

AN ABSTRACT OF THE THESIS OF

Joanne J. Cogswell for the Masters of Science

in Mathematics presented on May 7, 1992

Title The Theory of Indices Modulo n

Abstract Approved: Essam Alattaen

This thesis is intended for an audience familiar with basic elementary number theory and acquainted with some abstract algebra; it discusses the theory of indices modulo n . Chapter 1 presents definitions and theorems from elementary number theory that form a background for the rest of this paper. Because primitive roots play a crucial role in the study of indices, we discuss primitive roots in Chapter 2. In that chapter, we establish which moduli possess primitive roots. The objective of Chapter 3 is the study of scalar indices and their properties. We find that in both theory and application, indices are analogous to logarithms. This analogy is emphasized and is used as a motivation to introduce certain results. Applications of scalar indices in solving various types of congruence equations is discussed and illustrated. Also included is the construction of a modular slide rule based on index theory. Chapter 4 extends the theory as developed in the previous chapters to make it applicable to arbitrary moduli, this by means of vector indices. Again, applications are given. Chapter 5 takes a more general approach to the topic and looks at the theory of indices from an algebraic point

of view. This approach leads in a natural way to the generalization of indices to finite cyclic groups as well as to the direct product of two finite cyclic groups. We conclude by suggesting a direction for further study of this topic.

THE THEORY OF INDICES MODULO n

A Thesis

Presented to
the Division of Mathematics
Emporia State University

In Partial Fulfillment
of the Requirements for the Degree
Master of Science

by
Joanne J. Cogswell
May 1992

Essam Abatteen

Approved for the Major Division

Jaye Vowell

Approved for the Graduate Council

CONTENTS

CHAPTER 1:	INTRODUCTION	1
CHAPTER 2:	PRIMITIVE ROOTS	9
CHAPTER 3:	SCALAR INDICES	30
CHAPTER 4:	VECTOR INDICES	75
CHAPTER 5:	PRIMITIVE ROOTS AND INDICES FROM AN ALGEBRAIC VIEWPOINT	91
CHAPTER 6:	SUMMARY AND CONCLUSION	103

LIST OF TABLES OF INDICES

Table 1:	Indices Modulo 19	39
Table 2:	Indices Modulo 9	41
Table 3:	Indices Modulo 11	41
Table 4:	Indices Modulo 13	41
Table 5:	Indices Modulo 41	53

LIST OF FIGURES

Figure 1:	Two Aligned Straight-Edges	55
Figure 2:	Straight-Edges as Used for Addition	56
Figure 3:	Logarithm Slide Rule	57
Figure 4:	Modular Straight-Edge Slide Rule	58
Figure 5:	Modular Straight-Edge Slide Rule as Used for Multiplication	60
Figure 6:	A-, C-Scales on Modular Circular Slide Rule	62
Figure 7:	D-Scale on Modular Circular Slide Rule	62
Figure 8:	A-, C-, D-Scales on Modular Circular Slide Rule	63
Figure 9:	D-, R-Scales on Modular Circular Slide Rule	68
Figure 10:	Modular Circular Slide Rule	70

Chapter 1

INTRODUCTION

This paper will discuss the theory of indices modulo n and will indicate surprisingly many parallels between it and the better known theory of logarithms, though we will not be discussing logarithms as such. The nature of this study is more that of a compilation of existent ideas than that of a development of original ideas. The theorems, proofs, discussions, and examples constitute a melding of materials from multiple sources so that, even if possible, in most instances crediting a single source would not be appropriate, though occasionally a specific source is cited. We provide a list of references at the end of the paper.

Chapter 1 will present basic background from elementary number theory that is needed for the rest of this paper. Since the concept of indices depends on the concept of the order of an integer mod n and on the concept of primitive roots, Chapter 2 will deal with order and primitive roots. Chapter 3 will consider scalar indices for moduli that have primitive roots. It will present theory and applications. Chapter 4 will extend the notion of indices to apply to any modulus. Finally, Chapter 5 will discuss the topic of indices from an algebraic viewpoint.

The material in this paper is intended for an audience familiar with basic elementary number theory and, for

Chapter 5, some acquaintance with abstract algebra is necessary.

The remainder of this chapter consists of definitions and theorems, presented without discussion or proof, that are fundamental to elementary number theory and thus are a background for the rest of this paper.

1.1 DEFINITIONS

1. An integer b is said to be divisible by an integer $a \neq 0$, in symbols $a|b$, if there exists some integer c such that $b = ac$. We write $a \nmid b$ to indicate that b is not divisible by a .

2. Let a and b be given integers, with at least one of them different from zero. The greatest common divisor of a and b , denoted by $\gcd(a,b)$, is the positive integer d satisfying

- (1) $d|a$ and $d|b$,
- (2) if $c|a$ and $c|b$, then $c \leq d$.

3. Two integers a and b , not both of which are zero, are said to be relatively prime whenever $\gcd(a,b) = 1$.

4. The least common multiple of two nonzero integers a and b , denoted by $\text{lcm}[a,b]$, is the positive integer m satisfying

- (1) $a|m$ and $b|m$,

(2) if $a|c$ and $b|c$, with $c > 0$, then $m \leq c$.

5. An integer $p > 1$ is called a prime number, or simply prime, if its only positive divisors are 1 and p . An integer greater than 1 which is not a prime is termed a composite.

6. Let n be a fixed positive integer. Two integers a and b are said to be congruent modulo n , symbolized by $a \equiv b \pmod{n}$, if n divides the difference $a-b$; that is, provided that $a-b = kn$ for some integer k .

7. If $a \equiv b \pmod{n}$, then b may be said to be a residue of a modulo n . For each integer a , let \bar{a} be the set of all residues of a modulo n ; that is, $\bar{a} = \{x | x \text{ is an integer and } x \equiv a \pmod{n}\}$. Such a set \bar{a} is called a congruence or residue class modulo n .

8. A set C of integers is said to be a complete residue system modulo n if every integer is congruent modulo n to exactly one integer of the set C .

9. Let a be an integer. Then an integer x is said to be an inverse of a mod n if it satisfies the congruence equation $ax \equiv 1 \pmod{n}$. An inverse of $a \pmod{n}$ is denoted by a^* .

10. For $n \geq 1$, let $\phi(n)$ denote the number of the positive integers that are less than n and that are relatively prime to n .

11. Given $n \geq 1$, a set of $\phi(n)$ integers which are relatively prime to n and which are incongruent modulo n is called a reduced residue system modulo n ; that is, a reduced residue system modulo n are those elements of a complete residue system modulo n which are relatively prime to n .

1.2 THEOREMS

1.1 (Division Algorithm) Given integers a and b , with $b > 0$, there exist unique integers q and r satisfying $a = qb + r$, where $0 \leq r < b$.

1.2 For positive integers a and b , $\gcd(a,b)\text{lcm}[a,b] = ab$.

Corollary

Given positive integers a and b , $\text{lcm}[a,b] = ab$ if and only if $\gcd(a,b) = 1$.

1.3 (Fundamental Theorem of Arithmetic) Every positive integer $n > 1$ can be expressed as a product of primes; this representation is unique, apart from the order in which the factors occur.

Corollary

Any positive integer $n > 1$ can be written uniquely in a canonical form $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, where, for $i = 1, 2, \dots, r$, each k_i is a positive integer and each p_i is a prime, with $p_1 < p_2 < \dots < p_r$.

1.4 For arbitrary integers a and b , $a \equiv b \pmod{n}$ if and only if a and b leave the same nonnegative remainder when divided by n .

1.5 Let $n > 0$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold:

- (1) $a \equiv a \pmod{n}$.
- (2) If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.
- (3) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
- (4) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.
- (5) If $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$ and $ac \equiv bc \pmod{n}$.
- (6) If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for any positive integer k .
- (7) If $a \equiv b \pmod{n}$ and $d|n$ for $d > 0$, then $a \equiv b \pmod{d}$.

1.6 If $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{n/d}$, where

$$d = \gcd(c, n).$$

Corollary 1

If $ca \equiv cb \pmod{n}$ and $\gcd(c, n) = 1$, then
 $a \equiv b \pmod{n}$.

Corollary 2

If $ca \equiv cb \pmod{p}$ and $p \nmid c$, where p is a prime number, then $a \equiv b \pmod{p}$.

1.7 If m_i for $i = 1, 2, \dots, k$ are positive integers, then
 $a \equiv b \pmod{m_i}$ for each i if and only if
 $a \equiv b \pmod{\text{lcm}[m_1, m_2, \dots, m_k]}$.

1.8 A set S of integers is a complete residue system mod n
if and only if

- (1) S has n elements,
- (2) Any two elements in S are not congruent mod n .

1.9 The linear congruence $ax \equiv b \pmod{n}$ has a solution if
and only if $d|b$, where $d = \gcd(a, n)$. If $d|b$, then the
congruence has d mutually incongruent solutions modulo n .

1.10 (Chinese Remainder Theorem) Let n_1, n_2, \dots, n_r be
positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then
the system of linear congruences

$$x \equiv a_1 \pmod{n_1},$$

$$x \equiv a_2 \pmod{n_2},$$

⋮

$$x \equiv a_r \pmod{n_r}$$

has a simultaneous solution, which is unique modulo the integer $n = n_1 n_2 \dots n_r$.

1.11 (Fermat's Little Theorem) If p is a prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Corollary

If p is a prime, then $a^p \equiv a \pmod{p}$.

1.12 $\phi(n) = n-1$ if and only if n is prime.

1.13 If p is a prime and $k > 0$, then

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k(1-(1/p)).$$

1.14 For $n > 2$, $\phi(n)$ is an even integer.

1.15 For each positive integer a , we have $\sum_{d|a} \phi(d) = a$.

1.16 (Lagrange) If p is a prime and

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, \text{ and } a_n \not\equiv 0 \pmod{p}$$

is a polynomial of degree $n \geq 1$ with integral coefficients, then the congruence $f(x) \equiv 0 \pmod{p}$ has at most n incongruent solutions modulo p .

1.17 (Euler) If n is a positive integer and a an integer such that $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Chapter 2

PRIMITIVE ROOTS

Since primitive roots play a crucial role in the study of indices, we devote this chapter to the investigation of this concept. Included will be a discussion concerning which integers possess primitive roots and which do not.

2.1 THE ORDER OF AN INTEGER MODULO n

By Euler's Theorem, if n is a positive integer and if a is an integer relatively prime to n , then $a^{\phi(n)} \equiv 1 \pmod{n}$. Therefore, at least one positive integer x satisfies the congruence relation $a^x \equiv 1 \pmod{n}$. Consequently, by the Well-Ordering Principle, there is a least positive integer x satisfying this congruence relation. This leads to the following definition.

Definition:

Let a and n be relatively prime positive integers. Then the least (or smallest) positive integer x such that $a^x \equiv 1 \pmod{n}$ is called the order of a modulo n . We denote the order of a modulo n by $\text{ord}_n(a)$.

Example:

To find $\text{ord}_7(2)$, we compute the least positive integer x such that $2^x \equiv 1 \pmod{7}$. We find that $2^1 \not\equiv 1 \pmod{7}$,

$2^2 \not\equiv 1 \pmod{7}$, but $2^3 \equiv 1 \pmod{7}$. Therefore, $\text{ord}_7(2) = 3$.

Similarly, $\text{ord}_7(3) = 6$.

Remarks:

1. The order of a positive integer a modulo n does not exceed $\phi(n)$; that is, $\text{ord}_n(a) \leq \phi(n)$.
2. In the literature of number theory, the order of a modulo n is often called the "exponent of a modulo n " or the "exponent to which a belongs modulo n ."

Now we proceed to establish several fundamental results related to the concept of order.

Theorem 2.1

If a and n are relatively prime positive integers, then a positive integer x is a solution of the congruence $a^x \equiv 1 \pmod{n}$ if and only if $\text{ord}_n(a) \mid x$.

Proof:

If $\text{ord}_n(a) \mid x$, then x is a multiple of $\text{ord}_n(a)$; that is, $x = k \text{ord}_n(a)$, where k is a positive integer. Hence $a^x = a^{k \text{ord}_n(a)} = (a^{\text{ord}_n(a)})^k \equiv 1 \pmod{n}$. Conversely, if $a^x \equiv 1 \pmod{n}$, we first use the Division Algorithm to write $x = q \text{ord}_n(a) + r$, $0 \leq r < \text{ord}_n(a)$. From this equation, we see that $a^x = a^{q \text{ord}_n(a) + r} = (a^{\text{ord}_n(a)})^q a^r \equiv a^r \pmod{n}$; the last congruence, follows from $a^{\text{ord}_n(a)} \equiv 1 \pmod{n}$. Since

$a^x \equiv a^r \pmod{n}$ and $a^x \equiv 1 \pmod{n}$, then $a^r \equiv 1 \pmod{n}$.

From the inequality $0 \leq r < \text{ord}_n(a)$, we conclude that $r = 0$, since, by definition, $y = \text{ord}_n(a)$ is the least positive integer such that $a^y \equiv 1 \pmod{n}$. Because $r = 0$, we have $x = q \text{ord}_n(a)$. Therefore, $\text{ord}_n(a) \mid x$. \square

Corollary

If a and n are relatively prime integers with $n > 0$, then $\text{ord}_n(a) \mid \phi(n)$.

Proof:

Since $\text{gcd}(a, n) = 1$, Euler's Theorem tells us that $a^{\phi(n)} \equiv 1 \pmod{n}$. Using theorem 2.1 we conclude that $\text{ord}_n(a) \mid \phi(n)$. \square

We can use the corollary as a shortcut when we compute orders. The following example illustrates the procedure.

Example:

To find the order of 5 modulo 17, we first note that $\phi(17) = 16$. Since the only positive divisors of 16 are 1, 2, 4, 8, and 16, by the corollary these are the only possible values of $\text{ord}_{17}(5)$. Since $5^1 \not\equiv 1 \pmod{17}$, $5^2 \not\equiv 1 \pmod{17}$, $5^4 \not\equiv 1 \pmod{17}$, $5^8 \not\equiv 1 \pmod{17}$, but $5^{16} \equiv 1 \pmod{17}$, we conclude that $\text{ord}_{17}5 = 16$.

Before we prove our next result concerning the order of an integer, we need the following lemma.

Lemma 2.2

If a and b are integers such that $\gcd(a,b) = 1$, then $\gcd(a^n, b^n) = 1$ for any positive integer n .

Proof:

First we prove $\gcd(a^n, b) = 1$. We do this by mathematical induction on n . For $n = 1$, $\gcd(a^1, b) = 1$ is given. Assume $\gcd(a^k, b) = 1$ for some integer $k \geq 1$. We need to prove $\gcd(a^{k+1}, b) = 1$. Since $\gcd(a^k, b) = 1$, we have $1 = a^kx + by$ and $\gcd(a, b) = 1$; then $1 = au + bv$ for some integers x, y, u, v . Then $1 = (a^kx + by) \cdot (au + bv)$ and $1 = a^{k+1}(xu) + b(a^kxv + yau + byv)$. Therefore, $\gcd(a^{k+1}, b) = 1$. So by induction, $\gcd(a^n, b) = 1$ for any positive integer n . Since $\gcd(a^n, b) = \gcd(b, a^n)$, by the above argument, we have $\gcd(b^n, a^n) = \gcd(a^n, b^n) = 1$. □

Theorem 2.3

If a and b are relatively prime positive integers, then $a^i \equiv a^j \pmod{n}$, where i and j are nonnegative integers, if and only if $i \equiv j \pmod{\text{ord}_n(a)}$.

Proof:

Suppose that $i \equiv j \pmod{\text{ord}_n(a)}$, and assume that i and j are chosen so that $j \leq i$. Then we have $\text{ord}_n(a) \mid (i-j)$ and hence $i = j + k \cdot \text{ord}_n(a)$ for some positive integer k . Thus $a^i = a^{j+k \cdot \text{ord}_n(a)} = a^j (a^{\text{ord}_n(a)})^k \equiv a^j \pmod{n}$ because $a^{\text{ord}_n(a)} \equiv 1 \pmod{n}$. Thus $a^i \equiv a^j \pmod{n}$. Conversely, assume that

$a^i \equiv a^j \pmod{n}$ and $j \leq i$. Since a and n are relatively prime we have $\gcd(a,n) = 1$ and by Lemma 2.2 we have $\gcd(a^j,n) = 1$. Now, $a^i \equiv a^j \cdot a^{i-j} \equiv a^j \pmod{n}$ implies, by Corollary 1 to Theorem 1.6, the cancellation of a^j : $a^{i-j} \equiv 1 \pmod{n}$. By Theorem 2.1 it follows that $\text{ord}_n(a) \mid (i-j)$ and hence $i \equiv j \pmod{\text{ord}_n(a)}$. □

Corollary

The integers $a, a^2, \dots, a^{\text{ord}_n(a)}$ are incongruent modulo n .

Proof:

To the contrary, we assume that $a^i \equiv a^j \pmod{n}$ for some integers i and j such that $i \neq j$ and $1 \leq i < j \leq \text{ord}_n(a)$. By the theorem, since $a^i \equiv a^j \pmod{n}$ is assumed to hold, then $i \equiv j \pmod{\text{ord}_n(a)}$. But since i and j are both less than or equal to $\text{ord}_n(a)$, then $j-i < \text{ord}_n(a)$ and $\text{ord}_n(a) \mid (i-j)$ implies $\text{ord}_n(a) \leq j-i$ and this leads to $\text{ord}_n(a) < \text{ord}_n(a)$, a contradiction. □

A natural question one may ask is "Is it possible to express $\text{ord}_n(a^h)$, where h is a positive integer, in terms of $\text{ord}_n(a)$?" The following theorem provides the answer.

Theorem 2.4

If $\text{ord}_n(a) = k$ and h is a positive integer, then $\text{ord}_n(a^h) = k / \gcd(k,h)$.

Proof:

Let $d = \gcd(h, k)$. Then $h = dl_1$ and $k = dl_2$, where $\gcd(l_1, l_2) = 1$. We need to show $(k / \gcd(h, k)) = ((dl_2) / d) = l_2 = \text{ord}_n(a^h)$. First we will show $(a^h)^{l_2} \equiv 1 \pmod{n}$. Because $(a^h)^{l_2} = (a^{dl_1})^{l_2} = (a)^{dl_1 l_2} = (a^{dl_2})^{l_1} = (a^k)^{l_1}$, and since $k = \text{ord}_n(a)$, then $a^k \equiv 1 \pmod{n}$. This implies $(a^k)^{l_1} \equiv 1 \pmod{n}$, which implies $(a^h)^{l_2} \equiv 1 \pmod{n}$. Thus by Theorem 2.1, $\text{ord}_n(a^h) \mid l_2$. Now let $r = \text{ord}_n(a^h)$. Then $r \mid l_2$ and $(a^h)^r \equiv 1 \pmod{n}$. Also $1 \equiv (a^h)^r \equiv (a^{dl_1})^r \equiv (a)^{dl_1 r} \pmod{n}$, and since $\text{ord}_n(a) = k$, then $k \mid dl_1 r$. Hence $dl_2 \mid dl_1 r$, and thus $l_2 \mid l_1 r$. But $\gcd(l_1, l_2) = 1$. Therefore $l_2 \mid r$. As previously noted, $r \mid l_2$. Therefore $r = l_2 = k/d = k/\gcd(h, k)$. □

Corollary 1

If $\text{ord}_n(a) = k$, then $\text{ord}_n(a^h) = k$ if and only if $\gcd(h, k) = 1$.

Corollary 2

If $\text{ord}_n(a) = k$, there are exactly $\phi(k)$ numbers of the set $\{a, a^2, \dots, a^k\}$ which has order k modulo n .

Proof:

By definition of $\phi(k)$, there are $\phi(k)$ integers less than k and relatively prime to k . Also, by corollary 1 of Theorem 2.4, if $\text{ord}_n(a) = k$, then $\text{ord}_n(a^h) = k$ if and only if h is relatively prime to k . Thus in the set $\{a, a^2, \dots, a^k\}$

the elements with order k modulo n are those elements a^h where h is an integer relatively prime to k and there are $\phi(k)$ of them. □

2.2 DEFINITION AND BASIC PROPERTIES OF PRIMITIVE ROOTS

Given a positive integer n , we are interested in integers a such that $\text{ord}_n(a) = \phi(n)$.

Definition:

If a and n are relatively prime positive integers such that $\text{ord}_n(a) = \phi(n)$, then a is called a primitive root modulo n , or simply a primitive root of n .

According to this definition a is a primitive root modulo n if $a^{\phi(n)} \equiv 1 \pmod{n}$ and $a^k \not\equiv 1 \pmod{n}$ for all positive integers $k < \phi(n)$. It is understood that, when looking for primitive roots, one may consider only the elements of the least residue system modulo n for, if a is a primitive root mod n and $a \equiv b \pmod{n}$, then b is also a primitive root mod n .

Example:

$a = 3$ is a primitive root modulo 7 since $\text{ord}_7(3) = 6 = \phi(7)$. Likewise 5 is a primitive root modulo 7. However $n = 8$ has no primitive roots. To see this, note that the only integers less than 8 and relatively prime to 8

are 1, 3, 5, and 7 but $\text{ord}_8(1) = 1$, $\text{ord}_8(3) = 2$, $\text{ord}_8(5) = 2$, and $\text{ord}_8(7) = 2$. Since $\phi(8) = 4$, there are no primitive roots modulo 8.

In section 2.3 we will determine all of the integers possessing primitive roots.

Remark: The notion of a primitive root modulo n bears some analogy to the algebraic notion of a primitive root of unity.

The next theorem deals with a reduced residue system. We are going to show that if, for positive integer n , there is a primitive root modulo n , then each reduced residue system modulo n can be expressed as a geometric progression of the primitive root.

Theorem 2.5

Let a and n be relatively prime positive integers. Then a is a primitive root modulo n if and only if the integers $a, a^2, \dots, a^{\phi(n)}$ form a reduced residue system modulo n .

Proof:

Assume that a is a primitive root modulo n . By Lemma 2.2 we have $\text{gcd}(a^k, n) = 1$ for $k = 1, 2, \dots, \phi(n)$. Hence a^k is relatively prime to n for any integer k . We need show only

that no two of these powers of a are congruent mod n . Assume that $a^i \equiv a^j \pmod{n}$ for some integers i and j such that $1 \leq i, j \leq \phi(n)$. By Theorem 2.3 this implies $i \equiv j \pmod{\phi(n)}$, and this implies $i = j$, a contradiction. Hence no two of these powers are congruent mod n . Because $a, a^2, \dots, a^{\phi(n)}$ are $\phi(n)$ distinct integers relatively prime to n , they form a reduced residue system mod n . For the converse, assume that $a, a^2, \dots, a^{\phi(n)}$ form a reduced residue system, where, by Euler's Theorem, $a^{\phi(n)} \equiv 1 \pmod{n}$. But no smaller power is congruent to 1 mod n , so a is a primitive root modulo n . □

Example:

Let $n = 14$ and $a = 3$ is a primitive root modulo 14. Then $\text{ord}_{14}(3) = 6 = \phi(14)$. One can verify that the set of integers $\{3, 3^2, 3^3, 3^4, 3^5, 3^6\}$ form a reduced residue system mod 14.

Corollary

If n has a primitive root, then it has exactly $\phi(\phi(n))$ primitive roots.

Proof:

Let r be a primitive root modulo n . Then Theorem 2.5 tells us that the integers $r, r^2, \dots, r^{\phi(n)}$ form a reduced residue system modulo n . By Corollary 1 to Theorem 2.4 we

know that r^u is a primitive root modulo n if and only if $\gcd(u, \phi(n)) = 1$. Since there are exactly $\phi(\phi(n))$ such integers u , there are exactly $\phi(\phi(n))$ primitive roots modulo n . □

Example:

To find all of the primitive roots of $n = 14$, check all of the integers less than and relatively prime to 14. The primitive roots are among them. In this case the numbers we need to check are 1, 3, 5, 9, 11, and 13. Note that $\phi(14) = 6$.

$$1^1 \equiv 1 \pmod{14} \text{ implies } \text{ord}_{14}(1) = 1; 1 \neq \phi(14).$$

$3^6 \equiv 1 \pmod{14}$ implies $\text{ord}_{14}(3) = 6$; $6 = \phi(14)$ so 3 is a primitive root modulo 14.

$5^6 \equiv 1 \pmod{14}$ implies $\text{ord}_{14}(5) = 6$; $6 = \phi(14)$ so 5 is a primitive root modulo 14.

$$9^3 \equiv 1 \pmod{14} \text{ implies } \text{ord}_{14}(9) = 3; 3 \neq \phi(14).$$

$$11^3 \equiv 1 \pmod{14} \text{ implies } \text{ord}_{14}(11) = 3; 3 \neq \phi(14).$$

$$13^2 \equiv 1 \pmod{14} \text{ implies } \text{ord}_{14}(13) = 2; 2 \neq \phi(14).$$

Notice that there are two primitive roots modulo 14, 3 and 5. This agrees with the corollary since $\phi(\phi(14)) = \phi(6) = 2$ primitive roots modulo 14.

Remark:

From the previous proof, it follows that, if a is a primitive root mod n , then the numbers in the set

$S = \{a^k: 1 \leq k \leq \phi(n), \text{ and } \gcd(k, \phi(n)) = 1\}$ are incongruent primitive roots of n .

2.3 THE EXISTENCE OF PRIMITIVE ROOTS

In this section our objective is to determine which integers have primitive roots. As a characterization of all integers that possess primitive roots, we will be proving the following theorem. Thus the other theorems which precede it in this section will be called lemmas.

Theorem 2.6 (Gauss)

An integer $n > 1$ has a primitive root if and only if n is one of the following $2, 4, p^k, 2p^k$, where p is an odd prime and k an arbitrary positive integer.

We begin by showing that certain integers cannot have primitive roots. This will be followed by lemmas necessary in establishing which integers do have primitive roots.

Lemma 2.7

If $n > 2$ and $m > 2$ are two relatively prime integers, then the composite number mn does not have a primitive root.

Proof:

By Theorem 1.14 for $n > 2$, $\phi(n)$ is an even integer. Thus $\phi(m)$ and $\phi(n)$ are even integers. Further, $\text{lcm}[\phi(m), \phi(n)] < \phi(m)\phi(n) = \phi(mn)$ because

$\text{lcm}[\phi(m), \phi(n)] \leq (\phi(m)\phi(n))/2$ since $\phi(m)$ and $\phi(n)$ are even.

Suppose $\text{gcd}(a, mn) = 1$. Then $\text{gcd}(a, m) = 1$ and $\text{gcd}(a, n) = 1$.

By Euler's Theorem, $a^{\phi(m)} \equiv 1 \pmod{m}$. Let

$\text{lcm}[\phi(m), \phi(n)] = k\phi(m)$ for some integer k . Then $(a^{\phi(m)})^k \equiv 1^k$

\pmod{m} . This is equivalent to $a^{\text{lcm}[\phi(m), \phi(n)]} \equiv 1 \pmod{m}$. By

a similar argument, $a^{\text{lcm}[\phi(m), \phi(n)]} \equiv 1 \pmod{n}$. From Theorem

1.2 and Theorem 1.7, it follows that

$a^{\text{lcm}[\phi(m), \phi(n)]} \equiv 1 \pmod{mn}$. Since $\text{lcm}[\phi(m), \phi(n)] < \phi(mn)$,

$\text{ord}_a(mn) \neq \phi(mn)$ and therefore mn does not have a primitive root. □

Corollary

Let $n = m_1 m_2 \dots m_k$ for $k \geq 2$, where all m_i are distinct and relatively prime integers and all $m_i > 2$. Then n has no primitive root.

Proof:

Let $q = m_1 m_2 \dots m_{k-1}$. Then $n = qm_k$. Since q and m_k are relatively prime, and $q > 2$ and $m_k > 2$, by the lemma, n has no primitive root. □

Lemma 2.8

If $k \geq 3$ is an integer, then the integer s^k does not have a primitive root.

Proof:

Let a be an integer relatively prime to 2^k . Thus a must be an odd integer. By Euler's Theorem, $a^{\phi(2^k)} \equiv 1 \pmod{2^k}$.

Claim: $a^{2^{k-2}} \equiv 1 \pmod{2^k}$.

The claim will be established by mathematical induction on $k \geq 3$. We will consider $k = 3$ first. Since a is odd, let $a = 2r+1$ for some integer r . Then $a^2 = 4r^2 + 4r + 1 = 4r(r+1) + 1$. This implies that $4r(r+1) + 1 \equiv 1 \pmod{2^3}$ because r and $r+1$ are two consecutive integers; that is, one is even and one odd. Next, assume $a^{2^{g-2}} \equiv 1 \pmod{2^g}$. We must show $a^{2^{g-1}} \equiv 1 \pmod{2^{g+1}}$. We know that $a^{2^{g-2}}$ is an odd integer. Let $a^{2^{g-2}} = 2^g \cdot s + 1$ for some integer s . Squaring both sides of the equality, we get

$$\begin{aligned}(a^{2^{g-2}})^2 &= (1 + s \cdot 2^g)^2 \\ a^{2^{g-1}} &= 1 + 2s \cdot 2^g + s^2 \cdot 2^{2g} \\ &= s^2 \cdot 2^{2g} + s \cdot 2^{g+1} + 1 \\ &= 2^{g+1}(s^2 2^{g-1} + s) + 1. \text{ This implies that}\end{aligned}$$

$2^{g+1}(s^2 2^{g-1} + s) + 1 \equiv 1 \pmod{2^{g+1}}$, which implies

$a^{2^{g-1}} \equiv 1 \pmod{2^{g+1}}$. Thus, by mathematical induction,

$a^{2^{k-2}} \equiv 1 \pmod{2^k}$ for any odd a and $k \geq 3$. Since

$\phi(2^k) = 2^k - 2^{k-1} = 2^{k-1}(2-1) = 2^{k-1}$, then $2^{k-2} < \phi(2^k)$. Therefore, for all odd a , $\text{ord}_{2^k}(a) \neq \phi(2^k)$ and thus 2^k does not have a primitive root. □

Lemma 2.7 and its corollary and Lemma 2.8 rule out the existence of primitive roots for some integers, specifically those integers of a form other than the ones included in Theorem 2.6. Our objective now is to prove the existence of

primitive roots for odd primes. We begin with the following lemma.

Lemma 2.9

Let p be an odd prime and let d be any positive divisor of $p-1$. If there exists an integer a which has order $d \pmod{p}$, then there are exactly $\phi(d)$ incongruent integers which have order $d \pmod{p}$.

Proof:

Let a be an integer such that $\text{ord}_p(a) = d$. By the corollary to Theorem 2.3, it follows that the numbers in the set $S = \{a, a^2, \dots, a^d\}$ are incongruent \pmod{p} . Corollary 2 to Theorem 2.4 (setting $k = d$) implies that among the elements of the set S there are exactly $\phi(d)$ integers which have order $d \pmod{p}$. Thus it remains to show that every integer which has order $d \pmod{p}$ is congruent \pmod{p} to an element of S . Consider the congruence equation $x^d \equiv 1 \pmod{p}$. . . (*). Since $\text{ord}_p(a) = d$, then $a^d \equiv 1 \pmod{p}$ and hence a is a solution to the congruence equation (*). Also, every power of a satisfies the congruence equation (*). In particular, the d numbers a, a^2, \dots, a^d are solutions to (*). But by Theorem 1.16, (*) has at most d incongruent solutions since the modulus is prime. Further, because the numbers a, a^2, \dots, a^d are incongruent, these numbers must be all of the solutions of (*). Thus every integer which satisfies the congruence equation (*) must be

congruent mod p to an element of S . But any integers which have order d mod p satisfy (*) and there are $\phi(d)$ such integers. That is, since there are at most d incongruent solutions to (*) and there are $\phi(d)$ integers with order d mod p and all of them solve (*), then there are exactly $\phi(d)$ incongruent integers which have order d modulo p . \square

Lemma 2.10

If p is an odd prime, then p has a primitive root.

Proof:

Let $R = \{1, 2, \dots, p-1\}$ be the least positive reduced residue system mod p . For each $a \in R$, $\text{ord}_p(a) \mid \phi(p) = p-1$.

Let $\{d_1, \dots, d_r\}$ be the set of all positive divisors of $p-1$, and let $f(d_i)$ denote the number of elements of R which have order d_i mod p . Clearly $\sum_{i=1}^r f(d_i) = p-1$. Moreover,

from Theorem 1.15, we have $\sum_{i=1}^r \phi(d_i) = p-1$. From Lemma 2.9,

we have $f(d_i) = \phi(d_i)$, provided that $f(d_i) \neq 0$. But since $\phi(d_i) > 0$, it follows that $f(d_i) \neq 0$ because otherwise we

would have $p-1 = \sum_{i=1}^r f(d_i) < \sum_{i=1}^r \phi(d_i) = p-1$, which is

impossible. Thus we have proved that for any divisor d of

$p-1$, there are $\phi(d)$ elements of R whose order mod p is equal

to d . In particular, if $d = p-1$, then there are $\phi(p-1)$

elements of R whose order mod p is $p-1 = \phi(p)$ and hence they

are primitive roots mod p . This completes the proof that

every odd prime has a primitive root. \square

We turn next to prove the existence of primitive roots for integers of the form p^k where p is an odd prime and $k \geq 2$. In seeking primitive roots mod p^k , it is natural to consider as candidates the primitive roots mod p . In other words, do p and p^k share the same primitive roots? Let g be a primitive root mod p . We will determine first under what conditions g might also be a primitive root mod p^2 . Since g is a primitive root mod p , we have $g^{p-1} \equiv 1 \pmod{p}$ and, since $\phi(p^2) = p(p-1) > p-1$, then g will certainly not be a primitive root mod p^2 if $g^{p-1} \equiv 1 \pmod{p^2}$. Therefore the condition $g^{p-1} \not\equiv 1 \pmod{p^2}$ is a necessary condition for a primitive root g mod p to also be a primitive root mod p^2 . Remarkably, this condition also is sufficient for g to be a primitive root mod p^2 and, even more generally, mod p^k where $k \geq 2$. We need the following lemma to prove the above observation.

Lemma 2.11

Let g be a primitive root mod p such that $g^{p-1} \not\equiv 1 \pmod{p^2}$. Then for every $k > 2$, we have $g^{\phi(p^{k-1})} \not\equiv 1 \pmod{p^k}$.

Proof:

The proof is by induction on k . For $k = 2$, it follows from the hypothesis. Now assume that $g^{\phi(p^{m-1})} \not\equiv 1 \pmod{p^m}$ for some integer $m \geq 2$. By Euler's theorem, we have

$g^{\phi(p^{m-1})} \equiv 1 \pmod{p^{m-1}}$. Thus $g^{\phi(p^{m-1})} = 1 + rp^{m-1}$ for some integer r . The integer r must satisfy the relation $p \nmid r$ because, if $p|r$, then $r = pb$ for some integer b and $g^{\phi(p^{m-1})} = 1 + p^m b$. This implies $g^{\phi(p^{m-1})} \equiv 1 \pmod{p^m}$, which would contradict our assumption. Raising both sides of the relation $g^{\phi(p^{m-1})} = 1 + rp^{m-1}$ to the p^{th} power and applying the Binomial Theorem, we have $g^{p\phi(p^{m-1})} = (1 + rp^{m-1})^p$. This implies $g^{\phi(p^m)} = 1 + rp^m + ((r^2 p(p-1))/2)p^{2(m-1)} + \dots + r^p p^{mp-p}$ and we have $g^{\phi(p^m)} \equiv 1 + rp^m \pmod{p^{m+1}}$. Now, since $p \nmid r$ as established earlier, we must have $g^{\phi(p^m)} \not\equiv 1 \pmod{p^{m+1}}$. This is because $g^{\phi(p^m)} \equiv 1 \pmod{p^{m+1}}$ implies a contradiction: $g^{\phi(p^m)} \equiv 1 \pmod{p^{m+1}}$ and $g^{\phi(p^m)} \equiv 1 + rp^m \pmod{p^{m+1}}$ imply $0 \equiv rp^m \pmod{p^{m+1}}$ which in turn implies $p^{m+1} | rp^m$ and thus $p|r$, a contradiction. Therefore the theorem is true for $m + 1$ and thus for any integer $k \geq 2$. □

We are now ready to state and prove the previously noted remarkable observation regarding the necessary and sufficient condition for the existence of primitive roots mod p^k .

Lemma 2.12

Let p be an odd prime. Then we have:

- (1) If g is a primitive root mod p , then g is also a primitive root mod p^k for any integer $k \geq 1$ if and only if $g^{p-1} \not\equiv 1 \pmod{p^2}$. . . (*)

(2) There is at least one primitive root $g \pmod p$ which satisfies (*). Thus there exists at least one primitive root $\pmod{p^k}$ if $k \geq 2$.

Proof:

(1) Let g be a primitive root $\pmod p$ and assume g is also a primitive root $\pmod{p^k}$ for all $k \geq 1$. Then, if g is such a primitive root, in particular, it is a primitive root $\pmod{p^2}$ and, since $\phi(p^2) = p(p-1) > p-1$, this implies $g^{p-1} \not\equiv 1 \pmod{p^2}$ because, for g to be a primitive root $\pmod{p^2}$, $\phi(p^2)$ is the least exponent of g . Now we prove the converse. Suppose that g is a primitive root $\pmod p$ which satisfies (*). We must show that g is also a primitive root $\pmod{p^k}$ for any $k \geq 2$. Let $\text{ord}_{p^k}(g) = t$. We must show $t = \phi(p^k)$. Since $\text{ord}_{p^k}(g) = t$, we have $g^t \equiv 1 \pmod{p^k}$; consequently $g^t \equiv 1 \pmod p$ since p is a divisor of p^k . But since g is a primitive root $\pmod p$ and $g^t \equiv 1 \pmod p$, we have $\phi(p) \mid t$ (Theorem 2.1). Thus $t = q\phi(p)$ for some integer q . Now $t \mid \phi(p^k)$, since $\text{ord}_{p^k}(g) \leq \phi(p^k)$ and by Theorem 2.1, so $q\phi(p) \mid \phi(p^k)$. But $\phi(p^k) = p^{k-1}(p-1)$. Thus $q(p-1) \mid p^{k-1}(p-1)$. This implies $q \mid p^{k-1}$. Therefore $q = p^r$ for some integer $r \leq k-1$. Hence $t = p^r(p-1)$. If we prove that $r = k-1$, then $t = \phi(p^k)$ and we are finished. We proceed by contradiction. We assume the contrary that $r < k-1$. Thus $r \leq k-2$ and we have $t = p^r(p-1) \mid p^{k-2}(p-1) = \phi(p^{k-1})$. Therefore, since $\phi(p^{k-1})$ is a multiple of t and $g^t \equiv 1 \pmod{p^k}$, this would imply $g^{\phi(p^{k-1})} \equiv 1 \pmod{p^k}$ which contradicts Lemma 2.11 so $r = k-1$.

(2) Let g be a primitive root mod p . If $g^{p-1} \not\equiv 1 \pmod{p^2}$, there is nothing to prove since by part (1) g is also a primitive root mod p^k . However, if $g^{p-1} \equiv 1 \pmod{p^2}$ then g is not a primitive root mod p^k . We are going to show that, in this case, another integer, $h = g + p$, satisfies the required condition $h^{p-1} \not\equiv 1 \pmod{p^2}$ and thus is a primitive root modulo p^k . We begin by assuming $g^{p-1} \equiv 1 \pmod{p^2}$ as given. By the Binomial Theorem, we have

$$h^{p-1} = (g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p + \frac{(p-1)(p-2)}{2} g^{p-3}p^2 + \dots + p^{p-1}.$$

This implies

$$\begin{aligned} h^{p-1} &\equiv g^{p-1} + p(p-1)g^{p-2} \pmod{p^2} \\ &\equiv g^{p-1} + p^2g^{p-2} - pg^{p-2} \pmod{p^2} \\ &\equiv g^{p-1} - pg^{p-2} \pmod{p^2}. \end{aligned}$$

Proceeding by contradiction, we assume $h^{p-1} \equiv 1 \pmod{p^2}$.

Subtracting the last equation from the original

$g^{p-1} \equiv 1 \pmod{p^2}$, results in $pg^{p-2} \equiv 0 \pmod{p^2}$. But we cannot have $pg^{p-2} \equiv 0 \pmod{p^2}$ for this would imply $g^{p-2} \equiv 0 \pmod{p}$ and, raising both sides to the p^{th} power, $g^{p-1} \equiv 0 \pmod{p}$, thus contradicting the fact that g is a primitive root mod p . Hence we cannot have $h^{p-1} \equiv 1 \pmod{p^2}$. So it must be the case that $h^{p-1} \not\equiv 1 \pmod{p^2}$. □

Lemma 2.13

Let g be a primitive root mod p^k , where p is an odd prime and k a positive integer. Then

- (1) If g is odd, g is also a primitive root mod $2p^k$.
 (2) If g is even, $g + p^k$ is a primitive root mod $2p^k$.

Proof:

(1) Let $r = \text{ord}_{2p^k}(g)$. We are going to show that $r = \phi(2p^k)$.
 Now since, by Euler's Theorem, $g^{\phi(2p^k)} \equiv 1 \pmod{2p^k}$ and by
 Theorem 2.1 $r | \phi(2p^k)$ and $\phi(2p^k) = \phi(2)\phi(p^k) = \phi(p^k)$, then
 $r | \phi(p^k)$. On the other hand, since $g^r \equiv 1 \pmod{2p^k}$ and p^k is
 a factor of $2p^k$, by Theorem 1.5 we have $g^r \equiv 1 \pmod{p^k}$.

Hence $\phi(p^k) | r$ since g is a primitive root mod p^k . Therefore
 $r = \phi(p^k) = \phi(2p^k)$ and hence g is a primitive root mod $2p^k$.

(2) If g is even, then $g+p^k$ is odd. Moreover, $g + p^k$ is a
 primitive root mod p^k . This follows from Lemma 2.12(2).

Now we apply the argument in part (1) to $g + p^k$ instead of
 g .

□

At this point a summary is in order. From Lemmas 2.12
 and 2.13, it follows that integers n of the form $n = p^k$ or
 $2p^k$, where p is an odd prime and k a positive integer, have
 primitive roots. Moreover, it follows by direct
 computations that $g = 1$ is a primitive root mod 2 and $g = 3$
 is a primitive root mod 4. Thus all of the integers
 mentioned in the statement of Theorem 2.6 have primitive
 roots. On the other hand, Lemmas 2.7 and 2.8 show that an
 integer n cannot have a primitive root if it is other than

one of the forms specified in the statement of Theorem 2.6.
In effect, then, we have completed a proof of Theorem 2.6.

Chapter 3

SCALAR INDICES

The objective of this chapter is the study of scalar indices and their basic properties. Throughout the rest of this study, scalar indices will be called simply indices. As we shall see, in both theory and application, indices are analogous to logarithms. The analogy, in theory and application, will be emphasized throughout this chapter and the rest of this paper. Moreover, the analogy between the two theories will be used as a motivation to introduce certain results.

3.1 THE DEFINITION AND BASIC PROPERTIES OF SCALAR INDICES

Let n be an integer which has a primitive root and let g be one of the primitive roots mod n . By Theorem 2.5 we know that the set of integers $\{g, g^2, \dots, g^{\phi(n)}\}$ form a reduced residue system mod n , and since $g^{\phi(n)} \equiv 1 \pmod{n}$, it follows that $\{1, g, g^2, \dots, g^{\phi(n)-1}\}$ also form a reduced residue system mod n .

As an illustration, take $n = 7$, $g = 3$ is a primitive root mod 7 since $\text{ord}_7(3) = 6$.

$$3^1 \equiv 3 \pmod{7}$$

$$3^2 \equiv 2 \pmod{7}$$

$$3^3 \equiv 6 \pmod{7}$$

$$3^4 \equiv 4 \pmod{7}$$

$$3^5 \equiv 5 \pmod{7}$$

$$3^6 \equiv 1 \pmod{7} \text{ and } 3^6 \equiv 3^0 \equiv 1 \pmod{7}$$

Hence $\{1, 3, 2, 6, 4, 5\}$ is a reduced residue system mod 7.

From the above fact and illustration, we see that, if a is an integer relatively prime to n , then there is a unique integer k where $0 \leq k \leq \phi(n)-1$ such that $g^k \equiv a \pmod{n}$.

This leads to the following definition.

Definition:

Let n be a positive integer with primitive root g . If a is an integer with $\gcd(a,n) = 1$, then the smallest positive integer k such that $g^k \equiv a \pmod{n}$ is called the index of a to the base g mod n (or the index of a relative to g).

Remarks:

1. If k is the index of a to the base g mod n , then we write $k = \text{ind}_g(a)$. Note that we need not indicate the modulus n since it is assumed to be understood from the context. But if we do wish to indicate the particular modulus n which is being used, we could write $\text{ind}_{g,n}(a)$. Further, when the primitive root remains the same and there is no danger of confusion, we write simply $\text{ind}(a)$.

2. From the discussion preceding the definition of the index, we see that $\text{ind}_g(a)$ is unique and satisfies $0 \leq \text{ind}_g(a) \leq \phi(n)-1$.

3. Since $\text{ind}_g(a)$ is defined only if $\text{gcd}(a,n) = 1$, in the future, when we speak of $\text{ind}_g(a)$, it is to be assumed that $\text{gcd}(a,n) = 1$ whether or not this fact is explicitly mentioned.

4. In the very definition of the index the reader will no doubt recognize the close analogy with the usual definition in algebra of the logarithm of a positive real number a to a base g . From the definition of a logarithm, we have $\log_g a = k$ if and only if $g^k = a$. Similarly, $\text{ind}_g a = k$ if and only if $g^k \equiv a \pmod{n}$ and $0 \leq k \leq \phi(n)-1$

5. Referring to the illustration on the previous page, notice that $\text{ind}_{3,7}(1) = 0$, $\text{ind}_3(2) = 2$, $\text{ind}(3) = 1$, $\text{ind}(4) = 4$, $\text{ind}(5) = 5$, and $\text{ind}(6) = 3$. This also shows the use of the various notation options. It should be noted and emphasized that a change of root in general results in a change of index. For example, $g = 5$ is another primitive root of 7 and $\text{ind}_5(2) = 4$, $\text{ind}_5(3) = 5$, $\text{ind}_5(4) = 2$, $\text{ind}_5(5) = 1$, and $\text{ind}_5(6) = 3$.

Theorem 3.1

Let g be a primitive root mod n and a, b be integers relatively prime to n . Then $\text{ind}_g(a) = \text{ind}_g(b)$ if and only if $a \equiv b \pmod{n}$.

Proof:

Assume $\text{ind}_g(a) = \text{ind}_g(b)$. By definition, $g^{\text{ind}_g(a)} \equiv a \pmod{n}$ and $g^{\text{ind}_g(b)} \equiv b \pmod{n}$. Since $\text{ind}_g(a) = \text{ind}_g(b)$, then $g^{\text{ind}_g(a)} = g^{\text{ind}_g(b)}$. Therefore $a \equiv b \pmod{n}$. For the converse, assume $a \equiv b \pmod{n}$. By definition, given primitive root $g \pmod{n}$, the index of a is the unique number with $0 \leq \text{ind}_g(a) \leq \phi(n)-1$ and the index of b is the unique number with $0 \leq \text{ind}_g(b) \leq \phi(n)-1$ that satisfies $g^{\text{ind}_g(a)} \equiv a \pmod{n}$ and $g^{\text{ind}_g(b)} \equiv b \pmod{n}$.

Since $a \equiv b \pmod{n}$, then $g^{\text{ind}_g(a)} \equiv g^{\text{ind}_g(b)} \pmod{n}$. By Theorem 2.3 this implies $\text{ind}_g(a) \equiv \text{ind}_g(b) \pmod{\text{ord}_n(g)}$ or $\text{ind}_g(a) \equiv \text{ind}_g(b) \pmod{\phi(n)}$. By the uniqueness of $\text{ind}_g(a)$ and $\text{ind}_g(b)$ and, since $0 \leq \text{ind}_g(a), \text{ind}_g(b) \leq \phi(n)-1$, we must have $\text{ind}_g(a) = \text{ind}_g(b)$. □

Examples:

Let $n = 7$; $g = 3$ is a primitive root modulo 7.

$\text{ind}_3(6) = 3$ since $3^3 \equiv 6 \pmod{7}$. It is also true that $13 \equiv 6 \pmod{7}$. So, from Theorem 3.1, $\text{ind}_3(13) = 3$. This is easily verified: $3^3 \equiv 13 \pmod{7}$ because $7 \mid (27-13)$.

$\text{ind}_3(5) = 5$ since $3^5 \equiv 5 \pmod{7}$; that is $7 \mid (243-5)=34$.

And $12 \equiv 5 \pmod{7}$ so $\text{ind}_3(12) = 5$. This means that $3^5 \equiv 12 \pmod{7}$; that is $7 \mid (243-12)=33$.

And $19 \equiv 5 \pmod{7}$ so $\text{ind}_3(19) = 5$. This means that $3^5 \equiv 19 \pmod{7}$; that is $7 \mid (243-19)=32$.

The following theorem shows how closely the theory of indices parallels the theory of logarithms.

Theorem 3.2

Let n be a positive integer with primitive root g and let a and b be integers relatively prime to n . Then

- (1) $\text{ind}_g(1) = 0$
- (2) $\text{ind}_g(g) = 1$
- (3) $\text{ind}_g(ab) \equiv \text{ind}_g(a) + \text{ind}_g(b) \pmod{\phi(n)}$
- (4) $\text{ind}_g(a^k) \equiv k \text{ind}_g(a) \pmod{\phi(n)}$, where k is a positive integer.
- (5) $g^{\text{ind}_g(a)} \equiv a \pmod{n}$ and $\text{ind}_g(g^k) \equiv k \pmod{\phi(n)}$, where k is a positive integer.

Proof:

- (1) $g^0 \equiv 1 \pmod{n}$ implies $\text{ind}_g(1) = 0$.
- (2) $g^1 \equiv g \pmod{n}$ implies $\text{ind}_g(g) = 1$.
- (3) $g^{\text{ind}_g(a)} \equiv a \pmod{n}$ and $g^{\text{ind}_g(b)} \equiv b \pmod{n}$. Multiplying these two congruences, we obtain $g^{\text{ind}(a)+\text{ind}(b)} \equiv ab \pmod{n}$. Also since $g^{\text{ind}(ab)} \equiv ab \pmod{n}$, we infer that $g^{\text{ind}(ab)} \equiv g^{\text{ind}(a)+\text{ind}(b)} \pmod{n}$. By Theorem 2.3 $\text{ind}(ab) \equiv \text{ind}(a) + \text{ind}(b) \pmod{\text{ord}_n(g)}$. But g is a primitive root so that $\text{ord}_n(g) = \phi(n)$. Therefore $\text{ind}(ab) \equiv \text{ind}(a) + \text{ind}(b) \pmod{\phi(n)}$.
- (4). By definition of index, $g^{\text{ind}(a^k)} \equiv a^k \pmod{n} \dots (*)$. Since $a \equiv g^{\text{ind}(a)} \pmod{n}$, then $a^k \equiv (g^{\text{ind}(a)})^k \pmod{n}$, which implies $a^k \equiv g^{k \text{ind}(a)} \pmod{n} \dots (\#)$. By equations (*) and

(#), $g^{\text{ind}(ak)} \equiv g^{k \text{ ind}(a)} \pmod{n}$. Thus by Theorem 2.3,

$\text{ind}(a^k) \equiv k \text{ ind}(a) \pmod{\phi(n)}$.

(5). The first identity, $g^{\text{ind}(a)} \equiv a \pmod{n}$ follows directly from the definition. To obtain the second identity, by (4)

we have $\text{ind}_g(g^k) \equiv k \text{ ind}_g(g) \pmod{\phi(n)}$ and by (1),

$\text{ind}_g(g) = 1$. Therefore $\text{ind}_g(g^k) \equiv k \pmod{\phi(n)}$. \square

Remark:

In dealing with indices, two indices shall be considered to be the same when they are congruent $\pmod{\phi(n)}$.

In the theory of logarithms, if a and b are positive real numbers, then $\log(a/b) = \log(a) - \log(b)$. A similar property holds for indices if we define the quotient of two integers mod n as follows:

Definition:

Let n be a positive integer and let a and b be integers with $b \neq 0$. The quotient of a by b mod n is an integer x such that $bx \equiv a \pmod{n}$. The quotient of a by b mod n is denoted by $(a/b) \pmod{n}$.

With this definition, we have the following theorem.

Theorem 3.3

Let g be a primitive root mod n and $a, b \neq 0$ be integers relatively prime to n . Then

$$\text{ind}_g((a/b) \pmod{n}) \equiv \text{ind}_g(a) - \text{ind}_g(b) \pmod{\phi(n)}.$$

Proof:

By definition, $((a/b) \pmod{n}) = x$ if and only if

$$bx \equiv a \pmod{n}. \text{ By Theorem 3.1, } \text{ind}(bx) = \text{ind}(a).$$

By Theorem 3.2, $\text{ind}(b) + \text{ind}(x) \equiv \text{ind}(a) \pmod{\phi(n)}$. This

implies $\text{ind}(x) \equiv \text{ind}(a) - \text{ind}(b) \pmod{\phi(n)}$. Thus

$$\text{ind}((a/b) \pmod{n}) \equiv \text{ind}(a) - \text{ind}(b) \pmod{\phi(n)}. \quad \square$$

Corollary

$\text{ind}_g(a^*) \equiv -\text{ind}_g(a) \pmod{\phi(n)}$, where a^* is an inverse of a mod n .

Now we are going to establish the relationship between indices taken with respect to different primitive roots of a fixed integer n .

Theorem 3.4

Let n be a positive integer with primitive roots g and g' . Then let $\text{ind}_g(a) \equiv \text{ind}_{g'}(a) \cdot \text{ind}_g(g') \pmod{\phi(n)}$.

Proof:

Let $\text{ind}_{g'}(a) = t$ and $\text{ind}_g(g') = w$. Then $a \equiv g'^t \pmod{n}$ and

$$g' \equiv g^w \pmod{n}. \text{ Thus } a \equiv g'^t \equiv g^{tw} \pmod{n}.$$

Since $g^{\text{ind}_g(a)} \equiv a \pmod{n}$, then $g^{\text{ind}_g(a)} \equiv g^{tw} \pmod{n}$.

But $tw = (\text{ind}_{g'}(a)) \cdot (\text{ind}_g(g'))$. Therefore,

$g^{\text{ind}_g(a)} \equiv g^{(\text{ind}_g(a)) \cdot (\text{ind}_g(g'))} \pmod{n}$ and, by Theorem 2.3,

$$\text{ind}_g(a) \equiv (\text{ind}_g(a)) \cdot (\text{ind}_g(g')) \pmod{\phi(n)}.$$

□

The above property is analogous to the change of base formula in the theory of logarithm, namely $\log_{g'}(a) = (\log_g(a))/(\log_g(g'))$ or $\log_{g'}(a) = (\log_g(a)) \cdot (\log_g(g'))$.

Theorem 3.5

Let n be a positive integer with a primitive root g and let a be an integer relatively prime to n . Then

(1) $\text{ind}_g(-1) = \frac{1}{2}\phi(n)$, if $n > 2$.

(2) $\text{ind}_g(n-a) = \text{ind}_g(-a) \equiv \frac{1}{2}\phi(n) + \text{ind}_g(a) \pmod{\phi(n)}$.

Proof:

(1) There are two cases to consider. Case 1: $n = 4$.

$\text{ind}_3(-1) = \frac{1}{2}\phi(4)$. $3^k \equiv -1 \pmod{4}$ holds if $k = 1$, and

$\frac{1}{2}\phi(4) \equiv 1$. Case 2: $n = p^k$ or $2p^k$. Since g is a primitive

root of n , $g^{\phi(n)} \equiv 1 \pmod{n}$. This implies $g^{\phi(n)} - 1 \equiv 0 \pmod{n}$.

For $n = 4, p^k$ or $2p^k$, where p is an odd prime number and

$k \geq 1$, $g^{\phi(n)} - 1 =$

$(g^{\frac{1}{2}\phi(n)} - 1) \cdot (g^{\frac{1}{2}\phi(n)} + 1) \equiv 0 \pmod{n}$. . . (*). First we

need to show $\text{gcd}(g^{\frac{1}{2}\phi(n)} - 1, p^k) = 1$. Assume the contrary,

$\text{gcd}(g^{\frac{1}{2}\phi(n)} - 1, p^k) > 1$. Since $\text{gcd}(g^{\frac{1}{2}\phi(n)} - 1, p^k) = p^h$ for

some $h \geq 1$. Then $p^h | (g^{\frac{1}{2}\phi(n)} - 1)$ and hence $p | (g^{\frac{1}{2}\phi(n)} - 1)$. We

now claim that $p \nmid (g^{\frac{1}{2}\phi(n)} + 1)$ because, if we assume

otherwise, we have a contradiction; that is, if

$p \mid (g^{\frac{1}{2}\phi(n)} + 1)$ and since $p \mid (g^{\frac{1}{2}\phi(n)} - 1)$, then

$p \mid ((g^{\frac{1}{2}\phi(n)} + 1) - (g^{\frac{1}{2}\phi(n)} - 1)) = 2$ which means $p \mid 2$, but $p \geq 3$

so this is impossible. Therefore $p \nmid (g^{\frac{1}{2}\phi(n)} + 1)$ and hence p

is not a prime factor of $(g^{\frac{1}{2}\phi(n)} + 1)$. From (*) we have

$n \mid (g^{\frac{1}{2}\phi(n)} - 1) \cdot (g^{\frac{1}{2}\phi(n)} + 1)$. If $n = p^k$, then since p is

not a factor of $g^{\frac{1}{2}\phi(n)} + 1$, $p^k \mid (g^{\frac{1}{2}\phi(n)} - 1)$. Hence

$g^{\frac{1}{2}\phi(n)} - 1 \equiv 0 \pmod{p^k}$. Moreover, if $n = 2p^k$, then it

follows from Lemma 2.13 that the primitive root g of n is

odd so $g^{\frac{1}{2}\phi(n)} - 1$ is even. In this case we then have

$g^{\frac{1}{2}\phi(n)} - 1 \equiv 0 \pmod{2}$, and this implies

$g^{\frac{1}{2}\phi(n)} - 1 \equiv 0 \pmod{2p^k}$. So we have shown that if either

$n = p^k$ or $n = 2p^k$, then we must have $g^{\frac{1}{2}\phi(n)} - 1 \equiv 0 \pmod{n}$.

But this contradicts the fact that g is a primitive root of

n . Therefore $\gcd(g^{\frac{1}{2}\phi(n)} - 1, p^k) = 1$. To complete the

proof, recall that $(g^{\frac{1}{2}\phi(n)} - 1) \cdot (g^{\frac{1}{2}\phi(n)} + 1) \equiv 0 \pmod{n}$.

We have proved that $n \nmid (g^{\frac{1}{2}\phi(n)} - 1)$, so $n \mid (g^{\frac{1}{2}\phi(n)} + 1)$. Thus

$g^{\frac{1}{2}\phi(n)} + 1 \equiv 0 \pmod{n}$ or $g^{\frac{1}{2}\phi(n)} \equiv -1 \pmod{n}$, which implies

that $\text{ind}_g(-1) = \frac{1}{2}\phi(n)$.

(2) Since $n - a \equiv -a \pmod{n}$, by Theorem 3.1,

$\text{ind}(n-a) = \text{ind}(-a)$. Factoring $(-a)$, $\text{ind}(-a) = \text{ind}((-1)(a))$.

According to Theorem 3.2,

$\text{ind}_g((-1)(a)) \equiv \text{ind}_g(-1) + \text{ind}_g(a) \pmod{\phi(n)}$. Therefore

$\text{ind}_g(n-a) = \text{ind}_g(-a) \equiv \frac{1}{2}\phi(n) + \text{ind}_g(a) \pmod{\phi(n)}$. □

From Theorem 3.5(2), it follows that if we want to

construct an index table to the base $g \pmod{n}$, we need

calculate only half of the table. The other half can be easily filled in with the help of the theorem. For example, if $n = 19$ and $g = 2$, we calculate the index to the base $g = 2$ for the numbers $a = 1, 2, 3, \dots, 9$. Then we can obtain the indices for the numbers $b = 10, 11, 12, \dots, 18$ from the formula $\text{ind}_2(n-a) = \text{ind}_2(b) \equiv \frac{1}{2}\phi(n) + \text{ind}_2(a)$. Thus $\text{ind}_2(19-1) = \text{ind}_2(18) \equiv \frac{1}{2}(18) + \text{ind}_2(1) \pmod{18}$, for $a = 1, b = 18$. This implies $\text{ind}_2(18) \equiv 9 + 0 \pmod{18}$ and $\text{ind}(18) \equiv 9 \pmod{18}$. Similarly, $\text{ind}_2(17) \equiv 9 + \text{ind}_2(2) \pmod{18}$ for $a=2, b=17$. Then $\text{ind}(17) \equiv 9 + 1 \pmod{18}$ and $\text{ind}(17) \equiv 10 \pmod{18}$. Similarly, $\text{ind}_2(16) \equiv 9 + \text{ind}_2(3) \pmod{18}$ for $a=3, b=16$. Then $\text{ind}(16) \equiv 9 + 13 \pmod{18}$ and $\text{ind}(16) \equiv 4 \pmod{18}$. Table 1 is the completed table of indices for $n = 19$.

Table 1

$n = 19; g = 2$

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\text{ind}_2(x)$	0	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

Corollary

Let p be an odd prime and let g be a primitive root mod p . Then $\text{ind}_g(p-1) = \frac{1}{2}(p-1)$.

Proof:

By Theorem 3.5(20, $\text{ind}_g(p-1) = \text{ind}_g(-1)$. By 3.5 (1),

$$\text{ind}_g(-1) = \frac{1}{2}\phi(p) = \frac{1}{2}(p-1).$$

□

3.2 APPLICATIONS OF SCALAR INDICES

One use of index theory is in solving congruence equations. This section will discuss the relevant theory and provide examples showing how indices are used in solving different types of congruence equations.

(i) LINEAR CONGRUENCES

Consider the linear congruence equation $ax \equiv b \pmod{n}$, where a and b are integers and n is a positive integer that has a primitive root. We know, by Theorem 1.9, that the equation has a solution if and only if $d|b$, where $d = \gcd(a,n)$. Furthermore, if $d|b$, the equation has d mutually incongruent solutions mod n .

There are two cases to consider when discussing the use of indices for solving this type of congruence.

Case 1: $\gcd(a,n) = 1$. In this case the congruence has a unique solution. There are two subcases.

Subcase 1: $\gcd(b,n) = 1$. If $\gcd(b,n) = 1$, we apply the theory of indices directly to find the solution. In this case, since $\gcd(a,n) = \gcd(b,n) = 1$, the equation $ax \equiv b \pmod{n}$ is equivalent to the congruence $\text{ind}(ax) \equiv \text{ind}(b) \pmod{\phi(n)}$, or $\text{ind}(a) + \text{ind}(x) \equiv \text{ind}(b) \pmod{\phi(n)}$, or

$\text{ind}(x) \equiv \text{ind}(b) - \text{ind}(a) \pmod{\phi(n)}$. A table of indices mod n gives values for $\text{ind}(b)$ and $\text{ind}(a)$ and x .

The following index tables are provided for use with the examples throughout this section.

Table 2

$n = 9; g = 2; \text{ and } \phi(9) = 6$

x	1	2	4	5	7	8
ind(x)	0	1	2	5	4	3

Table 3

$n = 11; g = 2$

x	1	2	3	4	5	6	7	8	9	10
ind(x)	0	1	8	2	4	9	7	3	6	5

Table 4

$n = 13; g = 2$

x	1	2	3	4	5	6	7	8	9	10	11	12
ind(x)	0	1	4	2	9	5	11	3	8	10	7	6

Examples:

a. Solve $7x \equiv 2 \pmod{9}$.

$\text{gcd}(7,9) = 1$, so there is a unique solution. Also

$\gcd(2,9) = 1$. The congruence is equivalent to $\text{ind}(7) + \text{ind}(x) \equiv \text{ind}(2) \pmod{\phi(9)}$, or to $\text{ind}(x) \equiv \text{ind}(2) - \text{ind}(7) \pmod{6}$. Consulting Table 1, we find that $\text{ind}(2) = 1$ and $\text{ind}(7) = 4$. The equation then becomes $\text{ind}(x) \equiv 1 - 4 \equiv 3 \pmod{6}$. Consulting the same table again, we get the solution $x \equiv 8 \pmod{9}$.

b. Solve $9x \equiv 16 \pmod{11}$.

$\gcd(9,11) = 1$, so there is a unique solution. The congruence is equivalent to $9x \equiv 5 \pmod{11}$, and since $\gcd(5,11) = 1$, this congruence is equivalent to $\text{ind}(x) \equiv \text{ind}(5) - \text{ind}(9) \pmod{10}$. This becomes $\text{ind}(x) \equiv 4 - 6 \pmod{10}$, and then $\text{ind}(x) \equiv 8 \pmod{10}$. The solution is $x \equiv 3 \pmod{11}$.

Subcase 2: $\gcd(b,n) = u > 1$ In this case there exist integers r and s such that $b = ur$ and $n = us$ and $\gcd(r,s) = 1$. We make a change of variables by taking $x = uy$ and the equation becomes $a(uy) \equiv ur \pmod{us}$. Upon the division of both sides by u , we obtain $ay \equiv r \pmod{s}$ and $\gcd(a,s) = \gcd(r,s) = 1$. Now we can apply the theory of indices as in subcase 1 to find the unique solution $y \pmod{s}$ from the equation $\text{ind}(y) \equiv \text{ind}(r) - \text{ind}(a) \pmod{\phi(s)}$. Then the solution to the original equation is given by $x \equiv uy \pmod{us}$, or $x \equiv uy \pmod{n}$.

Examples:

a. Solve $5x \equiv 2 \pmod{26}$.

$\gcd(5,26) = 1$ and $\gcd(2,26) = 2$, so we use a change of variables approach where $u = 2$, $r = 1$ and $s = 13$. We let $x = 2y$ and the equation becomes $5(2y) \equiv 2 \pmod{26}$, and then $5y \equiv 1 \pmod{13}$, upon division by 2. This is equivalent to $\text{ind}(5) + \text{ind}(y) \equiv \text{ind}(1) \pmod{\phi(13)}$, to $\text{ind}(y) \equiv \text{ind}(1) - \text{ind}(5) \pmod{12}$, and to $\text{ind}(y) \equiv 3 \pmod{12}$, so that $y \equiv 8 \pmod{13}$. Therefore, $x = 2y \equiv 16 \pmod{26}$ and the unique solution to the original equation is $x \equiv 16 \pmod{26}$.

b. Solve $4x \equiv 3 \pmod{27}$.

$\gcd(4,27) = 1$ and $\gcd(3,27) = 3$, so again we use a change of variables, $x = 3y$, and we get $4(3y) \equiv 3 \pmod{27}$. This implies $4y \equiv 1 \pmod{9}$, which is equivalent to $\text{ind}(4) + \text{ind}(y) \equiv \text{ind}(1) \pmod{6}$, or to $\text{ind}(y) \equiv \text{ind}(1) - \text{ind}(4) \pmod{6}$, or $\text{ind}(y) \equiv 0 - 2 \equiv \pmod{6}$. From this we get $y \equiv 7 \pmod{9}$ and $x = 3y \equiv 21 \pmod{27}$, so the unique solution is $x \equiv 21 \pmod{27}$.

Case 2: $\gcd(a,n) = d > 1$ In this case, the equation has a solution if and only if $d|b$. We can solve the congruence equation $ax \equiv b \pmod{n}$, where $\gcd(a,n) = d$ and $d|b$, by considering the congruence equation

$(a/d)x \equiv (b/d) \pmod{n/d}$. Since $\gcd(a/d, n/d) = 1$, we can again apply the theory of indices (as we did in case 1) to solve the equation $a'y \equiv b' \pmod{n'}$. . . (*), where $a' = a/d$, $b' = b/d$, and $n' = n/d$. If we assume that the unique solution to (*) is $y = y_0 \pmod{n'}$, we can use y_0 to obtain all of the d solutions to the original congruence. These d incongruent solutions mod n are given by $y_0, y_0 + (n/d), y_0 + 2(n/d), \dots, y_0 + (d-1)(n/d)$.

Example:

Solve $14x \equiv 10 \pmod{18}$.

$\gcd(14, 18) = 2$ and $2 \mid 10$, so there are two incongruent solutions mod 18. The original congruence is equivalent to $(14/2)y \equiv 10/2 \pmod{18/2}$, and to $7y \equiv 5 \pmod{9}$. This is equivalent to $\text{ind}(y) \equiv \text{ind}(5) - \text{ind}(7) \pmod{6}$, and $\text{ind}(y) \equiv 5 - 4 \equiv 1 \pmod{6}$. Then $y \equiv 2 \pmod{9}$ and the solutions to the original congruence are $x \equiv 2, (2 + 9) \pmod{18}$ or $x \equiv 2, 11 \pmod{18}$.

(ii) **FINDING THE k^{th} -POWER RESIDUE**

Definition:

If n and k are positive integers and c is an integer relatively prime to n , then we say that c is a k^{th} -power residue of n , if the congruence $x^k \equiv c \pmod{n}$ has a

solution. If the congruence has no solution, c is called a k^{th} -power non-residue of n .

When n is an integer possessing a primitive root, the following theorem gives a necessary and sufficient condition for an integer c , relatively prime to n , to be a k^{th} -power residue of n .

Theorem 3.6

Let n be a positive integer with a primitive root g . If k is a positive integer and c is an integer relatively prime to n , then the congruence $x^k \equiv c \pmod{n}$ has a solution if and only if $d \mid \text{ind}_g(c)$, where $d = \gcd(k, \phi(n))$. Furthermore, if there is a solution of $x^k \equiv c \pmod{n}$, then there are exactly d incongruent solutions mod n .

Proof:

The congruence $x^k \equiv c \pmod{n}$ is equivalent to the linear congruence in $\text{ind}_g(x)$, $k \text{ind}_g(x) \equiv \text{ind}_g(c) \pmod{\phi(n)}$. Now let $d = \gcd(k, \phi(n))$. But this linear congruence equation in $\text{ind}_g(x)$ has d incongruent solutions mod $\phi(n)$ if and only if $d \mid \text{ind}_g(c)$. □

Corollary 1 (Euler's Criterion)

The congruence $x^k \equiv c \pmod{n}$ is solvable if and only if $c^{(\phi(n))/d} \equiv 1 \pmod{n}$.

Proof:

From the theorem, we have $x^k \equiv c \pmod{n}$ is solvable if and only if $d \mid \text{ind}_g(c)$. But $d \mid \text{ind}_g(c)$ if and only if $\text{ind}_g(c) = dl$ for some integer l . Then $((\phi(n))/d) \text{ind}_g(c) = ((\phi(n))/d)(dl) = \phi(n)l \equiv 0 \pmod{\phi(n)}$. Thus $d \mid \text{ind}_g(c)$ is equivalent to $((\phi(n))/d) \text{ind}_g(c) \equiv 0 \pmod{\phi(n)}$. This implies $\text{ind}_g(c^{(\phi(n))/d}) \equiv \text{ind}_g(1) \pmod{\phi(n)}$, which in turn implies $c^{(\phi(n))/d} \equiv 1 \pmod{n}$. □

Corollary 2

Let p be an odd prime and let a be an integer relatively prime to p . Then $x^k \equiv c \pmod{p}$ is solvable if and only if $c^{(p-1)/d} \equiv 1 \pmod{p}$, where $d = \text{gcd}(k, p-1)$.

Examples:

a. Solve $x^4 \equiv 8 \pmod{11}$.

Does the congruence have a solution? It does if $d \mid \text{ind}(8)$, where $d = \text{gcd}(4, \phi(11)) = \text{gcd}(4, 10) = 2$. But $\text{ind}(8) = 3$ and $2 \nmid 3$. Therefore there are no solutions to this congruence; that is 8 is a 4th power non-residue of 11.

b. Solve $x^8 \equiv 7 \pmod{9}$.

$\text{gcd}(8, 6) = 2$, $\text{ind}(7) = 4$, and $2 \mid 4$. Therefore, there are two incongruent solutions. To solve the congruence, we note that it is equivalent to $8 \text{ind}(x) \equiv \text{ind}(7) \pmod{6}$, and to $8 \text{ind}(x) \equiv 4 \pmod{6}$. By Theorem 1.6, this is equivalent to

$2 \operatorname{ind}(x) \equiv 1 \pmod{3}$. Using the inverse of $2 \pmod{3}$, we have
 $2 \cdot 2 \operatorname{ind}(x) \equiv 2 \cdot 1 \pmod{3}$, which implies
 $\operatorname{ind}(x) \equiv 2, (2 + 3) \pmod{3}$, or $\operatorname{ind}(x) \equiv 2, 5 \pmod{3}$. This
means the two solutions to the original congruence are
 $x \equiv 4, 5 \pmod{19}$.

c. Solve $x^4 \equiv 5 \pmod{11}$.

$\gcd(4, 10) = 2$, $\operatorname{ind}(5) = 4$ and $2 \mid 4$; therefore there are two
solutions. The congruence is equivalent to

$4 \operatorname{ind}(x) \equiv \operatorname{ind}(5) \pmod{10}$, or $4 \operatorname{ind}(x) \equiv 4 \pmod{10}$.

This implies $\operatorname{ind}(x) \equiv 1, 6 \pmod{5}$. Thus $x \equiv 2, 9 \pmod{11}$.

The next theorem proves useful in recognizing which
 k^{th} -power congruence equations are solvable. In other
words, it identifies the k^{th} -power residues mod n .

Theorem 3.7

Let n be a positive integer with a primitive root g .
If k is a positive integer and c is an integer relatively
prime to n , then the k^{th} -power residues of n are the members
of the set $S = \{g^d, g^{2d}, \dots, g^{((\phi(n))/d) \cdot d}\}$ where
 $d = \gcd(k, \phi(n))$.

Proof:

By Theorem 3.6, the congruence $x^k \equiv c \pmod{n}$ has a solution
if and only if $d \mid \operatorname{ind}(c)$. This implies $\operatorname{ind}(c) = jd$ for some
integer j . By Theorem 3.2, $jd \equiv \operatorname{ind}_g(g^{jd}) \pmod{\phi(n)}$. Thus
 $jd \equiv \operatorname{ind}(g^{jd}) \equiv \operatorname{ind}(c) \pmod{\phi(n)}$. This implies

$g^{jd} \equiv c \pmod{n}$, and therefore the numbers g^{jd} are k^{th} -power residues mod n . Moreover, all g^{jd} are distinct modulo n since they form a subset of the reduced residue system $g, g^2, \dots, g^{\phi(n)}$. Now, let a be a specific k^{th} -power residue mod n so that $x^k \equiv a \pmod{n}$. By definition of k^{th} -power residues, $\gcd(a, n) = 1$, so $\text{ind}_g(a)$ exists. Moreover, $\text{ind}_g(a) = jd$ and $a \equiv g^{jd} \pmod{n}$ for some integer j . By the division algorithm applied to j and $(\phi(n))/d$, we have $j = ((\phi(n))/d)s + t$, with $0 \leq t < (\phi(n))/d$. Then $a \equiv g^{jd} \equiv g^{((\phi(n))/d)s + td} \equiv g^{(\phi(n)s/d) + td} \equiv g^{\phi(n)s} g^{td} \pmod{n}$. But, by Euler's Theorem, $g^{\phi(n)} \equiv 1 \pmod{n}$. Raising both sides of this congruence to the s^{th} power, we get $(g^{\phi(n)})^s \equiv 1^s \pmod{n}$ or $g^{\phi(n)s} \equiv 1 \pmod{n}$. Then $a \equiv g^{td} \pmod{n}$. Therefore a is congruent to one of the numbers in set S . Thus the members of the set S account for all k^{th} -power residues mod n . \square

(iii) BINOMIAL CONGRUENCES

We call a congruence of the form $ax^k \equiv b \pmod{n}$ a binomial congruence. In this section we will discuss the binomial congruences $ax^k \equiv b \pmod{n}$, where n is a positive integer with a primitive root and $\gcd(a, n) = 1$. Since $\gcd(a, n) = 1$, then a has an inverse a^* mod n such that $aa^* \equiv 1 \pmod{n}$. Multiplying the above congruence by a^* , we get $x^k \equiv a^*b \pmod{n}$. Thus we have reduced the problem of solving binomial congruences to one of solving congruences

of the simpler form $x^k \equiv c \pmod{n}$. This in turn is equivalent to determining whether or not c is a k^{th} -power residue of n .

Examples:

a. Solve $7x^3 \equiv 3 \pmod{11}$.

Using the above theory that, if $\gcd(a,n) = 1$, then a has an inverse, a^* , we find 7 has an inverse, 8, since

$7 \cdot 8 \equiv 1 \pmod{11}$. Thus $7 \cdot 8 x^3 \equiv 3 \cdot 8 \pmod{11}$ gives

$x^3 \equiv 24 \equiv 2 \pmod{11}$. To find the third power residue of 2, we use indices and the equivalent congruence

$3 \text{ ind}(x) \equiv \text{ind}(2) \pmod{10}$, which implies $3 \text{ ind}(x) \equiv 1 \pmod{10}$. We need to find the inverse of 3. It proves to be 7.

Thus $3 \cdot 7 \text{ ind}(x) \equiv 1 \cdot 7 \pmod{10}$. The congruence becomes

$\text{ind}(x) \equiv 7 \pmod{10}$, and the solution is $x \equiv 7 \pmod{11}$.

b. Solve $7x^5 \equiv 4 \pmod{9}$.

$\gcd(7,9) = 1$ so 7 has an inverse, 4. Therefore

$7 \cdot 4x^5 \equiv 4 \cdot 4 \pmod{9}$, and $x^5 \equiv 16 \equiv 7 \pmod{9}$. This implies

$5 \text{ ind}(x) \equiv \text{ind}(7) \pmod{6}$ or $5 \text{ ind}(x) \equiv 4 \pmod{6}$. Again

using an inverse, we have $5 \cdot 5 \text{ ind}(x) \equiv 4 \cdot 5 \pmod{6}$ or

$\text{ind}(x) \equiv 20 \equiv 2 \pmod{6}$, and a solution of $x \equiv 4 \pmod{9}$.

(iv) EXPONENTIAL CONGRUENCES

An exponential congruence is one of the form

$a^x \equiv b \pmod{n}$. If n has a primitive root and if $\gcd(a,n) = \gcd(b,n) = 1$, then it is possible to solve this kind of congruence by using the theory of indices.

We let g be a primitive root of n . Then the exponential congruence is equivalent to the linear congruence in x , $x \operatorname{ind}_g(a) \equiv \operatorname{ind}_g(b) \pmod{\phi(n)}$. Let $d = \gcd(\operatorname{ind}_g(a), \phi(n))$; then the last congruence has a solution if and only if $d \mid \operatorname{ind}_g(b)$, in which case there are d mutually incongruent solutions mod $\phi(n)$.

Examples:

a. Solve $9^x \equiv 5 \pmod{11}$.

$\gcd(9,11) = \gcd(5,11) = 1$. Thus the congruence is solvable and the congruence is equivalent to

$x \operatorname{ind}(9) \equiv \operatorname{ind}(5) \pmod{10}$, and to $6x \equiv 4 \pmod{10}$.

$\gcd(\operatorname{ind}(9), \phi(11)) = \gcd(6,10) = 2$, and $2 \mid \operatorname{ind}(5)$, so there are two solutions. Reducing the equation to $3x \equiv 2 \pmod{5}$, we again use an inverse $3 \cdot 2x \equiv 2 \cdot 2 \pmod{5}$. The two solutions are $x \equiv 4, 9 \pmod{11}$.

b. Solve $7^x \equiv 4 \pmod{9}$.

$\gcd(7,9) = \gcd(4,9) = 1$. The congruence is equivalent to $x \operatorname{ind}(7) \equiv \operatorname{ind}(4) \pmod{6}$, and to $4x \equiv 2 \pmod{6}$.

$\gcd(\operatorname{ind}(7), \phi(9)) = \gcd(4,6) = 2$. $2 \mid \operatorname{ind}(4) = 2$, so there are two solutions. We reduce the congruence $4x \equiv 2 \pmod{6}$ to the congruence $2x \equiv 1 \pmod{3}$. Multiplying by the inverse, we get $2 \cdot 2x \equiv 12 \pmod{3}$ and the solutions are

$$x \equiv 2, 5 \pmod{9}.$$

Remark:

In the foregoing applications of index theory in solving congruence equations, we were able to solve congruence equations if the modulus possessed a primitive root. However, in Chapter 4 we are going to see how to use vector indices to solve congruence equations with any moduli. Of course, in the case of binomial and, more generally, polynomial congruences, certain reductions can be made so that the problem becomes that of solving congruences with prime moduli. Moreover, since every prime has a primitive root, one can apply the index theory to solve binomial congruences with prime moduli and, in turn, this can be used to find the solution to any moduli.

FINDING THE ORDER OF AN INTEGER MOD n BY USING INDICES

Besides using the theory of indices to solve various congruence equations, we can also use it to determine the order of an integer a mod n . By definition, $k = \text{ord}_n(a)$ if k is the least positive divisor of $\phi(n)$ that satisfies the congruence $a^k \equiv 1 \pmod{n}$. If the modulus n has a primitive root, say g , then the congruence above is equivalent to $k \text{ ind}_g(a) \equiv 0 \pmod{\phi(n)}$, or $\text{ind}_g(a) \equiv 0 \pmod{(\phi(n))/k}$. Hence, k is the least positive divisor of $\phi(n)$ for which

$((\phi(n))/k) \mid \text{ind}_g(a)$, and consequently $(\phi(n))/k$ is the greatest divisor of $\phi(n)$ which divides $\text{ind}_g(a)$. That is $(\phi(n))/k = \text{gcd}(\phi(n), \text{ind}_g(a)) = d$. Therefore, $k = (\phi(n))/d$. Thus we have proven the following theorem.

Theorem 3.8

Let n be an integer with a primitive root g . If a is a positive integer relatively prime to n , then $\text{ord}_n(a) = (\phi(n))/d$, where $d = \text{gcd}(\phi(n), \text{ind}_g(a))$.

Corollary 1

If a in the theorem is a primitive root of n , and, in particular, if $a = g$, then $\text{ord}_n(a) = \phi(n)$.

Corollary 2

A reduced residue system mod n contains $\phi(k)$ integers of order k ; in particular, it contains $\phi(\phi(n))$ primitive roots.

Proof:

Let $S = \{r_1, r_2, \dots, r_{\phi(n)}\}$ be a reduced residue system mod n . For each $i = 1, 2, \dots, \phi(n)$, we have $\text{ord}_n(r_i) = (\phi(n))/d_i$, where $d_i = \text{gcd}(\phi(n), \text{ind}_g(r_i))$. The least indices of the elements of the reduced residue system S are among the integers $0, 1, 2, \dots, \phi(n)-1$. Thus $\text{ord}_n(r_i) = k$ if and only if $d_i = (\phi(n))/k$. Since $d_i \mid \text{ind}_g(r_i)$, then $\text{ind}_g(r_i) = d_i k_i$ for some k_i , where

$k_i \in \{0, 1, \dots, \phi(n)-1\}$. $d_i = (\phi(n))/k$ is equivalent to $\gcd(\phi(n), (\phi(n))/k_i) = (\phi(n))/k$ and this in turn is equivalent to $\gcd(\phi(n), k_i) = 1$. But the number of integers k_i that satisfies $\gcd(\phi(n), k_i) = 1$ is $\phi(k)$. Thus there are $\phi(k)$ elements of S whose order is k . □

Example:

For $n = 41$, let $S = \{1, 2, \dots, 40\}$. The elements of S whose order mod 41 is 10 are those elements satisfying the equation $\gcd(\phi(41), \text{ind}_g(r_i)) = (\phi(41))/10$, or $\gcd(40, \text{ind}_g(r_i)) = 40/10 = 4$. Thus $\text{ind}_g(r_i) = 4, 12, 28, 36$, since $\gcd(40, 4) = \gcd(40, 12) = \gcd(40, 28) = \gcd(40, 36) = 4$. Next we will identify the integers r_i . But to do so, we need an index table mod 41.

Table 5

$n = 41; g = 6$

x	1	2	3	4	5	6	7	8	9	10	11	12	13
$\text{ind}_6(x)$	0	26	15	12	22	1	39	38	30	8	3	27	31

continued

14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
25	37	24	33	16	9	34	14	29	36	13	4	17	5	11

continued

29	30	31	32	33	34	35	36	37	38	39	40
7	23	28	10	18	19	21	2	32	35	6	20

We find $r_i = 25, 4, 31, 23$. The number of these integers is $\phi(10) = 4$. Furthermore, the elements of S that are primitive roots mod 41 are those satisfying the equation $\gcd(\phi(41), \text{ind}_g(r_i)) = (\phi(41))/(\phi(41)) = 1$. Thus $\text{ind}_g(r_i)$ will be all of the elements in S that are relatively prime to 40, so $\text{ind}_g(r_i) = 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39$. Using the above table, we find that the primitive roots of 41, that is the r_i , are 6, 11, 29, 19, 28, 24, 26, 34, 35, 30, 12, 22, 13, 17, 15, 7. Hence, the number of primitive roots mod 41 is $\phi(\phi(41)) = \phi(40) = 16$.

The above example illustrates how, with the aid of a table compiled for one primitive root of a given modulus, a complete list of primitive roots for that modulus can be identified. This method is clearly more efficient than the cumbersome trial and error procedure of finding the order for each and every one of the integers relatively prime to n by repeated solving of the congruence $a^x \equiv 1 \pmod{n}$, and the matching x with $\phi(n)$ to see if each particular a is a primitive root of n .

3.3 THE MODULAR SLIDE RULE

As has been mentioned earlier, indices and logarithms have many similar properties and behave in much the same ways. Knowing this and knowing that the theory of

logarithms is the theory behind slide rules, we wonder if the theory of indices could be used to make a slide rule to carry out modular arithmetic. Such is the case. A slide rule that aids in the solving of modulo n congruence equations can be constructed based on indices. A complication not shared by logarithms, however, is that each modulo n class of congruences requires a separate slide rule constructed specifically for that modulo.

Before beginning the construction of a modular slide rule, let us see first how it is possible to carry out simple addition and subtraction with two equally spaced and marked straight-edges. In Figure 1 below, the two straight-edges, each having the numbers 1 through 9 spaced equally on it, are placed edge to edge so that the 1's match, the 2's match, and so on.

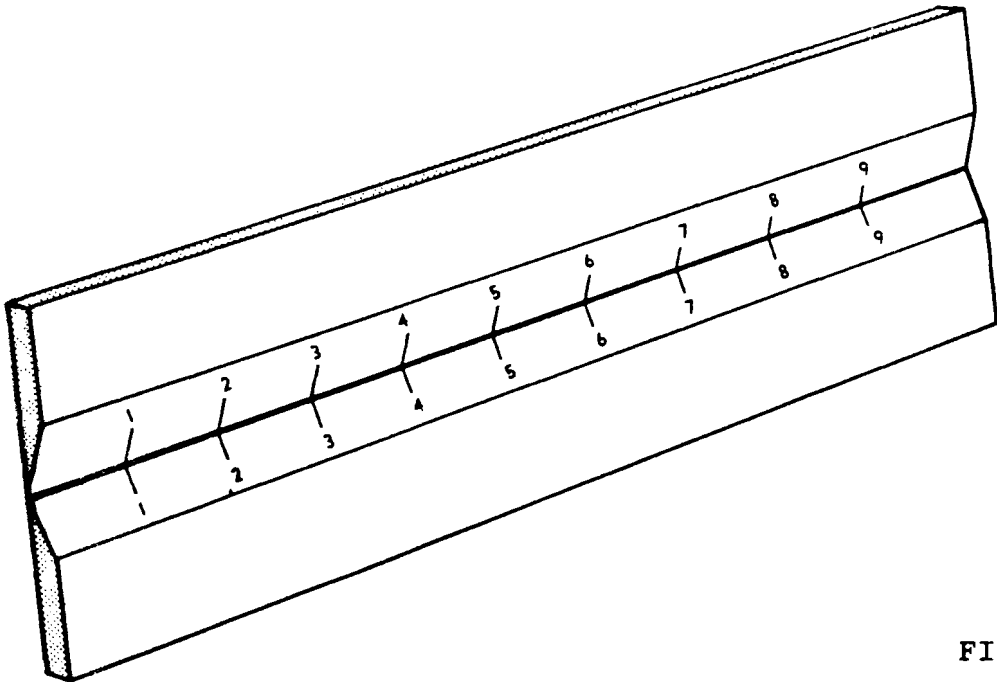


FIGURE 1

Now let us assume we want to add 2 and 3. We can accomplish this by sliding one of the straight-edges, say the top one, to the right until its left end which is marked 0 is above the 2 on the bottom straight edge, as in Figure 2 below. Then the answer is found by reading the number on the bottom straight-edge that is below the 3 on the top one. In effect, the addition of two numbers is equivalent to adding the corresponding lengths on the straight-edges. See Figure 2.

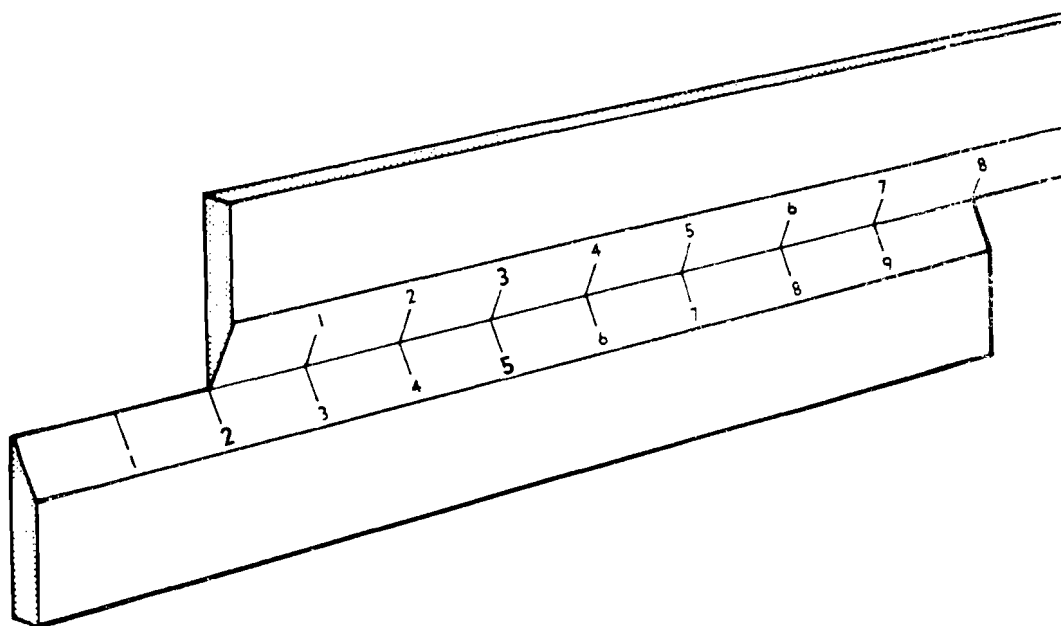


FIGURE 2

Something of the same procedure is used with ordinary slide rules. In a slide rule, though, the numbers on the C and D scales are marked off in lengths that correspond not to the numbers themselves but to the logarithms of the numbers. Since the product of two numbers can be obtained by adding their logarithms, it follows that this product can

be found on the slide rule by adding the two logarithmic lengths on the C and D scales as in Figure 3 below which shows the multiplication of 2 and 3.

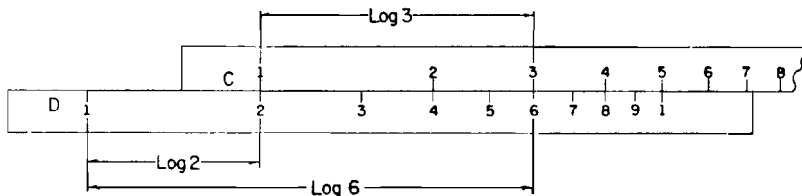


FIGURE 3

THE MODULAR STRAIGHT-EDGE SLIDE RULE

We are now going to construct a similar slide rule to carry out modular arithmetic operations. In particular, we will construct a modular slide rule to carry out calculations mod 29; we will use the primitive root 2. Again we use two equally spaced and marked straight-edges, each with the numbers positioned according to their indices. For example, notice the top straight-edge in Figure 4 on the following page. The number 8 is positioned under 3 because $\text{ind}_2(8) = 3$; also, the number 24 is placed under 8 because $\text{ind}_2(24) = 8$. The top straight-edge is called the c-scale and the bottom one the d-scale.

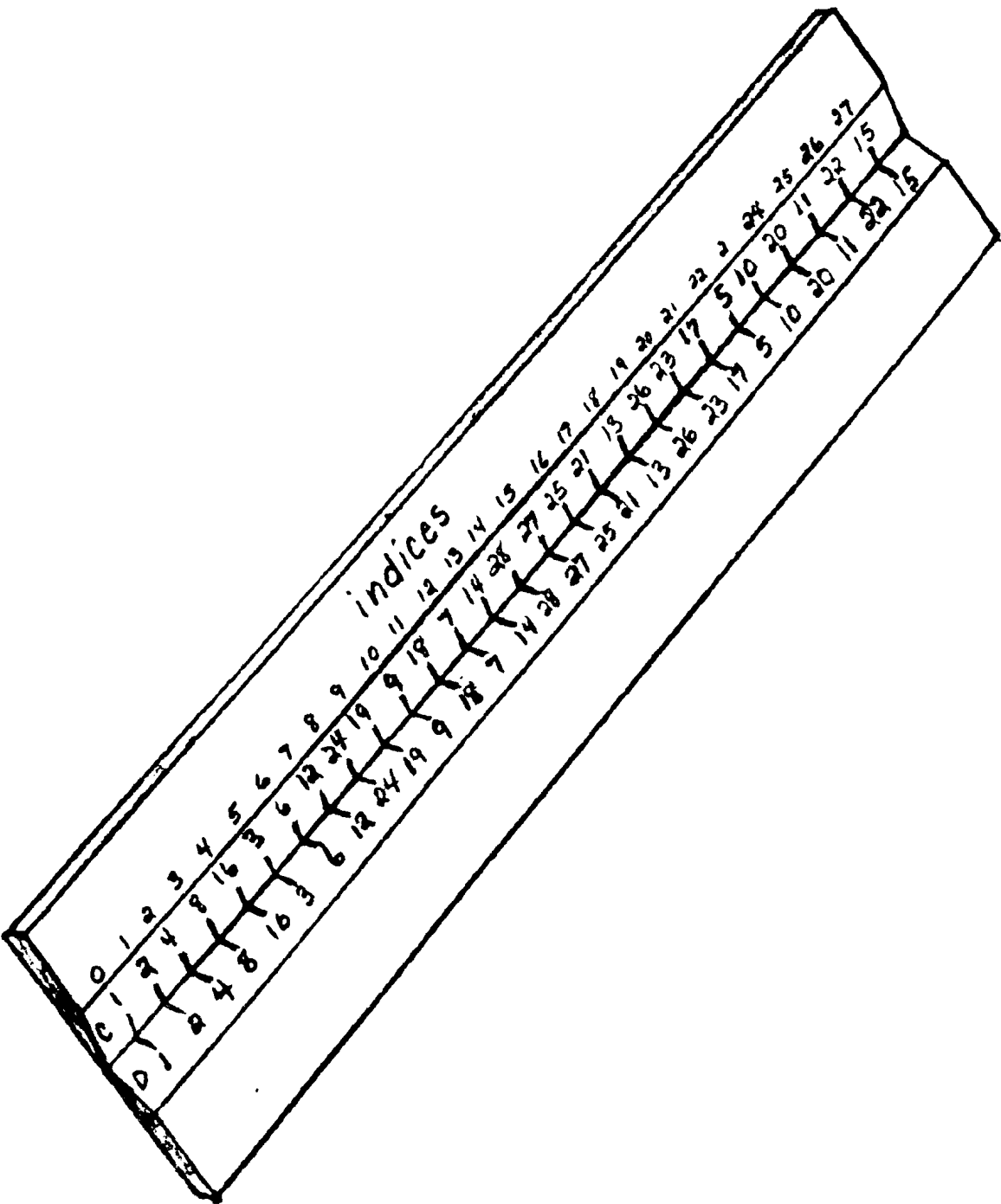


FIGURE 4

As with the ordinary slide rule, we can use the modular straight-edge slide rule to do multiplication. Since the product of two numbers mod 29 can be obtained by adding their indices, and since the numbers on the two scales mark off lengths that correspond to the indices of the numbers, then the product of two numbers x and y (mod 29) can be found on the modular slide rule by adding the two lengths corresponding to the indices of x and y on the c - and d -scales. For example, to multiply 8 and 6 (mod 29) we slide one of the two scales, say the c -scale, to the right until the number 1 on its left end is over the 8 on the d -scale. See Figure 5 on the following page. Opposite 6 on the c -scale we read off the product, 19 (mod 29), on the d -scale. If we keep the scales in the same position as shown above, we can see that $8 \cdot 13 \equiv 17 \pmod{29}$. However, if we try to find the product of 8 and 22, we notice that 22 on the c -scale does not correspond to any number on the d -scale; that is, the 22 is off the end of the d -scale and thus the slide rule seems to be of no use in finding the product of 8 and 22. The difficulty can be overcome and the product found by "wrapping" the straight-edge around so that the end of each scale connects to its beginning, thus allowing the answer to be read from the earlier entries on the now circular scale. Doing so, we find the number now opposite the 22 on the c -scale is the product of 8 and 22 (mod 29) which is 2. From this example, we see that a straight edge slide rule proves

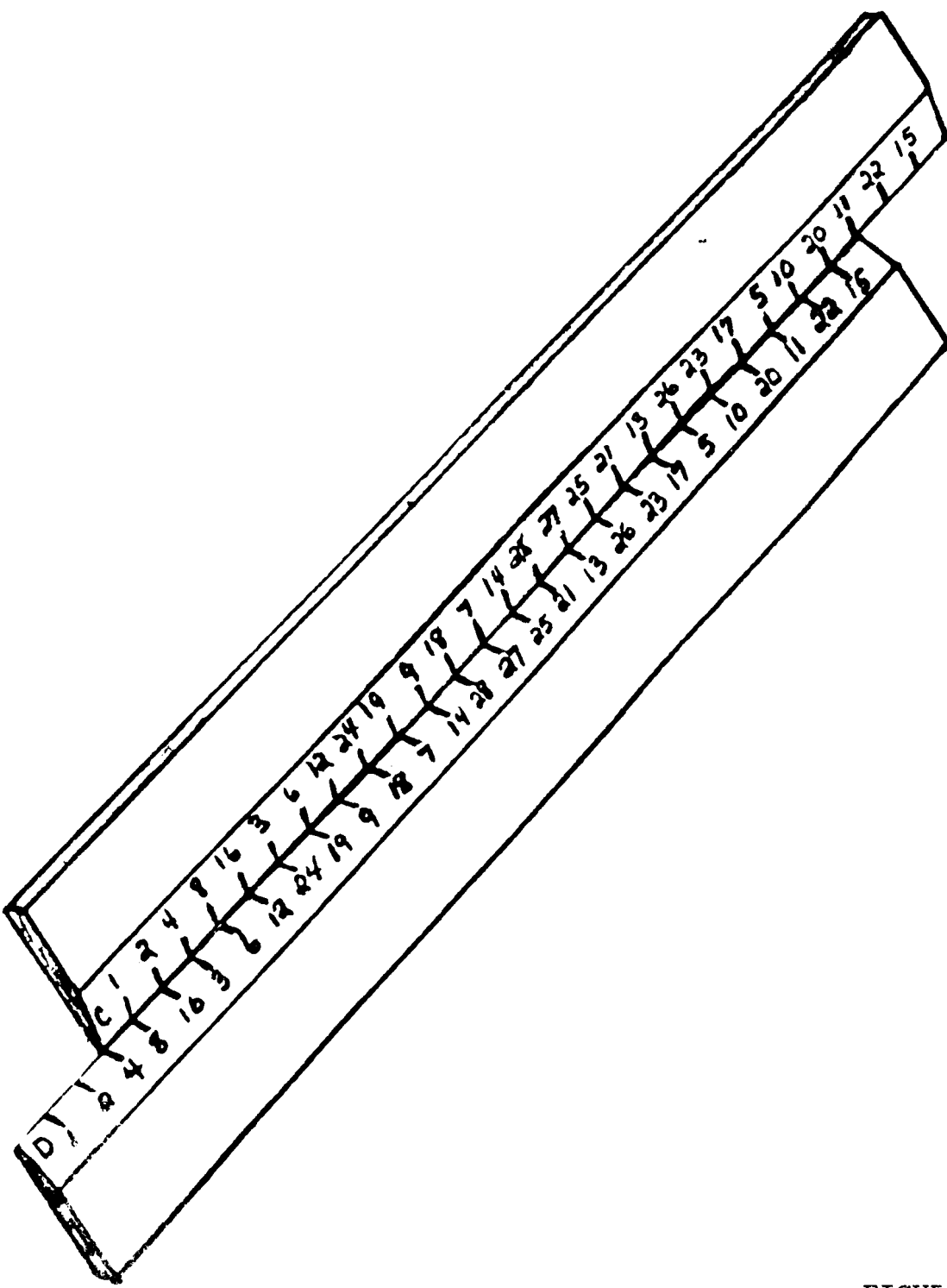


FIGURE 5

to be inefficient for modular calculations due to the cyclical nature of modular arithmetic. A circular slide rule, then, is a better alternative.

THE MODULAR CIRCULAR SLIDE RULE

In this section we will explain how to make a modular circular slide rule with modulo 29 and primitive root 2 and we will demonstrate its uses. (Much of the material on the modular circular slide rule comes from [18], pages 137-140.)

Modular Multiplication and Solving Linear Congruence

Equations

We begin with two circular disks of radii r_1 and r_2 where $r_1 < r_2$. We partition each of the two disks with 28 equally spaced marks. On the smaller disk we make two concentric circular scales. The inner scale has the numbers 1, 2, . . . , 28 printed consecutively in a counterclockwise direction. This scale is called the A-scale. On the other scale, called the C-scale, the numbers are positioned according to their indices so that the 2 on the C-scale is "under" the 1 on the A-scale because $\text{ind}(2) = 1$, the 4 is under 2 ($\text{ind}(4) = 2$), 8 under 3 ($\text{ind}(8) = 3$), and so on. See Figure 6 on the following page.

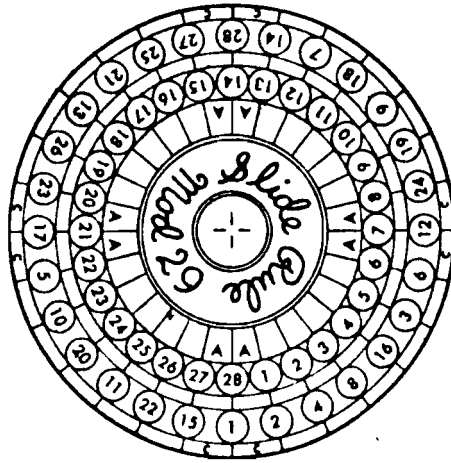


FIGURE 6

On the other disk, we construct a scale similar to the C-scale. It is called the D-scale and is pictured below.

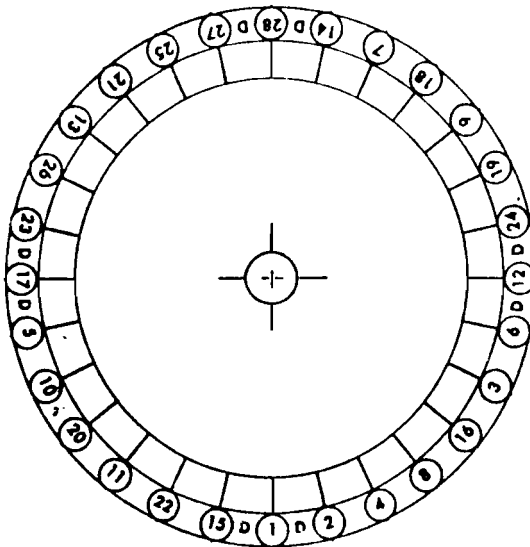


FIGURE 7

The two disks are constructed in such a way that the smaller disk fits inside the larger one and the smaller disk is free to be rotated at the common center of the two disks.

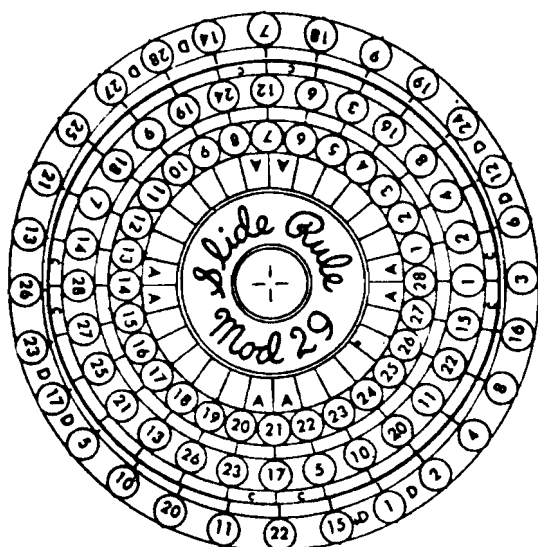


FIGURE 8

Earlier we used the modular straight edge slide rule to perform multiplication. We use the C-scale and D-scale of this circular slide rule to do the same. Suppose that we want to find the product of the integers x and y mod 29. We rotate the disk carrying the A- and C-scales so that the 1 on the C-scale falls upon the x on the D-scale. Then y on the C-scale coincides with z on the D-scale so that $xy = z$.

To see how and why the circular slide rule works, we will begin by describing the A-, C-, and D-scales in terms of polar coordinates. We take as a polar axis the ray, with its initial point the common center of the two disks, which passes through the number 28 marked on the A-scale, and through the 1's marked on the C-scale and D-scale. The three scales are described in polar coordinates (r, θ) as follows: r is the radius of the circle of each scale and θ takes on the values kx , where $k = (2\pi)/(28)$ and x ranges over the set of integers $\{1, 2, \dots, 28\}$ in some order

depending on the particular scale. The exact description of the polar angles of each scale is as follows:

A-scale: $\theta(a) = \alpha a$, $a = 1, 2, \dots, 28$, where α ranges over the marks of the A-scale in a counterclockwise direction.

C-scale: $\theta(c) = k \text{ ind}(c)$, $c =$ the numbers 2, 4, 8, . . . , 1 in the order as printed on the C-scale.

D-scale: $\theta(d) = k \text{ ind}(d)$, $d =$ the numbers as arranged on the C-scale.

Note that a ray extending from the A-scale to the C-scale satisfies the equation $a = \text{ind}(c)$. Thus the A- and C-scales provide a table of anti-indices in a graphic form. With a little searching (because the c 's are not appearing in the natural order), the A- and C-scales may also be considered as a graphic table of indices mod 29.

Before we continue our discussion of why the circular slide rule works, we want to extend the notion of the congruence modulo n relation on the set of integers to the set of all real numbers. This will facilitate the use of mod 2π .

Definition:

Let α be a fixed positive real number. Two real numbers a and b are said to be congruent modulo α , if and only if $a - b = \alpha k$ for some integer k . If a and b are congruent modulo α , we denote this by $a \equiv b \pmod{\alpha}$,

Clearly, this relation is an equivalence relation on the set of real numbers. Now we can use this notion to describe the equivalence of two polar angles. Recall that, if θ_1 and θ_2 are two polar angles with the same initial sides, then their terminal sides will coincide if and only if $\theta_1 \equiv \theta_2 + 2\pi k$, where k is an integer, or, in other words, if and only if $\theta_1 \equiv \theta_2 \pmod{2\pi}$. Thus $\theta_1 \equiv \theta_2 \pmod{2\pi}$ is equivalent to the usual "equal relation" for angles.

Now assume that $c_1 \equiv c_2 \pmod{29}$. Then $\text{ind}(c_1) \equiv \text{ind}(c_2) \pmod{28}$, and this implies $\text{ind}(c_1) = \text{ind}(c_2) + 28m$ for some integer m . Hence, by multiplying both sides by $k = (2\pi)/(28)$, we obtain $k \text{ind}(c_1) = k \text{ind}(c_2) + 2\pi m$ and this is equivalent to the congruence $k \text{ind}(c_1) \equiv k \text{ind}(c_2) \pmod{2\pi}$, so that, with reference to the C-scale, we have $\theta(c_1) \equiv \theta(c_2) \pmod{2\pi}$. This shows that $\theta(c_1)$ and $\theta(c_2)$ are congruent angles. This means that this slide rule automatically takes care of the need to stay within the same residue class, mod 29, in the C- and D-scales (and mod 28 in the case of the A-scale) for the same position on the circular scales.

Earlier we said that, using the circular slide rule, we could find the product of two nonzero integers x and y mod 29.

In the notation of the congruence relation, this becomes $xy \equiv z \pmod{29}$, which is equivalent to

$\text{ind}(x) + \text{ind}(y) \equiv \text{ind}(z) \pmod{28}$. This implies the equality of $\text{ind}(x) + \text{ind}(y) = \text{ind}(z) + 28m$ for some integer m . Multiplying all terms by $k = (2\pi)/28$, we get the equality $k \text{ind}(x) + k \text{ind}(y) = k \text{ind}(z) + 2\pi m$ which implies $k \text{ind}(x) + k \text{ind}(y) \equiv k \text{ind}(z) \pmod{2\pi}$. In terms of the polar angles of the C- and D-scales, this last congruence is equivalent to the congruence $\theta(x) + \theta(y) \equiv \theta(z) \pmod{2\pi}$. Thus multiplying two integers is accomplished by adding the polar angles corresponding to their indices.

Next we will show how to use the circular slide rule to solve linear congruences, that is, congruence equations of the form $ax \equiv b \pmod{29}$, where $\text{gcd}(a, 29) = \text{gcd}(b, 29) = 1$. Taking the index of both sides of the above congruence, we obtain $\text{ind}(a) + \text{ind}(x) \equiv \text{ind}(b) \pmod{28}$. Now we rotate the disk carrying the A- and C-scales so that the 1 on the C-scale coincides with the a on the D-scale. Then the solution x is the number on the C-scale that coincides with b on the D-scale.

Examples:

a. Solve $3x \equiv 7 \pmod{29}$.

We rotate the smaller disk so that $C(1)$ is on $D(3)$; that is, the 1 on the C-scale is on the 3 on the D-scale. Then $C(x)$, the answer, coincides with $D(7)$, so that $3 \cdot 12 \equiv 7 \pmod{29}$ or $x \equiv 12 \pmod{29}$. See the Figure 8 (of the A-, C-, D-scales).

b. Solve $21x \equiv 36 \pmod{29}$.

This congruence is equivalent to $21x \equiv 7 \pmod{29}$. We solve this congruence. Position C(1) over D(21). Locating D(7), we find the solution on the C-scale coinciding with D(7): $x \equiv 10 \pmod{29}$.

Inverses and Solving Binomial Congruences

Our next objective is to consider the possibility of using the slide rule to find the inverse of an integer a modulo 29.

First recall that, if a is an integer relatively prime to n, a solution to the equation $ax \equiv 1 \pmod{n}$ is called an inverse of a modulo n.

The equation $ax \equiv 1 \pmod{29}$ is equivalent to $\text{ind}(a) + \text{ind}(x) \equiv \text{ind}(1) \pmod{\phi(29)}$, and further to $\text{ind}(a) \equiv \text{ind}(1) - \text{ind}(x) \pmod{28}$. But $\text{ind}(1) = 0 \equiv 28 \pmod{28}$. Thus the equation $ax \equiv 1 \pmod{29}$ is equivalent to $\text{ind}(a) \equiv -\text{ind}(x) \pmod{28}$. Since we are using the circular slide rule, we express the congruence in terms of angles. Multiplying both sides of the congruence by $k = (2\pi)/(28)$, we have $((2\pi)/(28)\text{ind}(a) \equiv ((2\pi)/(28)(-\text{ind}(x)) \pmod{28 \cdot (2\pi)/(28)}$.

Hence $k \text{ind}(a) \equiv -k \text{ind}(x) \pmod{2\pi}$. It would seem, then, in order to calculate inverses, we need a scale with labels opposite to the D-scale (the last scale constructed so far),

or, in other words, the labels will be the same as on the D-scale but in a clockwise direction. Recall that numbers on the D-scale are the indices of the integers in the set $\{1, 2, \dots, 28\}$ placed in a counterclockwise direction. The fourth circular scale, the R-scale does this. See Figure 9.

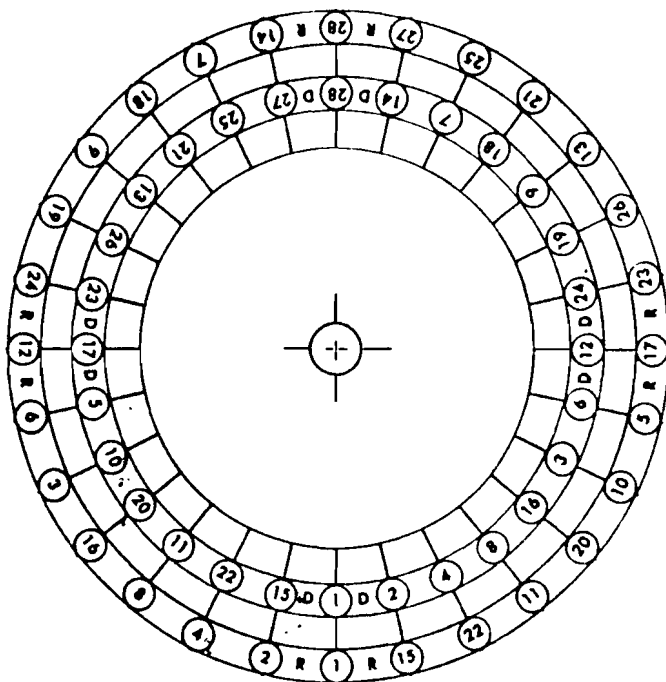


FIGURE 9

The exact description of the R-scale is:

R-scale: $\theta(r) = -k \text{ ind}(r)$, $r = 2, 4, \dots, 1$ as on the C-scale but in a clockwise direction. By the definition of the R-scale, the congruence $k \text{ ind}(a) \equiv -k \text{ ind}(x) \pmod{2\pi}$ becomes $k \text{ ind}(d) \equiv -k \text{ ind}(r) \pmod{2\pi}$, or, in polar angles, $\theta(d) \equiv \theta(r) \pmod{2\pi}$.

In this case, given a particular a , its inverse is the corresponding number on the R-scale. Thus a ray extending from the D-scale to the R-scale satisfies the equation

$dr \equiv 1 \pmod{29}$. This gives the inverse for d ; that is, it gives $r \pmod{29}$.

Examples:

a. Solve $7x \equiv 1 \pmod{29}$.

We locate 7 on the D-scale and read the number on the R-scale that coincides with it. In this case $x \equiv 25 \pmod{29}$.

b. Solve $13x \equiv 1 \pmod{29}$.

We locate 13 on the D-scale and find that, on the R-scale, 9 coincides with it so that $x \equiv 9 \pmod{29}$.

Finally, we would like to investigate the possibility of using the modular slide rule in solving binomial congruence equations of the form $ax^k \equiv b \pmod{29}$, where $\gcd(a, 29) = \gcd(b, 29) = 1$.

In Section 3.2 when we discussed solving binomial congruence equations, we found that, by the use of inverses, we could reduce the congruence to one of the form $x^k \equiv b \pmod{29}$. As we showed, we can find inverses by using the D- and R-scales.

Once we reduce the binomial congruence to the form $x^k \equiv b \pmod{29}$, how do we solve this equation with the modular slide rule? We will begin by considering quadratic congruence equations of the form $x^2 \equiv b \pmod{29}$. This equation is equivalent to the linear equation

$2 \text{ ind}(x) \equiv \text{ind}(b) \pmod{28}$. Theorem 3.6 says there is a solution to this congruence if and only if $d \mid \text{ind}(b)$ where $d = \text{gcd}(2, 28)$. In other words, the index of b must be an even integer and then there will be two solutions.

If we expect to solve the equation on the slide rule, we will need a specially tailored scale that provides two solutions for each number x . Further, it will be a scale with only half of the 28 indices, those with values that are even numbers since the odd valued indices have no solutions. The fifth circular scale, the Q-scale, is such a scale. Pictured below is the complete modular circular slide rule mod 29. (A workable model is provided for the reader on the next page.)

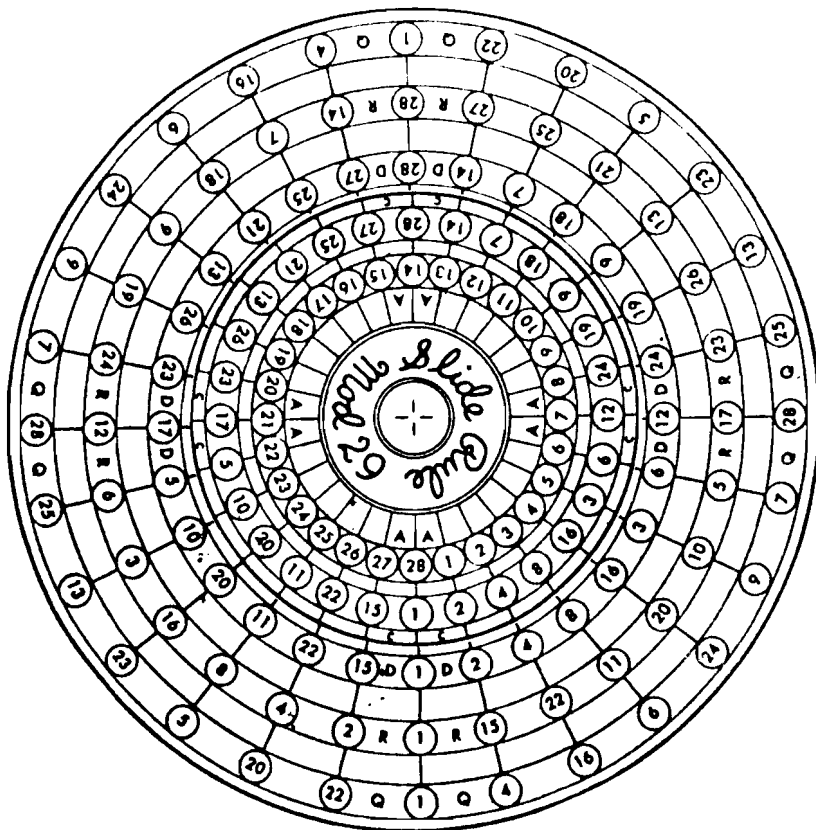
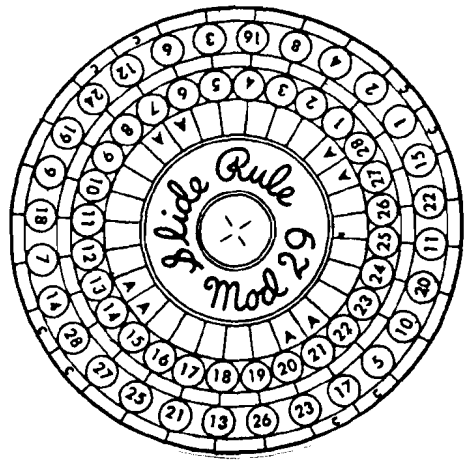
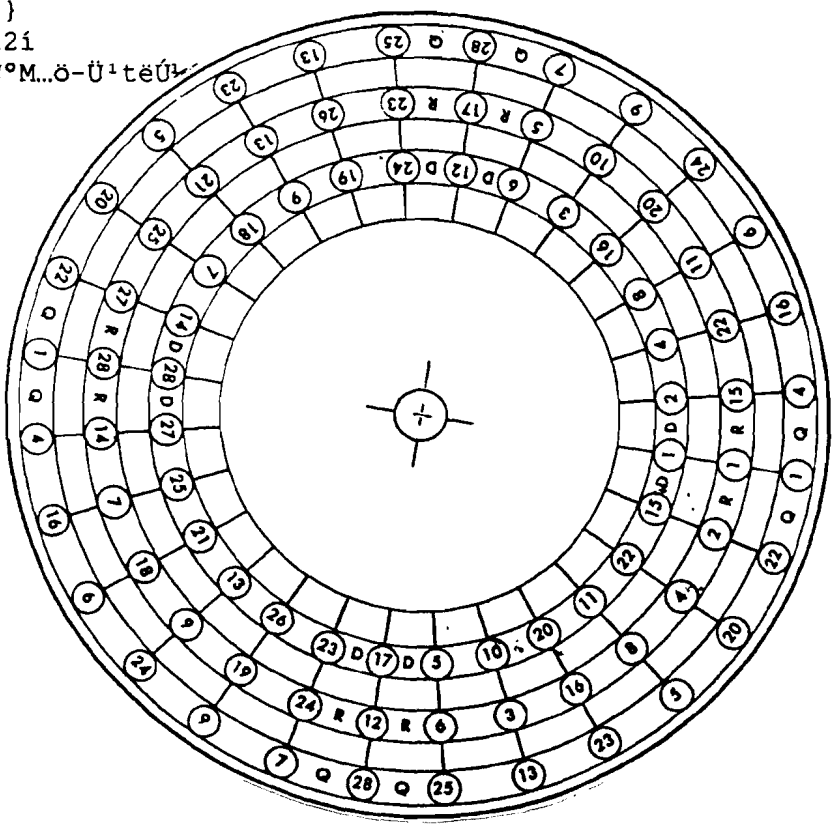
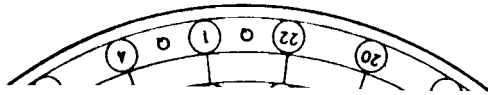


FIGURE 10

4~]žzofipip-°w>o YziBi[iYÀ·J
 -<~0;A |:|0lčA%ñ+rkhliÆp ;zü'p' \$Kš<%2¥È•,0²| 3|i™4kâsi3Sf <{úúy
 'D;D<~=Š4ér;J>:}
 5°ôŠFR½Š5«ö-\i2i
 6-øtdĚ-ûj6-úplŮ°M...ö-Ů'teŮ
 ø+PÀ,,





A WORKABLE MODEL OF THE
MODULAR CIRCULAR SLIDE RULE

The exact description of the Q-scale is:

Q-scale: $\theta(q) = k \text{ (ind}(q)\text{)}/2$, if $\text{ind}(q)$ is even;

$q = 4, 16, \dots, 1$ as given on the Q-scale. It should be

noted that each number listed on the Q-scale is listed

twice, π apart, since there will be two solutions. This

implies a modulus not of 2π but π . The definition of the Q-

scale allows for this. Using the D- and Q-scales to find

the solutions to the equation $x^2 \equiv b \pmod{29}$, we find the

congruence equivalent to $2 \text{ ind}(d) \equiv \text{ind}(q) \pmod{28}$, and

then to $\text{ind}(d) \equiv (\text{ind}(q))/2 \pmod{14}$, and then to

$k \text{ ind}(d) \equiv k (\text{ind}(q))/2 \pmod{\pi}$. By polar angles, this is

$\theta(d) \equiv \theta(q) \pmod{\pi}$.

The following example illustrates the mechanics of using the D- and Q-scales to solve quadratic congruences.

Example:

Solve $x^2 \equiv 24 \pmod{29}$.

This congruence is equivalent to $2 \text{ ind}(x) \equiv \text{ind}(24) \pmod{28}$.

Since $\text{ind}(24) = 8$, and even number, there are two

solutions. Locating the two(24)'s on the Q-scale and

following the two rays to the D-scale, we find $d_1 = 13$ and

$d_2 = 16$. thus $13^2 \equiv 24 \pmod{29}$ and $16^2 \equiv 24 \pmod{29}$.

This discussion of the Q-scale, along with the above example, supports the general situation in which, for

$x^2 \equiv a \pmod{p}$, there will be $\frac{1}{2}\phi(p)$ integers a that are quadratic residues mod p and $\frac{1}{2}\phi(p)$ integers a that are quadratic non-residues.

We know now that the circular slide rule aids in the solutions of quadratic congruences. In fact, it has a special scale, the Q-scale, specifically for these congruences. The next question is this: Is the slide rule useful in solving the more general equations of the form $x^k \equiv b \pmod{29}$? The answer is "only somewhat." Consider the following examples.

Examples:

a. Solve $x^4 \equiv 20 \pmod{29}$.

Theorem 3.6 says there will be a solution to the congruence if $d \mid \text{ind}(20)$ where $d = \text{gcd}(4, 28)$. Using the A- and C-scales, we find that $\text{ind}(20) = 24$. So there will be four solutions. This poses a problem if we intend to use the Q-scale to find the solutions since the Q-scale is equipped for dual solutions. We remedy the situation by letting $y = x^2$ and solving the alternate equation $y^2 \equiv 20 \pmod{29}$. Locating the two (20)'s on the Q-scale and following the two rays to the D-scale, we find $y_1 = 7$ and $y_2 = 22$. We then identify the four solutions to the original equations by solving the two congruences: $x^2 \equiv 7 \pmod{29}$, where x_1 will be 6 and x_2 will be 23, and $x^2 \equiv 22 \pmod{29}$, where $x_1 = 4$ and $x_2 = 15$. Thus the four solutions are

$x \equiv 6, 14, 15, 23 \pmod{29}$. With repeated substitutions and appropriate alternate congruences, it is possible, therefore, to use a modular slide rule to solve congruences of the form $x^{2^k} \equiv a \pmod{p}$ for positive integers k .

b. Solve $x^3 \equiv 7 \pmod{29}$.

There is a solution if $d \mid \text{ind}(7)$ where $d = \text{gcd}(3, 28)$. Of course d does divide $\text{ind}(7)$ so there is a unique solution. We note that the congruence is equivalent to $3 \text{ ind}(x) \equiv \text{ind}(7) \pmod{28}$. Using the A- and C-scales on the slide rule, we find that $\text{ind}(7) = 12$. The congruence now is $3 \text{ ind}(x) \equiv 12 \pmod{28}$. Dividing it by 3 reduces it to $\text{ind}(x) \equiv 4 \pmod{28}$. Again using the A- and C-scales, we discover that $x \equiv 16 \pmod{29}$. In arriving at the solution, we found the slide rule to be of no greater assistance than would be a regular index table mod 29.

This concludes our discussion of the modular, circular slide rule. We have shown that it is very useful in solving certain congruence equations. We wish to emphasize at this point, however, that our intent in discussing the modular slide rule was not to produce a "wonder tool." Rather, it was to establish the fact that, since indices can be used to construct a workable slide rule, this is another area of similarity between indices and logarithms.

Chapter 4
VECTOR INDICES

The index theory as developed in Chapter 3 is valid only for moduli with primitive roots. In this chapter our objective is to extend the theory of indices to arbitrary moduli.

4.1 INDICES TO ANY ODD MODULI

Let n be any odd integer with the canonical prime factorization $n = p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}$, where the p_i 's are distinct odd primes, $e_i > 0$, and $m \geq 2$. Let g_i be a primitive root of $p_i^{e_i}$. Then, using Theorem 1.10, the Chinese Remainder Theorem, we can find a unique solution $z \pmod{n}$ to the system of linear congruences:

$$\begin{aligned}x &\equiv g_1 \pmod{p_1^{e_1}} \\x &\equiv g_2 \pmod{p_2^{e_2}} \\&\vdots \\x &\equiv g_m \pmod{p_m^{e_m}}\end{aligned}$$

Thus for any $i = 1, 2, \dots, m$, we have $z \equiv g_i \pmod{p_i^{e_i}}$. We shall call the unique solution, $z \pmod{n}$, a pseudo primitive root of n . Let a be any number relatively prime to n and, therefore, relatively prime to all the $p_i^{e_i}$'s. For each $i = 1, 2, \dots, m$, let $h_i = \text{ind}_{g_i}(a)$ be the index of a to the base $g_i \pmod{p_i^{e_i}}$. Then $g_i^{h_i} \equiv a \pmod{p_i^{e_i}}$ and, since

$z \equiv g_i \pmod{p_i^{a_i}}$, we have $z^{h_i} \equiv a \pmod{p_i^{a_i}}$ for $i = 1, 2, \dots, m$. This observation leads to the following definition.

Definition:

Let n be an odd integer and a an integer relatively prime to n . The index vector of a to the base $z \pmod{n}$ is denoted by $IND_z(a)$ and is defined as an ordered m -tuple $IND_z(a) \equiv [h_1, h_2, \dots, h_m] \pmod{[\phi(p_1^{a_1}), \dots, \phi(p_m^{a_m})]}$, where h_i 's are integers that satisfy the congruences $z^{h_i} \equiv a \pmod{p_i^{a_i}}$ for $i = 1, 2, \dots, m$.

Examples:

For $n = 35$, find z and then find $IND_z(2)$ and $IND_z(4)$. To find z , we use the Chinese Remainder Theorem. We are looking for the common solution, \bar{x} , to the system

$$x_1 \equiv 2 \pmod{5}, \text{ where } 2 \text{ is a primitive root of } 5$$

$$x_2 \equiv 3 \pmod{7}, \text{ where } 3 \text{ is a primitive root of } 7.$$

$n = 5 \cdot 7 = 35$; let $N_1 = (35)/5 = 7$, and $N_2 = (35)/7 = 5$.

Now we consider an alternate set of congruences:

$$N_1 x_1 \equiv 1 \pmod{5}, \text{ or } 7x_1 \equiv 1 \pmod{5};$$

$$\text{the solution is } x_1 \equiv 3 \pmod{5}$$

$$N_2 x_2 \equiv 1 \pmod{7}, \text{ or } 5x_2 \equiv 1 \pmod{7};$$

$$\text{the solution is } x_2 \equiv 3 \pmod{7}.$$

By the Chinese Remainder Theorem, $\bar{x} = 2 N_1 x_1 + 3 N_2 x_2 = 2 \cdot 7 \cdot 3 + 3 \cdot 5 \cdot 3 = 87$. Therefore, $\bar{x} \equiv 87 \equiv 17 \pmod{35}$. Thus $z = 17$ is a pseudo primitive root of 35.

To find $\text{IND}_z(2)$, we consider the congruence

$\text{IND}_z(2) \equiv [h_1, h_2] \pmod{[4, 6]}$, where $h_1 \equiv \text{ind}_2(2) \pmod{5}$ and $h_2 \equiv \text{ind}_3(2) \pmod{7}$. We discover that $h_1 = 1$ and $h_2 = 2$. Therefore $\text{IND}_z(2) \equiv [1, 2] \pmod{[4, 6]}$.

To find $\text{IND}_z(4)$, we must identify h_1 and h_2 in the congruence

$\text{IND}_z(4) \equiv [h_1, h_2] \pmod{[4, 6]}$. We find that $h_1 = 2$ and $h_2 = 4$ so $\text{IND}_z(4) \equiv [2, 4] \pmod{[4, 6]}$.

Theorem 4.1

Let a and b be two integers relatively prime to an odd integer n . Then

(1) $\text{IND}_z(ab) \equiv \text{IND}_z(a) + \text{IND}_z(b) \pmod{[\phi(p_1^e), \dots, \phi(p_m^e)]}$, where the addition on the right hand side is the usual component wise addition of vectors.

(2) $\text{IND}_z(a^k) \equiv k \text{IND}_z(a) \pmod{[\phi(p_1^e), \dots, \phi(p_m^e)]}$, where k is a positive integer and $k \text{IND}_z(a)$ means the usual component wise scalar multiplication of k by the vector $\text{IND}_z(a)$.

Proof:

(1) Let $\text{IND}(a) = [h_1, h_2, \dots, h_m]$; then

$z^{h_i} \equiv a \pmod{p_i^e}$. . . (1) for all i . Let

$\text{IND}(b) = [h'_1, h'_2, \dots, h'_m]$; then

$z^{h'_i} \equiv b \pmod{p_i^e}$. . . (2) for all i . If we multiply (1) by

(2), we have the congruence $(z^{h_i}) \cdot (z^{h'_i}) \equiv ab \pmod{p_i^e}$, which

implies $z^{h_i+h'_i} \equiv ab \pmod{p_i^e}$. . . (3) Let

$\mathbf{IND}(ab) = [h''_1, h''_2, \dots, h''_m]$; then $z^{h''_i} \equiv ab \pmod{p_i^{e_i}} \dots$

(4) for all i . The congruences (4) and (3) imply

$z^{h''_i} \equiv z^{h_i+h'_i} \pmod{p_i^{e_i}}$ for all i . This implies

$h''_i \equiv h_i + h'_i \pmod{\phi(p_i^{e_i})}$ for all i , or

$[h''_1, h''_2, \dots, h''_m] \equiv [h_1, h_2, \dots, h_m] + [h'_1, h'_2, \dots, h'_m]$

$\pmod{[\phi(p_1^{e_1}), \dots, \phi(p_m^{e_m})]}$. Therefore

$\mathbf{IND}(ab) \equiv \mathbf{IND}(a) + \mathbf{IND}(b) \pmod{[\phi(p_1^{e_1}), \dots, \phi(p_m^{e_m})]}$.

(2) Let $\mathbf{IND}(a) = [h_1, h_2, \dots, h_m]$; then $z^{h_i} \equiv a \pmod{p_i^{e_i}}$.

If we raise the congruence $z^{h_i} \equiv a \pmod{p_i^{e_i}}$ to the k^{th} -power,

we have $(h_i)^k \equiv a^k \pmod{p_i^{e_i}}$, or $z^{kh_i} \equiv a^k \pmod{p_i^{e_i}} \dots$ (5).

Let $\mathbf{IND}(a^k) = [h'_1, h'_2, \dots, h'_m]$; then $z^{h'_i} \equiv a^k \pmod{p_i^{e_i}}$

\dots (6) Then, by (6) and (5), $z^{h'_i} \equiv z^{kh_i} \pmod{p_i^{e_i}}$. This

implies $h'_i \equiv kh_i \pmod{\phi(p_i^{e_i})}$. Therefore $\mathbf{IND}(a^k) \equiv k \mathbf{IND}(a)$

$\pmod{[\phi(p_1^{e_1}), \dots, \phi(p_m^{e_m})]}$. □

The above theorem and the foregoing definition, and examples imply that we can use the indices of the prime factors of n to solve congruences mod n , provided that $\gcd(a, n) = 1$.

Example:

Solve $4x^7 \equiv 25 \pmod{143}$.

This is equivalent to $4x^7 \equiv 5^2 \pmod{(11 \cdot 13)}$. This implies

$\mathbf{IND}(4) + 7 \mathbf{IND}(x) \equiv 2 \mathbf{IND}(5) \pmod{[10, 12]}$, or

$7 \mathbf{IND}(x) \equiv 2 \mathbf{IND}(5) - \mathbf{IND}(4) \pmod{[10, 12]}$, or

$7 \mathbf{IND}(x) \equiv 2 [4, 9] - [2, 2] \pmod{[10, 12]}$ or

$7 \text{ IND}(x) \equiv [8, 18] - [2, 2] \pmod{[10, 12]}$, or

$7 \text{ IND}(x) \equiv [6, 16] \equiv [6, 4] \pmod{[10, 12]}$. To complete the solution, we multiply by the inverse of 7 mod 10 and the inverse of 7 mod 12. The congruence then becomes

$\text{IND}(x) \equiv [6 \cdot 3, 4 \cdot 7] \equiv [18, 28] \pmod{[10, 12]}$, or

$\text{IND}(x) \equiv [8, 4] \pmod{[10, 12]}$. Therefore $x \equiv 3 \pmod{143}$.

4.2 INDICES FOR POWERS OF 2 MODULI

From Lemma 2.8, we know that if $\beta \geq 3$, then the integer $n = 2^\beta$ does not have a primitive root. Moreover, we have shown in Theorem 2.5 that an integer a , relatively prime to an integer n , is a primitive root mod n if and only if the integers $a, a^2, \dots, a^{\phi(n)}$ form a reduced residue system mod n . In the case of $n = 2^\beta$, $\beta \geq 3$, we are going to show that the two sets of integers, $\{5^\gamma | 1 \leq \gamma \leq 2^{\beta-2}\}$ and $\{-5^\gamma | 1 \leq \gamma \leq 2^{\beta-2}\}$, taken together, form a reduced residue system mod 2^β .

Theorem 4.2

Let β be an integer such that $\beta \geq 3$. Then

- (1) Every odd integer x satisfies the congruence $x^{2^{\beta-2}} \equiv 1 \pmod{2^\beta}$.
- (2) The order of 5 (mod 2^β) is $2^{\beta-2}$; that is $\text{ord}_{2^\beta}(5) = 2^{\beta-2}$.
- (3) The set of integers $\{\pm 5^\gamma | \gamma \text{ is an integer, and } 1 \leq \gamma \leq 2^{\beta-2}\}$ forms a reduced residue system mod 2^β .

Proof:

(1) The proof is by mathematical induction on β . The congruence is true for $\beta = 3$ since $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$. Assuming the congruence true for k , we will show it is true for $k+1$. Assume $x^{2^{k-2}} \equiv 1 \pmod{2^k}$ is true for some $k \geq 3$; then we have the equality $x^{2^{k-2}} = 1 + 2^k t$ for some integer t . Squaring both sides, we get

$$x^{2^{k-1}} = 1 + 2^{k+1}t + 2^{2k}t^2, \text{ which implies}$$

$$x^{2^{k-1}} \equiv 1 + \pmod{2^{k+1}} \text{ since } 2^{k+1} \mid (2^{k+1}t + 2^{2k}t^2 = 2^{k+1}(t + 2^{k-1}t^2)). \text{ Thus } x^{2^{\beta-2}} \equiv 1 \pmod{2^\beta} \text{ for every } \beta \geq 3.$$

(2) Let $\text{ord}_2(5) = \delta$. By part (1) we know $5^{2^{\beta-2}} \equiv 1 \pmod{2^\beta}$.

We claim the $\delta = 2^{\beta-2}$. By Theorem 2.1, $\delta \mid 2^{\beta-2}$. Assume the contrary, $\delta < 2^{\beta-2}$. First we are going to show $\delta \mid 2^{\beta-3}$. Since

$$\delta \mid 2^{\beta-2}, \text{ then } 2^{\beta-2} = \delta h \text{ for some even integer } h, \text{ say } 2m \text{ for}$$

$$\text{some integer } m. \text{ But } 2^{\beta-3} = 2^{\beta-2}2^{-1} = \delta h 2^{-1} = \delta 2m 2^{-1} = \delta m. \text{ And}$$

$$\text{therefore } \delta \mid 2^{\beta-3}. \text{ By Theorem 2.1, since } \text{ord}_{2^\beta}(5) \mid 2^{\beta-3}, \text{ then}$$

$$5^{2^{\beta-3}} \equiv 1 \pmod{2^\beta} \dots (*) \text{. Next we are going to show that}$$

$$\text{for all } \beta \geq 3, 5^{2^{\beta-3}} = 1 + 2^{\beta-1} + 2^\beta T \dots (\#) \text{ for some}$$

integer T . The proof is by mathematical induction on β .

$$\text{Let } \beta = 3. \text{ Then } 5^{2^0} = 5 = 1 + 2^2 + 2^3(0), \text{ where } T = 0.$$

Assuming $5^{2^{k-3}} = 1 + 2^{k-1} + 2^k T$ is true for some $k \geq 3$, where T is an integer, and squaring both sides, we get

$$5^{2^{k-2}} = 1 + 2^k + 2^{k+1} (T + 2^{k-3} + 2^{k-1}T + 2^{k-1}T^2). \text{ Thus we}$$

conclude by induction that $(\#)$ is valid for $\beta \geq 3$. But this

leads to a contradiction, since congruence $(*)$ implies

$1 \equiv 1 + 2^{\beta-1} + 2T \pmod{2^\beta}$ for some integer T . This implies $0 \equiv 2^{\beta-1} + 2^\beta T \pmod{2^\beta}$ or $0 \equiv 2^{\beta-1}(1 + 2T) \pmod{2^\beta}$ and this implies $2^\beta | 2^{\beta-1}(1 + 2T)$. Since $2^\beta \nmid 2^{\beta-1}$, then $2^\beta | (1 + 2T)$, a contradiction. Therefore $\delta = 2^{\beta-2}$.

(3) Let $S = \{\pm 5^\gamma | \gamma \text{ is an integer, and } 1 \leq \gamma \leq 2^{\beta-2}\}$; that is, $S = \{\pm 5^1, \pm 5^2, \dots, \pm 5^{2^{\beta-2}}\}$ or $S = \{(-1)^0 5, (-1)^0 5^2, \dots, (-1)^0 5^{2^{\beta-2}}, (-1)^1 5, (-1)^1 5^2, \dots, (-1)^1 5^{2^{\beta-2}}\}$. Let $U = \{(-1)^0 5, (-1)^0 5^2, \dots, (-1)^0 5^{2^{\beta-2}}\}$ and let $V = \{(-1)^1 5, (-1)^1 5^2, \dots, (-1)^1 5^{2^{\beta-2}}\}$ so that $U \cup V = S$. Now consider set U . By part (2), $\text{ord}_{2^\beta}(5) = 2^{\beta-2}$, so $2^{\beta-2}$ is the least integer for which the congruence $5^{2^{\beta-2}} \equiv 1 \pmod{2^\beta}$ is true. By the corollary to theorem 2.3, $5^1, 5^2, \dots, 5^{2^{\beta-2}}$ are incongruent mod 2^β . Note also that set U contains $2^{\beta-2}$ elements. Next consider set V . By the corollary to Theorem 2.3, and by the fact that $V = (-1)U$, all elements in V are incongruent mod 2^β and there are $2^{\beta-2}$ elements in the set. What, then, is true of set S ? Since all elements in U are congruent to $1 \pmod{2^\beta}$ and all elements in V are congruent to $-1 \pmod{2^\beta}$, no element in U is congruent to any element in V since $1 \equiv -1 \pmod{2^\beta}$ only if $\beta = 1$. Thus all elements in S are incongruent mod 2^β and there are $2(2^{\beta-2}) = 2^{\beta-1} = \phi(2^\beta)$ of them. Because all elements in S are odd, all element in S are relatively prime to 2. Therefore S forms a reduced residue system mod 2^β when $\beta \geq 3$. □

From part (3) of the previous theorem we know that, if a is a positive integer relatively prime to 2, then there are unique integers α and γ , where $\alpha = 0$ or 1 and $1 \leq \gamma \leq 2^{\beta-2}$ such that $a \equiv (-1)^\alpha 5^\gamma \pmod{2^\beta}$. This leads to the following definition.

Definition:

Let a be an integer relatively prime to 2. The index vector of $a \pmod{2^\beta}$ is defined to be the ordered pair (that is, vector) $[\alpha, \gamma]$ of the unique integers α and γ in the paragraph above. The index vector of $a \pmod{2^\beta}$ is denoted by $\mathbf{IND}(a)$ and we write $\mathbf{IND}(a) = [\alpha, \gamma]$.

Examples:

a. Find the index vectors of $a = 7$ and $a = 9 \pmod{16}$.

To find the index vector of $a = 7 \pmod{16}$, we know $\alpha = 0$ or 1 and $\gamma = 1, 2, \dots, 2^{\beta-2}$. For $\text{mod } 16 = \text{mod } 2^4$, $\beta = 4$ and $\gamma = 1, 2, 3$, or 4. Therefore we consider the congruence $(-1)^\alpha 5^\gamma \equiv 7 \pmod{16}$ for $\gamma = 1, 2, 3, 4$ and $\alpha = 0, 1$. We find that $(-1)^1 5^2 \equiv -25 \equiv 7 \pmod{16}$ since $16 \mid (-25-7)$.

Therefore $\mathbf{IND}(7) = [1, 2]$. To find the index vector of $a = 9 \pmod{16}$, we consider $(-1)^\alpha 5^\gamma \equiv 9 \pmod{16}$ for $\gamma = 1, 2, 3, 4$ and $\alpha = 0, 1$. We find that $(-1)^0 5^2 \equiv 25 \equiv 9 \pmod{16}$ since $16 \mid (25-9)$. Therefore $\mathbf{IND}(9) = [0, 2]$.

b. Find the index vectors of $a = 7$ and $a = 11 \pmod{32}$.

For mod $32 = 2^5$, $\beta = 5$, and $\gamma = 1, 2, \dots, 2^3$. To find the index vector of $a = 7 \pmod{32}$, we consider $(-1)^{\alpha} 5^{\gamma} \equiv 7 \pmod{32}$ for $\gamma = 1, 2, \dots, 8$ and $\alpha = 0, 1$. We find that $(-1)^1 5^2 \equiv -25 \equiv 7 \pmod{32}$ since $32 \mid (-25-7)$. Therefore $\text{IND}(7) = [1, 2]$. To find the index vector of $a = 11 \pmod{32}$ we consider $(-1)^{\alpha} 5^{\gamma} \equiv 11 \pmod{32}$ for $\gamma = 1, 2, \dots, 8$ and $\alpha = 0, 1$. We find that $(-1)^1 5^5 \equiv -3125 \equiv 11 \pmod{32}$ since $32 \mid 3136$. Therefore $\text{IND}(11) = [1, 5]$.

Theorem 4.3

The congruence $(-1)^{\alpha} 5^{\gamma} \equiv (-1)^{\alpha'} 5^{\gamma'} \pmod{2^{\beta}}$, $\beta \geq 3$ holds if and only if $\alpha \equiv \alpha' \pmod{2}$ and $\gamma \equiv \gamma' \pmod{\phi(2^{\beta-1})}$.

Proof:

Assume that $(-1)^{\alpha} 5^{\gamma} \equiv (-1)^{\alpha'} 5^{\gamma'} \pmod{2^{\beta}}$. . . (*). First we are going to show $\alpha \equiv \alpha' \pmod{2}$. Assume the contrary, namely $\alpha \not\equiv \alpha' \pmod{2}$; thus α and α' have different parity. WLOG, assume that α is even and α' is odd. With this assumption, congruence (*) becomes $5^{\gamma} \equiv -5^{\gamma'} \pmod{2^{\beta}}$, a contradiction. Thus $\alpha \equiv \alpha' \pmod{2}$. Hence congruence (*) becomes $5^{\gamma} \equiv 5^{\gamma'} \pmod{2^{\beta}}$ and, by Theorem 2.3, this implies $\gamma \equiv \gamma' \pmod{\text{ord}_{2^{\beta}}(5)}$; but $\text{ord}_{2^{\beta}}(5) = 2^{\beta-2}$. Hence we have $\gamma \equiv \gamma' \pmod{2^{\beta-2}}$ or $\gamma \equiv \gamma' \pmod{\phi(2^{\beta-1})}$. Conversely, assume that $\alpha \equiv \alpha' \pmod{2}$ and $\gamma \equiv \gamma' \pmod{\phi(2^{\beta-1})}$. $\alpha = \alpha' \pmod{2}$ implies $\alpha = \alpha' + 2k$ for some integer k and $\gamma \equiv \gamma' \pmod{\phi(2^{\beta-1})}$ implies $\gamma = \gamma' + m \cdot \phi(2^{\beta-1}) = \gamma' + m \cdot 2^{\beta-2}$ for some integer

m. Thus $(-1)^{\alpha}5^{\gamma} = (-1)^{\alpha'+2k} \cdot 5^{\gamma'+m} \cdot 2^{\beta-2} = (-1)^{\alpha'} \cdot (-1)^{2k} \cdot 5^{\gamma'} \cdot (5^{2^{\beta-2}})^m \equiv (-1)^{\alpha'} \cdot 5^{\gamma'} \pmod{2^{\beta}}$. □

Corollary:

Let a and b be integers relatively prime to 2. Let $\text{IND}(a) = [\alpha, \gamma]$ and $\text{IND}(b) = [\alpha', \gamma']$. Then $\text{IND}(a) = \text{IND}(b)$ if and only if $\alpha \equiv \alpha' \pmod{2}$ and $\gamma \equiv \gamma' \pmod{\phi(2^{\beta-1})}$.

Theorem 4.4

Let a and b be integers relatively prime to 2. Then

- (1) $\text{IND}(ab) \equiv \text{IND}(a) + \text{IND}(b) \pmod{[2, \phi(2^{\beta-1})]}$,
- (2) $\text{IND}(a^k) \equiv k \text{IND}(a) \pmod{[2, \phi(2^{\beta-1})]}$.

Proof:

(1) Let $\text{IND}(a) = [\alpha, \gamma]$; then $(-1)^{\alpha}5^{\gamma} \equiv a \pmod{2^{\beta}}$.

Let $\text{IND}(b) = [\alpha', \gamma']$; then $(-1)^{\alpha'}5^{\gamma'} \equiv b \pmod{2^{\beta}}$.

Multiplying $(-1)^{\alpha}5^{\gamma} \equiv a \pmod{2^{\beta}}$ by $(-1)^{\alpha'}5^{\gamma'} \equiv b \pmod{2^{\beta}}$, we get $((-1)^{\alpha}5^{\gamma})((-1)^{\alpha'}5^{\gamma'}) \equiv ab \pmod{2^{\beta}}$. This implies

$(-1)^{\alpha+\alpha'}5^{\gamma+\gamma'} \equiv ab \pmod{2^{\beta}}$. Now let $\text{IND}(ab) = [\alpha'', \gamma'']$; then

$(-1)^{\alpha''}5^{\gamma''} \equiv ab \pmod{2^{\beta}}$. Since $(-1)^{\alpha''}5^{\gamma''} \equiv ab \pmod{2^{\beta}}$ and

$(-1)^{\alpha+\alpha'}5^{\gamma+\gamma'} \equiv ab \pmod{2^{\beta}}$, then

$(-1)^{\alpha''}5^{\gamma''} \equiv (-1)^{\alpha+\alpha'}5^{\gamma+\gamma'} \pmod{2^{\beta}}$. By Theorem 4.3,

$[\alpha'', \gamma''] \equiv [\alpha+\alpha', \gamma+\gamma'] \pmod{[2, \phi(2^{\beta-1})]}$ or

$[\alpha'', \gamma''] \equiv [\alpha, \gamma] + [\alpha', \gamma'] \pmod{[2, \phi(2^{\beta-1})]}$. Therefore

$\text{IND}(ab) \equiv \text{IND}(a) + \text{IND}(b) \pmod{[2, \phi(2^{\beta-1})]}$.

(2) Let $\text{IND}(a) = [\alpha, \gamma]$ such that $(-1)^{\alpha}5^{\gamma} \equiv a \pmod{2^{\beta}}$. If we raise the congruence $(-1)^{\alpha}5^{\gamma} \equiv a \pmod{2^{\beta}}$ to the k^{th} power, we

get $((01)^{\alpha}5^{\gamma})^k \equiv a^k \pmod{2^{\beta}}$. This implies $(-1)^{k\alpha}5^{k\gamma} \equiv a^k \pmod{2^{\beta}}$. . . (*). Let $\text{IND}(a^k) = [\alpha', \gamma']$; then $(-1)^{\alpha'5^{\gamma'}} \equiv a^k \pmod{2^{\beta}}$. . . (#). Congruences (#) and (*) imply $(-1)^{\alpha'5^{\gamma'}} \equiv (-1)^{k\alpha}5^{k\gamma} \pmod{2^{\beta}}$. By Theorem 4.3, $[\alpha', \gamma'] \equiv [k\alpha, k\gamma] \pmod{[2, \phi(2^{\beta-1})]}$ or $[\alpha, \gamma] \equiv k[\alpha, \gamma] \pmod{[2, \phi(2^{\beta-1})]}$. Therefore $\text{IND}(a^k) \equiv k \text{IND}(a) \pmod{[2, \phi(2^{\beta-1})]}$. □

Examples:

a. Solve $11x^5 \equiv 7 \pmod{32}$.

By Theorem 4.4, this congruence is equivalent to the congruence $5 \text{IND}(x) \equiv \text{IND}(7) - \text{IND}(11) \pmod{[2, \phi(2^4)]}$. To solve this second congruence, we must know the value of $\text{IND}(7)$ and $\text{IND}(11) \pmod{16}$. From the examples worked earlier in this section, we recall that $\text{IND}(7) = [1, 2]$ and $\text{IND}(11) = [1, 5]$. Therefore

$$5 \text{IND}(x) \equiv [1, 2] - [1, 5] \pmod{[2, 8]}$$

or $5 \text{IND}(x) \equiv [0, -3] \pmod{[2, 8]}$. Now we find the inverses of 5 (mod 2) by solving $5y \equiv 1 \pmod{2}$ (we obtain $y = 1$), and the inverse of 5 (mod 8) by solving $5y' \equiv 1 \pmod{8}$ (we obtain $y' = 5$). Thus we have $\text{IND}(x) \equiv [0, -15] \pmod{[2, 8]}$ or $\text{IND}(x) \equiv [0, 1] \pmod{[2, 8]}$. The value of x is given by $x \equiv (-1)^{05^1} \pmod{32}$. Hence the solution is $x \equiv 5 \pmod{32}$.

b. Solve $3^x \equiv 7 \pmod{32}$.

This congruence is equivalent to $x \text{IND}(3) \equiv$

$\text{IND}(7) \pmod{[2,8]}$. We know $\text{IND}(7) = [1,2]$. To find the value of $\text{IND}(3)$, we consider the congruences $(-1)^0 5 \equiv 3 \pmod{32}$ for $\gamma = 1, 2, \dots, 8$, and $(-1)^1 5 \equiv 3 \pmod{32}$ for $\gamma = 1, 2, \dots, 8$. We find $(-1)^1 5^3 \equiv -125 \equiv 3 \pmod{32}$ since $32 \mid -128$. Therefore $\text{IND}(3) = [1,3]$ and the original congruence becomes $[1,3]x \equiv [1,2] \pmod{[2,8]}$. The inverse of $3 \pmod{8} = 3$, so the equation becomes $x \equiv [1,6] \pmod{[2,8]}$. The value of x is given by $x \equiv (-1)^1 5^6 \pmod{32}$. Thus the solution is $x \equiv 23 \pmod{32}$.

4.3 INDICES FOR ANY COMPOSITE MODULI

In this section we are going to employ the results of the previous two sections to generalize the theory of indices to any composite moduli.

To this end, let $n = 2^\beta p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}$ be the canonical prime factorization of n and let a be an integer relatively prime to n . If we let the ordered m -tuple $[g_1, \dots, g_m]$ be the primitive roots of $p_i^{e_i}$, then, as defined in section 4.1, the index vector of $a \pmod{p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}}$ is the ordered m -tuple $[h_1^{e_1}, h_2^{e_2}, \dots, h_m^{e_m}]$, where $h_1 = \text{ind}_{g_1}(a) \pmod{p_1^{e_1}}, \dots, h_m = \text{ind}_{g_m}(a) \pmod{p_m^{e_m}}$.

The factor 2^β requires the consideration of two cases. Recall that, according to Theorem 2.6, if $\beta \leq 2$, 2^β has a primitive root. Trivially 1 is the primitive root of 2 and,

since $3^2 \equiv 1 \pmod{4}$, 3 is the primitive root of 4. Call these roots g_0 and their indices h_0 . For $\beta \geq 3$, we defined $\text{IND}(a) \pmod{2^\beta}$ to be the ordered pair $[\alpha, \gamma]$ such that $(-1)^\alpha 5^\gamma \equiv a \pmod{2^\beta}$.

We can now combine these various ideas and definitions to arrive at the following definition for the index vector of an integer a , relatively prime to n , where n is any composite moduli.

Definition:

For any composite moduli n and for an integer a , relatively prime to n , the index vector of a modulo n is defined to be $[h_0^{e_0}, h_1^{e_1}, \dots, h_m^{e_m}]$ if $\beta \leq 2$ and $[\alpha, \gamma; h_1^{e_1}, h_2^{e_2}, \dots, h_m^{e_m}]$ if $\beta \geq 3$. This definition assumes the conditions as described above.

Examples:

a. For $n = 60 = 2^2 \cdot 3 \cdot 5$, find $\text{IND}(11)$ and $\text{IND}(43)$.

Since $\beta \leq 2$, we use 3 as a primitive root of 4. And 2 is a primitive root for 3 and 5. To find $\text{IND}(11)$, we must find the index of 11 (mod 4), (mod 3) and (mod 5) by solving the following congruence equations:

$$3^x \equiv 11 \pmod{4}, \text{ which has the solution } 3^1 \equiv 11 \pmod{4}$$

$$2^x \equiv 11 \pmod{3}, \text{ which has the solution } 2^1 \equiv 11 \pmod{3}$$

$$2^x \equiv 11 \pmod{5}, \text{ which has the solution } 2^4 \equiv 11 \pmod{5}$$

Thus $\text{IND}(11) = [1, 1, 4]$. To find $\text{IND}(43)$, we must solve the following congruence equations:

$$3^x \equiv 43 \pmod{4}, \text{ which has the solution } 3^1 \equiv 43 \pmod{4}$$

$$2^x \equiv 43 \pmod{3}, \text{ which has the solution } 2^2 \equiv 43 \pmod{3}$$

$$2^x \equiv 43 \pmod{5}, \text{ which has the solution } 2^3 \equiv 43 \pmod{5}$$

Thus $\text{IND}(43) = [1, 2, 3]$.

b. For $n = 120 = 2^3 \cdot 3 \cdot 5$, find $\text{IND}(17)$ and $\text{IND}(41)$.

Since $\beta \geq 3$, we use the ordered pair $[\alpha, \gamma]$ situation. To find $\text{IND}(17)$, we solve the following equations:

$$(-1)^{\alpha 5^\gamma} \equiv 17 \pmod{8}, \text{ which becomes } (-1)^{0 5^2} \equiv 17 \pmod{8}$$

$$2^x \equiv 17 \pmod{3}, \text{ which has the solution } 2^1 \equiv 17 \pmod{3}$$

$$2^x \equiv 17 \pmod{5}, \text{ which has the solution } 2^1 \equiv 17 \pmod{5}$$

Thus $\text{IND}(17) = [0, 2; 1, 1]$. To find $\text{IND}(41)$, we solve:

$$(-1)^{\alpha 5^\gamma} \equiv 41 \pmod{8}, \text{ which becomes } (-1)^{0 5^0} \equiv 41 \pmod{8}$$

$$2^x \equiv 41 \pmod{3}, \text{ which has the solution } 2^1 \equiv 41 \pmod{3}$$

$$2^x \equiv 41 \pmod{5}, \text{ which has the solution } 2^4 \equiv 41 \pmod{5}$$

Thus $\text{IND}(41) = [0, 0; 1, 4]$.

Theorem 4.5

Let a and b be integers relatively prime to n . Then

$$(1) \text{IND}(ab) = \begin{cases} \text{IND}(a) + \text{IND}(b) \pmod{[\phi(2^\beta), \phi(p_1^{\alpha_1}), \dots, \phi(p_m^{\alpha_m})]}, & \text{if } \beta \leq 2 \\ \text{IND}(a) + \text{IND}(b) \pmod{[2, \phi(2^{\beta-1}); \phi(p_1^{\alpha_1}), \dots, \phi(p_m^{\alpha_m})]}, & \text{if } \beta \geq 3 \end{cases}$$

$$(2) \text{IND}(a^k) = k \text{IND}(a) \begin{cases} \pmod{[\phi(2^\beta), \phi(p_1^{\alpha_1}), \dots, \phi(p_m^{\alpha_m})]}, & \text{if } \beta \leq 2 \\ \pmod{[2, \phi(2^{\beta-1}); \phi(p_1^{\alpha_1}), \dots, \phi(p_m^{\alpha_m})]}, & \text{if } \beta \geq 3 \end{cases}$$

Proof:

The proof follows directly from Theorems 4.1 and 4.4. \square

We close this section with examples of applying index theory to congruence equations with composite moduli.

Examples:

a. Solve $11x^7 \equiv 43 \pmod{60}$.

This congruence is equivalent to

$\text{IND}(11) + 7\text{IND}(x) \equiv \text{IND}(43) \pmod{[2,2,4]}$, or to

$7\text{IND}(x) \equiv \text{IND}(43) - \text{IND}(11) \pmod{[2,2,4]}$. Recall from the examples earlier in this section, that

$\text{IND}(43) = [1,2,3]$ and $\text{IND}(11) = [1,1,4]$. Therefore

$7\text{IND}(x) \equiv [1,2,3] - [1,1,4] \equiv [0,1,-1] \equiv [0,1,3]$

$\pmod{[2,2,4]}$. Since 7 is relatively prime to 2 and 4, we

find the inverses of 7 modulo these integers. The inverse

of 7 $\pmod{2} = 1$ and 7 $\pmod{4} = 3$. The congruence becomes

$\text{IND}(x) \equiv [0,1,3 \cdot 3] \equiv [0,1,1] \pmod{[2,2,4]}$. The integer x ,

then, will have to satisfy the following congruences:

$$3^0 \equiv x \pmod{4}$$

$$2^1 \equiv x \pmod{3}$$

$$2^1 \equiv x \pmod{5}$$

The Chinese Remainder Theorem can be used to identify x .

Since $4 \cdot 3 \cdot 5 = 60$ and $60/4 = 15$, $60/3 = 20$, and $60/5 = 12$, we consider the following congruences:

$$15x \equiv 1 \pmod{4} \text{ for which } x = 3$$

$$20x \equiv 1 \pmod{3} \text{ for which } x = 2$$

$$12x \equiv 1 \pmod{5} \text{ for which } x = 3$$

Then $\bar{x} = 1 \cdot 15 \cdot 3 + 2 \cdot 20 \cdot 2 + 2 \cdot 12 \cdot 3 = 197$. But

$197 \equiv 17 \pmod{60}$. Therefore, a solution to the original congruence is $x \equiv 17 \pmod{60}$.

b. Solve $13x^7 \equiv 281 \pmod{792}$.

This equation is equivalent to

$\text{IND}(13) + 7\text{IND}(x) \equiv \text{IND}(281) \pmod{[2,2;6,10]}$, or to

$7\text{IND}(x) \equiv \text{IND}(281) - \text{IND}(13) \pmod{[2,2,6,10]}$. . . (*).

What is $\text{IND}(281)$? What $\text{IND}(13)$? To find $\text{IND}(281)$, we solve the following congruences:

$(-1)^a 5^y \equiv 281 \equiv 1 \pmod{8}$, which becomes $(-1)^0 5^0 \equiv 1 \pmod{8}$

$2^x \equiv 281 \equiv 2 \pmod{9}$, which has the solution $2^1 \equiv 2 \pmod{9}$

$2^x \equiv 281 \equiv 6 \pmod{11}$, which becomes $2^9 \equiv 6 \pmod{11}$.

Thus $\text{IND}(281) = [0,0;1,9]$.

To find $\text{IND}(13)$, we solve the following congruences:

$(-1)^a 5^y \equiv 13 \pmod{8}$, which becomes $(-1)^0 5^1 \equiv 13 \pmod{8}$

$2^x \equiv 13 \equiv 4 \pmod{9}$, which has the solution $2^2 \equiv 4 \pmod{9}$

$2^x \equiv 13 \equiv 2 \pmod{11}$, which becomes $2^1 \equiv 2 \pmod{11}$

Thus $\text{IND}(13) = [0,1;2,1]$. Congruence (*) therefore becomes

$7\text{IND}(x) \equiv [0,0;1,9] - [0,1;2,1] \equiv [0,-1;-1,8] \equiv [0,3;5,8]$

$\pmod{[2,2;6,10]}$. Again finding the inverses of

7, $\pmod{2}$, $\pmod{6}$, and $\pmod{10}$, we have

$\text{IND}(x) \equiv [0,3 \cdot 1;5,8 \cdot 3] \equiv [0,1;5,4] \pmod{[2,2;6,10]}$. To

find x , we can make use of Table 2 and Table 3 in section

3.2. For $\pmod{9}$ and $\pmod{11}$, we find $x = 5$. Does this check

with $\pmod{8}$? Yes, since $(-1)^0 5^1 \equiv 5 \pmod{8}$. Therefore a

solution is $x \equiv 5 \pmod{792}$.

Chapter 5

PRIMITIVE ROOTS AND INDICES FROM AN ALGEBRAIC VIEWPOINT

In this chapter we are going to study briefly the concepts of primitive roots and indices from an algebraic point of view. Certain definitions from abstract algebra will be assumed and most of the results will be stated without proofs. However references are given for those results stated without proof.

In section 5.1 we introduce the ring of integers modulo n , \mathbb{Z}_n and investigate the group of its invertible elements. In section 5.2 we characterize the integers n that possess primitive roots as those integers for which the group of invertible elements in \mathbb{Z}_n is cyclic.

The introduction of algebraic structures places the theory of indices in the more general setting of abstract algebra. This approach to the study of primitive roots and indices leads in a very natural way to generalize indices to arbitrary finite cyclic groups. Section 5.3 discusses these ideas.

In moving the subject matter of this paper from the area of number theory on to the province of abstract algebra, we show the strong relationship between the two fields.

5.1 THE RING OF INTEGERS MODULO n

First, let us recall the concept of a congruence class mod n . If $a \in \mathbb{Z}$, then the set of integers congruent to a mod n , $\bar{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}$, is called a congruence (or residue) class mod n . Let \mathbb{Z}_n denote the set of all congruence classes mod n . The set \mathbb{Z}_n can be made into a ring by defining addition and multiplication on \mathbb{Z} as follows:

For $\bar{a}, \bar{b} \in \mathbb{Z}_n$, we define $\bar{a} + \bar{b} = \overline{a+b}$, and $\bar{a} \cdot \bar{b} = \overline{ab}$. With respect to these operations, it is routine to show that \mathbb{Z}_n is a commutative ring with identity, namely $\bar{1}$. This ring is called the ring of integers mod n .

Next, we are going to study the set of units in \mathbb{Z}_n , that is the set of multiplicatively invertible elements in \mathbb{Z}_n . So the question is "What are the units of \mathbb{Z}_n ?" An element $\bar{a} \in \mathbb{Z}_n$ is a unit if and only if there exists $\bar{x} \in \mathbb{Z}_n$ such that $\bar{a} \bar{x} = 1$. But $\bar{a} \bar{x} = 1$ is equivalent to saying that the congruence equation, $ax \equiv 1 \pmod{n}$, is solvable and this in turn is equivalent to saying $d \mid 1$, where $d = \gcd(a, n)$. We know that $d \mid 1$ if and only if $d = 1$. Thus $\bar{a} \in \mathbb{Z}_n$ is a unit if and only if a is relatively prime to n . Moreover, since there are $\phi(n)$ integers relatively prime to n , \mathbb{Z}_n has $\phi(n)$ units. In particular, if $n = p$ is a prime,

then every non-zero element of \mathbb{Z}_p is a unit and therefore $(\mathbb{Z}_p, +, \cdot)$ is a field.

The following theorem summarizes the above discussion.

Theorem 5.1

An element $\bar{a} \in \mathbb{Z}_n$ is a unit if and only if $\gcd(a, n) = 1$. There are exactly $\phi(n)$ units in \mathbb{Z}_n . \mathbb{Z}_n is a field if and only if n is a prime.

In what follows, we denote the set of all units of \mathbb{Z}_n by $U(n)$. It follows from Theorem 5.1 that if $\{r_1, r_2, \dots, r_{\phi(n)}\}$ is a reduced residue system mod n , then $U(n) = \{\bar{r}_1, \bar{r}_2, \dots, \bar{r}_{\phi(n)}\}$.

5.2 PRIMITIVE ROOTS AND THE GROUP STRUCTURE OF $U(n)$

In a more general context than $U(n)$, for any ring $(R, +, \cdot)$ with identity we denote by $U(R)$, the set of all units in R .

Theorem 5.2

$(U(R), \cdot)$ is a group.

(The proof of this theorem can be found in [4], page 185.)

The group $U(R)$ is called the group of units of R or the group of invertible elements of R . In particular, $U(n)$ is a group for any integer n ; it is the group of invertible integers mod n . From Theorem 5.1, it follows that the order of the group $U(n)$ is $\phi(n)$. Note that order, in the context of group theory, is defined to be the number of elements in $U(n)$.

Our objective in this section is to analyze the structure of the group $U(n)$. It turns out that $U(n)$ is either a cyclic group or a direct product of a cyclic group. In fact the next theorem gives necessary and sufficient conditions for the group $U(n)$ to be cyclic.

Theorem 5.3

$(U(n), \cdot)$ is cyclic if and only if n possesses a primitive root.

Proof:

Assume that $U(n)$ is cyclic. Thus there exists $\bar{g} \in U(n)$ such that $\langle \bar{g} \rangle = U(n)$. Hence the least positive integer k such that $\bar{g}^k = \bar{1}$ is $k = \phi(n)$. Thus the order of $g \pmod n$ is $\phi(n)$ and therefore g is a primitive root mod n . Conversely, assume that g is a primitive root mod n . Then the subgroup of $U(n)$ generated by \bar{g} is $U(n)$ since the order of $g \pmod n$ is $\phi(n)$; that is, $\langle \bar{g} \rangle = U(n)$. Thus $U(n)$ is a cyclic group.

□

Theorem 5.3 together with Theorem 2.6, implies the following result.

Corollary

$U(n)$ is cyclic if and only if n is of the form 2 , 4 , p^k , or $2p^k$, where p is an odd prime and $k \geq 1$.

Our next objective is to analyze the structure of $U(n)$ when n is other than of the form stated in the previous corollary.

The next three theorems (whose proof can be found in [14], pages 80-82) permit us to give a complete description of the group $U(n)$ for any positive integer n .

Theorem 5.4

If m and n are relatively prime positive integers, then $(U(mn), \cdot)$ is isomorphic to the direct product $U(m) \times U(n)$.

For the integers n of the form 2 , 4 , p^k , and $2p^k$, the group $U(n)$ is cyclic and therefore $U(n)$ is isomorphic to the additive group of integers mod $\phi(n)$. That is $(U(n), \cdot)$ is isomorphic to $(\mathbb{Z}_{\phi(n)}, +)$.

In the case where $n = 2^k$ when $k \geq 3$, we have the following result.

Theorem 5.5

The group $(U(2^k), \cdot)$, where $k \geq 3$ is isomorphic to the direct product of the additive groups $(\mathbb{Z}_2, +)$ and $(\mathbb{Z}_{2^{k-2}}, +)$.

That is, $U(2^k) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$.

Theorem 5.6

Let $n = 2^{k_0} p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ be the canonical prime factorization of n .

(1) The group $U(n)$ is isomorphic to the direct product $U(2^{k_0}) \times U(p_1^{k_1}) \times \dots \times U(p_r^{k_r})$.

(2) $U(p_i^{k_i})$ is a cyclic group of order $\phi(p_i^{k_i})$ and thus isomorphic to $(\mathbb{Z}_{\phi(p_i^{k_i})}, +)$.

(3) $U(2^{k_0})$ is a cyclic group of order 1 and 2 for $k_0 = 1$ and 2, respectively. If $k_0 \geq 3$, then $U(2^{k_0})$ is isomorphic to the direct product of two cyclic groups, one, $(\mathbb{Z}_2, +)$, of order 2, the other, $(\mathbb{Z}_{2^{k_0-2}}, +)$, of order 2^{k_0-2} .

5.3 INDICES IN GROUPS

First we are going to see how the definition of indices can be formulated in group theoretic language. Let n be a positive integer with a primitive root g . Then it follows from Theorem 5.3 that $U(n)$ is a cyclic group and \bar{g} is a generator of $U(n)$. That is, $U(n) = \langle \bar{g} \rangle$. Thus for any $\bar{a} \in U(n)$, or in other words, for any integer a relatively prime to n , there exists a unique integer k , where

$0 \leq k \leq \phi(n)-1$ and such that $\bar{g}^k = \bar{a}$; That is, for any integer a , there is a k such that $g^k \equiv a \pmod{n}$. The index of a to the base $g \pmod{n}$ is the unique integer k . From this it follows that if a and b are integers relatively prime to n and $a \equiv b \pmod{n}$, then $\bar{a} = \bar{b}$ and hence $\text{ind}_g(a) = \text{ind}_g(b)$. Conversely, if $\text{ind}_g(a) = \text{ind}_g(b)$, then $\bar{a} = \bar{b}$ and hence $a \equiv b \pmod{n}$. Thus we may consider the index as a map from the multiplicative group $(U(n), \cdot)$ into the additive group $(\mathbb{Z}_{\phi(n)}, +)$. Therefore we have the map $\text{ind}_g: (U(n), \cdot) \rightarrow (\mathbb{Z}_{\phi(n)}, +)$ defined by $\text{ind}_g(\bar{a}) = \overline{\text{ind}_g(a)}$. If we let $\bar{a} = \bar{g}^k$ and $\bar{b} = \bar{g}^h$, then $\bar{a}\bar{b} = \bar{g}^k \cdot \bar{g}^h$ or $\bar{a}\bar{b} = \bar{g}^{k+h}$. This implies $\text{ind}_g(\bar{a}\bar{b}) \equiv \text{ind}_g(\bar{a}) + \text{ind}_g(\bar{b}) \pmod{\phi(n)}$; hence ind_g is a group homomorphism. Clearly ind_g is one-to-one and onto. Thus we have the following theorem.

Theorem 5.7

The map $\text{ind}_g : (U(n), \cdot) \rightarrow (\mathbb{Z}_{\phi(n)}, +)$, as defined above, is a group isomorphism.

Note that this group isomorphism is analogous to the well-known group isomorphism of the multiplicative group of positive real numbers (\mathbb{R}^+, \cdot) onto the additive group of all real numbers given by $\log_a: (\mathbb{R}^+, \cdot) \rightarrow (\mathbb{R}, +)$, where a is a positive real number. Theorem 5.7 leads directly to the

concept of vector indices. Let n be any odd positive integer and let $n = p_1^{k_1} \dots p_r^{k_r}$ be the canonical prime factorization of n . By Theorem 5.6, we know there is a group isomorphism $\Psi: U(n) \rightarrow U(p_1^{k_1}) \times \dots \times U(p_r^{k_r})$. Each of the groups $U(p_i^{k_i})$ for $i = 1, 2, \dots, r$ is cyclic and hence, if $\langle \bar{g}_i \rangle = U(p_i^{k_i})$, then the map $\text{ind}_{\bar{g}_i}: U(p_i^{k_i}) \rightarrow \mathbb{Z}_{\phi(p_i^{k_i})}$ is a group isomorphism. The index vector mod n relative to the base $\bar{g} = [\bar{g}_1, \dots, \bar{g}_r]$ is defined as the composition of the two group isomorphisms Ψ and $\text{ind}_{\bar{g}_i}$. Thus

$$\begin{array}{ccc}
 \text{IND}_{\bar{g}} : U(n) & \xrightarrow{\Psi} & U(p_1^{k_1}) \times \dots \times U(p_r^{k_r}) \\
 \searrow & & \downarrow \\
 & & \mathbb{Z}_{\phi(p_1^{k_1})} \times \dots \times \mathbb{Z}_{\phi(p_r^{k_r})} \\
 & & \uparrow \\
 & & [\text{ind}_{\bar{g}_1}, \dots, \text{ind}_{\bar{g}_r}]
 \end{array}$$

is given by $\text{IND}_{\bar{g}}(\bar{a}) = [\text{ind}_{\bar{g}_1}(\bar{a}_1), \dots, \text{ind}_{\bar{g}_r}(\bar{a}_r)]$, where $\Psi(\bar{a}) = [\bar{a}_1, \dots, \bar{a}_r]$.

In the case $n = 2^k$, where $k \geq 3$, by Theorem 5.5 we have $U(2^k) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$. By Theorem 4.2, we know that if $\bar{a} \in U(2^k)$, then there exist unique integers α and γ with $\alpha = 0$ or 1 and $1 \leq \gamma \leq 2^{k-2}$ such that $\bar{a} = (-1)^\alpha 5^\gamma$. Thus the index vector mod n is defined as the group isomorphism $\text{IND} : U(2^k) \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$ given by $\text{IND}(\bar{a}) = [\alpha, \gamma]$.

The foregoing discussion leads easily to the generalization of indices to finite cyclic groups.

Definition:

Let G be a finite cyclic group of order n . Let g be a generator of G . For $a \in G$, we define the index of a relative to g to be the least nonnegative integer k for which $g^k = a$. We denote the index of a relative to g by $\text{ind}_g a$.

Clearly $0 \leq \text{ind}_g a \leq n-1$ and $g^{\text{ind}_g a} = a$ for any $a \in G$.

The following two theorems are immediate and their proofs follow directly from the definition above and the basic properties of groups.

Theorem 5.8

Let $G = \langle g \rangle$ be a cyclic group of order n . Let a and $b \in G$. Then $a = b$ if and only if $\text{ind}_g(a) \equiv \text{ind}_g(b) \pmod{n}$.

Theorem 5.9

Let $G = \langle g \rangle$ be a finite cyclic group of order n and let $a, b \in G$. Then

- (1) $\text{ind}_g e = 0$, where e is the identity element of G
- (2) $\text{ind}_g g = 1$
- (3) $\text{ind}_g a^{-1} \equiv -(\text{ind}_g a) \pmod{n} = n - \text{ind}_g a$
- (4) $\text{ind}_g(ab) \equiv \text{ind}_g a + \text{ind}_g b \pmod{n}$
- (5) $\text{ind}_g(a^k) \equiv k \text{ind}_g a \pmod{n}$, where k is any integer
- (6) $g^{\text{ind}_g a} = a$ and $\text{ind}_g g^k \equiv k \pmod{n}$
- (7) If g' is another generator of G , then $\text{ind}_{g'} a \equiv (\text{ind}_g a) \cdot (\text{ind}_g g') \pmod{n}$.

We are going to illustrate Theorem 5.10 by an example.

Let $G = \{1, -1, i, -i\}$ with ordinary multiplication of complex numbers. $G = \langle i \rangle$ is a cyclic group.

$$i^0 = 1 \rightarrow \text{ind}_i 1 = 0$$

$$i^1 = i \rightarrow \text{ind}_i i = 1$$

$$i^2 = -1 \rightarrow \text{ind}_i(-1) = 2$$

$$i^3 = -i \rightarrow \text{ind}_i(-i) = 3$$

Let us verify property (4).

$$\text{ind}_i((-1)(-i)) \equiv \text{ind}_i(-1) + \text{ind}_i(-i) \pmod{4}$$

$$\text{LHS} = \text{ind}_i((-1)(-i)) = \text{ind}_i(i) = 1$$

$$\text{RHS} = \text{ind}_i(-1) + \text{ind}_i(-i) = 2 + 3 = 5$$

$$\text{Thus } \text{ind}_i((-1)(-i)) = 1 \equiv \text{ind}_i(-1) + \text{ind}_i(-i) = 5 \pmod{4}$$

Next let us verify property (5).

$$\text{ind}_i((-i)^5) \equiv 5 \text{ind}_i(-i) \pmod{4}.$$

$$\text{LHS} = \text{ind}_i((-i)^5) = \text{ind}_i(-i) = 3$$

$$\text{RHS} = 5 \text{ind}_i(-i) = 5(3) = 15$$

$$\text{Thus } \text{ind}_i((-i)^5) = 3 \equiv 5 \text{ind}_i(-i) = 15 \pmod{4}$$

Now we verify property (3).

$$\text{ind}_i(-1)^{-1} \equiv -\text{ind}_i(-1) \pmod{4} = 4 - \text{ind}_i(-1)$$

$$\text{LHS} = \text{ind}_i(-1)^{-1} = \text{ind}_i(-1) = 2$$

$$\text{Thus } \text{ind}_i(-1)^{-1} = 2 \equiv -2 \pmod{4} = 4 - \text{ind}_i(-1) = 4 - 2.$$

Finally, we are going to verify property (7).

$g' = -i$ is another generator of G .

$$\text{ind}_i(-1) \equiv \text{ind}_{-i}(-1) \cdot \text{ind}_i(-i) \pmod{4}$$

$$\text{LHS} = \text{ind}_i(-1) = 2$$

$$\text{RHS} = \text{ind}_{-i}(-1) \cdot \text{ind}_i(-i) = (2)(3) = 6$$

Thus $\text{ind}_1(-1) = 2 \equiv \text{ind}_{-1}(-1) \cdot \text{ind}_1(-i) = 6 \pmod{4}$.

If $G = \langle g \rangle$ and $\text{ind}_g a = k$ and m is an integer such that $m \equiv k \pmod{n}$, then $m = k + nr$ for some integer r and this implies $g^m = g^k \cdot (g^n)^r = a(e)^r = a$. Thus we have $\text{ind}_g a \in \bar{k}$. Hence we may regard the index as a map from the multiplicative group G into the additive group of the ring of integers mod n, \mathbb{Z}_n ; that is $\text{ind}_g : (G, \cdot) \rightarrow (\mathbb{Z}_n, +)$. This map is called the index map to the base g or simply the index map.

Theorem 5.8 implies the map ind_g is one-to-one and, since the order of (G, \cdot) equals the order of $(\mathbb{Z}_n, +)$, then ind_g is onto. Theorem 5.9(4) implies ind_g is a group homomorphism. Thus we have proven the following theorem, a theorem from which Theorem 5.9(1,2,3, and 5) follows directly.

Theorem 5.10

The index map, $\text{ind}_g : (G, \cdot) \rightarrow ((\mathbb{Z}_n, +))$, is a group isomorphism.

Having established that the map ind_g is a group isomorphism, we are in a position to appreciate the importance of the concept of indices in group theory. The index provides no more and no less than a complete description of the whole group since the members of the

group G are determined by the powers of the generator, g .

That is, for any $a \in G$, $a = g^{\text{ind}_g(a)}$.

Chapter 6

SUMMARY AND CONCLUSION

In this thesis we have investigated the theory of indices modulo n . In the process we have indicated similarities to the theory of logarithms.

To make the paper self contained, in Chapter 1 we provided definitions and theorems from elementary number theory which would be useful to the reader as background.

Since primitive roots are basic to the theory of indices, we spent the next chapter investigating this idea. We began with the concept of the order of an integer modulo n . This led to the definition and the study of the basic properties of primitive roots. Chapter 2 concluded with a complete characterization of which integers have primitive roots and which do not.

The objective of Chapter 3 was the study of scalar indices and their basic properties. Where appropriate, we indicated similarities between indices and logarithms in both theory and applications. The analogy between indices and logarithms additionally served as a motivation to introduce certain results. We defined scalar indices for integers with primitive roots and we discussed their basic properties. We indicated that scalar indices can be used to solve various types of congruence equations. We discussed the theory involved as well as provided numerous examples.

In an extended examination of another application, we constructed a modular slide rule based on the properties of indices. We illustrated its use in solving congruence equations. This slide rule illustrates another point of similarity between indices and logarithms: each is the basis for a slide rule.

In Chapter 4 our objective was to extend the theory of indices to arbitrary moduli. We considered first arbitrary odd moduli and defined the appropriate index to be a vector index. We then considered moduli that were powers of 2. Finally, combining the two previous discussions, we could give a definition of the index for any modulo integer n as a vector index.

The tone and style of our investigation changed with Chapter 5. Chapter 5 became something of a cryptic discussion of primitive roots and indices from an algebraic point of view. In section 5.1, we introduced the ring of integers modulo n and directed our attention to the group of invertible elements in \mathbf{Z}_n . We then characterized the integers which possessed primitive roots as those integers for which the group of invertible elements in \mathbf{Z}_n is cyclic. Next we characterized indices in group theoretic language as group isomorphisms. This in turn allowed for the natural extension of indices to any moduli. We concluded the discussion of indices with a generalization of indices to arbitrary finite cyclic groups.

We acknowledge the fact that this thesis could have begun with Chapter 5. We could have defined indices in cyclic groups and moved on to consider the group of invertible elements in \mathbb{Z}_n as a specific example. We present that approach to the study of indices as a challenge for our reader to develop.

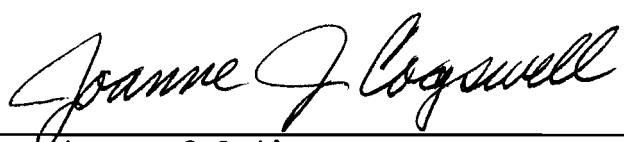
We also suggest for further study the expansion of the theorems and ideas that we dealt with only briefly in Chapter 5 to include, for example, finite abelian groups.

REFERENCES

- [1] Apostol, Tom M. Introduction to Analytic Number Theory. New York: Springer-Verlag, 1976.
- [2] Burton, David M. Elementary Number Theory. 2d ed. Dubuque, Ia: Wm. C. Brown, 1989.
- [3] Cohn, Harvey. Advanced Number Theory. New York: Dover, 1980.
- [4] Dean, Richard A. Classical Abstract Algebra. New York: Harper and Row, 1990.
- [5] Dickson, Leonard E. History of the Theory of Numbers. 3 vols. New York: Chelsea, 1952.
- [6] Gauss, Carl Friedrich. Disquisitiones Arithmeticae. Tran. Arthur A. Clarke, S.J. New Haven: Yale University Press, 1966.
- [7] Gupta, Hansraj. Selected Topics in Number Theory. Kent, England: Abacus, 1980.
- [8] Hunter, John. Number Theory. New York: Interscience, 1964.
- [9] Hurwitz, Adolf. Lectures on Number Theory. Ed. Nikolas Kritikos. Tran. William C. Schulz. New York: Springer-Verlag, 1986.
- [10] Long, Calvin T. Elementary Introduction to Number Theory. 3d ed. Englewood Cliffs, N.J.: Prentice-Hall, 1972.
- [11] Maxfield, John E., and Margaret W. Maxfield. Discovering Number Theory. Philadelphia: W. B. Saunders, 1972.
- [12] McCoy, Neal H. The Theory of Numbers. New York: Macmillian, 1965.
- [13] Nagell, Trygve. Introduction to Number Theory. 2d ed. New York: Chelsea, 1981.
- [14] Niven, Ivan and Herbert S. Zuckerman. An Introduction to the Theory of Numbers. 4th ed. New York: John Wiley and Sons, 1980.

- [15] Ore, Oystein. Number Theory and Its History. New York: McGraw-Hill, 1948.
- [16] Rosen, Kenneth. Elementary Number Theory and Its Applications. 2d ed. Reading, Mass.: Addison-Wesley, 1987.
- [17] Sierpinski, Waclaw. Elementary Theory of Numbers. Tran. A. Hulanicki. New York: Hafner, 1964.
- [18] Stewart, B. M. Theory of Numbers. 2d ed. New York: Macmillian, 1964.
- [19] Uspensky, J. V., and M. A. Heaslet. Elementary Number Theory. New York: McGraw-Hill, 1939.
- [20] Vinogradov, I. M. An Introduction to the Theory of Numbers. Trans. Helen Popova. London: Pergamon, 1955.

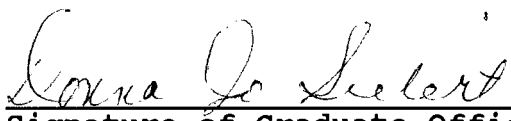
I, Joanne J. Cogswell, hereby submit this thesis/report to Emporia State University as partial fulfillment of the requirements for an advanced degree. I agree that the Library of the University may make it available for use in accordance with its regulations governing materials of this type. I further agree that quoting, photocopying, or other reproduction of this document is allowed for private study, scholarship (including teaching) and research purposes of a nonprofit nature. No copying which involves potential financial gain will be allowed without written permission of the author.



Signature of Author

May 15, 1992
Date

The Theory of Indices Modulo n
Title of Thesis/Research Project



Signature of Graduate Office Staff Member

May 14, 1992
Date Received

Distribution: Director, William Allen White Library
Graduate School Office
Author