NUMBER-THEORETIC FUNCTIONS OF TWO VARIABLES

By

GLORIA JANE GAUTIER

Bachelor of Science in Education
Northwestern State College
Alva, Oklahoma
1967

Master of Science
Oklahoma State University
Stillwater, Oklahoma
1970

Submitted to the Faculty of the Graduate College
of the Oklahoma State University
in partial fulfillment of the requirements
for the Degree of
DOCTOR OF EDUCATION
May, 1973

NUMBER-THEORETIC FUNCTIONS OF TWO VARIABLES

Thesis Approved:

Jeanne Agnew
Thesis Adviser

E. K. McLachlan

Vernon Troxel

Robert T. Alciatore

Paul G. Miller

N Durham
Dean of the Graduate College

ACKNOWLEDGMENTS

I would like to express my sincere appreciation to those people who have helped me in the preparation of this dissertation and in all my graduate work at Oklahoma State University. I especially want to thank Dr. Jeanne Agnew, my thesis adviser, for the many helpful suggestions she made in regard to this paper. The time she spent reading the material and working with me personally is greatly appreciated. Her concern for this project made each session a pleasant experience.

A special thanks goes to Dr. E. K. McLachlan for serving as the chairman of my committee and helping me to plan my graduate study. I am also grateful for the time spent in my behalf by the other committee members, Dr. Paul Miller, Dr. Robert Alciatore, and Dr. Vernon Troxel. A word of thanks also goes to Dr. John Jewett for the teaching assistantships I have had the past five years. The experience gained in this capacity has been invaluable.

Another special thanks goes to my many friends in the department who have made the pursuit of this degree much more than just an educational experience. Both in class and out they have been a pleasure to work with, and I value highly the friendships made. A word of thanks also goes to Mary Bonner for her excellent work in typing this thesis and for her willingness to help me as a graduate assistant.

A very sincere word of thanks goes to my family, especially my parents Mr. and Mrs. Howard Gautier, who have provided me with

many words of encouragement during the past five years. Their support and understanding means much more to me than words can possibly say. Without them this degree would not have been a reality.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

The concept of function is basic in all branches of mathematics. In number theory the number-theoretic, or arithmetic, function plays a key role, and the study of such functions motivates many of the topics considered in an elementary number theory course. This paper deals primarily with number-theoretic functions of two variables with special emphasis on functions defined in terms of unitary divisors. As the reader progresses through the material, it becomes evident that in some cases these functions of two variables are simply generalizations of more familiar number-theoretic functions of one variable.

A great many number-theoretic functions, especially those which are multiplicative, are defined by some property related to divisors. The author became interested in functions based on unitary divisors about three years ago, and this initial interest culminated in a master's report [7]. This report gives unitary analogues for τ, φ, σ, and μ along with the unitary counterparts of some of their basic properties. Some of the results of this paper are stated later for future reference. At this point a brief summary of Chapters II through V provides the reader with an overview of the topics studied.

In Chapter II number-theoretic functions of two variables are studied in the context of the familiar "divides" relation. Three particular functions are introduced, and various properties are shown.

One of these functions, Ramanujan's sum, appears again in Chapter III. At this time a class of functions of two variables, the set of even functions modulo r, is considered, and two representations for this class of functions are given. One of these representations is in terms of the Ramanujan sum.

Chapters IV and V are actually the unitary counterparts of Chapters II and III, and their development parallels that of the earlier chapters. After a discussion of some functions of two variables defined in terms of unitary divisors, the paper proceeds with the topic of unitary functions modulo r. These functions comprise another class of functions which is a subset of the class of even functions modulo r. As one might guess, it is possible to find representations for these unitary functions, and one of these representations is based on the unitary analogue of the Ramanujan sum. The applications of number-theoretic functions to specific problems are many and varied. One of the most interesting aspects of this study is the application of these representations to the problem of finding the number of solutions in the unitary context of certain congruences modulo r. Here a formula is derived for the number of solutions, and a characterization is stated which gives conditions under which there are no solutions.

Preliminary Concepts

It is impossible to state all of the results from elementary number theory which are used here. The reader is expected to have a knowledge of the basic concepts covered in any good number theory text, such as, Explorations in Number Theory by Jeanne Agnew [1]. A certain amount of basic information in regard to unitary divisors is

essential. These results are listed here for easy reference. Proofs are not included, but many of the results follow directly from the definition of unitary divisor. In many instances proofs can be found in [7]. Throughout the discussion all integers are positive integers.

Definition 1.1: An integer d is a unitary divisor of an integer r, written $d \| r$, if d is a divisor of r and $(d, r/d) = 1$.

Theorem 1.1: If $a \| b$ and $b \| c$, then $a \| c$.

Theorem 1.2: The unitary divisors of an integer occur in pairs; that is, $d \| r$ if and only if $r/d \| r$.

Theorem 1.3: Let $r = \prod_{i=1}^{m} p_i^{a_i}$ be the canonical representation of r. The unitary divisors d of r are of the form $d = \prod_{i=1}^{m} p_i^{b_i}$ where $b_i = 0$ or $b_i = a_i$.

Theorem 1.4: Let $r = \prod_{i=1}^{m} p_i^{a_i}$ be the canonical representation of r. The number of unitary divisors of r, denoted by $\tau^*(r)$, is $\tau^*(r) = 2^m$.

A modified generalization of the concept of relatively prime is the concept of semiprime. This definition follows after a description of some important notation.

Definition 1.2: Let a and b be integers where $b > 0$. Then $(a, b)_*$ is the greatest divisor of a which is a unitary divisor of b.

Definition 1.3: If $(a, b)_* = 1$, a is said to be semiprime to b.

Theorem 1.5: Let p be any prime. If $a < b$, $(p^a, p^b)_* = 1$. If $a \geq b$, $(p^a, p^b)_* = p^b$.

Theorem 1.6: For integers n and r, $((n, r), r)_* = (n, r)_*$.

Theorem 1.7: Let d be a unitary divisor of r. Then $(r/d, r)_* = 1$ if and only if $r = d$.

Theorem 1.8: A divisor d of n is a unitary divisor of r if and only if $d \| (n, r)_*$. If $d \| (n, r)_*$ and $(n/d, r/d)_* = 1$, then $d = (n, r)_*$.

Theorem 1.9: If $(a, b)_* = d$, $(a/d, b/d)_* = 1$.

Theorem 1.10: If $a \equiv b \pmod{r}$, $(a, r)_* = (b, r)_*$.

Theorem 1.11: For $(n_1, n_2) = 1$, $(x_2 n_1 + x_1 n_2, n_1 n_2)_* = 1$ if and only if $(x_1, n_1)_* = 1$ and $(x_2, n_2)_* = 1$.

Theorem 1.12: Let $(s, t) = 1$. If $(x, s)_* = 1$ and $(x, t)_* = 1$, then $(x, st)_* = 1$.

Theorem 1.13: If $r = \prod_{p \mid r} p^a$ is the canonical representation of r, $(n, r)_* = \prod_{p^a \mid n} p^a$ and $r/(n, r)_* = \prod_{p^a \nmid n} p^a$.

Theorem 1.14: For integers n and r, $d \| r/(n, r)_*$ if and only if $d \| r$ and $(n, d)_* = 1$.

A means of combining number-theoretic functions in the unitary context is given by the unitary convolution. This product and its properties are used extensively throughout the paper.

Definition 1.4: Let g and h be number-theoretic functions. The function $f(r) = \sum_{d \| r} g(d)\, h(r/d)$ is defined to be the unitary convolution of g and h, written $(g * h)(r)$.

Theorem 1.15: If f and g are multiplicative functions, $f * g$ is also multiplicative.

The next theorem is actually a special case of the preceding one where g is the identity function.

Theorem 1.16: If f is multiplicative, $F(r) = \sum_{d \| r} f(d)$ is also multiplicative.

Theorem 1.17: If f is multiplicative and $r = \prod_{p|r} p^a$ is the canonical representation of r, $\sum_{d \| r} f(d) = \prod_{p|r} (1 + f(p^a))$, where the product is defined to be 1 if $r = 1$.

Theorem 1.18: If f is multiplicative and $r = \prod_{p|r} p^a$ is the canonical representation of r, $\sum_{\substack{d \| r \\ (n,d)_* = 1}} f(d) = \prod_{p^a \nmid n} (1 + f(p^a))$.

The unitary analogue of a residue system modulo r is the semi-reduced residue system modulo r. Its definition and some related properties follow.

Definition 1.5: The set of integers semiprime to r and contained in a residue system modulo r is defined to be a semi-reduced residue system modulo r.

Theorem 1.19: If x ranges over a semi-reduced residue system modulo r and $(a, r) = 1$, the values ax also range over a semi-reduced residue system modulo r.

Theorem 1.20: The integers dx, where d ranges over the unitary divisors of r, and for each d, x ranges over a

semi-reduced residue system modulo r/d constitute a residue system modulo r.

Once the idea of a semi-reduced residue system has been introduced, a natural question to consider is the unitary analogue of the Euler φ-function. This analogue is defined in the following.

Definition 1.6: The function $\varphi^*(r)$ is defined to be the number of positive integers less than or equal to r and semiprime to r.

The unitary analogue of the Möbius function μ is given in Definition 1.7. The results following this definition form a sequence of steps which could be used to derive the formula for φ^* given in Theorem 1.28.

Definition 1.7: The unitary analogue of the Möbius function is denoted by μ^* and is defined to be $\mu^*(r) = (-1)^{h(r)}$ where $h(r)$ is the number of distinct prime divisors of r.

Theorem 1.21: The function μ^* is multiplicative.

Theorem 1.22: $\sum_{d \| r} \mu^*(d) = \begin{cases} 1 & \text{if } r = 1 \\ 0 & \text{if } r > 1 . \end{cases}$

Theorem 1.23: (The Unitary Analogue of the Möbius Inversion Formula) If $f(r)$ is any number-theoretic function and $F(r) = \sum_{d \| r} f(d)$, then $f(r) = \sum_{d \| r} \mu^*(d) F(r/d)$.

Theorem 1.24: If F is multiplicative and $F(r) = \sum_{d \| r} f(d)$, f is multiplicative.

Theorem 1.25: For an integer r, $r = \sum_{d \| r} \varphi^*(d)$.

Theorem 1.26: The function φ^* is multiplicative.

Theorem 1.27: For an integer r, $\varphi^*(r) = r \sum_{d \| r} \mu^*(d)/d$.

Theorem 1.28: Let $r = \prod_{p|r} p^a$ be the canonical representation of r where $r > 1$. Then $\varphi^*(r) = r \prod_{p|r} (1 - 1/p^a) = \prod_{p|r} (p^a - 1)$.

Theorem 1.29: If $r = \prod_{p|r} p^a$ is the canonical representation of r, $\varphi^*(r/(n, r)_*) = \prod_{p^a \| n} (p^a - 1)$.

Theorem 1.30: $\sum_{\substack{d \| r \\ (n, d)_* = 1}} 1/\varphi^*(d) = r\, \varphi^*((n, r)_*)/(n, r)_* \varphi^*(r)$.

The last basic number-theoretic function for which it is necessary to define a unitary analogue is σ.

Definition 1.8: The sum of the unitary divisors of a positive integer r is $\sigma^*(r)$.

Theorem 1.31: The function $\sigma^*(r)$ is multiplicative.

Theorem 1.32: If $r > 1$ and $\prod_{p|r} p^a$ is the canonical representation of r, $\sigma^*(r) = \prod_{p|r} (1 + p^a)$.

Generalization of the Unitary Divisor to the k-ary Divisor

After one has studied the concept of unitary divisor and seen it in action in various number-theoretic problems, it is natural to look for a generalization of this concept. The remainder of this chapter considers what is appropriately termed the k-ary divisor. Actually, two types of divisors are considered, k-ary and k-free. Their study

is combined here as both involve kth powers of integers, and in certain instances they have common properties.

The study of this generalization was inspired by a paper of Suryanarayana [13] of India. He is responsible for the generalizations of τ to the number of k-ary and k-free divisors of an integer. These generalizations then led to formulas for the sum of the k-ary and the k-free divisors of an integer. The discussion begins with two definitions, the first of which describes some notation.

Definition 1.9: If k is a fixed positive integer, and a and b are integers, not both zero, then $(a,b)_k$ is the greatest divisor of a and b which is a kth power.

Definition 1.10: A divisor d of r is said to be a k-ary divisor of r if $d\delta = r$ and $(d,\delta)_k = 1$.

If $k = 1$ in the preceding definition, d is just a unitary divisor of r. For $k = 2$, d is called a binary divisor of r, and for $k = 3$, d is called a ternary divisor of r. The following example provides some motivation for Theorem 1.33.

Example 1.1: Consider 16 as a divisor of 64. Since $(16,4) \neq 1$, 16 is not a unitary divisor of 64. Since $(16,4)_2 = 2^2$, 16 is not a binary divisor of 64. However, $(16,4)_3 = 1$ implies that 16 is a ternary divisor of 64. In fact, for any $k \geq 3$, $(16,4)_k = 1$ so that 16 is a k-ary divisor of 64 for $k \geq 3$.

Theorem 1.33: If d is a k-ary divisor of r, d is a (k+1)-ary divisor of r. If d is not a k-ary divisor of r, d is not a (k-1)-ary divisor of r.

Proof: If d is a k-ary divisor of r, $d\delta = r$ and $(d, \delta)_k = 1$. Since the highest kth power divisor of d and δ is 1, no (k+1)-power can divide both d and δ. Hence, $(d, \delta)_{k+1} = 1$, and d is a (k+1)-ary divisor of r. The second statement is straightforward from the first. Δ

A natural extension of the previous theorem is given in the following corollary. Its proof is direct from the theorem.

Corollary 1.33.1: If d is a k-ary divisor of r, then for any $q \geq k$, d is a q-ary divisor of r. If k is an integer greater than 1 for which d is not a k-ary divisor of r, then for any $q \leq k$, d is not a q-ary divisor of r.

A topic for consideration along with the study of k-ary divisors is that of k-free divisors. The following definition describes this divisor.

Definition 1.11: An integer $n > 0$ is said to be k-free if n is not divisible by the kth power of any integer greater than 1.

Example 1.2: If $n = 42$, then n is k-free since $42 = 2 \cdot 3 \cdot 7$ and hence is not divisible by the kth power of any integer greater than 1. On the other hand if $n = 56$, then $56 = 2^3 \cdot 7$ implies n is not k-free for $k = 2$ or 3.

The next definition provides some necessary notation.

Definition 1.12: The number of k-ary divisors of r and the sum of the k-ary divisors of r are denoted by $\tau_k^*(r)$ and $\sigma_k^*(r)$ respectively. The number of k-free divisors of r and the sum of the

k-free divisors of r are denoted by $\tau_{(k)}(r)$ and $\sigma_{(k)}(r)$ respectively.

It is clear from this definition that $\tau_k^*(1) = \tau_{(k)}(1) = 1$ and $\sigma_k^*(1) = \sigma_{(k)}(1) = 1$. A more general result relating τ_k^* and $\tau_{(k)}$ is given in Theorem 1.34.

Theorem 1.34: If $r = \prod_{i=1}^{m} p_i^{a_i}$ is the canonical representation of r, then $\tau_1^*(r) = \tau_{(2)}(r) = 2^m$.

Proof: On the basis of the given notation, $\tau_1^*(r)$ is the number of unitary divisors of r. Hence, $\tau_1^*(r) = 2^m$ by Theorem 1.4. Now $\tau_{(2)}(r)$ is the number of square-free divisors of r. To count these square-free divisors it is sufficient to count the number of possible subsets formed from the set $A = \{p_1, \ldots, p_m\}$ since the product of those elements in each subset is a square-free divisor of r. But since there are 2^m possible subsets, $\tau_{(2)}(r) = 2^m$. . Δ

Before deriving formulas for the number and sum of the k-free divisors of an integer, it is worthwhile to look at an example showing how to locate these divisors. Let $r = \prod_{p|r} p^a$ denote the canonical representation of r.

Example 1.3: In terms of its canonical representation $r = 360 = 2^3 \cdot 3^2 \cdot 5$. In looking for k-free divisors it is necessary to discard all terms p^k, p^{k+1}, p^{k+2}, ... For $r = 360$, the product $(2^0 + 2^1)(3^0 + 3^1)(5^0 + 5^1)$ is such that each term in its expansion is a square-free divisor of 360, and each square-free divisor of 360 is a term in the expansion. The product $(2^0 + 2^1 + 2^2)(3^0 + 3^1 + 3^2)(5^0 + 5^1)$

is such that each term in its expansion is a cube-free divisor of 360, and each cube-free divisor of 360 is a term in the expansion.

This example leads to a general method for locating the k-free divisors of $r = \prod_{p|r} p^a$. When $a < k$, form a product with factors $(p^0 + p^1 + \ldots + p^a)$. When $a \geq k$, form a product with factors $(p^0 + p^1 + \ldots + p^{k-1})$. The product

$$\prod_{a<k} (1 + p + p^2 + \ldots + p^a) \cdot \prod_{a\geq k} (1 + p + p^2 + \ldots + p^{k-1})$$

is such that each term in its expansion is a k-free divisor of r, and each k-free divisor of r is a term in the expansion.

Theorem 1.35: If $k \geq 2$ and $r = \prod_{p|r} p^a$ is the canonical representation of r, then

$$\tau_{(k)}(r) = \prod_{a<k} (a + 1) \cdot \prod_{a\geq k} (k).$$

Proof: Consider the product of the previous example. The theorem follows immediately from the number of terms in each factor. Δ

It is clear from this formula that if $a<k$ for every prime in the canonical representation of r, $\tau_{(k)}(r) = \tau(r)$. The fact that $\tau_{(k)}(r)$ is a multiplicative function of r can be shown rather easily by use of this formula. This result is noted here for future reference.

Corollary 1.35.1: The function $\tau_{(k)}(r)$ is a multiplicative function of r.

Example 1.4: Let $r = 360 = 2^3 \cdot 3^2 \cdot 5$. For $k = 2$, 5 is the only prime with $a < 2$. So $\tau_{(2)}(360) = (1+1)\cdot 2 \cdot 2 = 8$. For $k = 3$, both 3 and 5 satisfy $a < 3$. Hence, $\tau_{(3)}(360) = (2+1)(1+1)\cdot 3 = 18$. For $k = 4$, all primes in the representation satisfy $a < 4$. Hence, $\tau_{(4)}(360) = \tau(360) = (3+1)(2+1)(1+1) = 24$. Furthermore, for any $k \geq 4$, $\tau_{(k)}(360) = \tau(360) = 24$.

The product used earlier to find $\tau_{(k)}(r)$ in terms of the canonical representation of r can also be used to find $\sigma_{(k)}(r)$.

Theorem 1.36: If $k \geq 2$ and $r = \prod_{p|r} p^a$ is the canonical representation of r,

$$\sigma_{(k)}(r) = \prod_{a<k} (p^{a+1} - 1)/(p - 1) \cdot \prod_{a \geq k} (p^k - 1)/(p - 1).$$

Proof: Again the proof is immediate from the product of Example 1.3. △

If $a < k$ for all primes in the canonical representation of r, it is easy to see that $\sigma_{(k)}(r)$ reduces to $\sigma(r)$. This formula also yields the fact that $\sigma_{(k)}(r)$ is a multiplicative function of r. These results parallel those discovered for $\tau_{(k)}(r)$.

Corollary 1.36.1: The function $\sigma_{(k)}(r)$ is a multiplicative function of r.

Besides the formula for $\tau_{(k)}(r)$ based on the canonical representation of r, it is possible to write $\tau_{(k)}(r)$ in terms of a special convolution of μ and τ. Two lemmas are essential to the derivation of this second representation. Lemma 1.37 is a kth-power analogue

of a result of elementary number theory, and its proof is immediate. Lemma 1.38 shows an important property of this special convolution.

Lemma 1.37: Let $(r, s) = 1$. If d_1^k and d_2^k are kth power divisors of r and s respectively, then $(d_1 d_2)^k$ is a kth power divisor of rs, $(d_1, d_2) = 1$, and $(r/d_1^k, s/d_2^k) = 1$. Conversely, every kth power divisor of rs can be expressed as $(d_1 d_2)^k$ where $d_1^k | r$, $d_2^k | s$, $(d_1, d_2) = 1$, and $(r/d_1^k, s/d_2^k) = 1$.

Throughout this paper various convolutions are encountered. In most instances a particular problem requires a particular convolution. In working with kth power divisors it is necessary to use a convolution involving kth powers. Such a convolution is defined in Lemma 1.38, and it is seen that this convolution preserves the multiplicative property. It should also be noted that this convolution is only a special case of the ordinary convolution with the sum being taken over the kth power divisors of r rather than the divisors of r.

Lemma 1.38: If g and h are multiplicative, $f_k(r) = \sum_{d^k | r} g(d)h(r/d^k)$ is a multiplicative function of r.

Proof: Let $r = st$ where $(s, t) = 1$. By the definition of f_k, $f_k(st) = \sum_{d^k | st} g(d)h(st/d^k)$. By the previous lemma,

$$f_k(st) = \sum_{\substack{d_1^k | s \\ d_2^k | t}} g(d_1 d_2)h(st/d_1^k d_2^k).$$

Since g and h are multiplicative,

$$f_k(st) = \sum_{d_1^k | s} g(d_1) h(s/d_1^k) \sum_{d_2^k | t} g(d_2) h(t/d_2^k) = f_k(s) f_k(t).$$

Hence, f_k is multiplicative. Δ

With these preliminaries out of the way Theorem 1.39 gives a formula for $\tau_{(k)}(r)$ in terms of μ and τ.

Theorem 1.39: For $k \geq 2$, $\tau_{(k)}(r) = \sum_{d^k | r} \mu(d)\, \tau(r/d^k)$.

Proof: By the previous lemma the right hand side of the desired equality is multiplicative. Since $\tau_{(k)}(r)$ is also multiplicative, it is sufficient to show the formula for $r = p^a$ where p is a prime. For $a < k$,

$$\sum_{d^k | p^a} \mu(d)\, \tau(p^a/d^k) = \mu(1)\, \tau(p^a) = a + 1.$$

Also, $\tau_{(k)}(p^a) = a + 1$ when $a < k$. For $a \geq k$,

$$\begin{aligned} \sum_{d^k | p^a} \mu(d)\, \tau(p^a/d^k) &= \mu(1)\, \tau(p^a) + \mu(p)\, \tau(p^{a-k}) \\ &= (a+1) - (a-k+1) \\ &= k. \end{aligned}$$

For $a \geq k$, $\tau_{(k)}(p^a) = k$, and the theorem follows. Δ

The last big topic of this chapter is the derivation of formulas for $\tau_k^*(r)$ and $\sigma_k^*(r)$. Unlike the procedure for $\tau_{(k)}(r)$ and $\sigma_{(k)}(r)$, $\tau_k^*(r)$ and $\sigma_k^*(r)$ are shown first to be multiplicative, and the formulas follow as consequences of this multiplicative nature. Lemma 1.40 helps to prove that these functions are multiplicative.

Lemma 1.40: Let $(r, s) = 1$. The integer d_1 is a k-ary divisor of r and d_2 is a k-ary divisor of s if and only if $d_1 d_2$ is a k-ary divisor of rs.

Proof: Let d_1 be a k-ary divisor of r and d_2 a k-ary divisor of s. Then $d_1 | r$, $(d_1, r/d_1)_k = 1$, $d_2 | s$, and $(d_2, s/d_2)_k = 1$. It is clear that $d_1 d_2 | rs$. It remains to be shown that $(d_1 d_2, rs/d_1 d_2)_k = 1$. Suppose that $(d_1 d_2, rs/d_1 d_2)_k = x^k > 1$. Then there exists a prime p such that $p^k | d_1 d_2$ and $p^k | rs/d_1 d_2$. Since $(d_1, d_2) = 1$, either $p^k | d_1$ or $p^k | d_2$. Without loss of generality suppose $p^k | d_1$. Since $(r, s) = 1$, it follows that $(r/d_1, s/d_2) = 1$. So if $p^k | rs/d_1 d_2$, either $p^k | r/d_1$ or $p^k | s/d_2$. Since $p^k | d_1$ and $(r, s) = 1$, it follows that $p^k | r/d_1$. So $p^k | d_1$ and $p^k | r/d_1$, a contradiction to $(d_1, r/d_1)_k = 1$. Thus, $(d_1 d_2, rs/d_1 d_2)_k = 1$, and $d_1 d_2$ is a k-ary divisor of rs.

The converse is proved similarly. △

Theorem 1.41: The functions $\tau_k^*(r)$ and $\sigma_k^*(r)$ are multiplicative functions of r.

Proof: Let $r = st$ where $(s, t) = 1$. By the previous lemma d_1 is a k-ary divisor of s and d_2 is a k-ary divisor of t if and only if $d_1 d_2$ is a k-ary divisor of st. Hence, $(d_1, s/d_1)_k = (d_2, t/d_2)_k = 1$ if and only if $(d_1 d_2, st/d_1 d_2)_k = 1$. Thus, $\tau_k^*(s)\, \tau_k^*(t) = \tau_k^*(st)$ and $\sigma_k^*(s)\, \sigma_k^*(t) = \sigma_k^*(st)$. △

Suppose that $r = p^{10}$ where p is a prime, and suppose that the number of 3-ary divisors of r is to be determined. It is necessary to ascertain which numbers p^t satisfy $(p^t, p^{10-t})_3 = 1$. It is easy to

see that for $t = 0, 1, 2, 8, 9$, and 10, the condition holds. However, for $t = 3, 4, 5, 6$, and 7, $(p^t, p^{10-t})_3 = p^3$. So for $3 \leq t \leq 7$, p^t is not a k-ary divisor of p^{10}. These are the values of t which satisfy $k \leq t \leq 10 - k$ and hence satisfy $10 \geq 2k$. Theorem 1.42 pinpoints the k-ary divisors of a prime power.

Theorem 1.42: If $a < 2k$, any divisor of p^a is a k-ary divisor of p^a. If $a \geq 2k$, for any t such that $k \leq t \leq a - k$, p^t is not a k-ary divisor of p^a.

Proof: Suppose that $a < 2k$ and $d \mid p^a$. Then $d = p^b$ where $b \leq a$. It must be shown that $(p^b, p^{a-b})_k = 1$. If $(p^b, p^{a-b})_k = x > 1$, x must be the kth power of p. Hence, $p^k \mid p^b$ and $p^k \mid p^{a-b}$ so that $p^{2k} \mid p^a$. This implies $a \geq 2k$, a contradiction. So if $a < 2k$, any divisor of p^a is a k-ary divisor of p^a.

If $a \geq 2k$, then $k \leq a - k$. Let t be any integer such that $k \leq t \leq a - k$. For any of these values of t, $(p^t, p^{a-t})_k = p^k$, and p^t is not a k-ary divisor of p^a. Δ

Theorem 1.43: If $r = \prod_{p \mid r} p^a$ is the canonical representation of r, $\tau_k^*(r) = \prod_{a<2k} (a+1) \cdot \prod_{a \geq 2k} (2k)$.

Proof: Since $\tau_k^*(r)$ is multiplicative, the formula can be determined from $\tau_k^*(p^a)$ where $a < 2k$ and where $a \geq 2k$. If $a < 2k$, any divisor of p^a is a k-ary divisor of p^a. Hence, $\tau_k^*(p^a) = \tau(p^a) = a + 1$. If $a \geq 2k$, for any t such that $k \leq t \leq a - k$, p^t is not a k-ary divisor of p^a. There are $(a - k) - k + 1$ of these values of t. So for $a \geq 2k$, $\tau_k^*(p^a) = (a+1) - [(a - k) - k + 1] = 2k$. Therefore,

$$\tau_k^*(r) = \prod_{a<2k} (a+1) \cdot \prod_{a\geq 2k} (2k). \qquad \Delta$$

An immediate result of the previous theorem is that if $a < 2k$ for all values of a, τ_k^* reduces to the ordinary τ function. This basic formula also shows how the number of k-ary divisors can be expressed as a particular number of k-free divisors.

Corollary 1.43.1: $\tau_k^*(r) = \tau_{(2k)}(r)$.

Proof: From Theorem 1.35, $\tau_{(2k)}(r) = \prod_{a<2k} (a+1) \cdot \prod_{a\geq 2k} (2k)$. But this is just $\tau_k^*(r)$ from Theorem 1.43. Hence, $\tau_k^*(r) = \tau_{(2k)}(r)$. Δ

Example 1.5: Again take $r = 360 = 2^3 \cdot 3^2 \cdot 5$. To find the number of unitary divisors by use of this formula, note that 5 is the only prime for which $a < 2$. Hence, $\tau_1^*(360) = (1+1)\cdot 2 \cdot 2 = 8$. The corollary can be used to find the number of binary divisors since for each prime, $a < 2k = 4$. So $\tau_2^*(360) = (3+1)(2+1)(1+1) = 24$. In fact $\tau_k^*(360) = 24$ for every $k \geq 2$.

The multiplicative nature of $\sigma_k^*(r)$ and the result of Theorem 1.42 which points out the k-ary divisors of a prime power motivate the derivation of the formula for $\sigma_k^*(r)$.

Theorem 1.44: Let $k \geq 2$ and $r = \prod_{p|r} p^a$ be the canonical representation of r. Then

$$\sigma_k^*(r) = \prod_{a<2k} (p^{a+1} - 1)/(p-1) \cdot \prod_{a\geq 2k} (1 + p^{a-k+1}) \cdot (p^k - 1)/(p-1),$$

Proof: If $a < 2k$, any divisor of p^a is a k-ary divisor of p^a. So $\sigma_k^*(p^a) = 1 + p + p^2 + \ldots + p^a = \sigma(p^a) = (p^{a+1} - 1)/(p - 1)$. If $a \geq 2k$, p^t is not a k-ary divisor of p^a for any integer t satisfying $k \leq t \leq a - k$. Hence,

$$\begin{aligned}\sigma_k^*(p^a) &= (1 + p + \ldots + p^{k-1}) + (p^{a-k+1} + p^{a-k+2} + \ldots + p^a) \\ &= (1 + p + \ldots + p^{k-1}) + p^{a-k+1}(1 + p + \ldots + p^{k-1}) \\ &= (1 + p + \ldots + p^{k-1})(1 + p^{a-k+1}) \\ &= \frac{p^k - 1}{p - 1} \cdot (1 + p^{a-k+1}) .\end{aligned}$$

Upon multiplying these two results,

$$\sigma_k^*(r) = \prod_{a<2k} (p^{a+1} - 1)/(p - 1) \cdot \prod_{a\geq 2k} (1 + p^{a-k+1}) \cdot (p^k - 1)/(p - 1). \quad \Delta$$

It is immediate that $\sigma_k^*(r)$ reduces to the ordinary σ function when $a < 2k$ for all primes p in the canonical representation of r.

Example 1.6: This last example shows some calculations made with the formula of Theorem 1.44. In order to make the problem interesting, let $r = 2^8 \cdot 3^6 \cdot 5^2$ and find the sum of the binary divisors of r. Since $k = 2$, $a < 2k = 4$ for $p = 5$. Thus,

$$\begin{aligned}\sigma_2^*(r) &= \left(\frac{5^3 - 1}{5 - 1}\right)\left(1 + 2^{8-2+1}\right)\left(\frac{2^2 - 1}{2 - 1}\right)\left(1 + 3^{6-2+1}\right)\left(\frac{3^2 - 1}{3 - 1}\right) \\ &= 11,709,072 .\end{aligned}$$

To find the sum of the 4-ary divisors, note that $a < 2k = 8$ for $p = 5$

and $p = 3$. Hence,

$$\sigma_4^*(r) = \left(\frac{5^3 - 1}{5 - 1}\right)\left(\frac{3^7 - 1}{3 - 1}\right)\left(1 + 2^{8-4+1}\right)\left(\frac{2^4 - 1}{2 - 1}\right)$$

$$= 16,772,085 .$$

The sum of the 5-ary divisors is just $\sigma(r)$ since $a < 2k = 10$ for all the primes represented.

In the next chapter the reader is introduced to the main consideration of this paper, number-theoretic functions of two variables. The first functions of this type which are studied are defined in terms of the ordinary divides relation. Later on, some unitary analogues of these same functions are also encountered. In either situation an interesting topic to pursue further is the k-ary generalizations of these functions of two variables. This topic is not considered in this paper.

CHAPTER II

FUNCTIONS OF TWO VARIABLES

This is the first of four chapters which consider number-theoretic functions of two variables. The three functions studied here are interesting in their own right and also provide new ways of obtaining some of the standard functions of one variable encountered in elementary number theory. The first of these functions, the Nagell totient function, is a generalization of Euler's φ-function. The other two are closely related. One is an exponential type function, and the other, Ramanujan's sum, is a special sum of these exponential functions. They provide a basis for the discussion of even functions modulo r found in the next chapter. Later on, the unitary analogues of Nagell's function and Ramanujan's sum are also considered.

The Nagell Totient Function

The discussion begins with the definition of Nagell's function and two examples which show its use.

Definition 2.1: Let n be a nonnegative integer and r a positive integer. The Nagell totient function, denoted by $\theta(n, r)$, is defined to be the number of integers x such that

(i) $1 \leq x \leq r$

(ii) $(x, r) = (n - x, r) = 1$.

Example 2.1: As an example, if $n = 16$ and $r = 12$, then x is such that $1 \leq x \leq 12$. However, the values of $2, 3, 4, 6, 8, 9, 10$, and 12 for x do not satisfy $(x, 12) = 1$. For $x = 1$ or $x = 7$, $(x, 12) = 1$. But since $(16 - x, 12) = 3$ in both instances, these values of x must not be counted. This leaves only $x = 5$ and $x = 11$, both of which do satisfy (i) and (ii). Hence, $\theta(16, 12) = 2$.

Example 2.2: For a second example suppose that $n = r = 12$. As before, $x = 2, 3, 4, 6, 8, 9, 10$, and 12 must be omitted since $(x, 12) \neq 1$. For $x = 1, 5, 7$, or 11 both $(x, 12) = 1$ and $(12 - x, 12) = 1$. Hence, $\theta(12, 12) = 4$. Note that this is precisely the value of $\varphi(12)$. The following theorem shows that if $n = r$, then $\theta(n, r) = \varphi(r)$, the Euler totient function.

Theorem 2.1: If $n = r$, then $\theta(n, r) = \varphi(r)$.

Proof: The condition $(x, r) = 1$ implies $(r - x, r) = 1$. Hence, $\theta(r, r) = \varphi(r)$. △

Other properties concerning the Nagell totient function could be considered. No doubt some of these may have already occurred to the reader. However, this function is considered here only to introduce the topic of functions of two variables, and further consideration is saved for its unitary analogue. Attention is now focused on the other two functions mentioned at the beginning of this chapter.

The e-Function

To set the stage for the definition of the exponential type function, let r be a positive integer and let F be a field of characteristic zero

containing the rth roots of unity.

Definition 2.2: Let z and n be integers. The e-function is defined by $e_z(n) = e(zn, r) = e^{\frac{2\pi izn}{r}}$.

The preferred notation for this function is $e(zn, r)$ since it is easier to write than the last expression and clearer in meaning possibly than the first.

The first theorem concerning the e-function cites some of its properties which facilitate the work to follow. Since the first four properties follow readily from the algebraic properties of the integers and the laws of exponents, their proofs are omitted.

Theorem 2.2: The following properties hold for the e-function:

(i) $e(zn, r) = e(nz, r)$.

(ii) $e(z(n+m), r) = e(zn, r)\,e(zm, r)$.

(iii) $e((z+z')n, r) = e(zn, r)\,e(z'n, r)$.

(iv) $e(zn, r) = (e(z, r))^n$.

(v) The e-functions are the rth roots of unity.

(vi) For all n, $e(zn, r) = e(z'n, r)$ if and only if $z \equiv z' \pmod r$.

Proof of (v): In its exponential form $(e(zn, r))^r = e^{2\pi izn} = 1$. Hence, the e-functions are only the rth roots of unity.

Proof of (vi): If $e(zn, r) = e(z'n, r)$, the definition of the e-function implies that $z = z' + kr$ and hence $z \equiv z' \pmod r$.

Now if $z \equiv z' \pmod r$, then $r \mid z - z'$. Thus, $e((z - z')n, r) = 1$ and $e(zn, r) = e(z'n, r)$. △

The next theorem shows what happens when the functions $e(zn, r)$ are summed over the integers n in a complete residue system modulo r. Important to this proof is the fact that $e(zn, r) = (e(z, r))^n$.

Theorem 2.3: $\sum_{n(\mathrm{mod}\, r)} e(zn, r) = \begin{cases} r & \text{if } z \equiv 0 \,(\mathrm{mod}\, r) \\ 0 & \text{if } z \not\equiv 0 \,(\mathrm{mod}\, r) \end{cases}$, where the summation is over the integers n in a complete residue system modulo r.

Proof: If $z \equiv 0 \,(\mathrm{mod}\, r)$, then $r \mid z$ and $e(zn, r) = 1$. Hence, $\sum_{n(\mathrm{mod}\, r)} e(zn, r) = r$. On the other hand suppose $z \not\equiv 0 \,(\mathrm{mod}\, r)$. Then since $e(zn, r) = (e(z, r))^n$,

$$\sum_{n(\mathrm{mod}\, r)} e(zn, r) = \sum_{n=0}^{r-1} (e(z, r))^n = \frac{(e(z, r))^r - 1}{e(z, r) - 1} .$$

But since $(e(z, r))^r = 1$, the sum in this case is 0. Δ

Several different types of sums play important roles in the theory of numbers. One of the more common of these is the convolution product. Many recent elementary number theory texts devote a chapter to this topic. A modification of this product which is suitable in the unitary context is the unitary convolution considered in [7]. Both of these are related to the multiplication of Dirichlet series and are sometimes called Dirichlet products. Another type of product suggested by the product of power series is the Cauchy product. Of these products it is the Cauchy product which provides the necessary machinery to work with sums of products of the e-function.

Definition 2.3: If f and g are arithmetic functions for which $f(n) = f(m)$ and $g(n) = g(m)$ when $m \equiv n \,(\mathrm{mod}\, r)$, then the Cauchy

product h of f and g is defined by

$$h(n) = f \circ g(n) = \sum_{n \equiv a+b \pmod r} f(a)\, g(b)$$

where a and b are chosen from a complete residue system modulo r and $n \equiv a+b \pmod r$.

An alternate form for this product is often used. Since $n \equiv a+b \pmod r$, then $b \equiv n-a \pmod r$, and

$$\sum_{n \equiv a+b \pmod r} f(a)\, g(b) = \sum_{a \pmod r} f(a)\, g(n-a).$$

The theorem which follows gives a formula for the Cauchy product of two e-functions. Essential to the proof of this result are the basic properties of the e-function and the summation evaluated in Theorem 2.3.

Theorem 2.4: If a and b range over a complete residue system modulo r, the Cauchy product

$$e(zn, r) \circ e(z'n, r) = \sum_{n \equiv a+b \pmod r} e(za, r)\, e(z'b, r)$$

$$= \begin{cases} r \cdot e(zn, r) & \text{if } z \equiv z' \pmod r \\ 0 & \text{if } z \not\equiv z' \pmod r \end{cases}.$$

Proof: From the alternate form for the Cauchy product,

$$e(zn, r) \circ e(z'n, r) = \sum_{a \pmod r} e(za, r)\, e(z'(n-a), r).$$

The properties of the e-function imply that $e(za, r)\, e(z'(n-a), r) = e(z'n, r)\, e((z-z')a, r)$. But since $e(z'n, r)$ is

independent of the index of summation, this last sum is just $e(z'n, r) \sum_{a(\mathrm{mod}\, r)} e((z - z')a, r)$. The result is now immediate since

$$\sum_{a(\mathrm{mod}\, r)} e((z - z')a, r) = \begin{cases} r & \text{if } z - z' \equiv 0 \,(\mathrm{mod}\, r) \\ 0 & \text{if } z - z' \not\equiv 0 \,(\mathrm{mod}\, r) \end{cases} . \qquad \Delta$$

The next theorem shows that the set of functions $e(zn, r)$ for $z = 0, 1, \ldots, r - 1$ is linearly independent over the field F. Although this proof is based on the standard procedure for showing a set to be linearly independent, it does require the calculation of a Cauchy product of e-functions and thus makes use of the formula of the previous theorem.

Theorem 2.5: The functions $e(zn, r)$ for $z = 0, 1, \ldots, r - 1$ are linearly independent over F.

Proof: Let $g(n) = \sum_{z=0}^{r-1} a_z e(zn, r) = 0$ where a_z is in F. Also, let $e(z'n, r)$ be one of the functions under consideration where z' is fixed. From the definition of $g(n)$,

$$g(n) \circ e(z'n, r) = \left(\sum_{z=0}^{r-1} a_z e(zn, r) \right) \circ e(z'n, r) .$$

Since the Cauchy product distributes over sums [9],

$$g(n) \circ e(z'n, r) = \sum_{z=0}^{r-1} a_z e(zn, r) \circ e(z'n, r) .$$

But from the previous theorem $e(zn, r) \circ e(z'n, r) = r \cdot e(z'n, r)$ if $z \equiv z' \,(\mathrm{mod}\, r)$. Hence, $g(n) \circ e(z'n, r) = a_{z'} r \cdot e(z'n, r) = 0$. But

since r is a positive integer and $e(z'n, r) \neq 0$, then $a_{z'} = 0$. Since z' was a fixed yet arbitrary choice for z, then $a_z = 0$ for $z = 0, 1, \ldots, r-1$, and the functions $e(zn, r)$ are linearly independent over F. Δ

A generalized Cauchy product of e-functions in which the second variables are replaced by two divisors of r is evaluated in Theorem 2.7. The following lemma allows this product to be expressed in terms of these divisors rather than by a congruence.

Lemma 2.6: Suppose $d_1e_1 = r$, $d_2e_2 = r$, $(x, d_1) = 1$, and $(y, d_2) = 1$ where $d_1 \geq x > 0$ and $d_2 \geq y > 0$. Then the following hold:

(i) $xe_1 \equiv ye_2 \pmod{r}$ if and only if $xe_1 = ye_2$;

(ii) $xe_1 = ye_2$ if and only if $xd_2 = yd_1$;

(iii) $xd_2 = yd_1$ if and only if $d_1 = d_2$ and $x = y$.

Proof of (i): Because $d_1e_1 = r$ and $x \leq d_1$, then $0 < xe_1 \leq r$. Similarly, $0 < ye_2 \leq r$. Thus, since xe_1 and ye_2 are members of the same complete residue system modulo r, they are congruent if and only if they are equal.

Proof of (ii): If $xe_1 = ye_2$, then $e_1 = r/d_1$ and $e_2 = r/d_2$ imply $x(r/d_1) = y(r/d_2)$. Hence, $xd_2 = yd_1$. The converse follows in a similar manner.

Proof of (iii): If $d_1 = d_2$ and $x = y$, then $xd_2 = yd_1$. Suppose $xd_2 = yd_1$. Thus, $x \mid yd_1$. But since $(x, d_1) = 1$, then

$x|y$. Similarly, $xd_2 = yd_1$ and $(y, d_2) = 1$ imply that $y|x$. So $y = x$, and it follows that $d_1 = d_2$. Δ

Theorem 2.7: If $d_1|r$, $d_2|r$, $(x, d_1) = 1$, and $(y, d_2) = 1$ where $d_1 \geq x > 0$ and $d_2 \geq y > 0$, then

$$\sum_{n \equiv a+b \pmod r} e(ax, d_1)\, e(by, d_2) = \begin{cases} r \cdot e(nx, d) & \text{if } d_1 = d_2 = d \text{ and } x = y \\ 0 & \text{otherwise} \end{cases}.$$

Proof: Since $d_1|r$, there exists an e_1 such that $d_1 e_1 = r$. Likewise there exists an e_2 such that $d_2 e_2 = r$. Denote the left side of the desired equation by S. From the alternate form of the Cauchy product,

$$S = \sum_{a \pmod r} e(ax, d_1)\, e((n-a)y, d_2).$$

Since $e(ax, d_1)\, e((n-a)y, d_2) = e(ny, d_2)\, e(ax, d_1)\, e(-ay, d_2)$ and since $e(ny, d_2)$ is independent of the index of summation,

$$S = e(ny, d_2) \sum_{a \pmod r} e(ax, d_1)\, e(-ay, d_2).$$

If the e-functions in this summation are multiplied in exponential form, it follows that $e(ax, d_1)\, e(-ay, d_2) = e(a(xd_2 - yd_1), d_1 d_2)$. Now $d_1 e_1 = r$ and $d_2 e_2 = r$ imply $x/d_1 - y/d_2 = (xe_1 - ye_2)/r$. Thus, $e(a(xd_2 - yd_1), d_1 d_2) = e(a(xe_1 - ye_2), r)$ and

$$S = e(ny, d_2) \sum_{a \pmod r} e(a(xe_1 - ye_2), r).$$

This summation can be evaluated by use of the formula in Theorem 2.3 so that

$$\sum_{a(\mathrm{mod}\, r)} e(a(xe_1 - ye_2), r) = \begin{cases} r & \text{if } xe_1 - ye_2 \equiv 0 \,(\mathrm{mod}\, r) \\ 0 & \text{if } xe_1 - ye_2 \not\equiv 0 \,(\mathrm{mod}\, r) \end{cases}.$$

But by the previous lemma $xe_1 \equiv ye_2 \,(\mathrm{mod}\, r)$ if and only if $d_1 = d_2$ and $x = y$. Thus,

$$S = \begin{cases} r \cdot e(nx, d) & \text{if } d_1 = d_2 = d \text{ and } x = y \\ 0 & \text{otherwise} \end{cases}. \qquad \Delta$$

The Ramanujan Sum

The last function considered here is the Ramanujan sum. This function has been studied since 1900 by many mathematicians, including Jensen in 1913 and Landau. Although Ramanujan's contribution to its study did not appear until 1918, Hardy and Wright [10] note that Ramanujan was the first mathematician to see the full importance of this function and to use it systematically. Grosswald [8] gives Hardy credit for calling this sum a Ramanujan sum. Although this particular application is not pursued here, Ramanujan's sum is especially important in the theory of the representation of numbers by sums of squares.

Definition 2.4: A Ramanujan sum, denoted by $c(n, r)$, is defined by $c(n, r) = \sum_z e^{\frac{2\pi i z n}{r}}$ where z ranges over a reduced residue system modulo r. The integer n is called the argument, and r is called the index.

It is important to note that this sum is over a reduced residue system modulo r. Later on when the unitary analogue of $c(n, r)$ is discussed, the index of summation changes appropriately to a semi-reduced residue system modulo r.

Since $e^{\frac{2\pi izn}{r}} = e(zn, r)$, then $c(n, r) = \sum_{z} e(zn, r)$ where the summation is defined as above. This notation will be used whenever possible. Also, since the e-functions are the rth roots of unity, the summands in the Ramanujan sum are the rth roots of unity. Finally, it is clear from the definition that $c(n, 1) = 1$ for all values of n.

This first theorem about Ramanujan sums will be used later and follows quickly from a basic notion about reduced residue systems.

Theorem 2.8: If $(a, r) = 1$, then $c(an, r) = c(n, r)$.

Proof: Suppose that z ranges over a reduced residue system modulo r. Because $(a, r) = 1$, the values for az will also range over a reduced residue system modulo r. Hence, the definitions of $c(an, r)$ and $c(n, r)$ are equivalent. △

With the help of one lemma it is not difficult to show that Ramanujan sums are multiplicative functions of their indices. Since this lemma is a part of elementary number theory, its proof is not included here but can be found in Grosswald [8].

Lemma 2.9: Let $(m_1, m_2) = 1$. Let h_1 run through a reduced residue system modulo m_1 and let h_2 run through a reduced residue system modulo m_2. Then $h = h_2m_1 + h_1m_2$ runs through a reduced residue system modulo m_1m_2.

Theorem 2.10: Ramanujan sums are multiplicative functions of their indices; that is, if $(r, s) = 1$, then $c(n, r)\,c(n, s) = c(n, rs)$ for all integers n.

Proof: Let $(r, s) = 1$. Let z_1 run through a reduced residue system modulo r and z_2 run independently through a reduced residue system modulo s. Then by the definitions of $c(n, r)$ and $c(n, s)$ and from the laws of exponents

$$c(n, r)\,c(n, s) = \sum_{z_1} e(z_1 n, r) \sum_{z_2} e(z_2 n, s)$$

$$= \sum_{z_1} \sum_{z_2} e((z_1 s + z_2 r)n, rs) .$$

By the previous lemma this double sum can be expressed in the form

$$\sum_{z} e(nz, rs)$$

where $z = z_1 s + z_2 r$ runs through a reduced residue system modulo rs. But since this is only the definition of $c(n, rs)$, then $c(n, r)\,c(n, s) = c(n, rs)$. △

The following theorem provides a neat representation for $c(n, r)$ as a special convolution of the Möbius function and the identity function.

Theorem 2.11: Let $(n, r) = k$. Then $c(n, r) = \sum_{d \mid k} d\mu(r/d)$.

Proof: Let z range over a complete set of residues modulo r. By the summation property of μ,

$$\sum_{d_1 | (z, r)} \mu(d_1) = \begin{cases} 1 & \text{if } (z, r) = 1 \\ 0 & \text{if } (z, r) \neq 1 \end{cases} .$$

Recall that the definition of $c(n, r)$ requires it to be a sum of e-functions over a reduced residue system modulo r. Hence, if the coefficient $\sum_{d_1 | (z, r)} \mu(d_1)$ is inserted with each term in a sum of e-functions over a complete residue system modulo r, the summation changes from a complete residue system modulo r to a reduced residue system modulo r. Thus,

$$c(n, r) = \sum_{z (\text{mod } r)} e(zn, r) \sum_{d_1 | (z, r)} \mu(d_1) .$$

If $d_1 | (z, r)$, then $d_1 | z$ and $d_1 | r$, and the order of summation in the above equation can be interchanged so that one sum is over the divisors of r and one is over the divisors of z. Hence,

$$c(n, r) = \sum_{d_1 | r} \mu(d_1) \sum_{\substack{d_1 | z \\ 1 \leq z \leq r}} e(zn, r) .$$

Since $d_1 | z$, there exists an s such that $z = s d_1$. Also, since $1 \leq z \leq r$, then $s = 1, 2, \ldots, r/d_1$. So with $z = s d_1$,

$$c(n, r) = \sum_{d_1 | r} \mu(d_1) \sum_{s=1}^{r/d_1} e(s d_1 n, r)$$

$$= \sum_{d_1 | r} \mu(d_1) \sum_{s=1}^{r/d_1} e(sn, r/d_1) .$$

This second equality follows by writing $e(s d_1 n, r)$ in exponential form.

Now the summation over s is r/d_1 if $r/d_1 | n$ and is 0 if $r/d_1 \nmid n$. Thus,

$$c(n, r) = \sum_{\substack{d_1 | r \\ r/d_1 | n}} \mu(d_1) r/d_1 .$$

If r/d_1 is replaced by d, $c(n, r) = \sum_{d | r, d | n} \mu(r/d)d$. However, $d | r$ and $d | n$ if and only if $d | k$ with $k = (n, r)$. Hence,

$$c(n, r) = \sum_{d | k} d\mu(r/d). \qquad \Delta$$

Corollary 2.11.1: Let p be a prime.

(i) If $p^b \| n$ and $0 < b < a$, then $c(n, p^a) = \begin{cases} 0 & \text{if } a - b \geq 2 \\ -p^b & \text{if } a - b = 1 \end{cases}$.

(ii) If $p^b \| n$ and $b \geq a$, then $c(n, p^a) = p^{a-1}(p - 1)$.

(iii) If $p \nmid n$, then $c(n, p^a) = \begin{cases} 0 & \text{if } a \geq 2 \\ -1 & \text{if } a = 1 \\ 1 & \text{if } a = 0 \end{cases}$.

Proof of (i): Let p be a prime and suppose $p^b \| n$ where $0 < b < a$. Then $(n, p^a) = p^b$. Hence, from the previous theorem

$$c(n, p^a) = \sum_{d | p^b} d\mu(p^a/d) = \mu(p^a) + \ldots + p^{b-1}\mu(p^{a-b+1}) + p^b\mu(p^{a-b}) .$$

The value of this expression can be determined by looking at the last term $p^b\mu(p^{a-b})$ since $a - b$ is the smallest exponent involved in that position. If $a - b \geq 2$, all the terms are 0. If $a - b = 1$, only the last term $p^b\mu(p)$ is nonzero. Hence,

$$c(n, p^a) = \begin{cases} 0 & \text{if } a - b \geq 2 \\ -p^b & \text{if } a - b = 1 \end{cases}.$$

Proof of (ii): If $p^b \| n$ and $b \geq a$, then $(n, p^a) = p^a$. In this case $c(n, p^a) = \sum_{d | p^a} d\,\mu(p^a/d) = p^{a-1}\mu(p) + p^a\mu(1) = p^{a-1}(p - 1)$.

Proof of (iii): Now suppose $p \nmid n$. Then $p^a \nmid n$ and $(n, p^a) = 1$. Hence,

$$c(n, p^a) = \sum_{d | 1} d\,\mu(p^a/d) = \mu(p^a) = \begin{cases} 0 & \text{if } a \geq 2 \\ -1 & \text{if } a = 1 \\ 1 & \text{if } a = 0 \end{cases}. \qquad \Delta$$

Corollary 2.11.2: $c(1, r) = \mu(r)$.

Proof: Since $(1, r) = 1$ for all values of r,

$$c(1, r) = \sum_{d | 1} d\,\mu(r/d) = \mu(r). \qquad \Delta$$

At this point it would be interesting to compute some Ramanujan sums using both the definition and the theorem. As will be seen, when the definition is employed, the calculation involves determining cosines and sines for particular values. On the other hand, the use of the theorem involves mainly a knowledge of the definition of μ.

Example 2.3: The Ramanujan sum $c(10, 6)$ is calculated first by the definition. If z runs through a reduced residue system modulo 6, z has the values 1 and 5. Thus,

$$c(10, 6) = \sum_{z=1,5} e(10z, 6) = e(10, 6) + e(50, 6)$$

$$= (\cos 10\pi/3 + i \sin 10\pi/3) + (\cos 50\pi/3 + i \sin 50\pi/3)$$

$$= (-1/2 - i\sqrt{3}/2) + (-1/2 + i\sqrt{3}/2)$$

$$= -1 ,$$

To use the formula of the preceding theorem first note that $(10, 6) = 2$. Hence, $c(10, 6) = \sum_{d|2} d\,\mu(6/d) = \mu(6) + 2 \cdot \mu(3) = -1$.

Example 2.4: Suppose $c(6, 9)$ is to be determined. The integers z in a reduced residue system modulo 9 are $1, 2, 4, 5, 7$, and 8. Thus, by the definition $c(6, 9) = \sum_{z} e(6z, 9)$ where z takes on the values listed above. Therefore,

$$c(6, 9) = e(6, 9) + e(12, 9) + e(24, 9) + e(30, 9) + e(42, 9) + e(48, 9)$$

$$= (\cos 4\pi/3 + i \sin 4\pi/3) + (\cos 8\pi/3 + i \sin 8\pi/3) +$$

$$(\cos 16\pi/3 + i \sin 16\pi/3) + (\cos 20\pi/3 + i \sin 20\pi/3) +$$

$$(\cos 28\pi/3 + i \sin 28\pi/3) + (\cos 32\pi/3 + i \sin 32\pi/3)$$

$$= 3(-1/2 - i\sqrt{3}/2) + 3(-1/2 + i\sqrt{3}/2) = -3 .$$

This last calculation was even longer than that of the previous example. Since $c(6, 9) = c(6, 3^2)$ and $3 \| 6$, this result can be determined rather quickly by using part (i) of the first corollary. Since $b = 1$ and $a = 2$, $a - b = 1$, and it follows immediately that $c(6, 9) = -3$.

Hölder [3] is responsible for a formula which gives Ramanujan's sum in terms of φ and μ. This representation is different from that of Theorem 2.11 as no convolution is involved. The proof of this result relies heavily upon Corollary 2.11.1 which states the value of $c(n, p^a)$ where p is a prime, and a is any positive integer. In fact,

since all of the functions involved here are multiplicative, it suffices to verify the formula for prime powers in the canonical representation of r.

Theorem 2.12: If $m = r/(n, r)$, then $c(n, r) = \varphi(r)\mu(m)/\varphi(m)$.

Proof: Let p by any prime in the canonical representation of r and a any positive integer. Since $c(n, r)$, φ, and μ are all multiplicative with respect to r, it is sufficient to show the equality for $r = p^a$. It is necessary to consider three cases, one where $p^b \| n$ with $0 < b < a$, one where $p^b \| n$ with $b \geq a$, and one where $p \nmid n$.

If $p^b \| n$ with $0 < b < a$, then $m = p^a/p^b$. If R denotes the right side of the desired expression,

$$R = \varphi(p^a)\mu(p^{a-b})/\varphi(p^{a-b}) = p^{a-1}(p-1)\mu(p^{a-b})/p^{a-b-1}(p-1) = p^b\mu(p^{a-b}).$$

Hence,

$$R = \begin{cases} 0 & \text{if } a - b \geq 2 \\ -p^b & \text{if } a - b = 1 \end{cases}.$$

If $p^b \| n$ with $b \geq a$, $m = 1$ and $R = \varphi(p^a) = p^{a-1}(p-1)$.

If $p \nmid n$, then $(n, p^a) = 1$. So $R = \varphi(p^a)\mu(p^a)/\varphi(p^a) = \mu(p^a)$.

Thus,

$$R = \begin{cases} 0 & \text{if } a \geq 2 \\ -1 & \text{if } a = 1 \\ 1 & \text{if } a = 0 \end{cases}.$$

These values for R are the same as those obtained for $c(n, p^a)$ in Corollary 2.11.1. Hence, the equality follows. Δ

The following corollary is not a result which "naturally" comes to mind. However, it is essential in Chapter III and does follow from this particular representation of Ramanujan's sum.

Corollary 2.12.1: If d and δ are divisors of r, then $c(r/\delta, d)\,\varphi(\delta) = c(r/d, \delta)\,\varphi(d)$.

Proof: Let d and δ be divisors of r. The corollary follows from the fact that $d/(r/\delta, d) = \delta/(r/d, \delta)$. Δ

Orthogonality Properties of Ramanujan Sums

Ramanujan sums are interesting in themselves as examples of functions of two variables. But their importance in this context lies mainly in the fact that they are essential to the development of the representation of even functions modulo r, a topic to be considered in the next chapter. With this purpose in mind the remainder of this chapter is concerned with two orthogonality properties of Ramanujan sums. Theorem 2.13 is a result which later on will classify Ramanujan's sum as a special type of function.

Theorem 2.13: If $(n, r) = k$, then $c(n, r) = c(k, r)$.

Proof: Since $(n, r) = k$, then $c(n, r) = \sum_{d \mid k} d\,\mu(r/d)$. Now $(k, r) = ((n, r), r) = k$. Thus, $c(k, r)$ has precisely the same representation as $c(n, r)$. Δ

The next theorem is the first of the aforementioned orthogonality properties. The key to its proof lies in expressing the product of the Ramanujan sums as a product of sums of e-functions and then

arranging the summation so that the formula in Theorem 2.7 for the generalized Cauchy product of e-functions can be applied.

Theorem 2.14: If $d_1 | r$ and $d_2 | r$, then for every n,

$$\sum_{n \equiv a+b \pmod r} c(a, d_1)\, c(b, d_2) = \begin{cases} r \cdot c(n, d) & \text{if } d_1 = d_2 = d \\ 0 & \text{if } d_1 \neq d_2 \end{cases} .$$

Proof: Denote the left side of the desired equation by L. By the definition of Ramanujan's sum along with a change in the order of summation

$$L = \sum_{z_1, z_2} \sum_{n \equiv a+b \pmod r} e(a z_1, d_1)\, e(b z_2, d_2)$$

as z_1 runs through a reduced residue system modulo d_1, and z_2 runs through a reduced residue system modulo d_2. Without loss of generality, assume $d_1 \geq z_1 > 0$ and $d_2 \geq z_2 > 0$. Thus, by Theorem 2.7,

$$L = \begin{cases} r \sum_{z_1} e(n z_1, d) & \text{if } d_1 = d_2 = d \text{ and } z_1 = z_2 \\ 0 & \text{otherwise,} \end{cases}$$

where z_1 ranges over a reduced residue system modulo d. Hence,

$$L = \begin{cases} r \cdot c(n, d) & \text{if } d_1 = d_2 = d \\ 0 & \text{if } d_1 \neq d_2 \end{cases} . \qquad \Delta$$

Corollary 2.14.1: $$\sum_{a \pmod r} c(a, r) = \begin{cases} 1 & \text{if } r = 1 \\ 0 & \text{if } r > 1 \end{cases} .$$

Proof: If $r = 1$, then $\sum_{a(\mathrm{mod}\, r)} c(a, r) = c(a, 1) = 1$. Suppose $r > 1$ and let $d_1 = r$ and $d_2 = 1$ in the previous theorem. Then $\sum_{a(\mathrm{mod}\, r)} c(a, r)\, c(b, 1) = \sum_{a(\mathrm{mod}\, r)} c(a, r)$ since $c(b, 1) = 1$. On the other hand, $\sum_{a(\mathrm{mod}\, r)} c(a, r) = 0$ since $r \neq 1$. These last two equations show that $\sum_{a(\mathrm{mod}\, r)} c(a, r) = 0$ if $r > 1$. Δ

Theorem 2.16 is the second orthogonality property for Ramanujan sums. In this instance the property is given in terms of the divisors of r rather than by a congruence. The proof begins by looking at the same sum as that stated in the first orthogonality property and proceeds by replacing a complete residue system a modulo r by an equivalent system. The following lemma from elementary number theory allows such changes to be made.

Lemma 2.15: The integers $a = zd$ where d ranges over the divisors of r, and for each d, z ranges over a reduced residue system modulo r/d constitute a complete residue system modulo r.

Theorem 2.16: If $d_1 | r$ and $d_2 | r$, then

$$\sum_{d | r} c(r/d, d_1)\, c(r/d_2, d) = \begin{cases} r & \text{if } d_1 = d_2 \\ 0 & \text{if } d_1 \neq d_2 \end{cases}.$$

Proof: Let

$$R = \sum_{n \equiv a+b(\mathrm{mod}\, r)} c(a, d_1)\, c(b, d_2) = \sum_{a(\mathrm{mod}\, r)} c(a, d_1)\, c(n - a, d_2).$$

From the previous lemma a complete residue system a modulo r is given by $a = z(r/d)$ where d ranges over the divisors of r, and

for each d, z ranges over a reduced residue system modulo d. So

$$R = \sum_{z} \sum_{d|r} c(zr/d, d_1)\, c(n - zr/d, d_2)$$

as z ranges over a reduced residue system modulo d for every divisor d of r. Since $d_1 | r$, then $(z, d_1) = 1$, and it follows that $c(zr/d, d_1) = c(r/d, d_1)$. Hence,

$$R = \sum_{d|r} c(r/d, d_1) \sum_{z} c(n - zr/d, d_2)$$

where z ranges over a reduced residue system modulo d. Consider only the z-sum. By the definition of Ramanujan's sum,

$$\sum_{z} c(n - zr/d, d_2) = \sum_{z} \sum_{x} e((n - zr/d)x, d_2)$$

where x runs through a reduced residue system modulo d_2. Now $e((n - zr/d)x, d_2) = e(nx, d_2)\, e(-zrx/d_2, d)$. Because z ranges over a reduced residue system modulo d, this z-sum may be written as

$$\sum_{x} e(nx, d_2) \sum_{z} e(-zrx/d_2, d) = c(n, d_2)\, c(-zr/d_2, d).$$

Since $(-z, d) = 1$, then $c(-zr/d_2, d) = c(r/d_2, d)$. Hence,

$$R = \sum_{d|r} c(r/d, d_1)\, c(n, d_2)\, c(r/d_2, d)$$

$$= c(n, d_2) \sum_{d|r} c(r/d, d_1)\, c(r/d_2, d).$$

However, from the first orthogonality property,

$$R = \begin{cases} r \cdot c(n,d) & \text{if } d_1 = d_2 = d \\ 0 & \text{if } d_1 \neq d_2 . \end{cases}$$

Therefore, it follows from these two values of R that

$$\sum_{d|r} c(r/d, d_1)\, c(r/d_2, d) = \begin{cases} r & \text{if } d_1 = d_2 \\ 0 & \text{if } d_1 \neq d_2 . \end{cases}$$ △

Corollary 2.16.1: $\sum_{d|r} c(n,d) = \begin{cases} r & \text{if } r|n \\ 0 & \text{if } r \nmid n . \end{cases}$

Proof: In the previous theorem let $d_1 = 1$. Since $c(r/d, d_1) = 1$,

$$\sum_{d|r} c(r/d_2, d) = \begin{cases} r & \text{if } d_2 = 1 \\ 0 & \text{if } d_2 \neq 1 . \end{cases}$$

So the nonzero terms of the sum occur when $d_2 = 1$. In this case $c(r/d_2, d) = c(r, d)$. Since $d|r$, $(r,d) = d$. If $r|n$, then $(n,d) = d$. So $(r,d) = (n,d)$ if $r|n$. By Theorem 2.13, $c(r,d) = c((r,d),d) = c((n,d),d) = c(n,d)$ if $r|n$. So

$$\sum_{d|r} c(n,d) = \begin{cases} r & \text{if } r|n \\ 0 & \text{if } r \nmid n . \end{cases}$$ △

The e-function of this chapter laid the foundation for the development of Ramanujan's sum. Now Ramanujan's sum plays a key role in the study of even functions modulo r.

CHAPTER III

EVEN FUNCTIONS MODULO r

This chapter deals with a class of functions of two variables called even functions modulo r. Representations for these functions are derived, one of which involves the function $c(n, r)$. In Chapter V the unitary counterpart of the even function modulo r, called the unitary function modulo r, is discussed. At that time it is shown that a unitary function modulo r is also an even function modulo r. Hence, the representations derived in this chapter are significant in finding representations for the unitary function modulo r.

Let r be an arbitrary positive integer and F a field of characteristic zero which contains the rth roots of unity. If n is a non-negative integer, $f(n, r)$ is an element of F associated with the pair of integers n and r; that is, f is a function of n and r. In this setting the central theme of this chapter is that the class of even functions modulo r is identical to either of two classes of functions. One class is defined by $f(n, r) = \sum_{d \mid r} \alpha(d) c(n, d)$ where $\alpha(d) \in F$, and the other class is defined by $f(n, r) = \sum_{d \mid (n, r)} g(d, r/d)$ where g is an arbitrary function with values in F.

Definition 3.1: The function $f(n, r)$ is an even function of n modulo r if it satisfies the following:

(i) $f(m, r) = f(n, r)$ if $m \equiv n \pmod{r}$;

(ii) $f(n, r) = f(k, r)$ if $k = (n, r)$.

From (ii) it is evident that for every n the value of an even function $f(n, r)$ is determined by the greatest common divisor of n and r, (n, r). Also, since $n + r \equiv n \pmod{r}$, then $f(n+r, r) = f(n, r)$, and an even function modulo r is periodic in n with period r. Part (ii) of the definition is sufficient to show that f is an even function modulo r and hence can be taken as a characterization of even functions modulo r.

Theorem 3.1: The function $f(n, r)$ is an even function of n modulo r if and only if $f(n, r) = f(k, r)$ for $k = (n, r)$.

Proof: If $f(n, r)$ is an even function of n modulo r, the condition holds. Suppose that the condition holds. For any m and n with $m \equiv n \pmod{r}$, $(m, r) = (n, r) = k$. Thus, $f(n, r) = f(k, r) = f((m, r), r) = f(m, r)$. Hence, part (i) of the definition is satisfied, and $f(n, r)$ is even modulo r. Δ

One of the results of the previous chapter was that $c(n, r) = c(k, r)$ where $k = (n, r)$. This property, along with the above theorem, shows that Ramanujan's sum is an even function modulo r. This is nice to know; however, in deriving the representations for even functions modulo r, sums are encountered which involve $c(n, d)$ for $d \mid r$ rather than $c(n, r)$ itself. It is convenient to extend the definition of even function modulo r and define $f(n, d)$ as an even function of n modulo r.

Definition 3.2: Suppose $f(n, r)$ is an even function of n modulo r and $d \mid r$. Then $f(n, d)$ is an even function of n modulo r if and only if $f(n, d) = f((n, r), d)$.

Theorem 3.2: If δ is any divisor of r, then $c(n, \delta)$ is an even function of n modulo r.

Proof: If $\delta \mid r$, the proof is complete if $c(n, \delta) = c((n, r), \delta)$. From the characterization for Ramanujan's sum,

$$c(n, \delta) = \sum_{d \mid (n, \delta)} d\mu(\delta/d) \quad \text{and} \quad c((n, r), \delta) = \sum_{d' \mid ((n, r), \delta)} d'\mu(\delta/d').$$

Since the set of divisors of (n, δ) is the same as the set of divisors of $((n, r), \delta)$, the two sums are identical, and it follows that $c(n, \delta)$ is an even function of n modulo r. Δ

With these preliminaries out of the way the exciting part of the chapter is at hand. The first representation for $f(n, r)$, an even function of n modulo r, is in terms of Ramanujan's sum. To show that a representation of this form defines an even function modulo r is straightforward from the definition. The hard part is to show that an even function modulo r has this representation. At this point in the proof an outline of the major steps involved is given.

Theorem 3.3: Every even function $f(n, r)$ of n modulo r can be represented by the form

$$f(n, r) = \sum_{d \mid r} \alpha(d)\, c(n, d) \tag{1}$$

where $\alpha(d) \in F$. Conversely, every function of the form (1) is even

modulo r, and the coefficients $\alpha(d) = \alpha(d, r/d)$ are given by

$$\alpha(d) = 1/r \sum_{d_1 | r} f(r/d_1, r)\, c(r/d, d_1) \tag{1a}$$

or by the equivalent formula

$$\alpha(d) = 1/(r\varphi(d)) \sum_{m=1}^{r} f(m, r)\, c(m, d) . \tag{1b}$$

Proof: In order to show that the function $f(n, r) = \sum_{d | r} \alpha(d)\, c(n, d)$ is an even function modulo r, it is necessary to show that $f(n, r) = f(k, r)$ where $k = (n, r)$. This follows immediately from the fact that $c(n, d) = c(k, d)$ for all divisors d of r.

Now let $f(n, r)$ be an even function of n modulo r and $k = (n, r)$. The proof will be complete once two main points are verified. First, it must be shown that $f(n, r)$ has a representation of the type (1) with $\alpha(d)$ defined by (1a). Secondly, formulas (1a) and (1b) must be shown to be equivalent.

To justify the first point, consider a representation of the type (1) with $\alpha(d)$ determined by (1a). To make the notation simpler let (1) be denoted by S. Substituting (1a) into (1) for $\alpha(d)$ and noting that $c(n, d)$ is an even function modulo r for $d | r$,

$$S = \sum_{d | r} \left(\frac{1}{r} \sum_{d_1 | r} f(r/d_1, r)\, c(r/d, d_1) \right) c(n, d)$$

$$= \frac{1}{r} \sum_{d_1 | r} f(r/d_1, r) \sum_{d | r} c(r/d, d_1)\, c(k, d) .$$

By the second orthogonality property for Ramanujan sums

$$\sum_{d|r} c(r/d, d_1)\, c(k, d) = \sum_{d|r} c(r/d, d_1)\, c\left(\frac{r}{r/k}, d\right)$$

$$= \begin{cases} r & \text{if } d_1 k = r \\ 0 & \text{if } d_1 k \neq r \end{cases} .$$

This means that the nonzero terms in S occur only when $d_1 k = r$ so that $S = f(k, r)$. But $f(k, r) = f(n, r)$ since $f(n, r)$ is an even function modulo r. Hence, $f(n, r)$ has the representation (1) where $\alpha(d)$ is given by (1a).

In order to show that (1a) and (1b) are equivalent representations for $\alpha(d)$, begin with $\alpha(d)$ defined by (1b). This sum is taken over the integers x in a complete residue system modulo r. Lemma 2.15 allows this sum to be made over an equivalent complete residue system of the form rx/d_1 where $d_1 | r$ and $(x, d_1) = 1$. With this change in summation

$$\alpha(d) = \frac{1}{r\varphi(d)} \sum_{d_1|r} \sum_{\substack{(x, r)=1 \\ x (\mathrm{mod}\, d_1)}} f(rx/d_1, r)\, c(rx/d_1, d) .$$

Since $d_1 | r$ and $(x, r) = 1$, then $(rx/d_1, r) = r/d_1$, and thus $f(rx/d_1, r) = f(r/d_1, r)$ since $f(n, r)$ is an even function modulo r. Theorem 2.8 implies $c(rx/d_1, d) = c(r/d_1, d)$ since $(x, d) = 1$. Hence,

$$\alpha(d) = \frac{1}{r\varphi(d)} \sum_{d_1|r} \sum_{\substack{(x, r)=1 \\ x (\mathrm{mod}\, d_1)}} f(r/d_1, r)\, c(r/d_1, d) .$$

Since the x is no longer present in the inner summation, this sum

merely counts one $f(r/d_1, r)\, c(r/d_1, d)$ for each x in a reduced residue system modulo d_1. So the inner sum is only $f(r/d_1, r)\, c(r/d_1, d)\, \varphi(d_1)$. But since d_1 and d are arbitrary divisors of r, $c(r/d_1, d)\, \varphi(d_1) = c(r/d, d_1)\, \varphi(d)$ as was shown in Chapter II. Thus,

$$\alpha(d) = \frac{1}{r\varphi(d)} \sum_{d_1 | r} f(r/d_1, r)\, c(r/d, d_1)\, \varphi(d) ,$$

and the representation (1a) follows. Δ

Theorems 3.4 and 3.5 establish the equivalence of the class of functions $f(n, r) = \sum_{d | (n, r)} g(d, r/d)$ mentioned earlier and the set of all even functions modulo r. With this second representation it is possible to characterize an even function modulo r by either formula.

Theorem 3.4: Every even function modulo r may be written in the form

$$f(n, r) = \sum_{d | (n, r)} g(d, r/d) , \tag{2}$$

where

$$g(d, r/d) = d \sum_{d_1 | r/d} \alpha(d\, d_1)\, \mu(d_1) . \tag{2a}$$

Conversely, every function of this form is even modulo r.

Proof: Let $f(n, r)$ be an even function modulo r. Then $f(n, r)$ has the representation $f(n, r) = \sum_{\delta | r} \alpha(\delta)\, c(n, \delta)$. Since $c(n, \delta) = \sum_{d | (n, \delta)} d\, \mu(\delta/d)$, then $f(n, r) = \sum_{\delta | r} \alpha(\delta) \sum_{d | (n, \delta)} d\, \mu(\delta/d)$. Now $\delta | r$ and $d | (n, \delta)$ is equivalent to $d | (n, r)$, $\delta | r$, and $d | \delta$ so that

$f(n,r) = \sum_{d|(n,r)} d \sum_{\delta|r,\, d|\delta} \alpha(\delta)\mu(\delta/d)$. Since $d|\delta$, there exists a d_1 such that $dd_1 = \delta$. Since $\delta|r$, then $dd_1|r$, and it follows that $d_1|r/d$. With these alterations

$$f(n,r) = \sum_{d|(n,r)} d \sum_{d_1|r/d} \alpha(dd_1)\mu(d_1) .$$

Hence, $f(n,r)$ may be written in the form (2) where $g(d, r/d)$ has the form (2a).

To prove the converse suppose that $f(n,r) = \sum_{d|(n,r)} g(d, r/d)$ and that $k = (n,r)$. Since $d|(n,r)$ if and only if $d|((n,r), r)$, it follows that $f(n,r) = f(k,r)$, and $f(n,r)$ is even modulo r. Δ

Theorem 3.5: An even function of the form (2) has a representation of the form (1) where the coefficients $\alpha(d)$ are determined by

$$\alpha(d) = 1/r \sum_{d'|r/d} g(r/d', d') \cdot d' .$$

Proof: If $f(n,r)$ is an even function modulo r, by Theorems 3.4 and 3.3 it may be assumed that $f(n,r) = \sum_{\delta|(n,r)} g(\delta, r/\delta)$ and $f(n,r) = \sum_{d|r} \alpha(d)\, c(n,d)$. Also, Theorem 3.3 implies that

$$\alpha(d) = 1/r \sum_{d_1|r} f(r/d_1, r)\, c(r/d, d_1) .$$

Since $f(r/d_1, r) = \sum_{D|(r/d_1, r)} g(D, r/D)$, then

$$\alpha(d) = 1/r \sum_{d_1|r} c(r/d, d_1) \sum_{D|(r/d_1, r)} g(D, r/D) .$$

The second sum is over the divisors D of r/d_1 because

$(r/d_1, r) = r/d_1$. Since $d_1 | r$ and $D | r/d_1$ if and only if $D | r$ and $d_1 | r/D$, then

$$\alpha(d) = 1/r \sum_{D|r} g(D, r/D) \sum_{d_1|r/D} c(r/d, d_1) .$$

Since $D | r$, there exists an element d' such that $Dd' = r$. Hence,

$$\alpha(d) = 1/r \sum_{d'|r} g(r/d', d') \sum_{d_1|d'} c(r/d, d_1) .$$

But by Corollary 2.16.1,

$$\sum_{d_1|d'} c(r/d, d_1) = \begin{cases} d' & \text{if } d' | r/d \\ 0 & \text{if } d' \nmid r/d \end{cases} .$$

Therefore, $\alpha(d) = 1/r \sum_{d'|r/d} g(r/d', d') \cdot d'$ as was required. Δ

In summary this chapter dealt with an interesting class of functions of two variables, the class of even functions modulo r. The Ramanujan sum introduced in Chapter II turned out to be one of these even functions. It was shown that an even function modulo r can be characterized by either one of two representations, one of which is in terms of Ramanujan's sum.

In the next chapter attention is given to functions of two variables defined in terms of the unitary divisor. Three particular functions are studied, two of which are analogues of functions considered in Chapter II. Not only are the results interesting and important to the entire discussion, but the methods by which the results are obtained

should also be noticed, particularly the parallels between the methods of Chapters IV and V and Chapters II and III.

CHAPTER IV

SOME UNITARY ANALOGUES

In Chapter II several functions of two variables were discussed, and it was noted that the unitary analogues of these functions would also be developed. This chapter deals with the unitary analogues of the Nagell totient function and of Ramanujan's sum. A unitary convolution for two variables is also defined which leads to the unitary analogues of the Anderson-Apostol, Landau, and Brauer-Rademacher identities. The study of this convolution gives an added bonus for under special conditions it reduces to μ^*, φ^*, and σ^* respectively. The discussion begins with the function $\theta^*(n, r)$.

The Function $\theta^*(n, r)$

Definition 4.1: If n is a nonnegative integer and r is a positive integer, the unitary analogue of the Nagell totient function, denoted by $\theta^*(n, r)$, is defined to be the number of integers x such that

(i) $1 \leq x \leq r$

(ii) $(x, r)_* = (n - x, r)_* = 1$.

Example 4.1: Suppose that $n = 24$ and $r = 10$. Then one must determine the numbers x so that $1 \leq x \leq 10$ and $(x, 10)_* = (24 - x, 10)_* = 1$. Of the set $1 \leq x \leq 10$, only $1, 3, 7$, and

9 satisfy $(x, 10)_* = 1$. Since $(15, 10)_* = 5$, 9 does not satisfy $(24 - x, 10)_* = 1$. Thus, $\theta^*(24, 10) = 3$.

Just as the Nagell function reduces to Euler's function in the case where $n = r$, under this same condition $\theta^*(n, r)$ reduces to $\varphi^*(r)$.

Theorem 4.1: If $n = r$, then $\theta^*(n, r) = \varphi^*(r)$.

Proof: The number of integers x such that $1 \leq x \leq r$ and $(x, r)_* = 1$ is $\varphi^*(r)$. If $(x, r)_* = 1$, then $(r - x, r)_* = 1$. Hence, it follows that $\theta^*(r, r) = \varphi^*(r)$. Δ

It is clear from the definition that $\theta^*(n, 1) = 1$. Other evaluations would be useful, but if the definition were used each time $\theta^*(n, r)$ was calculated, the work could become rather tedious. A formula characterizing this function can be found using the multiplicative property of $\theta^*(n, r)$ and the value of $\theta^*(n, p^a)$ for any prime p and a any positive integer.

The proof that $\theta^*(n, r)$ is a multiplicative function of r is particularly interesting since it uses the properties of unitary divisors and one of the basic concepts of algebra, that of isomorphism. If $r = st$ where $(s, t) = 1$, $s \neq 1$, and $t \neq 1$, then $\theta^*(n, r)$ is multiplicative if $\theta^*(n, r) = \theta^*(n, s)\, \theta^*(n, t)$. Here appropriate sets R, S, and T are defined, and it is shown that R is isomorphic to $S \times T$. The actual isomorphism is shown in Theorem 4.3; Lemma 4.2 provides some necessary preliminaries.

Lemma 4.2: Let $r = st$ where $(s, t) = 1$, $s \neq 1$, and $t \neq 1$. For each nonnegative integer n define the sets S, T, and R as

follows:

$$S = \{y : 1 \leq y \leq s \quad \text{and} \quad (y, s)_* = (n - y, s)_* = 1\}$$

$$T = \{z : 1 \leq z \leq t \quad \text{and} \quad (z, t)_* = (n - z, t)_* = 1\} \tag{1}$$

$$R = \{x : 1 \leq x \leq r \quad \text{and} \quad (x, r)_* = (n - x, r)_* = 1\} .$$

If x is in R, and y and z are defined by the congruences

$$\begin{aligned} x &\equiv y \pmod{s} \quad \text{and} \quad 0 \leq y \leq s \\ x &\equiv z \pmod{t} \quad \text{and} \quad 0 \leq z \leq t , \end{aligned} \tag{2}$$

then y is in S, and z is in T.

Proof: By the definition of S it is necessary for y to satisfy $1 \leq y \leq s$ and $(y, s)_* = (n - y, s)_* = 1$. Because $0 \leq y \leq s$, the first condition follows if $y \neq 0$. If $y = 0$, $x \equiv y \pmod{s}$ implies that $s \mid x$. Since $r = st$ where $(s, t) = 1$, then $s \parallel r$. So $s \mid x$ and $s \parallel r$ imply $s \mid (x, r)_*$. But since $(x, r)_* = 1$, then $s = 1$, a contradiction to the hypothesis. Thus, $y \neq 0$.

If $(y, s)_* = d$, then $d \mid y$ and $d \parallel s$. Because $d \parallel s$ and $s \parallel r$, then $d \parallel r$. Since d is a divisor of both y and s, it follows that $d \mid x$ because $x \equiv y \pmod{s}$. Hence, $d \mid x$ and $d \parallel r$ imply $d \parallel (x, r)_*$. But $(x, r)_* = 1$ from the definition of R. Therefore, $d = 1$.

To complete the proof suppose that $(n - y, s)_* = d_1$. A succession of steps similar to those above yields d_1 a unitary divisor of $(n - x, r)_*$. But since $(n - x, r)_* = 1$, then $d_1 = 1$. These three steps imply that y must be in S. In a similar manner it follows that z is in T. Δ

Theorem 4.3: For each nonnegative integer n, $\theta^*(n, r)$ is a multiplicative function of r.

Proof: Let $r = st$ where $(s, t) = 1$, $s \neq 1$, and $t \neq 1$. Also let S, T, and R be defined by (1). Define the mapping $g : R \to S \times T$ by $g(x) = \langle y, z \rangle$ where y and z are defined by the congruences (2). The fact that g is well defined follows quickly from its own definition and the congruences (2). It remains to be shown that g is one-to-one and onto.

Let $g(x) = \langle y, z \rangle$ and $g(x') = \langle y, z \rangle$. By the definition of g,

$$x \equiv y \pmod{s} \qquad x' \equiv y \pmod{s}$$

and

$$x \equiv z \pmod{t} \qquad x' \equiv z \pmod{t} .$$

Since $(s, t) = 1$, the system of congruences

$$v \equiv y \pmod{s}$$
$$v \equiv z \pmod{t}$$

must have only one solution in the closed interval $[0, st]$. Thus, $x = x'$, and g is one-to-one.

To show that g is onto $S \times T$ let $\langle y, z \rangle \in S \times T$ and let x denote the unique solution of the system of congruences

$$v \equiv y \pmod{s}$$
$$v \equiv z \pmod{t}$$

in the interval $[0, st]$. The proof is complete if $x \in R$, that is, if $1 \leq x \leq r$ and $(x, r)_* = (n - x, r)_* = 1$. Since $(x, s)_* = 1$ and $(x, t)_* = 1$ where $(s, t) = 1$, Theorem 1.12 implies that

$(x, st)_* = (x, r)_* = 1$. Likewise, $(n - x, r)_* = 1$. So x is in R, and g is onto as was required.

Since g is both one-to-one and onto, R is isomorphic to $S \times T$, and the number of elements in R is equal to the number of elements in $S \times T$. Therefore, $\theta^*(n, r)$ is a multiplicative function of r. Δ

If p is any prime and a is a positive integer, $\theta^*(n, p^a)$ is the number of integers x such that $1 \leq x \leq p^a$ and $(x, p^a)_* = (n - x, p^a)_* = 1$. It is necessary to distinguish between the cases $p^a | n$ and $p^a \nmid n$ in determining $\theta^*(n, p^a)$.

Theorem 4.4: If p is any prime and n is a fixed nonnegative integer,

$$\theta^*(n, p^a) = \begin{cases} p^a - 1 & \text{if } p^a | n \\ p^a - 2 & \text{if } p^a \nmid n. \end{cases}$$

Proof: Let $X = \{1, 2, \ldots, p^a - 1\}$ and suppose $p^a | n$. Note that X contains the candidates x to be counted in determining $\theta^*(n, p^a)$. The only unitary divisors of p^a are 1 and p^a. But for every $x \in X$, $p^a \nmid x$ and $p^a \nmid n - x$. Hence, $(x, p^a)_* = (n - x, p^a)_* = 1$ for all $x \in X$. Therefore, if $p^a | n$, $\theta^*(n, p^a) = p^a - 1$.

Now suppose $p^a \nmid n$ and again consider the integers $x \in X$. The set $X + \{0\}$ is a complete residue system modulo p^a. Hence, there exists an x in $X + \{0\}$ such that $x \equiv n \pmod{p^a}$. But since $p^a \nmid n$, $x \neq 0$. This means there is an $x \in X$ such that $(n - x, p^a)_* \neq 1$. Hence, $\theta^*(n, p^a) = p^a - 2$ if $p^a \nmid n$. Δ

Since $\theta^*(n, r)$ is multiplicative and since $\theta^*(n, p^a)$ has been determined for any prime p, it is rather easy to find a formula for $\theta^*(n, r)$. Before this formula is stated, one point needs to be made in regard to notation. The canonical representation of r will be denoted by $r = \prod_{p|r} p^a$, unless otherwise specified.

Theorem 4.5: Let $r = \prod_{p|r} p^a$ be the canonical representation of r. Then $\theta^*(n, r) = \prod_{p^a|n} (p^a - 1) \cdot \prod_{p^a \nmid n} (p^a - 2)$.

Proof: Suppose that n is held fixed. Since $\theta^*(n, r)$ is a multiplicative function of r, $\theta^*(n, r) = \prod_{p|r} \theta^*(n, p^a)$. Since $\theta^*(n, p^a)$ is $p^a - 1$ if $p^a | n$ and is $p^a - 2$ if $p^a \nmid n$, then

$$\theta^*(n, r) = \prod_{p^a|n} (p^a - 1) \cdot \prod_{p^a \nmid n} (p^a - 2), \qquad \Delta$$

Example 4.2: The calculation of $\theta^*(24, 10)$ is easily done with this formula. Note that $10 = 2 \cdot 5$, and $2 | 24$ but $5 \nmid 24$. Thus, $\theta^*(24, 10) = (2 - 1)(5 - 2) = 3$.

Now let $r = \prod_{p|r} p^a$ be the canonical representation of r. If for every prime p, $p^a \nmid n$, the formula for $\theta^*(n, r)$ contains only factors of the form $p^a - 2$. If $p^a | n$ for every prime p that divides r, $\theta^*(n, r)$ is characterized by a product of factors of the form $p^a - 1$. These results are stated in the following corollaries, the second of which gives another condition for which $\theta^*(n, r) = \varphi^*(r)$.

Corollary 4.5.1: Let $r = \prod_{p|r} p^a$ be the canonical representation of r. If $(n, r)_* = 1$, then $\theta^*(n, r) = \prod_{p|r} (p^a - 2) = r \cdot \prod_{p|r} (1 - 2/p^a)$.

Proof: Since $(n, r)_* = 1$, no prime power in the canonical representation of r can divide n. Thus, $p^a \nmid n$ for any p. So from the general formula $\theta^*(n, r) = \prod_{p|r} (p^a - 2)$. The second quality is straightforward. Δ

Corollary 4.5.2: Let $r = \prod_{p|r} p^a$ be the canonical representation of r. If $r|n$, then

$$\theta^*(n, r) = \prod_{p|r} (p^a - 1) = r \cdot \prod_{p|r} (1 - 1/p^a) = \varphi^*(r).$$

Proof: Since $r|n$, $p^a|n$ for every prime p that divides r, and $\theta^*(n, r) = \prod_{p|r} (p^a - 1)$. Now

$$\prod_{p|r} (p^a - 1) = \prod_{p|r} p^a \cdot \prod_{p|r} (1 - 1/p^a) = r \cdot \prod_{p|r} (1 - 1/p^a).$$

But this last expression is only $\varphi^*(r)$. Hence, if $r|n$, then $\theta^*(n, r) = \varphi^*(r)$. Δ

When $c(n, r)$ was studied earlier, one of the properties listed was the value of the sum of all $c(n, d)$ where d was a divisor of r. A similar evaluation is made here for $\theta^*(n, d)$, but the sum is taken over the unitary divisors of r. Such sums, called unitary convolutions, were introduced in Chapter I. In the unitary case the convolution has an especially simple form since the only unitary divisors of p^a are 1 and p^a so that $\sum_{d \| p^a}$ reduces to two terms. Theorem 4.6 gives the values for four unitary convolutions. Each property is stated and proved separately.

Theorem 4.6: Let $r = \prod_{p|r} p^a$ be the canonical representation of r. Then (i) through (iv) hold.

(i) $$\sum_{d \| r} \theta^*(n,d) = \prod_{p^a | n} p^a \cdot \prod_{p^a \nmid n} (p^a - 1) = (n,r)_* \cdot \sum_{d \| r/(n,r)_*} \theta^*(n,d),$$

Proof: Let r have the given representation. Since $\theta^*(n,r)$ is multiplicative with respect to r, $\sum_{d \| r} \theta^*(n,d)$ is also multiplicative, and the value of this sum can be determined by calculating $\sum_{d \| p^a} \theta^*(n,d)$ for each p such that $p^a \| r$. By Theorem 4.4,

$$\begin{aligned} \sum_{d \| p^a} \theta^*(n,d) &= \theta^*(n,1) + \theta^*(n,p^a) \\ &= 1 + \theta^*(n,p^a) \\ &= \begin{cases} p^a & \text{if } p^a | n \\ p^a - 1 & \text{if } p^a \nmid n \end{cases}. \end{aligned}$$

Thus, $\sum_{d \| r} \theta^*(n,d) = \prod_{p^a | n} p^a \cdot \prod_{p^a \nmid n} (p^a - 1)$.

In Chapter I it was noted that if $r = \prod_{p|r} p^a$, then $(n,r)_* = \prod_{p^a | n} p^a$ and that $d \| r/(n,r)_*$ if and only if $d \| r$ and $(n,d)_* = 1$. Hence,

$$\sum_{d \| r/(n,r)_*} \theta^*(n,d) = \sum_{\substack{d \| r \\ (n,d)_* = 1}} \theta^*(n,d).$$

Theorem 1.18 implies

$$\sum_{\substack{d \| r \\ (n,d)_* = 1}} \theta^*(n,d) = \prod_{p^a \nmid n} (1 + \theta^*(n,p^a))$$

since $\theta^*(n,r)$ is multiplicative. However, $p^a \nmid n$ implies

$\theta^*(n, p^a) = p^a - 2$ so that this last product is $\prod_{p^a \nmid n} (p^a - 1)$. Hence,

$$(n, r)_* \cdot \sum_{d \| r/(n,r)_*} \theta^*(n, d) = \prod_{p^a | n} p^a \cdot \prod_{p^a \nmid n} (p^a - 1) . \qquad \Delta$$

(ii) $$\sum_{d \| r} \theta^*(n, d)/\varphi^*(d) = \prod_{p^a | n} 2 \cdot \prod_{p^a \nmid n} (2p^a - 3)/(p^a - 1)$$

$$= 2^{h((n,r)_*)} \cdot \prod_{p^a \nmid n} (2p^a - 3) \cdot \varphi^*((n, r)_*)/\varphi^*(r) .$$

Proof: Since θ^* and φ^* are both multiplicative, their quotient and hence the sum of their quotients over the unitary divisors of r are both multiplicative. This quotient makes sense since φ^* is never zero. Thus, it is sufficient to consider $\sum_{d \| p^a} \theta^*(n, d)/\varphi^*(d)$. This sum is only $\theta^*(n, 1)/\varphi^*(1) + \theta^*(n, p^a)/\varphi^*(p^a)$ so that

$$\sum_{d \| p^a} \theta^*(n, d)/\varphi^*(d) = \begin{cases} 1 + (p^a - 1)/(p^a - 1) = 2 & \text{if } p^a | n \\ 1 + (p^a - 2)/(p^a - 1) = (2p^a - 3)/(p^a - 1) & \text{if } p^a \nmid n \end{cases} .$$

The first equality of (ii) follows by taking the product of these factors over the appropriate values of p^a.

The product $\prod_{p^a \nmid n} (2p^a - 3)/(p^a - 1)$ can be written in a slightly simpler form by using the fact that $\varphi^*(r/(n, r)_*) = \prod_{p^a \nmid n} (p^a - 1)$. Since $\varphi^*(r/(n, r)_*) = \varphi^*(r)/\varphi^*((n, r)_*)$,

$$\prod_{p^a \nmid n} (2p^a - 3)/(p^a - 1) = \prod_{p^a \nmid n} (2p^a - 3) \cdot \varphi^*((n, r)_*)/\varphi^*(r) .$$

Because the number of distinct prime divisors of $(n, r)_*$, denoted by $h((n, r)_*)$, is equal to the number of distinct primes in the canonical

representation of r which divide n, $\prod_{p^a \| n} 2 = 2^{h((n,r)_*)}$. With this substitution the second equality of (ii) follows. Δ

(iii) $$\sum_{d \| r} 1/\theta^*(n,d) = \prod_{p^a \| n} p^a/(p^a - 1) \cdot \prod_{p^a \nmid n} (p^a - 1)/(p^a - 2)$$

$$= (n,r)_* \varphi^*(r)/\theta^*(n,r)\varphi^*((n,r)_*) .$$

Proof: As in the previous proofs $S = \sum_{d \| p^a} 1/\theta^*(n,d)$ has only two terms. So

$$S = 1/\theta^*(n,1) + 1/\theta^*(n,p^a)$$

$$= \begin{cases} 1 + 1/(p^a - 1) = p^a/(p^a - 1) & \text{if } p^a \| n \\ 1 + 1/(p^a - 2) = (p^a - 1)/(p^a - 2) & \text{if } p^a \nmid n \end{cases} .$$

The first equality of (iii) follows by taking the product of these factors over the appropriate values of p^a.

The second equality follows as a result of breaking the above product up into four separate products. If P denotes the product of the first equality,

$$P = \prod_{p^a \| n} p^a \cdot \prod_{p^a \| n} 1/(p^a - 1) \cdot \prod_{p^a \nmid n} (p^a - 1) \cdot \prod_{p^a \nmid n} 1/(p^a - 2)$$

$$= (n,r)_* \cdot \varphi^*(r/(n,r)_*) \cdot \prod_{p^a \| n} 1/(p^a - 1) \cdot \prod_{p^a \nmid n} 1/(p^a - 2) .$$

Since the product of the last two terms in P is $1/\theta^*(n,r)$, then the second equality of (iii) follows. Δ

(iv) $$\sum_{d \| r} 1/\theta^*(n,d) \sum_{\substack{d \| r \\ (n,d)_* = 1}} 1/\varphi^*(d) = r/\theta^*(n,r) .$$

Proof: By Theorem 1.30

$$\sum_{\substack{d \| r \\ (n,d)_* = 1}} 1/\varphi^*(d) = r \cdot \varphi^*((n,r)_*)/(n,r)_* \varphi^*(r) .$$

Multiplying this expression by that of (iii) yields the desired result. Δ

The final theorem regarding $\theta^*(n,r)$ allows $\theta^*(n,r)$ to be represented as a special convolution of μ^* and φ^*. As was true for many of the previous proofs, this result is based on the fact that μ^* and φ^* are multiplicative and hence upon one of the basic properties of multiplicative functions stated in Theorem 1.18.

Theorem 4.7: If $r = \prod_{p \mid r} p^a$ is the canonical representation of r, then

$$\theta^*(n,r) = \varphi^*(r) \sum_{\substack{d \| r \\ (n,d)_* = 1}} \mu^*(d)/\varphi^*(d) .$$

Proof: Since both μ^* and φ^* are multiplicative, and φ^* is never 0, their quotient is multiplicative. Hence, by Theorem 1.18,

$$\sum_{\substack{d \| r \\ (n,d)_* = 1}} \mu^*(d)/\varphi^*(d) = \prod_{p^a \| n} \left(1 + \mu^*(p^a)/\varphi^*(p^a)\right) .$$

Now $\varphi^*(p^a) = p^a - 1$ and $\mu^*(p^a) = -1$ so that

$$\sum_{\substack{d \| r \\ (n,d)_* = 1}} \mu^*(d)/\varphi^*(d) = \prod_{p^a \| n} (p^a - 2)/(p^a - 1) .$$

Since $\varphi^*(r) = \prod_{p \mid r} (p^a - 1)$,

$$\varphi^*(r) \sum_{\substack{d \| r \\ (n,d)_* = 1}} \mu^*(d)/\varphi^*(d) = \prod_{p \mid r} (p^a - 1) \cdot \prod_{p^a \nmid n} (p^a - 2)/(p^a - 1)$$

$$= \prod_{p^a \mid n} (p^a - 1) \cdot \prod_{p^a \nmid n} (p^a - 2)$$

$$= \theta^*(n, r), \qquad \Delta$$

The Function $c^*(n, r)$

The second unitary analogue to be studied in this chapter is the unitary analogue of Ramanujan's sum. Eckford Cohen [5] used this function to obtain formulas for φ^* and μ^* as well as some unitary analogues of other number-theoretic identities. These results are noted in the ensuing discussion. The main purpose, however, is to study this unitary analogue as a function of two variables while noting the parallels in this development with that of the ordinary Ramanujan sum.

The e-function studied earlier will have its same meaning in this context. Since this function does not depend on divisors, it is inappropriate to consider any kind of unitary analogue for it. But just as this function was central to the definition of $c(n, r)$, it is very important in defining $c^*(n, r)$, the unitary analogue of $c(n, r)$. In fact, the definition is the same except that for $c^*(n, r)$ the summation is over the integers in a semi-reduced residue system modulo r.

Definition 4.2: The function $c^*(n, r)$ is defined by $c^*(n, r) = \sum_x e(nx, r)$ where x ranges over a semi-reduced residue

system modulo r.

It is evident from the definition that $c^*(n, 1) = 1$. Also, the summands in $c^*(n, r)$ are the rth roots of unity, as was also the case for the summands of $c(n, r)$. Before pursuing any other properties of this function, it is helpful to see a calculation made with the definition.

Example 4.3: Suppose the problem is to evaluate $c^*(4, 12)$. The set $T = \{1, 2, 5, 7, 10, 11\}$ is a semi-reduced residue system modulo 12. Thus, $c^*(4, 12) = \sum_x e(4x, 12)$ where $x \in T$. So

$$c^*(4, 12) = e(4, 12) + e(8, 12) + e(20, 12) + e(28, 12) + e(40, 12) + e(44, 12)$$

$$= 3(\cos 2\pi/3 + i \sin 2\pi/3) + 3(\cos 4\pi/3) + i \sin 4\pi/3)$$

$$= 3(-1/2 + i\sqrt{3}/2) + 3(-1/2 - i\sqrt{3}/2) = -3 .$$

If $n = 0$, $c^*(n, r)$ reverts to the familiar function $\varphi^*(r)$ as the following theorem shows.

Theorem 4.8: $c^*(0, r) = \varphi^*(r)$.

Proof: For $n = 0$, $c^*(0, r) = \sum_x 1$ where x ranges through the set of integers in a semi-reduced residue system modulo r. This sum merely counts all those integers in a semi-reduced residue system modulo r, Thus, $c^*(0, r) = \varphi^*(r)$. △

The next result parallels an earlier property for the ordinary Ramanujan sum stated in Theorem 2.8.

Theorem 4.9: If $(a, r) = 1$, then $c^*(an, r) = c^*(n, r)$.

Proof: Suppose x runs through a semi-reduced residue system modulo r. Since $(a, r) = 1$, the values ax also run through a semi-reduced residue system modulo r. Thus, the values of $c^*(an, r)$ and $c^*(n, r)$ are the same. Δ

A complete residue system modulo r can be characterized by the set of integers dz where d ranges over the unitary divisors of r, and for every d, z ranges over a semi-reduced residue system modulo r/d. This result is essential in verifying the formula for the sum of the functions $c^*(n, d)$ where $d \| r$.

Theorem 4.10: $$\sum_{d \| r} c^*(n, d) = \begin{cases} r & \text{if } r \mid n \\ 0 & \text{if } r \nmid n \end{cases}.$$

Proof: In Chapter II it was shown that

$$\sum_{z (\mathrm{mod}\, r)} e(nz, r) = \begin{cases} r & \text{if } r \mid n \\ 0 & \text{if } r \nmid n \end{cases}$$

where the summation is over the integers z in a complete residue system modulo r. Due to the result mentioned prior to this theorem, $\sum_{z (\mathrm{mod}\, r)} e(nz, r) = \sum_{d \| r} \sum_{(z, r/d)_* = 1} e(ndz, r)$. The inner sum here is only $c^*(n, r/d)$. Thus,

$$\sum_{d \| r} c^*(n, r/d) = \sum_{z (\mathrm{mod}\, r)} e(nz, r) = \begin{cases} r & \text{if } r \mid n \\ 0 & \text{if } r \nmid n \end{cases}.$$

The r/d may be replaced by d since this will effect only a change in the order of summation. With this substitution the equation follows. Δ

Recall that in Corollary 2.16.1 it was shown that

$$\sum_{d \mid r} c(n,d) = \begin{cases} r & \text{if } r \mid n \\ 0 & \text{if } r \nmid n \end{cases}.$$

Thus, $\sum_{d \| r} c^*(n,d)$ and $\sum_{d \mid r} c(n,d)$ have the same value even though $c^*(n,r)$ and $c(n,r)$ are not necessarily the same.

The result of the following corollary is not new, but the approach is different from that in [7].

Corollary 4.10.1: If r is an integer, $\sum_{d \| r} \varphi^*(d) = r$.

Proof: Since $c^*(0,d) = \varphi^*(d)$ and $r \mid 0$, then

$$\sum_{d \| r} \varphi^*(d) = \sum_{d \| r} c^*(0,d) = r. \qquad \Delta$$

As one might suspect, $c^*(n,r)$ is a multiplicative function of r. The proof proceeds in the same manner as that for $c(n,r)$, except that semi-reduced residue systems are used instead of reduced residue systems.

Theorem 4.11: The function $c^*(n,r)$ is a multiplicative function of r; that is, if $(r,s) = 1$, then $c^*(n,rs) = c^*(n,r)c^*(n,s)$.

Proof: Let z_1 range over a semi-reduced residue system modulo r and z_2 range over a semi-reduced residue system modulo s. Then

$$\begin{aligned} c^*(n,r)c^*(n,s) &= \sum_{z_1} e(nz_1, r) \sum_{z_2} e(nz_2, s) \\ &= \sum_{z_1} \sum_{z_2} e(n(z_1 s + z_2 r), rs), \end{aligned}$$

this latter equality following from the properties of exponents. Because $\{z : z = z_2 r + z_1 s\}$ ranges over a semi-reduced residue system modulo rs, the double sum above can be written as the single sum $\sum_z e(nz, rs)$ where z ranges over a semi-reduced residue system modulo rs. Thus, $c^*(n, r)c^*(n, s) = c^*(n, rs)$. Δ

Since $c^*(0, r) = \varphi^*(r)$, the following corollary is immediate.

Corollary 4.11.1: The function $\varphi^*(r)$ is multiplicative.

In the preliminaries to this paper the unitary analogue μ^* of the Möbius function was discussed. Just as $c^*(n, r)$ leads to a different way to obtain $\varphi^*(r)$, it also provides an alternate means of studying $\mu^*(r)$. While the results obtained in this manner are not new, the approach is rather interesting. To begin the discussion μ^* is defined in a manner analogous to a property known about μ. In [7] Theorem 4.14 was used as the definition, and Definition 4.3 was derived as a theorem.

Definition 4.3: The unitary analogue of the Möbius function μ, denoted by μ^*, is defined by

$$\sum_{d \| r} \mu^*(d) = \begin{cases} 1 & \text{if } r = 1 \\ 0 & \text{if } r > 1 \end{cases},$$

One immediate consequence of this definition is that $\mu^*(1) = 1$. The following theorem gives the value for $\mu^*(p^a)$ where p is a prime, and a is a positive integer.

Theorem 4.12: If p is a prime, and a is a positive integer, then $\mu^*(p^a) = -1$.

Proof: Since $p^a > 1$, the definition of μ^* implies that $\sum_{d \| p^a} \mu^*(d) = 0$. Because 1 and p^a are the only unitary divisors of p^a, $\mu^*(1) + \mu^*(p^a) = 0$. However, $\mu^*(1) = 1$ implies $\mu^*(p^a) = -1$. Δ

The definition given for μ^* is rather indirect. If $\mu^*(r)$ can be shown to be one of the functions $c^*(n, r)$, there would follow a precise means of calculating μ^*, but more important than this, μ^* would be multiplicative. The proof that $\mu^*(r) = c^*(1, r)$ requires the unitary analogue of the Möbius inversion formula stated in Theorem 1.23.

Theorem 4.13: $\mu^*(r) = c^*(1, r)$.

Proof: Let $g(r) = \sum_{d \| r} c^*(1, d)$. Since

$$\sum_{d \| r} c^*(1, d) = \begin{cases} r & \text{if } r \mid 1 \\ 0 & \text{if } r \nmid 1 \end{cases},$$

then

$$g(r) = \begin{cases} 1 & \text{if } r = 1 \\ 0 & \text{if } r \neq 1 \end{cases}.$$

From the inversion formula, $c^*(1, r) = \sum_{d \| r} \mu^*(d)\, g(r/d)$. However, since

$$g(r/d) = \begin{cases} 1 & \text{if } r = d \\ 0 & \text{if } r \neq d \end{cases},$$

the only nonzero values in the sum for $c^*(1,r)$ occur when $r = d$. Thus, $c^*(1,r) = \mu^*(r)$. Δ

Since $c^*(n,r)$ is a multiplicative function of r, the above theorem implies that μ^* is multiplicative.

Corollary 4.13.1: The function $\mu^*(r)$ is a multiplicative function of r.

Since μ^* is multiplicative, it is rather easy to find its characterization in terms of the prime divisors of r. This characterization is the usual definition for μ^*.

Theorem 4.14: If $h(r)$ denotes the number of distinct prime divisors of r, then $\mu^*(r) = (-1)^{h(r)}$.

Proof: Let $r = \prod_{i=1}^{h(r)} p_i^{a_i}$ be the canonical representation of r. Then

$$\mu^*(r) = \prod_{i=1}^{h(r)} \mu^*(p_i^{a_i}) = \prod_{i=1}^{h(r)} (-1) = (-1)^{h(r)}. \quad \Delta$$

A second application of the unitary inversion formula is seen in the next theorem which shows that $c^*(n,r)$ is a special unitary convolution of μ^* and the identity function. This is analogous to the earlier result of Theorem 2.11.

Theorem 4.15: $c^*(n,r) = \sum_{d \| r,\, d \mid n} \mu^*(r/d) \cdot d$.

Proof: Define the function g by $g(r) = \begin{cases} r & \text{if } r \mid n \\ 0 & \text{if } r \nmid n \end{cases}$. Theorem 4.10 implies that $\sum_{d \| r} c^*(n,d) = g(r)$. By the unitary inversion

formula,

$$c^*(n, r) = \sum_{d \| r} \mu^*(d)\, g(r/d).$$

The only nonzero terms in this expression occur when $r/d \mid n$ and thus when $g(r/d) = r/d$. Therefore, these conditions imply that

$$c^*(n, r) = \sum_{\substack{d \| r \\ r/d \mid n}} \mu^*(d) \cdot r/d = \sum_{d \| r,\, d \mid n} \mu^*(r/d) \cdot d. \qquad \Delta$$

Corollary 4.15.1: $\varphi^*(r) = \sum_{d \| r} \mu^*(d) \cdot r/d$.

Proof: Recall that $\varphi^*(r) = c^*(0, r)$. In the case $n = 0$, the condition $d \mid n$ is redundant. Thus,

$$\varphi^*(r) = \sum_{d \| r} \mu^*(d) \cdot r/d. \qquad \Delta$$

Corollary 4.15.2: Let p be a prime and a any positive integer. Then

$$c^*(n, p^a) = \begin{cases} \varphi^*(p^a) & \text{if } p^a \mid n \\ -1 & \text{if } p^a \nmid n \end{cases}.$$

Proof: The unitary divisors of p^a are only 1 and p^a. If $p^a \mid n$, both of these values are acceptable in the formula of Theorem 4.15. So

$$c^*(n, p^a) = \sum_{d \| p^a} \mu^*(d) \cdot p^a/d$$

$$= \mu^*(1) \cdot p^a + \mu^*(p^a)$$

$$= p^a - 1 \quad \text{or} \quad \varphi^*(p^a) .$$

If $p^a \nmid n$, $d = p^a$ must be discarded. Hence, $c^*(n, p^a) = \mu^*(p^a) = -1$. Δ

This example shows that $c^*(4, 12)$ can be calculated much more easily with this characterization than by the definition.

Example 4.4: First note that $c^*(4, 12) = \sum_{d \| 12, d|4} \mu^*(12/d) \cdot d$, The unitary divisors of 12 are 1, 3, 4, and 12, but the sum is only over 1 and 4 since $3 \nmid 4$ and $12 \nmid 4$. So

$$c^*(4, 12) = \mu^*(12) + \mu^*(3) \cdot 4 = (-1)^2 + (-1)(4) = -3 .$$

A Unitary Convolution of Two Variables

The special unitary convolution in Theorem 4.15 is well worth further study. Since this sum is over the unitary divisors of r which are also divisors of n, the convolution here is more restricted than the usual unitary convolution. Also, the fact that the sum depends on common divisors of r and n implies that the convolution is completely determined by the values it takes on when n and r are powers of the same prime. Moreover, the difference between this convolution and the regular unitary convolution lies only in the choice of d since the terms of the summation do not involve n. This dependence on both n and r leads to a general definition of a function of two variables defined in terms of this restricted convolution.

Definition 4.4: If h(r) and k(r) are multiplicative functions,

$$H(n, r) = \sum_{d \| r, d|n} h(d)k(r/d) .$$

The function $H(n, r)$ like most of the others studied is a multiplicative function of r. But $H(n, r)$ has the added bonus of being multiplicative with respect to n. The importance of these two facts becomes apparent as the discussion continues.

Theorem 4.16: If n is held fixed, $H(n, r)$ is a multiplicative function of r.

Proof: Let $r = st$ where $(s, t) = 1$. The proof is complete if $H(n, r) = H(n, s)H(n, t)$. Since $d \| st$ where $(s, t) = 1$, then $d = d_1 d_2$ where $d_1 \| s$, $d_2 \| t$, and $(d_1, d_2) = 1$. Because $(d_1, d_2) = 1$, then $d_1 d_2 | n$ if and only if $d_1 | n$ and $d_2 | n$. Thus, since h and k are multiplicative,

$$\sum_{d \| r, d | n} h(d)\, k(r/d) = \sum_{d_1 \| s, d_1 | n} h(d_1)\, k(s/d_1) \sum_{d_2 \| t, d_2 | n} h(d_2)\, k(t/d_2)$$

which implies that $H(n, r) = H(n, s)H(n, t)$. Δ

Theorem 4.17: The function $H(n, r)$ is a multiplicative function of n.

Proof: Suppose that $n = n_1 n_2$ where $(n_1, n_2) = 1$. To show that $H(n, r)$ is a multiplicative function of n, it is necessary to show that $H(n, r) = H(n_1, r)H(n_2, r)$. Since $d | n_1 n_2$ where $(n_1, n_2) = 1$, d can be written as the product $d_1 d_2$ where $d_1 | n_1$, $d_2 | n_2$, and $(d_1, d_2) = 1$. Also, $(d_1, d_2) = 1$ implies $d_1 d_2 \| r$ if and only if $d_1 \| r$ and $d_2 \| r$. Thus,

$$\sum_{d \| r, d | n} h(d)\, k(r/d) = \sum_{d_1 \| r, d_1 | n_1} h(d_1)\, k(r/d_1) \sum_{d_2 \| r, d_2 | n_2} h(d_2)\, k(r/d_2)$$

since both h and k are multiplicative. Hence, $H(n, r) = H(n_1, r)H(n_2, r)$, and $H(n, r)$ is a multiplicative function of n. Δ

The function $H(n, r)$ helps to bridge the gap between the discussion of $c^*(n, r)$ and the last function, denoted by $f(n, r)$, to be considered in this chapter. Definition 4.5 describes $f(n, r)$.

Definition 4.5: Let $h(r)$ and $g(r)$ be multiplicative functions. Define $f(n, r)$ by $f(n, r) = \sum_{d \| r, d | n} h(d)\, g(r/d)\, \mu^*(r/d)$ and $f(0, r) = F(r)$.

Since μ^* is multiplicative, it is apparent from the definition that $f(n, r)$ is just a special case of $H(n, r)$ where $k = g \cdot \mu^*$. Hence, $f(n, r)$ enjoys the same properties as $H(n, r)$. This means $f(n, r)$ is a multiplicative function of both n and r. Furthermore, $f(n, r)$ is completely determined by the values it takes on when n and r are powers of the same prime.

The following example shows the calculation of $f(10, 18)$. As such it merely shows how the formula is used. The real interest occurs when h and g are known functions, and $f(n, r)$ turns out to be something known.

Example 4.5: If $f(10, 18)$ is to be evaluated, the sum is over all d in the intersection of $\{1, 2, 9, 18\}$ and $\{1, 2, 5, 10\}$. Thus, $f(10, 18) = h(1)g(18)\mu^*(18) + h(2)g(9)\mu^*(9)$. Since $\mu^*(18) = 1$ and $\mu^*(9) = -1$, then $f(10, 18) = h(1)g(18) - h(2)g(9)$.

One reason for studying $f(n, r)$ is that for special choices of h and g the function $f(n, r)$ reduces to one of the unitary analogues

encountered earlier. This function gives a general category to which the unitary analogues belong. The three theorems which follow are special cases of $f(n, r)$.

Theorem 4.18: If $h(r) = r$ and $g(r) = 1$, then $f(n, r) = c^*(n, r)$.

Proof: Let h and g be the given functions. With these substitutions in the definition of $f(n, r)$,

$$f(n, r) = \sum_{d \| r, d | n} d\mu^*(r/d) .$$

This sum is $c^*(n, r)$ by Theorem 4.15. Hence, $f(n, r) = c^*(n, r)$. Δ

Theorem 4.19: If $h(r) = r$ and $g(r) = 1$, then $F(r) = \varphi^*(r)$.

Proof: From the previous theorem $h(r) = r$ and $g(r) = 1$ imply $f(n, r) = c^*(n, r)$. Thus, $F(r) = f(0, r) = c^*(0, r) = \varphi^*(r)$. Δ

Theorem 4.20: If $h(r) = r$ and $g(r) = \mu^*(r)$, then $F(r) = \sigma^*(r)$.

Proof: Since $F(r) = f(0, r)$, $n = 0$. The condition $d | 0$ of the summation is redundant. So with $h(r) = r$ and $g(r) = \mu^*(r)$,

$$F(r) = \sum_{d \| r} d\mu^*(r/d)\mu^*(r/d) .$$

Because $\mu^*(r/d)$ is either 1 or -1, $F(r) = \sum_{d \| r} d$. But this sum only adds up all the unitary divisors of r so that $F(r) = \sigma^*(r)$. Δ

Suppose now that h and g are arbitrary multiplicative functions. For $n = 0$ the function $f(n, r)$ is defined only in terms of

the unitary convolution since the condition $d \mid 0$ is redundant. If $n = 0$ and $r = p^b$ for any prime p, then $f(0, p^b) = F(p^b)$ can be written as the difference $h(p^b) - g(p^b)$. From this it follows that if $h(p^b) \neq g(p^b)$ for all primes p and all $b > 0$, then $F(p^b) \neq 0$. Moreover, $F(r) \neq 0$ for all positive integers.

Theorem 4.21: For $b > 0$ and p any prime, $F(p^b) = h(p^b) - g(p^b)$.

Proof: With $d = 1$ or p^b,

$$F(p^b) = \sum_{d \parallel p^b} h(d)\, g(p^b/d)\, \mu^*(p^b/d)$$

$$= h(1)\, g(p^b)\, \mu^*(p^b) + h(p^b)\, g(1)\, \mu^*(1) .$$

Because h and g are multiplicative, $h(1) = 1$ and $g(1) = 1$. Thus, $\mu^*(p^b) = -1$ and $\mu^*(1) = 1$ imply $F(p^b) = h(p^b) - g(p^b)$. Δ

Since $f(n, r)$ is multiplicative with respect to r, its value can be determined by looking at $\prod_{p \mid r} f(n, p^b)$ where $r = \prod_{p \mid r} p^b$ is the canonical representation of r. This property is seen in action in the following corollary.

Corollary 4.21.1: If $r \mid n$, then $f(n, r) = F(r)$.

Proof: Since $r \mid n$, the sum in $f(n, r)$ is only over the unitary divisors of r. Now

$$f(n, p^b) = \sum_{d \parallel p^b} h(d)\, g(p^b/d)\, \mu^*(p^b/d)$$

$$= h(p^b) - g(p^b) = F(p^b) .$$

Thus, $f(n, p^b) = F(p^b)$ when $r \mid n$. Hence,

$$f(n, r) = \prod_{p \mid r} f(n, p^b) = \prod_{p \mid r} F(p^b) = F(r). \qquad \Delta$$

Another reason for studying $f(n, r)$ is that it is helpful in the formulation of unitary analogues for the Anderson-Apostol, Landau, and Brauer-Rademacher identities. Although these identities look rather complicated, they are proved without too much difficulty since all of the functions involved are multiplicative. In fact, if one can keep from becoming disenchanted by all the details, these proofs are good examples of how to use the multiplicative property on a function which is multiplicative with respect to both variables.

Suppose that q and p are unequal primes. Since $(q^a, p^b) = 1$, it follows that $f(q^a, p^b) = 1$, and in the determination of f by its multiplicative property the only factors that need to be retained are terms of the form $f(p^a, p^b)$. Lemma 4.22 gives the value of $f(p^a, p^b)$ in the two cases $a < b$ and $a \geq b$. This value involves the function F of Theorem 4.21.

Lemma 4.22: Let a and b be arbitrary positive integers. If p is any prime common to the canonical representations of n and r,

$$f(p^a, p^b) = \begin{cases} -g(p^b) & \text{if } a < b \\ F(p^b) & \text{if } a \geq b \end{cases}.$$

Proof: Recall that $(p^a, p^b)_* = 1$ if $a < b$ and that $(p^a, p^b)_* = p^b$ if $a \geq b$. By Theorem 1.8, $\sum_{d \| p^b, d \mid p^a} = \sum_{d \| (p^a, p^b)_*}$. So

$$f(p^a, p^b) = \sum_{d \| (p^a, p^b)_*} h(d)\, g(p^b/d)\, \mu^*(p^b/d) ,$$

If $a < b$, $f(p^a, p^b) = h(1)\, g(p^b)\, \mu^*(p^b) = -g(p^b)$. If $a \geq b$, $f(p^a, p^b) = h(1)\, g(p^b)\, \mu^*(p^b) + h(p^b)\, g(1)\, \mu^*(1) = h(p^b) - g(p^b) = F(p^b)$. Δ

Theorem 4.23 deals with the unitary analogue of the Anderson-Apostol identity. The theorem's first corollary shows an interesting relationship between $c^*(n, r)$ and the functions φ^* and μ^*. This corollary itself is the analogue of Theorem 2.12. The second corollary gives a relationship for σ^*. In this theorem as well as in those to follow it is assumed that p is a prime occurring in the canonical representations of both n and r. Also, a and b are positive integers.

Theorem 4.23: If g is a multiplicative function and $m = r/(n, r)_*$, then

$$f(n, r) = F(r)\, g(m)\, \mu^*(m)/F(m) .$$

Proof: Since all of the functions involved are multiplicative, it is sufficient to establish the identity for common prime powers of n and r. When $a < b$, $(p^a, p^b)_* = 1$ and $f(p^a, p^b) = -g(p^b)$. In this case $m = r/(n, r)_* = p^b/(p^a, p^b)_* = p^b$. So if R denotes the right side of the desired equality, $R = F(p^b)\, g(p^b)\, \mu^*(p^b)/F(p^b) = -g(p^b)$, and the identity holds for $a < b$.

For $a \geq b$, $(p^a, p^b)_* = p^b$ and $f(p^a, p^b) = F(p^b)$. So $m = 1$, and $R = F(p^b)\, g(1)\, \mu^*(1)/F(1) = F(p^b)$. Hence, the identity is valid for prime powers with $a \geq b$, and it follows that the identity is valid for all n and r. Δ

Corollary 4.23.1: If $m = r/(n,r)_*$, then $c^*(n,r) = \varphi^*(r)\,\mu^*(m)/\varphi^*(m)$.

Proof: Let $h(r) = r$ and $g(r) = 1$ in the definition of $f(n,r)$. With these choices, $f(n,r) = c^*(n,r)$ and $F(r) = \varphi^*(r)$ by Theorems 4.18 and 4.19 respectively. If these substitutions are made in the identity of the previous theorem, the result is immediate. Δ

For notation purposes $\sigma^*(n,r)$ is written for $f(n,r)$ when $h(r) = r$ and $g(r) = \mu^*(r)$. With this notation the next corollary follows.

Corollary 4.23.2: If $m = r/(n,r)_*$, then $\sigma^*(m)\,\sigma^*(n,r) = \sigma^*(r)$.

Proof: If $h(r) = r$ and $g(r) = \mu^*(r)$, Theorem 4.20 implies $F(r) = \sigma^*(r)$ and $F(m) = \sigma^*(m)$. Hence, with $f(n,r) = \sigma^*(n,r)$, $\sigma^*(n,r) = \sigma^*(r)\,\mu^*(m)\,\mu^*(m)/\sigma^*(m)$. But $\mu^*(m)\,\mu^*(m) = 1$ so that $\sigma^*(n,r) = \sigma^*(r)/\sigma^*(m)$. Δ

The second identity is the unitary analogue of the generalized Landau identity.

Theorem 4.24: If g and h are multiplicative,

$$\sum_{\substack{d \,\|\, r \\ (n,d)_*=1}} g(d)/F(d) = h(r)\,F((n,r)_*)/F(r)\,h((n,r)_*)\,.$$

Proof: The identity is investigated for prime powers common to n and r as previously defined. Let L denote the left side of the desired equality and suppose $a < b$. Then

$$L = \sum_{\substack{d \| p^b \\ (p^a, d)_* = 1}} g(d)/F(d) .$$

The unitary divisors of p^b are 1 and p^b, both of which satisfy the condition $(p^a, d)_* = 1$. Hence,

$$L = g(1)/F(1) + g(p^b)/F(p^b) = 1 + g(p^b)/F(p^b) .$$

Since $F(p^b) = h(p^b) - g(p^b)$, $L = h(p^b)/F(p^b)$. If R denotes the right side, $R = h(p^b)\,F(1)/F(p^b)h(1) = h(p^b)/F(p^b)$. Thus, $L = R$ when $a < b$.

Now suppose that $a \geq b$ and recall that this implies $(p^a, p^b)_* = p^b$. In this case the only unitary divisor d of p^b which satisfies $(p^a, d)_* = 1$ is $d = 1$. Hence, $L = g(1)/F(1) = 1$. On the other hand $R = h(p^b)\,F(p^b)/F(p^b)\,h(p^b) = 1$. So $L = R$ for $a \geq b$, and the identity follows for all n and r. △

This identity also offers two corollaries, the first of which was noted earlier in Theorem 1.30. This points out again how many of these results can be approached from altogether different angles. The second corollary gives the value for a special convolution of μ^* and $1/\sigma^*$.

Corollary 4.24.1: $$\sum_{\substack{d \| r \\ (n, d)_* = 1}} 1/\varphi^*(d) = r\,\varphi^*((n, r)_*)/\varphi^*(r) \cdot (n, r)_* .$$

Proof: When $h(r) = r$ and $g(r) = 1$, $F(r) = \varphi^*(r)$. With h and g defined in this manner, the result follows immediately. △

Corollary 4.24.2: $$\sum_{\substack{d \| r \\ (n,d)_* = 1}} \mu^*(d)/\sigma^*(d) = r\sigma^*((n,r)_*)/(n,r)_*\sigma^*(r).$$

Proof: Let $h(r) = r$ and $g(r) = \mu^*(r)$. Since $F(r) = \sigma^*(r)$, the result is obvious. Δ

The unitary analogue of the Brauer-Rademacher identity is a special unitary convolution of μ^* and the quotient h/F, where h is multiplicative. As was also the case for the other identities, when h and g are specially defined, this identity gives a relationship involving some of the known number-theoretic functions.

Theorem 4.25: If h is a multiplicative function of r,

$$F(r) \sum_{\substack{d \| r \\ (n,d)_* = 1}} h(d)\mu^*(r/d)/F(d) = \mu^*(r)f(n,r).$$

Proof: Again let L and R denote the left and right sides of the desired identity and calculate each side for prime powers. If $a < b$, $L = R = g(p^b)$. If $a \geq b$, $L = R = -F(p^b)$. Δ

Corollary 4.25.1: $$\varphi^*(r) \sum_{\substack{d \| r \\ (n,d)_* = 1}} d\mu^*(r/d)/\varphi^*(d) = \mu^*(r)c^*(n,r).$$

Proof: With $h(r) = r$ and $g(r) = 1$ for all r, $f(n,r) = c^*(n,r)$ and $F(r) = \varphi^*(r)$. So this corollary is a direct consequence of the Brauer-Rademacher identity. Δ

Corollary 4.25.2: $$\sigma^*(r) \sum_{\substack{d \| r \\ (n,d)_* = 1}} d\mu^*(r/d)/\sigma^*(d) = \mu^*(r)\sigma^*(n,r).$$

Proof: If $h(r) = r$ and $g(r) = \mu^*(r)$ for all values of r, the identity is immediate. Δ

The study of $\theta^*(n, r)$, $c^*(n, r)$, and $H(n, r)$ provides one with three different settings in which to work with the unitary divisor. It was seen that these functions are really only generalizations of functions of one variable in the unitary context. One of the most significant facts displayed in this chapter is the power of a multiplicative function; many of the results of this chapter were obtained with relative ease since the function was shown first to be multiplicative.

Just as the Ramanujan sum gave some foundation to the study of even functions modulo r, the function $c^*(n, r)$ provides a basis for the study of the class of unitary functions modulo r to be discussed in Chapter V.

CHAPTER V

UNITARY FUNCTIONS MODULO r

Throughout this paper certain parallels between the development of functions based on ordinary divisors and functions based on unitary divisors have been noted. One such parallel exists between the concepts of (n, r) and $(n, r)_*$. Recall from Chapter III that $f(n, r)$ is an even function of n modulo r if and only if $f(n, r) = f((n, r), r)$. A natural question concerns what functions have the property that $f(n, r) = f((n, r)_*, r)$. Definition 5.1 classifies $f(n, r)$ as a special type of function whenever this condition is met.

Definition 5.1: Let $f(n, r)$ be a complex-valued function defined for all n. If $f(n, r) = f((n, r)_*, r)$, then $f(n, r)$ is said to be a unitary function of n modulo r.

Since $c(n, r)$ is an even function modulo r, one might look to $c^*(n, r)$ in hopes of finding an example of a unitary function modulo r. Theorem 5.1 shows that this is a good choice.

Theorem 5.1: The function $c^*(n, r)$ is a unitary function modulo r.

Proof: By Theorem 4.15, $c^*(n, r) = \sum_{d \| r, d | n} \mu^*(r/d) \cdot d$. Since $d | n$ and $d \| r$ if and only if $d \| (n, r)_*$, the above sum may be written as

$$c^*(n, r) = \sum_{\substack{d \| r \\ d | (n, r)_*}} \mu^*(r/d) \cdot d \ .$$

But this last sum is just $c((n, r)_*, r)$. Hence, $c^*(n, r)$ is a unitary function of n modulo r, Δ

Again the definition of unitary modulo r is extended to $f(n, d)$ where $d \| r$. Recall that a similar case was considered for even functions modulo r in Chapter III. The following definition gives the necessary information.

Definition 5.2: Let $f(n, r)$ be a unitary function modulo r. The function $f(n, d)$ is a unitary function modulo r for $d \| r$ if and only if $f(n, d) = f((n, r)_*, d)$.

Theorem 5.2 shows that $c^*(n, d)$ is unitary modulo r for $d \| r$. This result is very important in the later discussion.

Theorem 5.2: The function $c^*(n, d)$ is a unitary function modulo r for every d such that $d \| r$.

Proof: By Theorem 4.15, $c^*(n, d) = \sum_{D \| d, D | n} \mu^*(d/D) \cdot D$. Since $D \| d$ and $D | n$ if and only if $D \| (n, d)_*$, $c^*(n, d) = \sum_{D \| (n, d)_*} \mu^*(d/D) \cdot D$. It can be shown that for $d \| r$, $((n, r)_*, d)_* = (n, d)_*$. Hence, it follows that $c^*(n, d) = c^*((n, r)_*, d)$, and $c^*(n, d)$ is unitary modulo r. Δ

Many of the results of this chapter are unitary analogues of results discussed earlier in Chapters II and III. In fact the motivating force behind this chapter is the desire to find representations for unitary functions modulo r just as it is possible to find representations

for even functions modulo r. The fact that a unitary function modulo r is also an even function modulo r helps in determining these representations and also shows the connection between these two classes of functions.

Theorem 5.3: The set of unitary functions modulo r is a subset of the set of even functions modulo r.

Proof: Suppose that $f(n, r)$ is a unitary function modulo r. The definition of unitary modulo r implies that $f((n, r), r) = f\left(((n, r), r)_*, r\right)$. By Theorem 1.6, $((n, r), r)_* = (n, r)_*$ so that $f((n, r), r) = f((n, r)_*, r)$. But since $f(n, r)$ is unitary modulo r, $f((n, r), r) = f((n, r)_*, r) = f(n, r)$. However, $f((n, r), r) = f(n, r)$ implies $f(n, r)$ is an even function modulo r. Δ

A direct consequence of these first two theorems is that $c^*(n, r)$ is an even function modulo r. As such it is possible to express $c^*(n, r)$ in terms of either of the two representations for even functions modulo r. By using the second representation found in Theorem 3.4, $c^*(n, r)$ can be shown to be a special sum of the ordinary Ramanujan functions $c(n, d)$ for $d \mid r$. The conditions for this sum require new notation.

Definition 5.3: The largest square-free divisor of r is denoted by $\nu(r)$.

Lemma 5.4: For unitary divisors d_1 and d_2 of r, $\nu(d_1) = \nu(d_2)$ if and only if $d_1 = d_2$.

Proof: If $d_1 = d_2$, then $\nu(d_1) = \nu(d_2)$.

Suppose that $\nu(d_1) = \nu(d_2)$ and that $r = \prod_{i=1}^{m} p_i^{a_i}$ is the canonical representation of r. Since $d_1 \| r$ and $d_2 \| r$,

$$d_1 = \prod_{i=1}^{m} p_i^{c_i} \quad \text{where} \quad c_i = 0 \quad \text{or} \quad c_i = a_i \quad \text{for all} \quad i = 1, \ldots, m$$

and

$$d_2 = \prod_{i=1}^{m} p_i^{b_i} \quad \text{where} \quad b_i = 0 \quad \text{or} \quad b_i = a_i \quad \text{for all} \quad i = 1, \ldots, m .$$

By the definition of square-free divisor,

$$\nu(d_1) = \prod_{i=1}^{m} p_i^{c_i'} \quad \text{where} \quad c_i' = 0 \quad \text{or} \quad c_i' = 1$$

and

$$\nu(d_2) = \prod_{i=1}^{m} p_i^{b_i'} \quad \text{where} \quad b_i' = 0 \quad \text{or} \quad b_i' = 1 .$$

Without loss of generality suppose the representations for $\nu(d_1)$ and $\nu(d_2)$ are in ascending order. Then since $\nu(d_1) = \nu(d_2)$, $p_i^{c_i'} = p_i^{b_i'}$ for every $i = 1, \ldots, m$. So either $c_i' = b_i' = 0$ or $c_i' = b_i' = 1$. In either case $c_i = b_i$ so that $p_i^{c_i} = p_i^{b_i}$ for these values of i. Hence, $d_1 = d_2$. Δ

With the added condition that $\nu(d) = \nu(r)$, $c^*(n, r)$ can be written as the sum of $c(n, d)$ where $d | r$. This proof, as well as several of the others in this chapter, is lengthy. It should be noted that length does not necessarily imply difficulty. In working with summations of the kind involved here it is often necessary to rearrange terms or to adjust the index of summation so that some

known property can be applied. These adjustments must be done very carefully so that the summations are still equal.

Theorem 5.5: $c^*(n, r) = \sum_{\substack{d \mid r \\ \nu(d)=\nu(r)}} c(n, d)$.

Proof: From Theorem 4.15, $c^*(n, r) = \sum_{d \| r, d \mid n} d\mu^*(r/d)$. A general formula for $c^*(n, r)$ is to be shown. Since $d \| r$ and $d \mid n$, $d \mid (n, r)$. If $c^*(n, r)$ is defined as a sum over the values d for which $d \mid (n, r)$, the condition $(d, r/d) = 1$ is lost. To avoid this loss, $c^*(n, r)$ may be written as $c^*(n, r) = \sum_{d \mid (n, r)} G^*(d, r/d)$ where $G^*(r_1, r_2) = r_1 \mu^*(r_2) \beta(r_1, r_2)$ and

$$\beta(r_1, r_2) = \begin{cases} 1 & \text{if } (r_1, r_2) = 1 \\ 0 & \text{if } (r_1, r_2) \neq 1 \end{cases}.$$

This second expression for $c^*(n, r)$ is equivalent to the first one since β compensates for the condition $(d, r/d) = 1$. Also, this last expression is just that of an even function modulo r as stated in Theorem 3.4. Hence, by Theorem 3.5, $c^*(n, r) = \sum_{d \mid r} \alpha^*(d, r) c(n, d)$ where $\alpha^*(d, r) = 1/r \sum_{\delta \mid r/d} G^*(r/\delta, \delta)\delta$. The proof is complete if it can be shown that $\alpha^*(d, r) = 1$ when $\nu(d) = \nu(r)$ and is 0 otherwise.

If $G^*(r/\delta, \delta)$ is written in terms of its definition above,

$$\alpha^*(d, r) = 1/r \sum_{\delta \mid r/d} [\mu^*(\delta)\beta(r/\delta, \delta)\, r/\delta] \cdot \delta$$

$$= \sum_{\delta \mid r/d} \mu^*(\delta)\beta(r/\delta, \delta).$$

From the definition of $\beta(r_1, r_2)$,

$$\beta(r/\delta, \delta) = \begin{cases} 1 & \text{if } \delta \| r \\ 0 & \text{if } \delta \nparallel r \end{cases}.$$

Hence, the nonzero terms in $\alpha^*(d, r)$ occur when $\delta \| r$ so that $\alpha^*(d, r) = \sum_{\delta \| r, \delta | r/d} \mu^*(\delta)$. Because a divisor δ of r/d is a unitary divisor of r if and only if $\delta \| (r/d, r)_*$, $\alpha^*(d, r) = \sum_{\delta \| (r/d, r)_*} \mu^*(\delta)$. But the summation property of μ^* implies that

$$\alpha^*(d, r) = \begin{cases} 1 & \text{if } (r/d, r)_* = 1 \\ 0 & \text{if } (r/d, r)_* \neq 1 \end{cases}.$$

Theorem 1.7 implies that $(r/d, r)_* = 1$ if and only if $r = d$. The previous lemma says $r = d$ if and only if $\nu(r) = \nu(d)$. Thus,

$$\alpha^*(d, r) = \begin{cases} 1 & \text{if } \nu(r) = \nu(d) \\ 0 & \text{if } \nu(r) \neq \nu(d) \end{cases},$$

and $c^*(n, r) = \sum_{\substack{d | r \\ \nu(d)=\nu(r)}} c(n, d)$. △

Since $\mu^*(r) = c^*(1, r)$ and $\mu(d) = c(1, d)$, this corollary is a direct consequence of the theorem.

Corollary 5.5.1: $\mu^*(r) = \sum_{\substack{d | r \\ \nu(d)=\nu(r)}} \mu(d)$.

Orthogonality Properties for $c^*(n, r)$

The unitary counterpart of the first orthogonality property for Ramanujan sums is shown in the next theorem. The key to its proof is to write the functions $c^*(a, d_1)$ and $c^*(b, d_2)$ in terms of the ordinary Ramanujan sum by using the previous theorem and then to rearrange the summation so the orthogonality property for ordinary Ramanujan sums can be applied.

Theorem 5.6: If d_1 and d_2 are unitary divisors of r,

$$\sum_{n \equiv a+b \pmod r} c^*(a, d_1) c^*(b, d_2) = \begin{cases} r \cdot c^*(n, d) & \text{if } d_1 = d_2 = d \\ 0 & \text{if } d_1 \neq d_2 \end{cases} .$$

Proof: Let L denote the left side of the desired equation. If $c^*(a, d_1)$ and $c^*(b, d_2)$ are written in terms of the ordinary Ramanujan sum,

$$L = \sum_{n \equiv a+b \pmod r} \sum_{\substack{D_1 \mid d_1 \\ \nu(D_1)=\nu(d_1)}} c(a, D_1) \sum_{\substack{D_2 \mid d_2 \\ \nu(D_2)=\nu(d_2)}} c(b, D_2)$$

$$= \sum_{\substack{D_1 \mid d_1, D_2 \mid d_2 \\ \nu(D_1)=\nu(d_1) \\ \nu(D_2)=\nu(d_2)}} \sum_{n \equiv a+b \pmod r} c(a, D_1) c(b, D_2) .$$

The inner sum of this expression can be evaluated by use of the first orthogonality property for ordinary Ramanujan sums. This says that

$$\sum_{n \equiv a+b \pmod r} c(a, D_1) c(b, D_2) = \begin{cases} r \cdot c(n, D) & \text{if } D_1 = D_2 = D \\ 0 & \text{if } D_1 \neq D_2 \end{cases} .$$

So the nonzero terms in L occur when $D_1 = D_2 = D$, and L may be simplified to

$$L = \sum_{\substack{D|d_1, D|d_2 \\ \nu(D)=\nu(d_1)=\nu(d_2)}} r \cdot c(n, D) .$$

Recall that for unitary divisors d_1 and d_2 of r, $\nu(d_1) = \nu(d_2)$ if and only if $d_1 = d_2$. Hence,

$$L = r \sum_{\substack{D|d_1 \\ \nu(D)=\nu(d_1)}} c(n, D) = \begin{cases} r \cdot c^*(n, d) & \text{if } d_1 = d_2 = d \\ 0 & \text{if } d_1 \neq d_2 \end{cases} . \qquad \Delta$$

For the case $n = 0$ and $a = b$, this property can be expressed in terms of φ^*.

Corollary 5.6.1: If d_1 and d_2 are unitary divisors of r,

$$\sum_{a \pmod r} c^*(a, d_1) c^*(a, d_2) = \begin{cases} r\, \varphi^*(d) & \text{if } d_1 = d_2 = d \\ 0 & \text{if } d_1 \neq d_2 \end{cases} .$$

Proof: If $n = 0$ in the previous theorem,

$$\sum_{a \pmod r} c^*(a, d_1) c^*(a, d_2) = \begin{cases} r \cdot c^*(0, d) & \text{if } d_1 = d_2 = d \\ 0 & \text{if } d_1 \neq d_2 \end{cases} .$$

The result follows from the fact that $c^*(0, d) = \varphi^*(d)$. Δ

The orthogonality property of Theorem 5.6 can be extended rather easily to s variables now that it has been shown for two

variables. This extended form is very useful in the discussion at the end of this chapter.

Theorem 5.7: If $d_1, d_2, \ldots, d_s$ are unitary divisors of r with $s \geq 2$, then

$$\sum_{n \equiv a_1 + \ldots + a_s \pmod{r}} c^*(a_1, d_1)\, c^*(a_2, d_2) \cdots c^*(a_s, d_s)$$

$$= \begin{cases} r^{s-1} c^*(n, d) & \text{if } d_1 = \ldots = d_s = d \\ 0 & \text{otherwise} \end{cases} .$$

Proof: The proof follows from Theorem 5.6 by induction on s. Δ

Representations for Unitary Functions Modulo r

Theorem 5.8 is the first of two representations for unitary functions modulo r. Both of these representations are somewhat similar to the representations for even functions modulo r discussed in Chapter III. In particular, the representation in this theorem is similar to the second representation for even functions modulo r given in Theorems 3.4 and 3.5 as it is based on the function $f(n, r) = \sum_{d \| r,\, d \mid n} g(d, r/d)$. It is clear that $f(n, r)$ defined in this manner is unitary modulo r since $d \| r$ and $d \mid n$ implies $d \| (n, r)_*$. The function μ^* can be used to express g in terms of f by an expression similar to the Möbius Inversion Formula.

Theorem 5.8: If $f(n, r)$ is a unitary function modulo r, $f(n, r)$ has the representation

$$f(n, r) = \sum_{d \parallel r,\, d \mid n} g(d, r/d) \tag{1}$$

where $g(r_1, r_2)$ is determined for $r_1 > 0$, $r_2 > 0$, $(r_1, r_2) = 1$, and $r = r_1 r_2$ by

$$g(r_1, r_2) = \sum_{d \parallel r_1} f(r_1/d, r)\mu^*(d) . \tag{2}$$

Conversely, if $(r_1, r_2) = 1$ and $f(n, r)$ is a unitary function defined by (1), then $g(r_1, r_2)$ has the representation (2).

Proof: Let $f(n, r)$ be a unitary function modulo r and let $g(r_1, r_2)$ be defined by (2) for integers r_1 and r_2 such that $(r_1, r_2) = 1$. Let $Q = \sum_{d \parallel r,\, d \mid n} g(d, r/d)$. It must be shown that $Q = f(n, r)$. Since g is defined by (2),

$$Q = \sum_{\substack{d \parallel r \\ d \mid n}} \left(\sum_{D \parallel d} f(d/D, r)\mu^*(D) \right) .$$

Since $d \parallel r$ and $d \mid n$ if and only if $d \parallel (n, r)_*$, $Q = \sum_{d \parallel (n, r)_*} \sum_{D \parallel d} f(d/D, r)\mu^*(D)$. Because $D \parallel d$, it follows that $\delta = d/D$ is also a unitary divisor of d. It can be shown that the set of integers for which $d \parallel (n, r)_*$ and $D \parallel d$ is the same as the set of integers for which $\delta \parallel (n, r)_*$ and $D \parallel (n, r)_*/\delta$. Hence, $Q = \sum_{\delta \parallel (n, r)_*} f(\delta, r) \sum_{D \parallel (n, r)_*/\delta} \mu^*(D)$. The only nonzero terms in Q occur when $(n, r)_*/\delta = 1$, that is, when $(n, r)_* = \delta$. With $(n, r)_* = \delta$, $Q = f((n, r)_*, r) = f(n, r)$ since f is a unitary function modulo r.

To prove the converse let $P = \sum_{d \| r_1} f(r_1/d, r)\mu^*(d)$ where $f(r_1/d, r)$ is defined by (1). The proof is complete if $P = g(r_1, r_2)$. Since $f(r_1/d, r)$ is defined by (1),

$$P = \sum_{d \| r_1} \left(\sum_{\substack{D \| r \\ D | r_1/d}} g(D, r/D) \right) \mu^*(d) = \sum_{D \| r} g(D, r/D) \sum_{\substack{d \| r_1 \\ D | r_1/d}} \mu^*(d) .$$

Since $D \| r$ and $D | r_1/d$, then $D \| r_1/d$, and it follows that the set of integers for which $d \| r_1$ and $D \| r_1/d$ is the same set of integers for which $D \| r_1$ and $d \| r_1/D$. Hence,

$$P = \sum_{D \| r_1} g(D, r/D) \sum_{d \| r_1/D} \mu^*(d) .$$

The summation property of μ^* implies the only nonzero terms in P occur when $r_1/D = 1$, that is, when $r_1 = D$. Thus,

$$P = \sum_{\substack{D \| r_1 \\ D = r_1}} g(D, r/D) = g(r_1, r/r_1) = g(r_1, r_2) . \qquad \Delta$$

The second representation for unitary functions modulo r is similar in form to the first representation for even functions modulo r given in Theorem 3.3. For the unitary case $c(n, d)$ is replaced by $c^*(n, d)$ and $\varphi(d)$ by $\varphi^*(d)$, and the summations involve unitary divisors. This representation actually comes from two theorems. Before the first theorem is stated, consider the function $f(n, r) = \sum_{d \| r} \alpha(d, r) c^*(n, d)$. It is clear that $f(n, r)$ is a unitary function modulo r since $c^*(n, d)$ is unitary modulo r for all unitary

divisors d of r. Theorem 5.9 considers a unitary function f(n, r) and shows it can be written in the above form. The proof of this representation relies on the fact that a unitary function f(n, r) can be expressed as $f(n,r) = \sum_{d \| r,\, d \mid n} g(d, r/d)$, the representation given in the previous theorem.

Theorem 5.9: If f(n, r) is a unitary function modulo r defined by $f(n,r) = \sum_{d \| r,\, d \mid n} g(d, r/d)$, f(n, r) has the representation

$$f(n,r) = \sum_{d \| r} \alpha(d,r)\, c^*(n,d)$$

where

$$\alpha(d,r) = 1/r \sum_{d_1 \| r/d} g(r/d_1, d_1)\, d_1$$

with $d \| r$.

Proof: Let f(n, r) be a unitary function modulo r defined by $f(n,r) = \sum_{d \| r,\, d \mid n} g(d, r/d)$. Define $\beta(n,d)$ to be d if $d \mid n$ and 0 if $d \nmid n$. Then f(n, r) can be multiplied by $\beta(n,d)/d$, and its value is unchanged. Hence,

$$f(n,r) = \sum_{d \| r} g(d, r/d) \cdot \frac{\beta(n,d)}{d} .$$

By Theorem 4.10, $\beta(n,d) = \sum_{D \| d} c^*(n,D)$ so that

$$f(n,r) = \sum_{d \| r} g(d, r/d)/d \sum_{D \| d} c^*(n,D) .$$

Since $D \| d$ and $d \| r$, $D \| r$. The set of integers for which $d \| r$ and $D \| d$ is the same set of integers for which $D \| r$ and $r/d \| r/D$. So

$$f(n,r) = 1/r \sum_{D \| r} c^*(n,D) \sum_{r/d \| r/D} g(d, r/d) \cdot r/d ,$$

and it follows that $f(n,r)$ has the desired representation. Δ

Theorem 5.10: If $f(n,r)$ is an arbitrary unitary function modulo r, $f(n,r)$ can be represented in the form

$$f(n,r) = \sum_{d \| r} \alpha(d,r) c^*(n,d) \tag{3}$$

where $\alpha(d,r)$ is determined by

$$\alpha(d,r) = \frac{1}{r\varphi^*(d)} \sum_{n (\mathrm{mod}\, r)} f(n,r) c^*(n,d) \quad \text{with} \quad d \| r . \tag{4}$$

Proof: Let $f(n,r)$ be a unitary function modulo r defined by (3). If this representation is multiplied by $c^*(n,\delta)$ where $\delta \| r$ and if this new expression is summed over all n in a residue system modulo r,

$$\sum_{n=1}^{r} f(n,r) c^*(n,\delta) = \sum_{d \| r} \alpha(d,r) \sum_{n=1}^{r} c^*(n,d) c^*(n,\delta) .$$

By Corollary 5.6.1,

$$\sum_{n=1}^{r} c^*(n,d) c^*(n,\delta) = \begin{cases} r\varphi^*(d) & \text{if } d = \delta \\ 0 & \text{if } d \neq \delta \end{cases} .$$

With $d = \delta$, $\sum_{n=1}^{r} f(n,r) c^*(n,\delta) = r\varphi^*(d)\alpha(d,r)$ from which it follows that $\alpha(d,r)$ has the representation (4). Δ

An Application to the Number of Solutions of Linear Congruences

This paper concludes with an example of the type of problem to which this material can be applied. This last section shows that these two representations for unitary functions modulo r help to determine a formula for the number of solutions in a unitary context for linear congruences modulo r. Definition 5.4 describes the congruence to be solved and the function which counts the number of solutions.

Definition 5.4: The function $\omega_s(n, r)$ denotes the number of solutions in x_i modulo r, $i = 1, 2, \ldots, s$, of the congruence

$$n \equiv x_1 + x_2 + \ldots + x_s \pmod{r}$$

where the components x_i are all semiprime to r and $s \geq 1$.

An example at this point is especially helpful.

Example 5.1: The number of solutions of $18 \equiv x_1 + x_2 \pmod{10}$ is to be determined. The definition of $\omega_2(18, 10)$ requires that the components x_i satisfy $(x_i, 10)_* = 1$. This condition is satisfied for $x_i = 1, 3, 7,$ or 9. In addition, the sum $x_1 + x_2$ must be congruent to 18 modulo 10 where x_1 and x_2 are chosen from $\{1, 3, 7, 9\}$. For $x_1 = 1$ and $x_2 = 7$ the semiprime condition is met and $18 \equiv 8 \pmod{10}$. Likewise $x_1 = 7$ and $x_2 = 1$ also provide a solution. If $x_1 = 9$, then $x_2 = 9$. Both values satisfy the semiprime requirements, and their sum solves the congruence. Hence, they provide a solution. If $x_1 = 3$, then $x_2 = 5$. These values solve the congruence but $(5, 10)_* \neq 1$. Hence, $x_1 = 3$ and $x_2 = 5$ do not

provide a solution. Since solutions are obtained only from possible sums of 1, 3, 7, and 9, all solutions have been determined and $\omega_2(18, 10) = 3$. It is important to note that both the solutions $x_1 = 1$, $x_2 = 7$ and $x_1 = 7$, $x_2 = 1$ are counted.

The function $\omega_1(n, r)$, denoted by $\omega(n, r)$, is the number of solutions of the congruence $n \equiv x_1 \pmod r$ such that $(x_1, r)_* = 1$. This function is very helpful in deriving a general formula for $\omega_s(n, r)$. To this end it is shown first that $\omega(n, r)$ is a unitary function modulo r. This proof relies on the fact that if $a \equiv b \pmod r$, $(a, r)_* = (b, r)_*$.

Theorem 5.11: The function $\omega(n, r)$ is a unitary function modulo r.

Proof: To show that $\omega(n, r)$ is a unitary function modulo r, first note that $\omega((n, r)_*, r)$ is the number of solutions of $(n, r)_* \equiv x_1 \pmod r$ such that $(x_1, r)_* = 1$. So $\omega((n, r)_*, r)$ is 1 or 0 according to whether $((n, r)_*, r)_* = 1$ or $((n, r)_*, r)_* \neq 1$. Since $((n, r)_*, r)_* = (n, r)_*$, $\omega((n, r)_*, r)$ is 1 or 0 according to whether $(n, r)_* = 1$ or $(n, r)_* \neq 1$. But since $\omega(n, r)$ is also 1 or 0 according to these same conditions, $\omega(n, r) = \omega((n, r)_*, r)$, and $\omega(n, r)$ is unitary modulo r. Δ

Example 5.2: This example is really a continuation of the previous one and provides some motivation for the generalization of $\omega(n, r)$ to $\omega_s(n, r)$. The purpose of this example is to show that

$$\omega_2(18, 10) = \sum_{18 \equiv a_1 + a_2 \pmod{10}} \omega(a_1, 10)\, \omega(a_2, 10).$$

Recall that $\omega(a_1, 10)$ is the number of solutions of $a_1 \equiv x_1 \pmod{10}$ where $(x_1, 10)_* = 1$. Similarly, $\omega(a_2, 10)$ is the number of solutions of $a_2 \equiv x_2 \pmod{10}$ where $(x_2, 10)_* = 1$. Now $\omega(a_1, 10)$ is 1 or 0 depending on whether $(a_1, 10)_* = 1$ or $(a_1, 10)_* \neq 1$. Likewise, $\omega(a_2, 10)$ is 1 or 0 depending on whether $(a_2, 10)_* = 1$ or $(a_2, 10)_* \neq 1$. So $\omega(a_1, 10)\,\omega(a_2, 10) = 1$ if $(a_1, 10)_* = 1$ and $(a_2, 10)_* = 1$. But these are the conditions for which it is possible to have a solution for $18 \equiv a_1 + a_2 \pmod{10}$. Hence,

$$\omega_2(18, 10) = \sum_{18 \equiv a_1 + a_2 \pmod{10}} \omega(a_1, 10)\,\omega(a_2, 10) .$$

Theorem 5.12 gives a general formula for finding $\omega_s(n, r)$ for $s \geq 1$. Its proof is a culmination of many of the key results of this chapter. Both of the representations for unitary functions modulo r are used as well as the extended form of the orthogonality property. While the arithmetic involved in using this formula is often time consuming, at least the counting procedure employed in Example 5.1 is eliminated.

Theorem 5.12: The function $\omega_s(n, r)$ is a unitary function modulo r and is given by the formula

$$\omega_s(n, r) = (\varphi^*(r))^s / r \cdot \sum_{d \,\|\, r} (\mu^*(d)/\varphi^*(d))^s c^*(n, d) .$$

Proof: For $s = 1$, $\omega(n, r)$ is the number of solutions for $n \equiv x_1 \pmod{r}$ where $(x_1, r)_* = 1$. Since $\omega(n, r)$ is 1 if $(n, r)_* = 1$ and is 0 if $(n, r)_* \neq 1$, it is possible to write $\omega(n, r)$ as a sum of $\mu^*(d)$ over the unitary divisors d of $(n, r)_*$. Furthermore, since

$d \| (n, r)_*$ if and only if $d | n$ and $d \| r$, then $\omega(n, r) = \sum_{d \| r,\, d | n} \mu^*(d)$. So $\omega(n, r)$ is in the form (1) of Theorem 5.8 where $g(r_1, r_2) = \mu^*(r_1)$, $r_1 r_2 = r$, and $(r_1, r_2) = 1$. This representation for $\omega(n, r)$ plus the fact that $\omega(n, r)$ is unitary modulo r implies that

$$\omega(n, r) = \sum_{d \| r} \alpha(d, r)\, c^*(n, d)$$

where

$$\alpha(d, r) = 1/r \sum_{d_1 \| r/d} g(r/d_1, d_1)\, d_1 \quad \text{and} \quad d \| r .$$

The task is to simplify $\alpha(d, r)$. Since $g(r_1, r_2) = \mu^*(r_1)$,

$$\alpha(d, r) = 1/r \sum_{d_1 \| r/d} \mu^*(r/d_1)\, d_1 = 1/r \sum_{\substack{d_1 \| r/d \\ (d_1 d_2 = r/d)}} \mu^*(d\, d_2)\, d_1 .$$

Since $(d, d_2) = 1$ and μ^* is multiplicative,

$$\alpha(d, r) = \mu^*(d)/r \cdot \sum_{\substack{d_1 \| r/d \\ (d_1 d_2 = r/d)}} \mu^*(d_2)\, d_1 .$$

By Corollary 4.15.1, this summation is just $\varphi^*(r/d)$, and

$$\alpha(d, r) = \mu^*(d)/r \cdot \varphi^*(r/d) .$$

Since $d \| r$, $\varphi^*(r/d) = \varphi^*(r)/\varphi^*(d)$. So with this value for $\alpha(d, r)$,

$$\omega(n, r) = \varphi^*(r)/r \cdot \sum_{d \| r} \left(\mu^*(d)/\varphi^*(d) \right) \cdot c^*(n, d) ,$$

and the theorem is true for $s = 1$.

From the definition of $\omega_s(n, r)$ it follows that

$$\omega_s(n, r) = \sum_{n \equiv a_1 + \ldots + a_s \pmod r} \omega(a_1, r) \cdots \omega(a_s, r) ,$$

Each $\omega(a_i, r)$ can be replaced by its value determined above so that

$$\omega_s(n, r) = \sum_{n \equiv a_1 + \ldots + a_s \pmod r} \prod_{i=1}^{s} \varphi^*(r)/r \sum_{d_i \| r} \left(\frac{\mu^*(d_i)}{\varphi^*(d_i)} \right) \cdot c^*(a_i, d_i)$$

$$= (\varphi^*(r)/r)^s \sum_{\substack{d_i \| r \\ i=1, \ldots, s}} \frac{\mu^*(d_1) \cdots \mu^*(d_s)}{\varphi^*(d_1) \cdots \varphi^*(d_s)} \sum_{n \equiv a_1 + \ldots + a_s \pmod r} c^*(a_1, d_1) \cdots c^*(a_s, d_s).$$

By the extended orthogonality property the summation involving the functions $c^*(a_i, d_i)$ is $r^{s-1} c^*(n, d)$ if $d_1 = d_2 = \ldots = d_s = d$. Otherwise, its value is 0. Therefore,

$$\omega_s(n, r) = (\varphi^*(r)/r)^s \sum_{d \| r} (\mu^*(d)/\varphi^*(d))^s \cdot r^{s-1} c^*(n, d)$$

$$= (\varphi^*(r))^s / r \cdot \sum_{d \| r} (\mu^*(d)/\varphi^*(d))^s \cdot c^*(n, d) .$$

The fact that $\omega_s(n, r)$ is unitary modulo r follows by repeated application of the property $((n, r)_*, r)_* = (n, r)_*$ along with the definition of $\omega_s(n, r)$. △

Example 5.3: As a final note to this theorem it is interesting to calculate $\omega_2(18, 10)$ by use of the formula. Hence,

$$\omega_2(18, 10) = (\varphi^*(10))^2 / 10 \cdot \sum_{d \| 10} (\mu^*(d)/\varphi^*(d))^2 \cdot c^*(18, d) .$$

With $\varphi^*(10) = 4$,

$$\omega_2(18, 10) = 16/10[1 + c^*(18, 2) + 1/16 \cdot c^*(18, 5) + 1/16 \cdot c^*(18, 10)].$$

By Corollary 4.15.2, $c^*(18, 2) = 1$ and $c^*(18, 5) = -1$. Since $c^*(n, r)$ is multiplicative with respect to r, $c^*(18, 10) = (1) \cdot (-1) = -1$. So $\omega_2(18, 10) = 16/10[1 + 1 - 1/16 - 1/16] = 16/10 \cdot 15/8 = 3$.

Since $\omega_s(n, r)$ is characterized by a unitary convolution of a product of multiplicative functions, $\omega_s(n, r)$ is itself multiplicative. The function $J_s(n, r) = r\omega_s(n, r)/(\varphi^*(r))^s$ is also multiplicative. Since $\varphi^*(r) \neq 0$ for any value of r, it is possible to determine conditions under which $\omega_s(n, r) = 0$ by examining $J_s(n, r)$. Lemma 5.13 shows the value of $J_s(n, r)$ for $r = p^a$ where p is a prime. This value is used to prove Theorem 5.14 which gives a characterization for which $\omega_s(n, r) = 0$. Proofs are omitted since they follow much the same pattern as previous ones.

Lemma 5.13: If $J_s(n, r) = r\omega_s(n, r)/(\varphi^*(r))^s$,

$$J_s(n, p^a) = \begin{cases} 1 + (-1)^s/(p^a - 1)^{s-1} & \text{if } p^a \mid n \\ 1 + (-1)^{s+1}/(p^a - 1)^s & \text{if } p^a \nmid n \end{cases},$$

where p is a prime.

Theorem 5.14: The function $\omega_s(n, r) = 0$ if and only if one of the following sets of conditions holds:

(i) $s = 1$, $(n, r)_* \neq 1$;

(ii) s is even, r is twice an odd integer, and n is odd;

(iii) s is odd, $s > 1$, r is twice an odd integer, and n is even.

Condition (i) of the above theorem is obvious from the definition of $\omega(n, r)$. This last example shows some congruences solved quickly by conditions (ii) and (iii).

Example 5.4: Consider the congruence $15 \equiv x_1 + x_2 + x_3 + x_4 \pmod{10}$. In this case $s = 4$, $r = 10 = 2 \cdot 5$, and $n = 15$. Hence, (ii) implies that $\omega_4(15, 10) = 0$. Now look at $16 \equiv x_1 + x_2 + x_3 \pmod{6}$. Here $s = 3$, $r = 6 = 2 \cdot 3$, and $n = 16$ so that (iii) yields $\omega_3(16, 6) = 0$. It is important to remember that the number of components x_i must be greater than 1 in order to use (iii).

In summary, the set of unitary functions modulo r is contained in the set of even functions modulo r and hence can be characterized by two representations. One of these representations is defined in terms of $c^*(n, r)$, a result analogous to what was true for even functions modulo r. These representations aid in the determination of a formula for the number of solutions of a linear congruence of s variables in the unitary context.

The study of functions of two variables could be pursued to include other relations, other applications, and new functions based on k-ary divisors. The beginning here indicates the direction such a study would take.

BIBLIOGRAPHY

(1) Agnew, Jeanne. Explorations in Number Theory. Monterey, California: Brooks/Cole Publishing Company, 1972.

(2) Cohen, Eckford. "Rings of Arithmetic Functions." Duke Mathematical Journal, Vol. 19, (1952), 115-129.

(3) Cohen, Eckford. "A Class of Arithmetical Functions." Proceedings of the National Academy of Sciences, Vol. 41, (1955), 939-944.

(4) Cohen, Eckford. "An Extension of Ramanujan's Sum. II. Additive Properties." Duke Mathematical Journal, Vol. 22, (1955), 543-550.

(5) Cohen, Eckford. "Arithmetical Functions Associated with the Unitary Divisors of an Integer." Mathematische Zeitschrift, Vol. 74, (1960), 66-80.

(6) Cohen, Eckford. "Unitary Functions (Mod r)." Duke Mathematical Journal, Vol. 28, (1961), 475-485.

(7) Gautier, Gloria. "Unitary Divisors and Associated Number-Theoretic Functions." (Unpublished M. S. thesis, Oklahoma State University, 1970).

(8) Grosswald, Emil. Topics from the Theory of Numbers. New York: The Macmillan Company, 1966.

(9) Hamel, Thomas Ray. "Selected Algebraic Structures of Number-Theoretic Functions." (Unpublished Ed. D. thesis, Oklahoma State University, 1971).

(10) Hardy, G. H. and E. M. Wright. An Introduction to the Theory of Numbers. Oxford at the Claredon Press, 1960.

(11) McCarthy, P. J. "Some More Remarks on Arithmetical Identities." Portugaliae Mathematica, Vol. 21, (1962), 45-57.

(12) Morgado, José. "Unitary Analogue of the Nagell Totient Function." Portugaliae Mathematica, Vol. 21, (1962), 221-232.

(13) Suryanarayana, D. "The Number of k-ary Divisors of an Integer." Monatshefte für Mathematik, Vol. 72, (1968), 445-450.

VITA

Gloria Jane Gautier

Candidate for the Degree of

Doctor of Education

Thesis: NUMBER-THEORETIC FUNCTIONS OF TWO VARIABLES

Major Field: Higher Education

Biographical:

Personal Data: Born in Enid, Oklahoma, September 25, 1945, the daughter of Mr. and Mrs. Howard S. Gautier.

Education: Graduated from Ames High School, Ames, Oklahoma, in May, 1963; received the Bachelor of Science degree with high honors from Northwestern State College, Alva, Oklahoma, in May, 1967, with a major in mathematics; received the Master of Science degree from Oklahoma State University in May, 1970; completed requirements for the Doctor of Education degree at Oklahoma State University in May, 1973.

Professional Experience: Student Teaching Assistant, Department of Mathematics, Northwestern State College, Fall, 1966; Graduate Teaching Assistant, Department of Mathematics and Statistics, Oklahoma State University, 1967-1972.

Professional Membership: Kappa Delta Pi.