INFORMATION TO USERS

This reproduction was made from a copy of a document sent to us for microfilming. While the most advanced technology has been used to photograph and reproduce this document, the quality of the reproduction is heavily dependent upon the quality of the material submitted.

The following explanation of techniques is provided to help clarify markings or notations which may appear on this reproduction.

1. The sign or "target" for pages apparently lacking from the document photographed is "Missing Page(s)". If it was possible to obtain the missing page(s) or section, they are spliced into the film along with adjacent pages. This may have necessitated cutting through an image and duplicating adjacent pages to assure complete continuity.

2. When an image on the film is obliterated with a round black mark, it is an indication of either blurred copy because of movement during exposure, duplicate copy, or copyrighted materials that should not have been filmed. For blurred pages, a good image of the page can be found in the adjacent frame. If copyrighted materials were deleted, a target note will appear listing the pages in the adjacent frame.

3. When a map, drawing or chart, etc., is part of the material being photographed, a definite method of "sectioning" the material has been followed. It is customary to begin filming at the upper left hand corner of a large sheet and to continue from left to right in equal sections with small overlaps. If necessary, sectioning is continued again beginning below the first row and continuing on until complete.

4. For illustrations that cannot be satisfactorily reproduced by xerographic means, photographic prints can be purchased at additional cost and inserted into your xerographic copy. These prints are available upon request from the Dissertations Customer Services Department.

5. Some pages in any document may have indistinct print. In all cases the best available copy has been filmed.

University Microfilms International

300 N. Zeeb Road
Ann Arbor, MI 48106

8319807

Temkin, Bharti

ON A LINEAR DIOPHANTINE PROBLEM OF FROBENIUS FOR THREE VARIABLES

City University of New York PH.D. 1983

University
Microfilms
International 300 N. Zeeb Road, Ann Arbor, MI 48106

PLEASE NOTE:

In all cases this material has been filmed in the best possible way from the available copy. Problems encountered with this document have been identified here with a check mark __√__.

1. Glossy photographs or pages _____
2. Colored illustrations, paper or print _____
3. Photographs with dark background _____
4. Illustrations are poor copy _____
5. Pages with black marks, not original copy __√__
6. Print shows through as there is text on both sides of page _____
7. Indistinct, broken or small print on several pages _____
8. Print exceeds margin requirements _____
9. Tightly bound copy with print lost in spine _____
10. Computer printout pages with indistinct print _____
11. Page(s) _____ lacking when material received, and not available from school or author.
12. Page(s) _____ seem to be missing in numbering only as text follows.
13. Two pages numbered _____. Text follows.
14. Curling and wrinkled pages _____
15. Other _____

University
Microfilms
International

ON A LINEAR DIOPHANTINE PROBLEM OF FROBENIUS FOR THREE VARIABLES

by

BHARTI TEMKIN

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.

1983

This manuscript has been read and accepted for the University Committee in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

29 April 1983
date

Chairmar of Examining Committee

Prof. L. Auslander

29 April 1983
date

Prof.A.Heller, Executive Officer

Prof. L. Auslander

Prof. A. Heller

Prof. A.T.Vasquez

Supervisory Committee

Dr. R.L. Graham
Head, Mathematical Studies Group,
Bell Laboratories

The City University of New York

"Not Failure but low aim is crime"

Lowell

Abstract

ON A LINEAR DIOPHANTINE PROBLEM OF FROBENIUS FOR THREE VARIABLES

by

Bharti Temkin

Let $a_1,\ldots,a_k$ be integers having no common divisor exceeding one. The question of determining the largest integer $g_k = g(a_1,\ldots,a_k)$ that is not representable in the form $\sum_{i=1}^{k} x_i a_i$ with the x_i nonnegative integers was proposed by G. Frobenius in the nineteenth century.

For $k = 2$ the problem has been solved by J. J. Sylvester [43] in 1884, who showed

$$g(a_1,a_2) = (a_1-1)(a_2-1) - 1 .$$

Since that time some progress has been made in establishing algorithms and bounds for g_k by a variety of researchers. However no general explicit formula even for g_3 has been conjectured. Four special cases for g_3 in which the explicit formulas are known are $g(t,t+1,t+2)$, $g(t,t+1,t+z)$ for $z > 2$ (due to J. B. Roberts), $g(a_1,a_2,a_3)$ where $a_2 \equiv -a_3 \pmod{a_1}$ with a_1,a_2,a_3 relatively prime in pairs (due to A. Brauer and J. E. Shockley) and $g(t,t+y,t+yz)$ where $z \geq 0$ and y an integer (due to G. R. Hofmeister).

The present work develops an algorithm for g_3 which leads to the following explicit formula for g_3: For $0 < a < b < c$ with $gcd(a,b,c) = 1$, $d = gcd(c-b,c-a)$, $0 < i \leq \frac{c-a}{d}$ defined by

$$c \equiv i\left(\frac{c-b}{d}\right) \quad \left(\text{mod } \frac{c-a}{d}\right), \text{ and}$$

$$g = \frac{cd-i(c-b)}{c-a}$$

$$g(a,b,c) = \begin{cases} ga + \frac{bc}{d} - \frac{ab}{d} - a - b - c & \text{if } 0 < i \leq \frac{b-a}{d} \\ ga + \frac{ac}{d} - \frac{ab}{d} + bi - a - b - c & \text{if } \frac{b-a}{d} < i \leq \frac{c-a}{d} \end{cases}$$

provided

$$c > \max\left\{c-a + \left(\frac{b-a}{d}\right)\left(\frac{c-a}{d} - i\right), (i)\left(\frac{c-b}{d}\right)\right\}.$$

The constructive proof of this formula based on an algorithm is given. It will be shown that the already known special cases mentioned above follow from this. Finally some further problems are proposed.

ACKNOWLEDGEMENTS

I wish to express my sincere appreciation to Dr. R. L. Graham, who made it possible for me to work at Bell Laboratories as a Resident Visitor and who suggested the Frobenius Problem to me. I also wish to express my deep appreciation to Dr. A. Odlyzko and Dr. R. L. Graham whose counsel and guidance have been invaluable. They have made it possible for me to solve the problem.

I wish to thank Prof. Auslander for accepting me as his student and making it possible for me to obtain my degree. I also wish to thank Prof. Heller for being understanding and making it possible for me to enjoy mathematics. Last, but not least, I wish to thank Ann Marie McDonough for typing my thesis very efficiently.

To

Heniek, Sarah and Eva

CONTENTS

CHAPTER I

1.1 INTRODUCTION

For $k \geq 2$, let the relatively prime positive integers, (i.e., integers having no common divisor exceeding one) $a_1,\ldots,a_k$ be called the basis elements. We say that an integer n is *representable* by (or *dependent* on) $\{a_1,\ldots,a_k\}$ if there exist non-negative integral coefficients $x_1,x_2,\ldots,x_k$ such that

$$n = x_1a_1+x_2a_2+\ldots+x_ka_k \ . \tag{1.1.1}$$

In this case, we say that x_i is an a_i-coefficient of n (this may not be unique). If (1.1.1) has no solution then n is *independent of* or *not representable by* $a_1,\ldots,a_k$. It is well known and easy to show that the Diophantine equation (1.1.1) has solutions when n is sufficiently large.

The problem of Frobenius consists of determining the largest integer

$$g_k = g(a_1,a_2,\ldots,a_k)$$

which is not representable by the basis elements $a_1,a_2,\ldots,a_k$ — i.e., finding the largest integer $n = g_k$ for which equation (1.1.1) has no solution with non-negative coefficients. (Note that when $gcd(a_1,\ldots,a_k) = d \geq 1$ the problem can be stated as follows:

If $S = \left\{\sum_{i=1}^{k} x_ia_i | x_i \geq 0\right\}$ then there exist a positive multiple of d, say g_k', such that g_k' does *not* belong to S. However all multiples of d greater than g_k' belong to S. The problem is to find g_k'.)

This problem has also been referred to as the coin exchange problem: given coins (in unbounded supply) of denominations $a_1,a_2,\ldots,a_k$, determine the largest amount which cannot be formed by means of these coins. In the rest of this chapter the historical background of the problem is reviewed. Functions related to g_k, connections to other problems and a chronological account of the bounds obtained for g_k are given. This is followed by various preliminary results and observations used in known special case expressions for $g(a_1,a_2,\ldots,a_k)$, and related function, $n(a_1,a_2,\ldots,a_k)$, as

defined in 1.2, and in this work.

An algorithm for g_3 is presented in Chapter 2. This algorithm appears extendable to the computation of g_k for $k \geqslant 4$ and $N_j(a_1,...,a_k)$, where the latter function represents the smallest positive integer such that all the integers greater than or equal to it have at least j distinct representations. A proof of the algorithm is followed by corollaries demonstrating that the strongest previous result for g_3 and a complementary new result can be obtained directly after the first step of the algorithm.

In Chapter 3 the algorithm is used to develop a general formula for g_3. In the corollaries following the proof of the formula, its compatibility with the previously known special cases is demonstrated.

1.2 RELATED FUNCTIONS

When we allow only positive x_i's in (1.1.1) it is easy to see that the corresponding function for the solvability of (1.1.1) is

$$f_k = f(a_1,a_2,...,a_k) = g_k+a_1+a_2+...+a_k \ , \tag{1.1.2}$$

i.e., for $n = f_k$, (1.1.1) has no solution with positive x_i, and for all $n > f_k$ (1.1.1) has a solution.

Obviously, there are only finitely many non-representable integers. Let the number of positive integers with no representation with non-negative integer coefficients be $n_k = n(a_1,...,a_k)$.

P. Erdös and R. L. Graham have introduced an extremal function [10]:

$$g(k,t) = \max_{a_i} g(a_1,a_2,...,a_k) \ , \tag{1.1.3}$$

where the maximum is taken over all a_i satisfying

$$0<a_1<...<a_k \leqslant t, \ \ gcd(a_1,a_2,...,a_k)=1.$$

Besides f_k, n_k and $g(k,t)$ the following more general function $N_j(a_1,...,a_k)$ was introduced by J. B. Roberts [33]:

Let $d(a_1,...,a_k,n)$ denote the number of non-negative solutions of (1.1.1). Define $N_j(a_1,...,a_k)$ to be the smallest positive integer such that $d(a_1,...,a_k,n) \geqslant j$ for all $n \geqslant N_j(a_1,...,a_k)$. It is easy to see that

$$N_1(a_1,...,a_k)-1 = g_k \ .$$

1.3 CONNECTIONS TO OTHER PROBLEMS

Recently R. Sedgewick [38] has exhibited a direct relationship between Shellsort* and the Frobenius' problem which enabled him to derive a sequence of $O(\log N)$ increments for Shellsort, for which the worst case running time is $O(N^{4/3})$ — a new upperbound for Shellsort. The previous best-known upper bound for any sequence of $O(\log N)$ increments was $O(N^{3/2})$.

The problem of Frobenius is also closely connected to the so-called postage stamp problem, (see E. S. Selmer [41]), — given stamps (in sufficient supply) of k different integral denominations

$$1 = a_1 < a_2 < ... < a_k \ , \tag{1.1.4}$$

what is the greatest consecutive range of postal rates from one unit upwards that can be formed when at most h stamps are allowed? That is, given a set $A_k = \{a_1,...,a_k\}$ of integers satisfying (1.1.4), consider all linear combinations

$$\sum_{i=1}^{k} x_i a_i \quad \text{where} \quad x_i \geqslant 0, \ \sum_{i=1}^{k} x_i \leqslant h \tag{1.1.5}$$

and find the smallest integer $N_h(A_k)$ which is not represented by such a combination. G.

* Shellsort is an algorithm for sorting an arbitrary list of integers (see D. E. Knuth [23]).

Meures [29] (see also O. J. Rödseth [36]) showed that

$$N_h(A_k) = ha_k - g(a_k-a_{k-1},\ldots,a_k-a_2,a_k-a_1,a_k) - 1 \tag{1.1.6}$$

if $h \geqslant h_1$ when h_1 is large enough.

A. L. Dulmage and N. S. Mendelsohn [8] connected the Frobenius problem to primitive matrices and graph theory; so did B. R. Heap and M. S. Lynn [15]. N. S. Mendelsohn [28] states that the solution to Frobenius' problem yields information valuable in statistics (Markoff chains) and in the theory of non-negative matrices.

In [45], it is shown that Farey series of orders less than or equal to a_1 give very interesting "partitions" of the set of linearly independent a_3 relative to a_1,a_2 when $gcd(a_1,a_2) = 1$.

1.4 BOUNDS

For the simplest case of $k = 2$, the problem of Frobenius was solved by J. J. Sylvester [41] in 1884 giving

$$g_2 = (a_1-1)(a_2-1) - 1$$

Complexity of the general solution to this problem seems to increase very rapidly for larger k's, and therefore upper bounds for g_k are of great interest. The existence of such a bound is used for instance in work done on the density of the sum of two sets of integers (see H. Rohrbach [37], p. 211).

Let $[x]$ stand for the greatest integer $\leqslant x$. Schur [2] showed in 1935 that

$$g_k \leqslant S := (a_1-1)(a_k-1) - 1 \tag{1.1.7}$$

when

$$1 \leqslant a_1 < a_2 < \ldots < a_k \ .$$

Brauer [2] proved in 1940 that equality in (1.1.7) holds if

(1.1.8) $$a_2 \equiv a_3 \equiv \ldots \equiv a_{k-1} \equiv 0 \pmod{a_1}$$

and

(1.1.9) $$a_k \not\equiv 0 \pmod{p}$$

for any p, where p is a proper factor of a_1. This is equivalent to giving only a_1 and a_k and using Sylvester's formula for g_2. Brauer also showed that

(1.1.10) $$g_k \leqslant T := \sum_{i=2}^{k} \left(\frac{d_{i-1}}{d_i} - 1 \right) a_i - a_1$$

where $d_1 = a_1$, $d_i = gcd(a_1,\ldots,a_i)$ for $i = 2,\ldots,k$, and equality holds if and only if . .

$$\frac{a_j}{d_j} = \sum_{i=1}^{k-1} \frac{a_i y_{ji}}{d_{j-1}} \quad \text{for each } j = 3,\ldots,k$$

with $y_{ji} \geqslant 0$. If $g_k < T$ then $g_k \leqslant T - \min\{a_i \mid i = 1,\ldots,k\}$. Also $S \geqslant T$ and the equality holds if and only if (1.1.8) and (1.1.9) are satisfied.

In 1956 Roberts [33] showed when $gcd(a_1,\ldots,a_k) = 1$, that

$$g(m, m+a_1, \ldots, m+a_k) \leqslant P + mQ - 1$$

where

$$P = g_k + 1, \quad Q = \max_{n \in K} (x_{1n} + \ldots + x_{kn}) \ ,$$

$$g_k = g(a_1,\ldots,a_k), \quad \text{and}$$

K is the set of n such that

$$P \leqslant n \leqslant P+m-1$$

and $x_{1n},\ldots,x_{kn}$ is a non-negative solution of (1.1.1) with smallest sum of the coefficients. In particular

$$g(m,m+a_1,m+a_2) \leqslant m(a_2-2+[\frac{m}{a_2}]) + (a_1-1)(a_2-1) - 1$$

where $\left[\frac{m}{a_2}\right]$ represent the largest integer less than or equal to real number $\frac{m}{a_2}$,

$$0 < a_1 < a_2 \text{ with } gcd(a_1,a_2) = 1, \text{ and } m \geqslant 2 .$$

Hofmeister [18] in 1966 proved that

(1.1.11) $$g(a_1,a_2,\ldots,a_k) \leqslant \max_{0\leqslant n\leqslant a_1-1} \sum_{i=2}^{k} e_i^{(n)}a_i - a_1 ,$$

where $e_i^{(n)}$'s are defined as follows:

Suppose $a_3,\ldots,a_k$ can be written in the form

(1.1.12) $$a_{i+1} = \nu_i a_i - \sum_{k=1}^{i} \beta_k(i)a_k \quad \text{with } 2 \leqslant i \leqslant k-1 ,$$

where all $\nu_i \geqslant 2$ and all $\beta_k^{(i)} \geqslant 0$. Note that when $gcd(a_1,a_2) = 1$, $a_3,\ldots,a_k$ can be written in the form (1.1.12).

Also suppose

(1.1.13) $$\sum_{l=0}^{h-1}\sum_{j=h}^{N}\beta_{m+l}(m+j) \leqslant 1$$

with $2 \leqslant m < m+N \leqslant k-1$ and $1 \leqslant h \leqslant N$.

Let $c_1,\ldots,c_k$ be defined by $c_1 = 0$, $c_2 = 1$,

(1.1.14) $$c_{l+1} = \nu_l c_l - \sum_{k=1}^{l-1}\beta_k(l)c_k \quad \text{with} \quad 2 \leqslant l \leqslant k-1 .$$

Then it is not too hard to see — when (1.1.12) and (1.1.13) are satisfied — that

$$1 = c_2 < c_3 < \ldots < c_k .$$

Define

$$e_k^{(n)},\ e_{k-1}^{(n)},\ldots,e_2^{(n)}$$

by

$$0 \leqslant n - \sum_{l=j}^{k} e_l^{(n)}c_l < c_j \quad \text{with } 2 \leqslant j \leqslant k .$$

It follows that

(1.1.15) $$n = \sum_{l=2}^{n} e_l^{(n)}c_l .$$

(This is called the Euclidean representation of n relative to c_l's).

For $k = 3$, Hofmeister's result is

(1.1.16) $$g_3 \leqslant \left[\frac{a_1-1}{y_1}\right]a_3 - a_2 - a_1 + \max\left(x_1a_1, a_2\left(a_1 - \left[\frac{a_1-1}{y_1}\right]y_1\right)\right) .$$

where $a_3 = y_1a_2 - x_1a_1$ with $y_1 \geqslant 2$.

Lewin [24] proved in 1971 that

$$g_k < \left[\frac{1}{2}(a_k-2)^2\right] \quad \text{where } a_1 < a_2 < \ldots < a_k .$$

He improved it [25] to

$$g_k < \left[\frac{1}{2}(a_{k-1}-1)(a_k-2)\right] .$$

He also conjectured that in general for large enough a_k

$$g_k < \left[\frac{1}{k+1}(a_k-2)(a_k-k-1)\right] .$$

Erdös and Graham [10] proved also later in that year that

$$g_k \leqslant 2a_{k-1}\left[\frac{a_k}{k}\right] - a_k \quad \text{where } a_1 < a_2 < \ldots < a_k.$$

Vitek [46] proved in 1973 that

$$g_k < \left[\frac{1}{2}(a_2-1)(a_k-2)\right] \quad \text{where } a_1 < a_2 < \ldots < a_k.$$

In his next paper [47] he proved:

If $a_k \geqslant (k+1)(k-2)$ then

$$g_k < \frac{a_k^2}{k+1}.$$

In 1976 Selmer [39] showed that:

$$g_k \leqslant 2a_k\left[\frac{a_1}{k}\right] - a_1 \quad \text{where } k \leqslant a_1 < \ldots < a_k .$$

1.5 PRELIMINARIES

Before the exact bounds which have been found for special cases are considered, we summarize preliminary various results and observations which will be useful for our later work. Brauer and Shockley [5] had observed that if one of the basis elements, say a_k, has a representation by $a_1,\ldots,a_{k-1}$, then clearly a_k can be removed from the basis elements without altering the value of g_k, because every linear combination of $a_1,\ldots,a_k$ with non-negative coefficients can also be expressed as a linear combination of $a_1,\ldots,a_{k-1}$ with non-negative coefficients. If none of the basis elements has a representation by the other ones, then $a_1,\ldots,a_k$ are independent, and

(1.2.1) $$k \leqslant \min\{a_i \mid i = 1,\ldots,k\} .$$

To see this note that if $k \geqslant a_1 + 1$, when we assume $a_1 = \min\{a_i \mid i = 1,\ldots,k\}$ then there are at least a_1 elements in $\{a_2,\ldots,a_k\}$. Obviously either there is an $i \geqslant 2$ such that $a_i \equiv 0 \pmod{a_1}$ or $i,j \geqslant 2$ with $a_i \equiv a_j \pmod{a_1}$, in both cases giving dependence between the basis elements. Trivially if any $a_i = 1$ then $g_k = -1$. Also the re-indexing of $a_1,\ldots,a_k$ does not alter the value of g_k.

In case $k = 3$, the reduction formula of Johnson [21] is as follows: If for $\{i,j,k\} = \{1,2,3\}$, $d_{ij} = (a_i,a_j)$, $a_i = b_i d_{ij} d_{ik}$ so that $(b_1,b_2) = (b_2,b_3) = (b_3,b_1) = 1$, then

(1.2.2) $$f(a_1,a_2,a_3) = d_{12}d_{23}d_{31}f(b_1,b_2,b_3)$$

i.e.

$$g(a_1,a_2,a_3) = (d_{12}d_{23}d_{31})g\left(\frac{a_1}{d_{12}d_{31}}, \frac{a_2}{d_{12}d_{23}}, \frac{a_3}{d_{13}d_{23}}\right) + (d_{23}-1)a_1$$

$$+ (d_{13}-1)a_2 + (d_{12}-1)a_3 .$$

If $d = gcd(a_1,a_2)$ then from the proof of (1.2.2) one can see that

$$g(a_1,a_2,a_3) = dg\left(\frac{a_1}{d}, \frac{a_2}{d}, a_3\right) + (d-1)a_3 . \tag{1.2.3}$$

Therefore without loss of generality we may assume

$$gcd(a_1,a_2) = 1. \tag{1.2.4}$$

Brauer and Shockley [5] generalized this result. If $gcd(a_1,\ldots,a_{k-1}) = d$, then

$$f(a_1,\ldots,a_k) = df\left(\frac{a_1}{d},\ldots,\frac{a_{k-1}}{d},a_k\right),$$

i.e.,

$$g(a_1,\ldots,a_k) = d\cdot g\left(\frac{a_1}{d},\ldots,\frac{a_{k-1}}{d},a_k\right) + (d-1)a_k \tag{1.2.5}$$

Therefore without loss of generality we may assume

$$gcd(a_1,\ldots,a_{k-1}) = 1 . \tag{1.2.6}$$

Lemma 1. Let $gcd(a_1,a_2) = 1$. Then every positive integer a_3 not divisible by neither a_1 nor a_2 can be *uniquely* written either in the form

$$a_3 = x_1a_1+y_1a_2 \quad \text{with } 0 < y_1 < a_1,\ 0 < x_1 \tag{F1}$$

or in the form

(F2) $$a_3 = -x_1a_1+y_1a_2 \quad \text{with } 0 < y_1 < a_1, 0 < x_1 < a_2$$

Every multiple a_3 of a_1, can be uniquely written as

(F3) $$a_3 = x_1a_1+y_1a_2 \quad \text{with } y_1 = 0, x_1 = \frac{a_3}{a_1} > 0$$

and every multiple a_3 of a_2 can be uniquely written as

(F4) $$a_3 = x_1a_1+y_1a_2 \text{ with } 0 \leqslant y_1 < a_1 \text{ and } x_1 \geqslant 0 .$$

Proof. Because $gcd(a_1,a_2) = 1$ and $a_3 \not\equiv 0 \pmod{a_i}$ with $i = 1$ or 2, there exists a *unique* y such that

$$a_3 \equiv ya_2 \pmod{a_1} \text{ with } 0 < y < a_1 .$$

Thus

$$a_3 = ya_2+xa_1 .$$

If $x > 0$,

then by letting $x_1 = x$ and $y_1 = y$ we have the form (F1).

If $x < 0$, ($x \neq 0$ since $a_3 \not\equiv 0 \pmod{a_2}$)

then $-a_2 < x < 0$, because if $x \leqslant -a_2$ then $a_3 = ya_2+xa_1 < a_1a_2-a_2a_1 = 0$ and this contradicts the assumption that a_3 is a positive integer.

Thus by letting $x_1 = -x$, $y_1 = y$ we have the form (F2). Uniqueness of x_1 follows because of the uniqueness of y_1. Obviously (F3) holds and so does (F4) when

$$x_1 = \left[\frac{a_3}{a_1a_2}\right]a_2, \quad y_1 = \frac{a_3}{a_2} - \left[\frac{a_3}{a_1a_2}\right]a_1 .$$

(F1) through (F4) combined together show that given $gcd(a_1,a_2) = 1$, $a_3 > 0$ can be *uniquely* written as

(F) $$a_3 = x_1a_1+y_1a_2 \quad \text{with} \quad -a_2 < x_1 \quad \text{and} \quad 0 \leq y_1 < a_1$$

Similarly it can be shown that given $gcd(a_1,a_2) = 1$, $a_3 > 0$ can be *uniquely* written as

(F') $$a_3 = x_1'a_1+y_1'a_2 \quad \text{with} \quad 0 \leq x_1' < a_2 \quad \text{and} \quad -a_1 < y_1' .$$

(Also note that (F'1) and (F'2) would be

(F'1) $$a_3 = x_1'a_1+y_1'a_2 \quad \text{with} \quad 0 < x_1' < a_2, \quad 0 < y_1' ,$$

(F'2) $$a_3 = x_1'a_1-y_1'a_2 \quad \text{with} \quad 0 < x_1' < a_2, \quad 0 < y_1' < a_1 .)$$

Given $gcd(a_1,a_2) = 1$, let us define a *canonical representation* of $a_3 > 0$ relative to a_1,a_2 as the pair of integral coefficients (x_1,y_1) or (x_1',y_1') such that a_3 can be written in the form (F) or the form (F'). Let x_1,y_1 be called canonical coefficients. When $ia_3 = x_ia_1+y_ia_2$ to get the coefficient for ia_3 in the form (F2) from the form (F'2) we take $ia_3 = (x_i-a_2)a_1+(a_1+y_i)a_2$ and to get the coefficient for ia_3 in the form (F'2) from the form (F2) we take $ia_3 = (x_i+a_2)a_1+(y_i-a_1)a_2$.

Note that a_3 has the form (F1) or the form (F'1) if and only if a_3 is *dependent* on a_1,a_2, and a_3 has the form (F2) or the form (F'2) if and only if a_3 is *independent* of a_1,a_2. Thus, when a_1,a_2,a_3 are independent basis elements with $gcd(a_1,a_2) = 1$ then a_3 must take the form (F2), if the form (F) is used or must take the form (F'2) if the form (F') is used.

When the form (F2) is used note that

$$\text{if} \quad y_1 = 1 \quad \text{then} \quad a_3 = a_2-x_1a_1 \quad \text{i.e.,} \quad a_2 = a_3+x_1a_1$$

and

$$\text{if } x_1 = a_2-1 \text{ then } a_3 = y_1a_2-(a_2-1)a_1 \text{ i.e., } a_1 = a_3+(a_1-y_1)a_2$$

Similarly when the form (F'2) is used note that

$$\text{if } x_1' = 1 \text{ then } a_3 = a_1-y_1'a_2 \text{ i.e., } a_1 = a_3+y_1'a_2$$

and

$$\text{if } y_1' = a_1-1 \text{ then } a_3 = x_1'a_1-(a_1-1)a_2 \text{ i.e., } a_2 = a_3+(a_2-x_1')a_1$$

Thus in these four cases we do not have independent basis elements.

Therefore by the observation of Brauer and Shockley made in the first paragraph of the Preliminaries, we have proved:

Lemma 1'. When a_1,a_2,a_3 are *independent* basis elements with $gcd(a_1,a_2) = 1$ then

(1.2.7) $a_3 = y_1a_2-x_1a_1$ if the form (F) is used with

$$0 < x_1 < a_2-1 \text{ and } 1 < y_1 < a_1$$

or

$a_3 = x_1'a_1-y_1'a_2$ if the form (F') is used with

$$1 < x_1' < a_2 \text{ and } 0 < y_1' < a_1-1$$

The following lemma by Brauer and Shockley is a frequently used result. Assuming that a_1 is an arbitrary basis element we have:

Lemma 2. Let L be a complete system of residues $l \not\equiv 0 \pmod{a_1}$. For each $l \in L$, let t_l be the smallest positive integer $t_l(a_1,\ldots,a_k) := t_l \equiv l \pmod{a_1}$ with a representation by $a_2,\ldots,a_k$. Then

(1.2.8) $$g_k = \max_{l \in L} t_l - a_1 .$$

Proof. Let n be a positive integer. If $n \equiv 0 \pmod{a_1}$, then n has a representation by a_1 alone. If $n \equiv l \not\equiv 0 \pmod{a_1}$, then n has a representation by $a_1,a_2,\ldots,a_k$ if and only if $n \geqslant t_l$.

Note that (if we assume $0 < l < a_1$) the equation $t_l - sa_1 = x_1a_1+\ldots+x_ka_k$ has no solution for each $l \in L$ and $1 \leqslant s \leqslant \frac{t_l-l}{a_1}$. Furthermore these are the only equations of the form (1.1.1) that have no solution. This leads to Selmer's formula [39]:

(1.2.9) $$n_k = \frac{1}{a_1} \sum_{l \in L} t_l - \frac{a_1 - 1}{2}.$$

Rödseth [34] obtained a reduction formula for the function $n(a_1,\ldots,a_k)$ when $gcd(a_2,\ldots,a_k) = d$ which is similar to (1.2.5) as follows: if $d > 1$ is a common divisor of $a_2,\ldots,a_k$ then

(1.2.10) $$t_{dl} = dt_l' \quad \text{where } t_l' = t_l\left(a_1, \frac{a_2}{d}, \frac{a_3}{d}, \ldots, \frac{a_k}{d}\right).$$

This follows because there are non-negative integers y_i such that

$$dt_l' = d \sum_{i=2}^{k} \frac{a_i}{d} y_i = \sum_{i=2}^{k} a_i y_i$$

and, by the definition of t_l', the sum is the smallest integer dependent on $a_1,a_2, \cdots ,a_k$ and $\equiv dl \pmod{a_1}$. Similarly to (1.2.9) we have

(1.2.11) $$n_k' = n\left(a_1, \frac{a_2}{d}, \ldots, \frac{a_k}{d}\right) = \frac{1}{a_1} \sum_{l \in L} t_l' - \frac{a_1 - 1}{2} .$$

As l runs through a complete residue system modulo a_1 so does dl (note that $(d,a) = 1$ because $(a_1,\ldots,a_k) = 1$). Hence, by (1.2.9) and (1.2.10)

(1.2.12) $$n_k = \frac{1}{a_1} \sum_{l \in L} t_{dl} - \frac{a_1 - 1}{2} ,$$

and so if d is a positive common factor of $a_2,\ldots,a_k$ then

(1.2.13) $$n(a_1,\ldots,a_k) = dn\left(a_1, \frac{a_2}{d},\ldots,\frac{a_k}{d}\right) + \frac{1}{2}(a_1-1)(d-1) .$$

Clearly if the basis elements are independent, then $a_2,\ldots,a_k$ are all part of the minimal system $\{t_l\}$. For if a non-negative combination of (say) $a_2,\ldots,a_{k-1}$ is congruent to $a_k \pmod{a_1}$ but less than or equal to a_k, then a_k has a representation by $a_1,\ldots,a_{k-1}$ and is dependent on $a_1,\ldots,a_{k-1}$. When we choose the maximum number of possible basis elements $k = a_1 = \min a_i$, these elements will represent all the residue classes $(\mathrm{mod}\ a_1)$ and $\{a_2,\ldots,a_k\}$ constitute the complete residue system $\{t_l\}$. Hence in this case

(1.2.14) $$g(k,a_2,\ldots,a_k) = \max_{2 \leq i \leq k} a_i - k \qquad \text{and}$$

(1.2.15) $$n(k,a_2,\ldots,a_k) = \frac{1}{k} \sum_{i=2}^{k} a_i - \frac{k-1}{2}.$$

Thus we conclude that in order to compute g_k the problem can be reduced to the case where each subset of $k-1$ elements from the basis elements $a_1,\ldots,a_k$ (with $k < \min a_i$) is relatively prime (see (1.2.6)) and that the basis elements must be independent with all $a_i \geq 2$.

The following result by Johnson [20] is not used as much as Brauer and Shockley's Lemma 2. However it appears to be just as important a result and may lead to a better understanding of the problem.

Proposition 1. For $k \geq 2$, f_k is the maximum of the restricted set of numbers N satisfying

(1.2.16) $$N \neq \sum_{i=1}^{k} x_i a_i \quad \text{for any } x_i > 0 .$$

and

(1.2.17) $$N+a_i = \sum_{j=1}^{k} y_{ij} a_j \quad \text{with } y_{ij} > 0 \quad \text{for each } i = 1,\ldots,k.$$

In particular

$$N = (y_{11}-1)a_1+y_{12}a_2+\ldots+y_{1k}a_k, \; y_{1j} > 0 .$$

But by (1.2.16) $y_{11}-1 \leqslant 0$ so that $y_{11} = 1$ since $y_{11} > 0$. By symmetry we have:

For every N satisfying (1.2.16) and (1.2.17) there are representations of N for each $i = 1,2,\ldots k$ of the form

(1.2.18) $$N = \sum_{\substack{j=1 \\ i \neq j}}^{k} y_{ij} a_j, \quad y_{ij} > 0 ,$$

and f_k is the maximum such N.

Using the notation of Hofmeister (already presented in 1.4) his main result is as follows:

Let $a_1,\ldots,a_k$ are relatively prime positive integers satisfying (1.1.12), and (1.1.13). Furthermore, let $\{c_1,c_2,\ldots,c_k\}$ be positive integers constructed as in (1.1.14), then

(1.2.19) $$g(a_1,\ldots,a_k) = \min \max \sum_{i=2}^{k} e_i^{(n)} a_i - a_1 .$$

Where for any complete system, L, of residues modulo a_1, the minimum is taken over $l \in L$ and the maximum is taken over $n \equiv la_2^{-1} \pmod{a_1}$. Note that the bound (1.1.11) is derived from (1.2.19).

1.6 KNOWN RESULTS FOR $g(a_1,\ldots,a_k)$ AND $n(a_1,\ldots,a_k)$

(I) $k = 2$.

Clearly the minimal system $\{t_i\}$ is given by $a_2, 2a_2, \ldots, (a_1-1)a_2$, has $\max t_i = (a_1-1)a_2$, and so gives

$$g(a_1,a_2) = (a_1-1)(a_2-1) - 1$$

and

$$n(a_1,a_2) = \frac{1}{2}(a_1-1)(a_2-1) = \frac{1}{2}(g_2+1) .$$

(II) $k = 3$.

The complexity in this case seems to be due to the fact that g_3 depends on the divisors of a_1,a_2,a_3 and no explicit formula for g_3 was known up to now, except in special cases. In chapter III we present an explicit formula for $g(t-n,t-m,t)$, where (for large enough t) $0 < m < n$ and $gcd(t-n,t-m,t) = 1$.

Brauer [2] showed in the special case in which the basis elements are consecutive integers that

$$(1.3.1) \qquad f(t,t+1,t+2) = \left[\frac{t+6}{2}\right]t+2 = \begin{cases} \left[\frac{t^2+6t+4}{2}\right] & \text{for even } t , \\ \frac{(t+5)t}{2} + 2 & \text{for odd } t > 1 . \end{cases}$$

Roberts [32] stated without presenting a proof that for $z > 2$,

$$(1.3.2) \qquad g(t,t+1,t+z) = \begin{cases} \left[\frac{t+1}{z}\right]t+(z-3)t-1 & \text{when } t \equiv z-1 \pmod z \\ & \text{and } t \geq z^2-5z+3\,, \\ \left[\frac{t+1}{z}\right](t+z)+(z-3)t-1 & \text{when } t \not\equiv z-1 \pmod z \\ & \text{and } t \geq z^2-4z+2\,. \end{cases}$$

Roberts [33] also gives,

$$g(t,t+2,t+3) = t\left[1+\left[\frac{t}{3}\right]\right]+1$$

and for $2 \leq t \leq 16$

$$g(t,t+2,t+5) = t\left[3+\left[\frac{t}{5}\right]\right]+3$$

when $t = 5,8,10,13,14,15$ but not for $t = 2,3,4,6,7,9,11,12,16$.

Johnson [21] was the first author who developed an algorithm and a symmetric expression for $f(a_1,a_2,a_3)$, where a_1,a_2,a_3 are pairwise relatively prime, independent basis elements. He proved that for cyclic permutations of subscripts

$$L_i = x_{ji}+x_{ki}$$

$$f(a_1,a_2,a_3) = L_i a_i + \max(x_{kj}a_j, x_{jk}a_k)$$

where $L_i a_i$ is the first multiple of a_i that is dependent on a_j,a_k with positive coefficients. ($L_i > 1$ since the basis elements are independent.) x_{kj} is the a_j-canonical coefficient of $L_k a_k$ relative to a_i,a_j.

Brauer and Shockley [5] presented an algorithm for computing $f(a_1,a_2,a_3)$ when a_1,a_2,a_3 are independent basis elements with $a_1 < a_2 < a_3$, which need not be relatively prime in pairs. They

observed

(1.3.3) $$f(a_1,a_2,a_3) = max(x_1a_2+y_3a_3, x_3a_2+y_2a_3) ,$$

where (1) y_2a_3 is the first multiple of a_3 that is dependent on a_1,a_2 with positive coefficients, (2) x_2 is the a_2-canonical coefficient of y_2a_3 relative to a_1,a_2, (3) $y_1 < y_2$ is such that for any $0 < y < y_2$ the a_2-canonical coefficient of ya_3 is greater than the a_2-canonical coefficient of y_1a_3, (4) the a_2-canonical coefficient of y_1a_3 equals x_1, (5) $x_3 = x_1-x_2$ and $y_3 = y_2-y_1$. (Brauer and Shockley looked at the congruence

(1.3.4) $$a_2x-a_3y \equiv 0 \pmod{a_1}$$

First we determine the solution (x_1,y_1) of (1.3.4) with smallest $x > 0$ so that $a_2x-a_3y > 0$ holds. Then we determine the solution (x_2,y_2) of (1.3.4) with smallest $y > 0$ so that $a_2x-a_3y < 0$. Let $x_3 = x_1-x_2$, $y_3 = y_2-y_1$.)

Using (1.3.3),

(1.3.5) $$f(a_1,a_2,a_3) = \max\left\{a_2\left[\frac{a_1a_3}{a_2+a_3}\right]+a_2+a_3,\ a_3\left[\frac{a_1a_2}{a_2+a_3}\right]+a_2+a_3\right\}$$

is obtained when $a_2 \equiv -a_3 \pmod{a_1}$ with a_1,a_2,a_3 relatively prime in pairs.

The strongest result given so far for $k = 3$ was proved by Hofmeister [18] (bis Folgerung 2, p. 20): Given a_1,a_2,a_3 with $gcd(a_1,a_2) = 1$ and

$$a_3 = y_1a_2-x_1a_1 \quad \text{with } 2 \leqslant y_1 < a_1 ,$$
$$a_1 = \alpha_1y_1+y_2 \quad \text{with } 0 \leqslant y_2 < y_1,$$

if $a_2 \geqslant x_1(\alpha_1+1)$ then

(1.3.6) $$g(a_1,a_2,a_3) = \alpha_1a_3-a_2-a_1+\max\{x_1a_1, y_2a_2\} .$$

In particular the value of $g(t,t+y,t+yz)$ could be determined using (1.3.6) for $z \geqslant 0$, y any integer, $a_1 = t$, $a_2 = t+y$, $a_3 = za_2-(z-1)a_1$ and when

$$t \geqslant (z-1)\cdot\left(\left[\frac{t}{z}\right]+1\right) - y\ .$$

An expression for $g(t,t+y,t+yz)$ will be given in Chapter 3, Corollary 6.

Hofmeister showed that all known formulas for $k = 3$ prior to his paper can be deduced from (1.3.6). Some results published after his paper can also be deduced from (1.3.6). For example, the first theorem of Byrnes [6] is an immediate consequence of (1.3.6). In fact Byrnes' conditions are overly restrictive since $a_2 \equiv 1$, $a_3 \equiv y_1 \pmod{a_1}$ can be replaced by the weaker condition $a_3 \equiv y_1a_2 \pmod{a_1}$. Under certain conditions, Lewin [27] gave formulas for $g(a_1,a_2,\ldots,a_k)$ and $n(a_1,\ldots,a_k)$ when $a_1,a_2,\ldots,a_k$ form an "almost arithmetic sequence," that is a sequence in which all but one of the basis elements form an ordinary arithmetic sequence. When $k = 3$, a_1,a_2,a_3 always form an almost arithmetic sequence, and Lewin's conditions shows that his formulas cover two types of cases: 1) After removing common factor, as in (1.2.2), we only get two independent basis elements or 2) by proper choice of a_1,a_2,a_3, Hofmeister's condition ($a_2 \geqslant x_1(a_1+1)$) is satisfied.

Equation (1.3.6) will be explained in terms of to the algorithm presented in Chapter 2 (Corollary 1). Furthermore the following complementing result will be proved (Corollary 2).

Let $(a_1,a_2) = 1$. Since a_3 is linearly independent of $\{a_1,a_2\}$ we can write

$$a_3 = y_1a_2-x_1a_1 \quad \text{where } 2 \leqslant y_1 < a_1 \quad \text{and } 0 < x_1 < a_2\ .$$

Also let

$$a_2 = \delta_1(a_2-x_1) + x_2 \quad \text{where } 0 \leqslant x_2 < (a_2-x_1)\ .$$

If $a_1 \geqslant (\delta_1+1)(a_2-x_1)$ then

(1.3.7) $$g_3 = \delta_1 a_3 - a_2 - a_1 + \max\{(a_1 - y_1)a_2, x_2 a_1\} .$$

Expressions (1.3.6) and (1.3.7) are found after the "first step" of the algorithm given in Chapter 2. Similar formulas could be found after any "step" of the algorithm.

Selmer [39] gave a direct and simple proof for (1.3.6) using the following table for the minimal system $\{t_i\}$ of Lemma 2:

(1.3.8)
$$\begin{cases} a_2 & 2a_2 & \cdots\cdots & (y_1-1)a_2 \\ a_3 & a_2+a_3 & 2a_2+a_3 & \cdots\cdots & (y_1-1)a_2+a_3 \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ (\alpha_1-1)a_3 & a_2+(\alpha_1-1)a_3 & 2a_2+(\alpha_1-1)a_3 & \cdots\cdots & (y_1-1)a_2+(\alpha_1-1)a_3 \\ \alpha_1 a_3 & a_2+\alpha_1 a_3 & 2a_2+\alpha_1 a_3 \ldots\ldots & (y_2-1)a_2+\alpha_1 a_3 & \end{cases}$$

and noticing that $\max\{t_i\}$ must occur at the two lower right corners. Summing over the diagram and using (1.2.9)

$$n(a_1,a_2,a_3) = n(a_1,a_2) - \frac{1}{2}\alpha_1 x_1 (a_1 - y_1 + y_2)$$

is found.

Selmer and Beyer [40] gave an algorithm using convergents of the (finite) simple continued fraction expansion of a_1/s, where s is determined by

$$a_3 \equiv \nu_{-1} a_2 \pmod{a_1} \quad \text{with} \quad 1 < \nu_{-1} < a_1 .$$

Furthermore if

$$r_{-2} = a_1 = q_0 r_{-1} + \gamma_0 \qquad 0 < \gamma_0 < s ,$$

$$r_{-1} = q_1 \gamma_0 + \gamma_1 \qquad 0 < \gamma_1 < \gamma_0 ,$$

$$\gamma_0 = q_2 \gamma_1 + \gamma_2 \qquad 0 < \gamma_2 < \gamma_1 ,$$

$$\vdots$$

$$\gamma_n = q_{n+2} \gamma_{n+1} + \gamma_{n+2} \qquad 0 < \gamma_{n+2} < \gamma_{n+1} ,$$

$$\vdots$$

with $\frac{\gamma_{2n+1}}{P_{2n+1}} < \frac{a_3}{a_2} < \frac{\gamma_{2n-1}}{P_{2n-1}}$ where $P_0 = q_0$, $P_1 = q_0 q_1 + 1, \ldots, P_n = P_{n-1} q_n + P_{n-2}$, then

$$g(a_1, a_2, a_3) = -a_1 + (\gamma_{2n} - 1) a_2 + (P_{2n} - 1) a_3$$

$$+ M\{(\gamma_{2n-1} - (i+1)\gamma_{2n}) a_2, (P_{2n-1} + jP_{2n}) a_3\}$$

$$i, j = 0, 1, \ldots q_{2n+1} - 1 .$$

The function

$$M(x_1, x_2, \ldots, x_{2m}) = x_{i_{m+1}} \text{ if } x_{i1} \leq x_{i2} \leq \ldots \leq x_{i2m}$$

i.e., we arrange the arguments after magnitude and select the smallest number in the upper half. They assert that when $a_1 = F_{2n+1} F_{2n+2} + F_{2n+3}$, $a_2 = a_1 + F_{2n+1}$, $a_3 = a_2 + 1$, $\{a_1, a_2, a_3\}$ are independent basis elements satisfying

$$a_1 < a_2 < a_3$$

and

$$\frac{\gamma_{2n+1}}{P_{2n+1}} < \frac{a_3}{a_2} < \frac{\gamma_{2n-1}}{P_{2n-1}}$$

where $F_i = F_{i-1}+F_{i-2}$ for $i \geq 2$ with $F_0 = 0$, $F_1 = 1$ are the Fibonacci numbers.

Rödseth [34] improved this algorithm and found simpler formulas for g_3 and n_3 using another continued fraction expansion of a_1/y_1 (with negative remainders). The Euclidean algorithm is used in the following form:

(1.3.9)
$$\begin{cases} a_1 = y_0 = q_1 y_1 - y_2, & 0 < y_2 < y_1; \\ y_1 = q_2 y_2 - y_3, & 0 < y_3 < y_2; \\ y_2 = q_3 y_3 - y_4, & 0 < y_4 < y_3; \\ \quad \cdots \\ y_{m-1} = q_m y_m - y_{m+1}, & 0 < y_{m+1} < y_m . \\ y_m = q_{m+1} y_{m+1}, \end{cases}$$

Integers P_i are defined by $P_{-1} = 0$, $P_0 = 1$ and

(1.3.10)
$$P_{i+1} = q_{i+1} P_i - P_{i-1} \quad \text{for } i = 0,1,\ldots,m.$$

Set $\frac{y_0}{P_{-1}} = \infty$ and regard any inequality $x < \infty$ (x real) as valid. Since $q_i \geq 2$, it follows by induction, using (1.3.10), that $P_{i+1} > P_i$. Hence

$$0 = \frac{y_{m+2}}{P_{m+1}} < \frac{y_{m+1}}{P_m} < \ldots < \frac{y_1}{P_0} < \frac{y_0}{P_{-1}} = \infty ,$$

and for a nonnegative real y there is a unique integer $\nu = \nu(y)$, $-1 \leq \nu \leq m$, satisfying

$$\frac{y_{\nu+2}}{P_{\nu+1}} \leq y < \frac{y_{\nu+1}}{P_\nu} .$$

When $y = \frac{a_3}{a_2}$, $gcd(a_1,a_2) = 1$ and ν is determined by the above inequality then

$$g(a_1,a_2,a_3) = -a_1+a_2(y_{r+1}-1)+a_3(P_{r+1}-1)-\min\{a_2y_{r+2},a_3P_r\}$$

and

$$n(a_1,a_2,a_3) = \frac{1}{2}\{1-a_1+a_2(y_{r+1}-y_{r+2}-1)+a_3(P_{r+1}-1)$$

$$+ y_{r+2}(P_{r+1}-P_r)\cdot\frac{(a_2y_{r+1}-a_3P_r)}{a_1}\}$$

(III) Arithmetic Progression.

Brauer [2] was the first to give explicit expression for $f(a_1,\ldots,a_k)$ where the a_i are k consecutive positive integers:

$$f(a,a+1,\ldots,a+k-1) = [\frac{a+k^2-3}{k-1}]a + \frac{k^2-k-2}{2}.$$

When the basis elements form an arithmetic progression

(1.3.11) $$a_i = a+(i-1)d$$

where $d > 0$ with $gcd(a,d) = 1$ and $1 \leq i \leq a$ as in (1.2.1) then we have (for $k \leq a$):

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

The result (1.3.12) was first given by Robert [32] with a complicated proof. Simpler proofs were later presented by Bateman [1], Brauer [3], Lewin [27], Selmer [39] and Rödseth [35]. Selmer uses the following diagram for the minimal system $\{t_i\}$ when $a-1 = \alpha(k-1)+\beta$ with $0 \leq \beta < k-1$.

$$(1.3.13)\qquad \begin{cases} a_2 & a_3 & \ldots\ldots & a_{k-1} & a_k \\ a_2+a_k & a_3+a_k & \ldots\ldots & a_{k-1}+a_k & 2a_k \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ a_2+(\alpha-1)a_k & a_3+(\alpha-1)a_k & \ldots\ldots & a_{k-1}+(\alpha-1)a_k & \alpha a_k \\ a_2+\alpha a_k & a_3+\alpha a_k & \ldots\ a_{\beta+1}+\alpha a_k & & \end{cases}$$

The last line occurs only for $\beta > 0$. In that case

$$g_k = \max t_i - a_1 = a_{\beta+1}+\alpha a_k - a_1 = \alpha a+(a-1)d\ .$$

When $\beta = 0$, we get

$$g_k = \alpha a_k - a_1 = (\alpha-1)a+(a-1)d\ ,$$

and both cases together give (1.3.12). Furthermore applying (1.2.9) to the system (1.3.13), a straightforward calculation gives:

$$(1.3.14)\qquad n(a,a+d,\ldots,a+(k-1)d) = \frac{1}{2}((a-1)(a+d)+\beta(a+1))\ ,$$

a result due to Grant [13]. The case $d = 1$ was first given by Nijenhuis and Wilf [31]. Lewin [27] showed that when $0 < k \leqslant 8$, (1.3.14) takes a simpler form

$$(1.3.15)\qquad n_k = <\frac{(a-1)(a+(k-1)d-1)}{2\cdot(k-1)}>$$

where $<x>$ denotes the least integer $\geqslant x$.

Nijenhuis and Wilf [31] proved

$$(1.3.16)\qquad \frac{n_k}{g_k} > \frac{1}{2}.$$

They based their proof on the simple observation that if x and y are positive integers with

$x+y = g_k$, then at most one of x and y can have a representation by $a_1,\ldots,a_k$ leading them to

$$n(a_1,\ldots,a_k) \geqslant \frac{1}{2}(g(a_1,\ldots,a_k)+1) . \tag{1.3.17}$$

Also, it is clear that

$$\frac{n_k}{g_k} \leqslant 1 . \tag{1.3.18}$$

In fact when $a_1 = k > 1$, $a_2 = k+1,\ldots,a_k = 2k-1$ then $a_1,\ldots,a_k$ are independent basis elements and all numbers $\geqslant k$ have representations. However no number $< k$ has a representation. Hence $n_k = g_k = k-1$. Furthermore as pointed out in Selmer [39], this case is the only possible case (with independent basis elements) in which $n_k = g_k$.

Note that when $a_1 = k$, $a_2 = k+d,\ldots,a_k = k+(k-1)d$, (1.3.12) is simply

$$g_k = (k-1)d$$

and (1.3.14) is

$$n_k = \frac{1}{2}(k-1)(d+1)$$

and

$$\frac{n_k}{g_k} = \frac{1}{2}\left(\frac{d+1}{d}\right) .$$

(IV) Almost Arithmetic Progression.

Lewin [27] introduced the almost arithmetic sequences. A sequence of distinct, relatively prime, positive integers is called an *admissible* sequence. An admissible, almost arithmetic progression is an admissible sequence where all but one of the basis elements form an arithmetic progression.

In the following let $p,a_0,\ldots,a_k$ be an admissible, almost arithmetic progression with

$$a_i = a_0 + id$$

for $i = 1,\ldots,k$.

As in (1.3.15), let $<x>$ denote the least integer $\geqslant x$.

If $p = a_0-\gamma d$, $1 < \gamma \leqslant k+1$, $a_0 \not\equiv d \pmod p$, then

$$g(p,a_0,\ldots,a_k) = <\frac{p-k-1}{k+\gamma}>p + (p+\gamma-1)d \ . \tag{1.3.19}$$

If $a_0 \equiv d \pmod p$, then, since obviously $(p,d) = 1$,

$$g(p,a_0,\ldots,a_k) = (a_0-d) + <\frac{p-1}{k+1}> + (p-1)[\min(a_0,d)-1] - 1 \ . \tag{1.3.20}$$

Letting $p = a_0-d$, Roberts' result (1.3.12) is obtained as a special case. Furthermore,

$$n(p,a_0,\ldots,a_k) = \frac{1}{2p}\left(\left[\frac{p-1}{k+1}\right]+1\right)(a_0-d)\left(<2(p-1)-(k+1)\left[\frac{p-1}{k+1}\right]>\right) \tag{1.3.21}$$

$$+ \frac{1}{2}(p-1)[\min(a_0,d)-1] \ .$$

Expression (1.3.14) follows when $a,a+d,\ldots,a+(k-1)d$ is an admissible arithmetic progression.

If $a_0 \equiv t\ d \pmod p$ for some t, $1 < t \leqslant k+1$, $t < p$ with $a_0 \geqslant t\ d$ then

$$g(p,a_0,\ldots,a_k) = (a_0-td)<\frac{p+t-1}{k+t}>+td+(p-1)(d-1)-1. \tag{1.3.22}$$

Also,

(1.3.23) $$n(p,a_0,\ldots,a_k) = \frac{1}{2}(p-1)(d-1)+(t-1)(d-h)-\frac{1}{2}i_0(i_0-1)(k+t)h$$

$$+i_0(p+t-1)h-\left(1+\left[\frac{p-1}{k+1}\right]\right)h,$$

where
$i_0 = <\frac{p+t-1}{k+t}>$, $h = \frac{a_0-t\,d}{p}$.

If $a_0 \equiv t\,d \pmod p$ for some t, $1 < t \leq k+1$, $t < p$, $a_0 < t\,d \leq a_0 < \frac{p}{t}>$ then

(1.3.24) $$g(p,a_0,\ldots,a_k) = \left(\left[\frac{p}{t}\right]+1\right)a_0-p-d+V$$

where

$$V = V(p,a_0,d,t) = \begin{cases} \max\{<td-a_0,\left(p-t\left[\frac{p}{d}\right]\right)>\} & \text{if } \gamma < t-1, \\ (t-1)d & \text{if } \gamma = t-1 \end{cases}$$

and $\gamma = p-t\cdot\left[\frac{p}{t}\right]$. Also

(1.3.25) $$n(p,a_0,\ldots,a_k) = \frac{1}{2}(p+\gamma)\gamma([\frac{p}{t}]+1)-[\frac{p}{t}]h+(t-1)d+\frac{1}{2}(p-1)(d-1)\,,$$

where

$$h = \frac{a_0-td}{p},\ \gamma = p-t\left[\frac{p}{t}\right].$$

When the almost arithmetic progression is of the form: $a_1 = a, a_2 = ha+d, a_3 = ha+2d, \ldots, a_k = ha+(k-1)d$ with $gcd(a,d) = 1$, $d > 0$, $h > 1$ and $k \leq a$

then Selmer showed (compare to (1.3.20) and (1.3.21)) that

$$(1.3.26) \qquad g(a,ha+d,ha+2d,\ldots,ha+(k-1)d) = \left(h\left[\frac{a-2}{k-1}\right]+h-1\right)a+(a-1)d$$

and

$$(1.3.27) \qquad n(a,ha+d,ha+2d,\ldots,ha+(k-1)d) = \frac{1}{2}((a-1)(h\alpha+d+h-1)+h\beta(\alpha+1))$$

where $a-1 = \alpha(k-1)+\beta$ as in (1.3.13).

Selmer also observes that the situation in (1.3.19) is only a special case of (1.3.22) when $a_0-td = a_0-\gamma d = p$ and furthermore, the conditions for (1.3.24) and (1.3.25) must be too weak since (1.3.24) gives the incorrect value 134 for $g(13,21,64) = 135$ as was noted by O. Beyer.

Rödseth in his recent paper [35] also deals with the almost arithmetic sequence

$a_i = a + id$ $(i = 0,..,k)$, $a_{k+1} = c$, where a,d,k,c are positive integers, $gcd(a,d) = 1$.

Let $y_0 = a$ and determine y_1 by $dy_1 \equiv c \pmod{y_0}$, $0 \leq y_1 < y_0$. Then using the notation that is used for (1.3.9), (1.3.10) etc. the following results are obtained.

$$(1.3.28) \qquad g(a,a+d,a+2d,\ldots,a+kd,c) =$$

$$d(y_{r+1}-1)+c(P_{r+1}-1) + \max\left\{a\left[\frac{y_{r+1}-y_{r+2}-2}{k}\right]-dy_{r+2},\ a\left[\frac{y_{r+1}-2}{k}\right]-cP_r\right\},$$

where $r = r(\frac{kc}{a+kd})$. (Note that since a_1,a_2,a_3 always form an almost arithmetic sequence his result in [34] is a special case of this one.) Alternatively if $y_0 = a+kd$ and y_1 is determined by $dy_1 \equiv -c \pmod{y_0}$, $0 \leq y_1 < y_0$, then

(1.3.29) $g(a,a+d,a+2d,\ldots,a+kd,c) =$

$$-d+c(P_{\nu+1}-1) + \max\left\{a\left[\frac{y_{\nu+1}-y_{\nu+2}-2}{k}\right]\right\},\left\{a\left[\frac{y_{\nu+1}-2}{k}\right] - cP_\nu\right\}, \text{ where}$$

$$\nu = \nu\left(\frac{kc}{a}\right).$$

To simplify the presentation for the corresponding results on n_k the following notation is used: For any integer x, define Σ_x by:

(1.3.30) $$\Sigma_x = \left[\frac{x-1}{k}\right]\left(x-1-\frac{k}{2}\left[\frac{x-1}{k}\right]-\frac{k}{2}\right) - 1 .$$

In particular

(1.3.31) $$\Sigma_x = \left[\frac{(x-1)(x-1-k)-1}{2k}\right] \quad \text{if } 1 \leqslant k \leqslant 7 .$$

Furthermore, let $a_0,a_1,\ldots,a_k,c$ be positive integers, where $a_i = a_0 + ie$, $i = 1,\ldots,k$, for some integer e (positive or negative) with $(a_0,e) = 1$; put $y_0 = a_0$, and determine y_1 by $ey_1 \equiv c \pmod{y_0}$, $0 \leqslant y_1 < y_0$. Then

(1.3.32) $$n(a_0,a_1,\ldots,a_k,c) = \frac{1}{2}\left\{1+a_0+e(y_{\nu+1}-y_{\nu+2}-1)+c(P_{\nu+1}-1)\right.$$

$$\left.+y_{\nu+2}(P_{\nu+1}-P_\nu)\cdot\frac{1}{a_0}(ey_{\nu+1}-cP_\nu)\right\}+(P_{\nu+1}-P_\nu)\Sigma_{y_{\nu+1}}+P_\nu\Sigma_{y_{\nu+1}-y_{\nu+2}},$$

$$\text{where } \nu = \nu\left(\frac{kc}{a_k}\right).$$

For $a_0 = a$, $e = d$ (1.3.32) corresponds to (1.3.28) and for $a_0 = a+kd$, $e = -d$ (1.3.32)

corresponds to (1.3.29). Taking $c = a$ in conditions for (1.3.28), we get $y_1 = 0$, $\nu = -1$ and (1.3.12) follows. Similarly (1.3.14) and (1.3.15) follow from (1.3.32).

Rödseth also gives Selmer's formulae (1.3.26) and (1.3.27). (1.3.27) is given in the following form:

$$n(a,ha+d,\ldots,ha+kd) = \frac{1}{2}(a-1)(d-1)+ha+h\Sigma_a .$$

Now let $c = a+Kd$, $k < K$, and put $a = \alpha K+\beta$, $0 \leqslant \beta < K$. Then if

(1.3.33) $$\beta = 0 \text{ or } \alpha+d \geqslant \left[\frac{K-\beta-1}{k}\right], \text{ we have}$$

(1.3.34) $$g(a,a+d,\ldots,a+kd,a+Kd) = (a+Kd)\alpha-d+\max\left\{a\left[\frac{\beta-2}{k}\right]+d\beta,\ a\left[\frac{K-2}{k}\right]-a\right\}.$$

For if $K < a$, using (1.3.28), we find that $y_1 = K$, and, by (1.3.33), $\nu = 0$, then (1.3.34) follows. If $a < K$, then, by (1.3.33), and by a lemma of Roberts' [30]:* $a+Kd$ is dependent on $a,\ldots,a+kd$, and (1.3.12) (when given as $g(a,a+d,\ldots,a+kd) = a\left[\frac{a-2}{k}\right] + d(a-1)$) shows that (1.3.34) is true also in this case.

If (1.3.33) is satisfied then (1.3.32) gives

(1.3.35) $$n(a,a+d,\ldots,a+kd,a+Kd) =$$

$$= \frac{1}{2}\{(\alpha+1)(a+\beta)+(a-1)(d-1)\}+\alpha\Sigma_K+\Sigma_\beta .$$

* (Let $a_0,\ldots,a_k$ be integers satisfying $a_i = a_0 + ie$, $i = 1,\ldots,k$, for some integer e. Then an integer n is dependent on $a_0,\ldots,a_k$ if and only if n has an integral representation $n = a_0 x + ey$ with $0 \leqslant y \leqslant kx$).

Let $c = a-Kd, a = \alpha K+\beta, 0 \leqslant \beta < K$ and suppose that

(1.3.36) $$\alpha > [\frac{\beta-1}{k}] + d.$$

Using (1.3.29) we find that $y_1 = k+K$, $\nu = 0$ and

(1.3.37) $$g(a,a+d,\ldots,a+kd,a-Kd) =$$

$$d(K-1) + \max\left\{a\left[\frac{K-y_2-2}{k}\right], a\left[\frac{K-2}{k}\right]-(a-Kd)\right\}+(a-Kd)q_1 .$$

By looking separately at the cases $\left[\frac{K-y_2-2}{k}\right] =$ and $< \left[\frac{K-2}{k}\right]$, we find that (1.3.37) may be written as

(1.3.38) $$g(a,a+d,\ldots,a+kd,a-Kd)=$$

$$d(K-1)+a[\frac{K-2}{k}]+(a-Kd)[\frac{a+kd+\zeta}{k+K}],$$

where ζ is determined by $\zeta \equiv K-2 (\mathrm{mod}\ k)$, $0 \leqslant \zeta < k$; that is, $\zeta = K-2-k[\frac{K-2}{k}]$. The formulae (1.3.34) and (1.3.38) were given by Siering [42], with a slightly different condition than (1.3.33) and with a more restrictive condition than (1.3.36). Selmer [39] gives (1.3.34) and (1.3.35) when $d = 1$.

Hofmeister [18] generalized Roberts' formula for arithmetic progression:

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

provided $d > (a-1)(l-1)a-2a$, where $l = \min\left\{k, \left[\frac{\log (a-1)}{\log a}\right]+2\right\}$. In case of $d = 1$ and

$t = 2$, Selmer [39] showed

(1.3.40) $$g(a,a+1,a+2,a+2^2,\ldots,a+2^k) =$$

$$(a+1)\left[\frac{a}{2^k}\right] + \sum_{i=0}^{k-1} 2^i \left[\frac{a+2^i}{2^k}\right] + (k-2)a - 1 ,$$

and showed that his method could be used to obtain (1.3.39) regardless of the magnitude of d.

CHAPTER II

2.1 INTRODUCTION TO AN ALGORITHM FOR $k = 3$

When $a_1 = t-n$, $a_2 = t-m$, $a_3 = t$ with $gcd(a_1,a_2,a_3) = 1$ none of the above algorithms seem to lead to an explicit formula for $g(a_1,a_2,a_3)$ in terms of n,m,t. The algorithm we present here leads to such a formula. We present this formula in the next chapter.

Because of Johnson's [20] reduction formula (1.2.3), and (1.2.7) in Chapter 1, the following assumptions can and will be made:

$(2A_1)$ $$gcd(a_1,a_2) = 1 \quad \text{with} \quad a_2 > a_1$$

$(2A_2)$ $$a_3 = y_1a_2 - x_1a_1 ,$$

if (F) form is used with $0 < x_1 < a_2-1$, $1 < y_1 < a_1$, or

$$a_3 = x_1a_1 - y_1a_2 ,$$

if (F') form is used with $1 < x_1 < a_2$ and $0 < y_1 < a_1-1$. The following notation will be used: The algorithm has three cases. Superscripts a and d are used for cases 2 and 3 respectively

$(2N_0)$
$$\begin{cases} x_0^g = x_0^d = a_2, \; y_0^g = y_0^d = a_1 \\ x_1^g = x_1, \; y_1^g = y_1, \; l_0^g = 0, \; \gamma_0^g = 1, \; \alpha_1 = \left[\dfrac{y_0^g}{y_1^g}\right] \\ x_1^d = a_2 - x_1, \; y_1^d = a_1 - y_1, \; l_0^d = 1, \; \gamma_0^d = 0, \; \delta_1 = \left[\dfrac{x_0^g}{x_1^d}\right] \end{cases}$$

For $\alpha_1 > 1$ and $p \geq 0$ define the following terms recursively:

$$(2N_1)\qquad \begin{cases} x^q_{2p+2} = x^q_{2p} - \alpha_{2p+1} x^q_{2p+1}, \\ y^q_{2p+2} = y^q_{2p} - \alpha_{2p+1} y^q_{2p+1} \\ \text{where } \alpha_{2p+1} = \left[\dfrac{y^q_{2p}}{y^q_{2p+1}}\right] \text{ and} \\ y^q_{2p+2} \text{ is the remainder when } y^q_{2p} \text{ is divided by } y^q_{2p+1}\ . \\ l^q_{2p+1} = l^q_{2p} + \alpha_{2p+1}\gamma^q_{2p},\ \gamma^q_{2p+1} = \gamma^q_{2p}, \\ m^q_{2p+1} = \gamma^q_{2p+1} + l^q_{2p+1} = m^q_{2p} + \alpha_{2p+1}\gamma^q_{2p+1}\ . \end{cases}$$

For $\alpha_1 > 1$ and $p \geqslant 1$

$$(2N_2)\qquad \begin{cases} x^q_{2p+1} = x^q_{2p-1} - \delta_{2p} x^q_{2p} \\ y^q_{2p+1} = y^q_{2p-1} - \delta_{2p} y^q_{2p} \\ \text{where } \delta_{2p} = \left[\dfrac{x^q_{2p-1}}{x^q_{2p}}\right] \text{ and} \\ x^q_{2p+1} \text{ is the remainder when } x^q_{2p-1} \text{ is divided by } x^q_{2p} \\ l^q_{2p} = l^q_{2p-1},\ \gamma^q_{2p} = \gamma^q_{2p-1} + \delta_{2p} l^q_{2p}\ , \\ m^q_{2p} = \gamma^q_{2p} + l^q_{2p} = m^q_{2p-1} + \delta_{2p} l^q_{2p}\ . \end{cases}$$

For $\delta_1 > 1$ and $p \geqslant 0$

$$(2N_3)\qquad \begin{cases} x^q_{2p+2} = x^q_{2p} - \delta_{2p+1} x^q_{2p+1} \\ y^q_{2p+2} = y^q_{2p} - \delta_{2p+1} y^q_{2p+1} \\ \text{where } \delta_{2p+1} = \left[\dfrac{x^q_{2p}}{x^q_{2p+1}}\right] \text{ and} \\ x^q_{2p+2} \text{ is the remainder when } \gamma^q_{2p} \text{ is divided by } \gamma^q_{2p+1}\ . \\ l^q_{2p+1} = l^q_{2p},\ \gamma^q_{2p+1} = \gamma^q_{2p} + \delta_{2p+1} l^q_{2p}, \\ m^q_{2p+1} = l^q_{2p+1} + \gamma^q_{2p+1} = m^q_{2p} + \delta_{2p+1} l^q_{2p}\ . \end{cases}$$

For $\delta_1 > 1$ and $p > 0$

$$(2N_4)\qquad \begin{cases} x^{q}_{2\rho+1} = x^{q}_{2\rho-1} - \alpha_{2\rho} x^{q}_{2\rho}, \\ y^{q}_{2\rho+1} = y^{q}_{2\rho-1} - \alpha_{2\rho} y^{q}_{2\rho} \\ \text{where } \alpha_{2\rho} = \left[\dfrac{y^{q}_{2\rho-1}}{y^{q}_{2\rho}}\right] \text{ and} \\ y^{q}_{2\rho+1} \text{ is the remainder when } y^{q}_{2\rho-1} \text{ is divided by } y^{q}_{2\rho}\,. \\ l^{q}_{2\rho} = l^{q}_{2\rho-1} + \alpha_{2\rho}\gamma^{q}_{2\rho-1},\ \gamma^{q}_{2\rho} = \gamma^{q}_{2\rho-1}, \\ m^{q}_{2\rho} = l^{q}_{2\rho} + \gamma^{q}_{2\rho} = m^{q}_{2\rho-1} + \alpha_{2\rho}\gamma^{q}_{2\rho-1}\,. \end{cases}$$

2.2 AN ALGORITHM

The algorithm is divided into three mutually exclusive cases.

Case 1. $\alpha_1 = \delta_1 = 1$.

Case 2. $\alpha_1 > 1, \delta_1 = 1$.

Case 3. $\delta_1 > 1, \alpha_1 = 1$.

If $\alpha_1 > 1$ then because of $(2N_0)$, $y_1 \leqslant \dfrac{a_1}{2}$.

Suppose $x_1 \geqslant \dfrac{a_2}{2}$ then

$$a_3 = y_1 a_2 - x_1 a_1 \leqslant \frac{a_1 a_2}{2} - \frac{a_1 a_2}{2} = 0$$

contradicting $a_3 > 0$.

Therefore,

$$0 < x_1 < \frac{a_2}{2}$$

and,

$$a_2 > a_2 - x_1 > \frac{a_2}{2}$$

and,

$$\delta_1 = 1 ,$$

because of $(2N_0)$.

Similarly when $\delta_1 > 1$, $\alpha_1 = 1$.

In case 1. $(\alpha_1 = \delta_1 = 1)$

$$g(a_1,a_2,a_3) = a_3 + \max\{x_1 a_1, (a_1 - y_1)a_2\} - a_1 - a_2 .$$

In case 2. $(\alpha_1 > 1, \delta_1 = 1)$

Simultaneously the Euclidean algorithms for $a_1 | y_1^{\alpha}$ and for $x_1^{\alpha} | x_2^{\alpha}$ are used until either (1) x_{2p}^{α} is not a remainder (i.e. $x_{2p}^{\alpha} \geqslant x_{2p-1}^{\alpha}$) or y_{2p}^{α} is the zero remainder or (2) y_{2p+1}^{α} is not a remainder (i.e. $y_{2p+1}^{\alpha} \geqslant y_{2p}^{\alpha}$) or x_{2p+1}^{α} is the zero remainder for some $p > 0$.

If (1) let $x^{\alpha} = x_{2p-1}^{\alpha}$, $y^{\alpha} = y_{2p}^{\alpha}$, $m^{\alpha} = m_{2p-1}^{\alpha}$,

If (2) let $x^{\alpha} = x_{2p+1}^{\alpha}$, $y^{\alpha} = y_{2p}^{\alpha}$, $m^{\alpha} = m_{2p}^{\alpha}$,

$$g_3 = (m^{\alpha} - 1)a_3 + \max\{x^{\alpha} a_1, y^{\alpha} a_2\} - a_1 - a_2 .$$

See diagram 1.

Diagram 1

Step 1.

$$\alpha_1 = \left[\frac{y_0^q}{y_1^q}\right]$$

$$y_2^q = a_1 - \alpha_1 y_1^q$$

$$x_2^q = a_2 - \alpha_1 x_1^q$$

If $x_2^q \geq x_1^q$ or $y_2^q = 0$.

The algorithm ends with

$x^e = x_1^q$, $y^e = y_2^q$

$m^e = m_1^q$

If $x_2^q < x_1^q$. Step 2.

$$\delta_2 = \left[\frac{x_1^q}{x_2^q}\right]$$

$$x_3^q = x_1^q - \delta_2 x_2^q$$

$$y_3^q = y_1^q - \delta_2 y_2^q.$$

If $y_3^q \geq y_2^q$ or $x_3^q = 0$

The algorithm ends with

$x^e = x_3^q$, $y^e = y_2^q$

$m^e = m_2^q$

If $y_3^q < y_2^q$. Step 3.

$$\alpha_3 = \left[\frac{y_2^q}{y_3^q}\right]$$

$$y_4^q = y_2^q - \alpha_3 y_3^q$$

$$x_4^q = x_2^q - \alpha_3 x_3^q$$

⋮

If $x_{2p}^q \geq x_{2p-1}^q$ or $y_{2p}^q = 0$

The algorithm ends with

$x^e = x_{2p-1}^q$, $y^e = y_{2p}^q$

$m^e = m_{2p-1}^q$

If $x_{2p}^q < x_{2p-1}^q$. Step 2p.

$$\delta_{2p} = \left[\frac{x_{2p-1}^q}{x_{2p}^q}\right]$$

$$x_{2p+1}^q = x_{2p-1}^q - \delta_{2p} x_{2p}^q$$

$$y_{2p+1}^q = y_{2p-1}^q - \delta_{2p} y_{2p}^q$$

If $y_{2p+1}^q \geq y_{2p}^q$ or $x_{2p+1}^q = 0$

The algorithm ends with

$x^e = x_{2p+1}^q$, $y^e = y_{2p}^q$

$m^e = m_{2p}^q$

If $y_{2p+1}^q < y_{2p}^q$. Step 2p+1.

$$\alpha_{2p+1} = \left[\frac{y_{2p}^q}{y_{2p+1}^q}\right]$$

$$y_{2p+2}^q = y_{2p}^q - \alpha_{2p+1} y_{2p+1}^q$$

$$x_{2p+2}^q = x_{2p}^q - \alpha_{2p+1} x_{2p+1}^q .$$

⋮

In case 3. $(\delta_1 > 1, \alpha_1 = 1)$

Simultaneously the Euclidean algorithms for $a_2|x_1^q$ and $y_1^q|y_2^q$ are used until either (1) $y_{2\rho}^q$ is not a remainder (i.e. $y_{2\rho}^q \geqslant y_{2\rho-1}^q$) or $x_{2\rho}^q$ is the zero remainder or (2) $x_{2\rho+1}^q$ is not a remainder (i.e. $x_{2\rho+1}^q \geqslant x_{2\rho}^q$) or $y_{2\rho+1}^q$ is the zero remainder.

If (1) let $x^d = x_{2\rho}^q$, $y^d = y_{2\rho-1}^q$, $m^d = m_{2\rho-1}^q$.

If (2) let $x^d = x_{2\rho}^q$, $y^d = y_{2\rho+1}^q$, $m^d = m_{2\rho}^q$.

$g_3 = (m^d-1)a_3+\max\{x^d a_1, y^d a_2\}-a_1-a_2$ see diagram 2 .

Diagram 2

Step 1.

$$\delta_1 = \left[\frac{x_0^q}{x_1^q}\right]$$

$$x_2^q = a_2 - \delta_1 x_1^q$$

$$y_2^q = a_1 - \delta_1 y_1^q$$

If $y_2^q \geqslant y_1^q$ or $x_2^q = 0$

The algorithm ends with

$x^d = x_2^q, y^d = y_1^q$

$m^d = m_1^q$

If $y_2^q < y_1^q$. Step 2.

$$\alpha_2 = \left[\frac{y_1^q}{y_2^q}\right]$$

$$y_3^q = y_1^q - \alpha_2 y_2^q$$

$$x_3^q = x_1^q - \alpha_2 x_2^q$$

If $x_3^q \geqslant x_2^q$ or $y_3^q = 0$

The algorithm ends with

$x^d = x_2^q, y^d = y_3^q$

$m^d = m_2^q$

If $x_3^q < x_2^q$. Step 3.

$$\delta_3 = \left[\frac{x_2^q}{x_3^q}\right]$$

$$x_4^q = x_2^q - \delta_3 x_3^q$$

$$y_4^q = y_2^q - \delta_3 y_3^q$$

⋮

If $y_{2p}^q \geqslant y_{2p-1}^q$ or $x_{2p}^q = 0$

The algorithm ends with

$x^d = x_{2p}^q, y^d = y_{2p-1}^q$

$m^d = m_{2p-1}^q$

If $y_{2p}^q < y_{2p-1}^q$. Step 2p.

$$\alpha_{2p} = \left[\frac{y_{2p-1}^q}{y_{2p}^q}\right]$$

$$y_{2p+1}^q = y_{2p-1}^q - \alpha_{2p} y_{2p}^q$$

$$x_{2p+1}^q = x_{2p-1}^q - \alpha_{2p} x_{2p}^q$$

If $x_{2p+1}^q \geqslant x_{2p}^q$ or $y_{2p+1}^q = 0$

The algorithm ends with

$x^d = x_{2p}^q, y^d = y_{2p+1}^q$

$m^d = m_{2p}^q$

If $x_{2p+1}^q < x_{2p}^q$. Step 2p+1.

$$\delta_{2p+1} = \left[\frac{x_{2p}^q}{x_{2p+1}^q}\right]$$

$$x_{2p+2}^q = x_{2p}^q - \delta_{2p+1} x_{2p+1}^q$$

$$y_{2p+2}^q = y_{2p}^q - \delta_{2p+1} y_{2p+1}^q$$

⋮

2.3 RESULTS FOR A PROOF OF THE ALGORITHM

First of all we observe that the algorithm terminates in a finite number of steps since the Euclidean algorithm for any two integers ends after a finite number of steps. When we have $x_p^e, y_p^e, x_p^f, y_p^f$ etc., we assume that at the $(p-1)$st step the algorithm has not ended.

The following results are used for the proof of the algorithm.

Lemma 3. For $p \geqslant 1$ if $x_{2p-1}^q > x_{2p}^q$ then

$$\begin{cases} a_2 = x_0^q > x_1^q > x_2^q \ldots > x_{2p-1}^q > x_{2p}^q > x_{2p+1}^q \geqslant 0 \\ a_1 = y_0^q > y_1^q > y_2^q \ldots > y_{2p-2}^q > y_{2p-1}^q > y_{2p}^q \geqslant 0 \end{cases} \tag{2.3.1}$$

For $p \geqslant 0$ if $y_{2p}^q > y_{2p+1}^q$ then

$$\begin{cases} a_2 = x_0^q > x_1^q > x_2^q > \ldots > x_{2p}^q > x_{2p+1}^q \geqslant 0 \\ a_1 = y_0^q > y_1^q > y_2^q > \ldots > y_{2p}^q > y_{2p+1}^q > y_{2p+2}^q \geqslant 0 \end{cases} \tag{2.3.2}$$

Similarly for $p \geqslant 1$ if $y_{2p-1}^q > y_{2p}^q$ then

$$\begin{cases} a_2 = x_0^q > x_1^q > x_2^q > \ldots > x_{2p-1}^q > x_{2p}^q \geqslant 0 \\ a_1 = y_0^q > y_1^q > y_2^q > \ldots > y_{2p}^q > y_{2p+1}^q \geqslant 0 \end{cases} \tag{2.3.3}$$

For $p \geqslant 0$ if $x_{2p}^q > x_{2p+1}^q$ then

$$\begin{cases} a_2 = x_0^q > x_1^q > x_2^q > \ldots > x_{2p}^q > x_{2p+1}^q > x_{2p+2}^q \geqslant 0 \\ a_1 = y_0^q > y_1^q > y_2^q > \ldots > y_{2p}^q > y_{2p+1}^q \geqslant 0 \end{cases} \tag{2.3.4}$$

Proof. The proof of lemma 3 is obvious when we note that at each particular inequality, the inequality holds either because of the conditions in the algorithm or because right-hand side of the inequality is a remainder.

Lemma 4. Let $a_1 > 1$ and $p > 0$. Then

(2.3.5) $$l^{\S}_{2p-1}a_3 = l^{\S}_{2p}a_3 = x^{\S}_{2p}a_1 - y^{\S}_{2p}a_2$$

(2.3.6) $$\gamma^{\S}_{2p-1}a_3 = y^{\S}_{2p-1}a_2 - x^{\S}_{2p-1}a_1$$

(2.3.7) $$\gamma^{\S}_{2p}a_3 = \gamma^{\S}_{2p+1}a_3 = y^{\S}_{2p+1}a_2 - x^{\S}_{2p+1}a_1$$

Therefore,

(2.3.8) $$m^{\S}_{2p-1}a_3 = (x^{\S}_{2p} - x^{\S}_{2p-1})a_1 + (y^{\S}_{2p-1} - y^{\S}_{2p})a_2$$

(2.3.9) $$m^{\S}_{2p}a_3 = (x^{\S}_{2p} - x^{\S}_{2p+1})a_1 + (y^{\S}_{2p+1} - y^{\S}_{2p})a_2$$

Similarly if $\delta_1 > 1$ and $p > 0$ then

(2.3.10) $$l^{\S}_{2p-1}a_3 = x^{\S}_{2p-1}a_1 - y^{\S}_{2p-1}a_2$$

(2.3.11) $$l^{\S}_{2p}a_3 = x^{\S}_{2p+1}a_1 - y^{\S}_{2p+1}a_2$$

(2.3.12) $$\gamma^{\S}_{2p-1}a_3 = \gamma^{\S}_{2p}a_3 = y^{\S}_{2p}a_2 - x^{\S}_{2p}a_1$$

Therefore,

(2.3.13) $$m^{\S}_{2p-1}a_3 = (x^{\S}_{2p-1} - x^{\S}_{2p})a_1 + (y^{\S}_{2p} - y^{\S}_{2p-1})a_2$$

(2.3.14) $$m^{\S}_{2p}a_3 = (x^{\S}_{2p+1} - x^{\S}_{2p})a_1 + (y^{\S}_{2p} - y^{\S}_{2p+1})a_2$$

Note: From now on γ_p, l_p, m_p, etc...will represent γ^e_p, l^e_p, m^e_p when $\alpha_1 > 1$ and will represent γ^d_p, l^d_p, m^d_p when $\delta_1 > 1$.

Proof. We use $(2N_1)$, $(2N_2)$ and induction on p when $\alpha_1 > 1$ and $p > 0$. For $p = 1$

$$l_1 \cdot a_3 = \alpha_1 a_3 = (\alpha_1 y^{\S}_1)a_2 - (\alpha_1 x^{\S}_1)a_1 = (\alpha_1 y^{\S}_1 - a_1)a_2 - (\alpha_1 x^{\S}_1 - a_2)a_1$$

$$= x^{\S}_1 a_1 - y^{\S}_1 a_2$$

$$\gamma_1 a_3 = a_3 = y^{\S}_1 a_2 - x^{\S}_1 a_1$$

$$l_2 a_3 = l_1 a_3 = x^{\S}_2 a_1 - y^{\S}_2 a_2$$

$$\gamma_2 a_3 = (\gamma_1 + \delta_2 l_1)a_3 = (y^{\S}_1 - \delta_2 y^{\S}_2)a_2 - (x^{\S}_1 - \delta_2 x^{\S}_2)a_1 = y^{\S}_2 a_2 - x^{\S}_2 a_1$$

Thus, the lemma is valid when $p = 1$.

Suppose the lemma is valid for $p = i$ where $i \geq 1$. Then for $p = i+1$

$$l_{2p-1}a_3 = l_{2l+1}\cdot a_3 = (l_{2l}+\alpha_{2l+1}\gamma_{2l})(a_3)$$

$$= (x^q_{2l}-\alpha_{2l+1}x^q_{2l+1})a_1-(y^q_{2l}-\alpha_{2l+1}y^q_{2l+1})a_2 \quad \text{because of (2.3.5) and (2.3.7)}$$

$$= x^q_{2l+2}a_1-y^q_{2l+2}a_2 \quad \text{because of } (2N_1)$$

$$= x^q_{2p}a_1-y^q_{2p}a_2$$

$$\gamma_{2p-1}a_3 = \gamma_{2l+1}a_3 = \gamma_{2l}a_3$$

$$= y^q_{2l+1}a_2-x^q_{2l+1}a_1$$

$$= y^q_{2p-1}a_2-x^q_{2p-1}a_1$$

and

$$l_{2p}a_3 = l_{2l+2}a_3 = l_{2l+1}a_3$$

$$= x^q_{2p}a_1-y^q_{2p}a_2$$

and

$$\gamma_{2p}a_3 = \gamma_{2l+2}a_3 = (\gamma_{2l+1}a_3+\delta_{2l+2}\cdot l_{2l+1}\cdot a_3)$$

$$= (y^q_{2l+1}-\lambda_{2l+2}\cdot y^q_{2l+2})a_2-(x^q_{2l+1}-\delta_{2l+2}x^q_{2l+2})a_1$$

$$= y^q_{2l+3}a_2-x^q_{2l+3}a_1$$

$$= y^q_{2p+1}a_2-x^q_{2p+1}a_1 .$$

Thus, the lemma is valid when $p = l+1$. The proof for when $\delta_1 > 1$ and $p > 0$ is similar.

Lemma 5. For $p \geq 1$ if $x^q_{2p-1} > x^q_{2p}$ then

(2.3.1') $\qquad y^q_{2p+1} > 0$

For $p \geq 0$ if $y^q_{2p} > y^q_{2p+1}$ then

(2.3.2') $\qquad x^q_{2p+2} > 0$

For $p \geq 1$ if $y^q_{2p-1} > y^q_{2p}$ then

(2.3.3') $\qquad x^q_{2p+1} > 0$

For $p \geq 0$ if $x^q_{2p} > x^q_{2p+1}$ then

(2.3.4') $$y^q_{2p+2} > 0$$

Proof. Suppose for $p \geq 1$, $x^q_{2p-1} > x^q_{2p}$. Then as defined in the algorithm $\delta_{2p} = \left[\frac{x^q_{2p-1}}{x^q_{2p}}\right]$.

Therefore,

$$x^q_{2p+1} = x^q_{2p-1} - \delta_{2p} x^q_{2p} \geq 0 .$$

If $y^q_{2p+1} \leq 0$ then as in Lemma 4

$$\gamma^q_{2p} a_3 = \gamma^q_{2p+1} a_3 = y^q_{2p+1} \cdot a_2 - x^q_{2p+1} a_1 \leq 0 .$$

This contradicts $a_3 > 0$ since $\gamma^q_{2p} > 0$ (because of $(2N_2)$). Therefore,

$$y^q_{2p+1} > 0 .$$

The rest of the proof is the same when for (2.3.2') we use α_{2p+1} and $l^q_{2p+1} \cdot a_3$, for (2.3.3') we use α_{2p} and $l^q_{2p} \cdot a_3$ and for (2.3.4') we use δ_{2p+1} and $\gamma^q_{2p+1} \cdot a_3$.

Lemma 6.

For $\alpha_1 > 1$ with $p > 0$

(2.3.15) $$(y^q_{2p-1})(m^q_{2p-1}) - (y^q_{2p-1} - y^q_{2p})(\gamma^q_{2p-1}) = a_1$$

(2.3.16) $$(y^q_{2p+1})(m^q_{2p}) - (y^q_{2p+1} - y^q_{2p})(\gamma^q_{2p}) = a_1 ,$$

and for $\delta_1 > 1$ with $p > 0$

(2.3.17) $$(y^q_{2p})(m^q_{2p-1}) - (y^q_{2p} - y^q_{2p-1})(\gamma^q_{2p-1}) = a_1$$

(2.3.18) $$(y^q_{2p})(m^q_{2p}) - (y^q_{2p} - y^q_{2p+1})(\gamma^q_{2p}) = a_1$$

Proof. We use $(2N_1)$, $(2N_2)$, lemma 4 and induction on p when $\alpha_1 > 1$ with $p > 0$.

For $p = 1$,

we note that $\gamma_1^q = 1$, $m_1^q = a_1+1$.

Therefore

$$(y_1^q)(m_1^q) - (y_1^q - y_2^q)(\gamma_1^q)$$

$$= y_1^q a_1 + y_2^q$$

$$= a_1 \text{ by the definition of } y_2^q .$$

Thus, (2.3.15) is true when $p = 1$.

Suppose for *odd* i (2.3.15) holds. That is suppose,

$$(y_1^q)(m_i^q) - (y_i^q - y_{i+1}^q)(\gamma_i^q) = a_1 . \tag{1}$$

Then

$$(y_{i+2}^q)(m_{i+1}^q) - (y_{i+2}^q - y_{i+1}^q)(\gamma_{i+1}^q)$$

$$= (y_{i+2}^q)(m_i^q + \delta_{i+1} l_{i+1}^q) - (y_{i+2}^q - y_{i+1}^q)(\gamma_i^q + \delta_{i+1} l_{i+1}^q)$$

by the definitions of m_{i+1}^q, γ_{i+1}^q in $(2N_2)$

$$= (y_i^q - \delta_{i+1} y_{i+1}^q)(l_{i+1}^q) + (y_{i+1}^q)(\gamma_i^q + \delta_{i+1} l_{i+1}^q)$$

because of the definition of y_{i+2}^q and $l_i^q = l_{i+1}^q = m_i^q - \gamma_i^q$

$$= (y_i^q)(m_i^q) - (y_i^q - y_{i+1}^q)(\gamma_i^q) = a_1 \quad \text{because of (1)}$$

Thus (2.3.16) holds, when (2.3.15) is valid.

Next, suppose for *even* i (2.3.16) holds. That is suppose

$$(y_{i+1}^q)(m_i^q) - (y_{i+1}^q - y_i^q)(\gamma_i^q) = a_1 . \tag{2}$$

Then

$$(y^{\varrho}_{l+1})(m^{\varrho}_{l+1}) - (y^{\varrho}_{l+1}-y^{\varrho}_{l+2})(\gamma^{\varrho}_{l+1})$$

$$= (y^{\varrho}_{l+1})(m^{\varrho}_{l}) + (a_{l+1}y^{\varrho}_{l+1}+y^{\varrho}_{l+2}-y^{\varrho}_{l+1})(\gamma^{\varrho}_{l})$$

by the definitions of m^{ϱ}_{l+1}, γ^{ϱ}_{l+1} in $(2N_1)$

$$= (y^{\varrho}_{l+1})(m^{\varrho}_{l})-(y^{\varrho}_{l+1}-y^{\varrho}_{l})(\gamma^{\varrho}_{l})$$

by the definition of y^{ϱ}_{l+2} .

$$= a_1$$ because of (2) .

Thus (2.3.15) holds when (2.3.16) is valid. Thus (2.3.15) and (2.3.16) are valid. We can prove (2.3.17) and (2.3.18) using $(2N_3)$, $(2N_4)$ and induction on p when $\delta_1 > 1$ and $p > 0$. Similarly we can prove the following lemma.

Lemma 7.

For $\alpha_1 > 1$ with $p > 0$

(2.3.19) $$(x^{q}_{2p})(m^{q}_{2p-1}) - (x^{q}_{2p}-x^{q}_{2p-1})(l^{q}_{2p-1}) = a_2$$

(2.3.20) $$(x^{q}_{2p})(m^{q}_{2p}) - (x^{q}_{2p}-x^{q}_{2p+1})(l^{q}_{2p}) = a_2$$

and for $\delta_1 > 1$ with $p > 0$

(2.3.21) $$(x^{q}_{2p-1})(m^{q}_{2p-1}) - (x^{q}_{2p-1}-x^{q}_{2p})(l^{q}_{2p-1}) = a_2$$

(2.3.22) $$(x^{q}_{2p+1})(m^{q}_{2p}) - (x^{q}_{2p+1}-x^{q}_{2p})(l^{q}_{2p}) = a_2 .$$

2.4 A PROOF OF THE ALGORITHM

In case 1. Hofmeister's result (1.3.6) mentioned in introduction is used.

$$\text{Since } \delta_1 = 1 \quad , \quad a_2-x_1 > \frac{1}{2}a_2 .$$

That is, $a_2 > 2x_1$ is precisely the condition used for (1.3.6). Thus, because $\alpha_1 = 1$, (1.3.6) gives:

$$g_3 = a_3+\max\{x_1a_1, (a_1-y_1)a_2\}-a_2-a_1 .$$

Lemma 2 is used for the proof in case 2.

Case 2a.

Let $p > 1$ be *odd* and let L be a complete system of residues modulo a_1. For each $l \not\equiv 0 \pmod{a_1}$ let $t_l \equiv l \pmod{a_1}$ be the smallest positive integer with a represention by a_2,a_3. Then there are pairs of non-negative integers (y,z) such that

$$t_l = ya_2+za_3 .$$

Let (y',z') be such a pair for which y' is minimal.

Suppose that the algorithm continues at $(p-1)^{st}$ step. Then one of the following (1) or (2) is valid.

$$(1) \quad y_p^e < y_{p-1}^e \text{ or } (2) \quad y_p^e \geqslant y_{p-1}^e .$$

If (1) is valid, then as in (2.3.2) $x_{p-2}^e > x_{p-1}^e > x_p^e \geqslant 0$, and therefore, as in (2.3.1') Lemma 5, $y_p^e > 0$ and

$$\begin{aligned} t_l - x_p^e a_1 &= y'a_2+z'a_3+\gamma_p a_3-y_p^e a_2 \qquad \text{because of (2.3.6)} . \\ &= (y'-y_p^e)a_2+(z'+\gamma_p)a_3 \end{aligned}$$

If $x_p^e > 0$ then by the definition of the t_l or if $x_p^e = 0$ then by the minimality of y'

$$(2.4.1) \qquad 0 \leqslant y' < y_p^e$$

If (2) is valid then the algorithm terminates. Furthermore, since (as in the algorithm) $x_{p-2}^e > x_{p-1}^e$ using (2.3.1), we have:

$$x_{p-1}^e > x_p^e \geqslant 0 \quad \text{and}$$

$$\begin{aligned} t_l-(x_{p-1}^e-x_p^e)a_1 &= y'a_2+z'a_3-m_{p-1}a_3+(y_p^e-y_{p-1}^e)a_2 \qquad \text{because of (2.3.9)} \\ &= (y'+(y_p^e-y_{p-1}^e))a_2+(z'-m_{p-1})a_3 . \end{aligned}$$

Therefore, because of the definition of t_l

(2.4.2) $$0 \leqslant z' < m_{p-1}$$

Furthermore note that $x^e_{p-1} > 0$ in both cases and

$$\begin{aligned} & t_l - x^e_{p-1}a_1 \\ &= (y'-y^e_{p-1})a_2+(z'-l_{p-1})a_3 \quad \text{because of (2.3.5)} \end{aligned}$$

Once again because of the definition of t_l

(2.4.3) $$0 \leqslant y' < y^e_{p-1} \quad \text{or} \quad 0 \leqslant z' < l_{p-1} = m_{p-1}-\gamma_{p-1}$$

Thus $(z',y') \in Y \cup Z$ where Y and Z are *disjoint* sets of pairs of integers:

$$Y = \{(y,z) | 0 \leqslant y < y^e_{p-1} \ , \ 0 \leqslant z < m_{p-1}\}$$

$$Z = \{(y,z) | y^e_{p-1} \leqslant y \leqslant y^e_p \ , \ 0 \leqslant z < l_{p-1}\} \ .$$

The number of elements in $Y \cup Z$ is given by

$$\begin{aligned} |Y \cup Z| = |Y|+|Z| &= (y^e_{p-1})(m_{p-1})+(y^e_p-y^e_{p-1})(m_{p-1}-\gamma_{p-1}) \\ &= y^e_p \cdot m_{p-1}-(y^e_p-y^e_{p-1})\gamma_{p-1} = a_1 \end{aligned}$$

because of (2.3.16) ,

Thus, $\{t_l | l \in L\} = \{ya_2+za_3 | (y,z) \in Y \cup Z\}$ forms a complete system L of residues modulo a_1. Also

$$\max_{(y,z) \in Y} \{ya_2+za_3\} = (y^e_{p-1}-1)a_2+(m_{p-1}-1)a_3$$

and if Z is not empty — i.e. if $y^e_p \geqslant y^e_{p-1}$ (precisely the condition used to terminate the algorithm after $(p-1)^{st}$ step.) — then

$$\max_{(y,z) \in Z} \{ya_2+za_3\} = (y^e_p-1)a_2+(m_{p-1}-\gamma_{p-1}-1)a_3 \ ,$$

giving — as in lemma 2 —

$$\begin{aligned} g_3 = \max_{l \in Y \cup Z} t_l - a_1 &= (m_{p-1}-1)a_3-a_2-a_1+\max\{y^e_{p-1}a_2, y^e_p a_2-\gamma_{p-1}a_3\} \\ &= (m^e-1)a_3+\max\{y^e a_2, x^e a_1\}-a_2-a_1 \ , \end{aligned}$$

because of (2.3.7) and by the definitions of m^e, y^e and x^e.

Case 2b.

Let $p > 0$ be *even* and let L be a complete system of residues modulo a_2. For each $l \not\equiv 0 \pmod{a_2}$ let $t_l \equiv l \ (a_2)$ be the smallest positive integer with a representation by a_2,a_3. Then there are non-negative integers (x,z) such that

$$t_l = xa_1+za_3 .$$

Let (x',z') be such a pair for which x' is minimal.

Suppose that the algorithm continues at $(p-1)^{st}$ step. Then one of the following (1) or (2) is valid.

$$(1) \quad x^e_{p-1} > x^e_p \text{ or } (2) \ x^e_p \geqslant x^e_{p-1} .$$

If (1) is valid, then as in (2.3.1), $y^e_{p-2} > y^e_{p-1} > y^e_p \geqslant 0$. Therefore, as in (2.3.2') Lemma 5, $x^e_p > 0$ and

$$\begin{aligned} t_l-y^e_pa_2 &= x'a_1+z'a_3+l_pa_3-x^e_pa_1 \quad \text{because of (2.3.5)} \\ &= (x'-x^e_p)a_1+(z'+l_p)a_3 \end{aligned}$$

If $y^e_p > 0$ then because of the definition of t_l or if $y^e_p = 0$. Then because of minimality of x'

$$0 \leqslant x' < x^e_p \tag{2.4.4}$$

If (2) is valid then the algorithm terminates. Furthermore, since (as in the algorithm) $y^e_{p-2} > y^e_{p-1}$ using (2.3.2), $y^e_{p-1} > y^e_p \geqslant 0$ and

$$\begin{aligned} t_l-(y^e_{p-1}-y^e_p)a_2 &= x'a_1+z'a_3-m_{p-1}a_3+(x^e_p-x^e_{p-1})a_1 \quad \text{because of (2.3.8)} \\ &= (x'+(x^e_p-x^e_{p-1}))a_1 + (z'-m_{p-1})a_3 \end{aligned}$$

Therefore, by the definition of t_l

$$0 \leqslant z' < m_{p-1} \tag{2.4.5}$$

Furthermore note that $y^e_{p-1} > 0$ in both cases and

$$t_l - y^e_{p-1}a_2 =$$

$$= x'a_1 + z'a_3 - \gamma_{p-1}a_3 - x^e_{p-1}a_1 \quad \text{because of (2.3.6)} .$$

$$= (x' - x^e_{p-1})a_1 + (z' - \gamma_{p-1})a_3$$

Once again due to definition of t_l

(2.4.6) $$0 \leqslant x' < x^e_{p-1} \quad \text{or} \quad 0 \leqslant z' < \gamma_{p-1}$$

Thus $(x',z') \in X \cup Z$ where X and Z are *disjoint* sets of pairs of integers:

$$X = \{(x,z) | 0 \leqslant x < x^e_{p-1} \ , \ 0 \leqslant z < m_{p-1}\}$$

$$Z = \{(x,z) | x^e_{p-1} \leqslant x < x^e_p \ , \ 0 \leqslant z < \gamma_{p-1}\} .$$

The number of elements in $X \cup Z$ is given by

$$|X \cup Z| = |X| + |Z| = (x^e_{p-1})(m_{p-1}) + (x^e_p - x^e_{p-1})(m_{p-1} - l_{p-1}) \quad \text{since } \gamma_{p-1} = m_{p-1} - l_{p-1} .$$

$$= x^e_p \cdot m_{p-1} - (x^e_p - x^e_{p-1})l_{p-1}$$

$$= a_2 \quad \text{because of (2.3.19)}$$

Thus,

$$\{t_l | l \in L\} = \{xa_1 + za_3 | (x,z) \in X \cup Z\}$$

forms a complete system of residues modulo a_2. Also

$$\max_{(x,z) \in X} \{xa_1 + za_3\} = (x^e_{p-1} - 1)a_1 + (m_{p-1} - 1)a_3$$

and if Z is not empty — i.e. when $x^e_p \geqslant x^e_{p-1}$ (precisely the condition used to terminate the algorithm) — then

$$\max_{(x,z) \in Z} \{xa_1 + za_3\} = (x^e_p - 1)a_1 + (\gamma_{p-1} - 1)a_3 \quad \text{giving — as in lemma 2 —}$$

$$g_3 = \max_{l \in X \cup Z} t_l - a_2 = (m_{p-1}-1)a_3 - a_1 - a_2 + \max\{x^a_{p-1}a_1, x^a_p a_1 - l_{p-1}a_3\}$$

$$= (m^a - 1)a_3 + \max\{y^a a_2, x^a a_1\} - a_2 - a_1$$

because of (2.3.5) and by the definitions of m^a, y^a, x^a.

The following completes the proof for case 2.

Let $p > 1$ be *odd* with $x^a_p = 0$ and $y^a_p < y^a_{p-1}$.

Then

$$y^a_p > y^a_{p+1} \geqslant 0 \text{ as in (2.3.2)}$$

$$x^a_{p-2} > x^a_{p-1} \text{ as in the algorithm}$$

$$x^a_{p-1} > x^a_p \geqslant 0 \text{ as in (2.3.1)}$$

and $\quad x^a_{p+1} = x^a_{p-1} - \alpha_p x^a_p = x^a_{p-1}$ by the definition of x^a_{p+1} as in $(2N_1)$

giving $x^a_{p+1} \geqslant x^a_p$.

Therefore the algorithm ends *after* pth step with $x^a = x^a_p = 0$, $y^a = y^a_{p+1}$, $m^a = m^a_p$ and

$$g_3 = (m^a_p - 1)a_3 + \max\{x^a_p a_1, y^a_{p+1}a_2\} - a_1 - a_2$$

$$= m^a_p a_3 + y^a_{p+1}a_2 - a_1 - a_2 - a_3$$

$$= m^a_{p-1}a_3 + \alpha_p \gamma^a_p a_3 + y^a_{p-1}a_2 - \alpha_p y^a_p a_2 - a_1 - a_2 - a_3$$

$$= (m^a_{p-1} - 1)a_3 + \max\{x^a_p a_1, y^a_{p-1}a_2\} - a_1 - a_2 \quad \text{using (2.3.7) and noting } x^a_p = 0 .$$

Thus if $x^a_p = 0$ we can end the algorithm after $(p-1)^{st}$ step. Similarly if $y^a_p = 0$ for *even* $p > 0$, then we can end the algorithm after $(p-1)^{st}$ step.

The proof for case 3 is exactly the same when a is replaced by d, even p replaced by odd p, and odd p replaced by even p, and is omitted.

Corollary 1. When $a_2 \geqslant x_1(a_1 + 1)$ (i.e., when Hofmeister's condition is satisfied for (1.3.6)) then

$$x_2^0 = x_0^0 - a_1 x_1^0 = a_2 - a_1 x_1 \geqslant x_1 = x_1^0 .$$

Therefore, the algorithm ends after the first step with (see Diagram 1)

$$x^e = x_1^0, y^e = y_2^0, m^e = m_1^0 = a_1 + 1$$

giving

$$g_3 = a_1 a_3 + \max\{x_1 a_1, (a_1 - a_1 y_1) a_2\} - a_1 - a_2 .$$

(i.e., giving (1.3.6).

Corollary 2. When $a_1 \geqslant (a_1 - y_1)(\delta_1 + 1)$ then (see Diagram 2)

$$y_2^0 = y_0^0 - \delta_1 y_1^0 = a_1 - \delta_1 \cdot (a_1 - y_1^0) \geqslant (a_1 - y_1) = y_1^0$$

Therefore, the algorithm ends after the first step with

$$x^d = x_2^0, y^d = y_1^0, m^d = m_1^0 = \delta_1 + 1$$

giving

$$g_3 = \delta_1 a_3 + \max\{(a_2 - \delta_1 \cdot (a_2 - x_1)) a_1, (a_1 - y_1) a_2\} - a_1 - a_2$$

(i.e., giving (1.3.7)).

Corollary 3. When $a_3 \equiv -a_2 \pmod{a_1}$ then

$$a_3 = \left[\frac{a_2 + a_3}{a_1}\right] \cdot a_1 - a_2 \quad \text{gives}$$

$$x_1^0 = \frac{a_2 + a_3}{a_1}, \; y_1^0 = 1 ,$$

$$\delta_1 = \left[\frac{a_2}{\frac{a_2 + a_3}{a_1}}\right] = \left[\frac{a_1 a_2}{a_2 + a_3}\right], \quad \alpha_1 = \left[\frac{a_1}{a_1 - 1}\right] = 1 .$$

Therefore,

$$x_2^{\delta} = a_2 - \left[\frac{a_1a_2}{a_2+a_3}\right]\cdot\left[\frac{a_2+a_3}{a_1}\right], \quad y_2^{\delta} = a_1 - \left[\frac{a_1a_2}{a_2+a_3}\right].$$

Also when $y_2^{\delta} \geqslant y_1^{\delta}$, i.e., when $a_1 \geqslant \left[\frac{a_1a_2}{a_2+a_3}\right] + 1$ then the algorithm ends after the first step with

$$x^{\delta} = x_2^{\delta},\ y^{\delta} = y_1^{\delta} = 1,\ m^{\delta} = \delta_1 + 1$$

giving

$$g_3 = \left[\frac{a_1a_2}{a_2+a_3}\right]\cdot a_3 + \max\{x^{\delta}\cdot a_1,\ y^{\delta}\cdot a_2\} - a_1 - a_2$$

$$= \max\left\{\left[\frac{a_1a_2}{a_2+a_3}\right]a_3 - a_1,\ \left[\frac{a_1a_2}{a_2+a_3}\right]a_3 + x^{\delta}a_1 - a_1 - a_2\right\}$$

and Brauer and Shockley's formula (1.3.5) follows when we note that

$$\left[\frac{a_1a_2}{a_2+a_3}\right] = \left[\frac{a_1\cdot((\frac{a_2+a_3}{a_1})\cdot a_1 - a_3)}{a_2+a_3}\right] = a_1 - \left[\frac{a_1a_3}{a_2+a_3}\right] - 1$$

and $x^{\delta}a_1 = a_1a_2 - \left[\frac{a_1a_2}{a_2+a_3}\right](a_2+a_3)$.

Chapter III

3.1 INTRODUCTION TO A FORMULA FOR $g(t-n,t-m,t)$ AND A PROOF

We use the following assumptions $(3A_1)$-$(3A_3)$, and notations $(3N_1)$-$(3N_5)$.

$(3A_1)$ $\quad gcd(t-n,t-m,t) = 1$, where $0 < m < n < t$.

$(3A_2)$ $\quad a_1 = \frac{t-n}{(n,t)}$, $a_2 = \frac{t}{(n,t)}$, where $(n,t) = gcd(n,t)$.

$(3A_3)$ $\quad j \frac{t}{(n,t)} \equiv m \left[\text{mod } \frac{n}{(n,t)}\right]$ with $0 < j < \frac{n}{(n,t)}$, $\frac{n}{(n,t)} \geq 2$.

$(3N_1)$ $\quad \bar{n} = \frac{n}{(n,t)}$.

$(3N_2)$ $\quad$ Let $J^a_{-1} = \bar{n}$, $J^a_0 = j$ and for $0 \leq p \leq s^a$,

$$J^a_{p-1} \equiv J^a_{p+1} \pmod{J^a_p} \quad \text{with } 0 \leq J^a_{p+1} < J^a_p < J^a_{p-1}$$

where s^a is such that $J^a_{s^a+1} = 0$. (Note that $s^a \geq 0$ does exist since the Euclidean Algorithm for $J_{-1} \mid J_0$ ends after a finite number of steps.) In addition

$$\text{let } J^d_{-1} = \bar{n}, J^d_0 = \bar{n}-j \text{ and for } 0 \leq p \leq s^d,$$

$$J^d_{p-1} \equiv J^d_{p+1} \pmod{J^d_p} \text{with } 0 \leq J^d_{p+1} < J^d_p < J^d_{p-1}$$

where s^d is such that $J^d_{s^d+1} = 0$.

$$(3N_3) \qquad k_p = \begin{cases} \sum_{l=0}^{l=p-1} \frac{1}{J_l J_{l+1}} & \text{if } p \text{ odd} \\ \sum_{l=1}^{l=p-1} \frac{1}{J_l J_{l+1}} & \text{if } p \text{ even} \end{cases} \qquad \text{with } k_p = 0 \text{ if } p \leqslant 0 .$$

$$(3N_4) \qquad i_p^a = \begin{cases} (J_p n)(k_{p-1}) - (J_p n)(k_p) + \frac{J_p}{J_0}(n,t) + \frac{n}{J_p} & \text{if } p \text{ odd} \\ (J_p n)(k_p) - (J_p n)(k_{p-1}) + \frac{J_p}{J_0}(n,t) & \text{if } p \text{ even} \end{cases}$$

Also

$$i_p^d = \begin{cases} (J_p n)(k_p) - (J_p n)(k_{p-1}) - \frac{J_p}{J_o}(n,t) & \text{if } p \text{ odd} \\ (J_p n)(k_{p-1}) - (J_p n)(k_p) - \frac{J_p}{J_0}(n,t) + \frac{n}{J_p} & \text{if } p \text{ even} \end{cases}$$

$(3N_5)$ Suppose $C_{2,-1}^q = n$, $C_{2,0}^q = \frac{m(n,t)}{J_0}$ then for $p \geqslant 1$ let (when $J_{p-1} \neq 0$)

$$C_p^q = \begin{cases} C_{2,p-2}^q + (n-m)\frac{n}{J_{p-2}\cdot(J_{p-2}-J_{p-1})} & \text{if } p \text{ odd} \\ C_{2,p-2}^q + \frac{mn}{J_{p-2}(J_{p-2}-J_{p-1})} & \text{if } p \text{ even}, \end{cases}$$

$$C_{1,p}^q = \begin{cases} C_{2,p-2}^q + (n-m)\left[\frac{n}{J_{p-2}J_{p-1}}\right]\left[\frac{J_{p-2}}{J_{p-1}} - 1\right] & \text{if } p \text{ odd} \\ C_{2,p-2}^q + \left[\frac{mn}{J_{p-2}J_{p-1}}\right]\left[\frac{J_{p-2}}{J_{p-1}} - 1\right] & \text{if } p \text{ even} \end{cases}$$

and (when $J_p \neq 0$)

$$C^1_{2,p} = \begin{cases} C^1_{2,p-2} + (n-m)\left(\frac{n}{J_{p-2}J_{p-1}}\right)\left(\frac{J_{p-2}}{J_p} - 1\right) & \text{if } p \text{ odd} \\ C^1_{2,p-2} + \left(\frac{mn}{J_{p-2}J_{p-1}}\right)\left(\frac{J_{p-2}}{J_p} - 1\right) & \text{if } p \text{ even} \end{cases}$$

Also suppose $C^1_{2,-1} = 0$, $C^1_{2,0} = n+(n-m)\left(\frac{(n,t)}{J_0}\right)$ then for $p \geq 1$ let (when $J_{p-1} \neq 0$)

$$C^1_p = \begin{cases} C^1_{2,p-2} + \frac{mn}{J_{p-2}(J_{p-2}-J_{p-1})} & \text{if } p \text{ odd} \\ C^1_{2,p-2} + \frac{(n-m)\cdot n}{J_{p-2}(J_{p-2}-J_{p-1})} & \text{if } p \text{ even}, \end{cases}$$

$$C^{1}_{2,p} = \begin{cases} C^{1}_{2,p-2} + \left(\frac{mn}{J_{p-2}J_{p-1}}\right)\left(\frac{J_{p-2}}{J_{p-1}} - 1\right) & \text{if } p \text{ odd} \\ C^{1}_{2,p-2} + \left(\frac{(n-m)(n)}{J_{p-2}J_{p-1}}\right)\left(\frac{J_{p-2}}{J_{p-1}} - 1\right) & \text{if } p \text{ even} \end{cases}$$

and (when $J_p \neq 0$)

$$C^{1}_{2,p} = \begin{cases} C^{1}_{2,p-2} + \left(\frac{mn}{J_{p-2}J_{p-1}}\right)\left(\frac{J_{p-2}}{J_{p}} - 1\right) & \text{if } p \text{ odd} \\ C^{1}_{2,p-2} + \left(\frac{(n-m)(n)}{J_{p-2}J_{p-1}}\right)\left(\frac{J_{p-2}}{J_{p}} - 1\right) & \text{if } p \text{ even} \end{cases}$$

To simplify notation J_p, i_p, C_p, $C_{1,p}$, $C_{2,p}$, s will represent J^a_p, i^a_p, C^a_p, $C^1_{1,p}$, $C^1_{2,p}$, s when case 2 of the algorithm is used or J^d_p, i^d_p, C^d_p, $C^1_{1,p}$, $C^1_{2,p}$, s^d when case 3 of the algorithm is used. Furthermore when superscript "a" is present, for instance γ^a_p, y^a_p, etc., the case 2 of the algorithm is being considered. When superscript "d" is present, for instance γ^d_p, y^d_p, etc., the case 3 of the algorithm is being considered. When both superscript "a" and "d" are present, cases 2 and 3 are being considered.

3.2 A FORMULA: THE MAIN THEOREM

For $t > n > m > 0$ with $gcd(t-n, t-m, t) = 1$ and $0 < i \leq \frac{n}{(m,n)}$ defined by

$$t \equiv i\,\frac{m}{(m,n)} \left[\text{mod } \frac{n}{(m,n)}\right]$$

$$(3.2.1)\; g(t-n,t-m,t) = \begin{cases} \left(\frac{(m,n)t-im}{n} + \frac{n}{(m,n)} - 3\right)(t-n) + (n-m)\left(\frac{n}{(m,n)} - 1\right) - n \quad (B_1) \\ \qquad \text{if } 0 < i \leq \frac{n-m}{(m,n)} \\ \left(\frac{(m,n)t-im}{n} + \frac{m}{(m,n)} + i - 3\right)(t-n) + (n-m)(i-1) - n \quad (B_2) \\ \qquad \text{if } \frac{n-m}{(m,n)} < i \leq \frac{n}{(m,n)} \end{cases}$$

$$\text{provided } t > \max\left\{n + \left(\frac{n-m}{(m,n)}\right)\left(\frac{n}{(m,n)} - i\right),\ (i)\left(\frac{m}{(m,n)}\right)\right\}$$

The Main Theorem takes the following form when the basis elements are $\{a,b,c\}$ and when we substitute t by c, n by $c-a$ and m by $c-b$:

For $0 < a < b < c$ with $gcd(a,b,c) = 1$, $d = gcd(c-b, c-a)$, $0 < i \leq \frac{c-a}{d}$ defined by

$$c \equiv i\left(\frac{c-b}{d}\right)\ \left(\text{mod } \frac{c-a}{d}\right), \text{ and}$$

$$g = \frac{cd - i(c-b)}{c-a}$$

$$g(a,b,c) = \begin{cases} ga + \frac{bc}{d} - \frac{ab}{d} - a - b - c & \text{if } 0 < i \leq \frac{b-a}{d} \\ ga + \frac{ac}{d} - \frac{ab}{d} + bi - a - b - c & \text{if } \frac{b-a}{d} < i \leq \frac{c-a}{d} \end{cases}$$

provided

$$c > \max\left\{c-a + \left(\frac{b-a}{d}\right)\left(\frac{c-a}{d} - i\right),\ (i)\left(\frac{c-b}{d}\right)\right\}.$$

3.3 RESULTS FOR A PROOF OF THE MAIN THEOREM

First we show that $J_s = (m,n)$.

Lemma 8. If $(\bar{n}, j) = d$ then $(m,n) = d$.

Proof.

(3.3.1) Obviously $\left[\frac{t}{(n,t)}, \bar{n}\right] = 1$,

$n \equiv 0 \pmod{d}$, and

$m \equiv 0 \pmod{d}$ due to $(3A_3)$.

Suppose $(m,n) = d \cdot d'$. Then

$$(t, d \cdot d') = 1 \quad \text{due to } (3A_1) ,$$

Thus,

$$((n,t), d \cdot d') = 1 ,$$

and

$$\bar{n} \equiv 0 \pmod{d \cdot d'}$$

Therefore,

$$j \equiv 0 \pmod{d \cdot d'} \text{ due to } (3A_3) .$$

Thus it follows that

$$d' = 1 \text{ since } (\bar{n}, j) = d .$$

Lemma 9.

(3.3.2) $$J_s = (m,n) ,$$

(3.3.3) $$(n,t) < \frac{n}{J_s} ,$$

(3.3.4) $$J_p \geq J_{p+1} + J_s$$

when $0 \leq p+1 \leq s$,

(3.3.5) $$J_{s-1} - J_s \geq J_s > 0 ,$$

and

(3.3.6) $$J_{p-2}-J_p \geqslant J_{p-1}$$

if $p < s+1$.

Proof. Because of $(3N_2)$ when $J_{s+1} = 0$,

$$J_{s-1} \equiv 0 \mod J_s .$$

Also

$$J_{s-2} \equiv J_s \mod J_{s-1} .$$

Therefore,

$$J_{s-1} \equiv J_{s-2} \equiv 0 \mod J_s, \text{ and}$$

$$\frac{J_{s-2}}{J_s} \equiv 1 \mod \frac{J_{s-1}}{J_s}$$

Thus,

$$gcd\left(\frac{J_{s-2}}{J_s}, \frac{J_{s-1}}{J_s}\right) = 1 . \qquad (1)$$

Because

$$J_{s-3} \equiv J_{s-1} \pmod{J_{s-2}} ,$$

we have

$$J_{s-3} \equiv 0 \mod J_s \text{ and}$$

$$\frac{J_{s-3}}{J_s} \equiv \frac{J_{s-1}}{J_s} \left(\mod \frac{J_{s-2}}{J_s}\right) .$$

If $gcd\left(\frac{J_{s-3}}{J_s}, \frac{J_{s-2}}{J_s}\right) > 1$ then $gcd\left(\frac{J_{s-2}}{J_s}, \frac{J_{s-1}}{J_s}\right) > 1$ contradicting (1).

Therefore,

$$\left(\frac{J_{s-3}}{J_s}, \frac{J_{s-2}}{J_s}\right) = 1 .$$

Using the same argument we end up with

$$\left(\frac{J_{-1}}{J_s}, \frac{J_0}{J_s}\right) = 1 \quad \text{giving}$$

$(\bar{n}, j) = J_s$ or $(\bar{n}, \bar{n}-j) = (\bar{n}, j) = J_s$.

Now lemma 8 gives $(m,n) = J_s$. Thus, (3.3.2) holds.

Also for $s \geqslant 0$, $\bar{n} > J_s$

Therefore,

$$(n,t) = \frac{n}{\bar{n}} < \frac{n}{J_s} .$$

Thus, (3.3.3) holds.

Furthermore, for $0 \leqslant p+1 \leqslant s$,

$$J_p \equiv J_{p+1} \equiv 0 \mod J_s$$

and

$$J_p > J_{p+1} > 0 .$$

(Note $J_{-1} > J_0 > J_1 \geqslant 0$ by $(3A_3)$ and $(3N_2)$.)

Thus, we have $J_p \geqslant J_{p+1}+J_s$. Thus, (3.3.4) holds.

For

$$p = s , \; J_{p+1} = 0 .$$

Therefore,

$$J_{p-1} \equiv 0 \pmod{J_p} \text{ with } 0 = J_{p+1} < J_p < J_{p-1},$$

giving

$$J_{p-1} \geq 2J_p \text{ i.e. } J_{p-1}-J_p \geq J_p .$$

Thus, (3.3.5) holds.

Finally, for $p < s+1$,

$$J_{p-2} \equiv J_p \pmod{J_{p-1}} \text{ with } 0 < J_p < J_{p-1} < J_{p-2} .$$

Therefore,

$$J_{p-2}-J_p \geq J_{p-1} .$$

Thus (3.3.6) holds.

Lemma 10. For odd $p \geq 1$,

$$C^{\P}_{1,p} = n+(n-m)\left[n(k_{p-2})-n(k_{p-1}) - \frac{(n,t)}{J_0} + \frac{n}{J_{p-1}J_{p-1}}\right],$$

$$C^{\P}_{2,p} = n+(n-m)\left[n(k_p)-n(k_{p-1}) - \frac{(n,t)}{J_0}\right],$$

$$C^{\P}_{1,p} = (mn)(k_{p-2})-(mn)(k_{p-1}) - \frac{m(n,t)}{J_0} + \frac{mn}{J_{p-1}J_{p-1}},$$

$$C^{\P}_{2,p} = (mn)(k_p)-(mn)(k_{p-1}) - \frac{m(n,t)}{J_0} \text{ and},$$

for even $p \geq 2$,

$$C^{q}_{1,p} = (mn)(k_{p-2})-(mn)(k_{p-1}) + \frac{m(n,t)}{J_0} + \frac{mn}{J_{p-1}J_{p-1}},$$

$$C^{q}_{2,p} = (mn)(k_{p})-(mn)(k_{p-1}) + \frac{m(n,t)}{J_0},$$

$$C^{q}_{1,p} = n+(n-m)\left[n(k_{p-2})-n(k_{p-1}) + \frac{(n,t)}{J_0} + \frac{n}{J_{p-1}J_{p-1}}\right],$$

$$C^{q}_{2,p} = n+(n-m)\left[n(k_{p})-n(k_{p-1}) + \frac{(n,t)}{J_0}\right].$$

Proof. First we prove lemma 10 for $C^{q}_{1,p}$ and $C^{q}_{2,p}$. We use induction on p. By $(3N_5)$ we have:

$$C_{1,1} = n+(n-m)\left[\frac{n}{J_0J_0} - \frac{(n,t)}{J_0}\right] \text{ and},$$

$$C_{2,1} = n+(n-m)\left[\frac{n}{J_0J_1} - \frac{(n,t)}{J_0}\right].$$

Thus, the lemma is true for $C^{q}_{1,p}$ and $C^{q}_{2,p}$ when $p = 1$.

Also

$$C_{1,2} = \frac{m(n,t)}{J_0} + \frac{mn}{J_1J_1} - \frac{mn}{J_0J_1} \text{ and } C_{2,2} = \frac{m(n,t)}{J_0} + \frac{mn}{J_1J_2} - \frac{mn}{J_0J_1}$$

Thus, the lemma is valid for $C^{q}_{1,p}$ and $C^{q}_{2,p}$ when $p = 2$.

Suppose the lemma is valid for $C^{q}_{1,p}$ and $C^{q}_{2,p}$ when *odd* $p > 1$. Then using $(3N_5)$ we have:

$$C_{1,p+2} = C_{2,p}+(n-m)\left[\frac{n}{J_pJ_{p+1}})(\frac{J_p}{J_{p+1}} - 1\right],$$

$$= n+(n-m)\left[nk_p)-n(k_{p-1}) - \frac{(n,t)}{J_0}\right]+(n-m)\left[\frac{n}{J_pJ_{p+1}}\right]\left[\frac{J_p}{J_{p+1}} - 1\right],$$

$$= n+(n-m)\left[n(k_p)-n(k_{p+1}) - \frac{(n,t)}{J_0} + \frac{n}{J_{p+1}J_{p+1}}\right].$$

$$C_{2,p+2} = C_{2,p}+(n-m)\left[\frac{n}{J_pJ_{p+1}}\right]\left[\frac{J_p}{J_{p+2}} - 1\right],$$

$$= n+(n-m)\left[n(k_{p+2})-n(k_{p+1}) - \frac{(n,t)}{J_0}\right].$$

Thus the lemma is valid for $C^q_{1,p+2}$ and $C^q_{2,p+2}$, when p is odd.

Similarly suppose the lemma is valid for $C^q_{1,p}$ and $C^q_{2,p}$ when *even* $p > 2$. Then using $(3N_5)$ we have:

$$C_{1,p+2} = C_{2,p} + \left[\frac{mn}{J_pJ_{p+1}}\right]\left[\frac{J_p}{J_{p+1}} - 1\right],$$

$$= (mn)(k_p)-(mn)(k_{p-1}) + \frac{m(n,t)}{J_0} + \left[\frac{mn}{J_pJ_{p+1}}\right]\left[\frac{J_p}{J_{p+1}} - 1\right],$$

$$= (mn)(k_p)-(mn)(k_{p+1}) + \frac{m(n,t)}{J_0} + \frac{mn}{J_{p+1}J_{p+1}} \text{ and}$$

$$C_{2,p+2} = C_{2,p} + \left[\frac{mn}{J_pJ_{p+1}}\right]\left[\frac{J_p}{J_{p+2}} - 1\right]$$

$$= (mn)(k_{p+2})-(mn)(k_{p+1}) + \frac{m(n,t)}{J_0}.$$

Thus, the lemma is true for $C^q_{1,p+2}$ and $C^q_{2,p+2}$, when p is even.

The proof for $C^q_{1,p}$ and $C^q_{2,p}$ is similar, and is omitted.

Lemma 11. For $p > 0$, $C_{2p-2} < C_p < C_{1p}$ if $p = s+1$ and

$C_{2p-2} < C_p < C_{2p}$ if $p < s+1$.

Proof. For $p \leq s+1$, by $(3N_2)$

$$J_{p-2} > J_{p-1} > 0 ,$$

Thus, because of $(3N_5)$

$$C_{2p-2} < C_p \ldots . \tag{1}$$

Furthermore, because of $(3N_5)$ and lemma 9, (3.3.5),

$$\left[\frac{J_{p-2}-J_{p-1}}{J_{p-1}J_{p-1}}\right] \geq \frac{1}{J_{p-1}} \geq \frac{1}{J_{p-2}-J_{p-1}} \quad \text{when } p = s+1$$

Thus,

$$C_p < C_{1p} \ldots . \tag{2}$$

Furthermore because of $(3N_5)$ and lemma 9, (3.3.6)

$$\left[\frac{J_{p-2}-J_p}{J_{p-1}J_p}\right] \geq \frac{1}{J_p} \geq \frac{1}{J_{p-2}-J_{p-1}} \quad \text{when } p < s+1$$

Thus,

$$C_p < C_{2p} \ldots . \tag{3}$$

Combining (1),(2) and (3) the proof is completed.

Lemma 12. For $0 < j < \frac{\bar{n}}{2}$ we use case 2 of the algorithm, or for $\frac{\bar{n}}{2} < j < \bar{n}$ we use case 3 of the algorithm, and for $j = \frac{\bar{n}}{2}$ we use case 1 of the algorithm.

If $0 < odd\ p \leq s+1$ we have α_p (in case 2) ≥ 1 or δ_p (in case 3) ≥ 1 and $\alpha_1 = \delta_1 = 1$ (in case 1).

$$\begin{matrix}\alpha_p \text{ (in case 2) or} \\ \delta_p \text{ (in case 3)}\end{matrix} = \begin{cases} \frac{J_{p-2}}{J_{p-1}} - 1 & \text{if } p = s+1 \text{ and } t > \max\{C_{2,p-1}, C_{1,p}\} \\ \frac{J_{p-2} - J_p}{J_{p-1}} & \text{if } p < s+1 \text{ and } t > \max\{C_{2,p-1}, C_{2,p}\} \end{cases}$$

Also if $x_p^a \neq 0$ (in case 2) or $y_p^d \neq 0$ (in case 3) then

$$(3.3.7) \quad x_{p+1}^a = \begin{cases} x_p^a + \frac{m}{J_{p-1}} & \text{if } p = s+1 \\ \left(\frac{J_p}{J_{p-1}}\right) x_p^a + \frac{m}{J_{p-1}} & \text{if } p < s+1 \end{cases}$$

$$(3.3.7a) \quad = \begin{cases} \frac{J_{p-1}t - \left(\frac{J_{p-1}}{J_0}\right) m(n,t)}{n} + (J_{p-1}m)(k_{p-2} - k_{p-1}) + \frac{m}{J_{p-1}} & \text{if } p = s+1 \\ \frac{J_p t - \left(\frac{J_p}{J_0}\right) m(n,t)}{n} + (J_p m)(k_p - k_{p-1}) & \text{if } p < s+1 , \end{cases}$$

$$(3.3.8)\quad x^d_{p+1} = \begin{cases} x^d_p - \dfrac{m}{J_{p-1}} & \text{if } p = s+1 \\ \left(\dfrac{J_p}{J_{p-1}}\right) x^d_p - \dfrac{m}{J_{p-1}} & \text{if } p < s+1\,, \end{cases}$$

$$(3.3.8a)\quad = \begin{cases} \dfrac{J_{p-1}t + \left(\dfrac{J_{p-1}}{J_0}\right) m(n,t)}{n} - (J_{p-1}m)(k_{p-2}-k_{p-1}) - \dfrac{m}{J_{p-1}} & \text{if } p = s+1 \\ \dfrac{J_p t + \left(\dfrac{J_p}{J_0}\right) m(n,t)}{n} - (J_p m)(k_p - k_{p-1}) & \text{if } p < s+1\,, \end{cases}$$

$$(3.3.9)\quad y^a_{p+1} = \begin{cases} y^a_p - \dfrac{(n-m)}{J_{p-1}} & \text{if } p = s+1 \\ \left(\dfrac{J_p}{J_{p-1}}\right) y^a_p - \dfrac{(n-m)}{J_{p-1}} & \text{if } p < s+1\,, \end{cases}$$

$$(3.3.9a)\quad = \begin{cases} x^a_{p+1} + \left(\dfrac{J_{p-1}}{J_0}\right)(n,t) - J_{p-1} - (J_{p-1}n)(k_{p-2}-k_{p-1}) - \dfrac{n}{J_{p-1}} & \text{if } p = s+1 \\ x^a_{p+1} + \left(\dfrac{J_p}{J_0}\right)(n,t) - J_p - (J_p n)(k_p - k_{p-1}) & \text{if } p < s+1\,, \end{cases}$$

$$(3.3.10)\quad y^d_{p+1} = \begin{cases} y^d_p + \dfrac{(n-m)}{J_{p-1}} & \text{if } p = s+1 \\ \left(\dfrac{J_p}{J_{p-1}}\right) y^d_p + \dfrac{(n-m)}{J_{p-1}} & \text{if } p < s+1\,, \end{cases}$$

$$(3.3.10a)\quad = \begin{cases} x^d_{p+1} - \left(\dfrac{J_{p-1}}{J_0}\right)(n,t) - J_{p-1} + (J_{p-1}n)(k_{p-2}-k_{p-1}) + \dfrac{n}{J_{p-1}} & \text{if } p = s+1 \\ x^d_{p+1} - \left(\dfrac{J_p}{J_0}\right)(n,t) - J_p + (J_p n)(k_p - k_{p-1}) & \text{if } p < s+1\,. \end{cases}$$

$$l_p^e = \begin{cases} -\gamma_p^e + \frac{\bar{n}}{J_{p-1}} & \text{if } p = s+1 \\ -(\frac{J_p}{J_{p-1}})\gamma_p^e + \frac{\bar{n}}{J_{p-1}} & \text{if } p < s+1 \end{cases}$$

$$\text{or } l_p^d = l_{p-1}^d$$

$$\gamma_p^d = \begin{cases} -l_p^d + \frac{\bar{n}}{J_{p-1}} & \text{if } p = s+1 \\ -\left(\frac{J_p}{J_{p-1}}\right) l_p^d + \frac{\bar{n}}{J_{p-1}} & \text{if } p < s+1 \end{cases}$$

$$\text{or } \gamma_p^d = \gamma_{p-1}^e$$

Furthermore if $p = s+1$ or (if $y_{p+1}^e = 0$ in case 2 or $x_{p+1}^d = 0$ in case 3) the algorithm terminates with

$$x^e = x_p^e,\ y^e = y_{p+1}^e,\ m^e = \frac{\bar{n}}{J_{p-1}},$$

or

$$x^d = x_{p+1}^d,\ y^d = y_p^d,\ m^d = \frac{\bar{n}}{J_{p-1}},\ \text{and}$$

$$t > \begin{cases} \max(C_{2p-1}, C_{1p}) & \text{if } p = s+1 \\ \max(C_{2p-1}, C_{2p}) & \text{if } y_{p+1}^e = 0,\ \text{or } x_{p+1}^d = 0. \end{cases}$$

Also if $p = s+1$ then

$$C_{1p}^{\prime} - C_{2p-1}^{\prime} \geq 0,\ \text{or } C_{2p-1}^{\prime} - C_{1p}^{\prime} \geq 0$$

when

$$\frac{n-m}{J_s} \geq i_s - J_s.$$

If $0 < \textit{even}\ p \leq s+1$ we have δ_p (in case 2) ≥ 1 or α_p (in case 3) ≥ 1 where

$$\delta_p \text{ (in case 2) or } \alpha_p \text{ (in case 3)} = \begin{cases} \frac{J_{p-2}}{J_{p-1}} - 1 & \text{if } p = s+1 \text{ and } t > \max\{C_{2,p-1}, C_{1,p}\} \\ \frac{J_{p-2} - J_p}{J_{p-1}} & \text{if } p < s+1 \text{ and } t > \max\{C_{2,p-1}, C_{2,p}\} \end{cases}$$

Also if $y_p^a \neq 0$ (in case 2) *or* $x_p^d \neq 0$ (in case 3) then the rest of the lemma is same except now a and d are interchanged. That is:

$$(3.3.11)\quad x^a_{p+1} = \begin{cases} x^a_p - \dfrac{m}{J_{p-1}} & \text{if } p = s+1 \\ \left(\dfrac{J_p}{J_{p-1}}\right) x^a_p - \dfrac{m}{J_{p-1}} & \text{if } p < s+1\,, \end{cases}$$

$$(3.3.11a)\quad = \begin{cases} \dfrac{J_{p-1}t - \left(\dfrac{J_{p-1}}{J_0}\right) m(n,t)}{n} + (J_{p-1}m)(k_{p-1}-k_{p-2}) - \dfrac{m}{J_{p-1}} & \text{if } p = s+1 \\ \dfrac{J_p t - \left(\dfrac{J_p}{J_0}\right) m(n,t)}{n} + (J_p m)(k_{p-1}-k_p) & \text{if } p < s+1\,, \end{cases}$$

$$(3.3.12)\quad x^d_{p+1} = \begin{cases} x^d_p + \dfrac{m}{J_{p-1}} & \text{if } p = s+1 \\ \left(\dfrac{J_p}{J_{p-1}}\right) x^d_p + \dfrac{m}{J_{p-1}} & \text{if } p < s+1\,, \end{cases}$$

$$(3.3.12a)\quad = \begin{cases} \dfrac{J_{p-1}t + \left(\dfrac{J_{p-1}}{J_0}\right) m(n,t)}{n} - (J_{p-1}m)(k_{p-1}-k_{p-2}) + \dfrac{m}{J_{p-1}} & \text{if } p = s+1 \\ \dfrac{J_p t + \left(\dfrac{J_p}{J_0}\right) m(n,t)}{n} - (J_p m)(k_{p-1}-k_p) & \text{if } p < s+1\,, \end{cases}$$

$$(3.3.13)\quad y^a_{p+1} = \begin{cases} y^a_p + \dfrac{(n-m)}{J_{p-1}} & \text{if } p = s+1 \\ \left(\dfrac{J_p}{J_{p-1}}\right) y^a_p + \dfrac{(n-m)}{J_{p-1}} & \text{if } p < s+1 \end{cases}$$

$$(3.3.13a)\quad = \begin{cases} x^a_{p+1} + \left(\frac{J_{p-1}}{J_0}\right)(n,t) - J_{p-1} - (J_{p-1}n)(k_{p-1}-k_{p-2}) + \frac{n}{J_{p-1}} & \text{if } p = s+1 \\ x^a_{p+1} + \left(\frac{J_p}{J_0}\right)(n,t) - J_p - (J_p n)(k_{p-1}-k_p) & \text{if } p < s+1\,, \end{cases}$$

$$(3.3.14)\qquad y^d_{p+1} = \begin{cases} y^d_p - \frac{(n-m)}{J_{p-1}} & \text{if } p = s+1 \\ \left(\frac{J_p}{J_{p-1}}\right) y^d_p - \frac{(n-m)}{J_{p-1}} & \text{if } p < s+1\,, \end{cases}$$

$$(3.3.14a)\quad = \begin{cases} x^d_{p+1} - \left(\frac{J_{p-1}}{J_0}\right)(n,t) - J_{p-1} + (J_{p-1}n)(k_{p-1}-k_{p-2}) - \frac{n}{J_{p-1}} & \text{if } p = s+1 \\ x^d_{p+1} - \left(\frac{J_p}{J_0}\right)(n,t) - J_p + (J_p n)(k_{p-1}-k_p) & \text{if } p < s+1\,, \end{cases}$$

$$l_p^d = \begin{cases} -\gamma_p^d + \dfrac{\bar{n}}{J_{p-1}} & \text{if } p = s+1 \\ -\left(\dfrac{J_p}{J_{p-1}}\right)\gamma_p^d + \dfrac{\bar{n}}{J_{p-1}} & \text{if } p < s+1 \end{cases}.$$

or $l_p^a = l_{p-1}^a$

$$\gamma_p^a = \begin{cases} -l_p^a + \dfrac{\bar{n}}{J_{p-1}} & \text{if } p = s+1 \\ -\left(\dfrac{J_p}{J_{p-1}}\right)l_p^a + \dfrac{\bar{n}}{J_{p-1}} & \text{if } p < s+1 \end{cases}$$

or $\gamma_p^d = \gamma_{p-1}^d$

Furthermore if $p = s+1$ or (if $x_{p+1}^a = 0$ in case 2 or $y_{p+1}^d = 0$ in case 3) the algorithm terminates with

$$x^a = x_{p+1}^a,\ y^a = y_p^a,\ m^a = \frac{\bar{n}}{J_{p-1}},$$

or

$$x^d = x_p^d,\ y^d = y_{p+1}^d,\ m^d = \frac{\bar{n}}{J_{p-1}},\ \text{and}$$

$$t > \begin{cases} \max(C_{2,p-1}, C_{1,p}) & \text{if } p = s+1 \\ \max(C_{2,p-1}, C_{2,p}) & \text{if } x_{p+1}^a = 0,\ \text{or } y_{p+1}^d = 0 \end{cases}$$

Also if $p = s+1$ then

$$C_{2,p-1}^l - C_{1,p}^l \geq 0,\ \text{or } C_{1,p}^l - C_{2,p-1}^l \geq 0$$

when

$$\frac{n-m}{J_s} \geq i_s - J_s .$$

Proof. A proof for (3.3.7a), (3.3.8a),.....,(3.3.14a) is presented after the rest of the lemma is proved so that the proof for the rest of the lemma does not become overly complex.

Because of $(3A_2)$,

$$a_1 = \frac{t-n}{(n,t)}, a_2 = \frac{t}{(n,t)} .$$

Because of $(3A_3)$,

$$j \frac{t}{(n,t)} \equiv m \pmod{\bar{n}} \text{ with } 0 < j < \bar{n}, \bar{n} \geq 2 .$$

Let $a_3 = t-m$. Then

$$a_3 = \left\lfloor \frac{j(t-n)+(n,t)(n-m)}{n} \right\rfloor a_2 - \left\lfloor \frac{jt-m(n,t)}{n} \right\rfloor a_1 \text{ with}$$

$$0 < \frac{j(t-n)+(n,t)(n-m)}{n} < a_1 \text{ and } 0 < \frac{jt-m(n,t)}{n} < a_2$$

when

$$\begin{cases} t > n + \dfrac{(n,t)(n-m)}{(\bar{n}-j)} = C_1^1 \\ \text{and} \\ t > n - \dfrac{(n,t)(n-m)}{j} \end{cases} \text{ and } \begin{cases} t > \dfrac{-mn}{(\bar{n}-j)} \\ \text{and} \\ t > \dfrac{m(n,t)}{j} = C_{2,0}^1 \end{cases}$$

Thus, for $t > \left\{ n + \dfrac{(n,t)(n-m)}{(\bar{n}-j)}, \dfrac{m(n,t)}{j} \right\}$ — as in the algorithm — we have:

$$x_1^q = \frac{jt-m(n,t)}{n}, \quad y_1^q = \frac{j(t-n)+(n,t)(n-m)}{n},$$

$$x_1^d = a_2-x_1^q = \frac{(\bar{n}-j)t+m(n,t)}{n}, \quad y_1^d = a_1-y_1^q = \frac{(\bar{n}-j)(t-n)-(n,t)(n-m)}{n}$$

$$\alpha_1 = \left\lfloor \frac{\frac{t-n}{(n,t)}}{\frac{j(t-n)+(n,t)(n-m)}{n}} \right\rfloor = \begin{cases} \frac{J_{-1}^a}{J_0^q} - 1 & \text{if } J_1 = 0 \text{ and } j(t-n) > \left(\frac{J_{-1}}{J_0} - 1\right)(n,t)(n-m) \\ & \text{i.e., if } s = 0 \text{ and } t > C_{1,1}^q \\ \frac{J_{-1}^a - J_1^q}{J_0^q} & \text{if } J_1 > 0 \text{ and } J_1(t-n) > \left(\frac{J_{-1}-J_1}{J_0}\right)(n,t)(n-m) \\ & \text{i.e., if } s > 0 \text{ and } t > C_{2,1}^q \end{cases}$$

Because of lemma 9, (3.3.5) and (3.3.6), if $J_1 = 0$ then $J_{-1} \geq 2J_0$ and if $J_1 > 0$ then $J_{-1}-J_1 \geq J_0$.

Therefore,

$$\alpha_1 \geq 1 .$$

Also

$$\delta_1 = \left\lfloor \frac{\frac{t}{(n,t)}}{\frac{(\bar{n}-j)t+m(n,t)}{n}} \right\rfloor = \begin{cases} \frac{J_{-1}^d}{J_0^q} - 1 & \text{if } J_1 = 0 \text{ and } J_0 t > \left(\frac{J_{-1}}{J_0} - 1\right) m(n,t) \\ & \text{i.e, if } s = 0 \text{ and } t > C_{1,1}^q \\ \frac{J_{-1}^d - J_1^q}{J_0^q} & \text{if } J_1 > 0 \text{ and } J_1 t > \left(\frac{J_{-1}-J_1}{J_0}\right) m(n,t) \\ & \text{i.e., if } s > 0 \text{ and } t > C_{2,1}^q \end{cases}$$

Because of lemma 9, (3.3.5) and (3.3.6), if $J_1 = 0$ then $J_{-1} \geq 2J_0$ and if $J_1 > 0$ then $J_{-1}-J_1 \geq J_0$.

Therefore,

$$\delta_1 \geq 1 .$$

Because of lemma 11 we do not need to consider C_1^q.

Thus, for

$$t > \begin{cases} \max(C^{q}_{2,0}, C^{q}_{1,1}, C^{\ell}_{1,1}) & \text{if } s = 0 \\ \max(C^{q}_{2,0}, C^{q}_{2,1}, C^{\ell}_{2,1}) & \text{if } s > 0 \end{cases} \tag{1}$$

α_1 and δ_1 are greater than or equal to one.

Where

$$C^{q}_{2,0} = \frac{m(n,t)}{j}$$

$$C^{q}_{1} = C^{\ell}_{2,0} = n + (n-m)\frac{(n,t)}{(\bar{n}-j)}$$

$$C^{q}_{1,1} = n + (n-m)\left[\frac{(n,t)}{j}\right]\left[\frac{\bar{n}}{j} - 1\right]$$

$$C^{\ell}_{1,1} = \frac{m(n,t)}{(\bar{n}-j)} \cdot \left[\frac{\bar{n}}{(\bar{n}-j)} - 1\right]$$

$$C^{q}_{2,1} = n + (n-m)\left[\frac{(n,t)}{j}\right]\left[\frac{\bar{n}}{J^{q}_{1}} - 1\right] \text{ and}$$

$$C^{\ell}_{2,1} = \frac{m(n,t)}{(\bar{n}-j)} \cdot \left[\frac{\bar{n}}{J^{\ell}_{1}} - 1\right].$$

Furthermore if $0 < j = J^{\ell}_{\delta} < \frac{1}{2}\bar{n} = \frac{J^{a}_{-1}}{2}$ then

$$\alpha_1 = \begin{cases} \dfrac{J^{a}_{-1}}{J^{\ell}_{\delta}} - 1 > 1 & \text{when } J_1 = 0 \\ \dfrac{J^{a}_{-1} - J^{q}_{1}}{J^{\ell}_{\delta}} > 1 & \text{when } 0 < J^{q}_{1} < J^{\ell}_{\delta} < \dfrac{J^{a}_{-1}}{2}. \end{cases}$$

Since $\frac{J^{a}_{-1} - J^{q}_{1}}{J^{\ell}_{\delta}} > \frac{J^{a}_{-1} - J^{\ell}_{\delta}}{J^{\ell}_{\delta}} = \frac{J^{a}_{-1}}{J^{\ell}_{\delta}} - 1$. Also

$$j < \frac{1}{2}\bar{n} < \bar{n} - j = J_0^q < \bar{n} - J_{-1}^q \tag{2}$$

Therefore,

$$J_1^q = J_{-1}^q - J_0^q - j > 0 . \tag{3}$$

Thus,

$$\delta_1 = 1 .$$

Therefore, we use case 2 of the algorithm.

Note that for $0 < j < \frac{1}{2}\bar{n}$

$C_{1,1}^q < \frac{m(n,t)}{j} = C_{2,0}^q$ because of (2) and

$C_{2,1}^q = \frac{m(n,t)}{j} = C_{2,0}^q$ because of (3) .

Therefore, because of (1)

$$t > \begin{cases} \max(C_{2,0}^q, C_{1,1}^q) & \text{if } s = 0 \\ (C_{2,0}^q, C_{2,1}^q) & \text{if } s > 0 \end{cases} \tag{4}$$

Similarly if $\frac{1}{2}\bar{n} < j < \bar{n}$ then

$$J_1^q = J_{-1}^q - J_0^q = \bar{n} - j > 0 \tag{5}$$

and

$$0 \leq J_1^q < \bar{n} - j < \frac{1}{2}\bar{n} < j \tag{6}$$

Thus

$$\alpha_1 = 1 ,$$

and

$$\delta_1 = \begin{cases} \dfrac{J^{\ell}_{-1}}{J^{\ell}_0} - 1 > 1 \quad \text{when } J_1 = 0, \text{ since } 0 < \bar{n} - J = J_0 < \dfrac{1}{2}\bar{n} = \dfrac{J_{-1}}{2}. \\ \dfrac{J^{\ell}_{-1} - J^{\ell}_1}{J^{\ell}_0} > 1 \quad \text{when } 0 < J_1 < J_0 < \dfrac{J_{-1}}{2}, \text{ since } \dfrac{J_{-1}-J_1}{J_0} > \dfrac{J_{-1}-J_0}{J_0} = \dfrac{J_{-1}}{J_0} - 1. \end{cases}$$

Thus, we use case 3 of the algorithm.

Note that for $\frac{1}{2}\bar{n} < j < \bar{n}$

$$C^{\ell}_{1,1} = \frac{m(n,t)}{(\bar{n}-j)} \cdot \left\lfloor \frac{j}{\bar{n}-j} \right\rfloor > \frac{m(n,t)}{(\bar{n}-j)} > \frac{m(n,t)}{j} \quad \text{because of (6)}.$$

Thus $C^{\ell}_{1,1} > C^{\ell}_{2,0}$.

$$C^{\ell}_{2,1} = n + (n-m) \cdot \frac{(n,t)}{(\bar{n}-j)} \quad \text{because of (5)}$$

Thus $C^{\ell}_{2,1} = C^{\ell}_{2,0}$.

Furthermore,

$$C^{\ell}_{1,1} = n + (n-m) \cdot \left\lfloor \frac{(n,t)}{j} \right\rfloor \cdot \left\lfloor \frac{\bar{n}}{j} - 1 \right\rfloor < C^{\ell}_{2,1} \quad \text{because of (5) and (6)}$$

and, when $J^{\ell}_1 \neq 0$,

$$C^{\ell}_{2,1} = \frac{m(n,t)}{(\bar{n}-j)} \cdot \left\lfloor \frac{\bar{n}}{J^{\ell}_1} - 1 \right\rfloor > \frac{m(n,t)}{(\bar{n}-j)} \cdot \left\lfloor \frac{\bar{n}}{(\bar{n}-j)} - 1 \right\rfloor = C^{\ell}_{1,1} \quad \text{because of (6)}.$$

Therefore, by (1)

$$t > \begin{cases} \max(C^{\ell}_{2,0}, C^{\ell}_{1,1}) & \text{if } s = 0 \\ \max(C^{\ell}_{2,0}, C^{\ell}_{2,1}) & \text{if } s > 0 \end{cases} \tag{7}$$

Finally if $j = \frac{1}{2}\bar{n}$ then $J_1^q = J_1^d = 0$ and $\alpha_1 = \delta_1 = 1$.

Therefore, we use case 1 of the algorithm.

Note that for $j = \frac{\bar{n}}{2}$

$$s^a = s^d = 0 .$$

Thus $C_{2,1}^q$ and $C_{2,1}^d$ do not exist.

Also,

$$C_{2,0}^q = C_{1,1}^d = \frac{m(n,t)}{\bar{n}/2} \quad \text{and}$$

$$C_{2,0}^d = C_{1,1}^q = n + (n-m) \cdot \frac{(n,t)}{\bar{n}/2}$$

Therefore, by (1)

$$t > \max\{C_{2,0}^q, C_{1,1}^q\} \tag{8}$$

We use induction on p for the rest of the proof.

Next let us assume $0 < j \leq \frac{1}{2}\bar{n}$. That is we deal with case 1 and case 2 of the algorithm, noting that for case 1, $s^a = 0$.

Simple calculation gives (since $x_1^q = x_1 \neq 0$):

$$x_2^s = x_0^s - \alpha_1 x_1^s = \begin{cases} x_1^s + \dfrac{m}{J_0} & \text{when } s = 0 \\ \left(\dfrac{J_1}{J_0}\right) x_1^s + \dfrac{m}{J_0} & \text{when } s > 0 \end{cases} \tag{9}$$

$$y_2^s = y_0^s - \alpha_1 y_1^s = \begin{cases} y_1^s - \dfrac{(n-m)}{J_0} & \text{when } s = 0 \\ \left(\dfrac{J_1}{J_0}\right) y_1^s - \dfrac{(n-m)}{J_0} & \text{when } s > 0 \end{cases} \tag{10}$$

$$l_1^s = l_0^s + \alpha_1 \cdot \gamma_1^s = \alpha_1 = \begin{cases} \dfrac{\bar{n}}{J_0} - 1 & \text{when } s = 0 \\ \dfrac{\bar{n} - J_1}{J_0} & \text{when } s > 0 \end{cases}$$

$$\gamma_1^s = \gamma_0^s = 1 .$$

Now if $s = 0$, then $x_2^s \geqslant x_1^s$ or if $y_2^s = 0$, the algorithm terminates with

$$x^e = x_1^s, \; y^e = y_2^s, \; m^e = m_1 = l_1^s + \gamma_1^s = \frac{\bar{n}}{J_0},$$

and (because of (4))

$$t > \begin{cases} \max(C_{2,0}^s, C_{1,1}^s) & \text{if } s = 0 \\ \max(C_{2,0}^s, C_{2,1}^s) & \text{if } y_2^s = 0 \end{cases}$$

Also because of lemma 10

$$C_{1,1}^s - C_{2,0}^s = n + (n)\left[\frac{n}{J_0 J_0} - \frac{(n,t)}{J_0}\right] - \frac{mn}{J_0 J_0} \geqslant 0 \quad \text{when}$$

$$\frac{n-m}{J_0} \geqslant (n,t) - J_0 = i_s - J_s$$

because of $(3N_4)$, when $s = 0$.

Thus, when case 2 of the algorithm is used the lemma is valid when $p = 1$, and when case 1 of the algorithm is used the lemma is proved.

If $s > 0$ and $y_2^q \neq 0$ the algorithm continues and we have:

$x_1^q > x_2^q$ when $x_1^q > \frac{m}{J_0 - J_1}$ i.e., when $t > C_2$,

$$\delta_2 = \left[\frac{x_1^q}{\frac{J_1 x_1^q + m}{J_0}} \right] = \begin{cases} \frac{J_0}{J_1} - 1 & \text{when } J_2 = 0 \text{ and } J_1 x_1^q > \left(\frac{J_0}{J_1} - 1 \right)(m) \\ & \text{i.e., when } s = 1 \text{ and } t > C_{1,2}. \\ \frac{J_0 - J_2}{J_1} & \text{when } J_2 > 0 \text{ and } J_2 x_1^q > \left(\frac{J_0 - J_2}{J_1} \right)(m) \\ & \text{i.e., when } s > 1 \text{ and } t > C_{2,2}. \end{cases}$$

Because of lemma 9, (3.3.5), if $J_2 = 0$ then $J_0 \geq 2J_1$, and because of (3.3.6), if $J_2 > 0$, then $J_0 - J_2 \geq J_1$, we have $\delta_2 \geq 1$.

Simple calculation gives:

$$x_3^q = x_1^q - \delta_2 x_2^q = \begin{cases} x_2^q - \dfrac{m}{J_1} & \text{when } s = 1 \\ \left(\dfrac{J_2}{J_1}\right) x_2^q - \dfrac{m}{J_1} & \text{when } s > 1 \end{cases} \tag{11}$$

$$y_3^q = y_1^q - \delta_2 y_2^q = \begin{cases} y_2^q + \dfrac{(n-m)}{J_1} & \text{when } s = 1 \\ \left(\dfrac{J_2}{J_1}\right) y_2^q + \dfrac{(n-m)}{J_1} & \text{when } s > 1 \end{cases} \tag{12}$$

$$\gamma_2^q = \gamma_1^q + \delta_2 \cdot l_2^q = \begin{cases} -l_2^q + \dfrac{\bar{n}}{J_1} & \text{when } s = 1 \\ -\left(\dfrac{J_2}{J_1}\right) l_2 + \dfrac{\bar{n}}{J_1} & \text{when } s > 1 \end{cases}$$

$$l_2^q = l_1^q$$

If $s = 1$, then $y_3^q \geq y_2^q$, or if $x_3^q = 0$, the algorithm terminates with

$$x^e = x_3^q,\ y^e = y_2^q,\ m^e = \gamma_2^q + l_2^q = \frac{\bar{n}}{J_1},$$

and (because of lemma 11)

$$t > \begin{cases} \max(C_{2,1}, C_{1,2}) & \text{if } s = 1 \\ \max(C_{2,1}, C_{2,2}) & \text{if } \gamma_3^q = 0 \end{cases}$$

Also because of lemma 10,

$$C_{2,1} - C_{1,2} = n + (n)\left[\frac{n}{J_0 J_1} - \frac{(n,t)}{J_0}\right] - (n)\,\frac{m}{J_1 J_1} \geq 0 \quad \text{when}$$

$$\frac{n-m}{J_1} \geq \frac{J_1(n,t)}{J_0} + \frac{n}{J_1} - \frac{n}{J_0} - J_1 = i_1 - J_1 = i_s - J_s$$

because of $(3N_4)$, when $s = 1$. Thus, when case 2 of the algorithm is used the lemma is valid when

$p = 2$.

Next suppose, when case 2 of the algorithm is used, that the lemma is valid for $2 < p \leqslant s+1$. If $p = s+1$ is odd then $x^a_{p+1} \geqslant x^a_p$ (or if $y^a_{p+1} = 0$) the algorithm terminates with $x^a = x^a_p$, $y^a = y^a_{p+1}$, $m^a = \frac{\bar{n}}{J_{p-1}}$, etc. and the proof is complete. Similarly if $p = s+1$ is even then $y^a_{p+1} \geqslant y^a_p$ (or if $x^a_{p+1} = 0$), the algorithm terminates with $x^a = x^a_{p+1}$, $y^a = y^a_p$, $m^a = \frac{\bar{n}}{J_{p-1}}$, etc. and the proof is complete.

Therefore, suppose, when case 2 of the algorithm is used, that the lemma is valid for $2 < p < s+1$ with $y^a_{p+1} \neq 0$ if p odd or $x^a_{p+1} \neq 0$ if p even.

Let p be *even* then we have:

$$y^a_p > y^a_{p+1} \text{ when } y^a_p > \frac{(n-m)}{(J_{p-1}-J_p)} \text{ using (3.3.13)}.$$

Thus when $t > C_{p+1}$ (using (3.3.7a) and (3.3.9a)).

$$\alpha_{p+1} = \left[\frac{y^a_p}{\frac{J_p y^a_p + (n-m)}{J_{p-1}}}\right] = \begin{cases} \frac{J_{p-1}}{J_p} - 1 & \text{if } J_{p+1} = 0 \text{ and } J_p y^a_p > \left[\frac{J_{p-1}}{J_p} - 1\right](n-m) \\ & \text{i.e., if } p = s \text{ and } t > C_{1,p+1} \\ \frac{J_{p-1}-J_{p+1}}{J_p} & \text{if } J_{p+1} > 0 \text{ and } J_{p+1} y^a_p > \left[\frac{J_{p-1}-J_{p+1}}{J_p}\right](n-m) \\ & \text{i.e., if } p < s \text{ and } t > C_{2,p+1} \end{cases}$$

Because of lemma 9, (3.3.5) with $p = s$, if $J_{p+1} = 0$, then $J_{p-1} \geqslant 2J_p$, or because of (3.3.6) with $p < s$, if $J_{p+1} > 0$, then $J_{p-1} - J_{p+1} \geqslant J_p$, we have $\alpha_{p+1} \geqslant 1$.

Simple calculation gives (using (3.3.11), (3.3.13), the expression for γ^a_p and by the definition of l^a_{p+1}, γ^a_{p+1}):

$$x^a_{p+2} = x^a_p - \alpha_{p+1}x^a_{p+1} = \begin{cases} x^a_{p+1} + \dfrac{m}{J_p} & \text{if } p = s \\ \left(\dfrac{J_{p+1}}{J_p}\right)x^a_{p+1} + \dfrac{m}{J_p} & \text{if } p < s \end{cases} \tag{13}$$

$$y^a_{p+2} = y^a_p - \alpha_{p+1}y^a_{p+1} = \begin{cases} y^a_{p+1} - \dfrac{(n-m)}{J_p} & \text{if } p = s \\ \left(\dfrac{J_{p+1}}{J_p}\right)y^a_{p+1} - \dfrac{(n-m)}{J_p} & \text{if } p < s\,. \end{cases} \tag{14}$$

$$l^a_{p+1} = l^a_p + \alpha_{p+1}\gamma^a_{p+1} = \begin{cases} -\gamma^a_{p+1} + \dfrac{\bar{n}}{J_p} & \text{if } p = s \\ -\left(\dfrac{J_{p+1}}{J_p}\right)\gamma^a_{p+1} + \dfrac{\bar{n}}{J_p} & \text{if } p < s \end{cases}$$

$$\gamma^a_{p+1} = \gamma^a_p\,.$$

If $p = s$, then $x^a_{p+2} \geqslant x^a_{p+1}$, or if $y^a_{p+2} = 0$, the algorithm terminates with

$$x^a = x^a_{p+1},\ y^a = y^a_{p+2},\ m^a = \frac{\bar{n}}{J_p}\,,$$

and (because of lemma 11)

$$t > \begin{cases} \max(C_{2,p}, C_{1,p+1}) & \text{if } p = s \\ \max(C_{2,p}, C_{2,p+1}) & \text{if } y^a_{p+2} = 0 \end{cases}$$

Also because of lemma 10,

$$C_{1,p+1} - C_{2,p} = n + (n)\left[n(k_{p-1}) - n(k_p) - \frac{n}{J_0} + \frac{n}{J_pJ_p}\right] - \frac{nm}{J_pJ_p} \geqslant 0$$

when $\dfrac{n-m}{J_p} \geqslant (J_pn)(k_p) - (J_pn)(k_{p-1}) + \dfrac{J_p}{J_0}(n,t) - J_p = i_p - J_p = i_s - J_s$ because of $(3N_4)$, when $p = s$.

Thus, when case 2 of the algorithm is used, the lemma is valid for $p+1$, when p is even.

Next let p be *odd* then we have:

$$x_p^a > x_{p+1}^a \text{ when } x_p^a > \frac{m}{(J_{p-1}-J_p)} \quad \text{i.e.,}$$

when $t > C_{p+1}$ (using (3.3.12a)).

$$\delta_{p+1} = \left\lfloor \frac{x_p^a}{\frac{J_p x_p^a + m}{J_{p-1}}} \right\rfloor = \begin{cases} \frac{J_{p-1}}{J_p} - 1 & \text{if } J_{p+1} = 0 \text{ and } J_p x_p^a > \left(\frac{J_{p-1}}{J_p} - 1\right) m \\ & \text{i.e., if } p = s \text{ and } t > C_{1,p+1} \\ \frac{J_{p-1} - J_{p+1}}{J_p} & \text{if } J_{p+1} > 0 \text{ and } J_{p+1} x_p^a > \left(\frac{J_{p-1} - J_{p+1}}{J_p}\right) m \\ & \text{i.e., if } p < s \text{ and } t > C_{2,p+1}. \end{cases}$$

Because of lemma 9, (3.3.5) with $p = s$, $J_{p+1} = 0$ and $J_{p-1} \geq 2J_p$, or because of (3.3.6) with $p < s$, $J_{p+1} > 0$, and $J_{p-1} - J_{p+1} \geq J_p$, we have $\delta_{p+1} \geq 1$.

Simple calculation gives (using (3.3.7), (3.3.9), the expression for γ_p^a and by the definition of l_{p+1}^a and γ_{p+1}^a):

$$x^a_{p+2} = x^a_p - \delta_{p+1}x^a_{p+1} = \begin{cases} x^a_{p+1} - \dfrac{m}{J_p} & \text{if } p = s \\ \left(\dfrac{J_{p+1}}{J_p}\right)x^a_{p+1} - \dfrac{m}{J_p} & \text{if } p < s \end{cases} \tag{15}$$

$$y^a_{p+2} = y^a_p - \delta_{p+1}y^a_{p+1} = \begin{cases} y^a_{p+1} + \dfrac{(n-m)}{J_p} & \text{if } p = s \\ \left(\dfrac{J_{p+1}}{J_p}\right)y^a_{p+1} + \dfrac{(n-m)}{J_p} & \text{if } p < s\,. \end{cases} \tag{16}$$

$$\gamma^a_{p+1} = \gamma^a_p + \delta_{p+1}l^a_{p+1} = \begin{cases} -l^a_{p+1} + \dfrac{\bar{n}}{J_p} & \text{if } p = s \\ -\left(\dfrac{J_{p+1}}{J_p}\right)l^a_{p+1} + \dfrac{\bar{n}}{J_p} & \text{if } p < s \end{cases}$$

$$l^a_{p+1} = l^a_p\,.$$

If $p = s$, then $y^a_{p+2} \geqslant y^a_{p+1}$, or if $x^a_{p+2} = 0$, the algorithm terminates with

$$x^a = x^a_{p+2},\ y^a = y^a_{p+1},\ m^a = \frac{\bar{n}}{J_p}\,,$$

and (because of lemma 11)

$$t > \begin{cases} \max(C_{2p}, C_{1,p+1}) & \text{if } p = s \\ \max(C_{2p}, C_{2,p+1}) & \text{if } x^a_{p+2} = 0 \end{cases}$$

Also because of lemma 10

$$C_{2p} - C_{1,p+1} = n + (n)\left[n(k_p) - n(k_{p-1}) - \frac{(n,s)}{J_0}\right] - \frac{nm}{J_pJ_p} \geqslant 0$$

when $\dfrac{n-m}{J_p} \geqslant (nJ_p)(k_{p-1}) - (nJ_p)(k_p) + \dfrac{J_p}{J_o}(n,s) + \dfrac{n}{J_p} - J_p = i_p - J_p = i_s - J_s$ because of $(3N_4)$, when $p = s$.

Thus, when case 2 of the algorithm is used, the lemma is valid for $p+1$, when p is odd. Thus, we have proved the lemma, when case 2 of the algorithm is used.

Next let us assume that $\frac{1}{2}\bar{n} < j < \bar{n}$. Here as noted in (7) we use case 3 of the algorithm with $t > \{C_{2,0}, C_{1,1}\}$ if $s = 0$ or $t > \{C_{2,0}, C_{2,1}\}$ if $s > 0$, and we have:

$$x_1^t = \frac{J_0 t + m(n,t)}{n}, \quad y_1^t = \frac{J_0(t-n) - (n-m)(n,t)}{n}.$$

Furthermore, simple calculation gives:

$$x_2^t = x_0^t - \delta_1 x_1^t = \begin{cases} x_1^t - \frac{m}{J_0} & \text{if } s = 0 \\ \left(\frac{J_1}{J_0}\right) x_1^t - \frac{m}{J_0} & \text{if } s > 0 \end{cases}$$

$$y_2^t = y_0^t - \delta_1 y_1^t = \begin{cases} y_1^t + \frac{(n-m)}{J_0} & \text{if } s = 0 \\ \left(\frac{J_1}{J_0}\right) y_1^t + \frac{(n-m)}{J_0} & \text{if } s > 0 \end{cases}$$

$$\gamma_1^t = \gamma_0^t + \delta_1 l_1^t = \begin{cases} \frac{\bar{n}}{J_0} - 1 = -l_1^t + \frac{\bar{n}}{J_0} & \text{if } s = 0 \\ \frac{\bar{n} - J_1}{J_0} = -\left(\frac{J_1}{J_0}\right) l_1^t + \frac{\bar{n}}{J_0} & \text{if } s > 0 \end{cases}$$

$$l_1^t = l_0^t = 1$$

If $s = 0$, then $y_2^t \geq y_1^t$, or if $x_2^t = 0$, the algorithm terminates with

$$x^d = x_2^t, \quad y^d = y_1^t, \quad m^d = l_1^t + \gamma_1^t = \frac{\bar{n}}{J_0},$$

and (because of (7))

$$t > \begin{cases} \max(C_{2,0}, C_{1,1}) & \text{if } s = 0 \\ \max(C_{2,0}, C_{2,1}) & \text{if } x_2^{\ell} = 0 . \end{cases}$$

Also because of lemma 10,

$$C_{2,0}-C_{1,1} = n+n\frac{(n,t)}{J_0} - \frac{nm}{J_0 J_0} \geqslant 0 \quad \text{when}$$

$$\frac{n-m}{J_0} \geqslant \left[\frac{n}{J_0} - (n,t)\right] - J_0 = i_s - J_s , \quad \text{because of } (3N_4) \text{ when } s = 0 .$$

Thus, when case 3 of the algorithm is used the lemma is valid when $p = 1$.

If $s > 0$ and $x_2^{\ell} \neq 0$ the algorithm continues and we have:

$$y_1^{\ell} > y_2^{\ell} \text{ when } y_1^{\ell} > \frac{n-m}{(J_0-J_1)} \text{ i.e., when } t > C_2 ,$$

$$\alpha_2 = \left[\frac{y_1^{\ell}}{\frac{J_1 y_1^{\ell}+(n-m)}{J_0}}\right] = \begin{cases} \frac{J_0}{J_1} - 1 & \text{when } J_2 = 0 \text{ and } J_1 y_1^{\ell} > \left[\frac{J_0}{J_1} - 1\right](n-m) \\ & \text{i.e., when } s = 1 \text{ and } t > C_{1,2} \\ \frac{J_0-J_2}{J_1} & \text{when } J_2 > 0 \text{ and } J_2 y_1^{\ell} > \left[\frac{J_0-J_2}{J_1}\right](n-m) \\ & \text{i.e., when } s > 1 \text{ and } t > C_{2,2} . \end{cases}$$

Because of lemma 9, (3.3.5), if $J_2 = 0$, then $J_0 \geqslant 2J_1$, and because of (3.3.6), if $J_2 > 0$, then $J_0-J_2 \geqslant J_1$ we have $\alpha_2 \geqslant 1$.

Simple calculation gives:

$$x_3^q = x_1^q - \alpha_2 x_2^q = \begin{cases} x_2^q + \dfrac{m}{J_1} & \text{if } s = 1 \\ \left(\dfrac{J_2}{J_1}\right) x_2^q + \dfrac{m}{J_1} & \text{if } s > 1 \end{cases}$$

$$y_3^q = y_1^q - \alpha_2 y_2^q = \begin{cases} y_2^q - \dfrac{(n-m)}{J_1} & \text{if } s = 1 \\ \left(\dfrac{J_2}{J_1}\right) y_2^q - \dfrac{(n-m)}{J_1} & \text{if } s > 1 \end{cases}$$

$$l_2^q = l_1^q + \alpha_2 \gamma_2^q = \begin{cases} -\gamma_2^q + \dfrac{\bar{n}}{J_1} & \text{if } s = 1 \\ -\left(\dfrac{J_2}{J_1}\right) \gamma_2^q + \dfrac{\bar{n}}{J_1} & \text{if } s > 1 , \end{cases}$$

$$\gamma_2^q = \gamma_1^q .$$

If $s = 1$, then $x_3^q \geq x_2^q$, or if $y_3^q = 0$, the algorithm terminates with

$$x^d = x_2^q,\ y^d = y_3^q,\ m^d = \gamma_2^q + l_2^q = \frac{\bar{n}}{J_1} ,$$

and (because of lemma 11)

$$t > \begin{cases} \max(C_{2,1}, C_{1,2}) & \text{if } s = 1 \\ \max(C_{2,1}, C_{2,2}) & \text{if } y_3^q = 0 . \end{cases}$$

Also because of lemma 10,

$$C_{1,2} - C_{2,1} = n + (n)\left[\frac{(n,t)}{J_0} - \frac{n}{J_0 J_1} + \frac{n}{J_1 J_1}\right] - \frac{nm}{J_1 J_1} \geq 0 \quad \text{when}$$

$$\frac{n-m}{J_1} \geq \frac{n}{J_0} - \frac{J_1(n,t)}{J_0} - J_1 = i_s - J_s , \quad \text{because of } (3N_4) \text{ when } s = 1 .$$

Thus, when case 3 of the algorithm is used, the lemma is valid when $p = 2$.

Next suppose, when case 3 of the algorithm is used, that the lemma is true for $2 < p \leqslant s+1$. If $p = s+1$ is odd, then $y^d_{p+1} \geqslant y^d_p$ (or if $x^d_{p+1} = 0$) the algorithm terminates with $x^d = x^d_{p+1}$, $y^d = y^d_p$, $m^d = \frac{\bar{n}}{J_{p-1}}$, etc. and the proof is complete. Similarly if $p = s+1$ is even, then $x^d_{p+1} \geqslant x^d_p$ (or if $y^d_{p+1} = 0$) the algorithm terminates with $x^d = x^d_p$, $y^d = y^d_{p+1}$, $m^d = \frac{\bar{n}}{J_{p-1}}$, etc and the proof is complete.

Therefore suppose, when case 3 of the algorithm is used, that the lemma is true for $2 < p < s+1$ with $x^d_{p+1} \neq 0$ if p odd and $y^d_{p+1} \neq 0$ if p even.

Let p be *even* then we have:

$$x^d_p > x^d_{p+1} \text{ when } x^d_p > \frac{m}{(J_{p-1}-J_p)} \text{ i.e.,}$$

when $t > C_{p+1}$ (using (3.3.8a)).

$$\delta_{p+1} = \left[\frac{x^d_p}{\frac{J_p x^d_p + m}{J_{p-1}}}\right] = \begin{cases} \frac{J_{p-1}}{J_p} - 1 & \text{if } J_{p+1} = 0 \text{ and } J_p x^d_p > \left(\frac{J_{p-1}}{J_p} - 1\right) m \\ & \text{i.e., if } p = s \text{ and } t > C_{1,p+1} \\ \frac{J_{p-1}-J_{p+1}}{J_p} & \text{if } J_{p+1} > 0 \text{ and } J_{p+1} x^d_p > \left(\frac{J_{p-1}-J_{p+1}}{J_p}\right) m \\ & \text{i.e., if } p < s \text{ and } t > C_{2,p+1} \end{cases}$$

By lemma 9, (3.3.5) with $p = s$, if $J_{p+1} = 0$, then $J_{p-1} \geqslant 2J_p$, or because of (3.3.6) with $p < s$, if $J_{p+1} > 0$, then $J_{p-1} - J_{p+1} \geqslant J_p$ we have $\delta_{p+1} \geqslant 1$.

Simple calculation gives (using (3.3.12), (3.3.14), the expression for l^d_p and by the definitions of l^d_{p+1}, γ^d_{p+1}):

$$x^d_{p+2} = x^d_p - \delta_{p+1}x^d_{p+1} = \begin{cases} x^d_{p+1} - \dfrac{m}{J_p} & \text{if } p = s \\ \left(\dfrac{J_{p+1}}{J_p}\right)x^d_{p+1} - \dfrac{m}{J_p} & \text{if } p < s\,. \end{cases}$$

$$y^d_{p+2} = y^d_p - \delta_{p+1}y^d_{p+1} = \begin{cases} y^d_{p+1} + \dfrac{n-m}{J_p} & \text{if } p = s \\ \left(\dfrac{J_{p+1}}{J_p}\right)y^d_{p+1} + \dfrac{n-m}{J_p} & \text{if } p < s\,. \end{cases}$$

$$\gamma^d_{p+1} = \gamma^d_p + \delta_{p+1}l^d_{p+1} = \begin{cases} -l^d_{p+1} + \dfrac{\bar{n}}{J_p} & \text{if } p = s \\ -\left(\dfrac{J_{p+1}}{J_p}\right)l^d_{p+1} + \dfrac{\bar{n}}{J_p} & \text{if } p < s \end{cases}$$

$$l^d_{p+1} = l^d_p\,.$$

If $p = s$, then $y^d_{p+2} \geqslant y^d_{p+1}$, or if $x^d_{p+2} = 0$, the algorithm terminates with

$$x^d = x^d_{p+2},\ y^d = y^d_{p+1},\ m^d = \frac{\bar{n}}{J_p}\,,$$

and (because of lemma 11)

$$t > \begin{cases} \max(C_{2,p}, C_{1,p+1}) & \text{if } p = s \\ \max(C_{2,p}, C_{2,p+1}) & \text{if } x^d_{p+2} = 0 \end{cases}$$

Also because of lemma 10,

$$C_{2,p} - C_{1,p+1} = n + (n)\left[n(k_p) - n(k_{p-1}) + \frac{(n,t)}{J_0}\right] - \frac{nm}{J_pJ_p} \geqslant 0$$

when $\frac{n-m}{J_p} \geqslant \frac{n}{J_p} - (nJ_p)(k_p) + (nJ_p)(k_{p-1}) - \frac{J_p}{J_o}(n,t) - J_p = i_s - J_s$, because of $(3N_4)$ when $p = s$.

Thus, when case 3 of algorithm is used, the lemma is true for $p+1$ when p is even.

Next let p be *odd* then we have:

$$y_p^d > y_{p+1}^d \quad \text{when } y_p^d > \frac{n-m}{(J_{p-1}-J_p)} \text{ i.e.,}$$

when $t > C_{p+1}$ (using (3.3.12a) and (3.3.14a)).

$$\alpha_{p+1} = \left\lfloor \frac{y_p^d}{\frac{J_p y_p^d + (n-m)}{J_{p-1}}} \right\rfloor = \begin{cases} \frac{J_{p-1}}{J_p} - 1 & \text{if } J_{p+1} = 0 \text{ and } J_p y_p^d > \left\lfloor \frac{J_{p-1}}{J_p} - 1 \right\rfloor \cdot (n-m) \\ & \text{i.e., if } p = s \text{ and } t > C_{1,p+1} \\ \frac{J_{p-1}-J_{p+1}}{J_p} & \text{if } J_{p+1} > 0 \text{ and } J_{p+1} y_p^d > \left\lfloor \frac{J_{p-1}-J_{p+1}}{J_p} \right\rfloor (n-m) \\ & \text{i.e., if } p < s \text{ and } t > C_{2,p+1}\,. \end{cases}$$

Because of lemma 9, (3.3.5) with $p = s$, $J_{p-1} \geq 2J_p$, or because of (3.3.6) with $p < s$, $J_{p+1} > 0$, $J_{p-1}-J_{p+1} \geq J_p$, we have $\alpha_{p+1} \geq 1$.

Simple calculation gives (using (3.3.8), (3.3.10), the expression for γ_p^d, and by the definitions of l_{p+1}^d and γ_{p+1}^d):

$$x^d_{p+2} = x^d_p - \alpha_{p+1}x^d_{p+1} = \begin{cases} x^d_{p+1} + \dfrac{m}{J_p} & \text{if } p = s \\ \left(\dfrac{J_{p+1}}{J_p}\right)x^d_{p+1} + \dfrac{m}{J_p} & \text{if } p < s\,, \end{cases}$$

$$y^d_{p+2} = y^d_p - \alpha_{p+1}y^d_{p+1} = \begin{cases} y^d_{p+1} - \dfrac{(n-m)}{J_p} & \text{if } p = s \\ \left(\dfrac{J_{p+1}}{J_p}\right)y^d_{p+1} - \dfrac{(n-m)}{J_p} & \text{if } p < s\,, \end{cases}$$

$$l^d_{p+1} = l^d_p + \alpha_{p+1}\gamma^d_{p+1} = \begin{cases} -\gamma^d_{p+1} + \dfrac{\bar{n}}{J_p} & \text{if } p = s \\ -\left(\dfrac{J_{p+1}}{J_p}\right)\gamma^d_{p+1} + \dfrac{\bar{n}}{J_p} & \text{if } p < s\,, \end{cases}$$

$$\gamma^d_{p+1} = \gamma^d_p\,.$$

If $p = s$, then $x^d_{p+2} \geqslant x^d_{p+1}$, or if $y^d_{p+2} = 0$, the algorithm terminates with

$$x^d = x^d_{p+1},\ y^d = y^d_{p+2},\ m^d = \frac{\bar{n}}{J_p}\,,$$

and (because of lemma 11)

$$t > \begin{cases} \max(C_{2,p}, C_{1,p+1}) & \text{if } p = s \\ \max(C_{2,p}, C_{2,p+1}) & \text{if } y^d_{p+2} = 0\,. \end{cases}$$

Also because of lemma 10,

$$C_{1,p+1} - C_{2,p} = n + (n)\left[n(k_{p-1}) - n(k_p) + \frac{(n,t)}{J_0} + \frac{n}{J_pJ_p}\right] - \frac{nm}{J_pJ_p} \geqslant 0$$

when $\dfrac{n-m}{J_p} \geqslant (nJ_p)(k_p) - (nJ_p)(k_{p-1}) - \dfrac{J_p}{J_o}(n,t) - J_p = i_s - J_s$, because of $(3N_4)$, when $p = s$.

Thus, when case 3 of the algorithm is used, the lemma is valid for $p+1$ when p is odd.

We use induction on p for the proof of (3.3.7a), (3.3.9a), (3.3.11a) and (3.3.13a). By (9) and (10) and by substituting values of x_1^q, y_1^q we have, when $p = 1$:

$$x_2^q = \begin{cases} x_1^q + \frac{m}{J_0} = \frac{J_0 t - m(n,t)}{n} + \frac{m}{J_0} & \text{if } p = s+1 \\ \left(\frac{J_1}{J_0}\right) x_1^q + \frac{m}{J_0} = \frac{J_1 t - \left(\frac{J_1}{J_0}\right) m(n,t)}{n} + \frac{m}{J_0} & \text{if } p < s+1 \end{cases}$$

$$y_2^q = \begin{cases} y_1^q - \frac{(n-m)}{J_0} = x_2^q + (n,t) - J_0 - \frac{n}{J_0} & \text{if } p = s+1 \\ \left(\frac{J_1}{J_0}\right) y_1^q - \frac{(n-m)}{J_0} = x_2^q + \frac{J_1}{J_0}(n,t) - J_1 - \frac{n}{J_0} & \text{if } p < s+1 \end{cases}$$

Thus, (3.3.7a) and (3.3.9a) are true if $p = 1$.

If $p = 2$, then by (11), (12) and after some calculation we have:

$$x_3^q = \begin{cases} x_2^q - \frac{m}{J_1} - \frac{J_1 t - \left(\frac{J_1}{J_0}\right) m(n,t)}{n} + \frac{m}{J_0} + \frac{m}{J_1} & \text{if } p = s+1 \\ \left(\frac{J_2}{J_1}\right) x_2^q - \frac{m}{J_1} = \frac{J_2 t - \left(\frac{J_2}{J_0}\right) m(n,t)}{n} + \frac{J_2 m}{J_0 J_1} - \frac{m}{J_1} & \text{if } p < s+1 \end{cases}$$

$$y_3^q = \begin{cases} y_2^q + \frac{n-m}{J_1} = x_3^q + \frac{J_1}{J_0}(n,t) - J_1 - \frac{n}{J_0} + \frac{n}{J_1} & \text{if } p = s+1 \\ \left(\frac{J_2}{J_1}\right) y_2^q + \frac{n-m}{J_1} = x_3^q + \frac{J_2}{J_0}(n,t) - J_2 - \frac{J_2 n}{J_0 J_1} + \frac{n}{J_1} & p < s+1 \end{cases}$$

Thus, (3.3.11a) and (3.3.13a) are true if $p = 2$.

Suppose (3.3.7a) and (3.3.9a) are valid for *odd* p with $0 < p < s+1$ then

$$x^a_{p+1} = \frac{J_p t - (\frac{J_p}{J_0}) m(n,t)}{n} + (J_p m)(k_p - k_{p-1}) \tag{17}$$

and

$$y^a_{p+1} = x^a_{p+1} + (\frac{J_p}{J_0})(n,t) - J_p - (J_p n)(k_p - k_{p-1}) \tag{18}$$

By (3.3.11) and (3.3.13) we have (since $p+1$ is *even*)

$$x^a_{p+2} = \begin{cases} x^a_{p+1} - \frac{m}{J_p} & \text{if } p = s \\ (\frac{J_{p+1}}{J_p}) x^a_{p+1} - \frac{m}{J_p} & p < s \end{cases}$$

$$= \begin{cases} \frac{J_p t - (\frac{J_p}{J_0}) m(n,t)}{n} + (J_p m)(k_p - k_{p-1}) - \frac{m}{J_p} & \text{if } p = s \\ \frac{J_{p+1} t - (\frac{J_{p+1}}{J_0}) m(n,t)}{n} + (J_{p+1} m)(k_p - k_{p+1}) & \text{if } p < s \end{cases}$$

because of (17),

and

$$y^o_{p+2} = \begin{cases} y^o_{p+1} + \dfrac{(n-m)}{J_p} & \text{if } p = s \\ (\dfrac{J_{p+1}}{J_p}) y^o_{p+1} + \dfrac{(n-m)}{J_p} & \text{if } p < s \end{cases}$$

$$= \begin{cases} x^o_{p+2} + (\dfrac{J_p}{J_0})(n,t) - J_p - (J_p n)(k_p - k_{p-1}) + \dfrac{n}{J_p} & \text{if } p = s \\ x^o_{p+2} + (\dfrac{J_{p+1}}{J_0})(n,t) - J_{p+1} - (J_{p+1} n)(k_p - k_{p+1}) & \text{if } p < s \end{cases}$$

becuase of (18).

Thus (3.3.11a) and (3.3.13a) are true for $p+1$. Similarly when p is *even* with $0 < p < s+1$ we can prove that (3.3.7a) and (3.3.9a) are valid for $p+1$, using (3.3.7) and (3.3.9).

The proof for (3.3.8a), (3.3.10a), (3.3.12a) and (3.3.14a) is similar.

Lemma 13. For $0 <$ *odd* $p \leq s+1$

$$y^o_{p+1} \not\equiv 0 \text{ and } x^d_{p+1} \not\equiv 0 \text{ if } p = s+1 \text{ and } t > C_{1,p},$$
$$\text{or if } p < s+1 \text{ and } t > C_{2,p}$$

For $0 <$ even $p \leq s+1$

$$x^o_{p+1} \not\equiv 0 \text{ and } y^d_{p+1} \not\equiv 0 \text{ if } p = s+1 \text{ and } t > C_{1,p}$$
$$\text{or if } p < s+1 \text{ and } t > C_{2,p}.$$

Proof. Suppose that for *odd* $p = s+1$, $y^o_{p+1} = 0$. Then by (3.3.9a) and (3.3.7a)

$$y^o_{p+1} = x^o_{p+1} + \frac{J_{p-1}}{J_0}(n,t) - J_{p-1} - (J_{p-1}n)(k_{p-2}) + (J_{p-1}n)(k_{p-1}) - \frac{n}{J_{p-1}}$$

$$= \frac{J_{p-1}t - \left[\dfrac{J_{p-1}}{J_0}\right] m(n,t)}{n} - (n-m)J_{p-1}\left[k_{p-2} - k_{p-1} + \frac{1}{J_{p-1}J_{p-1}}\right] + \frac{J_{p-1}}{J_0}(n,t) - J_{p-1} = 0$$

Therefore,

$$t = n+(n-m)\left[nk_{p-2}-nk_{p-1}-\frac{(n,t)}{J_0}+\frac{n}{J_{p-1}J_{p-1}}\right] = C^1_{1,p}$$

as in lemma 10.

Thus, if $t > C^1_{1,p}$, then $y^e_{p+1} \neq 0$.

Similarly because of (3.3.8a) we can show that $x^d_{p+1} \neq 0$ if $t > C^1_{1,p}$.

Next suppose that for *odd* $p < s+1$, $y^e_{p+1} = 0$. Then by (3.3.9a) and (3.3.7a),

$$y^e_{p+1} = \frac{J_p t-\left[\frac{J_p}{J_0}\right]m(n,t)}{n} - (n-m)J_p(k_p-k_{p-1}) + \frac{J_p}{J_0}(n,t) - J_p = 0$$

Therefore,

$$t = n+(n-m)\left[nk_p-nk_{p-1}-\frac{n}{J_0}\right] = C^1_{2,p}$$

as in lemma 10.

Thus, if $t > C_{2,p}$, then $y^e_{p+1} \neq 0$.

Similarly because of (3.3.8a) we can show that $x^d_{p+1} \neq 0$ if $t > C^1_{2,p}$.

Suppose that for *even* $p = s+1$, $x^e_{p+1} = 0$. Then because of (3.3.11a),

$$x^e_{p+1} = \frac{J_{p-1}t-\left[\frac{J_{p-1}}{J_0}\right]m(n,t)}{n} + (J_{p-1}m)(k_{p-1})-(J_{p-1}m)(k_{p-2}) - \frac{m}{J_{p-1}} = 0\,.$$

Therefore,

$$t = \frac{m(n,t)}{J_0} + \frac{mn}{J_{p-1}J_{p-1}} + (mn)(k_{p-2}-k_{p-1}) = C^1_{1,p}$$

as in lemma 10.

Thus, if $t > C^{e}_{1,p}$, then $x^{e}_{p+1} \neq 0$.

Similarly because of (3.3.14a) and (3.3.12a) we can show that $y^{d}_{p+1} \neq 0$ if $t > C^{d}_{1,p}$.

Finally suppose that for *even* $p < s+1$, $x^{e}_{p+1} = 0$. Then because of (3.3.11a)

$$x^{e}_{p+1} = \frac{J_p t - \left\lfloor \frac{J_p}{J_0} \right\rfloor m(n,t)}{n} + (J_p m)(k_{p-1}) - (J_p m)(k_p) = 0$$

Therefore,

$$t = \frac{m(n,t)}{J_0} + (mn)(k_p - k_{p-1}) = C^{e}_{2,p} .$$

as in lemma 10.

Thus, if $t > C^{e}_{2,p}$, then $x^{e}_{p+1} \neq 0$.

Similarly because of (3.3.14a) and (3.3.12a) we can show that $y^{d}_{p+1} \neq 0$ if $t > C^{d}_{2,p}$.

Lemma 14. If $0 \leq p < s$ then

$$i^{e}_{p+1} = \begin{cases} \left\lfloor \frac{J_{p+1}}{J_p} \right\rfloor \left\lfloor i_p - \frac{n}{J_p} \right\rfloor + \frac{n}{J_p} & \text{if } p \text{ odd} \\ \left\lfloor \frac{J_{p+1}}{J_p} \right\rfloor (i_p) + \frac{n}{J_{p+1}} - \frac{n}{J_p} & \text{if } p \text{ even} \end{cases}$$

and

$$i^d_{p+1} = \begin{cases} \left(\frac{J_{p+1}}{J_p}\right)(i_p) + \frac{n}{J_{p+1}} - \frac{n}{J_p} & \text{if } p \text{ odd} \\ \left(\frac{J_{p+1}}{J_p}\right)\left(i_p - \frac{n}{J_p}\right) + \frac{n}{J_p} & \text{if } p \text{ even} \end{cases}$$

Proof. For *odd* p using $(3N_4)$ and simple calculation we have:

$$\begin{aligned} i^a_{p+1} &= (J_{p+1}n)(k_{p+1}) - (J_{p+1}n)(k_p) + \frac{J_{p+1}}{J_0}(n,t) \\ &= \left(\frac{J_{p+1}}{J_p}\right)(J_pn)(k_{p-1}) + \frac{n}{J_p} - \left(\frac{J_{p+1}}{J_p}\right)(J_pn)(k_p) + \left(\frac{J_{p+1}}{J_p}\right)\left(\frac{J_p}{J_0}(n,t)\right) \\ &= \left(\frac{J_{p+1}}{J_p}\right)\left(i_p - \frac{n}{J_p}\right) + \frac{n}{J_p}, \end{aligned}$$

because $i^a_p = (J_pn)(k_{p-1}) - (J_pn)(k_p) + \frac{J_p}{J_0}(n,t) + \frac{n}{J_p}$

Also for *even* p using $(3N_4)$ we have:

$$\begin{aligned} i^a_{p+1} &= (J_{p+1}n)(k_p) - (J_{p+1}n)(k_{p+1}) + \left(\frac{J_{p+1}}{J_0}\right)(n,t) + \frac{n}{J_{p+1}} \\ &= \left(\frac{J_{p+1}}{J_p}\right)(J_pn)(k_p) - \left(\frac{J_{p+1}}{J_p}\right)(J_pn)(k_{p-1}) - \frac{n}{J_p} + \left(\frac{J_{p+1}}{J_p}\right)\left(\frac{J_p}{J_0}(n,t)\right) + \frac{n}{J_{p+1}} \\ &= \left(\frac{J_{p+1}}{J_p}\right)(i_p) + \frac{n}{J_{p+1}} - \frac{n}{J_p}, \end{aligned}$$

because $i^a_p = (J_pn)(k_p) - (J_pn)(k_{p-1}) + \left(\frac{J_p}{J_0}\right)(n,t)$.

Similar calculations give a proof for the corresponding result for i^d_{p+1}.

Lemma 15. If $0 \leq p \leq s$ then for case 2 of the algorithm (i.e., when $0 < j < \frac{\bar{n}}{2}$)

$$0 < i_p < \frac{n}{J_s} \quad \text{if } p = s, \text{ or even } p < s,$$

and

$$0 < i_p < \frac{n}{J_s} + \frac{n}{J_p} \quad \text{if odd } p < s,$$

Proof. We use induction on p. Suppose $p = 0$. Then because of $(3N_4)$ and (3.3.3),

$$0 < i_0 - (n,t) < \frac{n}{J_s}.$$

Thus, the lemma holds when $p = 0$.

Suppose $p = 1$. Then because of the lemma 14

$$i_1 = \left[\frac{J_1}{J_0}\right](i_0) + \frac{n}{J_1} - \frac{n}{J_0}$$

By substituting bounds for i_0 we have: (note that $0 < J_1 < J_0$).

If $s = 1$, then

$$0 < \frac{n}{J_1} - \frac{n}{J_0} < i_1 < \frac{n}{J_1}$$

If $s > 1$, then

$$0 < \frac{n}{J_1} - \frac{n}{J_0} < i_1 < \left[\frac{J_1}{J_0}\right]\left[\frac{n}{J_s}\right] + \frac{n}{J_1} - \frac{n}{J_0} < \frac{n}{J_s} + \frac{n}{J_1}.$$

Thus, the lemma holds when $p = 1$.

Suppose the lemma is valid for $p < s$.

Then for *odd* p we have:

$$0 < i_p < \frac{n}{J_s} + \frac{n}{J_p}.$$

Because of lemma 14

$$i_{p+1} = \left\lfloor \frac{J_{p+1}}{J_p} \right\rfloor (i_p) + \frac{n}{J_p} - \left\lfloor \frac{J_{p+1}}{J_p} \right\rfloor \left\lfloor \frac{n}{J_p} \right\rfloor .$$

By substituting bounds for i_p we have: If $p+1 = s$, then

$$0 < \frac{n}{J_p} - \frac{J_{p+1} n}{J_p J_p} < i_{p+1} < \frac{2n}{J_p} \leq \frac{n}{J_s} .$$

The first inequality holds because $0 < J_{p+1} < J_p$, and the last inequality holds because of (3.3.5).

If $p+1 < s$, then

$$0 < \frac{n}{J_p} - \frac{J_{p+1} n}{J_p J_p} < i_{p+1} < \frac{J_{p+1}}{J_p} \cdot \frac{n}{J_s} + \frac{n}{J_p} = \frac{n}{J_p} \left\lfloor \frac{J_{p+1} + J_s}{J_s} \right\rfloor \leq \frac{n}{J_s} .$$

The last inequality holds because of (3.3.4).

Thus, the lemma is valid for $p+1$ when p is odd.

Similarly for p even we have:

$$0 < i_p < \frac{n}{J_s} .$$

Because of lemma 14,

$$i_{p+1} = \left\lfloor \frac{J_{p+1}}{J_p} \right\rfloor (i_p) + \frac{n}{J_{p+1}} - \frac{n}{J_p} .$$

By substituting bounds for i_p we have: If $p+1 = s$, then

$$0 < \frac{n}{J_{p+1}} - \frac{n}{J_p} < i_{p+1} < \frac{n}{J_s} .$$

The first inequality holds because $0 < J_{p+1} < J_p$.

If $p+1 < s$, then

$$0 < \frac{n}{J_{p+1}} - \frac{n}{J_p} < i_{p+1} < \left\lfloor \frac{J_{p+1}}{J_p} \right\rfloor \left\lfloor \frac{n}{J_s} \right\rfloor + \frac{n}{J_{p+1}} - \frac{n}{J_p} < \frac{n}{J_s} + \frac{n}{J_{p+1}} .$$

The last inequality holds because $0 < J_{p+1} < J_p$ and because $\frac{n}{J_p}$ is positive.

Thus, the lemma is valid for $p+1$ when p is even.

Lemma 16. If $0 \leq p \leq s$, then for case 3 of algorithm (i.e., when $\frac{\bar{n}}{2} < j < \bar{n}$)

$$0 < i_p < \frac{n}{J_s} \quad \text{if } p = s .$$

$$-\frac{n}{J_s} < i_p < \frac{n}{J_s} \quad \text{if } p \text{ odd} < s \text{ and}$$

$$\frac{n}{J_p} - \frac{n}{J_s} < i_p < \frac{n}{J_p} + \frac{n}{J_s} \quad \text{if } p \text{ even} < s .$$

Proof. We use induction on p. Suppose $p = 0$. Then because of $(3N_4)$ and (3.3.3),

$$\frac{n}{J_0} - \frac{n}{J_s} < i_0 = \frac{n}{J_0} - (n,s) < \frac{n}{J_0} .$$

If $s = 0$ then,

$$0 < i_0 < \frac{n}{J_0} .$$

If $s > 0$ then,

$$\frac{n}{J_0} - \frac{n}{J_s} < i_0 < \frac{n}{J_0} < \frac{n}{J_0} + \frac{n}{J_s}$$

Thus, the lemma is valid when $p = 0$.

Suppose $p = 1$. Then because of lemma 14

$$i_1 = \left\lfloor \frac{J_1}{J_0} \right\rfloor (i_0) + \frac{n}{J_0} - \left\lfloor \frac{J_1}{J_0} \right\rfloor \left\lfloor \frac{n}{J_0} \right\rfloor$$

By substituting bounds for i_0 we have:

If $s = 1$, then

$$\left(\frac{J_1}{J_0}\right)\left(\frac{n}{J_0} - \frac{n}{J_1}\right) + \frac{n}{J_0} - \frac{J_1 n}{J_0 J_0} = 0 < i_1 < \left(\frac{J_1}{J_0}\right)\left(\frac{n}{J_0} + \frac{n}{J_1}\right) + \frac{n}{J_0} - \frac{J_1 n}{J_0 J_0} = \frac{2n}{J_0} \leqslant \frac{n}{J_1}.$$

The last inequality is true because of (3.3.5).

If $s > 1$, then since

$$\left(\frac{J_1}{J_0}\right)\left(\frac{n}{J_0} - \frac{n}{J_s}\right) + \frac{n}{J_0} - \frac{J_1 n}{J_0 J_0} = \frac{n}{J_0} - \frac{J_1}{J_0}\frac{n}{J_s},$$

$$-\frac{n}{J_s} < \frac{n}{J_0} - \frac{n}{J_s} < \frac{n}{J_0} - \frac{J_1}{J_0}\frac{n}{J_s} < i_1 < \left(\frac{J_1}{J_0}\right)\left(\frac{n}{J_0} + \frac{n}{J_s}\right) + \frac{n}{J_0} - \frac{J_1}{J_0}\frac{n}{J_0} = \left(\frac{n}{J_0}\right)\left(\frac{J_1 + J_s}{J_s}\right) \leqslant \frac{n}{J_s}.$$

The second inequality holds because $0 < J_1 < J_0$ and the last inequality holds because of (3.3.4) — i.e., $J_0 \geqslant J_1 + J_s$. Thus, the lemma is valid when $p = 1$.

Suppose the lemma is valid for $p < s$.

Then for *odd* p we have:

$$-\frac{n}{J_s} < i_p < \frac{n}{J_s}.$$

Because of lemma 14

$$i_{p+1} = \left(\frac{J_{p+1}}{J_p}\right)(i_p) + \frac{n}{J_{p+1}} - \frac{n}{J_p}.$$

By substituting bounds for i_p, we have:

If $s = p+1$, then

$$0 \leqslant \frac{n}{J_{p+1}} - \frac{2n}{J_p} < i_{p+1} < \frac{n}{J_{p+1}}.$$

The first inequality holds because of (3.3.5).

If $s > p+1$, then

$$\left(\frac{J_{p+1}}{J_p}\right)\left(-\frac{n}{J_s}\right) + \frac{n}{J_{p+1}} - \frac{n}{J_p} = \frac{n}{J_{p+1}} - \left(\frac{n}{J_p}\right)\left(\frac{J_{p+1}+J_s}{J_s}\right) < i_{p+1}$$

$$< \left(\frac{J_{p+1}}{J_p}\right)\left(\frac{n}{J_s}\right) + \frac{n}{J_{p+1}} - \frac{n}{J_p} = \frac{n}{J_{p+1}} + \left(\frac{n}{J_p}\right)\left(\frac{J_{p+1}-J_s}{J_s}\right)$$

i.e., $\frac{n}{J_{p+1}} - \frac{n}{J_s} < i_{p+1} < \frac{n}{J_{p+1}} + \frac{n}{J_s}$.

The inequalities hold because of (3.3.4). Thus, the lemma is valid for $p+1$ when p is odd.

Similarly for even p we have:

$$\frac{n}{J_p} - \frac{n}{J_s} < i_p < \frac{n}{J_p} + \frac{n}{J_s}.$$

Because of lemma 14,

$$i_{p+1} = \left(\frac{J_{p+1}}{J_p}\right)(i_p) + \frac{n}{J_p} - \left(\frac{J_{p+1}}{J_p}\right)\left(\frac{n}{J_p}\right).$$

By substituting bounds for i_p we have:

If $s = p+1$, then

$$\left(\frac{J_{p+1}}{J_p}\right)\left(\frac{n}{J_p} - \frac{n}{J_{p+1}}\right) + \frac{n}{J_p} - \left(\frac{J_{p+1}}{J_p}\right)\left(\frac{n}{J_p}\right) = 0 < i_{p+1},$$

$$< \left(\frac{J_{p+1}}{J_p}\right)\left(\frac{n}{J_p} + \frac{n}{J_{p+1}}\right) + \frac{n}{J_p} - \left(\frac{J_{p+1}}{J_p}\right)\left(\frac{n}{J_p}\right) = \frac{2n}{J_p} \leq \frac{n}{J_{p+1}}$$

i.e., $0 < i_{p+1} < \frac{n}{J_{p+1}}$.

The last inequality holds because of (3.3.5).

If $s > p+1$, then since

$$\left\lfloor \frac{J_{p+1}}{J_p} \right\rfloor \left(\frac{n}{J_p} - \left\lfloor \frac{n}{J_s} \right\rfloor \right) + \left\lfloor \frac{n}{J_p} \right\rfloor - \left\lfloor \frac{J_{p+1}}{J_p} \right\rfloor \left\lfloor \frac{n}{J_p} \right\rfloor = \frac{n}{J_p} - \frac{J_{p+1}}{J_p} \left\lfloor \frac{n}{J_s} \right\rfloor ,$$

we have

$$- \frac{n}{J_s} < \frac{n}{J_p} - \left\lfloor \frac{n}{J_s} \right\rfloor < \frac{n}{J_p} - \frac{J_{p+1}}{J_p} \left\lfloor \frac{n}{J_s} \right\rfloor < i_{p+1} <$$

$$\left\lfloor \frac{J_{p+1}}{J_p} \right\rfloor \left(\frac{n}{J_p} + \left\lfloor \frac{n}{J_s} \right\rfloor \right) + \left\lfloor \frac{n}{J_p} \right\rfloor - \left\lfloor \frac{J_{p+1}}{J_p} \right\rfloor \left\lfloor \frac{n}{J_p} \right\rfloor - \left\lfloor \frac{n}{J_p} \right\rfloor \left\lfloor \frac{J_{p+1}+J_s}{J_s} \right\rfloor \leq \frac{n}{J_s} .$$

The second inequality holds because $0 < J_{p+1} < J_p$ and the last inequality holds because of (3.3.4).

Thus, the lemma is valid for $p+1$ when p is even. This completes the proof for Lemma 16.

3.4 PROOF OF THE MAIN THEOREM

Because of Johnson's reduction formula (1.2.3)

$$g(t-n,t-m,t) = (n,t) \cdot g\left(\frac{t-n}{(n,t)}, \frac{t}{(n,t)}, t-m \right) + ((n,t)-1)(t-m)$$

Thus, when case 2 of the algorithm is used with $a_1 = \frac{t-n}{(n,t)}$, $a_2 = \frac{t}{(n,t)}$, $a_3 = t-m$, we have:

$$g(t-n,t-m,t) =$$

$$(n,t) \cdot \left\{ (m^e-1)(t-m) + \max\left[(x^e)\left\lfloor \frac{t-n}{(n,t)} \right\rfloor, (y^e)\left\lfloor \frac{t}{(n,t)} \right\rfloor \right] - \frac{2(t-n)+n}{(n,t)} \right\} + ((n,t)-1)(t-m)$$

Because of lemma 11, lemma 12 and lemma 13,

$$\text{for } t > \max\{C_{2,s}, C_{1,s+1}\} \text{ we have } m^e = \frac{\bar{n}}{J_s} .$$

Therefore,

$$\therefore \quad g(t-n,t-m,t) =$$

$$\left(\frac{n}{J_s} - (n,t) \right)(t-m) + \max\{(x^e)(t-n), (y^e)(t)\} - 2(t-n) - n + ((n,t)-1)(t-m)$$

$$= \begin{cases} \left(\frac{J_s t - i_s m}{n} + \frac{n}{J_s} - 3\right)(t-n) + (n-m)\left(\frac{n}{J_s} - 1\right) - n & \text{if } 0 < i_s \leqslant \frac{n-m}{J_s} \\ \left(\frac{J_s t - i_s m}{n} + i_s + \frac{m}{J_s} - 3\right)(t-n) + (n-m)(i_s - 1) - n & \frac{n-m}{J_s} < i_s < \frac{n}{J_s}, \end{cases}$$

because of the following (1), (2) and (3).

(1) $$(t-m) = (t-n) + (n-m),\ t = (t-n) + n .$$

(2) *If* s is *even* then because of lemma 12 and lemma 13 (note that $s+1$ is odd) we have:

$$x^a = x^a_{s+1} , y^a = y^a_{s+2} .$$

Thus,

$$(x^a)(t-n) - (y^a)(t) = (x^a_{s+1})(t-n) - (y^a_{s+2})(t)$$

$$= (x^a_{s+1})(t-n) - \left(x^a_{s+1} + \frac{J_s}{J_0}(n,t) - J_s - (J_s n)(k_{s-1}) + (J_s n)(k_s) - \frac{n-m}{J_s}\right)(t) ,$$

because of (3.3.9a) and (3.3.7).

$$= (-n)\left(\frac{J_s t - \left(\frac{J_s}{J_0}\right) m(n,t)}{n} + (J_s m)(k_{s-1}) - (J_s m)(k_s)\right)$$

$$- \left(\frac{J_s}{J_0}(n,t) - J_s - (J_s n)(k_{s-1}) + (J_s n)(k_s) - \frac{n-m}{J_s}\right)(t) \quad \text{because of (3.3.11a) noting that } s < s+1$$

$$= \left(\frac{n-m}{J_s} + (J_s n)(k_{s-1}) - (J_s n)(k_s) - \frac{J_s}{J_0}(n,t)\right)(t)$$

$$+ \left(\frac{J_s}{J_0} m(n,t) + (J_s mn)(k_s) - (J_s mn)(k_{s-1})\right)$$

$$= \left(\frac{n-m}{J_s} - i_s\right)(t) + i_s m \quad \text{because of } (3N_4)$$

> 0 when $\frac{n-m}{J_s} \geqslant i_s$. (Note that $i_s > 0$ because of lemma 15.)

Also

(3.4.1) $x^a = x^a_{s+1} = \dfrac{J_s t - i_s m}{n}$ because of $(3N_4)$ and (3.3.11a) .

$y^a = y^a_{s+2} = x^a_{s+1} + i_s - J_s - \dfrac{n-m}{J_s}$, because of $(3N_4)$ and (3.3.9a) ,

and

$$(y^a_{s+2})(t) = \left[x^a_{s+1} + i_s - \frac{n-m}{J_s}\right](t-n) + i_s(n-m) - \frac{n}{J_s}(n-m) .$$

(3) if s is *odd* then because of lemma 12 and lemma 13 (note that $s+1$ is even) we have:

$$x^a = x^a_{s+2},\ y^a = y^a_{s+1} .$$

Thus,

$$(x^a)(t-n)-(y^a)(t) = (x^a_{s+2})(t-n) - (y^a_{s+1})(t)$$

$= (x^a_{s+2})(t-n)-(x^a_{s+2} + \dfrac{m}{J_s} + \dfrac{J_s}{J_0}(n,t) - J_s - (J_s n)(k_s) + (J_s n)(k_{s-1})(t))$ because of (3.3.9a) and (3.3.11).

$$= -(n)\left[\frac{J_s t - \left[\frac{J_s}{J_0}\right] m(n,t)}{n} + (J_s m)(k_s) - (J_s m)(k_{s-1}) - \frac{m}{J_s}\right] - \left[\frac{m}{J_s} - \frac{n}{J_s} + i_s - J_s\right](t)$$

because of (3.3.11a), and $(3N_4)$.

$= \left[\dfrac{n-m}{J_s} - i_s\right](t) + i_s m$ because of $(3N_4)$.

> 0 when $\dfrac{n-m}{J_s} \geqslant i_s$. (Note that $\dfrac{n}{J_s} > i_s > 0$ because of lemma 15.) Also

(3.4.2) $$x^e = x^e_{s+2} = \frac{J_s t - i_s m}{n}\ ,\ \text{because of } (3N_4) \text{ and } (3.3.11a)\ .$$

$$y^e = y^e_{s+1} = x^e_{s+2} + i_s - J_s - \frac{(n-m)}{J_s}\ ,$$

and

$$(y^e_{s+1})(t) = \left[x^e_{s+2} + i_s - \frac{(n-m)}{J_s}\right](t-n) + i_s(n-m) - \frac{n}{J_s}(n-m)\ .$$

Similarly we also obtain the same $g(t-n,t-m,t)$ when case 3 of the algorithm is used.

Also note that $0 < i_s < \frac{n}{J_s}$ as in lemma 15 or lemma 16. The following results, i.e., lemma 17, lemma 18, lemma 19 (the special case of $j = 0$) and lemma 20 (the special case of $j = \frac{\bar{n}}{2}$) will complete the proof.

Lemma 17. $i = i_s$ where i is defined by $t \equiv i\ \frac{m}{(m,n)} \mod (\frac{n}{(m,n)})$ as in Chapter 3.2, with $0 < i \leq \frac{n}{(m,n)}$.

Proof. When case 2 of the algorithm is used

$$x^e = \frac{J_s t - i_s m}{n} \quad \text{because of (3.4.1) or (3.4.2)}\ .$$

Thus,

$$t = (x^e)\left[\frac{n}{J_s}\right] + \frac{i_s m}{J_s}\ .$$

Therefore,

$$t \equiv i_s\ \frac{m}{J_s} \quad \left[\mod \left[\frac{n}{J_s}\right]\right]$$

where $J_s = (m,n)$ because of (3.3.2) .

Similarly, when case 3 of the algorithm is used we would also have

$$i \equiv i_s \frac{m}{(m,n)} \left[\mod \left[\frac{n}{J_s} \right] \right].$$

Thus $i = i_s$, by lemma 15 and 16.

Note that if we take $i = 0$ then $g(t-n,t-m,t)$ given by (B1) in (3.2.1) is same as $g(t-n,t-m,t)$ given by (B2) in (3.2.1) when $i = \frac{n}{(m,n)}$.

Lemma 18.

$$C^q_{i,s} = \begin{cases} n + \left(\frac{n-m}{J_s}\right)\left(\frac{n}{J_s} - i_s\right) & \text{if } s \text{ odd} \\ \left(\frac{i_s}{J_s}\right)(m) & \text{if } s \text{ even} \end{cases}$$

$$C^q_{i,s+1} = \begin{cases} \left(\frac{i_s}{J_s}\right)(m) & \text{if } s \text{ odd} \\ n + \left(\frac{n-m}{J_s}\right)\left(\frac{n}{J_s} - i_s\right) & \text{if } s \text{ even} \end{cases}$$

and

$$C^q_{i,s} = \begin{cases} \left(\frac{i_s}{J_s}\right)(m) & \text{if } s \text{ odd} \\ n + \left(\frac{n-m}{J_s}\right)\left(\frac{n}{J_s} - i_s\right) & \text{if } s \text{ even} . \end{cases}$$

$$C^q_{i,s+1} = \begin{cases} n + \left(\frac{n-m}{J_s}\right)\left(\frac{n}{J_s} - i_s\right) & \text{if } s \text{ odd} \\ (m)\left(\frac{i_s}{J_s}\right) & \text{if } s \text{ even} \end{cases}$$

Proof. Because of lemma 10 and ($3N_4$) we have:

$$C^{q}_{2,s} = \begin{cases} n+(n-m)\left[nk_s - nk_{s-1} - \dfrac{(n,t)}{J_0}\right] = n+\left[\dfrac{n-m}{J_s}\right]\left[\dfrac{n}{J_s} - i_s\right] & \text{if } s \text{ odd} \\ (m)\left[nk_s - nk_{s-1} + \dfrac{(n,t)}{J_0}\right] = (m)\left[\dfrac{i_s}{J_s}\right] & \text{if } s \text{ even} \end{cases}$$

$$C^{q}_{1,s+1} = \begin{cases} (m)\left[nk_{s-1} - nk_s + \dfrac{n}{J_s J_s} + \dfrac{(n,t)}{J_0}\right] = (m)\left[\dfrac{i_s}{J_s}\right] & \text{if } s \text{ odd} \\ n+(n-m)\left[nk_{s-1} - nk_s + \dfrac{n}{J_s J_s} - \dfrac{(n,t)}{J_0}\right] = n + \left[\dfrac{n-m}{J_s}\right]\left[\dfrac{n}{J_s} - i_s\right] & \text{if } s \text{ even} \end{cases}$$

Similarly, $C^{q}_{2,s}$ and $C^{q}_{1,s+1}$ can be found.

Lemma 19. Suppose we allow $j = 0$ in $(3A_3)$. Then $(m,n) = \bar{n}$, $t = 0$ and

$$g(t-n,t-m,t) = \left[\frac{\bar{n}\cdot t}{n} + \frac{n}{\bar{n}} - 3\right](t-n) + (n-m)\left[\frac{n}{\bar{n}} - 1\right] - n$$

Proof.

$$m = 0 \pmod{\bar{n}} \quad \text{because } j = 0 \text{ in } (3A_3)\,. \tag{1}$$

Also

$$t \equiv 0 \left[\bmod \frac{n}{\bar{n}}\right] \quad \text{because} \quad (n,t) = \frac{n}{\bar{n}}\,, \tag{2}$$

and

$$(n,t) > 1 \tag{3}$$

because if $(n,t) = 1$ then $m \equiv 0 \pmod{n}$ — not possible since $0 < m < n$.

Furthermore,

$$(\bar{n},(n,t)) = 1$$

and

$$\left(\frac{m}{\bar{n}}, (n,t)\right) = 1$$

because of $(3A_1)$ and (1).

Therefore,

$$(m,n) = \bar{n} . \tag{4}$$

Thus

$$t = 0$$

because of (2) and (4).

Noting that

$$\left(\frac{t-n}{(n,t)}, \frac{t}{(n,t)}\right) = 1 ,$$

set

$$a_1 = \frac{t-n}{(n,t)} , \quad a_2 = \frac{t}{(n,t)} .$$

Then

$$a_3 = t-m = \left(\frac{m}{\bar{n}}\right)a_1 + \left(\frac{n-m}{\bar{n}}\right)a_2 .$$

Thus, a_3 is a linear combination of a_1,a_2 with positive coefficients.

Therefore,

$$g(a_1,a_2,a_3) = g(a_1,a_2) = (a_1-1)(a_2-1) - 1$$

and using Johnson's Reduction formula (1.2.3) we have:

$$g(t-n,t-m,t) = (n,t)\{(a_1-1)(a_2-1)-1\} + ((n,t)-1)(t-m)$$
$$= \left\lfloor \frac{\bar{n}t}{n} + \frac{n}{\bar{n}} - 3 \right\rfloor (t-n) + (n-m)\left\lfloor \frac{n}{\bar{n}} - 1 \right\rfloor - n \cdot$$
$$\left\lfloor \frac{n-m}{\bar{n}} \right\rfloor \left\lfloor \frac{n}{\bar{n}} \right\rfloor .$$

Note that the case $\frac{n}{(n,t)} = 1$ is covered here, because $m \equiv 0 \pmod{\frac{n}{(n,t)}}$ gives $j = 0$.

Lemma 20. Suppose $j = \frac{\bar{n}}{2}$. Then $(m,n) = J_0$, $i = (n,t)$ and

$$g(t-n,t-m,t) = \begin{cases} \left\lfloor \frac{J_0 t - m(n,t)}{n} + \frac{n}{J_0} - 3 \right\rfloor (t-n) + (n-m)\left\lfloor \frac{n}{J_0} - 1 \right\rfloor - n & \text{if } 0 < (n,t) \leqslant \frac{n-m}{J_0} \\ \left\lfloor \frac{J_0 t - m(n,t)}{n} + \frac{m}{J_0} + (n,t) - 3 \right\rfloor (t-n) + (n-m)\left\lfloor (n,t)-1 \right\rfloor - n & \text{if } \frac{n-m}{J_0} < (n,t) < \frac{n}{J_0} . \end{cases}$$

Proof. $J_0^{\delta} = J_0^{\delta'}$ since $j_0^{\delta} = j$ and $j_0^{\delta'} = \bar{n} - j = j$.

Also $J_1 = 0$ since $\bar{n} = 2J_0$

Thus, $s = 0$ and $(m,n) = J_0$ because of (3.3.2).

As in lemma 12 we use case 1 of the algorithm with

$$x_1 = x_1^{\delta} = \frac{J_0 t - m(n,t)}{n}, \quad a_1 - y_1 = y_1^{\delta} = \frac{(\bar{n}-J_0)(t-n)-(n,t)(n-m)}{n}$$

Therefore,

$$t \equiv (n,t) \cdot \frac{m}{J_0} \left[\bmod \frac{n}{J_0} \right]$$

giving

$$t = (n,t) .$$

Also $g(t-n,t-m,t) = (n,t)g\left(\frac{t-n}{(n,t)},\frac{t}{(n,t)},t-m\right) + ((n,t)-1)(t-m)$ because of Johnson's reduction formula (1.2.3). i.e.,

$g_3 = (n,t)(t-m) + \max\{(x_1)(t-n),(a_1-y_1)(t)\} - 2(t-n)-n + ((n,t)-1)(t-m)$ as in the algorithm .

$$= \begin{cases} \left(\frac{J_0t-m(n,t)}{n} + \frac{n}{J_0} - 3\right)(t-n) + (n-m)\left(\frac{n}{J_0} - 1\right) - n & \text{for } 0 < (n,t) \leqslant \frac{n-m}{J_0} \\ \left(\frac{J_0t-m(n,t)}{n} + \frac{m}{J_0} + (n,t) - 3\right)(t-n) + (n-m)((n,t)-1) - n & \text{for } \frac{n-m}{J_0} < (n,t) < \frac{n}{J_0} \end{cases}$$

because of the following expressions (1), (2), (3).

(1) $$(x_1)(t-n)-(a_1-y_1)(t) = \frac{1}{n}\cdot(n,t)\cdot(n-2m)(t)+mn(n,t)] \geqslant 0 ,$$

when $2m \leqslant n$ i.e., when $\frac{n}{2} \leqslant n-m$. Thus $(x_1)(t-n)$ is maximum when $0 < (n,t) \leqslant \frac{n-m}{J_0}$

(2) $$0 < (n,t) < \frac{n}{J_0} \quad \text{as in (3.3.3)}$$

(3) $$(a_1-y_1)(t) = \left(\frac{J_0t-m(n,t)}{n} + \frac{m}{J_0} - (n,t)\right)(t-n) - (n,t)(n-m) .$$

Corollary 4. When $n = 2$ and $m = 1$ then $(m,n) = 1$, $\frac{n-m}{(m,n)} = 1$ and the formula gives:

$$g(t, t+1, t+2) = \begin{cases} (\frac{t+2}{2} - 1)(t) - 1 = \frac{t^2}{2} - 1 & \text{when } t \equiv 0 \bmod 2 \\ & \text{and } t > 2 . \\ (\frac{t+1}{2} - 1)(t) - 1 = \frac{t^2-t}{2} - 1 & \text{when } t \equiv 1 \bmod 2 \\ & \text{and } t > 1 . \end{cases}$$

and Brauer's [2] formula (1.3.1) follows.

Corollary 5. When $n = z > 2$ and $m = z - 1$ then $(m,n) = 1$, $\frac{n-m}{(m,n)} = 1$ and the formula gives:

$$g(t, t+1, t+z) = \begin{cases} (\frac{t+1}{z} + z - 3)(t) - 1 & \text{when } i = 1 \text{ (i.e. } t \equiv z-1 \bmod z) \\ & \text{and } t > z-1 . \\ (\frac{t+i}{z} + z - 3)t + i - z - 1 & \text{when } 1 < i \leqslant z \\ & \text{(i.e. } t \equiv i(z-1) \equiv -i \bmod z) \text{ and} \\ & t + z > \max\{z+(z-i),(i)(z-1)\} \end{cases}$$

and Robert's [32] formula (1.3.2) follows when we note that

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

Corollary 6. When $n = yz$, $m = (z-1)y$ with $z \geqslant 0$ and y any integer then $(m,n) = y$, $\frac{n-m}{y} = 1$ and the formula gives

$$g(t, t+y, t+yz) = \begin{cases} (\frac{t+yz-(z-1)}{z} + z - 3)(t) + y(z-1) - yz & \text{when } i=1 \text{ (i.e. } t \equiv z-1 \bmod z) \\ & \text{and } t > z-1. \\ (\frac{t+yz+i}{z} + z - 4)(t) + y(i-1) - yz & \text{when } t \equiv i(z-1) \equiv -i \pmod z \text{ with } 1 < i \leqslant z \\ & \text{and } t + yz > \max\{yz+y\cdot(z-i), (i)\cdot(z-1)\} \end{cases}$$

If we use G. R. Hofmeister's formula (1.3.6) to derive $g(t, t+y, t+yz)$ we derive the same formula when we note that

$$\left[\frac{t}{z}\right](t+yz) = \left[\frac{t+i}{z} - 1\right](t+yz) = \left[\frac{t+i}{z} + y - 1\right](t) + y(i-z) .$$

APPENDIX

FURTHER PROBLEMS

Some of the problems below are followed by conjectures, or results whose proofs are not given here.

(1) Determine or accurately estimate $g(a_1,\ldots,a_k)$ for $k \geq 4$.

Result:

$$g(a_1,a_2,\ldots a_k) = -a_1-a_2+\max\{y(a_i)a_2-x(a_{i-1})a_1$$
$$| \ 2 < i \leq k+1, x(a_2) = 0, y(a_{k+1}) = a_1\}$$

when the following conditions are satisfied.

(C1) $$gcd(a_1,a_2) = 1$$

(C2) $$\text{For } 2<i\leq k, 0<x(a_i)\leq [\frac{a_2}{2}] \text{ and } <\frac{a_1}{2}> \leq y(a_i) < a_1$$

where $a_i = y(a_i)a_2-x(a_i)a_1$.

(C3) $$0 < x(a_3) < x(a_4) < x(a_5) < \ldots < x(a_k)\ .$$

Note that condition (C3) is "artificial" since if (C3) does not hold than we can reindex the a_i's so that it does hold.

(2) Determine or accurately estimate $N_j(a_1,a_2,\ldots,a_k)$ for $j \geq 2$ and $k \geq 3$. $N_j(a_1,\ldots,a_k)$ is defined to be the smallest positive integer such that for all $n \geq N_j(a_1,\ldots,a_k)$, n has at least j representations.

Result: $N_j(a_1,a_2) = ja_1a_2-a_1-a_2$

(3) Determine or accurately estimate $g(k,s)$ for $k \geq 4$ and find the sets of integers that

achieve $g(k,t)$. Define

$$g(k,t) := \max_{a_i} g(a_1,a_2,\ldots,a_k)$$

where the maximum is taken over all a_i's satisfying

$$0 < a_1 < \ldots < a_k \leqslant t .$$

The Erdös, Graham conjucture, later proved by Lewin is

$$g(3,t) = \left[\frac{(t-2)^2}{2}\right] - 1 \text{ with the sets } \{t/2,t-1,t\} \text{ or}$$

$\{t-2,t-1,t\}$ for even t and $\{\frac{t-1}{2},t-1,t\}$ for odd t achieving $g(3,t)$.

Conjectures: $g(4,t) = \left[\frac{(t-2)(t-3)}{3}\right] - 1$ with the sets $\{\frac{t}{3},\frac{2t}{3},t-1,t\}$ when $t \equiv 0$ (mod 3), $\{\frac{t-1}{3},\frac{2(t-1)}{3},t-1,t\}$ when $t \equiv 1$ (mod 3) and $\{t-3,t-2,t-1,t\}$ when $t \equiv 2$ (mod 3) achieving $g(4,t)$.

$$g(5,t) = \begin{cases} \left[\frac{(t-2)(t-4)}{4}\right] - 1 & \text{when } t \equiv 0,1,2 \pmod 4 \\ \left[\frac{(t-2)(t-4)}{4}\right] - \frac{t+1}{4} + 1 & \text{when } t \equiv 3 \pmod 4 \end{cases}$$

with the set $\{\frac{t}{4},\frac{t}{2},\frac{3t}{4},t-1,t\}$ or $\{\frac{t}{2}-1,\frac{t}{2},t-2,t-1,t\}$ when $t \equiv 0$ (mod 4), $\{\frac{t-1}{4},\frac{(t-1)}{2},\frac{3(t-1)}{4},(t-1),t\}$ when $t \equiv 1$ (mod 4), $\{\frac{t-2}{2},\frac{t-2}{2}+1,t-2,t-1,t\}$ or $\{t-4,t-3,t-2,t-1,t\}$ when $t \equiv 2$ (mod 4) and $\{t-4,t-3,t-2,t-1,t\}$ when $t \equiv 3$ (mod 4) achieving $g(s,t)$.

(4) Determine or accurately estimate $h(k,t)$ for $k \geqslant 3$ and find the sets that achieve $h(k,t)$. Define

$$h(k,t) := \min_{a_i} g(a_1,a_2,\ldots,a_k)$$

where the minimum is taken over all a_i's satisfying

$$0 < t \leqslant a_1 < a_2 < \ldots < a_k$$

(5) Determine or accurately estimate g_k for some interesting sets $\{a_1,\ldots,a_k\}$. For example

$a_1 = t^p$, $a_2 = (t+1)^p,\ldots,a_k = (t+k-1)^p$ with integer $p \geqslant 2$, or

$a_1 = P(t)$, $a_2 = P(t+1),\ldots,a_k = P(t+k-1)$ where P is a polynomial.

(6) Determine or accurately estimate

$$\lim_{t\to\infty} g(t,t+1,\ldots,t+k) - g(k+1,t)\ ,$$

$$\lim_{t\to\infty} g(t,t-1,\ldots,t-k) - h(k+1,t)\ .$$

$$\lim_{t\to\infty} \frac{g(t,t+1,\ldots,t+k)}{g(k+1,t)} \quad \text{and}$$

$$\lim_{t\to\infty} \frac{g(t,t-1,\ldots,t-k)}{h(k+1,t)}\ .$$

(7) Determine or accurately estimate $G_j(k,t)$, $H_j(k,t)$ for j and $k \geqslant 2$. Define

$$G_j(k,t) := \max_{a_i} N_j(a_1,\ldots,a_k)$$

where the maxima is taken over all a_i's satisfying

$$0 < a_1 < \ldots < a_k \leqslant t\ , \quad \text{and}$$

$$H_j(k,t) := \min_{a_i} N_j(a_1,\ldots,a_k)$$

where the minimum is taken over all a_i's satisfying

$$0 < t \leqslant a_1 < a_2 < \ldots < a_k$$

(8) Determine or accurately estimate B_k, b_k, where for any positive integer a_{k+1} we define

$$B_k := B((a_1,\ldots,a_k),(a_{k+1})) = \{a \mid a > 0 \text{ and } g(a,a_1,\ldots,a_k) = a_{k+1}\}$$

and

$$b_k := b((a_1,\ldots,a_k),(a_{k+1}))$$

to be the number of integers in the set B_k.

(9) Derive a sequence of $O(\log N)$ increments for Shellsort, for which the worst case running time is better than $O(N^{4/3})$. (see Chapter 1,1.3)

(10) Determine $N_k(A_k)$ and h_1 for some interesting sets. (see Chapter 1, 1.3)

(11) Explore the connection relating the Frobenius problem to primitive matrices and graph theory (see Chapter 1, 1.3).

References

[1] P. T. Bateman, Remark on recent note on linear forms, Amer. Math. Monthly 65 (1958), 517-518.

[2] A. Brauer, On a problem of partitions, Amer. J. Math. 64 (1942), 299-312.

[3] A. Brauer, Review on J. B. Roberts: Note on linear forms, Math. Rev. 19 (1958), 1038.

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

[5] A. Brauer and J. E. Shockley, On a problem of Frobenius, J. reine angew. Math. 211 (1962), 215-220.

[6] J. S. Byrnes, On a partition problem of Frobenius, J. Comb. Theory (A) 17 (1974), 162-166.

[7] J. S. Byrnes, A partition problem of Frobenius. II, Acta Arithm. 28 (1975), 81-87.

[8] A. L. Dulmage and N. S. Mendelsohn, Gaps in the exponent set of primitive matrices, Illinois J. Math. 8 (1964), 642-565.

[9] P. Erdös, Problem P-84, Can. Math. Bull. 14 (1971), pp. 275-277.

[10] P. Erdös and R. L. Graham, On a linear diophantine problem of Frobenius, Acta Arithm. 21 (1972).

[11] W. Feller, An introduction to Probability Theory and its Applications, New York, 1950.

[12] G. Frobenius, Über Matrizen aus nicht negative Elementen. S.B. Preuss. Akad. Wiss. Berlin, (1912), 456-477.

[13] D. D. Grant, On linear forms whose coefficients are in arithmetic progression, Isreal J. Math. 15 (1973), 204-209.

[14] H. Greenberg, An Algorithm for a Linear Diophantine Equation and a Problem of Frobenius, Numer. Math. 34 (1980), 349-352.

[15] B. R. Heap and M. S. Lynn, The Index of Primitivity of a Non-Negative Matrix, Numer. Math. 6 (1964), 120-141.

[16] B. R. Heap and M. S. Lynn, A graph-theoretic algorithm for the solution of a linear diophantine problem of Frobenius, Numer. Math. 6 (1964), 346-354.

[17] B. R. Heap and M. S. Lynn, On a linear diophantine problem of Frobenius: an improved algorithm, Numer. Math. 7 (1965), 226-231.

[18] G. R. Hofmeister, Zu einem Problem von Frobenius, Norske Videnskabers Selskabs Skrifter 1966 Nr. 5, 1-37.

[19] Hann-Shue: Huang, An Algorithm for the Solution of a Linear Diophantine Problem of Frobenius, Chinese Journal of Math., Vol. 9, Number 1, June 1981.

[20] C. A. Jones, Using Linear Forms to Determine the Set of Integers Realizable by $(g_0,g_1,\ldots,g_n)$-trees (to appear).

[21] S. M. Johnson, A linear diophantine problem, Canad. J. Math. 12 (1960), 390-398.

[22] S. Kertzner, The linear diophantine equation, Classroom Notes, March 1981, 200-203.

[23] D. E. Knuth, The Art of computer programming, Addison-Wesley Publishing Company, 1973.

[24] M. Lewin, A bound for a solution of a linear diophantine problem, J. London Math. Sco. (2) 6 (1972), 61-69.

[25] M. Lewin, On a linear diophantine problem, Bull. London Math. Soc. 5 (1973), 75-78.

[26] M. Lewin, On a problem of Frobenius for an almost consecutive set of integers, J. reine angew. Math. 273 (1975), 134-137.

[27] M. Lewin, An algorithm for a solution of a problem of Frobenius, J. Reine angew. Math. 276 (1975), 68-82.

[28] N. S. Mendelsohn, A linear diophantine equation with applications to nonnegative matrices, Ann. New York Acad. Sci. 175 (1970), 287-294.

[29] G. Meures, Zusammenhang zwischen Reichweite und Frobeniuszahl, Staatsexamensarbeit, Maiz, 1978.

[30] M. Nogata and H. Mutsumura, A theory in elementary arithmetic, Sûgaku 13 (1961/62), 161. (Math. Rev. 26 (1963), No. 2386.)

[31] A. Nijenhuis and H. S. Wilf, Representations of integers by liner forms in nonnegative integers, J. Number Theory 4 (1972), 98-106.

[32] J. B. Roberts, Note on linear forms, Proc. Amer. Math. Soc. 7 (1956), 465-469.

[33] J. B. Roberts, On a diophantine problem, Canad. J. Math. 9 (1957), 219-222.

[34] O. J. Rödseth, On a linear Diophantine Problem of Frobenius, J. reine agnew. Math. 301 (1978), 171-178.

[35] O. J. Rödseth, On a linear diophantine problem of Frobenius. II, J. reine angew. Math. (1979), 431-440.

[36] Ö. J. Rödseth, On h-bases for n, Math. Scand. (to appear).

[37] H. Rohrbach, Einige neuere Untersuchungen über die Dichte in der additiven Zahlentheorie, Jahresbericht der Deufschen Mathematiker Vereinigung, 48 (1939), 199-236.

[38] R. Sedgewick, A New Upper Bound for Shellsort. (to appear)

[39] E. S. Selmer, On the linear Diophantine problem of Frobenius, J. Reine Angew. Math. 293/294 (1977), 1-17.

[40] E. S. Selmer and Ö. Beyer, On the linear Diophantine problem of Frobenius in three variables, J. Reine Angew. Math. 301 (1978), 161-170.

[41] E. S. Selmer, On the postage stamp problem with three stamp denominations, Math. Scand. 47 (1980), 29-71.

[42] E. Siering, Über lineare Formen und ein Problem von Frobenius. I, J. reine angew. Math. 271 (1974), 177-202.

[43] C. Smorynski, Skolem's solution to a Problem of Frobenius.

[44] J. J. Sylvester, Mathematical questions, with their solutions, Education Times 41 (1844), 21.

[45] B. Temkin, (to appear).

[46] Y. Vitek, Bounds for a linear diophantine problem of Frobenius, J. London Math. Soc. (2) 10 (1975), 79-85.

[47] Y. Vitek, Bounds for a linear diophantine problem of Frobenius. II, Canad. J. Math. 28 (1976), 1280-1288.

[48] B. Vizveri, Uber die Zusammenhänge zwischen dem Frobenius-Problem und der Knapsack-Aufgabe. (to appear)