. This implies that $x \notin D$ and therefore $D \cap dB = \emptyset$.

Finally if $x \in dB$ then $x = dy$, $y \in B$ which shows that $x \in Sp(a_0, d)$. That is, $x \notin C$. Therefore $C \cap dB = \emptyset$.

Since $|A| = n(a_0, a_1, \ldots, a_s)$, we get

$$n(a_0, a_1, \ldots, a_s) = d\, n\left(a_0, \frac{a_1}{d}, \ldots, \frac{a_s}{d}\right) + n(a_0, d).$$

The numbers t_r, $r = 1, 2, \ldots, a_0 - 1$, are related in a nice way. This is given by the following proposition.

2.1.9 ***Proposition***. Let $a_0, a_1, \ldots, a_s$ be relatively prime positive integers Suppose for each integer r, $0 \le r \le a_0 - 1$,

$$t_r = \sum_{i=1}^{s} a_i x_{ir}, \text{ for integers } x_{ir} \ge 0.$$

Then for every j with $x_{jr} \ge 1$, $t_r - a_j = t_m$ for some m.

Proof. Suppose, for simplicity, $x_{1r} \ge 1$. Let $t_r - a_1 \equiv k \pmod{a_0}$. Write $T_k = t_r - a_1$. Then, by definition, we have $t_k \le T_k$. If $t_k < T_k$, then $t_k < t_r - a_1$. But then $t_k + a_1 < t_r$. Since $t_k + a_1 \equiv k + a_1 \equiv t_r \equiv r \pmod{a_0}$, we see that the last inequality contradicts the fact that t_r is the smallest representable number congruent to r modulo a_0. Hence we must have $t_k = T_k$.

2.2 *Two known algorithms for computing* $g(a, b, c)$.

2.2.1 The problem of finding the numbers t_r occuring in 2.1.4 is in general not easy even by using computers. It seems that for three variables a, b, c, S. M. Johnson [9] was the first one to develop a method to find $g(a, b, c)$. Later, A. Brauer and J. E. Shockley [3] found a simpler method to find $g(a, b, c)$. The latter method is to find the set of points (x_r, y_r), with integer coordinates $x_r, y_r \geq 0$, so that the expression

$$b\,x_r + c\,y_r$$

assumes precisely the value $t_r \equiv r \pmod{a}$ at (x_r, y_r) for each $r = 1, 2, \ldots, a-1$. In the next chapter we will develop a similar method to get an upper bound for $g(S)$ for any set S of $s+1, s \geq 2$, relatively prime positive integers. Now we give an outline of the the method [3] for finding $g(a, b, c)$ where a, b, c are relatively prime positive integers.

By Lemma 2.1.7 it is no restriction to assume that the three integers are relatively prime in pairs. We will also assume that none of the three numbers is a non-negative linear combination of the other two. Thus the three numbers are independent. Define the function

(11) $$H(x, y) = b\,x + c\,y.$$

Consider the congruence

(12) $$bx - cy \equiv 0 \pmod{a}.$$

We first show that there exists a solution to (12) satisfying

$$0 < x_r \leq a,\ 0 < y_r \leq a.$$

Taking $y_r = 1$, $bx_r \equiv 0(mod\ a)$. Now g.c.d$(c, b) = 1$ and therefore there exists x_r such that $bx_r - c \equiv 0(mod\ a)$. If $x_r > a$ then $x_r = pa + q$, $0 \le q < a - 1$. If $q = 0$ then $c \equiv 0(mod\ a)$, a contradiction. Therefore $0 < q \le a - 1$. Hence there exists an x_r such that $0 < x_r \le a - 1$ and $y_r = 1$ satisfying $bx_r - cy_r \equiv 0 \pmod{a}$. Consider the set S_1 of all integer solutions (x_r, y_r) to (12) satisfying $0 < x_r \le a$, $0 < y_r \le a$.

We claim that in S_1 there is a solution $(x_r, 1)$ such that

(13) $\qquad bx_r - c > 0$

Suppose $bx_r - c = -sa$, $s \ge 0$. Then $c = bx_r + sa$, in which case $c \in Sp(a, b)$, a contradiction.

Thus there exist solutions (x_r, y_r) to (12) satisfying

$0 < x_r \le a$, $0 < y_r \le a$ and $bx_r - cy_r > 0$.

In the same way we can see that

(13) $\qquad 0 < cy - bx \equiv 0 \pmod{a}$, and $0 < x \le a$, $0 < y \le a$

has solutions (x, y), for example $x = 1$ leads to such a y.

Let (x_1, y_1) be the solution of (12) with smallest x, and (x_2, y_2) be the solution of (13) with smallest y. Define $x_3 = x_1 - x_2$, and $y_3 = y_2 - y_1$. We now show that $x_3 > 0$ and $y_3 > 0$.

From (12) and (13) by addition we get

$$0 < (x_1 - x_2)b + (y_2 - y_1)c \equiv 0 \pmod{a}$$

Define $x_3 = x_1 - x_2$, and $y_3 = y_2 - y_1$. If $x_1 - x_2 < 0$, then we get a contradiction from (13) to the choice of y_2 and if $y_2 - y_1 < 0$, we get a contradiction from (12) to the choice of x_1. Moreover $x_1 - x_2 \ne 0$, and $y_2 - y_1 \ne 0$. Otherwise if $x_1 - x_2 = 0$, then $0 < (y_2 - y_1)c \equiv 0 \pmod{a}$. As $y_1, y_2 \le a$, and g.c.d.$(a, c) = 1$, the congruence

$(y_2 - y_1)\, c \equiv 0 \pmod{a}$ is impossible. Similarly one can see that $y_2 - y_1 \neq 0$. Therefore (x_3, y_3) has both coordinates strictly positive.

Define the rectangle R by

$$R = \{(x,y) : 0 \leq x \leq x_1 \text{ and } 0 \leq y \leq y_2 \}.$$

For each non-negative integral point (x, y) not in R, consider $H(x, y)$. If $H(x, y) \equiv r \pmod{a}$, then we are interested in finding t_r. If $x \geq x_1$, we choose

$$u = x - x_1,\ v = y + y_1,$$

so that by using (12),

$$H(u, v) = H(x, y) - bx_1 + cy_1 \equiv H(x, y) \pmod{a}$$

and $$H(u, v) < H(x, y).$$

If $y \geq y_2$, we set

$$u = x + x_2,\ v = y - y_2.$$

Using (13) we see that

$$H(u,v) \equiv H(x,y) \pmod{a}$$

and $$H(u,v) < H(x,y).$$

We continue this procedure until we reach a point in the region R. We can show that we will obtain a point in R. Otherwise if there is an infinite sequence (x_1, y_1), (x_1, y_1), ..., all lying outside R then $H(x, y) < H(x_1, y_1) < \ldots$ shows that $\{h(x_r, y_r)\}$ is a decreasing sequence of positive integers congruent to $H(x, y) (mod\ a)$ which is not possible. For example if $H(x, y) = pa + r$, $0 \leq r \leq a$, then the procedure brings (x, y) to a point in R in almost p steps of successive translations.This shows that $H(x, y)$ assumes a value $\equiv r \pmod{a}$ in the rectangle R for each $r \pmod{a}$.

Now we can also show that (x_3, y_3) is the point with least positive coordinates in R such that $H(x, y) \equiv 0 \pmod{a}$.

Suppose (p, q) is any point in R such that $H(p, q) \equiv 0 \pmod{a}$. Then $pb + qc \equiv 0$, and $x_2b - y_2c \equiv 0 \pmod{a}$. Therefore $(x_2 + p)b - (y_2 - q) \equiv 0 \pmod{a}$.

If $p < x_1 - x_2$, then $x_2 + p < x_1$, and the last congruence contradicts the choice of x_1. Therefore $p \geq x_1 - x_2 = x_3$. Similarly, we get $q \geq y_2 - y_1 = y_3$. That is (x_3, y_3) is the point with least positive coordinates in R such that $H(x, y) \equiv 0 \pmod{a}$.

Now consider the region U given by

$U = \{(x,y) : 0 \leq x < x_1 \text{ and } 0 \leq y < y_3\} \cup \{(x, y) : 0 \leq x < x_3 \text{ and } 0 \leq y < y_2\}$

If (ξ, η) is a point of R not in U, then

$$H(\xi, \eta) \equiv H(\xi - x_3, \eta - y_3) \pmod{a}$$

and $$H(\xi, \eta) > H(\xi - x_3, \eta - y_3).$$

We now show that the function H assumes all residues mod a in the smaller region U. That is if $t_r = b\alpha_r + c\beta_r = H(\alpha_r, \beta_r)$, then (α_r, β_r) is not in R we can apply the translation procedure and bring it to a point (p, q) in R such that

$$H(p, q) \equiv H(\alpha, \beta) \text{ and } H(p, q) < H(\alpha_r, \beta_r).$$

But $H(\alpha_r, \beta_r)$ being the least representable integer $\equiv r \pmod{a}$, this is not possible. Thus $(\alpha_r, \beta_r) \in R$. But then $(\alpha_r, \beta_r) \in U$, for otherwise

$$H(\alpha_r - x_3, \beta_r - y_3) < t_r.$$

Therefore if $t_r = H(\alpha_r, \beta_r)$, then $(\alpha_r, \beta_r) \in U$. Moreover if there exists another point (α_r^*, β_r^*) in U such that $H(\alpha_r, \beta_r) \equiv H(\alpha_r^*, \beta_r^*)$ then

$$0 < \left|\alpha_r - \alpha_r^*\right| < x_1, \; 0 < \left|\beta_r - \beta_r^*\right| < y_3.$$

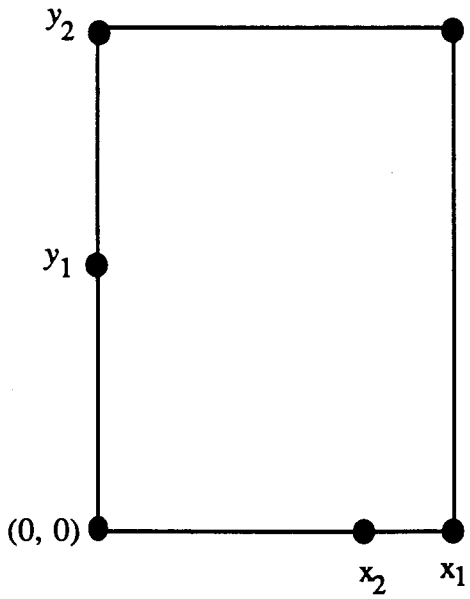
Therefore $(\alpha_r - \alpha_r^*)b + (\beta_r - \beta_r^*)c \equiv 0 \pmod{a}$. If $\alpha_r - \alpha_r^*$ and $\beta_r - \beta_r^*$ are both positive then the same congruence contradicts the fact (x_3, y_3) in U has the least positive coordinates such that $bx_3 + cy_3 \equiv 0 \pmod{a}$. If $\alpha_r - \alpha_r^*$ and $\beta_r - \beta_r^*$ are both negative then we get a similar contradiction again. If these have opposite signs then we

get a contradiction to (12) or (13). Therefore $H(x, y)$ assumes least positive numbers in each residue class mod a in U.

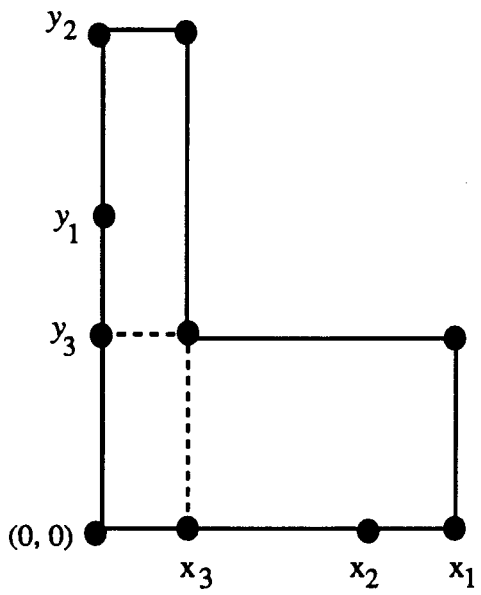
Therefore by Lemma 2.1.4, we get

$$g(a, b, c) = max\{x_1 b + y_3 c, x_3 b + y_2 c\} - a.$$

We have shown below the region U.



The rectangle **R**



The region **U**

Figure 1

Example. The following example used by S. M. Johnson [8] is often referred to in the literature. Let $a = 137$, $b = 251$, $c = 256$. The solution (x_1, y_1) of congruence (12) $0 < b\,x - c\,y \equiv 0 \pmod{a}$, is (13, 9). The solution (x_2, y_2) of (13) is (5, 14). Then $(x_3, y_3) = (8, 5)$. Therefore we have

$$g(137, 251, 256) = max\{12\,(251) + 4(256), 7(251) + 13(256)\} - 137$$
$$= 4948.$$

2.2.2 ***Another algorithm to find g(a, b, c).*** Another well known algorithm for the computation of $g(a, b, c)$ is given by E. Selmer and Ö. Beyer [20] by considering the convergents of a finite continued fraction expansion of $\frac{a}{s_0}$ where the integer s_0 is determined by

(14) $$bs_0 \equiv c \pmod{a},\ 0 \le s_0 < a.$$

This algorithm has been modified and a simpler one is given by Ö.J.Rödseth [18]. The outline of the latter method is as follows.

If g.c.d.$(a, b) = d$, then by the reduction formula in 2.1.7 we have

$$g(a, b, c) = dg\left(\frac{a}{d}, \frac{b}{d}, c\right) + (d-1)c$$

so that we may assume a, b to be relatively prime. If c is representable by a, b then $g(a, b, c) = g(a, b) = a\,b - a - b$. So we can also assume that $s_0 \neq 0$. We use the euclidean algorithm to obtain

(15)
$$\begin{array}{llll} a = s_{-1} & = q_1 s_0 - s_1, & 0 \le s_1 & < s_0; \\ s_0 & = q_2 s_1 - s_2, & 0 \le s_2 & < s_1; \\ s_1 & = q_3 s_2 - s_3, & 0 \le s_3 & < s_2; \\ \cdots & \cdots & \cdots & \cdots \end{array}$$

$$s_{m-2} = q_m s_{m-1} - s_m, \quad 0 \le s_m < s_{m-1};$$

$$s_{m-1} = q_{m+1} s_m, \quad 0 = s_{m+1} < s_m.$$

Define integers P_i by $P_{-1} = 0, P_0 = 1$, and

(16) $$P_{i+1} = q_{i+1} P_i - P_{i-1}, \quad i = 0, 1, \ldots, m.$$

We write $\frac{a}{0} = \frac{s_{-1}}{P_{-1}} = \infty$. Since $q_i \ge 2$ for all i, it follows by induction from (16) that $P_{i+1} > P_i$. Hence

$$0 = \frac{s_{m+1}}{P_{m+1}} < \frac{s_m}{P_m} \cdots < \frac{s_0}{P_0} < \frac{s_{-1}}{P_{-1}} = \infty$$

and there is a unique integer v, $-1 \le v \le m$, satisfying

(17) $$\frac{s_{v+1}}{P_{v+1}} \le \frac{c}{b} < \frac{s_v}{P_v}.$$

The exact value of $g(a, b, c)$ is now given by the following theorem.

2.2.3 ***Theorem*** [16]. Let a, b, c be positive integers where a, b are relatively prime and c is not representable by a, b. Then

(18) $g(a, b, c) = -a + b(s_v - 1) + c(P_{v+1} - 1) - min\ \{bs_{v+1}, cP\}$ where v is the unique integer determined by (17).

2.2.4 ***Remark***. For the function $f(a, b, c)$ the above result looks even simpler.

$$f(a, b, c) = bs_v + cP_{v+1} - min\ \{bs_{v+1}, cP\}.$$

It is also interesting that this algorithm gives the number $n(a, b, c)$ of non-representable integers. The following is proved in [16].

2.2.5 ***Theorem***. Following the above notations,

$$n(a, b, c) = \frac{1}{2}\{(1 - a + b(s_v - s_{v+1} - 1) + c(P_{v+1} - 1)\}$$
$$+ s_{v+1}(P_{v+1} - P_v)\frac{1}{2a}(bs_v - cP_v).$$

2.2.6 ***Example***. It is easy to apply the method in numerical cases. The best known example used by several authors, for example first by S.M.Johnson [8], is as follows. Let

$$a = 137, b = 251, c = 256.$$

The congruence (14) gives $s_0 = 108$, and applying the Euclidean algorithm (15) we get

$$137 = 2.\ 108 - 79, \quad P_1 = 2,$$
$$108 = 2.\ 79 - 50, \quad P_2 = 3$$
$$79 = 2.\ 50 - 21, \quad P_3 = 4$$
$$50 = 3.\ 21 - 13, \quad P_4 = 9$$
$$21 = 2.\ 13 - 5, \quad P_5 = 14,$$

where the numbers P_i are obtained by using (16).

Now we find v. We note that

$$\frac{s_5}{P_5} = \frac{5}{14} < \frac{256}{251} < \frac{13}{9} = \frac{s_4}{P_4},$$

and therefore by 2. 2. 3

$$g(137, 251, 256) = -137 + 251\cdot 12 + 256\cdot 13 - min\{251\cdot 5, 256\cdot 9\}$$

$$= 4948.$$

Using 2.2.5 we find that the number

$$n(a, b, c) = \frac{1}{2}\left\{1 - 137 + 251\cdot 7 + 256\cdot 13 + 5\cdot 5\cdot\frac{1}{137}(251\cdot 13 - 256\cdot 9)\right\}$$

$$= 2562.$$

In some cases it is possible to reduce the number of times we apply the Euclidean algorithm by re-naming the given numbers. For instance, in our present example let $a' = 251$, $b' = 137$, $c' = 256$. We see that $s_0 = 55$, so that

$$251 = 5\cdot 55 - 24, \qquad P_1 = 5,$$

$$55 = 3\cdot 24 - 17, \qquad P_2 = 14,$$

and therefore

$$\frac{17}{14} < \frac{256}{137} < \frac{24}{5}.$$

We now obtain

$$g(137, 251, 256)$$

$$= -251 + 137\cdot 23 + 256\cdot 13 - min\{137\cdot 17, 256\cdot 5\} = 4948,$$

and

$$n(137, 251, 256)$$

$$= \frac{1}{2}\left\{1 - 251 + 137\cdot 6 + 256\cdot 13 + 17\cdot 9\cdot\frac{1}{251}(137\cdot 24 - 256\cdot 5)\right\}$$

$$= 2562.$$

2.3 ***The exact solution for*** $g(a, b, c)$ ***when*** $b + c \equiv 0 \pmod{a}$. Given relatively prime integers $1 < a < b < c$, the reduction formula (8) in Lemma 2.1.6 implies that we may assume that each pair of the integers a, b, c is relatively prime. We may also assume that the set $\{a, b, c\}$ is independent. A. Brauer and J..E. Shockley [3] determined the value of $g(a, b, c)$ as an explicit function of a, b, c when $b + c \equiv 0 \pmod{a}$. We determine the exact value of $g(a, b, c)$ in the case of $b + c \equiv 0 \pmod{a}$, by using a completely different method and we get a different formula. We need also g.c.d.(a, b) = g.c.d.$(a, c) = 1$.

2.3.1 ***Lemma.*** Let a, b, c, $1 < a < b < c$, be relatively prime integers with g.c.d. (a, b) = g.c.d.$(a, c) = 1$ and $b + c \equiv 0 \pmod{a}$. Let

$$m = \left[\frac{a}{2}\right],\ A = \{b, 2b, \ldots, mb\},\ B = \{c, 2c, \ldots, mc - \delta c\}$$

where

$$\delta = \begin{cases} 0, & \text{if } a \text{ is odd} \\ 1, & \text{if } a \text{ is even} \end{cases} \tag{19}$$

Then $A \cup B$ contains a complete non-zero residue system mod (a).

Proof. Since g.c.d. (a, b) = g.c.d. $(a, c) = 1$, the sets A and B each have distinct non-zero residues modulo a. Let $1 \le i \le m$ and $1 \le j \le m - \delta$.

Suppose $ib \in A$ and $jc \in B$ satisfy $ib \equiv jc \pmod{a}$, then

$$ib \equiv -jb \pmod{a}, \text{ since } b + c \equiv 0 \pmod{a}$$

That is, $$(i + j)b \equiv 0 \pmod{a}$$

Since g.c.d.$(a, b) = 1$ and $i + j \neq 0$, we must have $i + j = ta$ for some integer $t \ge 1$. But

$$i + j \le m + (m - \delta) \le a - 1.$$

Therefore we can not have

$$ib \equiv jc \pmod{a}$$

for any $1 \le i \le m$ and $1 \le j \le m - \delta$. Clearly $0 \notin A$ and $0 \notin B$. Thus $A \cup B$ contains a complete non-zero residue system mod (a).

2.3.2 ***Lemma***. Let a, b, c, m, δ be as in Lemma 2. 3. 1. Then for any integer x with $1 \le x \le m$,

$$mb + xb \equiv mc - xc + (1 - \delta)c \ (mod\ a).$$

Proof. Since $xb \equiv -xc(mod\ a)$, we only need to show that

$$mb \equiv mc + (1 - \delta)c \ (mod\ a)$$

If a is even, then $a = 2m$ and $mb \equiv -mc \equiv mc \pmod{a}$.

If a is odd, then $a = 2m + 1$ and $mb \equiv -mc \equiv (m+1)c \pmod{a}$.

2.3.4 ***Theorem***.. Let a, b, c, $1 < a < b < c$ be relatively prime integers with g.c.d. (a, b) = g.c.d.$(a, c) = 1$ and $b + c \equiv 0 \pmod{a}$. Let m and δ be as in Lemma 2.3.1. Then

$$g(a, b, c) = max\ \{mb + \alpha b, mc - \alpha c - \delta c\} - a.$$

where

$$\alpha = \left[\frac{(c - b)m + c(1 - \delta)}{c + b}\right].$$

Proof. Following the notation in 2.1.3, for $r = 1, 2, \ldots, a - 1$, let t_r denote the least positive integer $\equiv r \pmod{a}$ and representable by b and c. By Lemma 2.4.1, $A \cup B$ is

a complete non-zero residue system mod a. Our aim is to find the minimum residues t_r, for $r = 1, 2, \ldots, a-1$. Consider the following list of multiples of b and c.

COLUMN 1	COLUMN 2
b	c
$2\ b$	$2\ c$
.	.
.	.
.	.
$m\ b$	$m\ c$
.	.
.	.
.	.

We observe the following.

1. The numbers in each column are increasing.

2. In each non-zero residue class modulo a, the smallest number representable by b and c has the form xb or yc, where $1 \leq x \leq a-1$, $1 \leq y \leq a-1$. (For if $x > y$ then $xb + yc \equiv (x-y)b \pmod{a}$, and if $x < y$, then $xb + yc \equiv (y-x)c \pmod{a}$.) Therefore it is enough to consider the first a rows in order to find the minimum residue for each $r = 1, 2, \ldots, a-1$.

3. The first m rows contain a complete non-zero residue system modulo a by Lemma 2.3.1.

4. If a is even, the numbers below mb are respectively congruent mod a to the numbers above mc, by Lemma 2.3.2.

5. If a is odd, the numbers below mb are respectively congruent mod a to the numbers above $(m + 1)c$, by Lemma 2.3.2.

It is easy to see that each of the numbers $b, 2b, \ldots, mb$ in column 1 is a minimum residue. That is, for $1 \le i \le m$,

$$t_{ib} = ib.$$

We have two cases now.

Case (*i*) Suppose $mb + b > mc - \delta c$.

Since $mb + b \equiv mc - \delta c \pmod{a}$,

$$t_{mb+b} \le mc - \delta c.$$

But $mc - \delta c$ is neither congruent to any number above it in the second column nor congruent to any number above $mb+b$ in the first column. Hence $t_{mb+b} = mc - \delta c$. For $x = 1, 2, \ldots, m - \delta$, we have

$$mb + b + (x - 1)b > mc - \delta c - (x - 1)c.$$

Moreover, the two numbers on either side of the above inequality are congruent by (22). Therefore each of the numbers $c, 2c, \ldots, (m - \delta)c$ in the second column is a minimum residue. In other words the set $A \cup B$ is a set of minimum residues so that

$$\{ib : i = 1, 2, \ldots, m\} \cup \{jc : j = 1, 2, \ldots, m - \delta\}$$

forms a complete system of minimum non-zero residues mod a. Thus we obtain $g(a, b, c) = max\{m b, (m - \delta)c\} - a$. The theorem is proved in this case if we show $\alpha = 0$. In fact,

$$mb + b > mc - \delta c$$

yields $c + b > m(c - b) + c(1 - \delta)$ in which case

$$\alpha = \left[\frac{(c-b)m + c(1-\delta)}{c+b}\right] = 0.$$

Case (ii). Suppose $mb + b \leq mc - c + (1-\delta)c$. Then we can find a positive integer α such that α is the largest positive integer with

$$mb + \alpha b \leq mc - \alpha c + (1-\delta)c.$$

That is the set B does not form a system of minimum residues. Since by (22)

$$mb + xb \equiv mc - xc + (1-\delta)c$$

and $$mb + xb \leq mc - x c + (1-\delta)c$$

for any integer $1 \leq x \leq \alpha$, we certainly have

$$t_{mb+xb} \leq mb + xb.$$

Let $mb + xb \equiv r_x \pmod{a}$. Then $r_x \pmod{a}$ appears as $mb + xb$ in the first column for the first time and in the second column it appears as $m c - xc + (1-\delta)c$ for the first time. Since each column is increasing,

$$t_{r_x} = mb + xb.$$

If $x > \alpha$, then

$$mb + xb > mc - xc + (1-\delta)c$$

and therefore the numbers

$$c, 2c, \ldots, mc - (\alpha + 1)c + (1-\delta)c$$

are minimum residues mod a. Hence

$$\{b, 2b, \ldots, mb + \alpha b\} \cup \{c, 2c, \ldots, mc - \alpha c + (1-\delta)c\}$$

forms a complete system of minimum non-zero residues mod a. This gives

$g(a, b, c) = max\{mb + \alpha b, mc - \alpha c - \delta c\} - a$

where α is the largest non-negative integer such that

(23) $$mb + \alpha b \le mc - \alpha c + (1 - \delta)c$$

which yields

$$\alpha = \left[\frac{(c - b)m + c(1 - \delta)}{c + b}\right].$$

2.3.4 ***Example***. We shall find $g(9, 16, 20)$.

Here $m = 4$, $\delta = 0$, $\alpha = \left[\frac{(20-16)4 + 20}{36}\right] = 1$. By Theorem 2.3.4, $g(9, 16, 20) = max\{5b, 3c\} - 9 = 80 - 9 = 71$.

Directly, by finding the number t_r, $r = 1, 2, \ldots, 8$, in each residue class $\{r, r+9, r + 18, \ldots\}$, we get the same result.

2.4 ***Extending*** $\{a, b\}$ ***to an independent set*** $\{a, b, c\}$. Most of the difficulties of finding the exact solution of the Frobenius problem for $s \ge 2$ appear to be contained in the case $s = 2$. So we study the effect of extending any given set $\{a, b\}$ of relatively prime integers $1 < a < b$ to $\{a, b, c\}$ where c is non-representable by a, b. Then we have the following.

2.4.1 ***Theorem***. Let $\{a, b, c\}$, $1 < a < b < c$, be relatively prime integers. Let $(a, b) = 1$. Let c be non-representable by a, b. Then

(i) $g(a, b, c) \le g(a, b) - a$,

(ii) if $c = g(a, b)$, then $g(a, b, c) = g(a, b) - a$,

and (iii) if $g(a, b, c) = g(a, b) - a$, then b divides $(a + c)$.

Proof. According to Lemma 1.5.2, exactly one of the numbers

$$g(a, b) - x \text{ and } x$$

is representable by a, b for all $0 \leq x \leq g(a, b)$. For $1 \leq x \leq a - 1$, it is trivial that x is non-representable and therefore $g(a, b) - x$ is representable by a, b. In particular, $g(a, b) - x$ is representable by a, b, c for every x with $1 \leq x \leq a - 1$. Since c is non-representable by a, b, it is necessary that $c \leq g(a, b)$. Hence $g(a, b) - c$ is non-negative and since c is non-representable, $g(a, b) - c$ is representable by a, b. It now follows that $g(a, b)$ is representable by a, b, c. That is,

$$g(a, b) - x, \quad 0 \leq x \leq a - 1$$

is representable by a, b, c. However, if an integer $n > g(a, b)$, it is representable by a, b (and c). This shows that if $n \geq g(a, b) - (a - 1)$, then $n \in Sp(a, b, c)$

We therefore conclude

$$g(a, b, c) \leq g(a, b) - a.$$

This proves (i). We now show (ii).

Suppose $c = g(a, b)$. Since a is in $Sp(a, b)$, $g(a, b) - a \notin Sp(a, b)$. Further since $g(a, b) - a < c$,

$$g(a, b) - a \notin Sp(a, b, c).$$

However, any integer $n \geq g(a, b) - (a - 1)$ is in $Sp(a, b, c)$, by the above theorem. It now follows that

$$g(a, b, c) = g(a, b) - a$$

To show (iii), let c be non-representable by a, b. Let $c < g(a, b)$ and

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

Since $1, 2, \ldots, a - 1$ are non-representable by a, b we see that $g(a, b) - 1$, $g(a, b) - 2, \ldots, g(a, b) - (a - 1)$ are representable by a, b. Therefore $c \leq g(a, b) - a$. By our

assumption $g(a, b, c) = g(a, b) - a$ and hence $c < g(a, b) - a$. We assert that $a + c$ is representable by a, b. For, otherwise if

$$g(a, b) - a - c \in Sp(a, b)$$

then

$$g(a, b) - a \in Sp(a, b, c).$$

This contradicts the fact that $g(a, b, c) = g(a, b) - a$.

Now let

(26) $a + c = a x + b y, x, y$ being non-negative integers.

We must have $x = 0$. For, if $x \geq 1$, then $c = a(x - 1) + b y$, and consequently $c \in Sp(a, b)$, a contradiction. From (26) it follows now that

$b \mid (a + c)$.

2.4.2 ***Remark.*** Suppose now that $g(a, b, c) = g(a, b) - a$ and $a + c = k b$.

Case 1. $a \geq 2k + 1$.

Now

$$\begin{aligned} g(a, b) - a &= a b - 2 a - b \\ &= [a - (2 k + 1)]b + 2 c. \\ &\geq 2 c \end{aligned}$$

Case 2. $a < 2 k + 1$.

Now,

$$\left(\frac{a - 1}{2}\right) b < k b = a + c.$$

$$a b - b < 2 a + 2 c$$

That is, $g(a, b) - a = a b - 2 a - b < 2 c$.

2.4.3 ***Remark***. In general if S is an independent set of relatively prime positive integers and if S is extended again to an independent set $S' = S \cup \{t\}$, say, then $g(S') \leq g(S)$. It is possible to have equality as in the above example. Indeed, if S is any non-empty set of relatively prime integers and S' contains S, then $g(S') \leq g(S)$.

2.4.4 ***Remark***. If $c \in Sp(a, b)$, then we have $g(a, b) = g(a, b, c)$. On the other hand, by (i) of 2.4.1 if we extend a given set $\{a, b\}$ of relatively prime positive integers to an independent set $\{a, b, c\}$ then

$$g(a, b, c) < g(a, b).$$

However this is not true for more than three variables. Suppose we have the set $\{5, 7, 9\}$. The numbers form an arithmetic sequence and therefore we use the formula in [1], namely

$$g(a, a+d, \ldots, a+kd) = \left[\frac{a-2}{k}\right] a + (a-1)\, d,$$

and obtain $g(5, 7, 9) = 13$. Now take one more element 11 and consider the set $\{5, 7, 9, 11\}$. We note that 11 is non-representable by 5, 7, 9. We see that

$$g(5, 7, 9, 11) = 13$$

which is exactly $g(5, 7, 9)$.

Using the ' *reduction formula* ' (8), Lemma 2.1.7, we can deduce easily the upper bound obtained by A.Brauer [2].

2.4.5 ***Theorem***. Let $a_0, a_1, \ldots, a_s$ be positive integers such that

$$d_i = \text{g.c.d.}(a_0, a_1, \ldots, a_i),\ i = 1, 2, \ldots, s-1.$$

Let $d_0 = a_0$, and $d_s = 1$. Then

$$g(a_0, a_1, \ldots, a_s) \leq \sum_{i=1}^{s} a_i \left(\frac{d_{i-1}}{d_i} - 1 \right) - a_0$$

Proof. We prove this by induction on s. For s = 1, by 1.5.1 we know that

$$\begin{aligned} g(a_0, a_1) &= a_1 (a_0 - 1) - a_0 \\ &= a_1 \left(\frac{d_0}{d_1} - 1 \right) - a_0 \end{aligned}$$

since $d_1 = 1$ and $d_0 = a_0$. Therefore the theorem is true for $s = 1$. Now let $s \geq 2$. By using the result (8) of Lemma 2.1.7, we have

$$g(a_0, a_1, \ldots, a_s)$$

$$= d_{s-1}\, g\left(\frac{a_0}{d_{s-1}}, \frac{a_1}{d_{s-1}}, \ldots, \frac{a_{s-1}}{d_{s-1}}, a_s \right) + (d_{s-1} - 1)\, a_s$$

$$\leq d_{s-1}\, g\left(\frac{a_0}{d_{s-1}}, \frac{a_1}{d_{s-1}}, \ldots, \frac{a_{s-1}}{d_{s-1}} \right) + (d_{s-1} - 1)\, a_s$$

using the remark 2.4.4. We can apply our induction hypothesis to the s elements $\frac{a_0}{d_{s-1}}, \frac{a_1}{d_{s-1}}, \ldots, \frac{a_{s-1}}{d_{s-1}}$ which are relatively prime. This yields

$$g(a_0, a_1, \ldots, a_s)$$

$$\leq d_{s-1} \left\{ \sum_{i=1}^{s-1} \frac{a_i}{d_{s-1}} \left(\frac{d_{i-1}}{d_i} - 1 \right) - \frac{a_0}{d_{s-1}} \right\} + (d_{s-1} - 1)\, a_s$$

$$= \sum_{i=1}^{s-1} a_i \left(\frac{d_{i-1}}{d_i} - 1 \right) - a_0 + (d_{s-1} - 1)\, a_s$$

$$= \sum_{i=1}^{s-1} a_i \left(\frac{d_{i-1}}{d_i} - 1 \right) - a_0 + \left(\frac{d_{s-1}}{d_s} - 1 \right) a_s$$

Hence we have

$$g(a_0, a_1, \ldots, a_s) \leq \sum_{i=1}^{s} a_i \left(\frac{d_{i-1}}{d_i} - 1 \right) - a_0.$$

CHAPTER 3

3.1 *Upper bounds obtained by using additive number theory.*

3.1.1 ***Definition.*** Given a positive integer a and non-empty subsets A, B of non-negative integers, the set

$$\{x + y : x \in A,\ y \in B\}.$$

of all distinct integers of the form $x + y$ is denoted by $A + B$ or simply by $A + B$. It is convenient to write $A + A$ as $2A$ and more generally the m–fold sum by mA.

By using a strong form of a theorem by M.Kneser, (Theorem 16 ′, [8]), it was shown by P. Erdös and R. L. Graham

3.1.2 ***Theorem*** Let $S = \{a_1, a_2, \ldots, a_n\}$, $1 < a_1 < a_2 < \ldots < a_n$, be a set of relatively prime integers. Let $m = \left[\frac{a_n}{n}\right]$. Then

(1) $$g(S) \leq 2m a_{n-1} - a_n.$$

3.1.3 ***Remark.*** Let $S = \{a_1, a_2, \ldots a_{n-1}, a_n\}$ and let $S(b)$ denote the set of residues mod b of elements in S. Consider the set

$$S(a_n) = \{a_1, a_2, \ldots, a_n - 1, 0\}.$$

It was shown by Erdös and Graham that the set

$$2m\, S(a_n) = S(a_n) + S(a_n) + S(a_n) + \ldots + S(a_n),$$

(added 2 m times mod a_n) contains a complete system of residues (mod a_n).

So we may write

$$T_r = \sum_{i=1}^{n} a_i x_i$$

where the coefficients x_i are non-negative integers satisfying

$$\sum_{i=1}^{n} x_i \leq 2m.$$

It must be noted that the number T_r need not be the smallest number representable by $a_1, a_2, \ldots, a_n$ for each residue r (mod a_n).

E. Selmer [19] points out that instead of a_n we can take the least number a_1 in the given set S and assume that the set S is independent so that $S(a_1)$ consists of distinct incongruent residues mod a_1. Then (1) becomes

$$g(S) \leq 2\left[\frac{a_1}{n}\right] a_n - a_1. \tag{2}$$

This is an improvement of (1). If T_r' denotes the smallest positive integer $\equiv r$ (mod a_1) and representable by $a_1, a_2, \ldots, a_n$, in the form

$$T_r' = \sum_{i=2}^{n} a_i\, y_{ir}$$

then it was mentioned in [19] that

$$y_{ir} \leq 2\left[\frac{a_1}{n}\right]$$

for each $r = 1, 2, \ldots, a_1 - 1$. This is *not* true for the smallest representable number t_r. For example consider $S = \{5, 11, 19\}$. It can be easily calculated that

$$t_1 = 11,\ t_2 = 22,\ t_3 = 33,\ t_4 = 19.$$

Now $t_3 = 3.11$ so that the sum of the coefficients is 3. But $2\left[\frac{a_1}{n}\right] = 2$.

If S contains an element a_i which is relatively prime to every $a_j, j \neq i$, then we can use the following theorem [8] in additive number theory and deduce a sharp upper bound for $g(S)$ as shown below.

We remark that if S is independent and $t \in S$, then the elements of $S - \{t\}$ must be pairwise incongruent modulo t.

3.1.4 ***Cauchy – Davenport – Chowla Theorem.*** Let t be a given positive integer, $A = \{a_1, a_2, \ldots, a_r\}$, a subset of r incongruent residues mod t, and $B = \{0, b_1, b_2, \ldots, b_{s-1}\}$, a subset of s incongruent residues mod t. Let t be relatively prime to each $b_i \in B$. Then $A + B$ contains at least $min(r + s - 1, t)$ incongruent residues mod t.

3.1.5 ***Theorem.*** Let $S = \{a_0, a_1, \ldots, a_s\}$ be independent. If S has an element, say t, such that t is relatively prime to every member $a_i \neq t$, then

$$g(a_0, a_1, \ldots, a_s) \leq m \cdot max\{a_i : a_i \neq t\} - t,$$

where $m = \left[\frac{t-1}{s}\right] + 1$.

Proof. If $m = \left[\frac{t-1}{s}\right] + 1$, then $ms \geq t$. Let addition of sets be taken modulo t. By the above theorem, taking $A = S, B = S - \{t\}$, we get \x\le\ri(2S(mod t)) ≥ \x\le\ri((A + B)(mod t)) ≥ ... $min\{t, s+1 + s-1 = 2s\}$. By successive application of the theorem it is easy to see that

$$| mS | \geq min\{t, ms\} = t.$$

Hence mS contains a complete system of residues mod t. Let t_r denote the smallest non-negative integer $\equiv r$ (mod t) and representable by $a_0, a_1, \ldots, a_s$. By Lemma 2.1.4 we have $g(S) = max\{t_r : r = 1, 2, \ldots, t-1\} - t$ which implies that

$$g(S) \leq a_0 x_0 + a_1 x_1 + \ldots + a_s x_s - t,$$

where the sum of the coefficients x_i is at most m.

Therefore we may write

$$g(S) \leq \left(\sum_{i=0}^{s} x_i \right) max\{a_i : a_i \neq t\} - t$$

$$g(S) \leq m.\ max\{a_i : a_i \neq t\} - t.$$

<u>*Sharpness for s = 1*</u>. If $s = 1$, then we may choose $t = a_0$ so that $m = a_0 - 1$ and therefore $g(a_0, a_1) \leq m \cdot a_1 - a_0 = (a_0 - 1)a_1 - a_0$, which is exact.

A variant of Theorem 3.1.4 is also useful to deduce an upper bound for the case where $S = \{a_0, a_1, \ldots, a_s\}$contains some element, say t, such that 0 has no

representation of the form $a_i + a_j \equiv 0 \pmod{t}$, except when $a_i \equiv a_j \equiv 0 \pmod{t}$. We need the following result.

3.1.6 ***Theorem*** (Kemperman and Scherk [8, p.50]). Let t be a given integer. Let $A = \{0, a_1, \ldots, a_{r-1}\}$ be a given set of r incongruent residues mod t and $B = \{0, b_1, \ldots, b_{s-1}\}$ be a given set of s incongruent residues mod t. Let $a_i + a_j \equiv 0 \pmod{t}$ if and only if $a_i \equiv 0 \pmod{t}$ and $a_j \equiv 0 \pmod{t}$. Then $A + B$ contains at least $min\{t, r + s - 1\}$ distinct residues modulo t.

Using this theorem, we can alter the hypothesis of Theorem 3.1.4 accordingly. For certain sets S, this results in an improvement of known upper bounds. We state formally

3.1.7 ***Theorem***. Let $S = \{a_0, a_1, \ldots, a_s\}$ be an independent set of positive integers ≥ 2. Suppose S has an element t such that $a_i + a_j \equiv 0 \pmod{t}$ if and only if $a_i \equiv 0 \pmod{t}$ and $a_j \equiv 0 \pmod{t}$. Then

$$g(a_0, a_1, \ldots, a_s) \leq m \cdot max\{a_i : a_i \neq t\} - t$$

where $m = \left[\frac{t-1}{s}\right] + 1$.

Proof. The independence of S ensures that the set $S(t)$ of residues mod t will be a set of incongruent residues mod t. The rest of the proof is exactly similar to that of Theorem 3.1.4.

As mentioned before, the above bound is sharp for $s = 1$. We now compare the bounds obtained by using the Theorems 3.1.5 and 3.1.7 with some known upper bounds.

3.1.8 ***Example***. S = {137, 251, 256 }. Since 137 is a prime and the numbers 251 and 256 are incongruent mod 137, we can apply theorem 3.1.5 (or 3.1.7). Here $t =$ 137, $s = 2$, $max\ a_i = 256$ and $m = 69$ so that

(3) $$\boxed{g(137, 251, 256) \leq 69 \cdot 256 - 137 = 17527}.$$

We compare this value with the following known bounds.

J.J. Sylvester [21]	$(a_0 - 1)(a_1 - 1) - 1$	33999
Y.Vitek [23]	$\left[\frac{a_s^2}{s}\right] - 1$	32767
M.Lewin [14]	$\left[\frac{(a_{s-1} - 1)(a_s - 2)}{2}\right] - 1$	31749
P. Erdös & R. L. Graham [7]	$2a_{s-1}\left[\frac{a_s}{s+1}\right] - a_s.$	
	42414	

Now we turn to another result of this type.

3.1.9 ***Lemma.*** Let $A = \{0, a_1, a_2, \ldots, a_s\}$ be a set of distinct residues modulo a_0. If $a_0 \leq 2s + 1$, then $2A$ contains all residue classes modulo a_0.

Proof. Let $a_0 = m$. Consider the additive group Z_m of residues mod m. Suppose there exists an element g in Z_m such that g is not in $2A$. Define the set

$$B = \{g - x \pmod{m} : x \in A\}.$$

First we show that B is disjoint from A. For, otherwise $g - x \equiv y$ for some $y \in A$, then $g \equiv x + y, x, y \in A$, which contradicts the fact that g is not in $A + A$.

Next, we shall show that A and B have the same cardinality. Consider the map

$$x \to g - x$$

from A into B. If $g - x \equiv g - y$, then clearly $x \equiv y$. Since this map is also surjective, $|A| = |B|$. As A and B are disjoint,

$$|Z_m| \geq |A| + |A| = 2s + 2 \geq a_0 + 1 > a_0 = m,$$

a contradiction.

3.1.10 ***Theorem.*** Let $A = \{a_0, a_1, a_2, \ldots, a_s\}$, $1 < a_0 < a_1 < \ldots < a_s$, $s \geq 2$, be an independent set of relatively prime integers. Let $a_0 \leq 2s + 1$. Then

$$g(a_0, a_1, a_2, \ldots, a_s) \leq 2a_s - a_0.$$

Proof. Let $r_i \equiv a_i \pmod{a_0}$, $0 \leq r_i \leq a_0 - 1$, $i = 0, 1, 2, \ldots, s$. It follows from independence that $r_i \neq 0$ for $i = 1, 2, \ldots, s$ and $r_i \not\equiv r_j \pmod{a_0}$ for all $i \neq j$. For, if $r_i = 0$, for some $i \geq 1$, then $a_i \equiv a_0 \pmod{a_0}$. Since $a_i > a_0$, a_i has a representation $a_i = a_0 + t\,a_0$, $t \geq 1$, by a_0 alone. This contradicts independence.

Now suppose that

$$r_i \equiv r_j \pmod{a_0} \text{ for some } i < j.$$

Then $a_i \equiv a_j \pmod{a_0}$ so that a_j has a representation of the form

$$a_j = a_i + t\,a_0,$$

Again this contradicts independence.

Let

$$B = \{0,\ r_1, r_2, \ldots, r_s\}.$$

Then B is a set of distinct residues mod a_0. Now $s + 1 = |B|$ and $2s + 1 \geq a_0$. Therefore by Lemma 3.1.9, $B + B$ contains all residue classes mod a_0. Consider the set

$$\{a_i + a_j : 0 \leq i \leq j \leq s\}.$$

Clearly if $a_i + a_j \equiv r \pmod{a_0}$, and if t_r denotes the smallest integer $\equiv r \pmod{a_0}$ representable by the a_i's then $t_r \leq a_i + a_j$. Therefore

$$max\,\{t_r : r \in [1, a_0 - 1]\} \leq a_s + a_s.$$

Hence by Proposition 2.1.4,

$$g(a_0, a_1, \ldots, a_s) \leq 2\,a_s - a_0.$$

This completes the proof.

Example for sharpness. Theorem 3.1.10 gives a sharp bound. If

$$S = \{2s+1,\ 2s+2,\ \ldots, 3s + 1\},$$

then by [17], we have

$$g(S) = \left[\frac{2s - 1}{s}\right](2s + 1) + 2s = 4s + 1.$$

By the above theorem also we get

$$g(S) \leq 2\,(3s + 1) - (2s + 1) \leq 4s + 1.$$

3.2 *On the conjecture by M.Lewin.*

3.2.1 I. Shur was the first one to obtain an upper bound

(4) $$g(S) \leq (a_0 - 1)(a_s - 1) - 1$$

for any set S of $s + 1$ relatively prime positive integers where $s \geq 1$, $S = \{a_0, a_1, \ldots, a_s\}$, $a_0 < a_1 < \ldots, a_s$. This bound was published by A. Brauer [2].

M. Lewin [15] proved that for $s \geq 2$,

(5) $$g(S) \leq \left[\frac{1}{2}(a_s - 2)^2\right] - 1,$$

where $[x]$ denotes the greatest integer $\leq x$, and he also showed that for $s = 2$, this bound is sharp. He conjectured [15, page 69] that for any $s \geq 1$,

(6) $$g(S) \leq \left[\frac{(a_s - 2)(a_s - s)}{s}\right] - 1.$$

For a given set $S = \{a_0, a_1, \ldots, a_s\}$ of relatively prime integers, Y.Vitek [23] considered the two special cases

(7) *Case (i).* $a_0 \geq \frac{2}{3} a_s$.

(8) *Case (ii).* S contains distinct residues mod (a_0) such that for every divisor r of a_0 with $r < s$ such that r does not divide s, the number of residues (mod a_0/r) of S is not $1 + [s/r]$.

In each of these two cases he showed that

(9) $$g(S) \leq \left[\frac{(a_0 - 2 + s)}{s}\right](a_s - s) - 1.$$

Since $a_0 + s \leq a_s$, (9) shows that the conjecture of Lewin is valid in each of these two cases.

The purpose of this section is to show that the conjecture of M.Lewin is valid for any $s \geq 3$ in a special case different from the cases mentioned above. In fact the bound we obtain is stronger than (6) for all $s \geq 3$. Our main theorem is

3.2.2 ***Theorem.*** Let $S = \{a_0, a_1, a_2, \ldots, a_s\}$, $1 < a_0 < a_1 < \ldots < a_s$, $s \geq 2$, be a given independent set of relatively prime integers. Let

$$\frac{a_2}{2} \leq \frac{a_3}{3} \leq \ldots \leq \frac{a_s}{s}.$$

Then

(10) $$g(a_0, a_1, a_2, \ldots, a_s) \leq \left[\frac{a_0(a_s - s)}{s}\right].$$

We first prove a Lemma.

3.2.3 ***Lemma.*** Let $a_1, a_2, \ldots, a_s$, $1 < a_1 < \ldots < a_s$, satisfy

$$a_i \not\equiv a_j \pmod{a_1} \text{ for } i \neq j.$$

Let $d =$ g.c.d.$(a_1, a_2, \ldots, a_s)$. Then $d \leq \frac{a_1}{s}$.

Proof. Suppose $d > \frac{a_1}{s}$. Let $a_i = db_i$, $i = 1, 2, \ldots, s$. Let $r_i \equiv b_i \pmod{b_1}$, $i = 1, 2, \ldots, s$, $0 \leq r_i \leq b_1 - 1$. Suppose $r_i = r_j$, where $i < j$ then $b_j \equiv b_i \pmod{b_1}$. That is, $b_j - b_i = tb_1$ for some integer $t \geq 1$. This implies that

$$a_j - a_i \equiv 0 \pmod{a_1},$$

which contradicts the hypothesis. Therefore the set $\{r_1, r_2, \ldots, r_s\}$ has s distinct non-negative integers $\leq b_1 - 1$. In other words

$$| \{r_1, r_2, \ldots, r_s\} | = s \leq b_1 < s, \text{ which is not possible.}$$

Hence we must have $d \leq \frac{a_1}{s}$. This proves the Lemma.

We now prove Theorem 3.2.2.

Proof of Theorem 3.2.2. Let $d = \text{g.c.d.}(a_0, a_1, \ldots, a_{s-1})$. The numbers $a_0, a_1, \ldots, a_s$ are pairwise incongruent modulo a_0. For, otherwise if $a_i \equiv a_j \pmod{a_0}$ where $0 \leq i < j \leq s-1$, then $a_j = a_i + x\, a_0$ for some integer $x \geq 1$, which contradicts the fact that the set $\{a_0, a_1, \ldots, a_s\}$ is independent. We therefore assume that $a_i \not\equiv a_j \pmod{a_0}$ for all $i \neq j$. Now we can apply Lemma 3.2.3 to $\{a_0, a_1, \ldots, a_{s-1}\}$ which yields $d \leq \frac{a_0}{s}$.

We now prove the theorem by induction on s.

For $s = 2$, the result follows from (8) and (9) above. Let $s \geq 3$. By Lemma 2.1.7,

$$g(a_0, a_1, a_2, \ldots, a_s) = d \bullet g\left(\frac{a_0}{d}, \frac{a_1}{d}, \ldots, \frac{a_{s-1}}{d}, a_s\right) + (d-1)\, a_s. \tag{11}$$

Also we have

$$g\left(\frac{a_0}{d}, \frac{a_1}{d}, \ldots, \frac{a_{s-1}}{d}, a_s\right) \leq g\left(\frac{a_0}{d}, \frac{a_1}{d}, \ldots, \frac{a_{s-1}}{d}\right) \tag{12}$$

Using this in (11) we get

$$g(a_0, a_1, a_2, \ldots, a_s) \leq d \bullet g\left(\frac{a_0}{d}, \frac{a_1}{d}, \ldots, \frac{a_s - 1}{d}\right) + (d-1)\, a_s$$

Using the induction hypothesis, we get

$$g(a_0, a_1, a_2, \ldots, a_s) \leq d\left[\frac{\frac{a_0}{d}\left(\frac{a_s - 1}{d} - s + 1\right)}{s-1}\right] + (d-1)\, a_s$$

$$g(a_0, a_1, a_2, \ldots, a_s) \leq d\left\{\frac{a_0 a_{s-1}}{d^2(s-1)} - \frac{a_0}{d}\right\} + (d-1)\, a_s.$$

That is,

$$g(a_0, a_1, a_2, \ldots, a_s) \leq \frac{a_0\, a_s - 1}{d(s-1)} + d\, a_s - (a_0 + a_s).$$

Define the function

(13) $$u(x) = \frac{a_0 a_s - 1}{x(s-1)} + a_s \bullet x$$

Then,

(14) $$g(a_0, a_1, a_2, \ldots, a_s) \leq u(d) - (a_0 + a_s)$$

By Lemma 3.2.3, $d \leq \frac{a_0}{s}$ and therefore we consider $u(x)$ on $J = \left[1, \frac{a_0}{s}\right]$.

Clearly $u(x)$ is a continuous function of x on J, and $u''(x) > 0$ on this interval. This implies that $u'(x)$ is increasing on J. Therefore the absolute maximum of $u(x)$ on J is attained either at $x = 1$ or at $x = \frac{a_0}{s}$.

Now $$u(1) = \frac{a_0 a_s - 1}{s-1} + a_s$$

and

$$u\left(\frac{a_0}{s}\right) = \frac{sa_{s-1}}{s-1} + \frac{a_0 a_s}{s}.$$

$$u(1) - u\left(\frac{a_0}{s}\right) = \left(\frac{a_{s-1}}{s-1}\right)(a_0 - s) + \frac{a_s}{s}(s - a_0)$$

(15) $$u(1) - u\left(\frac{a_0}{s}\right) = (a_0 - s)\left(\frac{a_{s-1}}{s-1} - \frac{a_s}{s}\right).$$

Now by hypothesis,

(16) $$\frac{a_{s-1}}{s-1} \leq \frac{a_s}{s}.$$

As $\{a_0, a_1, a_2, \ldots, a_s\}$ is independent, the set constitutes $s + 1$ distinct residues mod a_0 and therefore $a_0 \geq s + 1$. This implies

(17) $$a_0 - s > 0.$$

Using (17)and (16) in (15), we see that

$$u(1) - u\left(\frac{a_0}{s}\right) \leq 0.$$

Now (14) yields

$$g(a_0, a_1, a_2, \ldots, a_s) \leq u\left(\frac{a_0}{s}\right) - (a_0 + a_s)$$

$$= \frac{sa_{s-1}}{s-1} + \frac{a_0 a_s}{s} - (a_0 + a_s)$$

$$= \frac{a_0 a_s}{s} - a_0 + \left(\frac{sa_{s-1}}{s-1} - a_s\right),$$

so using (16) we get

$$g(a_0, a_1, a_2, \ldots, a_s) \leq \frac{a_0 a_s}{s} - a_0,$$

That is,

$$g(a_0, a_1, a_2, \ldots, a_s) \leq \left[\frac{a_0(a_s - s)}{s}\right].$$

This completes the proof of Theorem 3.2.2.

3.2.4 ***Example***. Consider the set $S = \{15, 21, 26, 40, 65\}$. This set is independent since $21 \notin Sp(15)$, $26 \notin sSp(15, 21)$ $40 \notin Sp(15, 21, 26)$ and $65 \notin Sp(15, 21, 26, 40)$. Since g.c.d.(15, 26) = 1, the set S is relatively prime. Now Vitek's theorem cannot be applied since the conditions (7) and (8) are not true. That is,

$(1) a_0 < \frac{2}{3} a_4$ and

(2) $s = 4$, 3 divides 15, 5 divides 15 , $3 < s$, 3 does not divide s. Taking modulo 5, the elements of S are 0 and 1 only. But $1 + \left[\frac{4}{3}\right] = 2$.

However the condition of theorem 3.2.2 is true since

$$\frac{26}{2} \leq \frac{40}{3} \leq \frac{65}{4}.$$

Therefore we have

$$g(15, 21, 26, 40, 65) \leq \left[\frac{15(65 - 4)}{4}\right] = 228.$$

For comparison we give the following values obtained by using the best known bounds.

E. S. Selmer [19]	$2a_4\left[\frac{a_0}{5}\right] - a_0$	375
J. J. Sylvester [21]	$(a_0 - 1)(a_2 - 1) - 1$	349
Y. Vitek [23]	$\left[\frac{a_s^2}{s}\right] - 1$	1055
P. Erdös & R. L. Graham [7]	$2a_{s-1}\left[\frac{a_s}{s+1}\right] - a_s.$	975
M. Lewin [15]	$\left[\frac{(a_{s-1} - 1)(a_s - 2)}{2}\right] - 1$	1227

3.2.5 ***Example***. Consider the often quoted example [3] consisting of the three numbers 137, 251, 256. We will take $a_0 = 137$, $a_1 = 251$, $a_2 = 256$ and $a_3 = 385$. Then a_0, a_1, a_2, a_3 satisfy the above theorem and we obtain

$$\boxed{g(a_0, a_1, a_2, a_3) \leq 17444}.$$

We give below the values obtained by using other best known bounds which are proved in the general case.

J. J. Sylvester[21]	$(a_0 - 1)(a_1 - 1) - 1$	33999
A. Brauer [2]	$(a_0 - 1)(a_s - 1) - 1$	52223
Y. Vitek [23]	$\left[\frac{a_s^2}{s}\right] - 1$	49407

M. Lewin [14]	$\left[\frac{(a_{s-1}-1)(a_s-2)}{2}\right]-1$	48831
P. Erdös & R. L. Graham [7]	$2a_{s-1}\left[\frac{a_s}{s+1}\right]-a_s$	48767
E. S. Selmer [19]	$2a_3\left[\frac{a_0}{4}\right]-a_0$	26043

Using Lemma 3.2.3 and similar techniques as in Theorem 3.2.2 we can get a better bound in the special case when $S = \{a_0, a_1, a_2, a_3\}$consists of relatively prime integers with and g.c.d.$(a_0, a_1, a_2) = d \geq 2$. We have the folowing result in this direction. We use the sharp bound for three variables obtained by Y.Vitek (Theorem 1, [22]) which is stated below.

3.2.6 ***Lemma.*** Let p, q, r be an independent set of integers such that $p < q < r$ and $(p, q, r) = 1$. Then

$$g(p, q, r) \leq \left[\frac{p}{2}\right](r-2)-1.$$

3.2.7 ***Theorem.*** Let $\{a_0, a_1, a_2, a_3\}$, $1 < a_0 < a_1 < a_2 < a_3$, be an independent set of integers with g.c.d. $(a_0, a_1, a_2) = d \geq 2$. Then

$$g(a_0, a_1, a_2, a_3) \leq a_3\left(\left[\frac{a_0}{3}\right]+2\right)-a_0.$$

Proof. Let d = g.c.d.(a_0, a_1, a_2). Since a_0, a_1, a_2, a_3 are independent they are pairwise incongruent modulo a_0. Now using Lemma 3.2.3 for the numbers a_0, a_1, a_2 we get $d \leq \frac{a_0}{3}$. Consider the set $S = \left\{\frac{a_0}{d}, \frac{a_1}{d}, \frac{a_2}{d}\right\}$. Since $\{a_0, a_1, a_2\}$ is independent so is S. So we can apply Lemma 3.2.6 and obtain

$$g(S) \leq \left[\frac{a_0}{2d}\right]\left(\frac{a_2}{d} - 2\right) - 1. \tag{18}$$

By Lemma 2.1.7,

$$g(a_0, a_1, a_2, a_3) = d\, g\left(\frac{a_0}{d}, \frac{a_1}{d}, \frac{a_2}{d}, a_3\right) + (d-1)\, a_3. \tag{19}$$

Therefore $$g(a_0, a_1, a_2, a_3) \leq d.g\left(\frac{a_0}{d}, \frac{a_1}{d}, \frac{a_2}{d}\right) + (d-1)a_3$$

$$\leq d\left\{\left[\frac{a_0}{2d}\right]\left(\frac{a_2}{d} - 2\right) - 1\right\} + (d-1)a_3 \text{ , using (18)}$$

so that

$$g(a_0, a_1, a_2, a_3) \leq \frac{a_0 a_2}{2d} + (a_3 - 1)\, d - (a_0 + a_3).$$

Define

$$u(d) = \frac{a_0 a_2}{2d} + (a_3 - 1)\, d.$$

Then the last inequality becomes

$$g(a_0, a_1, a_2, a_3) \leq u(d) - (a_0 + a_3). \tag{20}$$

Since $u(d)$ is a continuous function of d for $d \geq 2$, (in fact for $d > 0$), and $u''(d) > 0$, $u'(d)$ is increasing for $d \geq 2$. Therefore the absolute maximum of $u(d)$ on $\left[2, \frac{a_0}{3}\right]$ is assumed either at $d = 2$ or at $d = \frac{a_0}{3}$. Now,

$$u(2) = \frac{a_0 a_2}{4} + 2(a_3 - 1),$$

$$u\left(\frac{a_0}{3}\right) = \frac{3a_2}{2} + \frac{a_0 a_3}{3} - \frac{a_0}{3}.$$

Therefore

$$u(2) - u\left(\frac{a_0}{3}\right) = \left(\frac{a_2}{4} - \frac{a_3}{3} + \frac{1}{3}\right)(a_0 - 6)$$

$$= \left(\frac{a_2}{4} - \frac{a_3 - 1}{3}\right)(a_0 - 6).$$

$$\leq \left(\frac{a_2}{3} - \frac{a_3 - 1}{3}\right)(a_0 - 6)$$

$$\leq 0,$$

since $2 \leq d \leq \frac{a_0}{3}$ and $a_2 \leq a_3 - 1$.

Returning to (20) we have

$$g(a_0, a_1, a_2, a_3) < u\left(\frac{a_0}{3}\right) - (a_0 + a_3)$$

$$= \frac{3a_2}{2} + \frac{a_0 a_3}{3} - \frac{a_0}{3} - (a_0 + a_3)$$

$$< \frac{a_0 a_3}{3} + \frac{a_3}{2} - \frac{4a_0}{3}$$

$$= a_3\left(\frac{1}{3}a_0 + \frac{1}{2} - \frac{a_0}{3a_3}\right) - a_0$$

$$\leq a_3\left(\left[\frac{a_0}{3}\right] + 2\right) - a_0.$$

This completes the proof of Theorem 3.2.7.

3.3 *An algorithm to find an upper bound for* $g(a_1, a_2, a_3, a_4)$.

3.3.1 We begin with a set $\{a_1, a_2, a_3, a_4\}$ of four given relatively prime integers ≥ 2, with $(a_i, a_1) = 1$ for $i = 2, 3, 4$, and a_2, a_3, a_4 pairwise incongruent modulo a_1. As $(a_1, a_2) = 1$, the congruence

$$a_2 x \equiv a_3 \pmod{a_1}$$

has a solution x_1 with $0 \leq x_1 < a_1$. As a_2 and a_3 are incongruent mod a_1, $x_1 > 1$. Hence there exist solutions (x, y) to the congruence

$$a_2 x \equiv a_3 y \pmod{a_1}, \quad 1 \leq y < x.$$

Let (x_1, y_1) be one such solution with least x_1. Then we have

$$a_2 x_1 \equiv a_3 y_1 \pmod{a_1}, \quad 1 \leq y_1 < x_1 \tag{30}$$

where x_1 is least satisfying (30).

Similarly we obtain (y_2, z_2) satisfying

$$a_3 y_2 \equiv a_4 z_2 \pmod{a_1}, \quad 1 \leq z_2 < y_2 \tag{31}$$

and y_2 is least with these properties.

Further, in the same way we get (x_3, z_3) satisfying

$$a_4 z_3 \equiv a_2 x_3 \pmod{a_1}, \quad 1 \leq x_3 < z_3 \tag{32}$$

with least z_3. Set $z_1 = x_2 = y_3 = 0$.

Define the *translation vectors* t_i, $i = 1, 2, 3$, as follows.

$$t_1 = (-x_1, y_1, z_1)$$

$$t_2 = (x_2, -y_2, z_2)$$

$$t_3 = (x_3, y_3, -z_3)$$

We note that

$$x_1 > y_1 + z_1, \qquad y_2 > x_2 + z_2, \qquad z_3 > x_3 + y_3.$$

If either

$$p \geq x_1 \qquad \text{or } q \geq y_2 \qquad \text{or } r \geq z_3$$

then add t_1 or t_2 or t_3 respectively to the point (p, q, r).

Define

$$M(x, y, z) = a_2 x + a_3 y + a_4 z.$$

Suppose $M(p, q, r) \equiv j \pmod{a_1}$. If $p \geq x_1$, then add t_1 to (p, q, r). We get

$$M(p - x_1, q + y_1, r + z_1) = M(p, q, r) + M(-x_1, y_1, z_1).$$

Using (30) we see that

$$M(p - x_1, q + y_1, r + z_1) \equiv M(p, q, r) \pmod{a_1}.$$

Similarly each of the translations t_2, or t_3 preserves the congruence (mod a_1). Moreover taking the distance function d as the sum of the absolute differences for any two 3-tuples, we see that point $(p - x_1, q + y_1, r + z_1)$ is closer to the origin than (p, q, r). Thus at each step of the translation by t_i, the point is moved closer to the origin. We continue the procedure until we arrive at the point (p_n, q_n, r_n), say, where

$$0 \leq p_n < x_1 \ , 0 \leq q_n < y_2, \ 0 \leq r_n < z_3.$$

Any further translation would result in a point with a negative integral coordinate.

Notice that as initially the point (p, q, r) is at a distance $p + q + r$ from the origin procedure must terminate in at most $p + q + r$ steps. Thus if (p, q, r) is any point with non-negative integer coordinates outside the region

$$P = \{(x,y, z) : 0 \leq x < x_1, 0 \leq y < y_2, 0 \leq z < z_3\}$$

and if $M(p, q, r) \equiv j \pmod{a_1}$, then there exists $(p_n, q_n, r_n) \in P$ with $M(p_n, q_n, r_n) \equiv j \pmod{a_1}$. It follows that the set

$$\{M(x, y, z) : (x, y, z) \in P\}$$

contains a complete system of residues mod a_1.

Therefore by Lemma 2.1.4 we have

$$g(a_1, a_2, a_3, a_4) = max\{t_r : r = 0, 1, \ldots, a_1 - 1\} - a_1$$

$$\leq max\{M(x,y, z) : (x,y, z) \in P\} - a_1$$

$$g(a_1, a_2, a_3, a_4) \leq (x_1-1)\, a_2 + (y_2-1)\, a_3 + (z_3-1)\, a_4 - a_1. \tag{33}$$

3.3.2 This algorithm can be generalized to any set $S = \{a_0, a_1, \ldots, a_s\}$, for $s \geq 3$. Assume that g.c.d.$(a_0, a_i) = 1$ for $i = 1, 2, \ldots, s$ and that $a_0, a_1, \ldots, a_s$ are pairwise incongruent modulo a_0. We can generalize the above algorithm for finding an upper bound for $g(a_0, a_1, \ldots, a_s)$, as follows.

We solve

$$a_i x \equiv a_{i+1} y \pmod{a_0}, \qquad 1 \leq x_{i+1} < x_i \tag{34}$$

for $i = 1, 2, \ldots, s$ where we set $a_{s+1} = a_1$. The solution with least x is denoted by (x_i, y_i). The corresponding translation vector t_i, $i = 1, 2, \ldots, s - 1$, is defined to be the s-tuple

$$t_i = (0, 0, \ldots, 0, -x_i, y_i, 0, \ldots, 0),$$

where the i-th position has $-x_i$ and the $(i+1)$-th position has y_i. For s, we have $t_s = (y_s, 0, \ldots, 0, -x_s)$.

The algorithm now gives

$$g(a_0, a_1, \ldots, a_s) \leq \sum_{i=1}^{s} (x_i - 1)\, a_i - a_0.$$

CHAPTER 4

4.1 ***Basic Definitions.*** A *rooted tree* is a connected acyclic digraph with a distinguished node called the root. The *height* of a node is the length of the unique path from the root to the node.

A node is called a *leaf* if it has outdegree zero. If the outdegree is not zero, the node is an internal node. The set of nodes of height m is called the mth level of the tree.

The notion of a (2, 3)–tree is well known (see for example [12]) in theoretical computer science. By definition, a (2, 3)–tree is a rooted tree such that

(i) the outdegree of each internal node is either 2 or 3,

(ii) the heights of all leaves are the same.

A (2, 3)–tree

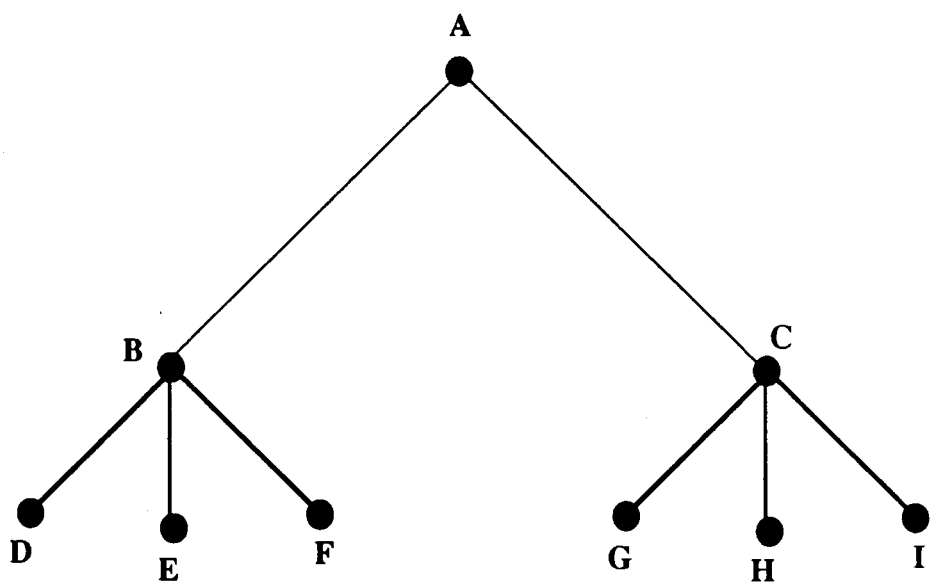


Figure 2

This concept of a (2,3)–tree has a natural extension [11] as follows.

Given positive integers $g_0, g_1, \ldots, g_s$, $1 \le g_0 \le g_1 \le \ldots \le g_s$, we define a $(g_0, g_1, \ldots, g_s)$–tree to be a rooted tree such that

(i) the outdegree of each internal node is either g_0, or g_1, or $\ldots$, g_s,

(ii) the heights of all leaves are the same.

It is easy to see that for any positive integer n there is a (2, 3)–tree having exactly n leaves.

We say that a positive integer n is *representable* by a $(g_0, g_1, \ldots, g_s)$–tree if there exists a $(g_0, g_1, \ldots, g_s)$–tree with exactly n leaves. It follows from the last statement that every positive integer is representable by a (2, 3)–tree. Figure 2 shows that 6 is representable by a (2, 3)–tree. If we take the integers 3 and 5 then it is not true that every positive integer has a representation by a (3, 5)–tree. For example, 8 is not representable by a (3,5)–tree.

A characterization (Theorem 1, [12]) for the representation of positive integers by $(g_0, g_1, \ldots, g_s)$–trees is as follows.

Given integers $g_0, g_1, \ldots, g_s$, $1 \le g_0 \le g_1 \le \ldots \le g_s$, $s \ge 1$, there exists a positive integer $N=N(g_0, g_1, \ldots, g_s)$ such that every integer $n \ge N$ can be represented by a $(g_0, g_1, \ldots, g_s)$–tree iff g.c.d.$(g_1 - g_0, g_2 - g_0, \ldots, g_s - g_0) = 1$.

The *conductor* $\kappa(g_0, g_1, \ldots, g_s)$ is the least positive integer such that for any $n \ge \kappa(a_0, a_1, \ldots, a_s)$ there exists a $(g_0, g_1, \ldots, g_s)$–tree with exactly n leaves.

Given positive integers $g_0, g_1, \ldots, g_s$, $1 < g_0 < g_1 < \ldots < g_s$, $s \ge 1$, with g.c.d.$(g_1 - g_0, g_2 - g_0, \ldots, g_s - g_0) = 1$, the problem of finding the exact value of $\kappa(g_0, g_1, \ldots, g_s)$ is closely related to the Frobenius problem. In [10] an upper bound for

$\kappa(g_0, g_1, \ldots, g_s)$ is given. This bound yields the exact value of $\kappa(g_0, g_1, \ldots, g_s)$ when $g_0, g_1, \ldots, g_s$ are consecutive integers.

In the next section we first find the exact value of $\kappa(a, a+1)$ and then deduce from this the exact value of $\kappa(a, a+1, \ldots, a+s)$ for any integer $s \geq 1$.

4.2 *The conductor $\kappa(a, a+1, \ldots, a+s)$ for $s \geq 1$.*

4.2.1 ***Theorem***. Let a, b, $1 < a, b=a+1$, be given integers. Then $\kappa(a, b) = a^{f(a)}$, where $f(a)$ is the least positive integer satisfying

$$a^{f(a)+1} \leq b^{f(a)} + 1.$$

Proof. Suppose N is any positive integer such that

(1) $a^{n-r+1} b^r \leq N \leq a^{n-r} b^{r+1}$, where r, n are integers such that $0 \leq r \leq n$.

Solving the equations

(2) $ax + by = N, \qquad x + y = a^{n-r} b^r$

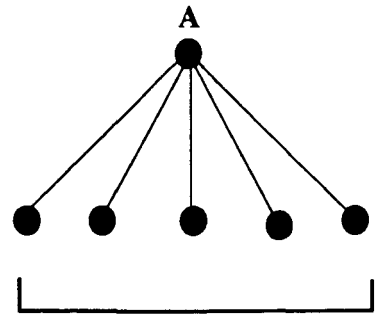
we get $x = a^{n-r} b^{r+1} - N$

$y = N - a^{n-r+1} b^r$.

By (1) we see that x and y are non-negative integers satisfying the system (2). We now construct an (a, b)–tree with exactly N leaves.

We start with the root. Replace the root by an a–tree. (An x–tree is a rooted tree with x leaves all at height one as shown in figure 3.)

An x–tree



x **leaves**

Figure 3

Now we have an a–tree. Replace each of the a leaves with an a–tree. Starting from the root we do this $n - r$ times. The resulting tree has a^{n-r} leaves, all at height $n - r$. Further, each of its internal nodes has outdegree a. Now replace each of these a^{n-r} leaves by a b–tree. We obtain an (a, b)–tree with $a^{n-r}b$ leaves. Repeat this procedure of replacing by a b-tree for r-levels. This construction now gives an (a, b)–tree with exactly $a^{n-r}b^r$ leaves. We complete the construction (figure 4) by replacing x of these $a^{n-r}b^r$ leaves by an a–tree and each of the remaining leaves by a b–tree. Since $ax + by = N$ and $x + y = a^{n-r}b^r$ the resulting (a, b)–tree has exactly N leaves.

Therefore every integer in the interval $[a^{n-r+1}\, b^r,\ a^{n-r}\, b^{r+1}]$, for integers r, n satisfying $0 \leq r \leq n$, is representable by an (a, b)-tree. For any fixed integer $n \geq 0$, we see that

$$\bigcup_{r=0}^{n} [a^{n-r+1} b^r,\ a^{n-r} b^{r+1}] = [a^{n+1},\ b^{n+1}] .$$

This implies that every integer in $[a^{n+1},\ b^{n+1}]$ is representable by an (a, b)–tree for each integer $n \geq 0$.

Denote by $f(a)$ the least positive integer such that

(3) $$a^{f(a)+1} \leq b^{f(a)} + 1.$$

That is,

(4) $$b^{f(a)-1} + 1 < a^{f(a)},\ a^{f(a)+1} \leq b^{f(a)} + 1.$$

Then it follows that every integer $\geq a^{f(a)}$ is representable by an (a, b)–tree. This proves that

$$\kappa(a, b) \leq a^{f(a)} .$$

In fact we can show that the equality holds.

Suppose $a^{f(a)} - 1$ is representable by an (a, b)–tree say T. Then there exist non-negative integers x, y such that

(5) $ax + by = a^{f(a)} - 1.$

It is easy to see that $a^{f(a)}$ is the least positive integer representable by an (a, b)–tree having $f(a)$ levels. Therefore the number h of levels in T is at most $f(a) - 1$. Observe that T has $x + y$ nodes at the $(h\text{-}1)$th level. Note that the largest integer representable by an (a, b)–tree of height t is b^t and therefore

$$x + y \leq b^{f(a)-2}.$$

Hence

$$ax + by < b(x + y) \leq b.\ b^{f(a)-2}.$$

Using (5), $a^{f(a)} - 1 < b^{f(a)-1}$

$a^{f(a)} \leq b^{f(a)-1}$, a contradiction to (4).

Therefore it follows that $\kappa(a, b) = a^{f(a)}$.

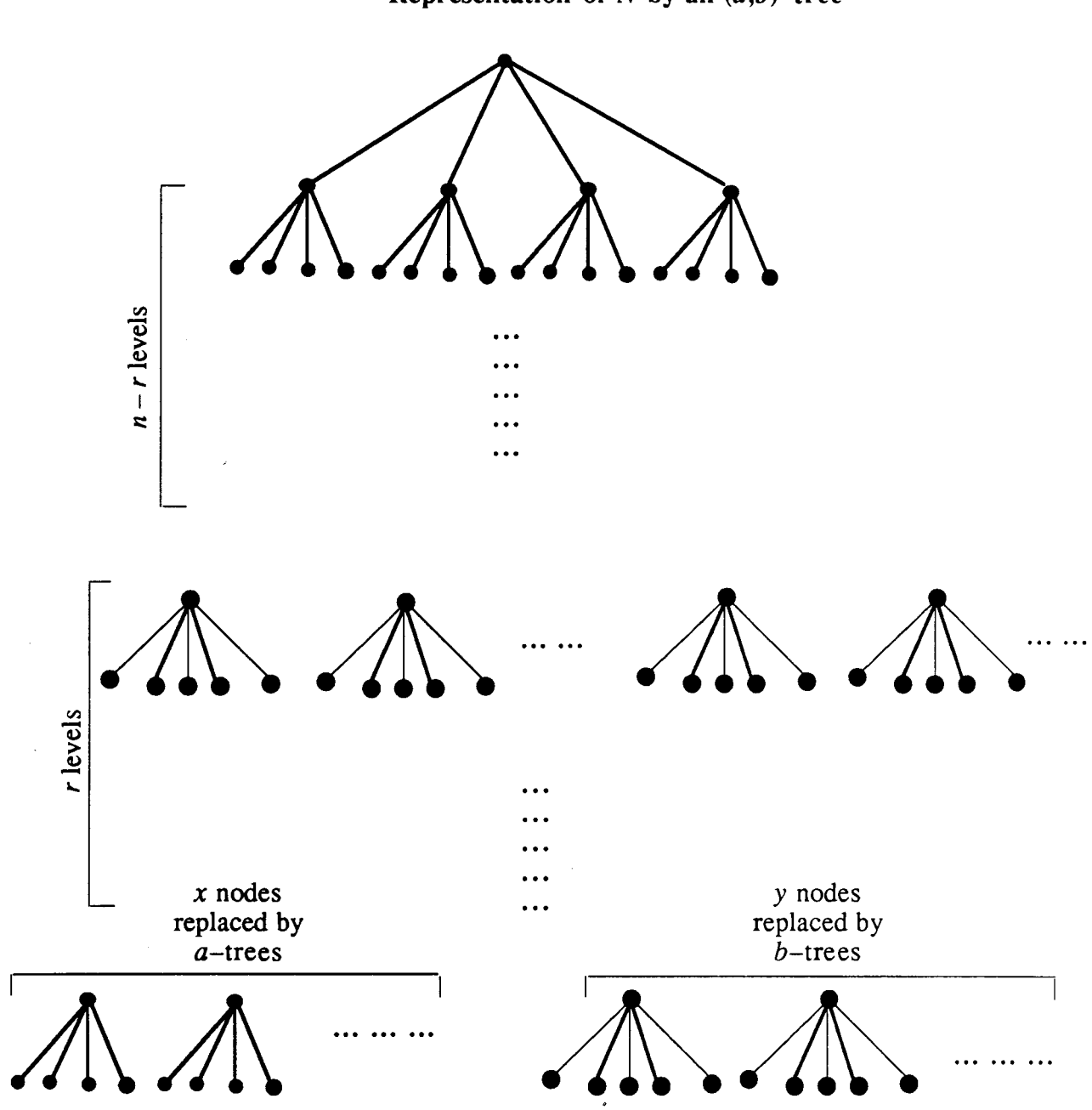

Representation of N by an (a,b)–tree
$n - r$ levels
r levels
x nodes replaced by a–trees
y nodes replaced by b–trees

Figure 4

4.2.2. *Corollary.* Given positive integers $a, a+1, a+2, \ldots, a+s, s \geq 1$, we can deduce that

$\kappa(a, a+1, a+2, \ldots, a+s) = a^k$, where k is the least positive integer such that

$$a^{k+1} \leq (a+s)^k + 1.$$

Proof. Clearly each integer in $[a, a+s]$ is representable by a $(a, a+1, \ldots, a+s)$–tree. By the proof of the above theorem each integer in $[(a+i)^n, (a+i+1)^n]$ is representable by an $(a+i, a+i+1)$- tree for $i=0, 1, \ldots, s-1$. If a number is representable by an $(a+i, a+i+1)$–tree then it is also representable by an $(a, a+1, \ldots, a+s)$–tree. Therefore every integer in $[a^n, (a+s)^n]$ is representable by an $(a, a+1, \ldots, a+s)$–tree for all $n \geq 1$. Therefore if k is the least positive integer such that

(6) $$a^{k+1} \leq (a+s)^k + 1$$

then

$$\kappa(a, a+1, a+2, \ldots, a+s) \leq a^k.$$

We will now show that the equality holds by a similar argument as in Theorem 4.2.1 for $s = 1$.

Suppose $a^k - 1$ is representable by an $(a, a+1, a+2, \ldots, a+s)$–tree say T. Then there exist non-negative integers x_i, $i=0, 1, \ldots, s$, such that

(7) $$\sum_{i=0}^{s} (a+i)x_i = a^k - 1.$$

It is easy to see that a^k is the least positive integer representable by an $(a, a+1, a+2, \ldots, a+s)$–tree having k levels. Therefore the number h of levels in T is at most $k-1$. Observe that T has $\sum x_i$ nodes at the $(h-1)$th level and therefore

$$\sum x_i \leq (a+s)^{k-2}.$$

Hence using (7) in

$$\sum_{i=0}^{s}(a+i)x_i < (a+s)\sum(x_i) \leq (a+s).(a+s)^{k-2},$$

we get

$$a^k - 1 < (a+s)^{k-1}.$$

That is,

$$a^k \leq (a+s)^{k-1},$$

a contradiction to the minimality of k in (6). Hence

$$\kappa(a, a+1, a+2, \ldots, a+s) = a^k.$$

4.3 ***A bound for*** $\kappa(g_0, g_1, \ldots, g_s)$. In the general case, given positive integers g_0, $g_1, \ldots, g_s$, $1 < g_0 < g_1 < \ldots < g_s$, $s \geq 1$, with g.c.d.$(a_1, a_2, \ldots, a_s) = 1$, $g_i - g_0 = a_i$, $i=1, 2, \ldots, s$, an upper bound for $\kappa(g_0, g_1, \ldots, g_s)$ is given in [10] using an upper bound for the Frobenius function $g(a_1, a_2, \ldots, a_s)$.

Let d_i = g.c.d.$(a_1, a_2, \ldots, a_i)$, $g(a_1, a_2, \ldots, a_s) \leq L$

where

$$L = 1 + \sum_{i=1}^{s-1}\frac{a_{i+1}.d_i}{d_{i+1}} - \sum_{i=1}^{s}a_i$$

is the upper bound obtained by A. Brauer in [2]. Define

$$A = g_0 \cdot g_n + L, \qquad C = g_0 \cdot g_n + a_1(g_n + 1) - 1.$$

Let $m \geq 2$ be the least integer satisfying

$$g_0^{m+1} - g_0^2 + A \leq g_n^m - g_n^2 + C + 1.$$

Then

$$\kappa(g_0, g_1, \ldots, g_s) \leq g_0^m - g_0^2 + A. \tag{8}$$

The set of integers representable by height 1 trees is clearly $\{g_0, g_1, \ldots, g_s\}$. Let d denote the maximum of the differences $(g_{i+1} - g_i)$, $i = 0, 1, \ldots, s-1$. To prove (8) it was shown in [10] that there is a set containing more than d consecutive positive integers representable by $g_0, g_1, \ldots, g_s$–trees of height 2 using an upper bound for the Frobenius function for s variables. It would be interesting to find the the exact value of $\kappa(g_0, g_1, \ldots, g_s)$ as a function of the exact value of $g(a_1, a_2, \ldots, a_s)$.

BIBILIOGRAPHY

1. *P.T. Bateman*, Remark on a recent note on linear forms, Amer. Math. Monthly, 65 (1958)517 – 518.

2. *A. Brauer*, On a problem of partitions, Amer. J. Math. 63 (1942), 299 – 312.

3. *A. Brauer* and *J. E. Shockley*, On a problem of Frobenius, J. reine angew. Math.211 (1952), 215 – 220.

4. *A. Brauer* and *B. M. Seelbinder*, On a problem of partitions–II, Amer. J. Math. 76 (1954), 343 – 346.

5. *J. S. Byrnes*, On partition problem of Frobenius, J. Comb. Theory (A) 17 (1974) 162 –166.

6. *Jacques Diximier*, Proof of a conjecture by Erdös and Graham concerning the Problem of Frobenius, Journal of Number Theory 34, 198–209 (1990).

7. *P. Erdös and R. L. Graham*, On a linear diophantine problem of Frobenius, Acta Arithm. 21 (1972), 399 – 408.

8. *H. Halberstam* and *K. F. Roth*, Sequences, Springer Edition, 1983.

9. *S. M. Johnson,* A linear diophantine problem, Canad. J. Math. 12 (1950), 390 – 398.

10. *C. A. Jones,* Using linear forms to determine the set of integers realizable by $(g_0, g_1, \ldots, g_k)$–trees, Discrete Mathematics 47(1983)247 – 254.

11. *D. E. Knuth,* The art of computer programming, Vol. 3, Sorting and Searching, Addison-Wesley, Reading, Ma, 1973.

12. *D. T. Lee, C. L. Liu* and *C. K. Wong,* $(g_0, g_1, \ldots, g_k)$–tree and unary OL systems, Theoretical Computer Science 22 (1983)209 – 217.

13. *M. Lewin,* On a problem of Frobenius for an almost consecutive set of integers, J. reine angew. Math. 273 (1976)134 – 137.

14. *M. Lewin,* On a linear diophantine problem, Bull. London Math. Soc. 5 (1973), 75 – 78.

15. *M. Lewin,* A bound for a solution of a linear diophantine problem, J. London Math. Soc. 6 (1972), 61 – 69.

16. *A. Nijenhuis and H. S. Wilf,* Representations of integers by linear forms in non-negative integers, J. Number Theory 4 (1972), 98 – 106.

17. *J. B. Roberts,* On a diophantine problem, Canad. J. Math. IX (1957), 219 – 222.

18. *Ö. J. Rödseth,* On a linear diophantine problem of Frobenius II, J. reine angew. Math. 307/309 (1979), 431 – 440.

19. *E. S. Selme,* On the linear diophantine problem of Frobenius, J. reine angew. Math. 293/4 (1977), 1 – 17.

20. *E. S. Selmer* and Ö. Beyer, On the linear diophantine problem of Frobenius in three variables, J. reine angew. Math. 301 (1978), 161 – 170.

21. *J. J. Sylvester,* Mathematical questions, with their solutions, Educational Times 41 (1884), 21.

22. *Y. Vitek,* Bounds for a linear diophantine problem of Frobenius, J. London Math. Soc. (2) 10 (1975), 79 – 85.

23. *Y. Vitek,* Bounds for a linear diophantine problem of Frobenius II, Canad. J. Math. 28 (1976), 1280 – 1288.