To the Graduate Council:

I am submitting herewith a dissertation written by Juliana H. Dowell, entitled "The Ring of Arithmetic Functions Under the Lucas Product." I recommend that it be accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, with a major in Mathematics.

Robert M. McConnel, Major Professor

We have read this dissertation and recommend its acceptance:

Accepted for the Council:

Vice Chancellor
Graduate Studies and Research

Thesis
776
.D684
cop. 2

THE RING OF ARITHMETIC FUNCTIONS UNDER THE LUCAS PRODUCT

A Dissertation

Presented for the

Doctor of Philosophy

Degree

The University of Tennessee, Knoxville

Juliana H. Dowell

March 1977

1315331

ACKNOWLEDGMENTS

The author wishes to thank her advisor, Dr. Robert M. McConnel, for a lot of sound advice, the members of her committee for their consideration and patience, and Jerry Warwick for her fortitude and surgical skill.

ABSTRACT

Any nonnegative integer n has a unique representation as

$$n = \sum_{i=0}^{k} a_i p^i \quad (0 \leq a_i < p),$$

where p is a fixed prime number. If

$$m = \sum_{i=0}^{k} a_i p^i \quad (0 \leq a_i < p),$$

$$n = \sum_{i=0}^{k} b_i p^i \quad (0 \leq b_i < p),$$

then we say that m is a p-factor of n if $a_i \leq b_i$ for i = 0, ..., k, and we symbolize this by $m \mid_p n$. If f and g are two arithmetic functions defined on the nonnegative integers, then the Lucas product of f and g is given by

$$f*g(n) = \sum_{d \mid_p n} f(d)g(n-d),$$

where d is taken over all p-factors of n.

If L is the set of all functions whose domains are the set N of nonnegative integers, and whose ranges are contained in a fixed field F, then the set L with addition defined by

$$(f+g)(n) = f(n) + g(n)$$

and multiplication defined by the Lucas product, is a commutative ring with unity. In Chapters II, III, and IV of this paper, some L-analogs of some common number-theoretic functions and concepts are obtained.

It has been shown that if $f_1, \ldots, f_k$ are elements of L, if $m_1, \ldots, m_k$ are positive integers, and if $\psi_{m_1}, \ldots, \psi_{m_k}$, are the characteristic functions at $m_1, \ldots, m_k$, respectively, then

$$f = f_1 * \psi_{m_1} + \ldots + f_k * \psi_{m_k}$$

is a nilpotent element of L. Moreover, if F has characteristic p ($p > 0$), then all singular elements of L are zero divisors. If the field F has characteristic zero, the problem of characterizing the zero divisors of L is more difficult. In Chapter V, some theorems are proven which delineate the properties of singular functions of L when F has characteristic zero and which, to some extent, indicate that the zero divisors of L in this case all have the form above.

TABLE OF CONTENTS

CHAPTER		PAGE
I.	INTRODUCTION	1
	Background Material	1
	Statement of Objectives	3
II.	L-ANALOGS OF SOME NUMBER THEORETIC FUNCTIONS	5
III.	THE UNITARY LUCAS PRODUCT	19
IV.	LUCAS-PERFECT AND LUCAS-AMICABLE NUMBERS	30
V.	ON THE ZERO DIVISORS OF L	36
	On the Nilpotent Elements of L	36
	On the Zero Divisors of L	51
	Algorithm for Obtaining a Quasi-Generator of g(n)	66
BIBLIOGRAPHY		98
VITA		100

CHAPTER I

INTRODUCTION

1.1. Background Material. Let F denote an arbitrary but fixed field. An arithmetic function is a mapping from the integers into F. In this paper the domain of all arithmetic functions will be the set N of nonnegative integers. If f, g are two arithmetic functions, the sum h = f + g is defined by

$$h(n) = f(n) + g(n). \tag{1.1}$$

The product for this discussion will be the Lucas product h = f*g, which will be defined as follows.

Any nonnegative integer n has a unique representation as

$$n = \sum_{i=0}^{k} a_i p^i \quad (0 \leq a_i < p),$$

where p is a fixed prime number. If

$$\begin{aligned} m &= \sum_{i=0}^{k} a_i p^i \quad (0 \leq a_i < p), \\ n &= \sum_{i=0}^{k} b_i p^i \quad (0 \leq b_i < p), \end{aligned} \tag{1.2}$$

then we say that m is a p-factor of n if $a_i \leq b_i$ for i = 0, ..., k. We symbolize this by $m \mid_p n$. We note that $0 \mid_p n$ for all $n \in N$.

The Lucas product of f and g will be given by

$$f*g(n) = \sum_{d \mid_p n} f(d)g(n-d), \qquad (1.3)$$

where the sum (1.3) is taken over all p-factors of n. The product (1.3) is called the Lucas product determined by p.

The Lucas product is commutative and associative, and the generalized Lucas product (for the product of t arithmetic functions) will be given by

$$f_1 * \ldots * f_t(n) = \sum_{d_1 +_p \ldots +_p d_t = n} f_1(d_1) \cdot \ldots \cdot f_t(d_t),$$

where "$+_p$" indicates that we are adding in base p without "carrying." Moreover each d_i $(1 \leq i \leq t)$ takes on every value of a p-factor of n.

We will denote by L the ring of all arithmetic functions from the set N of nonnegative integers into a fixed field F. The operations on L will be addition as defined in (1.1) and the Lucas product as defined in (1.3). The zero element of L is the function

$$z(n) = 0, \; n = 0, 1, \ldots ,$$

and the identity element of L for the Lucas product is

$$u(n) = \begin{cases} 1, & n = 0 \\ 0, & n > 0. \end{cases}$$

Another function that will be frequently used is

$$I(n) = 1, \quad n = 0, 1, 2, \ldots .$$

If m and n are as defined in (1.2), then the greatest common p-factor of m and n is

$$(m,n)_p = \sum_{i=0}^{k} \min \{a_i, b_i\} \cdot p^i .$$

1.2. Statement of Objectives. The ring of arithmetic functions under addition and the Lucas product contains some functions that are of particular interest. In Chapter II we develop some L-analogs of some major number-theoretic functions; for example, the σ-function (sum of divisors), the Euler ϕ-function, and Ramanujan's sum all have analogs in L.

The unitary (Dirichlet) product has an analog which we call the unitary Lucas product. Cohen [5] has developed analogs of some of the more important number-theoretic functions for the unitary product. In Chapter III we develop the idea of the unitary Lucas product and some analog functions associated with it.

Chapter IV is a brief foray into possibilities for defining analogs for the Lucas product, of perfect and amicable numbers.

Cashwell and Everett [3] have shown that the ring of arithmetic functions under addition and the Dirichlet product is a unique factorization domain. On the other hand, Carlitz [1] has shown that the ring

L of arithmetic functions under addition and the Lucas product contains zero divisors, and hence cannot be a unique factorization domain. In fact, if the field F has characteristic p, where p is a prime, then an element f of L is a zero divisor iff f is singular.

The characterization of the zero divisors of L when F has characteristic zero presents a very challenging problem in number theory. In Chapter V we present some theorems which clarify the problems involved in characterizing the zero divisors of L and which, to some extent, back up Carlitz' conjecture that an element f of L is a zero divisor iff f is nilpotent.

CHAPTER II

L-ANALOGS OF SOME NUMBER THEORETIC FUNCTIONS

We reiterate here some definitions made in Chapter I.

If $m = \sum_{i=0}^{r} a_i p^i$ and $n = \sum_{i=0}^{s} b_i p^i$, $0 \leq a_i, b_i < p$, then we say that m is a p-factor of n ($m \mid_p n$) if $r \leq s$ and $0 \leq a_i \leq b_i$ for $i = 0, \ldots, r$. The greatest common p-factor of m and n is

$$(m,n)_p = \sum_{i=0}^{\min\{r,s\}} \min\{a_i,b_i\} p^i,$$

and if $(m,n)_p = 0$ we say that m and n are relatively prime.

If f and g are in L we define

$$(f + g)(n) = f(n) + g(n),$$

$$f*g(n) = \sum_{d \mid_p n} f(d)g(n-d), \qquad (2.1)$$

where d is taken over all p-factors of n. The product (2.1) is commutative and associative, and is called the Lucas product.

The Lucas product may be generalized as follows:

$$f_1 * \ldots * f_k = \sum_{d_1 +_p \ldots +_p d_k = n} f_1(d_1) \ldots f_k(d_k),$$

where $+_p$ indicates that we are adding in base p without "carrying."

An arithmetic function will be called p-factorable if $f(0) = 1$ and if $f(m+n) = f(m)f(n)$ whenever $(m,n)_p = 0$. For the sake of consistency we consider only arithmetic functions from N into the real numbers.

Carlitz [1] has proven the following theorems.

THEOREM 2.1. (i) Let $g(n) = \sum_{d \mid p^n} f(d)$. If f is p-factorable, then g is p-factorable, and conversely.

(ii) If $h(n) = f*g(n)$, and if any two of f, g, h are p-factorable, then the third function is p-factorable.

THEOREM 2.2. (Inversion formula) If f and g are arithmetic functions and if $g(n) = \sum_{d \mid p^n} f(d)$, then $f(n) = g*\mu_p(n)$. ($\mu_p(n)$ is defined below.)

Carlitz [1] has also derived the following formulas.

If $n = \sum_{i=0}^{r} a_i p^i$, $0 \leq a_i < p$, then

$$\tau_p(n) = \sum_{d \mid p^n} 1 = \prod_{i=0}^{r} (a_i+1) = I*I(n),$$

where $I(n) = 1$ (all n),

$$\tau_{pk}(n) = \tau_{p(k-1)}*\tau_p(n) = \underbrace{I*I*\ldots*I(n)}_{k \text{ factors}}, \quad k \geq 2.$$

We note that $\tau_p(n) = \tau_{p2}(n)$, and that $\tau_p(n)$ gives the number of p-factors of n.

$$\mu_p(n) = \prod_{i=0}^{r} \mu_p(a_i p^i), \text{ where } \mu_p(a_i p^i) = \begin{cases} 1 \text{ if } a_i = 0 \\ -1 \text{ if } a_i = 1 \\ 0 \text{ if } a_i > 1 \end{cases}.$$

We note that μ_p is the inverse of I under the Lucas product. Each of the above functions is p-factorable.

DEFINITION 2.1. We will denote by s(n) the sum of the p-factors of n.

THEOREM 2.3. $s(n) = \frac{n\tau_p(n)}{2}$.

PROOF. If n = 0, then $s(n) = 0 = \frac{0\tau_p(0)}{2}$. If $n > 0$, then $n = \sum_{i=1}^{m} a_i p^{r_i}$, $0 < a_i < p$, $r_1 < \ldots < r_m$. We use mathematical induction on m.

If m = 1, then $n = ap^r$ $(0 < a < p)$ and

$$s(n) = 0 + p^r + 2p^r + \ldots + ap^r$$

$$= (1 + 2 + \ldots + a)p^r$$

$$= \frac{a(a+1)p^r}{2} = \frac{n\tau_p(n)}{2}.$$

If the theorem is true for $n = \sum_{i=1}^{k} a_i p^{r_i}$, $0 < a_i < p$, $r_1 < \ldots < r_k$, we let $n' = \sum_{i=1}^{k+1} a_i p^{r_i} = n + a_{k+1}p^{r_{k+1}}$, $0 < a_{k+1} < p$, $r_{k+1} > r_k$. Then

$$s(n') = \sum_{d|_p n'} d$$

$$= \sum_{d|_p n} d + \sum_{d|_p n} (d+p^{r_{k+1}}) + \ldots + \sum_{d|_p n} (d+a_{k+1}p^{r_{k+1}})$$

$$= (a_{k+1}+1)s(n) + \tau_p(n)p^{r_{k+1}} + \ldots + \tau_p(n)a_{k+1}p^{r_{k+1}}$$

$$= (a_{k+1}+1)\frac{n\tau_p(n)}{2} + \tau_p(n)(1 + \ldots + a_{k+1})p^{r_{k+1}}$$

$$= \frac{n\tau_p(n')}{2} + \tau_p(n)\frac{a_{k+1}(a_{k+1}+1)}{2}p^{r_{k+1}}$$

$$= \frac{n\tau_p(n')}{2} + \frac{a_{k+1}p^{r_{k+1}}\tau_p(n')}{2}$$

$$= \frac{n'\tau_p(n')}{2} .$$

We note that $s(n)$ is not p-factorable.

LEMMA. If f is p-factorable, and if $n = \sum_{i=0}^{k} a_i p^i$, $0 < a_i \leq p$, then $f(n) = \prod_{i=0}^{k} f(a_i p^i)$.

PROOF. The proof is by induction on k. If $k = 0$ then $n = a_0 p^0$, $0 < a_0 < p$, and $f(n) = f(a_0 p^0)$. Suppose the lemma is true for $k = m$; i.e., $n = \sum_{i=0}^{m} a_i p^i$ $(0 \leq a_i < p)$ and f is p-factorable. Then

$$f(n) = \prod_{i=0}^{m} f(a_i p^i).$$

Let $n' = \sum_{i=0}^{m+1} a_i p^i = n + a_{m+1}p^{m+1}$, $0 \leq a_i < p$. Then $(n, a_{m+1}p^{m+1}) = 0$, and $f(n') = f(n)f(a_{m+1}p^{m+1}) = \prod_{i=0}^{m+1} f(a_i p^i)$.

DEFINITION 2.2. $\sigma_p(n) = \sum_{d \mid_p n} p^d$.

THEOREM 2.4. If $n = \sum_{i=0}^{k} a_i p^i$, $0 \leq a_i < p$, then $\sigma_p(n) = \prod_{i=0}^{k} \frac{p^{(a_i+1)p^i} - 1}{p^{p^i} - 1}$.

PROOF. $f(n) = p^n$ is clearly p-factorable; so $\sigma_p(n)$ is p-factorable by Theorem 2.1 (i); hence $\sigma_p(n) = \prod_{i=0}^{k} \sigma_p(a_i p^i)$.

If $a_i = 0$, then $\sigma_p(a_i p^i) = \sigma_p(0) = p^0 = 1 = \dfrac{p^{(0+1)p^i}-1}{p^{p^i}-1}$.

If $a_i > 0$, then $\sigma_p(a_i p^i) = p^0 + p^{p^i} + \ldots + p^{a_i p^i} = \dfrac{p^{(a_i+1)p^i}-1}{p^{p^i}-1}$.

$\therefore \quad \sigma_p(n) = \prod_{i=0}^{k} \dfrac{p^{(a_i+1)p^i}-1}{p^{p^i}-1}$.

DEFINITION 2.3. $\sigma_{pk}(n) = \sum_{d \mid_p n} p^{kd}$.

THEOREM 2.5. If $n = \sum_{i=0}^{r} a_i p^i$, $0 \leq a_i < p$, then $\sigma_{pk}(n) = \prod_{i=0}^{r} \dfrac{p^{k(a_i+1)p^i}-1}{p^{kp^i}-1}$.

PROOF. The proof is analogous to that of Theorem 2.4.

DEFINITION 2.4. $\phi_p(n) = \sum_{d \mid_p n} p^d \mu_p(n-d)$, and $\phi_{pk}(n) = \sum_{d \mid_p n} p^{kd} \mu_p(n-d)$.

THEOREM 2.6. If $n = \sum_{i=1}^{r} a_i p^{s_i}$, $0 < a_i < p$, $s_1 < \ldots < s_r$, then

$\phi_p(n) = p^n \prod_{i=1}^{r} (1 - p^{-p^{s_i}})$, and $\phi_p(0) = 1$.

PROOF. $\phi_p(0) = p^0 \mu_p(0) = 1$.

If $n > 0$, then $n = \sum_{i=1}^{r} a_i p^{s_i}$, $0 < a_i < p$, $s_1 < \ldots < s_r$. ϕ_p is p-factorable by Theorem 2.1 (ii); so $\phi_p(n) = \prod_{i=1}^{r} \phi_p(a_i p^{s_i})$.

$$\phi_p(a_i p^{s_i}) = p^{a_i p^{s_i}} \mu_p(0) + p^{(a_i-1)p^{s_i}} \mu_p(p^{s_i})$$

$$= p^{a_i p^{s_i}} - p^{(a_i-1)p^{s_i}}$$

$$= p^{a_i p^{s_i}} (1 - p^{-p^{s_i}}).$$

Hence $\phi_p(n) = \prod_{i=1}^{r} p^{a_i p^{s_i}}(1 - p^{-p^{s_i}}) = p^n \prod_{i=1}^{r}(1 - p^{-p^{s_i}})$.

COROLLARY. $\phi_{pk}(n) = p^{kn}\prod_{i=1}^{r}(1-p^{-p^{ks_i}})$, and $\phi_{pk}(0) = 1$.

Smith [6] derived analogs of the Euler ϕ-function and the σ-function as follows. If $n = \sum_{i=0}^{k} a_i p^i$ $(0 \leq a_i < p)$, then $v(n) = \prod_{i=0}^{k} p_i^{a_i}$, where $p_0, p_1, \ldots,$ are the primes in order, and $\sigma = v*I$, $\phi = v*\mu_p$. If $v_k(n) = \prod_{i=0}^{k} p_i^{ka_i}$ then $\sigma_k = v_k*I$, and $\phi_k = v_k*\mu_p$. Smith's methods may be used to obtain σ_p, ϕ_p, σ_{pk}, and ϕ_{pk}. If we define $v_p(n) = p^n$ and $v_{pk}(n) = p^{kn}$, we obtain $\sigma_p = v_p*I$, $\phi_p = v_p*\mu_p$, $\sigma_{pk} = v_{pk}*I$, and $\phi_{pk} = v_{pk}*\mu_p$.

DEFINITION 2.5. $c_{np}(m) = \sum_{\substack{d \mid p^m \\ d \mid p^n}} p^d \mu_p(n-d)$.

THEOREM 2.7. If $(m,n)_p = a$ and $n = a + N$, then $c_{np}(m) = \dfrac{\mu_p(N)\phi_p(n)}{\phi_p(N)}$.

PROOF:

$$c_{np}(m) = \sum_{d \mid p^a} p^d \mu_p(n-d)$$

$$= \sum_{\substack{d \mid p^a \\ c=a-d}} p^{a-c} \mu_p(N+c)$$

$$= p^a \sum_{d \mid p^a} \frac{\mu_p(N+c)}{p^c}$$

$$= p^a \mu_p(N) \sum_{c \mid p^a} \frac{\mu_p(c)}{p^c}$$

$$(c,N)_p = 0,$$

since $\mu_p(N+c) = \begin{cases} \mu_p(N)\mu_p(c), \text{ if } (c,N)_p = 0 \\ 0, \text{ if } (c,N)_p \neq 0. \end{cases}$ Now

$$\sum_{\substack{c \mid p^a \\ (c,N)_p = 0}} \frac{\mu_p(c)}{p^c} = 1 + \sum_{\substack{p^r \mid p^a \\ (p^r,N)_p=0}} \frac{\mu_p(p^r)}{p^{p^r}} + \sum_{\substack{p^r+p^{r'} \mid p^a \\ (p^r+p^{r'},N)_p=0}} \frac{\mu_p(p^r+p^{r'})}{p^{p^r+p^{r'}}} + \cdots$$

$$= 1 - \sum_{\substack{p^r \mid p^n \\ p^r \nmid p^N}} \frac{1}{p^{p^r}} + \sum_{\substack{p^r+p^{r'} \mid p^n \\ p^r+p^{r'} \nmid p^N}} \frac{1}{p^{p^r} p^{p^r}} + \cdots$$

$$= \prod_{\substack{p^r \mid p^n \\ p^r \nmid p^N}} (1-p^{-p^r})$$

So $c_{np}(m) = p^a \mu_p(N) \prod_{\substack{p^r \mid p^n \\ p^r \nmid p^N}} (1-p^{-p^r})$.

$$\frac{\mu_p(N)\phi_p(n)}{\phi_p(N)} = \frac{\mu_p(N)p^n \prod_{p^r \mid p^n} (1-p^{-p^r})}{p^N \prod_{p^r \mid p^N} (1-p^{-p^r})}$$

$$= p^a \mu_p(N) \prod_{\substack{p^r \mid p^n \\ p^r \nmid p^N}} (1-p^{-p^r}) .$$

$$\therefore \quad c_{np}(m) = \frac{\mu_p(N)\phi_p(n)}{\phi_p(N)} .$$

COROLLARY. $c_{np}(m)$ is p-factorable; i.e., if $(n,k)_p = 0$, then

$$c_{(n+k)p}(m) = c_{np}(m)c_{kp}(m).$$

PROOF. If $(n,k)_p = 0$, then $(n+k,m)_p = a + b$, where $a = (n,m)_p$ and $b = (k,m)_p$; and $(n,k)_p = 0 \Rightarrow (a,b)_p = 0$ and $(n-a,k-b)_p = 0$. Hence

$$c_{(n+k)p}(m) = \frac{\mu_p(n+k-a-b)\phi_p(n+k)}{\phi_p(n+k-a-b)}$$

$$= \frac{\mu_p(n-a)\phi_p(n)}{\phi_p(n-a)} \cdot \frac{\mu_p(k-b)\phi_p(k)}{\phi_p(k-b)}$$

$$= c_{np}(m)c_{kp}(m).$$

THEOREM 2.8. $\sum_{d|_p n} \mu_p(d) = u(n) = \begin{cases} 1, & n = 0 \\ 0, & n > 0 \end{cases}$

PROOF. Carlitz [1] showed that $\mu_p = I^{-1}$; i.e., $\sum_{d|_p n} \mu_p(d) = \mu_p * I(n) = u(n)$.

DEFINITION 2.6. $\Lambda_p(n) = \begin{cases} p^r \log(p), \text{ if } n = ap^r,\ 0 < a < p \\ 0, \text{ otherwise.} \end{cases}$

THEOREM 2.9. $\Lambda_p(n) = \log(p) \sum_{d|_p n} d\mu_p(n-d).$

PROOF. Let $f(n) = \log(p) \sum_{d \mid_p n} d\mu_p(n-d)$. Then

$$f(0) = \log(p) \cdot 0 \cdot \mu_p(0) = 0 = \Lambda_p(0).$$

If $n = ap^r$, $0 < a < p$, then

$$f(n) = \log(p)(ap^r\mu_p(0) + (a-1)p^r\mu_p(p^r))$$

$$= \log(p)(ap^r - (a-1)p^r)$$

$$= p^r \log(p)$$

$$= \Lambda_p(n).$$

Suppose $n = \sum_{i=1}^{k} a_i p^{r_i}$, $0 < a_i < p$, $r_1 < \ldots < r_k$, where $k \geq 2$.

Let $n' = \sum_{i=1}^{k-1} a_i p^{r_i}$, so that $n = n' + a_k p^{r_k}$ and $n' > 0$. Then

$$f(n) = \log(p) \sum_{d \mid_p n} \mu_p(d)(n-d)$$

$$= \log(p)[\sum_{d \mid_p n'} \mu_p(d)(n' + a_k p^{r_k} - d) + \sum_{d \mid_p n'} \mu_p(d+p^{r_k})(n-d-p^{r_k})]$$

$$= \log(p)[\sum_{d \mid_p n'} \mu_p(d)(n'-d) + a_k p^{r_k} \sum_{d \mid_p n'} \mu_p(d)$$

$$+ \sum_{d \mid_p n'} \mu_p(d)\mu_p(p^{r_k})(n' + a_k p^{r_k} - d - p^{r_k})]$$

$$= \log(p)\Big[\sum_{d \mid_p n'} \mu_p(d)(n' - d) + 0$$

$$+ \mu_p(p^{r_k}) \sum_{d \mid_p n'} \mu_p(d)(n' + a_k p^{r_k} - d - p^{r_k})\Big]$$

$$= \log(p)\Big[\sum_{d \mid_p n'} \mu_p(d)(n'-d) - \sum_{d \mid_p n'} \mu_p(d)(n' + a_k p^{r_k} - d - p^{r_k}\Big]$$

$$= \log(p)\Big[\sum_{d \mid_p n'} \mu_p(d)(n'-d) - \sum_{d \mid_p n'} \mu_p(d)(n'-d)$$

$$- \sum_{d \mid_p n'} \mu_p(d)(a_k p^{r_k} - p^{r_k})\Big]$$

$$= \log(p)\Big[-(a_k p^{r_k} - p^{r_k}) \sum_{d \mid_p n'} \mu_p(d)\Big]$$

$$= 0.$$

$\therefore$ $\Lambda_p(n) = \log(p) \sum_{d \mid_p n} d\mu_p(n-d).$

We note that $\Lambda_p(n)$ is not p-factorable.

DEFINITION 2.7. If $n = \sum_{i=0}^{k} a_i p^i$, $0 \leq a_i < p$, then $\lambda_p(n) = (-1)^{\sum_{i=0}^{k} a_i}$, $\lambda_p(0) = 1$.

DEFINITION 2.8. If $n = \sum_{i=1}^{k} a_i p^{r_i}$, $0 < a_i < p$, $r_1 < \ldots < r_k$, then $\omega_p(n) = k$ = number of distinct powers of p in n; and $\omega_p(0) = 0$.

DEFINITION 2.9. If $n = \sum_{i=0}^{k} a_i p^i$, $0 \leq a_i < p$, where all a_i's are even, then we say that n is <u>p-square</u>, and we define

$$\rho_p(n) = \begin{cases} 1, \text{if } n \text{ is a p-square} \\ 0, \text{if } n \text{ is not a p-square.} \end{cases}$$

THEOREM 2.10. $\sum_{d|_p n} |\mu_p(d)| = 2^{\omega_p(n)}$.

PROOF. Let $f(n) = \sum_{d|_p n} |\mu_p(d)|$. Then $f(0) = |\mu_p(0)| = 1 = 2^0 = 2^{\omega_p(0)}$.

If $n > 0$, then $n = \sum_{i=1}^{k} a_i p^{r_i}$, $0 < a_i < p$, $r_1 < \ldots < r_k$. Now $f(a_i p^{r_i}) = |\mu_p(0)| + |\mu_p(p^{r_i})| = 1 + 1 = 2 = 2^{\omega_p(a_i p^{r_i})}$. Also f(n) is clearly p-factorable; so

$$f(n) = \prod_{i=1}^{k} f(a_i p^{r_i}) = \prod_{i=1}^{k} 2 = 2^k = 2^{\omega_p(n)}.$$

THEOREM 2.11. $\sum_{d|_p n} \phi_p(d) = p^n$.

PROOF. $\phi_p(n) = \sum_{d|_p n} p^d \mu_p(n-d)$

$$= \sum_{d|_p n} \mu_p(d) p^{n-d};$$

so by Theorem 2.2, $p^n = \sum_{d|_p n} \phi_p(d)$.

THEOREM 2.12. (i) $\sum_{d|_p^n} \lambda_p(d) = \rho_p(n)$.

(ii) $\sum_{d|_p^n} \mu_p(d)\rho_p(n-d) = \lambda_p(n)$.

PROOF. (i) Clearly $f(n) = \sum_{d|_p^n} \lambda_p(d)$ is p-factorable; so if $n = ap^r$, $0 \leq a < p$, then

$$f(n) = \lambda_p(0) + \lambda_p(p^r) + \ldots + \lambda_p(ap^r)$$

$$= 1 + (-1) + \ldots + (-1)^a$$

$$= \begin{cases} 1, \text{ if } a \text{ is even} \\ 0, \text{ if } a \text{ is odd;} \end{cases}$$

and if $n = \sum_{i=0}^{k} a_i p^i$, $0 \leq a_i \leq p$, then

$$f(n) = \prod_{i=0}^{k} f(a_i p^i)$$

$$= \begin{cases} 1, \text{ if } a_i \text{ is even for all } i \\ 0, \text{ if } a_i \text{ is odd for some } i \end{cases}$$

$$= \rho_p(n).$$

We note that 0 is p-square, and $f(0) = \lambda_p(0) = 1 = \rho_p(0)$.

(ii) is an immediate consequence of (i) and Theorem 2.2.

We have shown here some analogs of some of the functions and relations between them that are of major interest in the theory of numbers. All of the functions considered above are p-factorable except the functions $s(n)$, $\Lambda_p(n)$, and $\omega_p(n)$.

The function $\phi_p(n)$ is analogous to the Euler ϕ-function which is defined by

$$\phi(n) = \sum_{\substack{1\le h\le n \\ (h,n)=1}} 1 . \qquad (2.2)$$

Question 2.1. Is it possible to denote the function ϕ_p in a way that is analogous to (2.2)?

The answer to Question 2.1 is probably not, for if $n = \sum_{i=0}^{k} a_i p^i$, $0 < a_i < p$, $i = 0, \ldots, k$, then $H = \{h: 0 \le h \le n, (h,n)_p = 0\} = \{0\}$. For any fixed k, there are (p-1) possible a_i's for each p^i; i.e., $\frac{[(p-1)(k+1)]!}{(k+1)![(p-2)(k+1)]!}$ possible n's, and for each one, $H = \{0\}$, while $\phi_p(n)$ will consist of different sums of $\pm p^r$, $0 \le r \le k$ for each n.

The function $c_{np}(m)$ is an analog of Ramanujan's sum which is defined by

$$c_n(m) = \sum_{\substack{1\le h\le n \\ (h,n)=1}} e^{\frac{2\pi i h m}{n}} \qquad (2.3)$$

Question 2.2. Is it possible to denote the function $c_{np}(m)$ in a manner analogous to (2.3)?

The answer to Question 2.2 is also probably not for reasons similar to those for Question 2.1.

CHAPTER III

THE UNITARY LUCAS PRODUCT

If f and g are arithmetic functions whose domain is the set of nonnegative integers and whose range is contained in a field F, we define the unitary Lucas product of f and g by

$$f*_u g(n) = \sum_{d \mid_p^* n} f(d)g(n-d),$$

where d is taken over all p-factors of n such that $(d,n-d)_p = 0$. Such p-factors of n will be called unitary p-factors of n.

If L^* is the set of all arithmetic functions whose domain is N and whose ranges are contained in a field F, then L^* under ordinary addition of functions and the unitary Lucas product is easily shown to be a commutative ring with the same unity and zero as L. As in Chapter II, we assume that F is the field of real numbers.

DEFINITION 3.1. A function f is singular if $f(0) = 0$, and nonsingular if $f(0) \neq 0$. If $f*_u g = u$, then we call g the inverse of f.

THEOREM 3.1. A function f has an inverse if and only if it is nonsingular.

PROOF. If $f*_u g = u$, then $f*_u g(0) = f(0)g(0) = 1$; hence $f(0) \neq 0$. Conversely, if $f(0) \neq 0$, then we can define g(0) by $g(0) = \frac{1}{f(0)}$, and $f*_u g(0) = 1$. g(0) is uniquely determined by f(0). For $n > 0$,

if we set $f *_u g(n) = 0$, then the coefficient of $g(n)$ is $f(0)$. It follows that $g(n)$ is uniquely determined by $g(r)$ for all unitary p-factors r of n.

Let us consider the function $I(n) = 1$, $n = 0, 1, 2, \ldots$. $I(0) \neq 0$; so I has an inverse μ_p^* such that $I *_u \mu_p^* = u$.

THEOREM 3.2. If $n = \sum_{i=0}^{k} a_i p^i$, $0 \leq a_i < p$, then $\mu_p^*(n) = \prod_{i=0}^{k} \mu_p^*(a_i p^i)$, where $\mu_p^*(a_i p^i) = \begin{cases} -1, \text{if } a_i > 0 \\ 1, \text{if } a_i = 0. \end{cases}$

PROOF. $1 = I *_u \mu_p^*(0) = I(0)\mu_p^*(0)$, and $\mu_p^*(0) = 1$. Suppose $n = ap^r$, $0 < a < p$. Then

$$0 = I *_u \mu_p^*(n) = I(0)\mu_p^*(ap^r) + I(ap^r)\mu_p^*(0) = \mu_p^*(ap^r) + 1.$$

Hence $\mu_p^*(ap^r) = -1$.

Now suppose $n = \sum_{i=1}^{m} a_i p^{r_i}$, $0 < a_i < p$, $m \geq 1$, and

$$\mu_p^*(n) = \prod_{i=1}^{m} \mu_p^*(a_i p^{r_i}) = (-1)^m$$

Let $n' = \sum_{i=1}^{m+1} a_i p^{r_i}$, $0 < a_i < p$. Then

$$0 = I *_u \mu_p^*(n') = \sum_{d \mid_p^* n'} I(d)\mu_p^*(n'-d)$$

$$= \sum_{d \mid_p^* n} I(d)\mu_p^*(n+a_{m+1}p^{r_{m+1}}-d) + \sum_{d \mid_p^* n} I(d+a_{m+1}p^{r_{m+1}})\mu_p^*(n-d)$$

$$= \sum_{d|{}^{*}_{p}n} \mu_p^*(n+a_{m+1}p^{r_{m+1}}-d) + \sum_{d|{}^{*}_{p}n} I(d)\mu_p^*(n-d)$$

$$= \sum_{d|{}^{*}_{p}n} \mu_p^*(n+a_{m+1}p^{r_{m+1}}-d).$$

For $d > 0$, $n+a_{m+1}p^{r_{m+1}}-d$ contains at most m powers of p. So $\mu_p^*(n+a_{m+1}p^{r_{m+1}}-d) = \mu_p^*(n-d)\mu_p^*(a_{m+1}p^{r_{m+1}}) = -\mu_p^*(n-d)$. Hence

$0 = \sum_{d|{}^{*}_{p}n} \mu_p^*(n+a_{m+1}p^{r_{m+1}}-d) = -\sum_{\substack{d|{}^{*}_{p}n \\ d>0}} \mu_p^*(n-d) + \mu_p^*(n+a_{m+1}p^{r_{m+1}})$. So

$\mu_p^*(n') = \sum_{\substack{d|{}^{*}_{p}n \\ d>0}} \mu_p^*(n-d) = -\mu_p^*(n) = \prod_{i=1}^{m+1} \mu_p^*(a_i p^i)$. The theorem follows.

THEOREM 3.3. If $g(n) = \sum_{d|{}^{*}_{p}n} f(d)$, then $f(n) = \sum_{d|{}^{*}_{p}n} \mu_p^*(d)g(n-d) = \mu_p^{*}*_u g(n)$. Conversely, if $f = \mu_p^{*}*_u g$, then $g = I*_u f$.

PROOF. $g(n) = \sum_{d|{}^{*}_{p}n} f(d) = \sum_{d|{}^{*}_{p}n} f(d)I(n-d) = f*_u I(n)$; so

$\mu_p^{*}*_u g = g*_u \mu_p^* = (f*_u I)*_u \mu_p^* = f*_u (I*_u \mu_p^*) = f*_u u = f$. Conversely, if $f = \mu_p^{*}*_u g$, then $I*_u f = I*_u(\mu_p^{*}*_u g) = (I*_u \mu_p^*)*_u g = u*_u g = g$.

THEOREM 3.4. If f is a p-factorable function and g is the inverse of f under $*_u$, then g is p-factorable.

PROOF. Suppose $(m,n)_p = 0$. If $m=0$ or $n=0$, then $g(m+n) = g(m)g(n)$. For $m>0$, $n>0$, suppose that $(x,y)_p = 0$ implies that $g(x+y) = g(x)g(y)$ for all x and y with $x + y < m + n$. Now, every p-factor of $m + n$ can

be written in the form $a + c$, where $a \mid_p m$, $c \mid_p n$; and since $(m,n)_p = 0$ we have $(a,c)_p = 0$. Hence $f(a+c) = f(a)f(c)$. Then

$$0 = u(m+n) - u(m)u(n)$$

$$= f *_u g(m+n) - (f *_u g(m))(f *_u g(n))$$

$$= \sum_{\substack{a+b=m,\, c+d=n \\ (a,b)_p=(c,d)_p=0}} f(a+c)g(b+d)$$

$$- \left(\sum_{\substack{a+b=m \\ (a,b)_p=0}} f(a)g(b) \right) \left(\sum_{\substack{c+d=n \\ (c,d)_p=0}} f(c)g(d) \right)$$

$$= \sum_{\substack{a+b=m,\, c+d=n \\ (a,b)_p=(c,d)_p=0}} f(a+c)[g(b+d) - g(b)g(d)]$$

$$= f(0)[g(m+n) - g(m)g(n)]$$

$$+ \sum_{\substack{a+b=m,\, c+d=n \\ (a,b)_p=(c,d)_p=0 \\ a+c>0}} f(a+c)[g(b+d) - g(b)g(d)].$$

Now $(b,d)_p = 0$, and the requirement that $a + c > 0$ together with $(a+c) + (b+d) = m + n$ implies that $b + d < m + n$; so the last sum is zero. Since f is invertible, $f(0) \neq 0$ (in fact, $f(1) = 1$). So we must have that $g(m+n) = g(m)g(n)$.

COROLLARY 1. Let $h = f *_u g$. If any two of the functions f, g, h are p-factorable, then so is the third.

PROOF: Suppose that f and g are p-factorable and that $(m,n)_p = 0$. If $m = 0$ or $n = 0$, then $h(m + n) = h(m)h(n)$. For $m > 0$, and $n > 0$,

$$h(m)h(n) = (f *_u g(m))(f *_u g(n)) = \Big(\sum_{\substack{a+b=m \\ (a,b)_p=0}} f(a)g(b)\Big)\Big(\sum_{\substack{c+d=n \\ (c,d)_p=0}} f(c)g(d)\Big)$$

$$= \sum_{\substack{a+b=m,\, c+d=n \\ (a,b)_p=(c,d)_p=0}} f(a)f(c)g(b)g(d)$$

$$= \sum_{\substack{(a+c)+(b+d)=m+n \\ (a+c,b+d)_p=0}} f(a+c)g(b+d) = h(m+n).$$

If h and f are p-factorable, then $g = f^{-1} * h$, and g is p-factorable. Similarly, if h and g are p-factorable, then f is p-factorable.

COROLLARY 2. Let $g(n) = \sum_{d \mid_p^* n} f(d)$. If f is p-factorable, then g is p-factorable, and conversely.

DEFINITION 3.3. We define $\tau_p^*(n) = \sum_{d \mid_p^* n} 1$ = the number of unitary p-factors of n.

THEOREM 3.5. $\tau_p^*(n) = 2^{\omega_p(n)} = I *_u I(n)$.

PROOF. $\tau_p^*(0) = 1 = 2^0 = 2^{\omega p(0)}$. If $n = ap^r$, $0 < a < p$, then $\tau_p^*(n) = 2 = 2^1 = 2^{\omega p(n)}$. Suppose $n = \sum_{i=1}^{k} a_i p^{r_i}$, $0 < a_i < p$,

$r_1 < \ldots < r_k$, and $\tau_p^*(n) = 2^{\omega_p(n)} = 2^k$. Let $n' = \sum_{i=1}^{k+1} a_i p^{r_i}$, $0 < a_i < p$, $r_1 < \ldots < r_k < r_{k+1}$. Then

$$\tau_p^*(n') = \sum_{d \mid_p^* n'} 1 = \sum_{\substack{d \mid_p n' \\ (d,n'-d)_p=0}} 1 = \sum_{\substack{d \mid_p n \\ (d,n-d)_p=0}} 1 + \sum_{\substack{d \mid_p n \\ (d+a_{k+1}p^{r_{k+1}},n-d)_p=0}} 1$$

$$= \tau_p^*(n) + \tau_p^*(n) = 2\tau_p^*(n) = 2 \cdot 2^{\omega_p(n)} = 2^{\omega_p(n')}.$$

DEFINITION 3.4. $\tau_{pk}^*(n) = \underbrace{I *_u I *_u \ldots *_u I}_{k \text{ factors}}$, $k \geq 2$.

COROLLARY. $\tau_{pk}^*(n) = k^{\omega_p(n)} = \tau_{pk-1}^* *_u I(n)$.

We note that μ_p^* and τ_p^* are both p-factorable.

The above theorems and definitions are analogs of some results due to Carlitz [1]. We now proceed to develop analogs of the other arithmetic functions discussed in Chapter II.

DEFINITION 3.5. We will denote by $s^*(n)$ the sum of the unitary p-factors of n.

THEOREM 3.6. $s^*(n) = \frac{n\tau_p^*(n)}{2} = n \cdot 2^{\omega_p(n)-1}$.

PROOF. $S^*(0) = 0 = \frac{0\tau_p^*(n)}{2}$. If $n = ap^r$, $0 < a < p$, then

$s^*(n) = 0 + ap^r = \frac{ap^r \cdot 2}{2} = \frac{n\tau_p^*(n)}{2}$. Suppose $n = \sum_{i=1}^{k} a_i p^{r_i}$, $0 < a_i < p$, $r_1 < \ldots < r_k$, and $s^*(n) = \frac{n\tau_p^*(n)}{2}$. Let $n' = \sum_{i=1}^{k+1} a_i p^{r_i}$, $0 < a_i < p$,

$r_1 < \ldots < r_k < r_{k+1}$. Then

$$s^*(n') = \sum_{d|_p^* n'} d = \sum_{d|_p^* n} d + \sum_{d|_p^* n} (d + a_{k+1}p^{r_{k+1}})$$

$$= s^*(n) + \sum_{d|_p^* n} d + \sum_{d|_p^* n} a_{k+1}p^{r_{k+1}} = s^*(n) + s^*(n) + a_{k+1}p^{r_{k+1}}\tau_p^*(n)$$

$$= n\tau_p^*(n) + a_{k+1}p^{r_{k+1}}\tau_p^*(n) = n'\tau_p^*(n)$$

$$= \frac{n'\tau_p^*(n')}{2}.$$

The second equality follows immediately from Theorem 3.5.

DEFINITION 3.6. $\sigma_p^*(n) = \sum_{d|_p^* n} p^d$;

$$\sigma_{pk}^*(n) = \sum_{d|_p^* n} p^{kd}.$$

THEOREM 3.7. If $n = \sum_{i=1}^{k} a_i p^{r_i}$, $0 < a_i < p$, $r_1 < \ldots < r_k$, then

$\sigma_p^*(n) = \prod_{i=1}^{k} (1+p^{a_i p^{r_i}})$, and $\sigma_p^*(0) = 1$.

PROOF. $\sigma_p^*(0) = p^0 = 1$. If $n = ap^r$, $0 < a < p$, then $\sigma_p^*(n) = p^0 + p^{ap^r}$ $= 1 + p^{ap^r}$. σ_p^* is p-factorable by Theorem 3.4; so if $n = \sum_{i=1}^{k} a_i p^{r_i}$ then $\sigma_p^*(n) = \prod_{i=1}^{k} (1+p^{a_i p^{r_i}})$.

COROLLARY. If $n = \sum_{i=1}^{k} a_i p^{r_i}$, $0 < a_i < p$, $r_1 < \ldots < r_k$, then $\sigma^*_{pk}(n) = \prod_{i=1}^{k}(1+p^{ka_i p^{ri}})$, and $\sigma^*_{pk}(0) = 1$.

DEFINITION 3.7. $\phi^*_p(n) = \sum_{d \mid^*_p n} p^d \mu^*_p(n-d)$

$$\phi^*_{pk}(n) = \sum_{d \mid^*_p n} p^{dk} \mu^*_p(n-d).$$

THEOREM 3.8. If $n = \sum_{i=1}^{k} a_i p^{r_i}$, $0 < a_i < p$, $r_1 < \ldots < r_k$, then $\phi^*_p(n) = \prod_{i=1}^{k}(p^{a_i p^{r_i}} - 1)$ and $\phi^*_p(0) = 1$.

PROOF. $\phi^*_p(0) = p^0 \mu^*_p(0) = 1$. If $n = ap^r$, $0 < a < p$, then $\phi^*_p(n) = p^0 \mu^*_p(ap^r) + p^{ap^r} \mu^*_p(0) = p^{ap^r} - 1$. By Theorem 3.4, ϕ^*_p is p-factorable; so if $n = \sum_{i=1}^{k} a_i p^{r_i}$, $\phi^*_p(n) = \prod_{i=1}^{k}(p^{a_i p^{r_i}} - 1)$.

COROLLARY. If $n = \sum_{i=1}^{k} a_i p^{r_i}$, $0 < a_i < p$, $r_1 < \ldots < r_k$, then $\phi^*_{pk}(n) = \prod_{i=1}^{k}(p^{ka_i p^{r_i}} - 1)$ and $\phi^*_{pk}(0) = 1$.

THEOREM 3.9. $\sum_{d \mid^*_p n} \mu^*_p(d) = u(n)$.

PROOF. $\sum_{d \mid^*_p n} \mu^*_p(d) = \mu^* *_u I(n) = u(n)$.

DEFINITION 3.8. We define a to be the greatest common unitary p-factor of m and n if $a = (m,n)_p^*$ is the largest common p-factor of m and n such that $(a,m-a)_p = (a,n-a)_p = 0$; i.e., if $m = \sum_{i=0}^{r} a_i p^i$ and $n = \sum_{i=0}^{s} b_i p^i$, $0 \le a_i, b_i < p$, then $(m,n)_p^* = \sum_{i=0}^{\min\{r,s\}} c_i p^i$, where $c_i = 0$ unless $a_i = b_i$, in which case $c_i = a_i = b_i$.

DEFINITION 3.9. Let m be a fixed nonnegative integer. For any n, let $a = (m,n)_p^*$ and $n = N + a$. We define $c_{np}^*(m) = \sum_{d|_p^* a} p^d \mu_p^*(n-d)$.

THEOREM 3.10. $c_{np}^*(m) = \dfrac{\mu_p^*(N)\phi_p^*(n)}{\phi_p^*(N)} = \mu_p^*(N)\phi_p^*(a)$.

PROOF. $c_{np}^*(m) = \sum_{d|_p^* a} p^d \mu_p^*(n-d) = \sum_{d|_p^* a} p^{a-d} \mu_p^*(n-a+d) = p^a \sum_{d|_p^* a} \dfrac{\mu_p^*(N+d)}{p^d}$

$$= p^a \sum_{d|_p^* a} \frac{\mu_p^*(N)\mu_p^*(d)}{p^d}, \text{ since } (N,d)_p = 0,$$

$$= p^a \mu_p^*(N) \sum_{d|_p^* a} \frac{\mu_p^*(d)}{p^d}.$$

Now $\sum_{d|_p^* a} \dfrac{\mu_p^*(d)}{p^d} = 1 - \sum_{bp^r|_p^* a} \dfrac{1}{p^{p^r}} + \sum_{b_1 p^{r_1} + bp_2^{r_2}|_p^* a} \dfrac{1}{p^{b_1 p^{r_1}}\, p^{b_2 p^{r_2}}} - \cdots$

$$= \prod_{bp^r|_p^* a} (1 - \frac{1}{p^{bp^r}}) = p^{-a} \prod_{bp^r|_p^* a} (p^{bp^r} - 1) = p^{-a}\, \phi_p^*(a)$$

$$= \frac{\phi_p^*(n)}{p^a \phi_p^*(N)}.$$

Hence $c^*_{np}(m) = \dfrac{\mu^*_p(N)\phi^*_p(n)}{\phi^*_p(N)} = \mu^*_p(N)\phi^*_p(a)$.

COROLLARY. $c^*_{np}(m)$ is p-factorable; i.e., if $(k,n)_p = 0$, then

$$c^*_{(k+n)p}(m) = c^*_{kp}(m)c^*_{np}(m).$$

DEFINITION 3.10. $\Lambda^*_p(n) = \log(p) \sum_{d \mid^*_p n} \mu^*_p(d)(n-d)$.

THEOREM 3.11. $\Lambda^*_p(n) = \begin{cases} n\log(p), \text{ if } n = ap^r,\ 0 < a < p \\ 0, \text{ otherwise.} \end{cases}$

PROOF. $\Lambda^*_p(0) = \log(p)\mu^*_p(0)(0) = 0$. If $n = ap^r$, then

$$\Lambda^*_p(n) = \log(p)(\mu^*_p(0)n + \mu^*_p(n)\cdot 0)$$

$$= n\log(p).$$

Suppose $n = \sum_{i=1}^{m} a_i p^{r_i}$, $0 < a_i < p$, $r_1 < \ldots < r_m$, $m \geq 2$.

Let $n' = n - a_m p^{r_m}$. Then

$$\Lambda^*_p(n) = \log(p) \sum_{d \mid^*_p n} \Lambda^*_p(d)(n-d)$$

$$= \log(p)\Big[\sum_{d \mid^*_p n'} \mu^*_p(d)(n-d) + \sum_{d \mid^*_p n'} \mu^*_p(d+a_m p^{r_m})(n'-d)$$

$$= \log(p)\Big[\sum_{d \mid_p^* n'} \mu_p^*(d)(n'-d) + \sum_{d \mid_p^* n'} \mu_p^*(d) a_m p^{r_m} - \sum_{d \mid_p^* n'} \mu_p^*(d)(n'-d) \Big]$$

$$= \log(p) \cdot a_m p^{r_m} \sum_{d \mid_p^* n'} \mu_p^*(d)$$

$$= 0.$$

CHAPTER IV

LUCAS-PERFECT AND LUCAS-AMICABLE NUMBERS

There are least two ways of defining analogs of perfect numbers and amicable numbers in terms of Lucas functions. We recall that the analog of the σ-function is $\sigma_p(n) = \sum_{d|_p n} p^d$. σ_p is a strictly increasing function, since, for $m < n$, $\sigma_p(m) = \sum_{d|_p m} p^d < p^n \leq \sigma_p(n)$. So $\sigma_p(m) = \sigma_p(n)$ iff $m = n$. Hence some other analog of amicability must be found.

THEOREM 4.1. $\sigma_p(n) \neq 2n$ for all p and n.

PROOF. $0|_p n$ for all p and n $\Longrightarrow 1|_p \sigma_p(n)$ for all p and n. So if $\sigma_p(n) = 2n$, then p is odd.

$p^n|_p \sigma_p(n)$ for all p and n, and $p^n > 2n$ for $p > 2$, hence $\sigma_p(n) > 2n$.

One relation that exists between n and $\sigma_p(n)$ is that the sum of the exponents of the p-adic expansion of $\sigma_p(n)$ is sometimes equal to a multiple of n. The p-adic expansion of $\sigma_p(n)$ is given by its definition $\sigma_p(n) = \sum_{d|_p n} p^d$; so the sum of the exponents is given by $\sum_{d|_p n} d = s_p(n) = \frac{n\tau_p(n)}{2}$. Clearly $s_p(n)$ is a multiple of n only if $\tau_p(n)$ is even. Moreover it is easily shown that $s_p(n) = 2n$ if and only if either $n = p^r + p^s$ with $r \neq s$ or $n = 3p^r$ $(p > 3)$.

We could define a number n to be <u>Lucas perfect</u> (or <u>p-perfect</u>) iff $s_p(n) = 2n$, <u>triply Lucas perfect</u> (or <u>triply p-perfect</u>) iff $s_p(n) = 3n$, etc.

THEOREM 4.2. Let m be a fixed positive integer. Then $s_p(n) = mn$ iff $\tau_p(n) = 2m$.

PROOF. If $\tau_p(n) = 2m$, then $s_p(n) = \frac{n \cdot 2m}{2} = mn$. Conversely if $s_p(n) = mn$, then $n\tau_p(n) = 2mn$; and $\tau_p(n) = 2m$.

This means that if $n = \sum_{i=1}^{k} a_i p^{r_i}$ $(0 < a_i < p,\ r_1 < \ldots < r_k)$, then $s_p(n) = mn$ iff $2m = M_1 \cdot \ldots \cdot M_k$, where $M_i = a_i + 1$ $(i = 1, \ldots, k)$. Hence given any number m, we can list all the types of numbers n such that $s_p(n) = mn$. For example, if we take $m = 6$, then $2m = 2 \cdot 6 = 12$, and $12 = 2 \cdot 6 = 3 \cdot 4 = 2 \cdot 2 \cdot 3$. The following numbers are the <u>only</u> numbers n with $s_p(n) = 6n$:

$n = 0$ (Of course $s_p(0) = 0 = k \cdot 0$ for all positive integers k.)

$n = 11p^r$ $(p > 11)$

$n = p^r + 5p^s$ $(p > 5,\ r \neq s)$

$n = 2p^r + 3p^s$ $(p > 3,\ r \neq s)$

$n = p^r + p^s + 2p^t$ $(p > 2;\ r \neq s, t;\ s \neq t)$.

We could define two numbers m and n to be <u>Lucas amicable</u> (or p-amicable) iff $s_p(m) = s_p(n)$. There is no clear condition that is both necessary and sufficient for a pair of numbers to be p-amicable. However, the following theorem is easily proven.

THEOREM 4.3. Let $m = \sum_{i=1}^{k} a_i p^{r_i}$, $n = \sum_{i=1}^{t} b_i p^{s_i}$ $(0 < a_i, b_i < p;\ r_1 < \ldots < r_k;\ s_1 < \ldots < s_t)$. If m and n are p-amicable, then so are $m_j = \sum_{i=1}^{k} a_i p^{r_i+j}$ and $n_j = \sum_{i=1}^{t} b_i p^{s_i+j}$ for all j with $\min\{r_1+j, s_1+j\} \geq 0$.

PROOF. $s_p(m_j) = \frac{m_j \tau_p(m_j)}{2} = \frac{1}{2}\left(\sum_{i=1}^{k} a_i p^{r_i+j}\right) \prod_{i=1}^{k} (a_i+1)$

$$= \frac{p^j}{2}\left(\sum_{i=1}^{k} a_i p^{r_i}\right) \prod_{i=1}^{k} (a_i+1) = \frac{p^j m \tau_p(m)}{2} = p^j s_p(m).$$

Similarly $s_p(n_j) = p^j s_p(n)$. And since $s_p(m) = s_p(n)$, we have $s_p(m_j) = s_p(n_j)$.

THEOREM 4.4. There are no 2-amicable pairs of numbers.

PROOF. Let $m = \sum_{i=1}^{k} 2^{r_i}$, $n = \sum_{i=1}^{t} 2^{s_i}$ $(r_1 < \ldots < r_k, s_1 < \ldots < s_t)$, and suppose that $s_2(m) = s_2(n)$. Then $2^{k-1} \sum_{i=1}^{k} 2^{r_i} = 2^{t-1} \sum_{i=1}^{t} 2^{s_i}$; and $\sum_{i=1}^{k} 2^{r_i+k-1} = \sum_{i=1}^{t} 2^{s_i+t-1}$. Since 2-adic expansions are unique, we must have $k = t$ and $r_i = s_i$ for all i. Hence $s_2(m) = s_2(n) \Longrightarrow m = n$.

We list here some p-amicable pairs of numbers for p = 3, 5, 7, 13. $2 \cdot 3^k$ and 3^{k+1} are 3-amicable for $0 \leq k < \infty$. $4 \cdot 5^k + 2 \cdot 5^{k+1}$ and $1 \cdot 5^k + 4 \cdot 5^{k+1}$ are 5-amicable for $0 \leq k < \infty$. $6 \cdot 7^k$ and $2 \cdot 7^{k+1}$, $4 \cdot 7^k + 5 \cdot 7^{k+1}$ and $2 \cdot 7^k + 2 \cdot 7^{k+1} + 1 \cdot 7^{k+2}$, $6 \cdot 7^k + 1 \cdot 7^{k+2}$ and $4 \cdot 7^{k+1} + 1 \cdot 7^{k+2}$, $5 \cdot 7^k + 1.7^{k+1}$ and $2 \cdot 7^k + 2 \cdot 7^{k+1}$ are 7-amicable for $0 \leq k < \infty$. $7 \cdot 13^k$ and $1 \cdot 13^k + 1 \cdot 13^{k+1}$, $9 \cdot 13^k$ and $2 \cdot 13^k + 1 \cdot 13^{k+1}$, $12 \cdot 13^k$ and $3 \cdot 13^{k+1}$, $7 \cdot 13^k + 1 \cdot 13^{k+1}$ and $1 \cdot 13^k + 3 \cdot 13^{k+1}$, $6 \cdot 13^k + 2 \cdot 13^k + 3 \cdot 13^{k+1}$, $7 \cdot 13^k + 2 \cdot 13^{k+1}$ and $1 \cdot 13^k + 5 \cdot 13^{k+1}$ are 13-amicable for $0 \leq k < \infty$.

CONJECTURE. There are no 11-amicable pairs of numbers

Another possible way to define an analog of perfect numbers is as follows: We could say that a number n is p-perfect iff $n \mid_p \sigma_p(n)$. Since $\sigma_p(n) = \sum_{d \mid_p n} p^d$, it follows immediately that $n = \sum_{i=1}^{k} p^{r_i}$ $(r_1 < \ldots < r_k)$ and that $r_i \mid_p n$ for all i. Moreover if $n = \sum_{i=1}^{k} p^{r_i}$ where $r_i \mid_p n$ for all i, then $n \mid_p \sigma_p(n)$. This gives us

THEOREM 4.5. $n \mid_p \sigma_p(n) \iff n = \sum_{i=1}^{k} p^{r_i}$ $(r_1 < \ldots < r_k)$, where $r_i \mid_p n$ for $i = 1, \ldots, k$.

We list here some numbers n such that $n \mid_p \sigma_p(n)$ for p = 2, 3, 5.

p = 2; n = 0, 1, 3, 7, 11, 15.

p = 3; n = 0, 1, 4, 31, 112.

p = 5; n = 0, 1, 6, 3131.

Since 0 is a p-factor of every nonnegative integer it follows that $0 \mid_p \sigma_p(0)$ and $1 \mid_p \sigma_p(1)$ for all primes p.

THEOREM 4.6. If $n \mid_p \sigma_p(n)$ and $n \neq 0$, then $1 \mid_p n$. Moreover, if $n > 1$, then $1 + p \mid_p n$.

PROOF. If $n \mid_p \sigma_p(n)$ and $n \neq 0$ then by Theorem 4.5, $n = p^{r_1} + \ldots + p^{r_n}$ $(r_1 < \ldots < r_n)$, where $r_i \mid_p n$ for $i = 1, \ldots, n$. Now $r_1 \mid_p n$ and $r_1 < p^{r_1}$ (since $p \geq 2$) implies that $r_1 = 0$; hence $p^{r_1} = 1$ and $1 \mid_p n$.

If $n > 1$, then $k \geq 2$, $n = 1 + p^{r_2} + \ldots + p^{r_n}$, $0 < r_2$, $r_2 \mid_p n$, and $r_2 < p^{r_2} \Rightarrow r_2 = 1$. Hence $p^{r_2} = p^1 = p$ and $1 + p \mid_p n$.

NOTE. Because of the form of n and the fact that $r_i \Big|_p n$ for all i, it is clear that the r_i's must be of the form 0, 1, p, p^p, p^{p^p}, ... or sums of such numbers.

If we define p-perfect numbers as above, we could define two numbers m and n to be p-amicable iff $m \Big|_p \sigma_p(n)$ and $n \Big|_p \sigma_p(m)$.

THEOREM 4.7. $m \Big|_p \sigma_p(n)$ and $n \Big|_p \sigma_p(m)$ iff $m = \sum_{i=1}^{k} p^{r_i}$, $n = \sum_{i=1}^{t} p^{s_i}$ $(r_1 < \ldots < r_k, s_1 < \ldots < s_k)$; and $r_i \Big|_p n$ $(i = 1, \ldots, k)$, $s_i \Big|_p m$ $(i = 1, \ldots, t)$.

PROOF. Obvious.

We tabulate in Table 1 some pairs (m,n) such that $m \Big|_p \sigma_p(n)$ and $n \Big|_p \sigma_p(m)$ for p = 2, 3, 5.

Table 1

Table of p-amicable pairs

p	2		3		5	
	m	n	m	n	m	n
0	1	0	1	0	1	
1	2	1	3	1	5	
1	3	1	4	1	6	
2	5	3	28	5	3126	
3	5	4	28	6	3126	
3	6	4	31	6	3131	
3	7	4	82	6	15626	
3	9	4	85	6	15631	
3	11	4	109	6	18751	
3	13	4	112	6	18756	
3	15					

CHAPTER V

ON THE ZERO DIVISORS OF L

Cashwell and Everett [3] have shown that the ring of arithmetic functions under addition and the Dirichlet product is a unique factorization domain. Carlitz [1] has shown that the ring L of arithmetic functions under addition and the Lucas product contains zero divisors, and hence cannot be a unique factorization domain. The characterization of the zero divisors of L poses an interesting problem in number theory. Carlitz [1] has shown that if the ranges of the elements of L are contained in a field of characteristic p (p a prime), then an element f of L is a zero divisor if and only if f is singular, and that every zero divisor is nilpotent. We will establish here some results toward characterizing the zero divisors of L when the ranges of the elements of L are contained in a field of characteristic zero.

5.1. On the Nilpotent Elements of L. Carlitz [1] has proven the following theorem.

THEOREM 5.1. If $\psi_{m_1}, \ldots, \psi_{m_k}$, are the characteristic functions at $m_1, \ldots, m_k$, respectively; if $f_1, \ldots, f_k$, are arbitrary functions; and if

$$f = f_1 * \psi_{m_1} + \ldots + f_k * \psi_{m_k} \qquad (5.1)$$

then $f^c = z$ for $c > k(p-1)$.

(Recall that z is the zero function of L; i.e., $z(n) = 0$ for all $n \in N$.)

If f has the form (5.1) then c may actually be less than $k(p-1)$; for if $p = 3$ and $f : N \to C$ is defined by

$$f(2+2\cdot 3) = c \neq 0, \qquad f(2+2\cdot 3^3) = -i,$$

$$f(2+2\cdot 3^2) = i, \qquad f(2\cdot 3+2\cdot 3^3) = 1,$$

$$f(2\cdot 3+2\cdot 3^2) = -1, \qquad f(2\cdot 3^2+2\cdot 3^3) = -2i/c,$$

and $f(n) = 0$ for $n \neq 2 + 2 \cdot 3,\ 2 + 2 \cdot 3^2,\ 2 \cdot 3 + 2 \cdot 3^2,\ 2 + 2 \cdot 3^3,\ 2 \cdot 3 + 2 \cdot 3^3,\ 2 \cdot 3^2 + 2 \cdot 3^3$; then $f^2 = z$. But $f = f_1 * \psi_1 + f_2 * \psi_3 + f_3 * \psi_{3^2}$, where

$$f_1(n) = \begin{cases} c, & \text{if } n = 1 + 2 \cdot 3 \\ i, & \text{if } n = 1 + 2 \cdot 3^2 \\ -i, & \text{if } n = 1 + 2 \cdot 3^3 \\ 0, & \text{otherwise.} \end{cases}$$

$$f_2(n) = \begin{cases} -1, & \text{if } n = 3 + 2 \cdot 3^2 \\ 1, & \text{if } n = 3 + 2 \cdot 3^3 \\ 0, & \text{otherwise} \end{cases}$$

$$f_3(n) = \begin{cases} -2i/c, & \text{if } n = 3^2 + 2 \cdot 3^3 \\ 0, & \text{otherwise.} \end{cases}$$

Here $(p-1)k = 2 \cdot 3 = 6$, but c can be equal to 2. Moreover $f^c = z$ for $c > 2$. In this case, f cannot be written as the sum of less than three functions of the form $f_i * \psi_{m_i}$.

Carlitz [1] conjectures that a function f is a zero divisor of L if and only if f is of the form (5.1). If this is the case, then every zero divisor will be nilpotent.

Carlitz [1] showed that every zero divisor is singular. However, there are singular functions that are not zero divisors; e.g.,

$$f(n) = \begin{cases} 0, & n = 0, \\ 1, & n > 0, \end{cases}$$

is a singular function that is not a zero divisor for $p > 2$. The proof of this is as follows.

Suppose that $f*g = z$ for some $g \in L$. Then

$$0 = f*g(1) = f(0)g(1) + f(1)g(0) = g(0).$$

Now suppose that $g(n) = 0$ for all n with $0 \leq n < t$ for some $t > 0$.

If $1 \mid_p t+1$, then

$$0 = f*g(t+1) = \sum_{d \mid_p t+1} f(d)g(t+1-d)$$

$$= \sum_{\substack{d \mid_p t \\ d>1}} f(d)g(t+1-d) + \sum_{\substack{d \mid_p t \\ d+1 \nmid_p t}} f(d+1)g(t-d)+f(1)g(t), \quad \text{(since } f(0) = 0\text{)}$$

$$= f(1)g(t),$$

since $d > 1$ implies that $t-d < t+1-d < t$. So $g(t-d) = g(t+1-d) = 0$. Hence $0 = f(1)g(t) = g(t)$.

If $1 \nmid_p t+1$, let r be the least positive integer such that $p^r \mid_p t+p^r$. Then $m \mid_p t$, where $m = \sum_{i=0}^{r-1} (p-1)p^t$, $t + p^r - m = t + 1$, and $t + 1 \mid_p t+p^r$. Also $t \nmid_p (t+p^r - m + 1)$. We have

$$0 = f*g(t+p^r - m+1) = \sum_{\substack{d \mid_p t-m \\ d>1}} f(d)g(t+p^r-m+1-d)$$

$$+ \sum_{\substack{d \mid_p t-m \\ d+p^r \nmid_p t-m}} f(d+p^r)g(t-m+1-d) + f(1)g(t+p^r-m)+f(1+p^r)g(t-m).$$

Now $d > 1 \Longrightarrow d \geq p^r$; so $t + p^r - m + 1 - d < t - m + 1 < t$, and $t - m + 1 - d < t - m + 1 - p^r < t$. So $g(t + p^r - m + 1 - d)$ $= g(t - m + 1 - d) = 0$. Also $g(t - m) = 0$ since $t - m < t$. Hence

$$0 = f(1)g(t + p^r - m) = g(t + p^r - m) = g(t + 1).$$

Suppose $g(t + p^r - m + i) = g(t + i + 1) = 0$ for $i = 0, 1, \ldots,$ $k < m - 1$. Then

$$0 = f*g(t + p^r - m + k + 2) = \sum_{i=0}^{k+1} \sum_{\substack{d \mid_p t-m \\ d>0}} f(d+i)g(t+p^r-m+k+2-d-i)$$

$$+ \sum_{i=0}^{k+1} \sum_{\substack{d \mid p^{t-m} \\ d>0}} f(d+i+p^r)g(t-m+k+2-d-i)$$

$$+ \sum_{i=0}^{k+1} \sum_{d \mid p^{t-m}} f(i)g(t+p^r+k+2-i) \ .$$

$d > 0 \Longrightarrow d \geq p^r$; so $t + p^r - m + k + 2 - d - i \leq t - m + k + 2 - i < t$ for $i = 0, 1, \ldots, k+1$. Hence $g(t + p^r - m + k + 2 - d - i) = 0$ for $i = 0, 1, \ldots, k + 1$. Also $g(t + p^r + k + 2 - i) = 0$ for $i = 0, 1, \ldots, k$. So

$$0 = f(1)g(t + p^r + k + 2 - 1) = g(t + p^r + k + 1).$$

Now

$$0 = f*g(t+p^r) = \sum_{\substack{d \mid p^t \\ d \neq p^r}} f(d)g(t+p^r-d) + \sum_{d \mid p^t} f(d+p^r)g(t-d)+f(p^r)g(t)$$

$$= f(p^r)g(t)$$

$$= g(t).$$

By similar methods we can show that the function

$$f(n) = \begin{cases} 1, n = p^r, \ r = 0, 1, 2, \ldots \\ 0, n \neq p^r \end{cases}$$

is singular but not a zero divisor for $p > 2$.

DEFINITION 5.1. If $n = \sum_{i=1}^{k} a_i p^{r_i}$, $0 < a_i < p$, $r_1 < \ldots < r_k$, $k \geq 1$, we define $\delta_p(n) = p^{r_1}$, $\delta_p(0) = 0$.

DEFINITION 5.2. If f is any singular function, we define

$$S_f = \{n \in N^* : f(n) \neq 0\},$$

where N^* is the set of positive integers.

DEFINITION 5.3. Any singular function that is of the type (5.1) will be called a Carlitz-type nilpotent function.

If f is a Carlitz-type nilpotent function, then there is a function $g \neq z$ such that $f*g = z$. However g is not necessarily unique for any fixed f. We consider the following example.

EXAMPLE 5.1. Let $S_f = \{n \in N^* : \delta_3(n) = 3 \text{ or } \delta_3(n) = 9\}$. We define the function f as follows: $f(n) \neq 0$ for $n \in S_f$; $f(n) = 0$ for $n \notin S_f$.

Now f is a Carlitz-type nilpotent element; hence f is a zero divisor, and there is a $g \in L$ such that $f*g = z$ with $g \neq z$. We would like to find a "maximal" g such that $f*g = z$; i.e., a $g \in L$ with $f*g = z$ and $S_g = \{n \in N^* : g(n) \neq 0\}$ maximal.

A minimal g such that $f*g = z$ and $g \neq z$ is any $g \in L$ with $S_g = \{m\}$, where $24 = 2 \cdot 3 + 2 \cdot 9$ is a 3-factor of m. This works because $f*g(n) = \sum_{d|_3 n} f(d)g(n-d)$, where $f*g$ contains non-zero terms iff $f(d) \neq 0$ and $g(n-d) \neq 0$. Now $g(n-d) \neq 0$ only if $n - d = m$, and if $d|_3 n$, then $n - d|_3 n$ and $n - d = m \Rightarrow 3 \nmid_3 d$, $9 \nmid_3 d$, and $d \notin S_f$; so $f(d) = 0$.

On the other hand, if $d \in S_f$, then $3|_3 d$ or $9|_3 d$ and $n - d|_3 n$; so $n - d \neq m$. Hence for all n, $f*g(n)$ contains only zero tems, and $f*g(n) = 0$. Similarly, if S_g contains only numbers of which 24 is a 3-factor, then $f*g = z$.

To find a "maximal" g, we first examine what happens to $g(3^r)$, $r \geq 0$.

$$0 = f*g(1 + 3) = f(3)g(1) \Longrightarrow g(1) = 0.$$

$$0 = f*g(2\cdot 3) = f(3)g(3) \Longrightarrow g(3) = 0.$$

$$0 = f*g(2\cdot 9) = f(9)g(9) \Longrightarrow g(9) = 0.$$

For $r > 2$, $f*g(3+3^r) = f(3)g(3^r) + f(3+3^r)g(0) = f(3)g(3^r)$. (Carlitz [1] established that all zero divisors are singular.) Hence $g(3^r) = 0$ for $r = 1, 2, \ldots$.

Hereafter, in order to keep continuity of discussion, proofs of all statements will be left until the end of this discussion.

It is easily shown by mathematical induction that $g(\sum_{i=1}^{k} 3^{r_i}) = 0$ $2 < r_1 < \ldots < r_k$. Similarly,

$$g(1 + \sum_{i=1}^{k} 3^{r_i}) = g(2 + \sum_{i=1}^{k} 3^{r_i}) = g(3 + \sum_{i=1}^{k} 3^{r_i})$$

$$= g(1 + 3 + \sum_{i=1}^{k} 3^{r_i}) = g(2 + 3 + \sum_{i=1}^{k} 3^{r_i}) = g(9 + \sum_{i=1}^{k} 3^{r_i})$$

$$= g(1 + 9 + \sum_{i=1}^{k} 3^{r_i}) = g(2 + 9 + \sum_{i=1}^{k} 3^{r_i}) = 0. \qquad (5.2)$$

If

$$t = \sum_{i=1}^{k} \varepsilon_i 3^{r_i},\ \varepsilon_i = 1 \text{ or } 2,\ 2 < r_1 < \ldots < r_k, \qquad (5.3)$$

then it is easy (but tedious) to show that $g(t) = 0$, by induction on the number of ε_i's that are equal to 2 and on the length of t. By using (5.2) together with induction on the number of ε_i's that are equal to 2 and on the length of n, one can also show that $g(1+t) = g(2+t) = g(3+t) = g(1+3+t) = g(2+3+t) = g(9+t) = g(1+9+t) = g(2+9+t) = 0$, where t is as in (5.3).

If $n = 6$ or $6 + t$ (t as in (5.3)), then $g(n)$ is not uniquely determined by f and $g(d)$ for $d < n$.

If $n = 3 + 9$ or $3 + 9 + t$ or $2 \cdot 9$ or $2 \cdot 9 + t$ (t as in (5.3)), then $g(n)$ is uniquely determined by f and $g(m)$ for $m = 6$ or $6 + t$ $(6 + t < n)$. $g(n)$ may, in fact, be equal to zero in this instance, depending on how f is defined for elements of S_f. It is not clear whether or not we could define f in such a way as to prevent getting zero images under g for all n of this type since, for sufficiently large n, $g(n)$ may have large numbers of non-zero terms, both + and -, containing $g(6)$ or $g(6+t)$. In this case, one cannot guarantee that the terms will add up to zero. So there is probably at most a finite number of elements $6 + t$ with non-zero images under g.

We can now separate the nonnegative integers into three sets, depending on their images under g, as follows.

S_U = {n ε N : g(n) is uniquely determined by f and g(d) (d < n)};

S_I = {n ε N^* : $24 \mid_3 n$};

S_t = {n ε N^* : $6 \mid_3 n$, $24 \nmid_3 n$}.

We could further divide S_U into S_6 = {n ε N^* : g(n) is uniquely determined by f and g(6) or g(6+t), t as in (5.3)} and S_0 = {0, t, 1+t, 2+t, 3+t, 1+3+t, 2+3+t, 9+t, 1+9+t, 2+9+t : t as in (5.3)}. Note that for n ε S_I, g(n) is totally independent of f and g(m) for m ≠ n; while for n ε S_t, g(n) is not uniquely determined by f and g(d) for d < n, but g(n) is not totally independent of f and g.

PROOFS. Let $K = \sum_{i=1}^{k} 3^{r_i}$, $2 \leq r_1 < \ldots < r_k$. We have already shown that g(K) = 0 for k = 1. Suppose g(k) = 0 for k = 1, ..., n, and let $K' = K + 3^{r_{n+1}}$, where $r_{n+1} \neq r_i$, i = 1, ..., n, and $r_{n+1} \geq 2$. Then

$$0 = f*g(9+K') = f(9)g(K') + \sum_{\substack{d \mid_3 K' \\ d>9 \\ d \in S_f}} f(d)g(9+K'-d) + \sum_{\substack{d \mid_3 K' \\ d \in S_f}} f(9+d)g(K'-d)$$

$$= f(9)g(K'),$$

for if d > 9 and d ε S_f, then $9 \mid_3 d$, and 9+K'-d and K'-d each have at most 2^n values. Hence g(9+K'-d) = g(K'-d) = 0 for d > 9 and d ε S_f, and we have g(K') = 0.

Similarly, if $K = \sum_{i=1}^{k} 3^{r_i}$, $2 < r_1 < \ldots < r_k$, then g(3+K) = 0. (For the induction step we use f*g(2·3+K).)

Again we let $K = \sum_{i=1}^{k} 3^{r_i}$, $2 \leq r_1 \ldots r_k$, and consider $g(1+K)$. If $k = 1$ and $r_1 = 2$, then

$$0 = f*g(1+2\cdot 3^2) = f(3^2)g(1+3^2) + f(2\cdot 3^2)g(1).$$

But $g(1) = 0$; hence $g(1+3^2) = 0$. If $k = 1$ and $r_1 > 2$, then

$$0 = f*g(1+3+3^{r_1}) = f(3)g(1+3^{r_1}) + f(3+3^{r_1})g(1),$$

where $g(1) = 0$, and again we have $g(1+3^{r_1}) = 0$.

Now we assume that $g(1+K) = 0$ for $k = 1, \ldots, n$, and let $K' = K + 3^{r_{n+1}}$, $f*g(1+9+K') = 0 \Longrightarrow g(1+K') = 0$ by an argument similar to the induction step above. Similarly if $K = \sum_{i=1}^{k} 3^{r_i}$, $2 < r_1 \ldots < r_k$, then $g(1+3+K) = 0$. (We use $f*g(1+2\cdot 3+K')$ for the induction step.)

If $t = \sum_{i=1}^{k} \varepsilon_i 3^{r_i}$, $\varepsilon_i = 1$ or 2, $2 < r_1 \ldots < r_k$, we must use a double induction to show that $g(t) = 0$.

First suppose that $t = 2 \cdot 3^r$ $(r > 2)$. Then

$$0 = f*g(3+2\cdot 3^r) = f(3)g(2\cdot 3^r) + f(3+3^r)g(3^r) + f(3+2\cdot 3^r)g(0),$$

with $g(3^r) = g(0) = 0$. Hence $g(2\cdot 3^r) = 0$ for $r > 2$.

Now suppose that $g(t) = 0$ for $\varepsilon_i = 2$, $\varepsilon_j = 1$ $(j \neq 1)$, and for $k = 1, \ldots, n$. If $t = \sum_{i=1}^{n} \varepsilon_i 3^{r_i}$, we let $t' = t + 3^{r_{n+1}}$, where $r_{n+1} \neq r_i$ $(1 \leq i \leq n)$ and $r_{n+1} > 2$. Then

$$0 = f*g(3+t') = f(3)g(t') + \sum_{\substack{d \mid_3 t' \\ d>0}} f(3+d)g(t'-d) = f(3)g(t'),$$

since $3^{r_i} \mid_3 d \Longrightarrow t' - d$ is of the form $\sum_{i=1}^{m} 3^{s_i}$, and $g(t'-d) = 0$. If $3^{r_i} \not\mid_3 d$, then $2 \cdot 3^{r_i} \mid_3 t'-d$ but $d > 0 \Longrightarrow t' - d$ contains at most n terms; and again $g(t'-d) = 0$. So $g(t) = 0$ if $\varepsilon_i = 2$ for exactly one i.

Suppose that $g(t) = 0$ if $\varepsilon_i = 2$ for m of the i's, $m = 1, \ldots, n$, $n \leq k$. Let $t' = \sum_{i=1}^{n+1} 2 \cdot 3^{r_i}$, $2 < r_1 \ldots < r_{n+1}$. Then

$$0 = f*g(3+t') = f(3)g(t') + \sum_{\substack{d \mid_3 t' \\ d>0}} f(3+d)g(t'-d) = f(3)g(t'),$$

since $d > 0 \Longrightarrow t' - d$ contains at most n terms with $\varepsilon_i = 2$. Hence $g(t') = 0$.

Now suppose that $g(t') = 0$ for $t' = \sum_{i=1}^{k} \varepsilon_i 3^{r_i}$, for $k = m+1, \ldots, m+s$, where $m + 1$ of the ε_i's are equal to 2. Let $t'' = 3^{r_{m+s+1}}$, where $r_{m+s+1} \neq r_i$ $(1 \leq i \leq m + s + 1)$ and $r_{m+s+1} > 2$. Then

$$0 = f*g(3+t'') = f(3)g(t'') + \sum_{\substack{d \mid_3 t'' \\ d>0}} f(3+d)g(t''-d) = f(3)g(t''),$$

since $d > 0 \Longrightarrow$ either $t'' - d$ has at most $m + s$ terms or at most m terms with $\varepsilon_i = 2$. So $g(t''-d) = 0$ for all d, and we must have $g(t'') = 0$. Hence, $g(t) = 0$ for any k and any number of ε_i's equal to 2.

Similarly, $g(1+t) = g(2+t) = g(3+t) = g(1+3+t) = g(2+3+t) = g(9+t) = g(1+9+t) = g(2+9+t) = 0$, where $t = \sum_{i=1}^{k} \varepsilon_i 3^{r_i}$, $2 < r_1 \ldots < r_k$, $\varepsilon_i = 1$ or 2.

Since there is no $n \in S_f$ such that $n \mid_3 n + 6$ and n = least 3-factor of $n + 6$ that is in S_f, we cannot get an immediate representation (see definitions which follow) for $g(6)$. So our only hope of getting a formula for $g(6)$ is to find a number n such that $g(n)$ can be found in two ways, and such that $g(n)$ depends on $g(6)$ or on $g(m)$, where $g(m)$ depends on $g(6)$. The only numbers n such that $g(n)$ can be found in two ways are $n = t$, $1 + t$, $2 + t$, $9 + t$, $1 + 9 + t$, and $2 + 9 + t$, all of which have zero images under g and do not depend on $g(6)$ in any way. Hence $g(6)$ and similarly $g(m)$ (where $6 \mid_3 m$) cannot be uniquely determined by f and $g(d)$ for $d < 6$ ($d < m$).

Suppose $f*g = z$ with $f \neq z$, $f(0) = 0$, and g undetermined.

DEFINITION 5.4. $g(n)$ has an <u>immediate representation</u> or <u>formula</u> if there is a $v \in S_f$ such that $v \mid_p v + n$, and v is the least p-factor of $v + n$ that is in S_f.

DEFINITION 5.5. For $n \in N^*$, $g(n)$ is <u>totally independent</u> if $n \not\mid_p n + v$ for any $v \in S_f$.

DEFINITION 5.6. For $n \in N^*$, $g(n)$ is <u>uniquely determined</u> if $g(n)$ depends on f and $g(d)$ for $d < n$.

NOTE. If f is any singular function, there may be more than one way to obtain a formula for $g(n)$ for some fixed n. If $g(n) = g_1(n)$ and $g(n) = g_2(n)$, then in order for g to be well-defined, we must assume that $g_1(n) = g_2(n)$.

DEFINITION 5.7. g(n) is not uniquely determined if the conditions in Definition 5.6 are not satisfied. (g(n) could depend on f and g(d) for d > n.)

THEOREM 5.2. If $f : N \to F$, where F is a field of characteristic zero, and if f is singular, then the following statements are equivalent:

i) f is a Carlitz-type nilpotent function;

ii) If $S_\delta = \{\delta_p(n) : n \in S_f\}$, then S_δ is finite;

iii) There exists $c \in N^*$ such that $f^c(n)$ contains no nonzero terms for all $n \in N^*$;

iv) There exists $m \in N^*$ such that $m \nmid_p m + u$ for all $u \in S_f$.

PROOF. ii) $\Longrightarrow$ i) f is a Carlitz-type nilpotent iff there exist $m_1, \ldots, m_k \in N^*$ and functions $f_1, \ldots, f_k : N \to F$ such that $f = f_1 * \psi_{m_1} + \ldots + f_k * \psi_{m_k}$. For any $n \in S_f$, $f(n) \neq 0 \Longrightarrow f_i * \psi_{m_i} \neq 0$ for some i; so $m_i \mid_p n$; i.e., for all $n \in S_f$, $m_i \mid_p n$ for some i, $1 \leq i \leq k$. So for all $n \in S_f$, $\delta_p(n) \leq \max\{\delta_p(m_i) : 1 \leq i \leq k\}$, and S_δ is finite.

i) $\Longrightarrow$ iii) Carlitz [1] has shown that if $f = f_1 * \psi_{m_1} + \ldots + f_k * \psi_{m_k}$, and if we take $c > k(p-1)$, then $f^c(n)$ contains no nonzero terms for all $n \in N^*$.

iii) $\Longrightarrow$ ii) To prove the contrapositive of iii) $\Longrightarrow$ ii), we assume S_δ is infinite. Then for any $c > 0$, we can find $n_1, \ldots, n_c \in S_f$ such that $\delta_p(n_{i+1}) > n_i$; $1 \leq i \leq c-1$; and $i \neq j \Longrightarrow (n_i, n_j)_p = 0$. If $n = \sum_{i=1}^{c} n_i$, then $f^c(n)$ contains the term $\prod_{i=1}^{c} f(n_i) \neq 0$.

ii) $\Longrightarrow$ iv) We assume that $S_\delta = \{p^{r_1}, \ldots, p^{r_k}\}$, $p^{r_1} < \ldots < p^{r_k}$ with $k \geq 1$. Let $m = \sum_{i=1}^{k} (p-1)p^{r_i}$. Then $m \nmid_p m + u$ for all $u \in S_f$ since, for all $u \in S_f$, $p^{r_i} \mid_p u$ for at least one i, $1 \leq i \leq k$.

iv) $\Longrightarrow$ ii) If there exists $m \in N^*$ such that $m \nmid_p u + m$ for all $u \in S_f$, and if $m = \sum_{i=1}^{k} a_i p^{r_i}$, $0 < a_i < p$, $r_1 < \ldots < r_k$, then for all $u \in S_f$, $(p-a_i)p^{r_i} \mid_p u$ for at least one i, $1 \leq i \leq k$. Hence $S_\delta \subseteq \{p^0, \ldots, p^{r_k}\}$ which is finite.

THEOREM 5.3. If $f*g = z$, $f \neq z$, $f(0) = 0$, and g is undetermined, then $g(n)$ is totally independent iff $g(n)$ does not depend on f or $g(m)$ for any $m \neq n$.

PROOF. Suppose $g(n)$ does not depend on f or $g(m)$ for any $m \neq n$, and suppose further that there is a $v \in S_f$ such that $v \mid_p n + v$. Then

$$0 = f*g(n+v) = \sum_{\substack{d \mid_p n+v \\ d \in S_f}} f(d)g(n+v-d).$$

Let k be the largest of the $n + v - d$'s. Then

$$g(k) = - \sum_{\substack{d \mid_p n+v \\ d \in S_f \\ d > n+v-k}} f(d)g(n+v-d)/f(n+v-k),$$

where either $k = n$ or the term $-f(v)g(n)/f(n+v-k)$ is in the formula

for g(k). Either way, g(n) depends on g(m) for some $m \neq n$, a contradiction.

The converse follows immediately from Theorem 5.2.

THEOREM 5.4. If $f^c(n) = 0$ for some $c \geq 2$, for all $n = \sum_{i=0}^{k} a_i p^i$ $(0 \leq a_i < p)$ and $[\frac{p-1}{c}] > 0$, then $f(n) = 0$ for all n with $r = \sum_{i=0}^{k} a_i \leq [\frac{p-1}{c}]$.

PROOF. We will use mathematical induction on r. We note that $c \geq 2$ and $[\frac{p-1}{c}] > 0 \iff$ p is an odd prime and $c \leq p-1$.

If $r = 1$, then $n = p^i$ for some $i \geq 0$, and

$$0 = f^c(cn) = f^c(cp^i) = [f(p^i)]^c.$$

Hence $f(p^i) = 0$.

Suppose the theorem is true for $r = 1, 2, \ldots, m < [\frac{p-1}{c}]$. Let $r = m + 1 \leq [\frac{p-1}{c}]$. Then $n = \sum_{i=0}^{k} a_i p^i$, $0 \leq a_i < p$, and $\sum_{i=0}^{k} a_i = m + 1 \leq [\frac{p-1}{c}]$. Then $f^c(cn) = \sum_{\substack{d_i \mid p^{cn} \\ d_1 +_p +\ldots+_p d_c = cn}} f(d_1)f(d_2) \cdot \ldots \cdot f(d_c)$. Now $d_j = \sum_{i=0}^{k} a_{ij} p^i$, $0 \leq a_{ij} \leq ca_i$, and some d_j in each term of $f^c(cn)$ will have $\sum_{i=0}^{k} a_{ij} \leq m$ unless $d_1 = d_2 = \ldots = d_c = n$. If $\sum_{i=0}^{k} a_{ij} \leq m$, then $f(d_j) = 0$. Hence $0 = f^c(cn) = [f(n)]^c$, and $f(n) = 0$.

The condition in Theorem 5.4 is not sufficient for f to be nilpotent; for if we define

$$f(n) = \begin{cases} 1, & n = (p-1)p^r,\ r = 0, 1, 2, \ldots, \\ 0, & \text{otherwise} \end{cases}$$

for $p > 2$, then f satisfies the condition that $f(n) = 0$ for $\sum_{i=0}^{k} a_i \leq [\frac{p-1}{c}]$ for any $c \geq 2$, but f is clearly not nilpotent since for any c, $f^c \left(\sum_{i=0}^{c} (p-1)p^i \right) = \prod_{i=0}^{c} f((p-1)p^i) = 1 \neq 0$.

COROLLARY. If $f^c = z$ for some $c \geq 2$, then there are at most $c - 1$ numbers p^r with $f(p^r) \neq 0$.

5.2. On the Zero Divisors of L. For the following discussion we will assume that

1. f and g are elements of L;
2. $f*g = z$ with $f \neq z$,
3. $S_f = \{n \in N^* : f(n) \neq 0\}$ and $S_g = \{n \in N^* : g(n) \neq 0\}$.

THEOREM 5.5. If g(n) is not uniquely determined by f and g(d) for $d < n$ (for some fixed $n \in N^*$), then either

(i) $n \not|_p\ n + u$ for all $u \in S_f$, or

(ii) for all $u \in S_f$, such that $n \mid_p n + u$, there exists $u' \in S_f$ such that $u' \mid_p n + u$, $u' < u$, and $g(n+u-u') \neq 0$.

PROOF. If (i) is true, then f is a Carlitz-type nilpotent element, and (i) is consistent with g(n) being not uniquely determined by f and g(d) for $d < n$.

Suppose (i) is not true. Then there exists $u \in S_f$ such that $n \mid_p n+u$. If u is the least p-factor of $n+u$ that is in S_f, then

$$0 = f*g(n+u) = \sum_{d \mid_p n+u} f(d)g(n+u-d) = f(u)g(n) + \sum_{\substack{d \mid_p n+u \\ d>u}} f(d)g(n+u-d),$$

and $g(n) = \frac{1}{f(u)} \sum_{\substack{d \mid_p n+u \\ d>u}} f(d)g(n+u-d)$; i.e., $g(n)$ is uniquely determined, since $d > u \Rightarrow n+u-d < n$.

The converse of Theorem 5.5 is not necessarily true. For some n's for which (ii) holds, $g(n)$ can be determined in the following manner.

If $\delta_p(n)$ is sufficiently large, there can be two (or more) elements u_1 and u_2 of S_f such that $u_i \mid_p u_i + n$ and u_i is the least p-factor of $u_i + n$ that is in S_f $(i = 1, 2)$. In which case

$$g(n) = [- \sum_{\substack{d \mid_p n+u_1 \\ d > u_1}} f(d)g(n+u_1-d)]/f(u_1)$$

$$= [- \sum_{\substack{d \mid_p n+u_2 \\ d>u_2}} f(d)g(n+u_2-d)]/f(u_2).$$

Hence $$\sum_{\substack{d \mid_p n+u_1 \\ d>u_1}} f(u_2)f(d)g(n+u_1-d) = \sum_{\substack{d \mid_p n+u_2 \\ d>u_2}} f(u_1)f(d)g(n+u_2-d).$$

Using this equation we can solve for $f(D_1)$ where D_1 is the maximal element of $S_1 = \bigcup_{i=1}^{2} \{n + u_i - d\}_{\substack{d>u_i \\ d\in S_f}}$, or the maximal element of S_1 such that $f(u_2)f(n+u_1-D_1) - f(u_1)f(n+u_2-D_1) \neq 0$. $f(u_2)f(n+u_1-D_1) - f(u_1)f(n+u_2-D_1) = 0$ only if $D_1 |_p n + u_1$ and $D_1 |_p n + u_2$ and $n + u_1 - D_1 \in S_f$ and $n + u_2 - D_1 \in S_f$ with $f(u_2)f(n+u_1-D_1) = f(u_1)f(n+u_2-D_1)$.

Let $K_1 = n + u_1 - D_1$, $K_2 = n + u_2 - D_1$, and note that $K_2 + u_1 = K_1 + u_2$. $g(D_1)$ is equal to exactly one of the following:

$$g(D_1) = \Big[\sum_{\substack{d|_p n+u_2 \\ d>u_2}} f(u_1)f(d)g(n+u_2-d) - \sum_{\substack{d|_p n+u_1 \\ d>u_1}} f(u_2)f(d)g(n+u_1-d) \Big]/f(K_1)f(u_2)$$

or

$$g(D_1) = \Big[\sum_{\substack{d|_p n+u_1 \\ d>u_1}} f(u_2)f(d)g(n+u_1-d) - \sum_{\substack{d|_p n+u_2 \\ d>u_2}} f(u_1)f(d)g(n+u_2-d) \Big]/f(K_2)f(u_1)$$

or (5.4)

$$g(D_1) = \Big[\sum_{\substack{d|_p n+u_1 \\ d>K_1}} f(u_2)f(d)g(n+u_1-d) - \sum_{\substack{d|_p n+u_2 \\ d>K_2}} f(u_1)f(d)g(n+u_2-d) \Big] / [f(K_2)f(u_1)-f(K_1)f(u_2)].$$

Now if there exists $u_3 \in S_f$ such that $u_3 |_p u_3 + D_1$ and u_3 is the least p-factor of $u_3 + D_1$ that is in S_f, then

$g(D_1) = [-\sum_{\substack{d|_p u_3+D_1 \\ d>u_3}} f(d)g(u_3+D_1-d)]/f(u_3)$. Because g is a function, the above formula must be equal to one of the formulas (5.4) and we can then find a formula for $g(D_2)$, where D_2 is the maximal element of $S_2 = (S_1 - D_1) \cup \{u_3 + D_1 - d\}_{\substack{d>N_3 \\ d\in S_f}}$, or the maximal element of S_2 whose coefficients do not cancel out of the equation

$$(5.4) = [-\sum_{\substack{d|_p u_3+D_1 \\ d>u_3}} f(d)g(u_3+D_1-d)]/f(u_3).$$

We can continue this process until we find $g(D_i)$, where for all $u \in S_f$ such that $u|_p u + D_i$, there exists $u' < u$ such that $u'|_p u + D_i$.

It may be possible to obtain another formula for $g(D_i)$ through a process similar to the one above, but starting from a different n, u_1, and u_2; in which case we may obtain a formula for $g(D_j)$ for some $D_j < D_i$ by the process of setting the two formulas for $g(D_i)$ equal to each other and solving for $g(D_j)$. We can do this as long as, one way or another, we can obtain two formulas for $g(D_i)$ in terms of f and g(d) for $d < D_i$.

Note that for all n for which g(n) is uniquely determined, g(n) can be written in the form

$$g(n) = \frac{\sum_{i=1}^{r} \alpha_i f(a_{i1}) \cdot \ldots \cdot f(a_{ik})g(b_i)}{\sum_{j=1}^{s} \beta_j f(c_{j1}) \cdot \ldots \cdot f(c_{jm})} \qquad (5.5)$$

where α_i, β_j are nonzero integers, $b_i < n$, a_{it}, $c_{jv} \in S_f$ $(i = 1, \ldots, r;$ $t = 1, \ldots, k;\ j = 1, \ldots, s;\ v = 1, \ldots, m)$, $\sum_{j=1}^{s} \sum_{v=1}^{m} f(c_{jv}) \neq 0$, and where

$$\sum_{t=1}^{k} a_{it} + b_i - \sum_{v=1}^{m} c_{jv} = n.$$

From the formula (5.5) we can easily obtain the following.

THEOREM 5.6. If $f*g = z$ with $f \neq z$ and $g \neq z$, and if n is the least element of S_g, then $g(n)$ cannot be uniquely determined by f and $g(d)$ for $d < n$.

PROOF. If $g(n)$ is uniquely determined by f and $g(d)$ for $d < n$, then

$$g(n) = \frac{\sum_{i=1}^{r} \sum_{t=1}^{k} \alpha_i f(a_{it}) g(b_i)}{\sum_{j=1}^{s} \sum_{v=1}^{m} \beta_j f(c_{jv})},$$

where $b_i < n$, α_i, β_i are nonzero integers, a_{it}, $c_{jv} \in S_f$ $(1 \leq t \leq r,$ $1 \leq t < n,\ 1 \leq j \leq s,\ 1 \leq v \leq m)$. But $b_i < n \Rightarrow g(b_i) = 0$; so $g(n) = 0$, a contradiction.

EXAMPLE 5.2 We define f by $S_f = \{n \in N^* : 1 \mid_3 n\} \cup \{3^r + 3^s : 0 \leq r < s\}$. We assume $f*g = z$ with g undetermined. Clearly 1 is the least element of S_f. Moreover, the only elements of N^* such that $g(n)$ has an immediate representation are those numbers n such that $1 \mid_3 1 + n$. Any number n such that $n \equiv 2 \pmod 3$ does not have an immediate representation; so

$g(2)$ does not have an immediate representation. $g(2)$ may be found from $f*g(2\cdot3^r + 2\cdot3^s + 2\cdot3^t)$, $1 \leq r < s < t$.

The formula for $f*g(2\cdot3^r + 2\cdot3^s + 2\cdot3^t)$ depends on several numbers $g(n)$, where $n > 2$, at various levels of substitution, but all of these numbers $g(n)$ have immediate representations; so $f*g(2\cdot3^r + 2\cdot3^s + 2\cdot3^t)$ may be reduced to a formula which depends on f, $g(1)$, and $g(2)$. Hence $g(2)$ can be obtained. $g(2)$ may also be obtained from the formulas for $f*g(2\cdot3^r + 2\cdot3^s + 3^t + 3^u)$, $f*g(2\cdot3^r + 3^s + 2\cdot3^t + 3^u)$, $f*g(2\cdot3^r + 3^s + 3^t + 2\cdot3^u)$, $f*g(3^r + 2\cdot3^s + 3^t + 2\cdot3^u)$, $f*g(3^r + 3^s + 2\cdot3^t + 2\cdot3^u)$, $1 \leq r < s < t < u$.

We can similarly obtain $g(2+3)$, $g(2+3^2)$, $g(2+3^3)$, and $g(2+3^4)$, from $f*g(3 + 2\cdot3^2 + 2\cdot3^3 + 2\cdot3^4)$, $f*g(2\cdot3 + 3^2 + 2\cdot3^3 + 2\cdot3^4)$, $f*g(2\cdot3 + 2\cdot3^2 + 3^3 + 2\cdot3^4)$, $f*g(2\cdot3 + 2\cdot3^2 + 2\cdot3^3 + 2\cdot3^4)$, respectively. Moreover, for each n above, $f*g(n)$ depends on all of $\{g(2+3^i)\}_{i=1}^{4}$, plus some other numbers $g(m)$, all of which have immediate formulas.

From this point on we will assume the following:

i) $f : N \to F$, where F is a field of characteristic zero;

ii) $f \neq z$;

iii) $f(0) = 0$;

iv) f is not a Carlitz-type nilpotent function;

v) $f*g = z$ with g undetermined.

We will attempt to determine as much as possible about g. Recall that we already have $g(0) = 0$.

The following definition is in part a revision of Definition 5.4.

DEFINITION 5.8. For a fixed n, g(n) has a primary or order 1 representation (formula) if there exists $u \in S_f$ such that $u|_p n + u$ and u is the least p-factor of n + u that is in S_f. In this case

$$g(n) = - \sum_{\substack{d|_p n+u \\ d>n \\ n+u-d \in S_f}} f(n+u-d)g(d)/f(u);$$

M = n + u is a primary or order 1 generator of g(n); and if there is more than one such M, then the least one will be called the least primary generator (LPG) of g(n).

One might be tempted to assume that if g(n) has an order 1 representation, then the LPG of g(n) is the least element M of N^* such that $n|_p M$ with $M - n \in S_f$. This is not always true. Consider the following example.

EXAMPLE 5.3. Let $S_f = \{1 + 3^r : r \geq 1\} \cup \{3^r + 3^s : 2 \leq r < s, s \geq 4\}$. We assume f*g = z with g undetermined. For $n = 2 \cdot 3$, the least element M of N^* such that $n|_3 M$ with $M - n \in S_f$ is $M = 1 + 2 \cdot 3 + 3^2 = 2 \cdot 3 + (1+3^2)$. But f*g(M) gives an order 1 formula for $g(3 + 3^2)$; in fact, M is the LPG of $g(3 + 3^2)$. However, for $M' = 2 \cdot 3 + 3^2 + 3^4$, we have $0 = f*g(M') = f(3^2 + 3^4)g(2 \cdot 3)$; hence $g(2 \cdot 3) = 0$. M' is the LPG of $g(2 \cdot 3)$ with $M' > M$.

DEFINITION 5.9. For a fixed n, g(n) has a secondary or order 2 representation (formula) if

i) there exists a positive integer $M > n$ such that $g(n)$ appears in $f*g(M)$ at some level of substitution, and the coefficients of $g(n)$ do not cancel;

ii) for all $x \in N^*$ with $n < x < M$ such that $g(x)$ appears in $f*g(M)$ with a nonzero coefficient, $g(x)$ has a primary representation with the LPG of $g(x)$ different from M;

iii) there is at least one x with $n < x < M$ and $x|_p M$ with $M - x$ in S_f.

NOTE. We do not require that $n|_p M$. In some cases we even have $(M,n)_p = 0$, as in $n = 2$, $M = 2\cdot 3 + 2\cdot 3^2 + 2\cdot 3^3$ from Example 5.2. In fact $(M,2)_3 = 0$ for all secondary generators M given in Example 5.2.

DEFINITION 5.10. For a fixed n, $g(n)$ has an <u>order k</u> ($k > 1$) <u>representation</u> (<u>formula</u>) if

i) there exists a positive integer $M > n$ such that $g(n)$ appears in $f*g(M)$ with a nonzero coefficient at some level of substitution, and the coefficients of $g(n)$ do not cancel;

ii) for all $x \in N^*$ with $n < x < M$ such that $g(x)$ appears in $f*g(M)$ with nonzero coefficients, $g(x)$ has a representation of order t for some $t < k$, with the least order t generator of $g(x)$ different from M;

iii) at least one such x has an order $k - 1$ representation.

M will be called an <u>order k generator</u> of $g(n)$, and the least such number will be the <u>least order k generator</u> of $g(n)$.

DEFINITION 5.11. The order of g(n) is the least number k such that g(n) has an order k representation. If g(n) has order k, we will write $o(g(n)) = k$.

THEOREM 5.7. If $o(g(n)) \neq 1$ then for all $u \in S_f$ such that $u \mid_p n + u$, there exists $v \in S_f$ such that $v < u$ and $v \mid_p n + u$.

PROOF. If the conclusion is not true, then $o(g(n)) = 1$ by Definition 5.8.

THEOREM 5.8. If $o(g(n)) = 1$, and if $m \mid_p n$, then $o(g(m)) = 1$.

PROOF. Let M be the LPG of g(n). Then $M = n + v$, where v is the least p-factor of M that is in S_f. $m \mid_p n \Longrightarrow v \mid_p m + v$. Let $m + v = M'$. If there exists $v' \in S_f$ such that $v' < v$ and $v' \mid_p M'$, then $M' \mid_p M \Longrightarrow v' \mid_p M$, a contradiction.

THEOREM 5.9. If $o(g(n)) \neq 1$, and if $n \mid_p m$, then $o(g(m)) \neq 1$.

PROOF. Let u be any element of S_f such that $u \mid_p u + m$. $n \mid_p m \Longrightarrow u \mid_p u + n$. $o(g(n)) \neq 1 \Longrightarrow$ there exists $u' < u$ such that $u' \in S_f$ and $u' \mid_p u+n$. $n \mid_p m \Longrightarrow u + n \mid_p u + m \Longrightarrow u' \mid_p u + m$. Hence $o(g(m)) \neq 1$.

THEOREM 5.10. If $1 \in S_f$, and if $S = \{v \in S_f : v + m$ is the LPG of $g(m)$ for some $m \in N^*\}$, then S is finite. (In fact, $S = \{1\}$.)

PROOF. Let m be any positive integer. If $1 \mid_p 1 + m$, then clearly $1 + m$ is the LPG of g(m). If $1 \nmid_p 1 + m$, then $m \equiv p - 1 \pmod p$, $1 \mid_p m$, and for all $u \in S_f$ such that $u \mid_p u + m$, $u > 1$ and $1 \mid_p u + m$. Hence $o(g(m) \neq 1$, and $S = \{1\}$.

COROLLARY. If the least element of S_f is $v_o \leq \frac{p-1}{2}$ $(p > 2)$, then S is finite. $(S = \{v_o\}.)$

DEFINITION 5.12. If $n = \sum_{i=1}^{k} a_1 p^{r_i}$, $0 < a_i < p$, $r_1 < \ldots < r_k$, then $\Delta_p(n) = p^{r_k}$, and $\Delta_p(0) = 0$.

THEOREM 5.11. If $p^r \in S_f$ for some $r \geq 0$, then S (as defined in Theorem 5.10) is finite. In fact, $v \leq p^{r_o}$ for all $v \in S$, where p^{r_o} is the least power of p that is in S_f.

PROOF. The case for $r = 0$ is proven in Theorem 5.9. We assume $r > 0$ and that m is an arbitrary element of N^*.

Case 1. If p^{r_o} is the least element of S_f, then $p^{r_o} \mid_p p^{r_o} + m \Longrightarrow p^{r_o} + m$ is the LPG of g(m). $p^{r_o} \mid_p p^{r_o} + m \Longrightarrow (p-1)p^{r_o} \mid_p m$. If $u \in S_f$ and $u \mid_p u + m$, then $u \geq p^{r_o}$ and $p^{r_o} \mid_p u + m$. Hence $o(g(m)) \neq 1$ and $S = \{p^{r_o}\}$.

Case 2. If p^{r_o} is not the least element of S_f, we assume that $v_1, \ldots, v_t$ are the elements of S_f that are less than p^{r_o} and that $v_1 < \ldots < v_t$. Then $\Delta_p(v_1) < p^{r_o}$, $1 \leq i \leq t$; i.e., $(v_i, p^{r_o})_p = 0$.

If $o(g(m)) = 1$, then the possibilities are:

i) $v_i \mid_p v_i + m$ for some i, $1 \leq i \leq t$, and v_i is the least p-factor of $v_i + m$ that is in S_f;

ii) $p^{r_o} \mid_p p^{r_o} + m$ and p^{r_o} is the least p-factor of $p^{r_o} + m$ that is in S_f;

iii) neither i) nor ii).

If neither i) nor ii) occurs, then both of the following must hold.

iv) for all i, $1 \leq i \leq t$, either $v_i \nmid_p v_i+m$, or for all i such $v_i \mid_p v_i+m$ there exists $v_j < v_i$ with $v_j \mid_p v_i+m$;

v) $p^{r_o} \nmid_p p^{r_o} + m$, or $p^{r_o} \mid_p p^{r_o} + m$ but $v_i \mid_p p^{r_o} + m$ for some i, $1 \leq i \leq t$.

If $v_i \nmid_p v_i + m$, $1 \leq i \leq t$, and $p^{r_o} \nmid_p p^{r_o} + m$, then $(p-1)p^{r_o} \mid_p m$, and for all $u \in S_f$ such that $u \mid_p u+m$, $u > p^{r_o}$ and $p^{r_o} \mid_p u+m$. Hence $o(g(m)) \neq 1$.

If $v_i \nmid_p v_i+m$, $1 \leq i \leq t$, and $p^{r_o} \mid_p p^{r_o} + m$ but $v_i \mid_p p^{r_o} + m$ for some i, then $v_i \mid_p m$ and $v_i \mid_p u+m$ for all $u \in S_f$ such that $u > p^{r_o}$ and $u \mid_p u+m$. Again we have $o(g(m)) \neq 1$.

If for all i such that $v_i \mid_p v_i + m$ there exists $v_j < v_i$ with $v_j \mid_p v_i+m$, and if $p^{r_o} \nmid_p p^{r_o} + m$, then $(p-1)p^{r_o} \mid_p m$. If for all $u \in S_f$ such that $u > p^{r_o}$ and $u \mid_p u + m$, we have $p^{r_o} \mid_p u+m$, and $o(g(m)) \neq 1$.

If for all i such that $v_i \mid_p v_i+m$ there exists $v_j < v_i$ such that $v_j \mid_p v_i+m$, and if $p^{r_o} \mid_p p^{r_o} + m$ but $v_i \mid_p p^{r_o} + m$ for some i, $1 \leq 1 \leq t$, then $v_i \mid_p m$. For all $u \in S_f$ with $u > p^{r_o}$ and $u \mid_p u+m$, we have $v_i \mid_p u+m$ and $o(g(m)) \neq 1$.

Hence $o(g(m)) = 1 \Longrightarrow$ either i) or ii) must hold, and $S \subseteq \{v_1, \ldots, v_t, p^{r_o}\}$.

COROLLARY. If $ap^r \in S_f$ with $p > 2$ and $0 < a \leq \frac{p-1}{2}$, then S is finite; and $v \in S \Longrightarrow v \leq a_o p^{r_o}$, where $a_o p^{r_o}$ is the least number of this form in S_f.

There are singular functions for which S is infinite. One of the simplest examples of this type of function is Example 5.4 below.

EXAMPLE 5.4. We define f by $S_f = \{(p-1)p^i : p > 2, i = 0, 1, 2, \ldots\}$. In this example, $S = S_f$, for any number of the form $n = \sum_{i=1}^{k} p^i$ has order one, and the LPG of g(n) is $M = n + (p-1)p^{k+1}$.

Another interesting example of this type is

EXAMPLE 5.5. If $S_f = \{\sum_{i=n}^{2n} 3^i : n = 1, 2, \ldots\}$, then any number

$$n_1 = \sum_{i=1}^{k} 2\cdot 3^{2i} \text{ or } n_2 = \sum_{i=0}^{k} 2\cdot 3^{2i+1} \text{ or } n_3 = \sum_{i=0}^{k} 2\cdot 3^{3i+1} \text{ or } n_4 = \sum_{i=0}^{k} 2\cdot 3^{3i+2},$$

has order 1. If M_j is the LPG of $g(n_j)$ $(j = 1, 2, 3, 4)$, then

$$M_1 = n_1 + \sum_{i=2k+2}^{2(2k+2)} 3^i,\ M_2 = n_2 + \sum_{i=2k+3}^{2(2k+3)} 3^i\ M_3 = n_3 + \sum_{i=3(k+1)}^{6(k+1)} 3^i,$$

$$M_4 = n_4 + \sum_{i=3(k+4)}^{6k+8} 3^i.$$

CONJECTURE. If f is a singular function, then the set $S = \{v \in S_f : v + m \text{ is the LPG of } g(m) \text{ for some } m \in N^*\}$ is infinite iff there is an infinite sequence $\{n_i\}_{i=1}^{\infty}$ of elements of N^* such that $n_i < n_{i+1}$, $n_i \mid_p n_{i+1}$ $(i = 1, 2, \ldots)$, $o(g(n_i)) = 1$, and if $v_i + n_i$ is the LPG of $g(n_i)$, then $\Delta_p(v_i) > \Delta_p(n_i)$.

DEFINITION 5.13. An <u>order k substitution</u> $(k > 1)$ within a formula f*g(M) is the substitution for g(n), where $o(g(n)) = k$ and where the formula used for the substitution is obtained from the least order k generator of g(n).

THEOREM 5.12. If $o(g(n)) = k > 1$ and M is any order k generator of g(n), then there exist positive integers $x_1, \ldots, x_k = n$ such that $M > x_1 > \ldots > x_k = n$, $o(g(x_t)) = t$, and M is an order t generator of $g(x_t)$, $1 \leq t \leq k$.

Moreover, if M_t is the least order t generator of $g(x_t)$ $(1 \leq t < k)$, then $M_t < M$.

PROOF. If no proper p-factor of M is in S_f, then either M is not a generator of g(x) for any $x \in N$, or M generates only g(0) = 0. So there exists $u \in S_f$ such that $u|_p M$, $u < M$. Let u_o be the least such number. Let $x_1 = M - u_o$. Clearly M is a primary generator of $g(x_1)$, and $o(g(x_1)) = 1$. Since f*g(M) depends on g(n) at some level of substitution, and since x_1 must be the largest number x such that f*g(M) depends on g(x), we must have $x_1 \geq n$. $x_1 > n$ since $o(g(n)) \neq 1$.

Since M is an order k $(k > 1)$ generator of g(n), the LPG of $g(x_1)$ must be different from M; in fact the LPG of $g(x_1)$ must be less than M by Definition 5.8.

If k = 2 we need go no further. Otherwise we make all possible order 1 substitutions within f*g(M).

Let x_2 be the largest positive integer such that $g(x_2)$ appears in this version of f*g(M), $o(g(x_2)) \neq 1$, and the coefficients of $g(x_2)$ do not cancel. Then $x_2 < x_1$, M is an order 2 generator for $g(x_2)$, and $o(g(x_2)) \neq 1 \Rightarrow o(g(x_2)) = 2$. Moreover, if M_2 is the least order 2 generator of $g(x_2)$, then $M_2 < M$ by Definition 5.10.

If k = 3 we need go no further. Otherwise we make all possible order 2 substitutions within f*g(M). We assume that for every order 2 substitution we make for some g(x) in f*g(M), all possible order 1 substitutions have already been made within the formula for g(x). Let x_3 be the largest number such that $g(x_3)$ appears in this form of f*g(M). M is an order 3 generator of $g(x_3)$, and $o(g(x_3)) \neq 1, 2 \Rightarrow o(g(x_3)) = 3$.

Moreover $x_3 < x_2 < x_1$, and if M_3 is the least order 3 generator of $g(x_3)$, then $M_3 < M$ by Definition 5.10.

Continuing this process we must obtain $x_1 > \ldots > x_k = n$, where $o(g(x_t)) = t$ for all t with $1 \leq t \leq k$; for if we arrive at g(n) in less than k applications of this process, we will have $o(g(n)) < k$, a contradiction. If it takes more than k applications of the process to obtain g(n), we contradict M's being an order k generator of g(n).

DEFINITION 5.14. If $o(g(n)) \neq 1$, a positive integer Q will be called a quasi-generator of g(n) if Q is not the LPG of g(m) for any $m \in N$ and if either g(n) appears in f*g(Q) with substitutions of order 1, or $n|_p Q$ with $Q - n \in S_f$.

COROLLARY. If $o(g(n)) = 2$, then any order 2 generator of g(n) is a quasi-generator of g(n).

THEOREM 5.11. If Q is a quasi-generator of g(n), and if either $n \nmid_p Q$ or $n|_p Q$ with $Q - n \notin S_f$, then there exist numbers $u_1, \ldots, u_k \in S_f$ $(k > 1)$ and $v_1, \ldots, v_{k-1} \in S_f$ such that $Q = n + u_1 - v_1 + \ldots u_k$, for some $k \in N^*$.

PROOF. g(n) appears in f*g(Q) with substitutions of order 1 $\Longrightarrow$ there exists $m_1 \in N^*$ such that $o(g(m_1)) = 1$, $m_1|_p Q$, $Q - m_1 = u_1 \in S_f$, and $g(m_1)$ depends on g(n). Moreover Q is not the LPG of $g(m_1)$. Let M_1 be the LPG of $g(m_1)$, and let $v_1 = M_1 - m_1$. Then $v_1 \in S_f$ and is the least p-factor of M_1 that is in S_f. If $n|_p M_1$ with $M_1 - n \in S_f$, we let $u_2 = M_1 - n$. Then $Q = m_1 + u_1 = M_1 - v_1 + u_1 = n + u_2 - v_1 + u_1$.

If $n \nmid {}_pM_1$ or if $n|{}_pM_1$ but $M_1 - n \notin S_f$, then $g(m_1)$ must depend on $g(n)$ with one or more order 1 substitutions. So there exists m_2 such that $m_2|{}_pM_1$, $M_1 - m_2 = u_2 \in S_f$, and $g(m_2)$ depends on $g(n)$. Moreover, $m_2 < m_1$; so M_1 is not the LPG of $g(m_2)$. Let M_2 be the LPG of $g(m_2)$, and let $v_2 = M_2 - m_2$. $v_2 \in S_f$ and is the least p-factor of M_2 that is in S_f. If $n|{}_pM_2$ with $M_2 - n \in S_f$, we let $u_3 = M_2 - n$. We have

$$\begin{aligned} Q &= m_1 + u_1 \\ &= M_1 - v_1 + u_1 \\ &= m_2 + u_2 - v_1 + u_1 \\ &= M_2 - v_2 + u_2 - v_1 + u_1 \\ &= n + u_3 - v_2 + u_2 - v_1 + u_1. \end{aligned}$$

If $n \nmid {}_pM_2$ or if $n|{}_pM_2$ but $M_2 - n \notin S_f$, then there must be a number m_3 such that $o(g(m_3)) = 1$, $m_3|{}_pM_2$, $M_2 - m_3 = u_3 \in S_f$, and $g(m_3)$ depends on $g(n)$ with at most order 1 substitutions.

The fact that $g(n)$ appears in $f*g(Q)$ with order 1 substitutions guarantees that a continuation of this process will produce sequences of numbers $m_1, \ldots, m_{k-1}$ $(k > 1)$, where $o(g(m_i)) = 1$, and $M_1, \ldots, M_{k-1}$ are the LPG's of $g(m_1), \ldots, g(m_{k-1})$, respectively; $n|{}_pM_{k-1}$ with $M_{k-1} - n \in S_f$; and where $Q = m_1 + u_1$, $M_i = m_i + v_i = m_{i+1} + u_{i+1}$ $(1 \leq i \leq k - 1)$. Hence $Q = n + u_k - v_{k-1} + \ldots - v_1 + u_1$, $u_i \in S_f$ $(1 \leq i \leq k)$, and $v_i \in S_f$ $(1 \leq 1 \leq k - 1)$.

Note that if we renumber the u_i's and v_i's so that $u_i' = u_{k+1-i}$, and $v_i' = v_{k-i}$, then we get $Q = n + u_1' - v_1' + \ldots + u_k'$. If

$M_1' = n + u_1'$, $M_i' = n + u_1' - v_1' + \ldots + u_i'$ $(1 \leq i \leq k)$, then M_i' is the LPG of $g(m_i')$ $(1 \leq i \leq k - 1)$, where $m_i' = M_i' - v_i'$.

5.3. Algorithm for Obtaining a Quasi-Generator of g(n). $(o(g(n)) \neq 1)$

1. Let u_1 be any element of S_f such that $u_1 |_p n+u_1$ and let $Q_1 = n + u_1$. (The fact that f is not a Carlitz-type nilpotent function guarantees the existence of Q_1.) Let v_1 be the least element of S_f such that $v_1 |_p Q_1$. $v_1 < u_1$ by Theorem 5.7. Let $m_1 = Q_1 - v_1$. If Q_1 is not the LPG of $g(m_1)$, then Q_1 is a quasi-generator of g(n).

2. If Q_1 is the LPG of $g(m_1)$, then we choose any element u_2 of S_f such that $u_2 |_p u_2 + m_1$, $v_1 \nmid_p u_2$. Let $Q_2 = u_2 + m_1$, and let v_2 be the least p-factor of Q_2 that is in S_f, and let $m_2 = Q_2 - v_2$. Now $v_2 \leq u_2$. If $v_2 = u_2$, the $m_2 = m_1$, and Q_2 is not the LPG of $g(m_1) \Rightarrow Q_2$ is a quasi-generator of g(n). Otherwise $v_2 < u_2$. If Q_2 is not the LPG of $g(m_2)$, then Q_2 is a quasi-generator of g(n).

3. If Q_2 is the LPG of $g(m_2)$ we repeat the process of step 2, letting u_3 be any element of S_f such that $u_3 |_p u_3 + m_2$ and v_1, $v_2 \nmid_p u_3$. Let $Q_3 = m_2 + u_3$, and let v_3 be the least p-factor of Q_3 that is in S_f. If $v_3 = u_3$, then Q_3 is a quasi-generator of g(n). If $v_3 < u_3$, let m_3 $Q_3 - v_3$. If Q_3 is not the LPG of $g(m_3)$, then Q_3 is a quasi-generator of g(n).

If Q_3 is the LPG of $g(m_3)$, we continue repeating step 3 until we find a number Q_k which is not the LPG of $g(m_k)$. Q_k will be a quasi-generator of g(n).

If Q is any quasi-generator of g(n) which has been obtained by the algorithm, we can obtain a different quasi-generator from Q as

follows. If $m|_p Q$ with $Q - m \in S_f$, $o(g(m)) = 1$, and $g(n)$ appears in $g(m)$ with at most order 1 substitutions, we let $v = Q - m$, and let u be any element of S_f such that $u|_p u+m$ and $u + m$ is not the LPG of $g(m')$ for any $m' \in N^*$. $Q' = Q - v + u$ is also a quasi-generator of $g(n)$.

DEFINITION 5.15. A <u>minimal</u> quasi-generator of $g(n)$ is a quasi-generator that has been obtained in a minimal number of steps of the algorithm; i.e., either $Q = n + u$, $u \in S_f$, or if $Q = n + u_1 - v_1 + \ldots + u_k$ $(k > 1)$, then M_i is the LPG of $g(m_i)$ $(1 \leq i \leq k - 1)$, where $M_1 = n + u_1$, $M_i = n + u_1 - v_1 + \ldots + u_i$ $(i > 1)$, and $m_i = M_i - v_i$.

Actually, the proof of Theorem 5.13 shows us that any quasi-generator of $g(n)$ can be written in one of the forms above. However when we apply the algorithm there must be some number t_n such that the number of steps needed to obtain a quasi-generator of $g(n)$ is at least t_n. In Definition 5.15 we assume $k = t_n$.

THEOREM 5.14. If $o(g(n)) \neq 1$, and Q is a number which has been obtained by the algorithm, then Q is a quasi-generator of $g(n)$, and the coefficient of $g(n)$ in $f*g(Q)$ will not cancel for non-specified values of f.

PROOF. If $Q = n + u$ $(u \in S_f)$, then $f*g(Q)$ contains the term $f(u)g(n)$ with no substitutions. Moreover this will be the only time $g(n)$ occurs in $f*g(Q)$ with the coefficient $f(u)$; so the coefficient(s) of $g(n)$ will not cancel for non-specified values of f.

If $Q = n + u_1 - v_1 + \ldots + u_k$ $(k > 1)$, where $u_i \in S_f$ $(1 \leq i \leq k)$, $v_i \in S_f$ $(1 \leq i \leq k - 1)$, we let $Q_1 = n + u_1$, $Q_i = n + u_1 - v_1 + \ldots + u_i$

$(i > 1)$. Then Q_i is the LPG of $g(Q_i - v_i) = g(m_i)(i < k)$. $g(m_1)$ is obtained from $f*g(Q_1)$ and contains the term $f(u_1)g(n)/f(v_1)$ with no substitutions. If $k>2$, $g(m_2)$ is obtained from $f*g(Q_2)$ and contains the term $f(u_2)g(m_1)/f(v_2)$, which in turn contains the term $f(u_1)f(u_2)g(n)/f(v_1)f(v_2)$ with one order 1 substitution.

Continuing this argument we find that $f*g(Q)$ contains the term $f(u_k)g(m_{k-1})$ which, with $k - 1$ order 1 substitutions contains the term

$$f(u_1) \cdot \ldots \cdot f(u_k)g(n)/f(v_1) \cdot \ldots \cdot f(v_{k-1}). \quad (5.6)$$

Hence $g(n)$ will appear in $f*g(Q)$ with at most order 1 substitutions. Moreover, since the term (5.6) is the only term containing $g(n)$ in $f*g(Q)$ with the coefficient

$$f(u_1) \cdot \ldots \cdot f(u_k)/f(v_1) \cdot \ldots \cdot f(v_{k-1}),$$

the coefficients of $g(n)$ in $f*g(Q)$ will not cancel for non-specified values of f.

DEFINITION 5.16. $g(n)$ is <u>accessible</u> if either $o(g(n)) = 1$ or a quasi-generator of $g(n)$ can be obtained by the algorithm.

THEOREM 5.15. If $f*g = z$ with $f \neq z$ and $f(0) = 0$, then f is a Carlitz-type nilpotent function iff there exists $n \in N^*$ which is not accessible.

PROOF. If f is a Carlitz-type nilpotent function, then there exists $n \in N^*$ such that $v \nmid_p v+n$ for all $v \in S_f$ (Theorem 5.2). Clearly $g(n)$

is not accessible for this n.

To prove the converse we assume that f is not a Carlitz-type nilpotent function and show that g(n) is accessible for any $n \in N^*$.

Let $n \in N^*$. If $o(g(n)) = 1$, then g(n) is accessible. If $o(g(n)) \neq 1$, then for all $u \in S_f$ such that $u|_p u+n$, there exists $v \in S_f$ such that $v < u$ and $v|_p u+n$. f is not a Carlitz-type nilpotent function; so for $r = 0, 1, 2, \ldots$, there exists $u \in S_f$ such that $\delta_p(u) > p^r$. Let u_1 be any element of S_f such that $\delta_p(u_1) > \Delta_p(n)$ and such that u_1 has no proper p-factor in S_f. Then $(u_1,n)_p = 0$ and $u_1|_p u_1+n$. Let $Q_1 = n + u_1$.

Let v_1 be the least p-factor of Q_1 that is in S_f. Then $v_1 < u_1$ and by choice of u_1, we have $(v_1,n)_p > 0$. Let $m_1 = Q_1 - v_1$. If Q_1 is not the LPG of $g(m_1)$, then Q_1 is a quasi-generator of g(n), and g(n) is accessible.

If Q_1 is the LPG of $g(m_1)$, let u_2 be any element of S_f such that $\delta_p(u_2) > \Delta_p(u_1)$ and such that u_2 has no proper p-factor in S_f. Then $u_2|_p m_1 + u_2$ and $(u_2,Q_1)_p = 0$. Let $Q_2 = m_1 + u_2 = n + u_1 - v_1 + u_2$. Let v_2 be the least p-factor of Q_2 that is in S_f and $m_2 = Q_2 - v_2$. If Q_2 is not the LPG of $g(m_2)$ then Q_2 is a quasi-generator of g(n).

If Q_2 is the LPG of $g(m_2)$, then $v_2 = v_1$ and $p > 2$. (Clearly $v_2 \geq v_1$, and if $v_2 > v_1$ then $v_1|_p v_1+Q_1 - v_1 \Rightarrow v_1|_p v_1 + Q_1 - v_1 + u_2$ by choice of u_2. Hence $v_1|_p v_1 + Q_2 - v_2 = v_1 + m_2$. If there exists $v' \in S_f$ such that $v' < v_1$ and $v'|_p v_1 + m_2$, then $v'|_p n+u_1 = Q_1$. But Q_1 is the LPG of $g(m_1)$. Hence $v_1 + m_2$ is a primary generator of $g(m_2)$ that is less than Q_2, a contradiction.)

Let u_3 be any element of S_f such that $\delta_p(u_3) > \Delta_p(u_2)$ and such that u_3 has no proper p-factor in S_f. Then $u_3 |_p Q_2 - v_2 + u_3$ and $(u_3, Q_2)_p = 0$. Let $Q_3 = Q_2 - v_2 + u_3$, let v_3 be the least p-factor of Q_3 that is in S_f, and let $m_3 = Q_3 - v_3$. If Q_3 is not the LPG of $g(m_3)$, then Q_3 is a quasi-generator of $g(n)$.

If Q_3 is the LPG of $g(m_3)$, then as before $v_3 = v_2 = v_1$ and $p > 3$. It is clear that we need only continue the process for at most $k + 1$ steps, where $kv_1 |_p n + u_1$, $(k + 1)v_1 \nmid_p n + u_1$, in order to obtain a quasi-generator of $g(n)$. The fact that f is not a Carlitz-type nilpotent function guarantees that we may choose u_i $(1 \leq i \leq k + 1)$ with $\delta_p(u_i)$ as large as we need and that we can find such a u_i with no proper p-factor in S_f. Moreover we must have that $k + 1 \leq p$ since the largest number of times that v_1 can possibly be a p-factor of n is $p - 1$.

THEOREM 5.16. Suppose $o(g(n)) \neq 1$ and that no p-factor of n is in S_f. Let U be an infinite sequence of elements u_i of S_f such that

i) $\Delta_p(n) < \delta_p(u_1)$,

ii) $\delta_p(u_{i+1}) > \Delta_p(u_i)$ $(i \geq 1)$,

iii) u_i has no proper p-factor in S_f, $i = 1, 2, \ldots$.

Then there exists $r \in N^*$ such that $n + u_i$ is a quasi-generator of $g(n)$ for all $i > r$.

PROOF. $o(g(n)) \neq 1 \Longrightarrow$ for each i there exists $v \in S_f$ such that $v < u_i$ and $v |_p n + u_i$. For each i, let v_i be the least such number.

No element of S_f is a p-factor of n and u_i has no proper p-factor in $S_f \Longrightarrow \alpha_i = (v_i, n)_p > 0$ and $\beta_i = (v_i, u_i)_p > 0$. Since $u_1 < u_2 < \ldots$,

we must have $v_1 < v_2 < \ldots$, with $v_i = \alpha_i + \beta_i$, and $(\alpha_i,\beta_i)_p = 0$.

Since U is infinite and since n has only a finite number ($\tau_p(n)$) of p-factors, the α_i's will have only a finite number, say t, of distinct forms $\alpha_{i_1}, \ldots, \alpha_{i_t}$ $(i_1 < \ldots < i_t)$. We will assume that v_r is the least v_i where α_{i_t} occurs. Hence for $i > r$, $v_i = \alpha_i + \beta_i$ $= \alpha_{i_j} + \beta_i$ for some j with $1 \leq j \leq t$.

For $i > r$, $n + u_i$ is not the LPG of $g(m_i)$ (where $m_i = n + u_i - v_i$), since there exists v_j with $j < r$ such that $\alpha_i = \alpha_j$. Hence $v_j \mid_p v_j + m_i$ by choice of the u_i's. If there exists $v < v_j$ with $v \in S_f$ and $v \mid_p v_j + m_i$, then

$$v_j = \alpha_j + \beta_j = \alpha_i + \beta_j,\ \alpha_i = \alpha_j \mid_p n,\ \beta_j \mid_p u_j;$$

$$m_i = \varepsilon_i + \omega_i,\ \varepsilon_i \mid_p n,\ \omega_i \mid_p u_i;$$

$$v_j + m_i = \alpha_j + \beta_j + \varepsilon_i + \omega_i$$

$$= \alpha_i + \beta_j + \varepsilon_i + \omega_i$$

$$= n + \beta_j + \omega_i;$$

and $v < v_j$ and $(v_j,u_i)_p = 0 \Longrightarrow (v,u_i)_p = 0$; so $(v,\omega_i)_p = 0$. So $v \mid_p n + \beta_j \Longrightarrow v \mid_p n+u_j$. This contradicts the assumption that v_j is the least p-factor of $n + u_j$ that is in S_f. Hence $v_j + m_i$ is a primary generator of $g(m_i)$ that is less than $v_i + m_i = n + u_i$. Therefore for $i > r$, $n + u_i$ is a quasi-generator of g(n).

COROLLARY. If no p-factor of n is in S_f and if $o(g(n)) \neq 1$, then there exists $r \in N^*$ such that if $u \in S_f$ with $\delta_p(u) > p^r$, $n + u$ is a quasi-generator of $g(n)$.

We note that if n is itself the LPG of g(m) for some $m \in N$, then $n + u$ cannot be a quasi-generator of g(n) for any $u \in S_f$.

THEOREM 5.17. Suppose $o(g(n)) \neq 1$, at least one proper p-factor of n is in S_f, and n is not itself the LPG of g(m) for any $m \in N^*$. Let U be an infinite sequence of elements u_i of S_f such that

i) $\delta_p(u_1) > \Delta_p(n)$;

ii) $\delta_p(u_{i+1}) > \Delta_p(u_i)$ $(i \geq 1)$,

iii) no proper p-factor of u_i is in S_f, $i = 1, 2, \ldots$.

Then $n + u_i$ is a quasi-generator of g(n), $i = 1, 2, \ldots$.

PROOF. Let v_1 be the least p-factor of $n + u_1$ that is in S_f. Then by choice of the u_i's, $v_1 |_p n$ and is the least p-factor of n that is in S_f. Moreover v_1 is the least p-factor of $n + u_i$ that is in S_f, $i = 1, 2, \ldots$.

Let $m_1 = n + u_1 - v_1$. Then $m_1 = t + u_1$, where $t |_p n$, $t > 0$. n is not the LPG of g(t), but $o(g(t)) = 1$. Let M be the LPG of g(t). Then $M = v_o + t$, where $v_o \in S_f$, and v_o is the least p-factor of M that is in S_f. Also $M < n \Longrightarrow v_o < v_1$.

Now $o(g(m_1)) = 1$ and $n + u_1$ is a primary generator of $g(m_1)$. $M + u_1 < n + u_1$ and is the LPG of $g(m_1)$; so $n + u_1$ is a quasi-generator of g(n).

Similarly $n + u_i$ is a quasi-generator of g(n) for $i > 1$.

If the only p-factor of n that is in S_f is n itself, then n is a primary generator of g(0). n is not the LPG of g(0) unless n is the least element of S_f. If n is the least element of S_f and $o(g(n)) \neq 1$, then for any $u_1, u_2 \in S_f$ with $\delta_p(u_1) > \Delta_p(n)$ and $\delta_p(u_2) > \Delta_p(u_1)$, $n + u_1 - n + u_2 = u_1 + u_2$ is a quasi-generator of g(n).

Henceforward we will proceed under the following assumptions. (We reiterate here the earlier assumptions and add some new ones.)

i) f is a singular function that is not a Carlitz-type nilpotent function;

ii) $f*g = z$ with g undetermined;

iii) $S_f = \{n \in N^* : f(n) \neq 0\}$;

iv) $o(g(n)) \neq 1$ for any n or g(n) under discussion, unless otherwise stated;

v) U is an infinite sequence of elements u_i of S_f such that

a) $\delta_p(u_1) > \Delta_p(n)$,

b) $\delta_p(u_{i+1}) > \Delta_p(u_i)$ $(i \geq 1)$,

c) no proper p-factor of u_i is in S_f, $i = 1, 2, \ldots$;

vi) if n is not itself the LPG of g(m) for some $m \in N$, then $n + u_i$ is a quasi-generator of g(n), $i = 1, 2, \ldots$. (5.7)

THEOREM 5.18. If $Q = n + u_{i_1} - v_1 + \ldots + u_{i_k}$ $(k > 1)$, (5.8) $u_{i_j} \in U$ $(1 \leq i_j \leq k)$, $M_1 = n + u_{i_1}$, $M_j = n + u_{i_1} - v_1 + \ldots + u_{i_j}$ $(j > 1)$, v_j is the least p-factor of M_j that is in S_f $(1 \leq j \leq k - 1)$, $m_j = M_j - v_j$, and M_j is the LPG of $g(m_j)$ $(i \leq j \leq k - 1)$; then $(n, M_j)_p > 0$ $(1 \leq j \leq k - 1)$.

PROOF. Clearly $(n,M_1)_p > 0$.

If $k > 2$, then $M_2 = n + u_{i_1} - v_1 + u_{i_2}$. Suppose $(n,M_2)_p = 0$. Then by choice of the u_i's $(n,M_j)_p = 0$ for $j > 2$. Also $n|_p v_1$, and we must have $v_2 > v_1$. If $m_2 = M_2 - v_2$, then $k > 2 \Longrightarrow M_2$ is the LPG of $g(m_2)$.

Now $$v_1 + M_2 = v_1 + n + u_{i_1} - v_1 + u_{i_2}$$

$$= n + u_{i_1} + u_{i_2},$$

and by choice of the u_{i_j}'s, $v_1|_p v_1 + M_2$. Hence $v_1|_p v_1 + m_2$, and

$$v_1 + m_2 = v_1 + M_2 - v_2$$

$$= v_1 + m_1 + u_{i_2} - v_2$$

$$= v_1 + M_1 - v_1 + u_{i_2} - v_2$$

$$= M_1 + u_{i_2} - v_2$$

$$= n + u_{i_1} + u_{i_2} - v_2.$$

v_1 must be the least p-factor of $v_1 + m_2$ that is in S_f. Hence $v_1 + m_2$ is a primary generator of $g(m_2)$ that is less than M_2, a contradiction. So $(n,M_2)_p > 0$.

We assume the theorem is true for M_j $(1 \leq j \leq t, k > t)$, and let $j = t + 1$ $(k > t + 1)$. The proof of the inductive step is as follows.

$M_{t+1} = n + u_{i_1} - v_1 + \ldots + u_{i_t} - v_t + u_{i_{t+1}}$. If $(n,M_{t+1})_p = 0$, then $n|_p v_1 + \ldots + v_t$, and $(n,v_{t+1})_p = 0$. Also $(n,M_j)_p > 0$ for $j \leq t \Rightarrow (v_j,n)_p > 0$, $j \leq t$. We must have $v_1 \leq v_{t+1}$. By choice of the u_{i_j}'s, and since $(v_t,n)_p > 0$ and $(v_{t+1},n)_p = 0$, we have $v_1 < v_{t+1}$.

By an argument similar to the one in the case for M_2, we obtain $v_1|_p v_1 + m_{t+1}$ and $v_1 + m_{t+1}$ is a primary generator of $g(m_{t+1})$ that is less than M_{t+1}. This contradicts M_{t+1}'s being the LPG of $g(m_{t+1})$.

COROLLARY 1. If Q is a quasi-generator of g(n) that has the form (5.8), then $v_1 = \ldots = v_{k-1}$.

COROLLARY 2. If Q is a quasi-generator of g(n) that has the form (5.8), then $v_i|_p n + u_{i_1}$, $1 \leq j \leq k - 1$.

COROLLARY 3. If Q is a quasi-generator of g(n) that has the form (5.8) and if n is itself the LPG of g(m) for some $m \in N$, then $v_j|_p n$, $1 \leq j \leq k - 1$.

COROLLARY 4. If n is the LPG of g(m) for some $m \in N$, if

$$Q = n + u_{i_1} - v_1 + \ldots + u_{i_r},$$

$$Q' = n + u_{j_1} - v_1 + \ldots + u_{j_s},$$

are quasi-generators of g(n) that have the form (5.8), then r = s.

We note that for $\delta_p(u_1)$ large enough, it is not necessary to take more than one step of the algorithm to obtain a quasi-generator

of g(n) unless n is itself the LPG of g(m) for some $m \in N$. We assume from here on that Q has the form (5.8) only if n is the LPG of g(m) for some $m \in N$.

THEOREM 5.19. If Q is a quasi-generator of g(n) that has the form (5.8), then

i) $v_1 |_p v_1 + Q$, and

ii) if $m |_p Q$, then $o(g(m)) = 1$.

PROOF. By Corollaries 1 and 3, $Q = n - (k-1) + \sum_{j=1}^{k} u_{i_j}$ $(k > 1)$, where $(k-1)v_1 |_p n$. Since $u_{i_j} \in U$ $(1 \leq j \leq k)$, we must have $v_1 |_p v_1 + Q$.

$m |_p Q \Longrightarrow v_1 |_p v_1 + m$. If there is a number $v' \in S_f$ such that $v' < v_1$ and $v' |_p v_1 + m$, then $m |_p Q \Longrightarrow v_1 + m |_p M_{k-1} + u_{i_k} \Longrightarrow v' |_p M_{k-1}$. But M_{k-1} is the LPG of $g(M_{k-1} - v_1)$; so we have a contradiction; i.e., $o(g(m)) = 1$.

THEOREM 5.20. Let n be a fixed positive integer with $o(g(n)) \neq 1$. For each $u_i \in U$, let $S_i = \{u \in S_f : u \leq u_i \text{ and } u |_p n + u_i\}$. For each i, let $S_i' = \{(n,u)_p : u \in S_i\}$. Then there is an infinite subsequence U' of U such that $S_i' = S_j'$ for all $u_i, u_j \in U'$.

PROOF. Note that $0 \in S_i'$, $i = 1, 2, \ldots$, and $o(g(n)) \neq 1 \Longrightarrow$ there exists $u \in S_i$ such that $u < u_i$ with $(n,u)_p > 0$.

Since U is infinite there are infinitely many sets S_i', but each set S_i' contains at most $\tau_p(n)$ elements, all of which are p-factors of n. Hence there must be an infinite subsequence U' of U so that for all $u_i \in U'$, S_i' contains some fixed number, say t, of elements. Similarly there must be an infinite subsequence U'' of U' such that for all

$u_i, u_j \in U''$, $S'_i = S'_j$.

From here on we will assume that the u_i's in U are chosen so that for $u_i, u_j \in U$, $S'_i = S'_j$.

If Q is a quasi-generator of g(n), if g(m) appears in f*g(Q) with at most order 1 substitutions, and if $m > n$, then $m = \alpha + \beta$, where $\Delta_p(\alpha) < \delta_p(u_1)$ and $\delta_p(\beta) \geq \delta_p(u_1)$. The numbers α and β will be called, respectively, the α-part and the β-part of m and will be denoted by $\alpha(m)$ and $\beta(m)$, respectively. Note that $o(g(m)) \neq 1 \Longrightarrow \alpha(m) \neq 0$. $m > n$ does not necessarily imply that $\beta(m) \neq 0$.

If $Q_i = n + u_i$ $(i = 1, 2, \ldots)$, if $m_j \mid_p Q_i$ with $Q_i - m_j = x_j \in S_f$ $(1 \leq j \leq t_i)$, and if $m_j > n$ then for all j with $1 \leq j \leq t_i$, there is an h with $1 \leq h \leq t_k$ (for $Q_k = n + u_k$), and with $\alpha(m_j) = \alpha(m_k)$. (This is immediate from Theorem 5.20.) Note that we do not assume that $t_i = t_k$, since for any t_i there might be m_{j_1} and m_{j_2} with $\alpha(m_{j_1}) = \alpha(m_{j_2})$ and $\beta(m_{j_1}) \neq \beta(m_{j_2})$ $(1 \leq j_1, j_2 \leq t_i)$.

Again by Theorem 5.20 if we choose u_1 with $\delta_p(u_1)$ large enough we can guarantee that if $m \mid_p Q_1 = n + u_1$, if $m > n$, if $Q_1 - m = x_1 \in S_f$, if $o(g(m)) = 1$, and if M is the LPG of g(m), then $\alpha(v) = v$, where $v = M - m$. (It might be that $M = Q_1$, in which case $v = x_1$ and $v \mid_p n$.) The same will be true if $m \mid_p Q_i = n + u_i$ $(i > 1)$ with $Q_i - m \in S_f$ and $o(g(m)) = 1$.

By the above and Theorem 5.20, if $m \mid_p Q_i$ with $Q_i - m = v \in S_f$, $m > n$, and $o(g(m)) = 1$, then for $Q_j \neq Q_i$ there exists m' with $m' \mid_p Q_j$, $Q_j - m' = v' \in S_f$, $m' > n$, and $\alpha(m') = \alpha(m)$. Moreover if $v_o + m$ is the LPG of g(m), then $v_o + m'$ is the LPG of g(m'), and $\alpha(v_o) = v_o < u_1$.

Let $S = \{Q_1, Q_2, \ldots\}$, $(Q_i = n + u_i)$. For each i, let $T_i = \{m \in N^* : o(g(m)) \neq 1, m > n, g(m)$ appears in $f*g(Q_i)$ after all order 1 substitutions have been made$\}$, and let $T_i' = \{\alpha(m) : m \in T_i\}$. There are infinitely many sets T_i. Some of them may be empty, in which case $T_i' = \phi$.

If at most a finite number of the T_i's are empty, then we may obtain a sequence $U' = \{u_{i_j}\}_{j=1}^{\infty} \subseteq U$, where $T_{i_j} \neq \phi$ for all j. Now T_{i_j}' is finite and non-empty, j = 1, 2, ..., and T_{i_j}' contains at most $\tau_p(p^c - 1)$ elements, where $p^c = \delta_p(u_1)$. (Note that u_1 in this case is in U but not necessarily in U'.)

By the same argument as in the proof of Theorem 5.20 we can find an infinite subsequence U'' of U', where $U' = \left\{u_{i_{j_k}}\right\}_{k=1}^{\infty}$ with $T'_{i_{j_1}} = T'_{i_{j_2}} = \ldots$.

If infinitely many of the T_i's are empty we can obtain an infinite sequence $U' = \{u_{i_j}\}_{j=1}^{\infty} \subseteq U$ where $T_{i_j} = \phi$ for all j.

We have just proven

THEOREM 5.21. If $Q_i = n + u_i$ $(u_i \in U)$, i = 1, 2, ..., if $T_i = \{m \in N^* : m > n, o(g(m)) \neq 1$, and $g(m)$ appears in $f*g(Q_i)$ after all order 1 substitutions have been made$\}$, and if $T_i' = \{\alpha(m) : m \in T_i\}$, then either

i) There exists an infinite subsequence U' of U such that for all Q_i, Q_j, $i \neq j \Rightarrow T_i' = T_j'$, $T_i', T_j' \neq \phi$, or

ii) There exists an infinite subsequence U' of U such that for all i, $T_i = \phi$.

Note that if Q_i is a quasi-generator of g(n) for all i, and if $T_i = \phi$ for even one i, then g(n) can be obtained, and o(g(n)) = 2.

How we choose u_1 will depend on n and the function f and its properties. If $S = \{v \in S_f : v + m$ is the LPG of g(m) for some $m \in N\}$ is finite, then it would be natural to choose u_1 as follows. Let

$$\begin{aligned} p^r &= \Delta_p(n), \\ p^s &= \max\{\Delta_p(v) : v \in S\}, \\ p^c &= \max\{p^r, p^s\}, \text{ and} \\ P &= \sum_{i=0}^{c} (p-1)p^i. \end{aligned} \tag{5.9}$$

We make certain that $\delta_p(u_1) > p^c$. Then if Q is any quasi-generator of g(n) that is obtained by using elements of U (and the algorithm), and if m is any number such that either $m \mid_p Q$ with $Q - m \in S_f$ or m appears in f*g(Q) with order 1 substitutions, then

$$\begin{aligned} \alpha(m) &= (m,P)_p, \\ \beta(m) &\mid_p \beta(Q), \end{aligned} \tag{5.10}$$

where $\beta(Q)$ is equal to some sum of u_i's in U. Moreover we can guarantee that for all $v \in S$, $\alpha(v) = v$, $\beta(v) = 0$.

If S is infinite then the choice of u_1 is more difficult, particularly when the elements of U are such that $\omega_p(u_i)$ becomes

arbitrarily large and the possibility exists of having $\omega_p(m)$ very large with $o(g(m)) = 1$. We need to be able to choose u_1 large enough so that if $g(m)$ appears in $f*g(Q)$ with at most order 1 substitutions and if $o(g(m)) = 1$, then any element v of S that is needed to obtain the LPG of $g(m)$ will be such that $\alpha(v) = v$. This will insure that $\beta(m) \mid_p \beta(Q)$; i.e., the important differences in these m's will depend only on their α-parts, of which there will only be a finite number.

For the present we will deal only with those functions f for which the set S is finite. In the succeeding theorems, unless otherwise stated, we assume that S is finite and that $\alpha(m)$ and $\beta(m)$ are defined as in (5.9) and (5.10).

THEOREM 5.22. If $Q_1 = n + u_{i_1}$, $Q_2 = n + u_{i_2}$, $i_1 \neq i_2$, and if there exists m with $o(g(m)) \neq 1$, $g(m)$ appears in $f*g(Q_1)$ with at most order 1 substitutions, and $u_{i_1} \mid_p m$, then there exists m' with $\alpha(m') = \alpha(m)$, $g(m')$ appears in $f*g(Q_2)$ with at most order 1 substitutions, and $u_{i_2} \mid_p m'$, and conversely.

PROOF. If $m \mid_p Q_1$ with $Q_1 - m = u \in S_f$, then $u \mid_p n$, $u \mid_p Q_2$, and $m' = Q_2 - u$.

If $Q_1 = m + w_1 - v_1 + \ldots + w_k$ $(k > 1)$, $w_j \in S_f$ $(i \leq j \leq k)$, $v_j \in S_f$ $(1 \leq j \leq k - 1)$, then we may assume that $\alpha(v_j) = v_j$, $1 \leq j \leq k - 1$ (Theorem 5.13). $u_{i_1} \mid_p m \Rightarrow \beta(w_i) = 0$ $(1 \leq j \leq k)$. So $w_k \mid_p n$, $Q_2 - w_k + v_{k-1} + \ldots + v_1 - w_1 = m'$, and $u_{i_2} \mid_p m'$.

The argument for the converse is the dual of the above argument.

THEOREM 5.23. If Q_1 and Q_2 are quasi-generators of $g(n)$ of the form (5.7) or (5.8) with $(\beta(Q_1), \beta(Q_2))_p=0$, and if Q_1 is an order 2 generator of $g(m)$ for some $m > n$, then for all m' with $\alpha(m') = \alpha(m)$ such that Q_2 is a quasi-generator of $g(m')$, an order 2 generator of $g(m')$ can be obtained.

PROOF. We must consider the following cases.

Case 1. $Q_1 = n + u_{i_1}$, $Q_2 = n + u_{i_2}$, $u_{i_1} \neq u_{i_2}$, $u_{i_j} \in U$.

Subcase a. $m|_p Q_1$ with $Q_1 - m \in S_f$.

Subcase b. $Q_1 = m + w_1 - v_1 + \ldots + w_k$ $(k > 1)$, $w_j \in S_f$ $(1 \leq j \leq k)$, $v_j \in S_f$ $(i \leq j \leq k - 1)$.

Case 2. $Q_1 = n + u_{i_1} - v_o + \ldots + u_{i_t}$,

$Q_2 = n + u_{j_1} - v_o + \ldots + u_{j_t}$, $t > 1$, $u_{i_r}, u_{j_r} \in U$ $(1 \leq r \leq t)$.

PROOF OF CASE 1. $Q_1 = n + u_{i_1}$, $Q_2 = n + u_{i_2}$, $u_{i_1}, u_{i_2} \in U$.

Subcase a. Suppose the largest number m such that $m > n$, $o(g(m)) \neq 1$, and Q_1 is a quasi-generator of $g(m)$ is such that $m|_p Q_1$, $Q_1 - m = w \in S_f$. Then by Theorem 5.21 there exists m' with $\alpha(m') = \alpha(m)$ and $m'|_p Q_2$ with $Q_2 - m' \in S_f$. $Q_1 = m + w$ is a quasi-generator of $g(m) \Rightarrow \alpha(m) + w$ is a quasi-generator of $g(\alpha(m))$. So $m' + w$ is a quasi-generator of $g(m')$. Also $m > n \Rightarrow w < u_{i_1}$. u_{i_1} has no proper p-factors in S_f; hence $(w,n)_p = \alpha(w) > 0$. $\alpha(m) + \alpha(w) = n$.

Suppose there exists $m'' > m'$ such that $o(g(m'')) \neq 1$ and $m' + w$ is a quasi-generator of $g(m'')$. If $m''|_p m' + w$ with $m' + w - m'' = w' \in S_f$, then $w' < w$ and $w'|_p \alpha(m') + w = \alpha(m) + w$. Hence $w'|_p Q_1$ and $\alpha(Q_1 - w') = \alpha(m'')$. Moreover $w' < w \Rightarrow Q_1 - w' > m$, and $o(g(m'')) \neq 1$. So $o(g(\alpha(m''))) \neq 1 \Rightarrow o(g(Q_1 - w')) \neq 1$. This contradicts Q_1's being an order 2 generator of $g(m)$.

If $m' + w = m'' + w_1 - v_1 + \ldots + w_t$ where $w_i \in S_f$ $(1 \leq i \leq t)$ and v_i is the least p-factor of M_i that is in S_f $(1 \leq i \leq t-1)$, let $m_i = M_i - v_i$ $(1 \leq i \leq t-1)$. $(M_1 = m'' + w_1$, $M_i = m'' + w_1 - v_1 + \ldots + w_i$ $(i > 1).)$. Then $m_i > m''$, $1 \leq i \leq t-1$; so $w_i < w$, $1 \leq i \leq t$, and $\sum_{i=1}^{t} \beta(w_i) \mid_p \beta(w)$. M_i is the LPG of $g(m_i)$, $1 \leq i \leq t-1$, so $\alpha(v_i) = v_i$, $1 \leq i \leq t-1$. Hence $\alpha(m'' + w_1 - v_1 + \ldots + w_t) \mid_p n$. Then $(\alpha(m'') + w_1 - v_1 + \ldots + w_t) \mid_p Q_1$; in particular, $w_t \mid_p Q_1$. So we must have $\alpha(Q_1 - w_t + v_{t-1} - \ldots - w_1) = \alpha(m'')$. $w < u_{i_1}$; so $\beta(Q_1 - w_t + v_{t-1} \ldots - w_1) > \beta(m)$. There must exist a number $m''' > m$ with $\alpha(m''') = \alpha(m'')$ and such that Q_1 is a quasi-generator of $g(m''')$. This again contradicts Q_1's being an order 2 generator of $g(m)$.

Subcase b. Suppose $Q_1 = m + w_1 - v_1 + \ldots + w_t$ $(t > 1)$, $w_i \in S_f$, $1 \leq i \leq t$. If $M_1 = m + w_1$, $M_i = m + w_1 - v_1 + \ldots + w_i$ $(i > 1)$, then M_i is the LPG of $g(m_i)$, where $m_i = M_i - v_i$, $1 \leq i \leq t-1$, and $\alpha(v_i) = v_i$.

There exists m' with $\alpha(m') = \alpha(m)$ and Q_2 is a quasi-generator of $g(m')$. Let $Q' = m' + w_1 - v_1 + \ldots + w_t$. We know that $(\beta(w_i), u_{i_2})_p = 0$, $1 \leq i \leq t$, and $\beta(m') \mid_p u_{i_2} \Longrightarrow \beta(w_i) \mid_p u_{i_1}$, $1 \leq i \leq t$. Also $\alpha(w_i) \mid_p \alpha(Q_1) = n$, since $\alpha(Q') = \alpha(Q_1)$.

Suppose there exists m'' with $o(g(m'')) \neq 1$, $m'' > m'$, and Q' is a quasi-generator of $g(m'')$. If $m'' \mid_p Q'$ with $Q' - m'' = w \in S_f$, then $m'' > m' \Longrightarrow \beta(m'') \geq \beta(m')$; so $\beta(m') \mid_p \beta(m'')$ and $\beta(w') \mid_p u_{i_1}$. Also $\alpha(w) \mid_p Q_1$ since $\alpha(Q') = \alpha(Q_1) = n$. So $w \mid_p Q_1$ with $Q_1 - w = m'''$, where $\alpha(m''') = \alpha(m'')$. Now $m'' > m' \Longrightarrow w < w_1 - v_1 + \ldots + w_t = Q' - m' = Q_1 - m$. Hence $m''' > m$, a contradiction.

Suppose $Q' = m'' + w_1' - v_1' + \ldots + w_r'$. Again $m'' > m'$, $\beta(m')|_p\beta(m'')$; so $\sum_{i=1}^{r} \beta(w_i')|_p u_{i_1}$. In fact, $w_r'|_p Q_1$, and $Q_1 - w_r' + v_{r-1}' - \ldots - w_1' = m'''$, where $\alpha(m''') = \alpha(m'')$. So $Q' = m' + w_1 - v_1 + \ldots + w_t = m'' + w_1' - v_1' + \ldots + w_r'$, and $m'' > m' \Longrightarrow w_1' - v_1' + \ldots + w_r' < w_1 - v_1 + \ldots + w_t$. Since $Q_1 = m + w_1 - v_1 + \ldots + w_t = m''' + w_1' - v_1' + \ldots + w_r'$, we must have $m''' > m$, a contradiction. Therefore the theorem is true for case 1.

The proof of case 2 is similar to the argument in the second half of case 1, subcase b.

Carlitz [1] conjectures that an element of L is a zero divisor iff f has the form (5.1); or equivalently, if $f*g = z$ with $f \neq z$ $(f(0)) = 0)$, then f is not a Carlitz-type nilpotent function iff $g = z$. In order to prove this conjecture, it will be sufficient to prove that if f is a singular function that is not a Carlitz-type nilpotent function, and if $f*g = z$, then $g(n)$ is uniquely determined for all $n \in N^*$. (We already know that $g(0) = 0$.) Toward this end, we define the following sets.

Let n be any positive integer with $o(g(n)) \neq 1$, and let U be as defined above. We assume that $n + u_{i_1} - v_o + \ldots + u_{i_k}$ $(k \geq 1)$, $u_{i_j} \in U$, $(1 \leq j \leq k)$, is a minimal quasi-generator of $g(n)$. Let

$$U_o = \{u_1, \ldots, u_{k+p} : u_i \in U,\ 1 \leq i \leq k + p\},$$

$$R_o = \{Q = n + u_{i_1} - v_o + \ldots + u_{i_k} : u_{i_j} \in U_o,\ 1 \leq j \leq k\},$$

$$X_o = \{x > n : Q \in R_o \text{ is a quasi-generator of } g(x)\}.$$

$$A_o = \{\alpha(x) : x \in X_o\}.$$

If $\#(R_o) > \#(X_o)$, then clearly g(n) may be obtained. Otherwise, we continue.

$$U_1 = \{u_1, \ldots, u_{k+2p}\},$$

$$R_1 = \{Q = n + u_{i_1} - v_o \ldots + u_{i_k} : u_{i_j} \in U_1,\ 1 \leq j \leq k + 2p\},$$

$$S_1 = \{Q : Q \text{ is a minimal quasi-generator of } g(x)\ (x \in X_o)$$
$$\text{formed by using numbers } u_i \in U_1,\ (u_i, x)_p = 0\},$$

$$T_1 = R_1 \cup S_1,$$

$$X_1 = \{x > n : Q \in R_1 \text{ is a quasi-generator of } g(x)\},$$

$$Y_1 = \{y > n : Q \in S_1 \text{ is a quasi-generator of } g(y)\},$$

$$W_1 = X_1 \cup Y_1$$

$$A_1 = \{\alpha(x) : x \in W_1\},$$

.
.
.

$$U_i = \{ u_1, \ldots, u_{k+(i+1)p} \},$$

$$R_i = \{Q = n + u_{i_1} - v_o + \ldots + u_{i_k} : u_{i_j} \in U_i\},$$

$$S_i = \{Q : Q_i \text{ is a minimal quasi-generator of } g(x) \ (x \in W_{i-1}) \text{ formed by using } u_j \in U_i,\ (u_j,x)_p = 0\},$$

$$T_i = R_i \cup S_i$$

$$X_i = \{x > n : Q \in R_i \text{ is a quasi-generator of } g(x)\},$$

$$Y_i = \{y > n : Q \in S_i \text{ is a quasi-generator of } g(y)\},$$

$$W_i = X_i \cup Y_i ,$$

$$A_i = \{\alpha(x) : x \in W_i\},$$

.
.
.

Since $\alpha(x) = (x,P)_p$, the number of possible values for $\alpha(x)$ is finite, and there exists $B > 0$ such that for all $i > B$, $A_i = A_B$. Moreover, for all substitutions of any order in $f*g(Q)$ for any $Q \in T_i$, any $x > n$ that appears in $f*g(Q)$ must be an element of W_i.

We note that

$$U_i \subseteq U_{i+1} \qquad (i \geq 0)$$

$$R_i \subseteq R_{i+1} \qquad (i \geq 0)$$

$$S_1 \subseteq S_{i+1} \qquad (i \geq 1)$$

$$T_i \subseteq T_{i+1} \qquad (i \geq 1)$$

$$X_i \subseteq X_{i+1} \qquad (i \geq 0)$$

$$Y_i \subseteq W_i \subseteq Y_{i+1} \qquad (i \geq 1)$$

$$W_i \subseteq W_{i+1} \qquad (i \geq 1)$$

$$A_i \subseteq A_{i+1} \qquad (i \geq 0) .$$

For each i, we define

$$R'_i = R_i - R_{i-1} \quad (i \geq 1) \text{ with } R'_o = R_o,$$

$$S'_i = S_i - S_{i-1} \quad (i \geq 2) \text{ with } S'_1 = S_1,$$

$$T'_i = T_i - T_{i-1} \quad (i \geq 1) \text{ with } T'_o = R'_o = R_o,$$

$$X'_i = X_i - X_{i-1} \quad (i \geq 1) \text{ with } X'_o = X_o,$$

$$Y'_i = Y_i - W_{i-1} \quad (i \geq 2) \text{ with } Y'_1 = Y_1 - X_0,$$

$$W'_i = W_i - W_{i-1} \quad (i \geq 1) \text{ with } W'_o = X'_o = X_o,$$

$$A'_i = A_i - A_{i-1} \quad (i \geq 1) \text{ with } A'_o = A_o .$$

It is clear that for any $i \geq 0$ and for all $x \in W_i'$, there are at least p elements of U_i such that $(x,u_i)_p = 0$. Moreover for each i, R_i contains exactly $\binom{k+(i+1)p}{k}$ elements.

THEOREM 5.24. For each $i \geq 0$, there is a one-to-one mapping $\theta: W_i' \to S_{i+1}'$.

PROOF. We define $\theta: W_0' = X_0 \to S_1' = S_1$ by $\theta(x)$ = the least quasi-generator of $g(x)$ that is in S_1. Let $x, x' \in X_0$. If $x \neq x'$, then either $\alpha(x) \neq \alpha(x')$ or $\beta(x) \neq \beta(x')$.

Suppose $x \neq x'$ and $\alpha(x) = \alpha(x')$. Then $\beta(x) \neq \beta(x')$. Let t_x be the number of steps of the algorithm needed to obtain a minimal quasi-generator of $g(x)$ (using u_j's in U_1). Then $t_x = t_{\alpha(x)} = t_x'$. Hence if Q and Q' are the least quasi-generators of $g(x)$ and $g(x')$ respectively, in S_1, then $\alpha(Q) = \alpha(Q')$.

Let $\beta_1 = (\beta(x),\beta(x'))_p$. Then $x = \alpha(x) + \beta_1 + \beta_2$, $x' = \alpha(x) + \beta_1 + \beta_2'$, where $(\beta_2,\beta_2')_p = 0$. Now $Q = Q' \Longrightarrow \beta_2$ and β_2' both consist of sums of u_j's (by definition of S_1). If γ_x is the number of distinct u_j's (in U_0) such that $(x,u_j)_p > 0$, then $Q = Q' \Longrightarrow \gamma_x = \gamma_{x'}$. Let γ_1 be the number of u_j's such that $(\beta_1,u_j)_p > 0$; let γ_2 be the number of u_j's such that $(\beta_2,u_j)_p > 0$; and let γ_2' be the number of u_j's such that $(\beta_2',u_j)_p > 0$. Then $\gamma_2 = \gamma_2' = \gamma_x - \gamma_1$, with $0 < \gamma_2 \leq t_x$. Moreover $0 \leq \gamma_1 < \gamma_x \leq k$; so $2p + k - \gamma_x \geq 2p$, and there are $\binom{2p+k-\gamma_x}{t_x}$ quasi-generators of $g(x)$ (and $g(x')$) in S_1. There are $\binom{p+k-\gamma_1}{\gamma_2}$ possible values for β_2 (and β_2') with $\binom{p+k-\gamma_1}{\gamma_2} \leq \binom{2p+k-\gamma_x}{t_x}$, since $\gamma_1,\gamma_2 \leq \gamma_x \leq k \leq p$, $\gamma_2 \leq t_x \leq p$.

If either β_2 or β_2' does not consist of a sum of u_i's, or if β_2 and β_2' consist of sums of different numbers of u_i's, then $Q \neq Q'$ even if the same u_i's are used to obtain both Q and Q'.

Suppose $\alpha(x) \neq \alpha(x')$ and that Q and Q' minimal quasi-generators of g(x) and g(x') respectively. We need to show that $\alpha(Q) \neq \alpha(Q')$.

Suppose $\alpha(Q) = \alpha(Q')$. Then $\alpha(Q) = \alpha(x) - tv$ $(0 \leq t < p)$, and $\alpha(Q') = \alpha(x') - rv'$ $(0 \leq r \leq p)$, where $v, v' \in S = \{v \in S_f : v + x$ is the LPG of g(x) for some $x \in N\}$. $\alpha(Q) = \alpha(Q') \Longrightarrow \alpha(x) - tv = \alpha(x') - rv'$. $v = v'$ and $t = r \Longrightarrow \alpha(Q) \neq \alpha(Q')$, since $\alpha(x) \neq \alpha(x')$. $v = v'$ and $t \neq r \Longrightarrow$ either $t < r$ or $r < t$. Suppose $t < r$. Then $\alpha(x) = \alpha(x') - (r-t)v \Rightarrow (r-t)v \mid_p \alpha(x) + (r-t)v$, so $v \mid_p \alpha(x) + v$. $\alpha(x')$ is the LPG of $g(\alpha(x') - v)$ (for $t \geq 1$). Suppose there exists $v_o < v$ such that $v_o \in S_f$ and $v_o \mid_p \alpha(x) + v$. Then $\alpha(x) + v = \alpha(x') - (r-t)v + v$ and $v' \mid_p \alpha(x') - (r-t+1)v = \alpha(x) - tv \Longrightarrow v' \mid_p \alpha(x)$, a contradiction. Hence $t \not< r$. Similarly $r \not< t$. Since we cannot have $v = v'$ and $t = r$, we must have $v \neq v'$. (5.11).

If $r = 0$ then $t \neq 0$ and $v \mid_p v + x'$; in fact $v + \alpha(x') = v + (\alpha(x)-v)$, and $o(g(x')) = 1$, a contradiction. So $r \neq 0$. Similarly $t \neq 0$. (We cannot have $r = 0$ and $t = 0$ by (5.11)). So $r \geq 1$ and $t \geq 1$.

Either $v < v'$ or $v' < v$. Suppose $v < v'$. We know that $v \not\mid_p \alpha(x')$ but $v \mid_p \alpha(x') - rv' + v$. In fact $tv \mid_p \alpha(x') - rv' + tv$.

Now $\alpha(x') - (r-1)v'$ is the LPG of $g(\alpha(x) - rv')$, but $\alpha(x') - rv' = \alpha(x) - tv \Longrightarrow v \mid_p \alpha(x') - rv' + v$. Moreover if there exists $v_o < v$ with $v_o \in S_f$ such that $v_o \mid_p^{\alpha} (x') - rv' + v$, then

$v_o|_p\alpha(x) - tv + v$. This contradicts $\alpha(x) - (t-1)v$'s being the LPG of $g(\alpha(x) - tv)$. So $v \nmid v'$. Similarly $v' \nmid v$. v cannot be equal to v', or we contradict (5.11). Therefore we must have $\alpha(x) \neq \alpha(x') \Rightarrow \alpha(Q) \neq \alpha(Q')$. Hence $Q \neq Q'$, and we can obtain a one-to-one mapping $\theta: X_o \to S_1$. In a similar manner we may extend θ to a one-to-one mapping $\theta : W_i' \to S_{i+1}'$, $i = 1, 2, \ldots$.

COROLLARY. For all i, $\#(S_{i+1}) \geq \#(W_i) \geq \#(Y_i)$.

With examples one can usually show for a fixed n that, for some i, $\#(T_i) > \#(W_i)$, and g(n) may be obtained for the defining n of these sets. However, the hypothesis $\#(T_i) > \#(W_i)$ seems insufficient to guarantee that a formula for g(n) may be obtained even if g(x) may be obtained for all $x \in W_i$.

THEOREM 5.25. If $\#(R_i) > \#(X_i)$ or if $\#(S_i) \geq \#(Y_i)$ for some $i > 0$, then a formula for g(n) may be obtained.

PROOF. Every element of R_i is an order 2 generator of some element of X_i. Moreover, if $Q \in R_i$ is a quasi-generator of g(x) for some $x \in W_i$, then $x \in X_i$; (i.e., $x \notin Y_i - X_i$). So $\#(R_i) > \#(X_i)$ clearly implies that a formula for g(x) may be obtained for every element x of X_i, and there is a Q' in R_i such that Q' is not needed as a generator of g(x) for any $x \in X_i$. For all $Q \in R_i$, Q is a quasi-generator of g(n); hence a formula for g(n) may be obtained from $f*g(Q')$.

Suppose $\#(S_i) \geq \#(Y_i)$. Every element of S_i is an order 2 generator of g(y) for some $y \in Y_i$. Moreover if $Q \in S_i$ is a quasi-generator of g(x) for some $x \in W_i$, then $x \in Y_i$ (i.e., $x \notin X_i - Y_i$). So it is

clear that for all $y \in Y_i$, $g(y)$ may be obtained from $f^*g(Q)$, for some $Q \in S_i$.

Let Q' be any element of R_o. Then $Q' \in R_i$, $Q' \notin S_i$, and Q' has not been used as a generator of $g(y)$ for any $y \in Y_i$. We make all possible order 1 substitutions within $f^*g(Q')$. For all $x \in W_i$ such that $g(x)$ appears in this version of $f^*g(Q')$, $x \in X_o \subseteq Y_1 \subseteq Y_i$. So a formula for $g(x)$ has already been obtained in terms of $g(x')$, where $x' \leq n$.

Now $g(n)$ appears in $f^*g(Q')$ and its coefficients do not cancel for non-specified values of f. Hence we may obtain a formula for $g(n)$ after substitutions have been made for $g(x)$ for all $x \in X_o$ with Q' a quasi-generator of $g(x)$.

There are good reasons to suppose that we might be able to show that there is a number D such that for all $i \geq D$, either $\#(R_i) > \#(X_i)$ or $\#(S_i) \geq \#(Y_i)$. For each i, $\#(R_i) = \binom{k + (i+1)p}{k}$, which increases rapidly as i increases. We also know (Theorem 5.24) that $\#(S_i') \geq \#(W_{i-1}') \geq \#(Y_{i-1}')$. It might be possible to use the techniques of the proof of Theorem 5.24 to obtain a one-to-one mapping $\theta' : W_i \to S_{i+1}'$. If θ' may be obtained, it might then be possible to show that $\#(W_{i+1}') \leq \#(S_i)$, or at least that $\#(Y_{i+1}') \leq \#(S_i)$. In any case we would have $\#(Y_{i+1}) \leq \#(S_{i+1})$.

For each x, let γ_x be the number of distinct u_j's in U_i such that $(\beta(x), u_j)_p > 0$. Then $k + (i+1)p - \gamma_x \geq p$, and S_{i+1}' must contain at least

$$\binom{k + (i+1)p - \gamma_x}{t_x - 1}\binom{p}{1} + \ldots + \binom{k + (i+1)p - \gamma_x}{0}\binom{p}{t_x}$$

quasi-generators of $g(x)$ for each $x \in W_i$, where t_x is the number of steps of the algorithm needed to obtain a minimal quasi-generator of $g(x)$ using u_j's in U_i with $(u_j,x)_p = 0$. It is possible that some x and x' might have the same set of quasi-generators in S'_{i+1}, but by an argument similar to that in Theorem 5.24, one may be able to show that there are fewer such x's than quasi-generators in the set.

If one can obtain $\#(S_i) \geq \#(Y_i)$ for some i, then in order to prove that Carlitz' conjecture is indeed true it will be necessary to show that infinitely many generators of $g(x)$ may be obtained, and that it is impossible to define f in such a way that the coefficients of $g(x)$ will cancel in all of them.

THEOREM 5.26. If x is any element of some set W_i (as defined above), then $x = n + w_1 - t_1 + \ldots + w_m - t_m$, where w_j, $t_j \in S_f$, $1 \leq j \leq m$, and w_j, $t_j \mid_p p + \sum_{i=1}^{k+(i+1)p} u_i$.

PROOF. If $x \in X_i$, then some $Q \in R_i$ is a quasi-generator of $g(x)$.

$$Q = n + u_{i_1} - v_o + \ldots + u_{i_k} \quad (k \geq 1)$$

$$= x + w_1 - v_1 + \ldots + w_r \quad (r \geq 1),$$

where $w_j \in S_f$ $(1 \leq j \leq r)$ and $v_j \in S_f$ $(1 \leq j \leq r-1)$. Hence

$$x = n + u_{i_1} - v_o + \ldots + u_{i_k} - w_r + v_{r-1} - \ldots - w_1,$$

where all u_{i_j}'s, w_j's, v_j's, and v_o are in S_f and are p-factors of

$$p + \sum_{j+1}^{k+(i+1)p} u_j.$$

If $x \in Y_i$ then some $Q \in S_i$ is a quasi-generator of $g(x)$. The first possibility is that there exists $x' \in X_i$ such that

$$Q = x' + u_{i_1} - v + \ldots + u_{i_s} \quad (s \geq 1)$$

$$x = w_1 - v_1 + \ldots + w_r \quad (r \geq 1).$$

In this case there exists $Q' \in R_i$ with Q' a quasi-generator of $g(x')$ and

$$Q' = n + u'_{i_1} - v_o + \ldots + u'_{i_k}$$

$$= x' + w'_1 - v'_1 + \ldots + w'_t \quad (t \geq 1).$$

So

$$x = x' + u_{i_1} - v + \ldots + u_{i_s} - w_r + w_{r-1} - \ldots - w_1$$

$$= n + u'_{i_1} - v_o + \ldots + u'_{i_k} - w'_t + v'_{t-1} - \ldots - w'_1$$

$$+ u_{i_1} - v + \ldots + u_{i_s} - w_r + v_{r-1} - \ldots - w_1,$$

where clearly all u_{i_j}, u'_{i_j}, w_j, w'_j, v_j, v'_j, v, and v_o are elements of S_f and are p-factors of

$$P + \sum_{i=1}^{k+(i+1)p} u_i.$$

If we continue the argument we obtain similar results.

This theorem might in some way help to obtain a bound for $\#(W'_i)$ which depends on i.

THEOREM 5.27. If $S = \{v \in S_f : v + m$ is the LPG of $g(m)$ for some $m \in N\}$ is infinite, then we can choose $u_1 \in U$ with $\delta_p(u_1)$ large enough so that for all m such that $o(g(m)) = 1$ and $g(m)$ appears in $f*g(Q)$ $(Q \in R_i)$ with order 1 substitutions, $\beta(m) \mid_p \beta(Q)$.

PROOF. Let $Q_o = n + u_1 - v_o + \ldots + u_k$,

$$Q_1 = n + u_2 - v_o + \ldots + u_{k+1},$$

$$\vdots$$

$$Q_i = n + u_i - v_o + \ldots + u_{k+i},$$

$$\vdots$$

Suppose that for all i ($i \geq 0$) there is an m_i such that $f*g(Q_i)$ depends on $g(m_i)$ with at most order 1 substitutions, $o(g(m_i)) = 1$, and if $v_i \in S$ with $v_i + m_i$ the LPG of $g(m_i)$, then $(v_i,u_j)_p > 0$, for some $j \geq i$. For some fixed i, let x_1 be such that $x_1 |_p Q_i$, $Q_i - x_1 = w_1 \in S_f$, $o(g(x_1)) = 1$, and $g(x_1)$ depends on $g(m_j)$ with at most order 1 substitutions. If $k > 1$, $x_1 \neq m_i$, since the LPG of $g(x_1)$ is $M_1 = x_1 + v$, $v_1' \leq v_o$. We will not arrive at $g(m_i)$ until we go through at least k - 2 more substitutions in $f*g(M_1)$.

Suppose we find m_i after t_i levels of substitution ($t_i > k - 1$) within $f*g(Q_i)$, where at level r we obtain

$$x_r |_p M_{r-1},$$

$$M_{r-1} - x_r \in S_f$$

M_r is the LPG of $g(x_r)$

$$M_r - x_r = v_r \in S.$$

At each level we have $x_r = a_r + b_r$, $\Delta_p(a_r) < \delta_p(u_i)$, $b_r = x_r - a_r$. For $r \leq k - 1$, $v_r' \leq v_o$, $a_r \leq n$, and $b_r |_p u_i + \ldots + u_{i+k}$.

At some level t', $k - 1 < t' \leq t_i$, we obtain $x_{t'} = a_{t'} + b_{t'}$, with $v_{t'} > a_{t'}, a_{t'} > n$, and from this point a_r and v_r must continue to increase until $\Delta_p(v_t) \geq \delta_p(u_i)$. Moreover, as i increases, t_i increases.

Now the numbers $x_1 = a_1 + b_1$ such that $x_1 |_p Q_i$, $Q_i - x_1 \in S_f$, $o(g(x_1)) = 1$, and $g(x_1)$ depends on $g(m_i)$ with order 1 substitutions, all have the property that $a_1 |_p n$, $b_1 |_p u_i + \ldots + u_{i+k}$. For each r, $o(g(x_r)) = 1 \Longrightarrow o(g(a_r)) = 1$, and $a_r + v_r$ is the LPG of $g(a_r)$ $(r = 1, 2, \ldots)$. Also $x_{r+1} |_p x_r + v_r$ with $x_r + v_r - x_{r+1} \in S_f$ $\Longrightarrow a_{r+1} |_p a_r + v_r$ with $a_r + v_r - a_{r+1} \in S_f$. So $a_{r+1} < a_r$, since v_r is the least p-factor of $a_r + v_r$ that is in S_f. This contradicts the necessity for a_r to increase from $r > t'$.

Hence there exists a positive integer c such that for all $j > c$, if $f*g(Q_j)$ depends on g(m) with at most order 1 substitutions, and if $o(g(m)) = 1$ with $M = v + m$ the LPG of g(m), then we must have $\Delta_p(v) < \delta_p(u_j)$. It is clear that if we choose $u_1 = u_j$ for any $j > c$, we must have $\beta(m) |_p \beta(Q)$ for any $Q \in R_i$ in which g(m) appears.

COROLLARY. If S is infinite, then we can choose $u_1 \in U$ with $\delta_p(u_1)$ large enough so that for all x with $Q \in R_i$ a quasi-generator of g(x), $\beta(x) |_p \beta(Q)$.

Theorem 5.27 tells us that all theorems that have been proven under the assumption that S is finite will also hold for S infinite, for the proper choice of u_1.

Finally, we have a theorem which gives some properties of one kind of singular function.

DEFINITION 5.17. Let $n = \sum_{i=1}^{k} a_i p^{r_i}$ $(0 < a_i < p, r_1 < \ldots < r_k)$. The <u>coefficient k-tuple</u> (<u>coefficient vector</u>) of n is $(a_1, \ldots, a_k)$.

THEOREM 5.28. Let f be a singular function that is not a Carlitz-type nilpotent function. Suppose that S_f contains infinitely many numbers u such that $\omega_p(u) \leq k$ for some fixed $k \in N^*$. Let $V = \{u \in S_f : \omega_p(u) \leq k\}$, and assume that for all $r > 0$ there exists $u \in V$ with $\delta_p(u) > p^r$. Then there is a fixed number t with $1 \leq t \leq k$ such that

i) infinitely many elements u of V satisfy $\omega_p(u) = t$;

ii) there is a fixed t-tuple $v = (a_1, \ldots, a_t)$ $(0 < a_i < p)$ such that infinitely many elements of V have coefficient t-tuple v;

iii) if $V_t = \{u \in V : u = \sum_{i=1}^{t} a_i p^{r_i}$ $(r_1 < \ldots < r_t)\}$, then for any $r > 0$ there exists $u \in V_t$ with $\delta_p(u) > p^r$;

iv) for any $r > 0$ there exists $u \in V_t$ with $\delta_p(u) > r$ and such that u has no proper p-factor in S_f.

PROOF. We construct an infinite sequence $T = \{u_i\}_{i=1}^{\infty}$ of elements of V by letting u_1 be any element of V which has no proper p-factor in S_f and choosing u_{i+1} so that $\delta_p(u_{i+1}) > \Delta_p(u_i)$, i = 1, 2, ... For each u_i we make certain that $\omega_p(u_i)$ is minimal, and if $v_i = (a_{i1}, \ldots, a_{is})$ is the coefficient s-tuple $(1 \leq s \leq k)$ of u_i $(0 < a_{ij} < p)$, we choose u_i with $\sum_{j=1}^{s} a_{ij}$ minimal, i = 1, 2, ...

T is infinite and there are only k possible values for $\omega_p(u_i)$, for $u_i \in T$. Hence there is a fixed t, $1 \leq t \leq k$, such that infinitely many elements u_i of T satisfy $\omega_p(u_i) = t$, and i) is proven.

Let t be the least positive integer such that infinitely many elements of T satisfy $\omega_p(u_i) = t$. There are $(p - 1)^t$ possible

coefficient t-tuples for these numbers. Hence there is at least one fixed t-tuple $(a_1, \ldots, a_t)$ $(0 < a_i < p)$ which corresponds to infinitely many elements of the chosen sequence; so ii) holds.

$V_t = \{u \in T : u = \sum_{i=1}^{t} a_i p^{r_i}, r_1 < \ldots < r_t\}$. Then $V_t \subseteq T$, and by choice of the elements of T, iii) is satisfied.

We chose t to be the least number such that infinitely many elements of T satisfied $\omega_p(u) = t$. If there is more than one t-tuple v such that infinitely many elements of T have v as coefficient t-tuple, then we choose v so that $\sum_{i=1}^{t} a_i$ is minimal. If only a finite number, say c, of the u_i's in V_t have proper p-factors in S_f, then we let $V_t' = v_t - \{u_{i_1}, \ldots, u_{i_c}\}$, where u_{i_j} has a proper p-factor in S_f, $1 \leq j \leq c$. If infinitely many of the elements of V_t have proper p-factors in S_f, we let $W = \{u_j'\}_{u=1}^{\infty}$ be the set of all such numbers. Let q_j be the least p-factor of u_j' that is in S_f, $j = 1, 2, \ldots$. Then $0 < q_j < u_j'$ and $0 < \omega_p(q_j) \leq \omega_p(u_j') = t$. For each $u_i \in T$ we chose u_i so that $\omega_p(u_i)$ was minimal $(i > 1)$. Hence we must have that $\omega_p(q_j) = t$, $j = 1, 2, \ldots$. Since $q_j < u_j'$ for all $u_j' \in W$, we must also have that if $(a_{j1}, \ldots, a_{jt})$ is the coefficient t-tuple of q_j $(j = 1, 2, \ldots)$, then $\sum_{i=1}^{t} a_{ji} < \sum_{i=1}^{t} a_i$. This contradicts the minimality of $\sum_{i=1}^{t} a_i$; and iv) is satisfied.

BIBLIOGRAPHY

BIBLIOGRAPHY

1. L. Carlitz, "Arithmetic functions in an unusual setting," Amer. Math. Monthly, Vol. 73 (1966), 582-590.

2. _____, "Arithmetic functions in an unusual setting, II," Duke Math Journal, Vol. 34 (1967), 757-759.

3. E. D. Cashwell and C. J. Everett, "The ring of number-theoretic functions," Pacific J. Math., Vol. 9 (1959), 975-985.

4. Eckford Cohen, "Arithmetical functions associated with the unitary divisors of an integer," Math. Z., Vol. 74 (1960), 66-80.

5. G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 4th ed., New York: Oxford University Press, 1960.

6. David A. Smith, "Generalized arithmetic function algebras," Lecture Notes in Math., Vol. 251, Berlin: Springer, 1972.

7. R. Vaidyanathaswamy, "The theory of multiplicative arithmetic functions," Trans. Amer. Math. Soc., Vol. 33 (1931), 579-662.

8. Charles R. Wall, Selected Topics in Number Theory, Columbia, S. C.: University of South Carolina Press, 1974.

VITA

Juliana H. Dowell was born in Bradford, Pennsylvania on July 21, 1942. She attended public schools in Laurel, Mississippi. She received her BA (1963) from Mississippi University for Women. After teaching in Mississippi public schools for two years she entered the Graduate School at the University of Tennessee in September, 1965, and completed the M.A. degree in 1967.

After leaving the University of Tennessee in 1969, Ms. Dowell taught at The University of Maryland, Eastern Shore (1969-73), East Carolina University (1973-74), and Martin Technical Institute, Williamston, North Carolina (1975-76). She completed requirements for the Doctor of Philosophy degree with a major in mathematics in March, 1977.

Ms. Dowell is married and the mother of one son.