NOTICE: When government or other drawings, specifications or other data are used for any purpose other than in connection with a definitely related government procurement operation, the U. S. Government thereby incurs no responsibility, nor any obligation whatsoever; and the fact that the Government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture, use or sell any patented invention that may in any way be related thereto.

INSTITUTE OF TECHNOLOGY

AIR UNIVERSITY

UNITED STATES AIR FORCE

SCHOOL OF ENGINEERING

THESIS

WRIGHT-PATTERSON AIR FORCE BASE, OHIO

AF-WP-B-SEP 60 5M

GE/EE/61-13

A RELAY COMPUTER USING THE PRINCIPLES OF MODULAR ARITHMETIC

THESIS

Presented to the faculty of the School of Engineering of
the Institute of Technology
Air University
in Partial Fulfillment of the
Requirements for the Degree of
Master of Science

By
Gerald Forrest Mackey, B.S.
Capt. USAF
Graduate Electrical Engineering
August 1961

Preface

This report presents a practical realization of the theory of modular arithmetic. One device was constructed and two others were proposed. All take advantage of the speed offered by the absence of carry in modular arithmetic. The computer which was constructed has been retained by the laboratory which sponsored this thesis, the Bionics and Computer Branch, Electronic Technology Laboratory, ASD.

The proof of the Chinese Remainder Theorem, which is in Appendix A, may seem excessively involved to some readers. For that reason an outline of the proof is given at the beginning of Appendix A.

The ideas basic to this report are not mine alone. However, any errors that may appear are a direct result of my efforts.

I wish to acknowledge my indebtedness to Prof. Jerzy Lubelfeld, Capt. F. M. Brown, and Lt. L. R. MCulloh of the Institute of Technology and to Mr. E. C. Maupin and Mrs. L. H. Tackett of the Bionics and Computer Branch. Their guidance and counsel has been invaluable.

Gerald F. Mackey

Contents

	Page
Preface	ii
List of Figures	v
List of Tables	v
Abstract	vi
I. Introduction	1
II. Modular Arithmetic	3
Congruence	3
A Residue Set	5
Uniqueness	6
The Chinese Remainder Theorem	7
Reduction of a Fraction	9
A Modular Computer	10
Difficulties	11
Division	11
Relative Magnitude	13
Negative Numbers	14
Determination of Algebraic Sign	15
Fractions	16
Summary of Difficulties	16
III. The Computer	17
General Operation	17
Decimal to Modular Converter	17
Adder-Multiplier	20
Display Units	21
Wiring Diagram Description	21
IV. A Modular Set to Mixed Radix Converter	26
The Algorithm	26
The Converter	28
V. A Polynomial Evaluator	30
General	30
Description	30

Contents

Page

VI. Conclusions 33

Bibliography 34

Appendix A: 35

List of Figures

Figure			Page
1	Block Diagram of the Computer	facing	17
2	Decimal to Modulo 3 Converter	facing	18
3	Mod 3 Adder-Multiplier	facing	20
4	Wiring Diagram of the Computer		23
5	Computer Exterior		24
6	Computer Interior		25
7	Modular to Mixed Radix Converter . .	facing	26
8	Multiplier (by $\frac{1}{5}$)	facing	27
9	Reducer (to Mod 3 and Mod 4)	facing	28
10	Complementer	facing	30
11	A General Polynomial Evaluator . . .	facing	30
12	Mod 3, 4, 5 Polynomial Evaluator . .	facing	31

List of Tables

Table			Page
I	X Modulo 3, 4, and 5 ($0 \leq X \leq 59$) . .	facing	6
II	X Mod 2 and 4 ($0 \leq X \leq 7$)		7

Abstract

A description of the application of the theory of modular arithmetic to the problems of addition and multiplication in a relay computer is given. Modular arithmetic is explained. Emphasis is given to the advantage of modular arithmetic, its absence of carry, and its disadvantages, division, fractions, and sign determination. The description of a multiplier-adder using decimal input modular output and a plan for a modular-to-mixed radix converter are given. A device for the evaluation of P(X) of a polynomial is proposed. The idea of a residue set as a vector is the basis for the proof of the Chinese Remainder Theorem which is given.

Report on
A RELAY COMPUTER
USING THE PRINCIPLES OF MODULAR ARITHMETIC

I. Introduction

In recent years the Air Force has sponsored considerable research on the theoretical problems of designing a digital computer that would use the principles of modular arithmetic, which is explained in Section II. Modular arithmetic has been considered as a basis for computer logic because of the absence of carry, which allows for a faster computer. The Air Force-sponsored research has produced a body of theory which provides a basis for a digital computer of limited scope. The scope is limited by the fact that operations involving fractions, division, and sign determination are difficult problems. The purpose of this report is to describe the application of the theory to the problems of multiplication and addition in a relay computer. The emphasis of this report is on the ideas of modular arithmetic rather than on hardware techniques.

The history of residue number theory can be traced at least as far back as 100 A.D. to the Chinese mathematician Sun-Tsu (Ref 4:57-64). The ideas basic to modular arithmetic are expressed in C. F. Gauss' Disquisitiones Arithmeticae which was published in 1801. The Czech mathematician M. Valach first suggested a practical use for this branch of number theory in 1957. In this country, theoretical research in modular arithmetic has been pioneered by H. Aiken and W. Semon at Harvard University. Several groups are working now on modular arithmetic theory as it applies to digital computation. Among them are the Harvard

Computation Laboratory, the University of Michigan, Lockheed Missiles and Space Division, and Scope, Inc.

This report is divided into six sections and an appendix. As previously mentioned, Section II is an explanation of modular arithmetic with emphasis on its advantages and disadvantages for digital computation. Section III is a description and explanation of the computer which was constructed. Section IV is a description and explanation of the design for a converter which takes a residue set (a modular representation of a given number) and converts it to a mixed radix number. The idea of a mixed radix number is explained in Section II under Relative Magnitude. Section V is the description and explanation of a polynomial evaluator using the principles of modular arithmetic. Section VI is conclusions.

This report is limited to application of present published theory, although a proof of the Chinese Remainder Theorem based on H. L. Garner's idea of a modular number (a residue set) as a vector (Ref 5:144) is given in Appendix A. The Chinese Remainder Theorem is fundamental to conversion of a residue set to a decimal number. The device which was constructed and which is described in this report is a computer which accepts decimal numbers and provides a sum or product, as desired, in modular form. The diagrams of the previously mentioned modular-to-decimal converter are given in Section IV in order to show the ease of such conversion. The construction of a converter would require more time and effort than were available for this project.

II. Modular Arithmetic

This section, which is offered as an explanation of modular arithmetic, will include the basic principles of modular arithmetic and will point out the features that specifically concern its application to computing circuits. A general familiarity with the important concepts of number theory is presumed. These concepts are well presented by Vinogradov (Ref 7:31-43).

Congruence

The idea of congruence, as proposed by C. F. Gauss (Ref 6:211) is fundamental to this work. The idea of congruence can be expressed as

$$q \equiv b \pmod{m} \tag{1}$$

or q is congruent b modulo m. This means that

$$q = b + mt \tag{2}$$

where t is some integer.

Example:

$$14 \equiv 2 \pmod{3}$$

can be expressed as

$$14 = 2 + 3x4$$

where

$$t = 4$$

For this work always take $0 \leq b < m$. When b is

restricted in this way it is called the least positive residue of q modulo m. In the above example 2 is the least positive residue of 14 modulo 3.

Another notation for

$$q = b + mt$$

where

$$0 \leq b < m \tag{2}$$

is

$$|q|_m = b \text{ (Ref 1:1-1)} \tag{3}$$

This notation states that the least positive residue of q modulo m equals b. The notation was first seen in reports from the Harvard Computation Laboratory and is credited to H. Aiken and W. Semon.

Example:

$$|14|_3 = 2$$

or

$$|12|_4 = 0$$

Now notice that

$$q = m\left[\frac{q}{m}\right] + |q|_m \tag{4}$$

where $\left[\frac{q}{m}\right]$ is defined as the greatest integer in $\frac{q}{m}$.

Example:

$$14 = 3\left[\frac{14}{3}\right] + |14|_3$$

or

$$14 = 3x4 + 2 = 12 + 2 = 14$$

The following is a list of important properties of reduction to a least positive residue (Ref 1:1-2). These properties are needed to develop the equations that follow.

$$|m|_m = 0 \tag{5}$$

$$\left||X|_m\right|_m = |X|_m \tag{6}$$

$$|X \pm mY|_m = |X|_m \tag{7}$$

$$|-X|_m = |(m-1)X|_m \tag{8}$$

$$|X \pm Y|_m = \left||X|_m \pm Y\right|_m = \left|X \pm |Y|_m\right|_m = \left||X|_m \pm |Y|_m\right|_m \tag{9}$$

A Residue Set

From equations (2) and (3) it follows that any integer can be expressed as a least positive residue for a given modulus. It is also evident that any integer can be expressed as a least positive residue to more than one modulus. For example,

$$|14|_3 = 2, \ |14|_4 = 2, \text{ and } |14|_5 = 4$$

Another way to express this property is as follows: For the moduli 3, 4, and 5, 14 reduces to 2, 2, and 4, or one may express 14 by (2, 2, 4).

Thus, it may be said that, for a given set of moduli, m_1, m_2, and m_3, any integer maps to a residue set, (r_1, r_2, r_3). Or

Table I

X Modulo 3, 4, and 5 ($0 \leq X \leq 59$)

X	$\|X\|_3$	$\|X\|_4$	$\|X\|_5$	X	$\|X\|_3$	$\|X\|_4$	$\|X\|_5$	X	$\|X\|_3$	$\|X\|_4$	$\|X\|_5$
0	0	0	0	20	2	0	0	40	1	0	0
1	1	1	1	21	0	1	1	41	2	1	1
2	2	2	2	22	1	2	2	42	0	2	2
3	0	3	3	23	2	3	3	43	1	3	3
4	1	0	4	24	0	0	4	44	2	0	4
5	2	1	0	25	1	1	0	45	0	1	0
6	0	2	1	26	2	2	1	46	1	2	1
7	1	3	2	27	0	3	2	47	2	3	2
8	2	0	3	28	1	0	3	48	0	0	3
9	0	1	4	29	2	1	4	49	1	1	4
10	1	2	0	30	0	2	0	50	2	2	0
11	2	3	1	31	1	3	1	51	0	3	1
12	0	0	2	32	2	0	2	52	1	0	2
13	1	1	3	33	0	1	3	53	2	1	3
14	2	2	4	34	1	2	4	54	0	2	4
15	0	3	0	35	2	3	0	55	1	3	0
16	1	0	1	36	0	0	1	56	2	0	1
17	2	1	2	37	1	1	2	57	0	1	2
18	0	2	3	38	2	2	3	58	1	2	3
19	1	3	4	39	0	3	4	59	2	3	4

$$X \rightarrow (r_1, r_2, r_3)$$

where

$$|X|_{m_1} = r_1, \quad |X|_{m_2} = r_2, \text{ and } |X|_{m_3} = r_3 \qquad (10)$$

In the previous example of 14, for moduli 3, 4, and 5, called a 3, 4, 5 modular number system, or briefly a 3, 4, 5 system, equation (10) takes the form

$$14 \rightarrow (2, 2, 4)$$

Uniqueness

It has been shown that any integer can be expressed as a residue set. From equations (2), (3), and (10), it is seen that to every integer X, for a given set of moduli, $(m_1, m_2, \cdots, m_n)$, there exists one and only one residue set, $(r_1, r_2, \cdots, r_n)$. Conversely, for every residue set $(r_1, r_2, \cdots, r_n)$, for a given set of moduli, $(m_1, m_2, \cdots, m_n)$, all moduli relatively prime, there exists one and only one integer $0 \leq X < M$, where M is the product of the moduli. This property of the uniqueness of an integer represented by a residue set is proven in Appendix A.

Table 1 is given as an example of the residue sets for a 3, 4, 5 system. Of course, for X outside the range $0 \leq X \leq 59$ the uniqueness property no longer holds. For example, the residue set for X = 60 is

$$X \rightarrow (0, 0, 0)$$

which is the same residue set as for X = 0.

The requirement that the moduli be relatively prime

is essential to the uniqueness property. Table II gives an example of the residues associated with two moduli, 2 and 4, which are not relatively prime. It is seen from Table II that if $\frac{m_2}{m_1} = 2$ the range of unique integers for a given residue set is not $0 \leq X < M$, but instead is reduced by half.

To summarize, X maps, in a one-to-one relationship, to a unique residue set when $0 \leq X \leq M - 1$ if the moduli of the residue set are relatively prime. Also, a given residue set maps, in a one-to-one relationship, to a unique X where $0 \leq X \leq M - 1$. For $X > M - 1$, X maps to a unique residue set but a given residue set maps to an infinite number of X's.

Table II

X Mod 2 and 4

$0 \leq X \leq 7$

X	$\|X\|_2$	$\|X\|_4$
0	0	0
1	1	1
2	0	2
3	1	3
4	0	0
5	1	1
6	0	2
7	1	3

The Chinese Remainder Theorem

A formal statement of the uniqueness of the integer represented by a residue set and a method of determination of that integer, X, is given in the Chinese Remainder Theorem (Ref 3:16, 1:1-7). A proof of this theorem based on H. L. Garner's idea of a residue set as a vector is given in Appendix A.

The theorem states

$$|X|_M = \left| \sum_{i=1}^{n} \hat{m}_i \left| \frac{|X|_{m_i}}{\hat{m}_i} \right|_{m_i} \right|_M$$

which by equation (6) is

$$= \left| \sum_{i=1}^{n} \hat{m}_i \left| \frac{X}{\hat{m}_i} \right|_{m_i} \right|_M \tag{11}$$

where

$$\hat{m}_i = \frac{M}{m_i} \tag{12}$$

In other words, for a given residue set the residues $|X|_{m_i}$ and the moduli, $(m_1, m_2, \cdots, m_n)$, determine a unique integer $0 \leq X < M$.

For example, let the moduli be

$$(3, 4, 5)$$

and the given residue set be

$$(2, 2, 4)$$

(of course, M = 60). The unique integer determined by the given residue set and the given moduli is

$$|X|_M = \left| 20 \left| \frac{2}{20} \right|_3 + 15 \left| \frac{2}{15} \right|_4 + 12 \left| \frac{4}{12} \right|_5 \right|_{60}$$

or

$$|X|_M = \left| 20 |2x2|_3 + 15 |1x2|_4 + 12 |3x4|_5 \right|_{60}$$

therefore

$$|X|_M = |20 + 30 + 24|_{60} = |74|_{60} = 14$$

Reduction of a Fraction

As a parenthetical remark, the following method is probably the quickest way to handle the reduction of a fractional number when the modulus is prime and X is not divisible by m. Consider

$$\left|\frac{1}{X}\right|_m$$

Now recall Fermat's Theorem (Ref 7:37)

$$X^{p-1} \equiv 1 \pmod{p} \tag{13}$$

or in Aiken's notation

$$\left|X^{p-1}\right|_p = 1 \tag{14}$$

therefore

$$\left|\frac{1}{X}\cdot 1\right|_m = \left|\left|\frac{1}{X}\right|_m \left|X^{m-1}\right|_m\right|_m = \left|\frac{1}{X}\cdot X\cdot X^{m-2}\right|_m$$

which is

$$= \left|X^{m-2}\right|_m \tag{15}$$

Example:

$$\left|\frac{1}{3}\right|_5 = \left|\frac{1}{3}\, 3\cdot 3^3\right|_5 = \left|\left|3\cdot 3\right|_5 \cdot 3\right|_5$$

which is

$$= \left|4\cdot 3\right|_5 = 2$$

A general method for any problem is given by Vinogradov (Ref 6:61).

A Modular Computer

A coding system for integers where each integer is expressed as a residue set is a modular number system. It was first noted by Valach (Ref 1:1-7) that a modular number system would have the definite advantage, for computational purposes, of no carry in the algorithms for addition and multiplication. Hence, electric circuits used to implement these operations would be economical with time and equipment.

The algorithm for addition is (Ref 1:1-7): Given the set of moduli

$$(m_1, m_2, \cdots, m_n)$$

$$X \rightarrow (|X|_{m_1}, |X|_{m_2}, \cdots, |X|_{m_n})$$

and

$$Y \rightarrow (|Y|_{m_1}, |Y|_{m_2}, \cdots, |Y|_{m_n})$$

to find X + Y

$$(X + Y) \rightarrow \left\{ \left| |X|_{m_1} + |Y|_{m_1} \right|_{m_1}, \cdots, \left| |X|_{m_n} + |Y|_{m_n} \right|_{m_n} \right\} \quad (16)$$

For example, for a 3, 4, 5 system, given

$$X = 19 \rightarrow (1, 3, 4)$$

$$Y = 14 \rightarrow (2, 2, 4)$$

$$(X + Y) \rightarrow (|1 + 2|_3, |3 + 2|_4, |4 + 4|_5) =$$

$$33 \rightarrow (0, 1, 3)$$

The algorithm for multiplication is (Ref 1:1-7): Given the set of moduli, X, and Y as in the addition algorithm, to find XY

$$XY \rightarrow \left\{ \left| |X|_{m_1} |Y|_{m_1} \right|_{m_1}, \left| |X|_{m_2} |Y|_{m_2} \right|_{m_2}, \ldots, \left| |X|_{m_n} |Y|_{m_n} \right|_{m_n} \right\} \tag{17}$$

For example, for a 3, 4, 5 system, given

$$X = 19 \rightarrow (1, 3, 4)$$

$$Y = 3 \rightarrow (0, 3, 3)$$

$$XY \rightarrow (|0|_3, |9|_4, |12|_5) =$$

$$57 \rightarrow (0, 1, 2)$$

The residues in the examples of equations (17) and (18) can be checked in Table I.

Difficulties

No discussion of this subject would be complete without consideration of some of the difficulties that are encountered in computation by modular arithmetic. The most serious difficulty is encountered in division. Other difficulties are found in determination of relative magnitude, representation of negative numbers, determination of the algebraic sign of a number, and expression of fractions.

Division. The algorithm for division is: Given the set of moduli, X, and Y as in the addition algorithm, to find $\frac{X}{Y}$

$$\frac{X}{Y} \rightarrow \left\{ \left| \frac{|X|_{m_1}}{|Y|_{m_1}} \right|_{m_1}, \ldots, \left| \frac{|X|_{m_n}}{|Y|_{m_n}} \right|_{m_n} \right\} \tag{18}$$

In a system where only integers are defined, which is the system used in this report, division cannot be performed unless Y divides X. Example:

$$X = 14 \rightarrow (2, 2, 4) \qquad Y = 7 \rightarrow (1, 3, 2)$$

then

$$\frac{X}{Y} = \frac{14}{7} \rightarrow \left(\left| \frac{2}{1} \right|_3, \left| \frac{2}{3} \right|_4, \left| \frac{4}{2} \right|_5 \right)$$

which is

$$(2, 2, 2) \leftarrow 2$$

Example:

$$X = 14 \rightarrow (2, 2, 4) \qquad Y = 11 \rightarrow (2, 3, 1)$$

$$\frac{X}{Y} = \frac{14}{11} \rightarrow \left(\left| \frac{2}{3} \right|_3, \left| \frac{2}{3} \right|_4, \left| \frac{4}{1} \right|_5 \right)$$

which yields

$$(1, 2, 4) \leftarrow 34$$

which is incorrect.

When the divisor has a zero residue the indeterminate case of dividing by zero is introduced. Example:

$$X = 14 \rightarrow (2, 2, 4) \qquad Y = 6 \rightarrow (0, 2, 1)$$

$$\frac{X}{Y} = \frac{14}{6} \rightarrow \left(\left| \frac{2}{0} \right|_3, \left| \frac{2}{2} \right|_4, \left| \frac{4}{1} \right|_5 \right)$$

and the above mentioned situation of $\left|\frac{2}{0}\right|_3$ is indeterminate.

An algorithm which overcomes these difficulties has been devised (Ref 1:9-2): However, it complicates addition and multiplication so it will not be discussed here.

Relative Magnitude. Each element in a residue set is of equal significance. The equal significance of all elements is contrasted to a decimal number where the left hand digit is the most significant. It seems that the only practical way to determine the relative magnitude of modular numbers is to convert the residue sets to ordered numbers, such as fixed radix numbers or mixed radix numbers, and compare the ordered numbers. Examples of fixed radix numbers are decimal numbers (radix 10) and binary numbers (radix 2).

An ordered, mixed radix number, X, is

$$X = a_o + \sum_{i=1}^{n} a_i \left(\prod_{j=1}^{i} r_j\right)$$

where

$$r_i = (r_1, r_2, \cdots, r_{n+1})$$

is the set of radices of the number, and

$$\begin{aligned} a_o &< r_1 \\ a_1 &< r_2 \\ &\vdots \\ a_n &< r_{n+1} \end{aligned} \tag{19}$$

The number is customarily represented by a_i's given

in reverse order; i.e.,

$$X = a_n, a_{n-1}, \ldots, a_1, a_0 \qquad (20)$$

For example, consider a given decimal number 129 which is to be converted to a mixed radix number where

$$r_i = 3, 5, 7$$

Then from equation (20)

$$X = a_2(15) + a_1(3) + a_0$$

from which

$$a_0 = 0, \; a_1 = 3, \text{ and } a_2 = 8$$

That is,

$$X = 8, 3, 0$$

As another example, consider a mixed radix number 1, 1, 1 where

$$r_i = 5, 3, 4$$

Then from equation (20)

$$X = 1x(15) + 1x(5) + 1 = 21$$

in decimal form.

Negative Numbers. A set of relatively prime moduli specify a range, $0 \leq X < M$, of unique integer representation. When $X \geq M$ more than one value of X can map to one residue set. This fact was shown previously in the section on Uniqueness. It is convenient to think of a modular

number system as a circle of integers. There are M integers in the circle. These integers can take on any value one wishes to assign them. If negative numbers are to be considered, part of the circle of integers of the system can be designated as negative numbers, then the remainder of the circle is designated as positive integers.

For example, consider a mod 3, 4, 5 system. It is seen that this system is a circle of 60 integers. In Table I they are designated

$$0 \leq X \leq 59$$

Recall that the residue set for 60 is the same as the residue set for 0. It is also evident that 50 can also be expressed as -10. This is analogous to the fact that 50 minutes past the hour is the same as 10 minutes before the next hour. As an example of a consideration of negative numbers, the range of X could be

$$-20 \leq X \leq 39$$

Negative numbers are considered in this way in modular number systems.

Determination of Algebraic Sign. From the above sections on A Modular Computer and Negative Numbers it is evident that modular addition and multiplication operations can be correctly completed without regard to sign. If negative numbers are to be considered then the system designer only needs to specify the range of negative and positive numbers. All addition and multiplication then is completed properly without further consideration of sign.

The determination of the sign of some completed operation is a difficult operation. Theoretical research

indicates that sign determination can be completed only by converting a modular set to an ordered number. This restriction would make it difficult to detect the sign change in the subtraction iteration of a division.

The difficulty of a quick sign determination is the major obstacle to the application of modular arithmetic to general purpose digital computation.

Fractions. The idea of a decimal point, or more generally of a radix point, is directly connected to positional notation. At the present time there is no satisfactory method for representation of fractions.

Summary of Difficulties. The problems of modular arithmetic, as used in computation, result from two facts. The first fact is that division may produce a result out of the integer class. The second fact is that a residue set is a representation (a vector representation as seen in Appendix A) of a scalar integer and the sign and magnitude of the integer represented is not quickly determinable. These difficulties do not restrict the capability of counting, addition, and multiplication in modular number systems.

If a method of quick sign determination is developed, division can be accomplished by the method of iterative subtraction which is now used in digital computers.

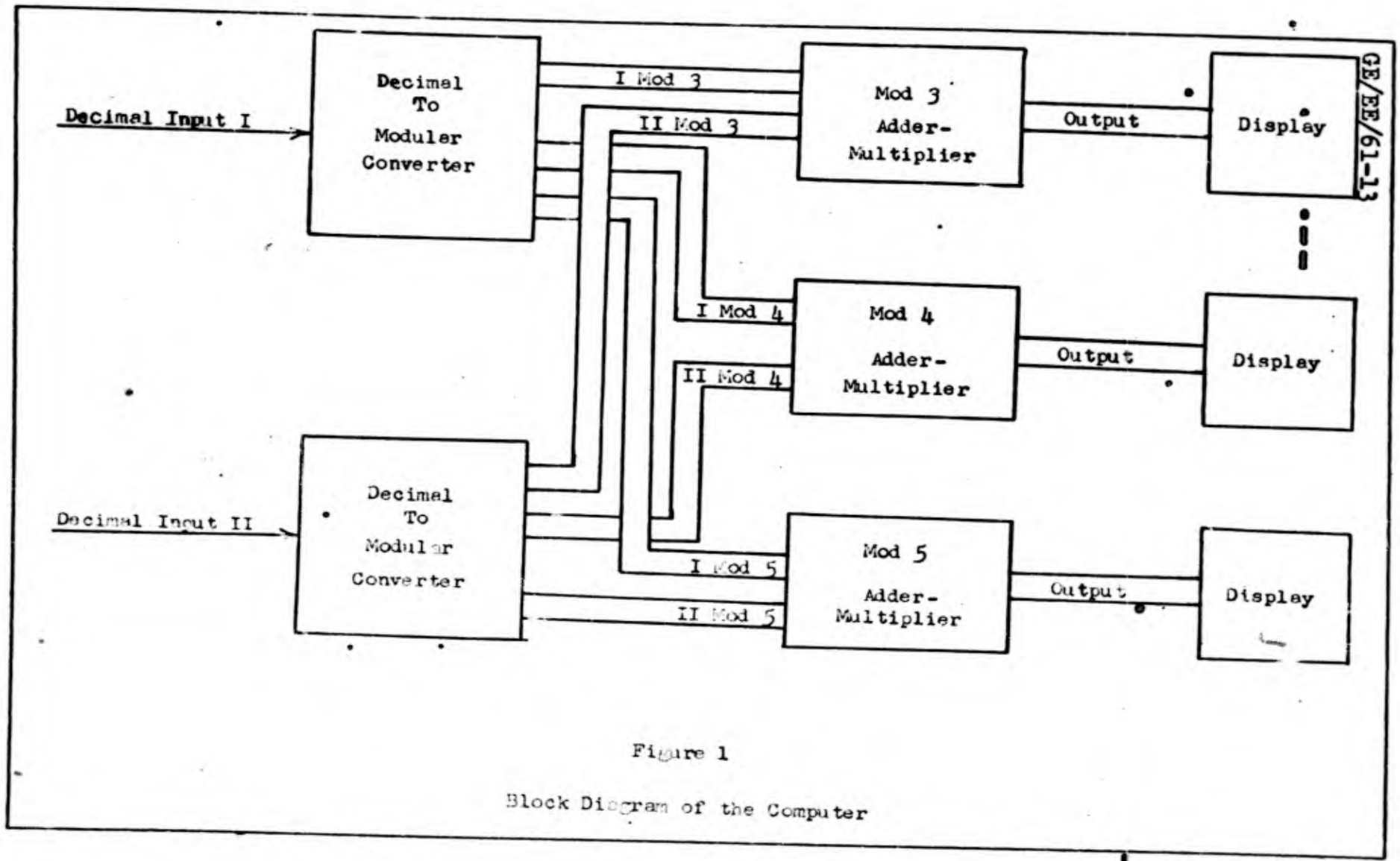


Figure 1

Block Diagram of the Computer

III. The Computer

General Operation

In the previous section it was shown that it is theoretically possible to count, add, and multiply without considering the operation of carry. The circuits for modular addition and multiplication for a relay computer are presented and described in this section. For simplicity of design and construction, the computer uses 110 volts A.C.

Figure 1 is a block diagram of the computer. On the left side of the figure are the decimal inputs I and II. These inputs can each range in value from 0 to 59. In the decimal to modular converter each input is converted to the proper residue modulo 3, modulo 4, and modulo 5. The two decimal to modular converters are identical. In this computer there is a separate wire for each number capable of representation by each modulus. Therefore, the double lines labelled I mod 3, II mod 3, I mod 4, etc., may be considered as channels which carry the designated information. The mod 3 channel is three wires, the mod 4 channel is four wires, and the mod 5 channel is five wires. In the center of Figure I are the three adder-multiplier units. The mod 3 adder-multiplier unit adds or multiplies, as desired, modulo 3. The mod 4 and mod 5 units perform the same operations modulo 4 and modulo 5 respectively. The output of each adder-multiplier unit is sent to a display where a light indicates the sum or product, as appropriate.

Decimal to Modular Converter

The decimal to least positive residue conversion is performed by a factor method. Consider a decimal number AB

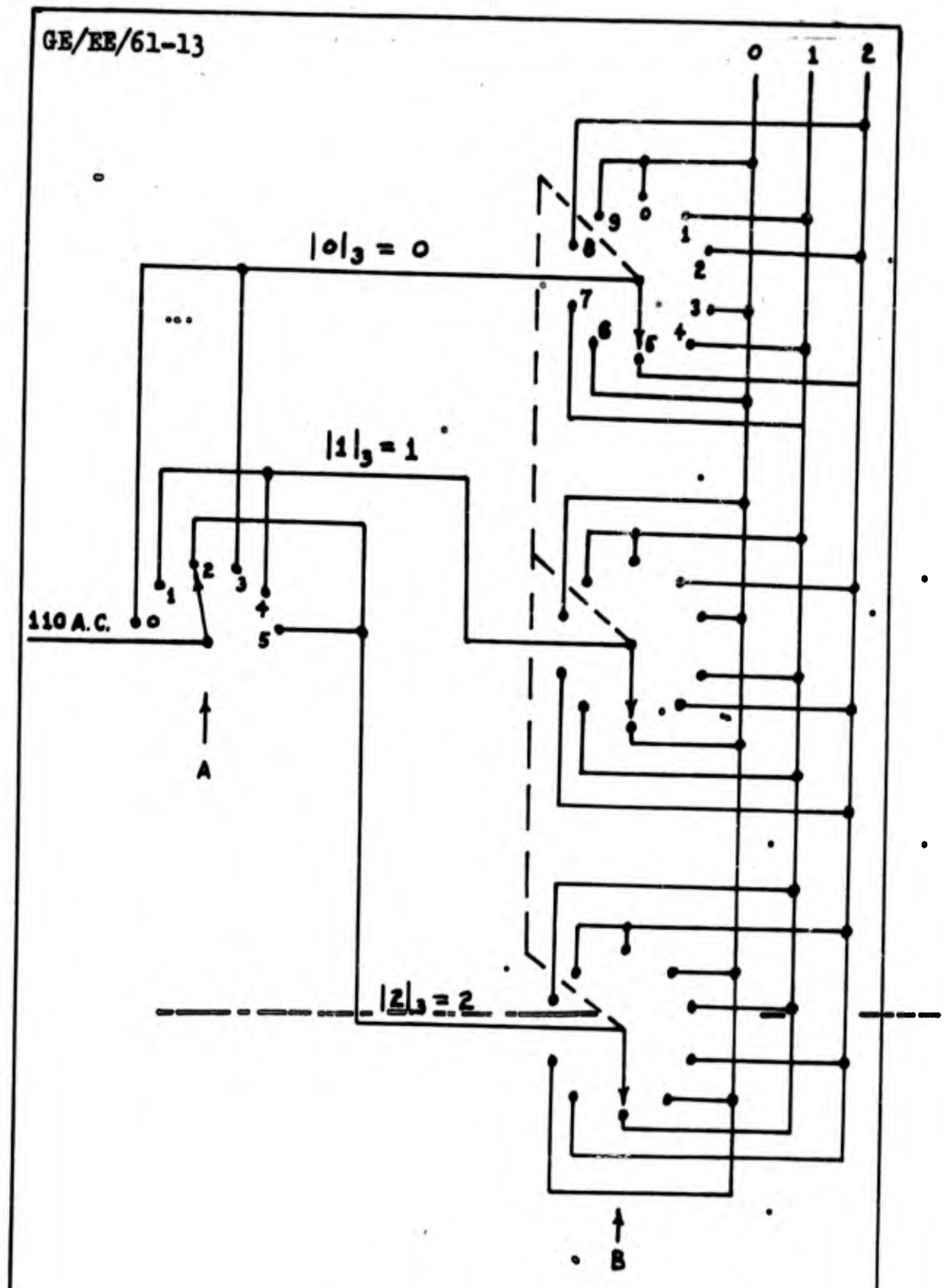


Figure 2

Decimal to Modulo 3 Converter

where A is the tens digit and B is the units digit. Then

$$|AB|_3 = |Ax10 + B|_3$$

which is also

$$= \left| |Ax10|_3 + |B|_3 \right|_3 = \left| \left| |A|_3 x |10|_3 \right|_3 + |B|_3 \right|_3$$

or

$$= \left| \left| |A|_3 x1 \right|_3 + |B|_3 \right|_3$$

which reduces to

$$|AB|_3 = \left| |A|_3 + |B|_3 \right|_3 \qquad (21)$$

Example:

$$|25|_3 = \left| |2|_3 + |5|_3 \right|_3 = |2 + 2|_3$$

which is

$$|4|_3 = 1$$

A similar conversion can be carried out for modulo 4 or modulo 5. For instance, for modulo 4

$$|AB|_4 = |Ax10 + B|_4 = \left| \left| |A|_4 x |10|_4 \right|_4 + |B|_4 \right|_4$$

which is

$$= \left| \left| |A|_4 x2 \right|_4 + |B|_4 \right|_4 \qquad (22)$$

In addition, it is seen that when $0 \leq A \leq 5$,

$$\left| |A|_4 x2 \right|_4 = 0 \text{ or } 2$$

This means that for any integer $AB \leq 59$, either a 0 or a 2 will be added to $|B|_4$ in the determination of $|AB|_4$. If A is an odd number $|Ax10|_4 = 2$, and if A is an even number $|Ax10|_4 = 0$.

The modulo 3 section of the decimal-to-modular converter is shown in Figure 2. The complete converter is shown in the computer wiring diagram, Figure 4.

The operation of the converter is as follows. The tens digit is entered on switch A and is reduced to the appropriate residue modulo 3. The tens digit is reduced by directing the voltage to the appropriate output line. The presence of the voltage on the upper line out of switch A represents 0. The presence of the voltage on the middle line represents 1 and the presence of the voltage on the bottom line represents 2.

This appropriate residue modulo 3 is added to the units digit, the input of switch B, as required by equation (20). This residue is added to input B by connecting each pole of switch B to the correct output line. The three output lines represent the three possible residues of X modulo 3. Example:

Consider the number 25 which is to be reduced to the least positive residue modulo 3.

In Figure 2 the input A is 2 and input B is 5. Since

$$|A|_3 = |2|_3 = 2$$

the input voltage, 110 A.C., is connected to the pole 2, by switch A, and is directed through the 2 output line to switch B. From equation (20) it is noted that 2 is to be

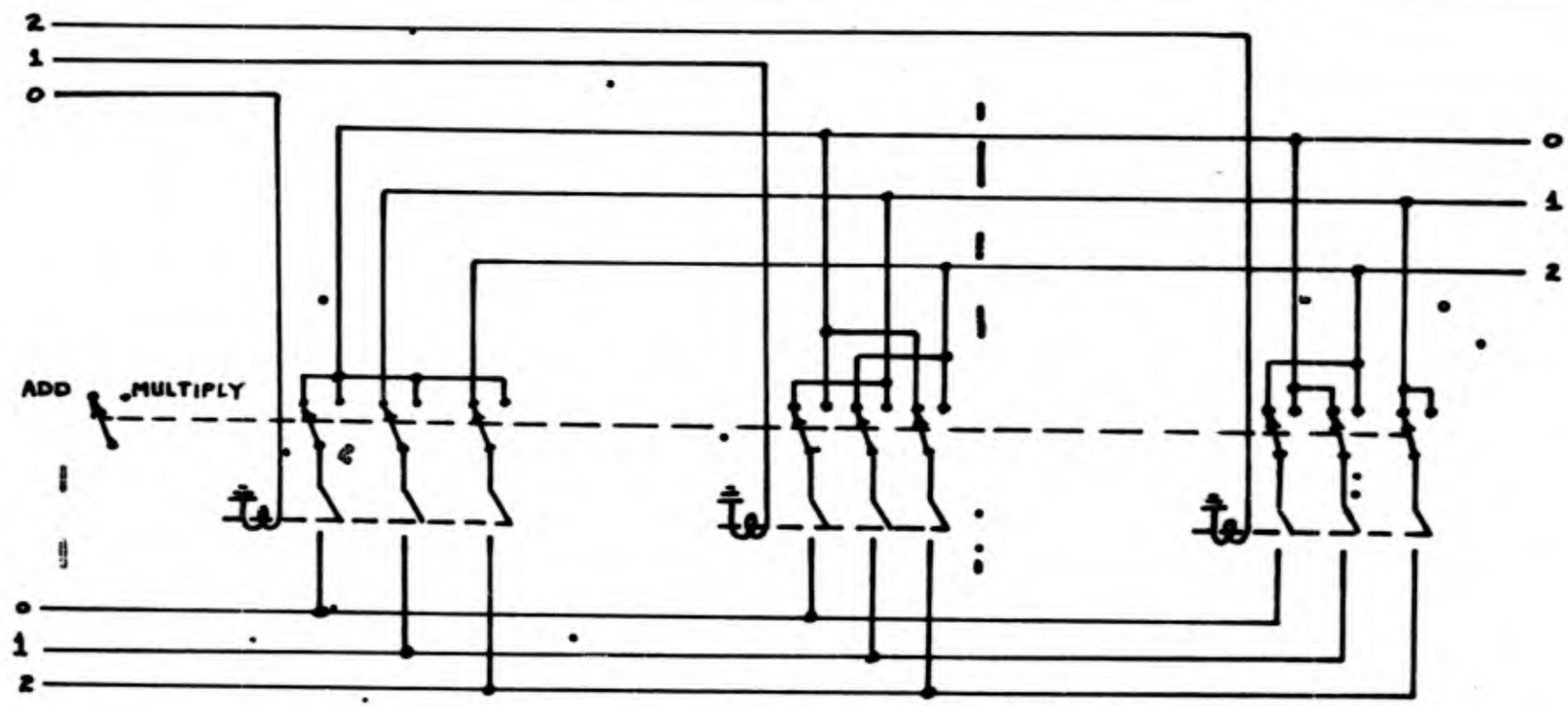


Figure 3

Mod 3 Adder-Multiplier

added to B and the sum reduced modulo 3. Note that

$$|B|_3 = |5|_3 = 2$$

and equation (20) takes the form

$$|2 + 2|_3 = |4|_3 = 1$$

Therefore, the pole 5 is connected to the output line which represents 1.

Adder-Multiplier

It is seen in Figure 1 that the output of each decimal-to-modular converter goes to the adder-multiplier units. The modulo 3 adder-multiplier unit is shown in Figure 3 as an example of the operation of the system.

The modular representation of decimal input I is applied to the relay coils and the modular representation of decimal input II is applied to one set of contacts of the relays.

Input I, when applied to the appropriate relay coil, will cause the contacts of that relay to close. Input II will be applied to the add-multiply switches connected to the relay that closed. Current can only pass through these add-multiply switches in the manner appropriate to the wired-in addition and multiplication tables. Example:

Let input I = 0 and input II = 2. The coil for the relay which represents 0 will be the only coil activated. Therefore, the contacts of the zero coil are closed and the other coil contacts are open. Only the lower input line 2 is activated. In this case, the add-multiply switch is on the add contact. The voltage on the lower input 2 line is directed to the add 2 pole of the zero relay. The voltage

is then directed to the output 2 line. This output is the output of the adder-multiplier unit. Therefore, it is seen that this modulo 3 adder-multiplier correctly adds 0 + 2 = 2.

If the inputs are the same as those given above and the command is to multiply, then the steps are similar but with a different result. In this case the 0 relay is again activated and on the input II side only the 2 line is activated. However, in this case the add-multiply switch is in the multiply position. So the 0 output, of the 0 relay, is activated. That is, the modulo 3 unit correctly shows 2x0 = 0.

Display Units

The display units are arrays of lights. There are three lights for the modulo 3 display, four lights for the modulo 4 display, and 5 lights for the modulo 5 display. When the output 2 of the adder-multiplier unit is activated the light representing 2 is illuminated. When the output 0 is activated the light representing 0 is illuminated. The number of the light illuminated in each modular set corresponds to the sum or product modulo that modulus.

Wiring Diagram Description

Figure IV is the wiring diagram of the computer which was constructed. At the upper left is the decimal input I. The two components are labelled A_I and B_I. Similarly, at the lower left is the decimal input II. Its two components are labelled A_{II} and B_{II}.

The ganged rows of rotary switches at the top and bottom of the figure constitute the decimal to modular converters. The eight rotary switches at the top of the

figure are the switches for input I and the switches at the bottom of the figure are for input II. The two position add-multiply switches and the relays in the center of the figure are the adder-multiplier units.

The display units are the sets of lights, each located adjacent to its respective adder-multiplier unit.

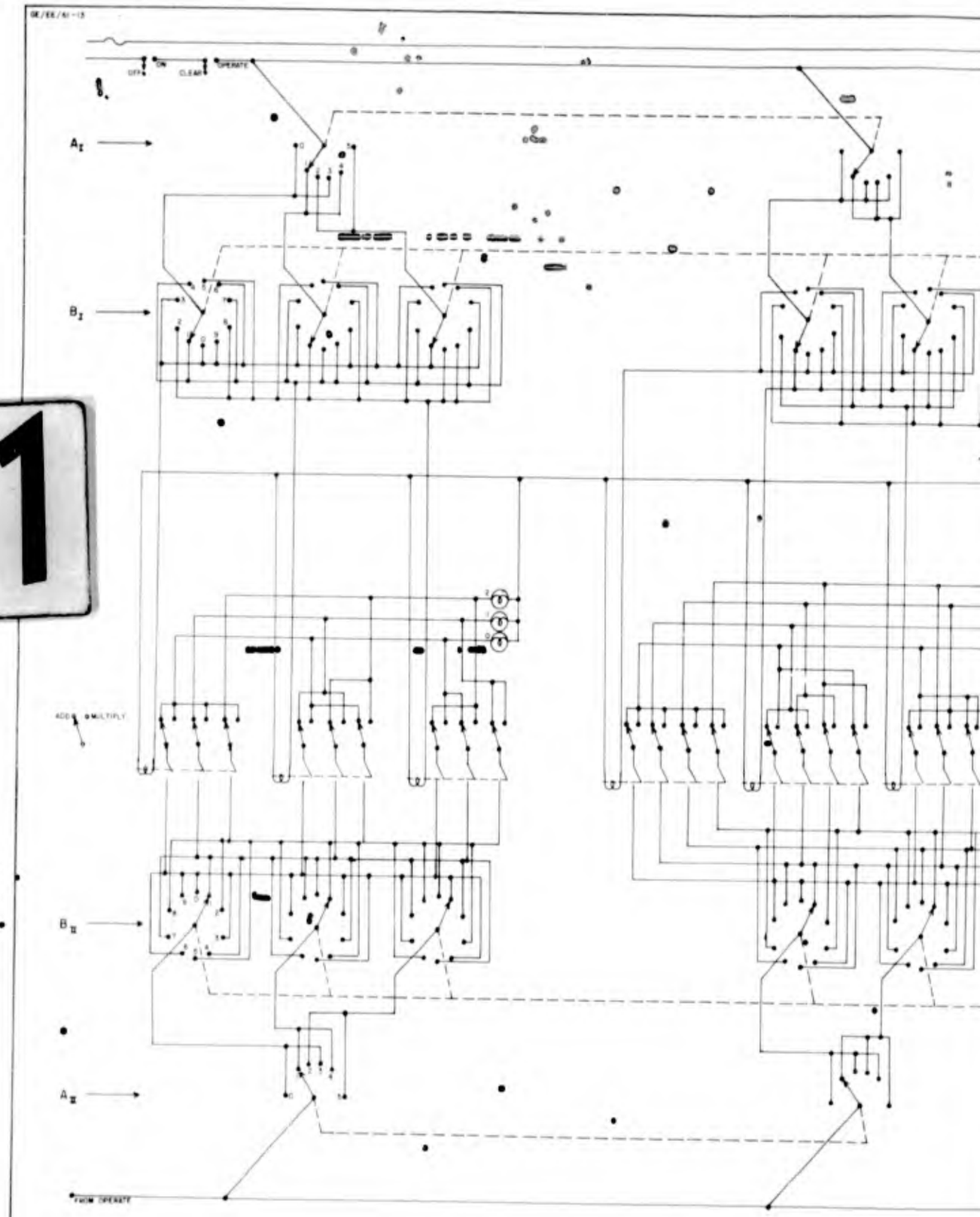


FIG
WIRING DIAGRAM

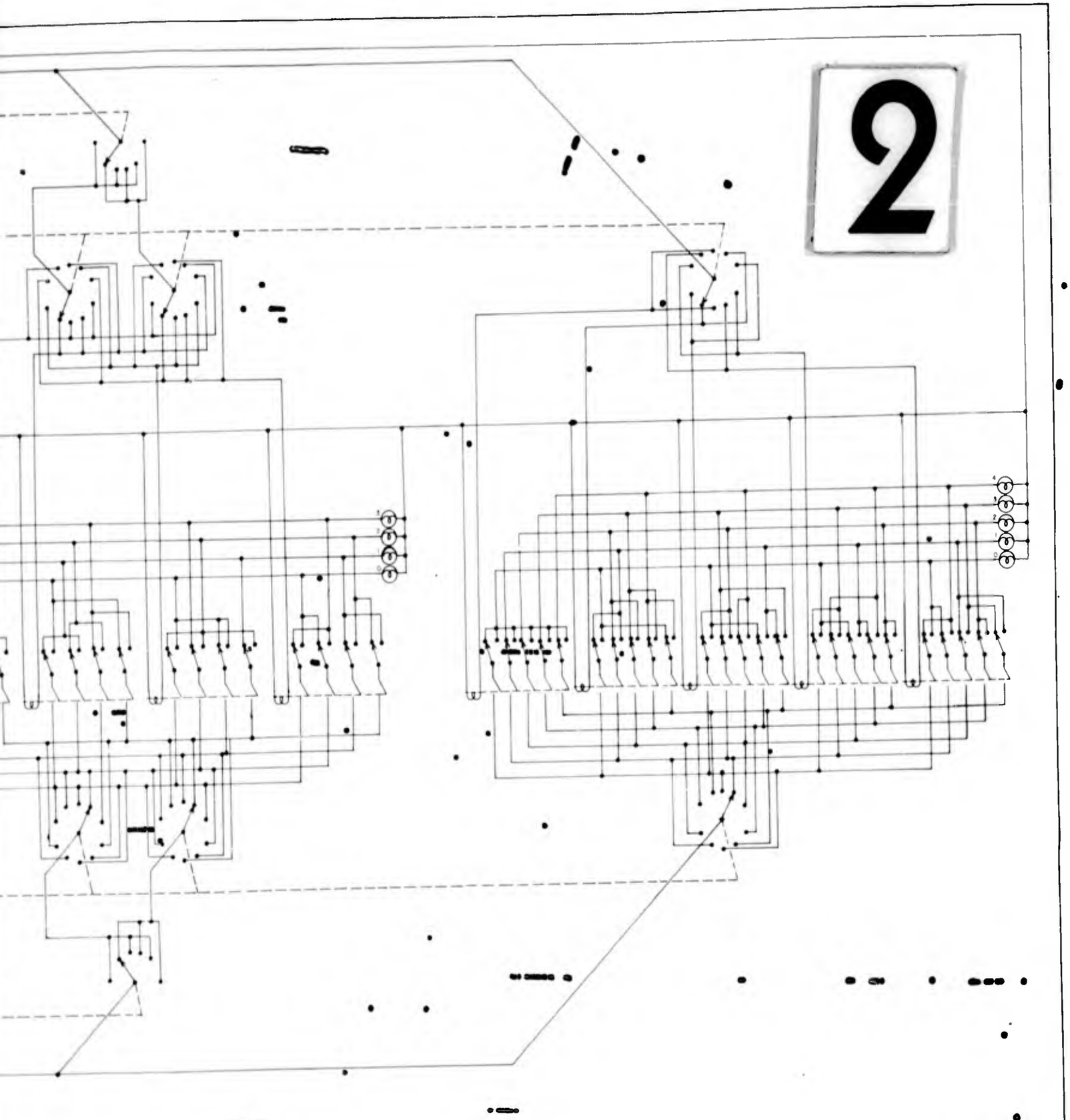


FIGURE 4
WIRING DIAGRAM OF THE COMPUTER

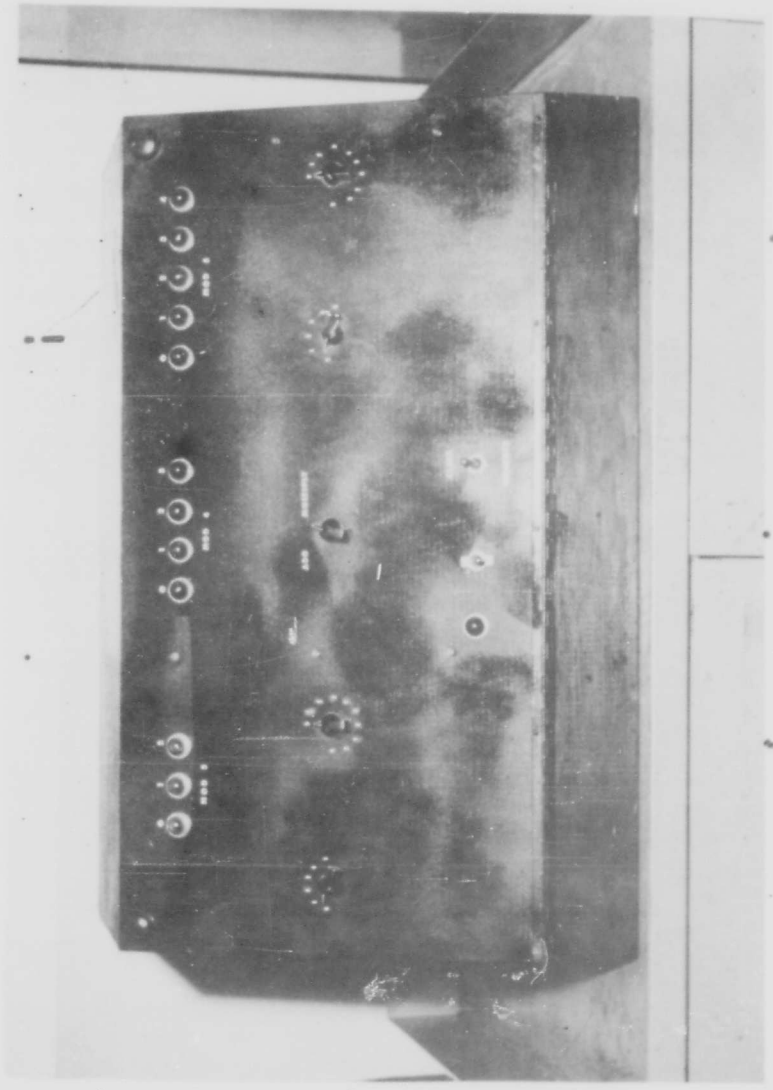


Figure 5
Computer Exterior

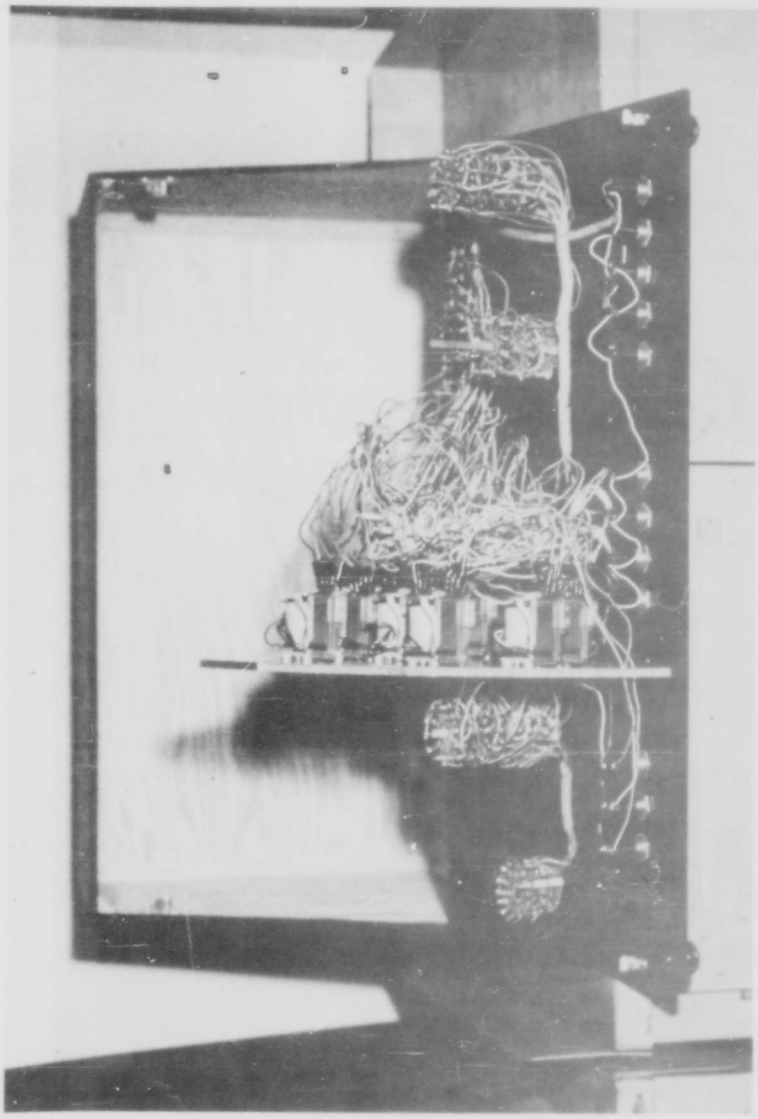


Figure 6
Computer Interior

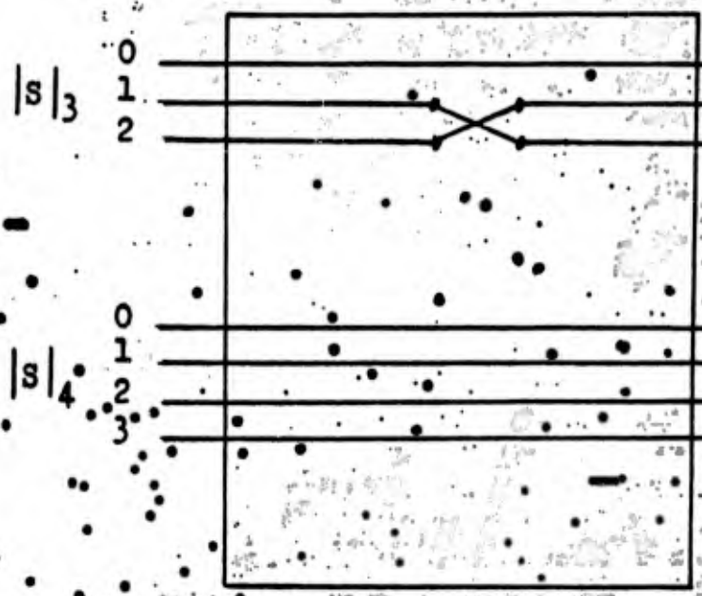
IV. A Modular Set to Mixed Radix Converter

The Algorithm

This section is presented to show that the modular form of a product or sum easily can be converted to an ordered number by electrical means. The theoretical development of the algorithm used was by D. Henderson (Ref 2: VI-5). In this example of Henderson's method the moduli 3, 4, and 5 are used. Only a general block diagram and wiring diagrams of sample components are shown. The complete wiring diagram is not needed to explain the general operation of the modular-to-mixed radix converter.

A numerical example of the conversion of a given modular set to a mixed radix number is given to show the method used to find the mixed radix number.

The given moduli are	3, 4, 5
The given residue set is	0, 3, (2)
In the first step a minus two is added to the given set. To accomplish this the complement of minus 2 is added to the given set.	1, 2, 3
Then the sum of the given set and the complement of minus 2, modulo 3, 4, and 5, is found	1, 1, 0
In the second step this sum is divided by 5, i.e., the sum is multiplied by $\frac{1}{5}$ modulo 3, 4	



Note:

$$\left|\frac{1}{5}\right|_3 = \left|\frac{1+3\cdot 8}{5}\right|_3 = \left|\frac{1+24}{5}\right|_3 = \left|\frac{25}{5}\right|_3 = |5|_3 = 2$$

and

$$\left|\frac{1}{5}\right|_4 = \left|\frac{1+4}{5}\right|_4 = |1|_4 = 1$$

Figure 8

Multiplier (By $\frac{1}{5}$)

and 5 respectively. Note that $\left|\frac{1}{5}\right|_5 = 0$ and $\frac{0}{0}$ is indeterminate. $\frac{0}{0}$ is indicated by an X.

$$\left|\frac{1}{5}\right|_3 = \left|\frac{(1 + 3x3)}{5}\right|_3 = 2$$

and

$$\left|\frac{1}{5}\right|_4 = \left|\frac{(1 + 4x1)}{5}\right|_4 = 1$$

$$\frac{2,\ 1,\ X}{2,\ (1)}$$

The third step is analogous to the first step. The complement of -1 is added to the existing set.

$$\frac{2,\ 3}{1,\ 0}$$

In the fourth step the sum is multiplied by $\left|\frac{1}{4}\right|_3 = 1$

$$(1),\ X$$

In the last step it is noted that the circled numbers are the coefficients of the mixed radix number. The mixed radix number is 112. Its decimal equivalent is

$$1x(4x5) + 1x(5) + 2x(1) = 1x20 + 1x5 + 2x1$$

which is

$$= 27$$

in decimal form

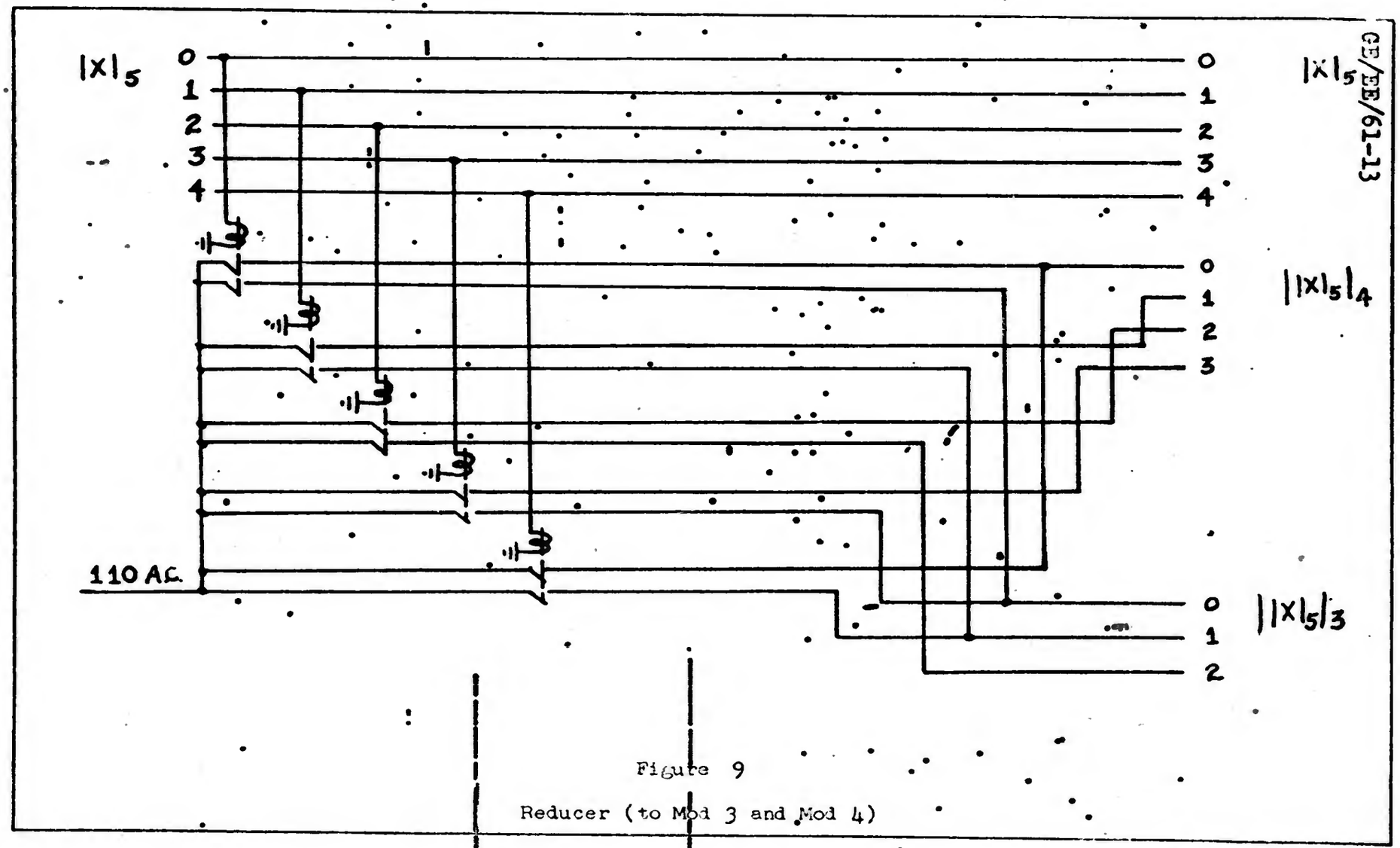


Figure 9

Reducer (to Mod 3 and Mod 4)

The Converter

Figure 7 is the block diagram of the modular-set-to-mixed radix converter. The modular set input is introduced to the converter at the upper left on the lines labelled $|X|_3$, $|X|_4$, and $|X|_5$, where X represents the number in decimal form. For the same reasons as those given in Section III, General Operation, the lines connecting blocks may be considered channels for the information. The $|X|_3$ line represents 3 wires, the $|X|_4$ line represents 4 wires, and the $|X|_5$ line represents 5 wires.

The first step of the previously given numerical example is accomplished in the following manner. The input $|X|_5$ is reduced to $\left||X|_5\right|_3 = |X|_3$ and to $|X|_4$. The wiring diagram of this reducer is given in Figure 9. The output of this reducer is $\left||X|_5\right|_3$, $\left||X|_5\right|_4$, and $|X|_5$ as shown on Figure 7.

In the next step the three outputs of the reducer are complemented. The wiring diagram for the complementer is given in Figure 10. As seen from Figure 10, the complementer is a wiring connection that connects each input to the correct output line. The complements that have been found enter the adder. The adder adds

$$|X|_3 + \left\{-\left||X|_5\right|_3\right\} = |S|_3$$

$$|X|_4 + \left\{-\left||X|_5\right|_4\right\} = |S|_4$$

$$|X|_5 + \left\{-|X|_5\right\} = 0$$

and works in the same way as the adder part of Figure 4.

The second step of the previously given numerical example is accomplished by the multiplier (by $\frac{1}{5}$). A wiring

diagram for this multiplier is given in Figure 8. This multiplier is a wiring connection that connects each input to the correct output line. The output of the multiplier is $|X|_3$ and $|X|_4$.

As was stated in the numerical example, the third step is analogous to the first step. This analogy is apparent in the successive blocks of Figure 7. The output of the multiplier (by $\frac{1}{5}$) is reduced to modulo 3 and modulo 4 and then complemented. The complements then enter the second adder where they are added to the outputs of the multiplier (by $\frac{1}{5}$). The output of this second adder, when multiplied by $\left|\frac{1}{4}\right|_3 = 1$, is the most significant digit. The product of the radices is 20 in this case.

The output of the multiplier (by $\frac{1}{5}$) which is designated $|X|_4$ is the next most significant digit. The product of the radices is 5 in this case.

The input $|X|_5$ is the least significant digit. The coefficient of this digit is always 1.

The problems of conversion of this mixed radix number to a decimal number are not formidable. Each digit would be multiplied by its coefficient and then the three products would be added. However, as seen in Section II, the mixed radix number is ordered and for most purposes is as convenient to use as a decimal or other fixed radix number.

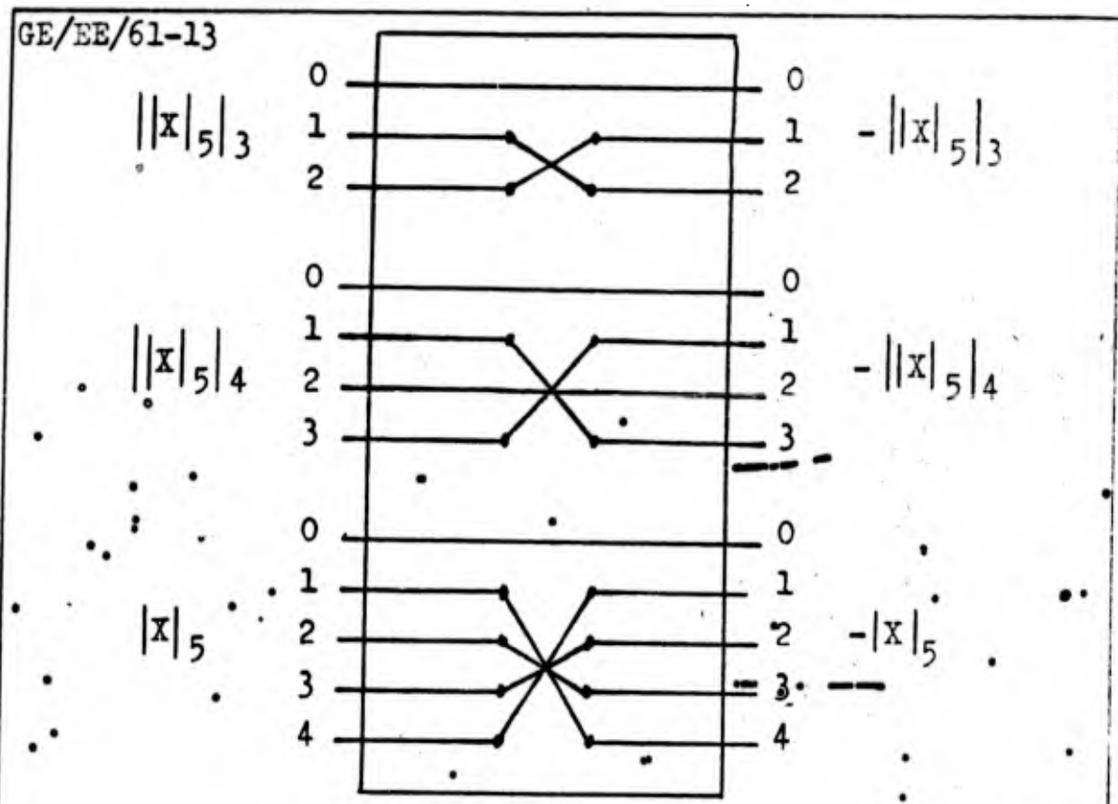


Figure 10
Complementer

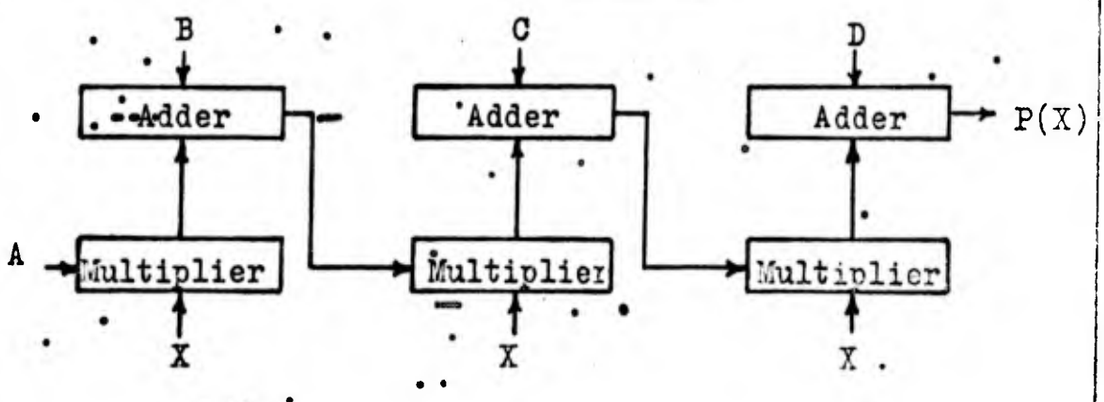


Figure 11
A General Polynomial Evaluator

V. A Polynomial Evaluator

General

This section presents the design for a polynomial evaluator that uses the principles of modular arithmetic. This polynomial evaluator establishes the value of P(X) for given values of the independent variable, X, and values of the variable coefficients.

The function chosen, which is general enough to demonstrate the method, is

$$P(X) = AX^3 + BX^2 + CX + D \qquad (23)$$

The method of evaluation of this function is the same factor method used in Section III to reduce a decimal integer to a modular set. In that same way this function will be factored and reduced to its representation modulo 3, 4, and 5.

The function P(X) can be factored as follows:

$$P(X) = \{(AX + B)X + C\}X + D \qquad (24)$$

Figure 11 is a block diagram of the way this multiplication and addition, which constitute the evaluation of P(X) can be performed.

Description

In the specific case of polynomial evaluation using the moduli 3, 4, and 5 there are actually three separate evaluators, one for each modulus, and P(X) is expressed modulo 3, modulo 4, and modulo 5.

With this representation P(X) is a unique integer on the range $0 \leq P(X) \leq 59$.

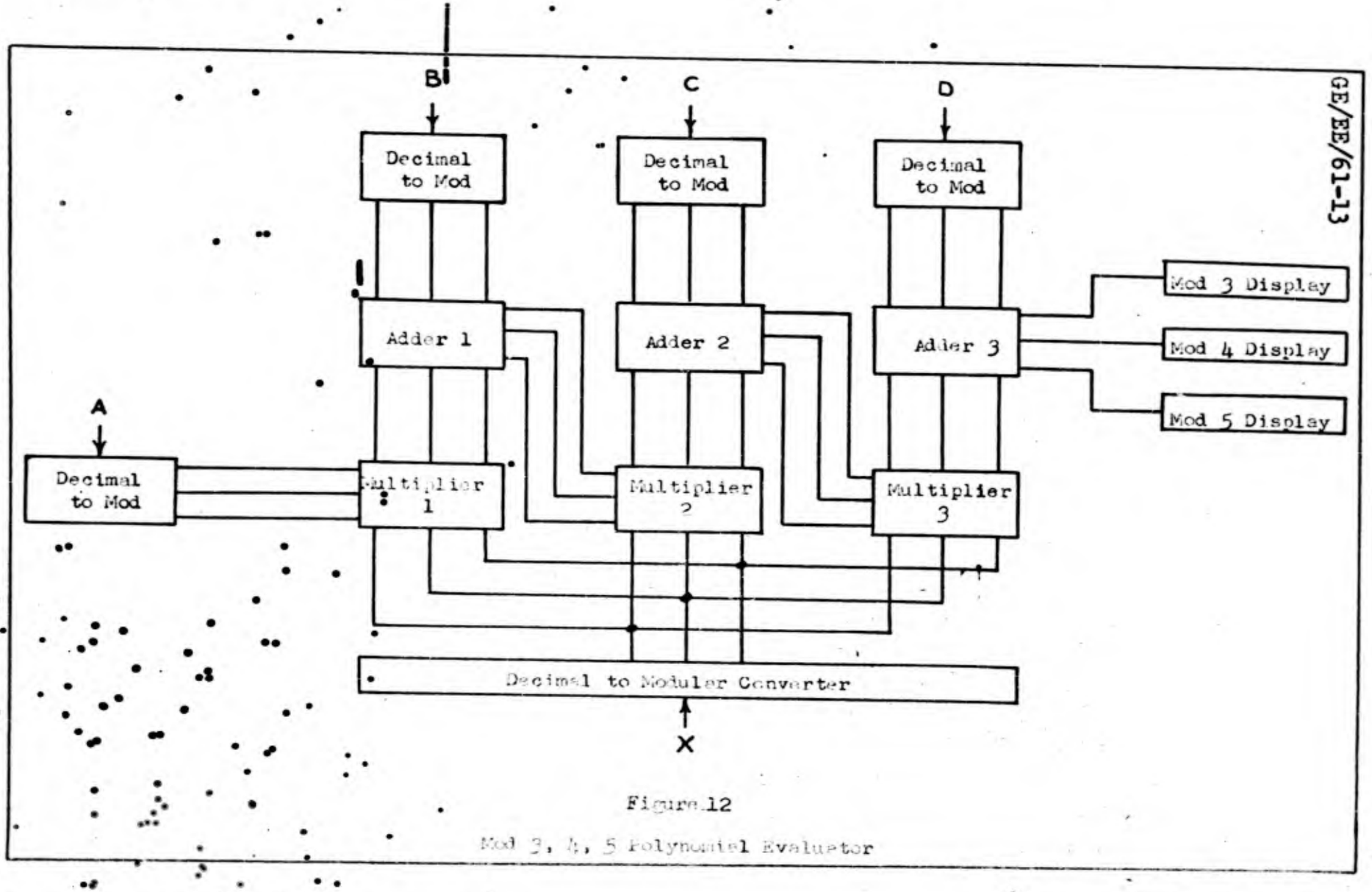


Figure 12

Mod 3, 4, 5 Polynomial Evaluator

Figure 12 is a block diagram of a polynomial evaluator using the moduli 3, 4, and 5. It must be emphasized that in theory any number of relatively prime moduli of any magnitude could be used. The moduli 3, 4, and 5 are used for convenience of demonstration. All the components of this evaluator are identical to those corresponding components previously described in Section III.

At the bottom of Figure 12 is the decimal-to-modular converter for the independent variable X. X, mod 3, 4, and 5, may be considered as one of the inputs to each multiplier. X mod 3, 4, and 5 are three inputs, but each multiplier is in fact a modulo 3 multiplier, a modulo 4 multiplier, and a modulo 5 multiplier; therefore, each variable is reduced modulo 3, 4, and 5. The other input to multiplier 1 is A. The product AX modulo 3, 4, and 5 is designated $|P_1|_3$, $|P_1|_4$, and $|P_1|_5$.

P_1 and B are the inputs to adder 1. The output of adder 1 is

$$P_1 + B = AX + B \qquad (25)$$

and this output is multiplied by X in multiplier 2 to form the product P_2.

$$P_2 = (AX + B)\,X \qquad (26)$$

P_2 and C are the inputs to adder 2. The output of adder 2 is

$$P_2 + C = (AX + B)\,X + C \qquad (27)$$

and this output is multiplied by X in multiplier 3 to form the product P_3.

$$P_3 = \{(AX + B) X + C\} X \tag{28}$$

The inputs to adder 3 are P_3 and D. The output of adder 3 is

$$P(X) = \{(AX + B) X + C\} X + D \tag{29}$$

The output P(X) is displayed on a separate array of lights for each of the three modular systems. If a mixed radix or fixed radix expression of P(X) is desired, the modular representation could be converted to the desired form by the methods proposed in Section IV.

As was previously stated, the methods used here to evaluate P(X) are an extension of the method used in Section III to reduce a decimal integer to its modular equivalent. That part that was a constant 10 in Section III has become a variable X in this section.

This method of evaluation of P(X) could be extended to evaluate functions with higher powers of X with only modest requirements for additional equipment.

VI. Conclusions

It has been shown that modular arithmetic is a practical basis for computer logic in those specialized cases where integer addition and multiplication are the only operations required. The advantage offered by a modular system is speed. Since modular arithmetic operations do not involve carry, the time required for addition or multiplication, in the modular form, is only the time required for electrical energy to traverse the system.

Computation by the methods of modular arithmetic is seriously handicapped by the problems of division, fractional operations, and sign determination. Satisfactory solutions to these problems have not been found yet.

The design of the converter which transforms a modular set to a mixed radix number is offered to show that such a conversion is not difficult. The design of the polynomial evaluator of Section V is further evidence of the usefulness of modular arithmetic.

A method of addition and multiplication by modular arithmetic using gating components and a core matrix has been devised (Ref 1:5-1). Therefore, any device described in this report could be constructed using gating components and using the principles of modular arithmetic. A device constructed in this way should prove economical as to size and use of time.

The explanation of modular arithmetic offered in Section II is an introduction to the principles of this subject. It could serve the purpose of familiarizing one with the principles of a logic that shows promise of a significant advance in the computer art.

Bibliography

1. Aiken, H. and W. Semon Advanced Digital Computer Logic, WADC-TR-59-472 (1959).

2. Aiken, H. et. al. Progress Report No. AF-60, Notes On Modular Number Systems (Contract AF 33 (616)-6903), Cambridge, Mass., The Computation Laboratory, Harvard University (1960).

3. Dickson, L. E. Modern Elementary Theory of Numbers, Chicago, University of Chicago Press (1939).

4. Dickson, L. E. Theory of Numbers, Vol II; New York Chelsea (1952).

5. Garner, H. L. "The Residue Number System", IRE Transactions on Electronic Computers, (June, 1959).

6. Ore, O. Number Theory and Its History, New York, McGraw-Hill (1948).

7. Vinogradov, I. M. Elements of Number Theory, New York, Dover Publications (1954).

Appendix A

A Proof of the Chinese Remainder Theorem

The following is a summary of the proof of the Chinese Remainder Theorem. This proof is based on H. L. Garner's idea of a modular set as a vector.

The following statements are needed to frame the problem.

It can be shown that if a decimal integer, X, is expressed modulo m_1, m_2, . . . , and m_n (all m relatively prime integers) then the expression (labelled $(X_1, X_2, \ldots, X_n) = X$) is unique in the range

$$0 \leq X \leq M - 1.$$

where

$$M = m_1 m_2 \cdots m_n = \prod_{i=1}^{n} m_i \tag{30}$$

Now consider $\alpha(X)$ to be the mapping of a decimal integer to a modular set, $(X_1, X_2, \ldots, X_n) = X'$. Consider $\alpha^{-1}(X_1, X_2, \cdots, X_n)$ to be the mapping of a modular set to a decimal integer, X.

Note that

$$(X_1, X_2, \cdots, X_n) + (Y_1, Y_2, \cdots, Y_n) = (|X_1 + Y_1|_{m_1}, |X_2 + Y_2|_{m_2}, \ldots, |X_n + Y_n|_{m_n}) \tag{31}$$

and

$$A(X_1, X_2, \ldots, X_n) = (|AX_1|_{m_1}, |AX_2|_{m_2}, \ldots, |AX_n|_{m_n}) \tag{32}$$

The proof outline follows:

Consider that

$$\alpha^{-1}(X_1, X_2, \cdots, X_n) = \alpha^{-1}\{(X_1, 0, \cdots, 0) + (0, X_2, \cdots, 0) + \cdots + (0, 0, \cdots, X_n)\}$$

which is

$$= \alpha^{-1}\{X_1(1, 0, \cdots, 0) + X_2(0, 1, \cdots, 0) + \cdots + X_n(0, 0, \cdots, 1)\} \quad (33)$$

also consider that

$$\alpha^{-1}(X_1 + X_2 + X_3) = \left| \alpha^{-1}(X_1) + \alpha^{-1}(X_2) + \alpha^{-1}(X_3) \right|_M \quad (34)$$

and

$$\alpha^{-1}(AX_1 + BX_2 + CX_3) = \left| A\alpha^{-1}(X_1) + B\alpha^{-1}(X_2) + C\alpha^{-1}(X_3) \right|_M \quad (35)$$

then

$$\alpha^{-1}(X_1, X_2, \cdots, X_n) = \left| X_1\alpha^{-1}(1, 0, \cdots, 0) + X_2\alpha^{-1}(0, 1, \cdots, 0) + \cdots + X_n\alpha^{-1}(0, 0, \cdots, 1) \right|_M \quad (36)$$

which is

$$|X|_M = \left| X_1 k_1 \hat{m}_1 + X_2 k_2 \hat{m}_2 + \cdots + X_n k_n \hat{m}_n \right|_M \quad (37)$$

where

$$\hat{m}_i = \frac{M}{m_i} \quad (12)$$

therefore

$$|X|_M = \left| \sum_{i=1}^{n} X_i k_i \hat{m}_i \right|_M \tag{38}$$

note that

$$|k_i \hat{m}_i|_{m_i} = 1 \tag{39}$$

therefore, since k_i is always less than m_i

$$|k_i|_{m_i} = \left| \frac{1}{\hat{m}_i} \right|_{m_i} = k_i \tag{40}$$

and when this is substituted into equation (38) it yields

$$|X|_M = \left| \sum_{i=1}^{n} X_i \left| \frac{1}{\hat{m}_i} \right|_{m_i} m_i \right|_M \tag{41}$$

and since

$$X_i = |X|_{m_i}$$

then

$$|X|_M = \left| \sum_{i=1}^{n} \hat{m}_i \left| \frac{X}{\hat{m}_i} \right|_{m_i} \right|_M \tag{11}$$

This concludes the outline of the proof that follows. In the proof that follows all definitions are made formally and almost all statements, most of which are obvious from the linear property of transformation to a modular set, are proven.

As an introductory statement prior to the proof the following statements are made and notations are given:

From Gauss' idea of congruence a special case is considered;

$$q \equiv b \pmod{m} \tag{1}$$

where $0 \leq b < m$ can be symbolized

$$|q|_m = b \tag{3}$$

or stated as b is the residue of q mod m, or further

$$q = b + m\left[\frac{q}{m}\right] \tag{4}$$

where $\left[\frac{q}{m}\right]$ is defined as the greatest integer in $\frac{q}{m}$.

Definitions:

$I \doteq$ set of all integers ≥ 0 and X represents any integer in the set. (42)

$I_M \doteq$ set of all integers which are ≥ 0 and less than M, where M is an integer. $\overline{X}$ is any integer in the set I_M. (43)

$I' \doteq$ the set of all n-tuples $(X_1, X_2, \cdots, X_n)$ where $0 \leq X_1 < m_1$, $0 \leq X_2 < m_2, \cdots, 0 \leq X_n < m_n$ and $m_1, m_2, \cdots, m_n$ are relatively prime integers. X' is any vector in the set I'. (44)

$I'_M \doteq$ the set of all n-tuples $(X_1, X_2, \cdots, X_n)$ where $0 \leq X_1 < m_1$, $0 \leq X_2 < m_2, \cdots, 0 \leq X_n < m_n$ and $m_1, m_2, \cdots, m_n$ are relatively prime integers. X'_M is any vector in the set I'_M. (45)

The product

$$M \triangleq m_1 m_2 \cdots m_n = \prod_{i=1}^{n} m_i \tag{30}$$

The mapping

$$\alpha(X) \triangleq (X_1, X_2, \cdots, X_n) = X' \tag{46}$$

where

$$X_1 = |X|_{m_1},\ X_2 = |X|_{m_2}, \cdots,\ X_n = |X|_{m_n}$$

The mapping

$$\alpha_M(X) \triangleq X'_M = (X_1, X_2, \cdots, X_n) \tag{47}$$

where

$$X_1 = |X|_{m_1},\ X_2 = |X|_{m_2},\quad ,\ X_n = |X|_{m_n}$$

The sum

$$(X_1, X_2, \cdots, X_n) + (Y_1, Y_2, \cdots, Y_n) \triangleq (\ X_1+Y_1\ m_1,$$

$$X_2+Y_2\ m_2, \cdots,\ X_n+Y_n\ m_n) \tag{31}$$

The product

$$A\ (X_1, X_2, \cdots, X_n) \triangleq (|AX_1|_{m_1},\ |AX_2|_{m_2}, \cdots,\ |AX_n|_{m_n}) \tag{32}$$

Now note since m_i divides M

$$|X|_{m_i} = \Big|\ |X|_M\Big|_{m_i} \tag{48}$$

If

$$(b, m) = 1$$

then there exist numbers h and k such that

$$hm + kb = 1 \tag{49}$$

therefore

$$\left|\frac{1}{b}\right|_m = |k|_m \tag{50}$$

Equation (48) is directly from known number theory (Ref 6:34). The following remarks are given as a preparation for the proof of the Chinese Remainder Theorem.

From equations (46), (47), and (48) consider $X = \overline{X} (\text{mod } M)$. X maps to X′ by $\alpha(X) = X'$ and $\overline{X}$ maps to X'_M by $\alpha_M(X) = X'_M$ and $X' = X'_M$. (51)

A well known theorem from number theory (Ref 7:45) is:

> If a congruence, $X \equiv X_1$, is true for several moduli, then it is true for the modulus equal to the least common multiple of these moduli. (52)

The number

$$|X|_M = \alpha^{-1}(X_1, X_2, \cdots, X_n)$$

which is the digital number represented by a particular vector, $(X_1, X_2, \cdots, X_n)$. (53)

If the one-to-one property of this mapping is obvious the following proof may be omitted.

There are M possible integers in the set I_M. There are M possible vectors $X' = (X_1, X_2, \cdots, X_n)$. Presume that there are two numbers X_A and X_B which map to one vector

$$X' = (Y_1, Y_2, \cdots, Y_n)$$

therefore

$$\begin{aligned} |\bar{X}_A|_{m_1} &= Y_1 = |\bar{X}_B|_{m_1} \\ |\bar{X}_B|_{m_2} &= Y_2 = |\bar{X}_B|_{m_2} \\ &\vdots \quad\quad \vdots \quad\quad \vdots \\ |\bar{X}_A|_{m_n} &= Y_n = |\bar{X}_B|_{m_n} \end{aligned} \tag{54}$$

however, from theorem (52)

$$|\bar{X}_A|_M = |\bar{X}_B|_M = X_A = X_B \tag{55}$$

The following is the proof of the Chinese Remainder Theorem. From equation (31)

$$|X|_M = \bar{\alpha}^{-1}(X_1, X_2, \cdots, X_n) = \bar{\alpha}^{-1}\{(X_1, 0, \cdots, 0) + (0, X_2, \cdots, 0) + \cdots + (0, 0, \cdots, X_n)\}$$

which is

$$= \bar{\alpha}^{-1}\{X_1(1, 0, \cdots, 0) + X_2(0, 1, \cdots, 0) + \cdots + X_n(0, 0, \cdots, 1)\} \tag{33}$$

which represents X_i each times a unit vector.

Now

$$\bar{\alpha}^{-1}(X_1' + X_2' + X_3') = |\bar{\alpha}^{-1}(X_1') + \bar{\alpha}^{-1}(X_2') + \bar{\alpha}^{-1}(X_3')|_M \tag{34}$$

and

$$\alpha^{-1}(AX_1' + BX_2' + CX_3') = \left| A\alpha^{-1}(X_1') + B\alpha^{-1}(X_2') + C\alpha^{-1}(X_3') \right|_M \quad (35)$$

The proof of equations (34) and (35) is shown in the following slightly modified form of equation (35).

$$\alpha^{-1}(AX_1' + BX_2') = \left| A\alpha^{-1}(X_1') + B\alpha^{-1}(X_2') \right|_M \quad (56)$$

Consider

$$\alpha\left\{\alpha^{-1}(AX_1' + BX_2')\right\} = AX_1' + BX_2' \quad (57)$$

which from equations (31) and (32)

$$= \left|AX_{11} + BX_{21}\right|_{m_1}, \left|AX_{12} + BX_{22}\right|_{m_2}, \ldots, \left|AX_{1n} + BX_{2n}\right|_{m_n} \quad (58)$$

Also consider

$$\alpha\left|A\alpha^{-1}(X_1') + B\alpha^{-1}(X_2')\right|_M = \left\{\left|\left|A\alpha^{-1}(X_1') + B\alpha^{-1}(X_2')\right|_M\right|_{m_1}, \ldots, \left|\left|A\alpha^{-1}(X_1') + B\alpha^{-1}(X_2')\right|_M\right|_{m_n}\right\} \quad (59)$$

The following operations are taken for the residue modulo m_1 only. Residues mod m_2, $m_3, \ldots, m_n$ will follow similarly. Since m_1 divides M

$$\left|\left|A\alpha^{-1}(X_1') + B\alpha^{-1}(X_2')\right|_M\right|_{m_1} = \left|A\alpha^{-1}(X_1') + B\alpha^{-1}(X_2')\right|_{m_1} \quad (60)$$

and

$$= \left|\left|A\alpha^{-1}(X_1')\right|_{m_1} + \left|B\alpha^{-1}(X_2')\right|_{m_1}\right|_{m_1} \quad (61)$$

also

$$\left|A\tilde{\alpha}'(X_1')\right|_{m_1} = \left|\left|A\right|_{m_1}\left|\tilde{\alpha}'(X_1')\right|_{m_1}\right|_{m_1} \tag{62}$$

and

$$\left|B\tilde{\alpha}'(X_2')\right|_{m_1} = \left|\left|B\right|_{m_1}\left|\tilde{\alpha}'(X_2')\right|_{m_1}\right|_{m_1} \tag{63}$$

again from equation (46) it will be noted that

$$\left|\tilde{\alpha}'(X_1')\right|_{m_1} = X_{11} \quad \text{and} \quad \left|\tilde{\alpha}'(X_2')\right|_{m_1} = X_{21} \tag{64}$$

Therefore

$$\left|A\tilde{\alpha}'(X_1')\right|_{m_1} = \left|\left|A\right|_{m_1} X_{11}\right|_{m_1} = \left|AX_{11}\right|_{m_1} \tag{65}$$

and

$$\left|B\tilde{\alpha}'(X_2')\right|_{m_1} = \left|\left|B\right|_{m_1} X_{21}\right|_{m_1} = \left|BX_{21}\right|_{m_1} \tag{66}$$

It then follows that

$$\left|\left|A\tilde{\alpha}'(X_1')\right|_{m_1} + \left|B\tilde{\alpha}'(X_2')\right|_{m_1}\right|_{m_1} = \left|\left|AX_{11}\right|_{m_1} + \left|BX_{21}\right|_{m_1}\right|_{m_1}$$

$$= \left|AX_{11} + BX_{21}\right|_{m_1} \tag{67}$$

By following the same operations mod m_n, it is seen that

$$\alpha\left|A\tilde{\alpha}'(X_1') + B\tilde{\alpha}'(X_2')\right|_M = \left\{\left|AX_{11} + BX_{21}\right|_{m_1}, \cdots,\right.$$

$$\left.\left|AX_{1n} + BX_{2n}\right|_{m_n}\right\} \tag{68}$$

Therefore, the modified form of equation (35) is proven and from that it is seen that equations (34) and (35) are true statements. Therefore

$$\vec{\alpha}'(X_1, X_2, \cdots, X_n) = \left|X_1\vec{\alpha}'(1, 0, \cdots, 0)\right.$$

$$\left. + X_2\vec{\alpha}'(0, 1, \cdots, 0) + \cdots + X_n\vec{\alpha}'(0, 0, \cdots, 1)\right|_M \qquad (36)$$

and recall that the vector

$$\vec{\alpha}'(1, 0, \cdots, 0) = k_1 \frac{M}{m_1} = k_1\hat{m}_1, \cdots, \vec{\alpha}'(0, 0, \cdots, 1)$$

$$= k_n\hat{m}_n$$

where $k_i < m_i$.

So

$$\vec{\alpha}'(X_1, X_2, \cdots, X_n) = \left|X_1k_1\hat{m}_1 + X_2k_2\hat{m}_2 + \cdots + X_nk_n\hat{m}_n\right|_M \qquad (37)$$

$$= \left|\sum_{i=1}^{n} X_ik_i\hat{m}_i\right|_M \qquad (38)$$

Also recall the vector property and that

$$\left|k_im_i\right|_{m_i} = 1 \qquad (39)$$

and

$$\left|k_i\right|_{m_i} = k_i = \left|\frac{1}{\hat{m}_i}\right|_{m_i} \qquad (40)$$

Let

$$X = \sum_{i=1}^{n}\left|\frac{1}{\hat{m}_i}\right|_{m_i}\hat{m}_iX_i \qquad (69)$$

then by equation (37)

$$|X|_M = \alpha'(X_1, X_2, \cdots, X_n) \tag{70}$$

Since by equation (46)

$$|X|_{m_i} = \left| |X|_M \right|_{m_i} = X_i$$

and finally

$$|X|_M = \left| \sum_{i=1}^{n} \left| \frac{X}{\hat{m}_i} \right|_{m_i} \hat{m}_i \right|_M \tag{11}$$

Other proofs of the Chinese Remainder Theorem are given in the literature (Ref 1:2-3, 3:16).

Vita

Gerald Forrest Mackey was born on [redacted] he entered the College of Engineering of the University of California at Berkeley. In 1950 he entered the United States Naval Academy, Annapolis, Maryland, and was graduated in June 1954 with the degree of Bachelor of Science. He was commissioned as Lieutenant in the USAF upon graduation, he entered pilot training in August 1954. His military assignment prior to entry to the Institute of Technology was in the 82nd Fighter Interceptor Squadron.

Permanent address: [redacted]

This thesis was typed by Mrs. Gerald F. Mackey

UNCLASSIFIED