N FACTORABLE OR PRIME

By

GERALD KENNETH GOFF

Bachelor of Arts
Phillips University
Enid, Oklahoma
1950

Master of Education
Phillips University
Enid, Oklahoma
1953

Submitted to the faculty of the Graduate School of
Oklahoma State University
in partial fulfillment of
the requirements for the
degree of
DOCTOR OF EDUCATION
August, 1962

N FACTORABLE OR PRIME

Thesis Approved:

W. Ware Marsden
Thesis Adviser

Robert D Morrison

James H. Zant

James E. Moser

Dean of the Graduate School

PREFACE

The problem of determining whether a number is prime or composite is one of the classic problems of number theory. Many attempts by many mathematicians have as yet to produce a simple concise method of determination.

The methods explained in this report are not always simple for large numbers, but they are procedures which will determine whether a number is prime or composite. For small numbers, one thousand or less, the methods work very well.

I gratefully acknowledge indebtedness to Dr. W. Ware Marsden and Dr. James H. Zant for their guidance and constructive criticism given throughout the study. I thank Dr. James E. Frazier and Dr. Robert D. Morrison for their valuable assistance and helpful suggestions.

I also wish to acknowledge indebtedness to Mr. Ben Hermanski, Breckenridge, Oklahoma, for encouragement and common interest in the problem.

I owe special thanks to my wife, Louise, and my children, Kathy and Kelly, for their indulgence throughout this project.

G. K. G.

TABLE OF CONTENTS

CHAPTER I

HISTORICAL BACKGROUND

One of the philosophies concerning the foundations of mathematics is intuitionism. The intuitionist thesis is that mathematics is to be built solely by finite constructive methods on the intuitively given sequence of natural numbers. The intuitionists would embrace Leopold Kronecker, a twentieth century German mathematician, and his classic remark, "Die ganzen zahlen hat Gott gemacht, alles anderes ist Menschenwerk",[1] which translates as,"God made the whole numbers, all the rest is the work of man." This concept of the nature of mathematics places special emphasis on whole numbers as building blocks and, as a consequence, the special properties of the whole numbers play a very important role in any mathematical work.

While the whole numbers have many properties, the attribute of being composite or prime is possibly one of the most fascinating. In addition to being fascinating this property is quite useful in many investigations involving whole numbers. Prime whole numbers, usually referred to as prime numbers, are building blocks from which all real numbers may be constructed. For this reason, prime numbers have received much study and it would be a mathematician's delight to discover a function F(n) which would yield prime numbers for all positive

[1] B. M. Stewart, Theory of Numbers, New York: The Macmillan Company, 1952, p. 1.

integral n.

Prime numbers are important and useful in any problem relating to number theory but the study of prime numbers alone is not sufficient. The other aspect of this property, compositeness, is also of importance and one aspect cannot be completely divorced from the other. The purpose of this particular study is to develop an algorithm which will determine if a given whole number is prime or composite and, if it is composite, produce all factors of the whole number.

The procedure nearest at hand for determining whether a given whole number is composite or prime is closely related to Eratosthene's sieve.[2] This procedure consists of considering all primes less than the given whole number and determining whether any of these primes are factors of the given number by attempting to divide the number by each of the primes. If none of the primes divide the whole number it is prime. If one of the primes p does divide the given number n, one can write n = pm and then repeat the procedure with the smaller number m. Repeated application of this procedure will eventually produce all the prime divisors of the given number and enable one to express the number as a product of primes. The computation involved in this procedure is reduced by the fact that if a number is composite it must have a factor which does not exceed the square root of the number. This implies that only primes less than or equal to the square root of the given number need be considered. The computation required by this procedure can be reduced even more by utilizing Theorem I from Chapter II which will establish a smaller upper limit

[2] Howard Eves, An Introduction to the History of Mathematics, New York: Rinehart and Company, Inc., 1953, p. 144.

for the set of primes to be considered. Another useful observation is that when the smallest prime factor p of a number n is found to be greater than the cube root of n, the other factor m in $n = pm$ must be prime. This is easily shown since if m is composite, $m = ab$, both a and b will be greater than the cube root of n and this will lead to the obvious contradiction $n = pab > \sqrt[3]{n}\ \sqrt[3]{n}\ \sqrt[3]{n} = n$.

About 1640, Pierre de Fermat produced an algorithm for factoring composite numbers. Fermat's algorithm is based on the idea that an odd number which is not a square can be expressed as the difference of two squares in as many ways as it is the product of two factors. Fermat explained his method in a letter to F. M. Mersenne[3] and the essence of his method is illustrated in the following example. Given a number n, say 51, extract the square root. The square root r is 7 with the remainder 2. Subtract the latter from $2r + 1$ and you have 13 which is not a square. Hence add $2 + 2r + 1$ to 13 and you have 30 which is not a square. Continue until you get a square by adding the number two greater than the number previously added. In this case the next step would be to add 19 to 30 and this produces a square, 49. Now take the first number added, 17, and subtract from the last number added, 19, divide the difference by two and then add two. In this example this would produce a 3. Next, add 3 to the root $r = 7$ and this will give you 10. Finally, add and subtract the square root of the square produced by the additions and you have the two numbers nearest to r whose product is n. In this example, $(10 + 7)(10 - 7) = (17)(3) = 51$.

[3] L. E. Dickson, History of the Theory of Numbers, Vol. I, Washington: Carnegie Institute of Washington, 1919, p. 357.

The above example of Fermat's algorithm is vague and difficult to follow. The mathematical principles involved are not particularly difficult but the abstract symbolism to which we are accustomed was not available to Fermat at his time in history. Hence it was necessary for Fermat to express himself as illustrated. The concept of zero was only some three hundred years old during the time of Fermat and many notations used today were unheard of during his period.

Another method of factoring as proposed in 1796 by C. F. Kausler[4] consists of adding the square of 1 to n, the square of 2 to n, the square of 3 to n, et cetera until the sum is a square and then factoring as a difference of two squares. Using the same n as the previous example, this method is illustrated as follows:

$51 + 1 = 52$	not a square
$51 + 4 = 55$	not a square
$51 + 9 = 60$	not a square
$51 + 16 = 67$	not a square
$51 + 25 = 76$	not a square
$51 + 36 = 87$	not a square
$51 + 49 = 100$	square of 10

Now $51 = 100 - 49 = 10^2 - 7^2 = (10 + 7)(10 - 7) = (17)(3)$.

While the method of Kausler is mathematically sound, the computation involved has disadvantages. One must know the successive squares which are to be added and also, if one starts with a large number, this process creates still larger numbers which are troublesome. The difficulty of the successive squares to be added can be

[4] L. E. Dickson, History of the Theory of Numbers, Vol. I, Washington: Carnegie Institute of Washington, 1919, p. 357.

alleviated by making use of the fact that any square, n^2, can be represented as the sum of the odd numbers from 1 to $2n - 1$ inclusive. To utilize this fact one can alter the procedure slightly by not returning to the given number each time and then adding a square but instead, use the previous sum as an addend and the next odd number as the other addend to create the next sum. When one of the sums is a square, factors of the number can be found as before. Considering the given number of the previous example, 51, and incorporating this change, the method appears as follows:

$51 + 1 = 52$	not a square
$52 + 3 = 55$	not a square
$55 + 5 = 60$	not a square
$60 + 7 = 67$	not a square
$67 + 9 = 76$	not a square
$76 + 11 = 87$	not a square
$87 + 13 = 100$	square of 10

Now $51 = 100 - (\frac{1}{2}(13 + 1))^2 = 10^2 - 7^2 = (17)(3)$.

In 1889, C. J. Busk[5] gave a method for factoring a number which was essentially that of Fermat. This method of factoring was put into general algebraic form by W. H. H. Hudson[6] in the same year. If Fermat had known or had had available to him the algebraic notation of this period he probably would have presented his algorithm in much the same way as did Busk and Hudson. The following illustrates the algebraic form as given by Hudson:

[5] L. E. Dickson, History of the Theory of Numbers, Vol. I, Washington: Carnegie Institute of Washington, 1919, p. 358.

[6] Ibid.

Let N be the given number and x^2 the next higher square. Then $N = x^2 - r_o = (x + 1)^2 - r_1 = (x + 2)^2 - r_2 = \cdots$ where $r_1, r_2, r_3, \cdots$ are formed from r_o by successive additions of $2x + 1, 2x + 3, 2x + 5, \cdots$. Thus $r_y = r_o + 2xy + y^2$. If r_y is a square, then N is the difference of two squares and N can be represented as a product of two numbers.

The preceding illustration is based on the same mathematical principles underlying the illustration on pages 3 and 4. Thus Hudson, in comparison to Fermat, was able to express the same mathematical principles in a more concise manner through the use of algebraic notation.

As an example of the algorithm of Busk and Hudson, again consider 51 as the given number, then:

$51 = 8^2 - 13$, 13 is not a square

$51 = (8 + 1)^2 - (13 + 2(8) + 1) = 9^2 - 30$, 30 is not a square,

$51 = (8 + 2)^2 - (30 + 2(8) + 3) = 10^2 - 49$, 49 is 7^2.

Thus $51 = 10^2 - 7^2 = (10 + 7)(10 - 7) = (17)(3)$.

This method also involves computational difficulties. Since one must recognize squares to use this method, the mechanics are simplified a great deal if one knows the twenty-two possible combinations of the last two digits in any square. These twenty-two endings are listed in Appendix I. Another computational difficulty inherent in this method becomes evident when N is large. The labor involved in applying this algorithm may become prohibitive except in special cases. The computation involved in this method will be cut in half in Chapter II through the use of two theorems.

CHAPTER II

EXTENSIONS OF METHODS IN CHAPTER I

The methods of factoring discussed in Chapter I were designed primarily to be used on composite numbers. The method of Busk and Hudson will produce the pair of factors of a number which are nearest to the square root of the number. In many cases more than one pair of factors exist and in many other cases no proper factors exist. This particular method can be extended to include all cases.

Theorem I: If $n = ab$ and $a \leq b$ with N, a, b whole numbers then $a \leq \left[x_0 - \sqrt{r_0}\right]$ when $N = x_0^2 - r_0$ and $x_0 = -[-\sqrt{N}]$.

Proof: Let $x_j = (b + a)/2$ and $y_j = (b - a)/2$ then, $b = x_j + y_j$, $a = x_j - y_j$, and $N = ab = (x_j - y_j)(x_j + y_j) = x_j^2 - y_j^2$ with $x_j > 0$ and $y_j \geq 0$. Thus every factorization of a composite number can be represented uniquely as the difference of two squares. The minimum value of x_j is x_0 where $x_0 = -[-\sqrt{N}]$ for if $x_j < x_0$ this implies $-y_j^2 > 0$, an obvious contradiction. Now $N = x_0^2 - y_0^2 = x_1^2 - y_1^2 = \cdots = x_i^2 - y_i^2$ where $x_i = x_0 + i$, $i = 0, 1, 2, \cdots$ and y_i is a non-negative real number. Let $x_j > x_0$, $j = 1, 2, 3, \cdots$ and $x_j^2 - y_j^2 = x_0^2 - y_0^2$. Now $x_j^2 - x_0^2 = y_j^2 - y_0^2$ which implies $y_j > y_0$. Since $(x_j - y_j)(x_j + y_j) = (x_0 - y_0)(x_0 + y_0)$ then $x_j - y_j =$

$$\frac{(x_0 - y_0)(x_0 + y_0)}{x_j + y_j}.$$

But $x_0 > y_0 > 0$, $x_j > y_j > 0$, $x_j > x_0$, $y_j > y_0$ so $0 < (x_0 + y_0)/(x_j + y_j) < 1$ and $x_j - y_j < x_o - y_o = x_0 - \sqrt{r}$. Thus, if $N = ab$ and $a \leq b$, then $a \leq x_0 - \sqrt{r}$, and since a is a whole number, $a \leq \left[x_0 - \sqrt{r}\right]$.

In this particular method the initial representation for N is $x_0^2 - r_0$ and Theorem I assures us that any pair of factors will have one of the pair less than or equal to $\left[x_0 - \sqrt{r_0}\right]$. The steps of the algorithm will produce an ordered set of representations for N, $\left\{x_0^2 - r_0, x_1^2 - r_1, x_2^2 - r_2, \cdots, x_i^2 - r_i\right\}$ where $x_j > x_k$ if $j > k$. In this ordered set, $x_{j-1} - \sqrt{r_{j-1}} < x_j - \sqrt{r_j}$ from the proof of Theorem I, and if $x_i - \sqrt{r_i} = 1$ with $i > j$, then the set will produce all factors of N. Each pair of factors will correspond to one and only one $x_j^2 - r_j$ and no factors will be omitted since, for each pair of factors, $\left[x_0 - \sqrt{r_0}\right]$ is an upper bound for the smaller factor of the pair and $x_i - \sqrt{r_i}$ is a lower bound. Thus, the algorithm as extended will produce all factors of a given number if continued until the number $N = x_i^2 - r_i$ with $x_i - \sqrt{r_i} = 1$.

The method can now be extended to determine if N is prime. If r_i is a square and r_j is not a square for $j = 0, 1, 2, \cdots, i - 1$ then N is prime. This follows from the previous argument for if N has proper factors then some r_j must be a square. However, this contradicts the hypothesis and hence N has no proper factors.

With the initial representation of N determined by Theorem I, and taking $N = x_i^2 - r_i$ with $x_i - \sqrt{r_i} = 1$ as the terminal representation, one can now use the extended algorithm to determine whether N is composite or prime and if N is composite to produce all factors.

One of the obvious limitations of this algorithm is the amount of computation involved. In Chapter I it was mentioned that this computation could be reduced by approximately one-half through the use of two theorems. These two theorems are as follows:

Theorem II: If $N \equiv 1 \bmod 4$ and $N = x^2 - y^2$ then x is odd and y is even.

Proof: Since N is odd, $N \equiv 1 \bmod 4$ or $N \equiv 3 \bmod 4$. Assume x is even and y is odd. Let $x = 2p$ and $y = 2q + 1$, then $x^2 = 4p^2$ and $y^2 = 4(q^2 + q) + 1$. Now $x^2 - y^2 = 4p^2 - 4(q^2 + q) - 1$ or $4k - 1$ with $k = p^2 - q^2 - q$. $4k - 1 \equiv - 1 \bmod 4$ or $N \equiv 3 \bmod 4$ which contradicts the hypothesis. Therefore x must be odd and y must be even.

Theorem III: If $N \equiv 3 \bmod 4$ and $N = x^2 - y^2$ then x is even and y is odd.

Proof: The proof of this theorem follows immediately from the proof of Theorem II.

Thus is $N \equiv 1 \bmod 4$ the number of elements in the set $\{x_0^2 - r_0, x_1^2 - r_1, \cdots, x_i^2 - r_i\}$ is approximately one-half the number previously used since we need consider only odd numbers for x_i and the even ones can be deleted. If $N \equiv 3 \bmod 4$, the x_i values must be even and the odd values can be deleted, reducing the number of representations by approximately one-half. Examples illustrating this reduction will be given in Chapter III.

By making an additional observation, one can further reduce the computation necessary in the algorithm. Since we are considering only odd numbers as the given number, the number two cannot be a factor. This permits one to eliminate the steps in the algorithm between the representation $N = x_j^2 - r_j$ where $x_j - \sqrt{r_j} \leq 3$ and the terminal representation $N = x_i^2 - r_i$ with $x_i - \sqrt{r_i} = 1$.

Theorem I can also be used to reduce the computation involved in the method in which one uses prime trial divisors. Previously all primes, $p_i \leq \sqrt{N}$, were considered as possible divisors, whereas at this point only primes, $p_i \leq \left[x_0 - \sqrt{r_0}\right]$, need be considered. The two sets of primes determined by these upper bounds are identical if $r_0 = 0$. But if $r_0 > 0$ then the latter set will generally have a smaller number of elements and can never have a larger number of elements than the former set. The use of Theorem I to reduce the computation of this method will be illustrated in Chapter III.

CHAPTER III

EXAMPLES AND ILLUSTRATIONS

To illustrate how the extended method of Busk and Hudson will produce all factors of a composite number, consider $N = 105$:

$$\begin{array}{rrcrl}
N = 105 = & 11^2 & - & 16 & = (11 - 4)(11 + 4) = 7(15) \\
 & 23 & - & 23 & \text{since } 2(11) + 1 = 23 \\
105 = & 12^2 & - & 39 & \\
 & 25 & - & 25 & \text{since } 2(11) + 3 = 25 \\
105 = & 13^2 & - & 64 & = (13 - 8)(13 + 8) = 5(21) \\
 & 27 & - & 27 & \\
105 = & 14^2 & - & 91 & \\
 & 29 & - & 29 & \\
105 = & 15^2 & - & 120 & \\
 & 31 & - & 31 & \\
105 = & 16^2 & - & 151 & \\
 & 33 & - & 33 & \\
105 = & 17^2 & - & 184 & \\
 & 35 & - & 35 & \\
105 = & 18^2 & - & 219 & \\
 & 37 & - & 37 & \\
105 = & 19^2 & - & 256 & = (19 - 16)(19 + 16) = 3(35)
\end{array}$$

Since $19 - 16 \leq 3$ the terminal representation is the only other representation which will be the difference of two squares. $N = 53^2 - 52^2 = 1(105)$. Thus the set of factors for 105 is $\{1, 3, 5, 7, 15, 21, 35, 105\}$.

Using Theorem II with the same given number the x_j values must be odd since $N = 105 \equiv 1 \bmod 4$. The previous example can now be reduced to:

$$\begin{array}{rcrcl} N = 105 = & 11^2 & - & 16 & = (11 - 4)(11 + 4) = 7(15) \\ & 48 & - & 48 & \text{since } 13^2 = 11^2 + 4(11) + 4 \\ 105 = & 13^2 & - & 64 & = (13 - 8)(13 + 8) = 5(21) \\ & 56 & - & 56 & \\ 105 = & 15^2 & - & 120 & \\ & 64 & - & 64 & \\ 105 = & 17^2 & - & 184 & \\ & 72 & - & 72 & \\ 105 = & 19^2 & - & 256 & = (19 - 16)(19 + 16) = 3(35) \end{array}$$

Since $19 - 16 \leq 3$ the only other representation which can produce factors is the terminal representation.

$N = 53^2 - 52^2 = 1(105)$.

In this example, the application of Theorem II reduced the number of steps from eight to four not counting the initial and terminal steps. Thus the application of Theorem II or Theorem III, whichever is applicable, will reduce the computation necessary in this algorithm by approximately one-half.

The extended method of Busk and Hudson will also determine when a given number is prime. The following application of the algorithm will illustrate how this is done.

Let $N = 131 = 12^2 - \ 13$ and $131 \equiv 3 \bmod 4$

$52 - 52$

$131 = 14^2 - 65$

$60 - 60$

$131 = 16^2 - 125$

$68 - 68$

$131 = 18^2 - 193$

$76 - 76$

$131 = 20^2 - 269$

$84 - 84$

$131 = 22^2 - 353$

$92 - 92$

$131 = 24^2 - 445$; but $24 - \sqrt{445} \leq 3$ and the only representation of 131 as the difference of two squares is the terminal representation.

Therefore, 131 is prime.

One interesting problem for which the extended method of Busk and Hudson offers a systematic solution is:

A merchant has a number of ties priced at $2.00 each. He marked the price down and sold all the ties. The net proceeds from the sale of the ties was $603.77. How many ties did the merchant sell, and what was their selling price?

Let x be the number of ties and let y be the price in cents of the ties; then $xy = 60377$.

$$
\begin{array}{rcrcl}
60377 & = & 246^2 & - & 139 \text{ and } 60377 \equiv 1 \bmod 4 \\
 & & 493 & - & 493 \\
60377 & = & 247^2 & - & 632 \\
 & & 992 & - & 992 \\
60377 & = & 249^2 & - & 1624 \\
 & & 1000 & - & 1000 \\
60377 & = & 251^2 & - & 2624 \\
 & & 1008 & - & 1008 \\
60377 & = & 253^2 & - & 3632 \\
 & & 1016 & - & 1016 \\
60377 & = & 255^2 & - & 4648 \\
 & & 1024 & - & 1024 \\
60377 & = & 257^2 & - & 5672 \\
 & & 1032 & - & 1032 \\
60377 & = & 259^2 & - & 6704 \\
 & & 1040 & - & 1040 \\
60377 & = & 261^2 & - & 7744 = 261^2 - 88^2 = (261 - 88)(261 + 8) \\
60377 & = & 173(349) & &
\end{array}
$$

Since 173 and 349 are prime the two solutions are $x = 349$, $y = 173$ and $x = 60377$, $y = 1$. The most reasonable answer is 349 ties sold at $1.73 each.

Theorem I can be used in conjunction with the method of using prime trial divisors. The upper bound for the prime divisors of a number will determine the maximum number of trials necessary and since Theorem I establishes an upper bound less than or equal to the upper bound previously used, the computation is therefore reduced. This reduction is illustrated in the two examples which follow:

Example I: Let $N = 53 = 8^2 - 11$. Using $\sqrt{N}$ as the upper bound, the set of trial divisors is $\{2, 3, 5, 7\}$ and four divisions are necessary to determine whether 53 is prime or composite and to find all factors if it is composite. Using the upper bound from Theorem I, $[8 - \sqrt{11}] = 4$, the set of prime trial divisors is $\{2, 3\}$ and only two divisions are necessary to complete the method. Since 2 does not divide 53 and 3 does not divide 53, we can conclude that 53 is prime.

Example II: Let $N = 403 = 21^2 - 38$. Using $\sqrt{N}$ as the upper bound the set of prime trial divisors will be $\{2, 3, 5, 7, 11, 13, 17, 19\}$. Using the upper bound determined by Theorem I, $[21 - \sqrt{38}] = 14$, the set is $\{2, 3, 5, 7, 11, 13\}$. Now 2, 3, 5, 7, 11 do not divide 403 but 13 does divide 403. Since $13 > \sqrt[3]{403}$ the other factor is also prime and $403 = 13(31)$, the only pair of proper factors of 403.

CHAPTER IV

A METHOD OF FACTORING USING MATRICES

An integer can be represented as the determinant of a two by two matrix since $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$. If the elements a, b, c, d are taken as $a = d = x$ with $b = r$ and $c = 1$, then $N = x^2 - r = \begin{vmatrix} x & r \\ 1 & x \end{vmatrix}$.

Before proceeding with this method it will be necessary to prove the following theorem:

Theorem IV: If $N = \begin{vmatrix} x & y \\ 1 & z \end{vmatrix}$ with x, y, z integers and if d divides x then d divides N if and only if d divides y. And, if d divides y then d divides N if and only if d divides x or z.

Proof: If d divides y then $y = dq$. $x = dp$ by hypothesis and $N = \begin{vmatrix} dp & dq \\ 1 & z \end{vmatrix} = dpz - dq = d(pz - q)$. Since $N = d(pz - q)$, d divides N. If d does not divide y, assume d divides N. Now $N = dM$. $dM = \begin{vmatrix} dp & y \\ 1 & z \end{vmatrix} = dpz - y$ and $y = dpz - dM$. Since $y = d(pz - M)$, d divides y which is a contradiction and if d does not divide y, d does not divide N. The second part of the theorem follows since interchanging any two lines of a matrix merely changes the sign of the determinant and the determinant A equals the determinant of A transpose.

Since N is represented in terms of the determinant of a matrix the properties and theorems of matrix algebra can be utilized in the method. Two theorems from matrix algebra which will be used in this method are as follows:

"Theorem 2.7.6 Let B be a square matrix the same as A except that all the elements of some line of B are k times the corresponding elements of the corresponding line of A. Then det B = k det A."[7]

"Theorem 2.7.8 If in A we add any multiple of one line to a different, parallel line, the determinant of the new matrix equals det A."[8]

Using these two theorems in conjunction with Theorem I and Theorem IV, it is now possible to determine whether a given number N is composite or prime and if composite to determine all prime factors.

Let N = $\begin{vmatrix} x & r \\ 1 & x \end{vmatrix}$ with $x = -[\sqrt{N}]$. Now if N has factors there must be some prime p_i such that p_i belongs to the set $\{p_i \mid p_i \leq [x - \sqrt{r}]\}$. To test each p_i in the set, operate on the determinant of the matrix so as to create a multiple of p_i in the upper left position. This can be done by multiplying the second row by k and adding to the first row where x + k will be a multiple of p_i. Now if p_i divides the element in the upper right position, p_i is a factor of N and if p_i does not divide the element in the upper right position, it is not a factor of N. If one exhausts the p_i's and does not find a factor of N, then N is prime.

The method is illustrated in the following examples:

Example I: Let N = 371 = $\begin{vmatrix} 20 & 29 \\ 1 & 20 \end{vmatrix}$. $p_i \leq [20 - \sqrt{29}] = 14$

[7] Franz E. Hohn, Elementary Matrix Algebra, New York: The Macmillan Company, 1958, p. 36.

[8] Ibid., p. 37.

and the set of p_i's = $\{2, 3, 5, 7, 11, 13\}$. $N = \begin{vmatrix} 20 & 29 \\ 1 & 20 \end{vmatrix}$. 2 divides 20, 2 does not divide 29, therefore 2 does not divide 371. 5 divides 20, 5 does not divide 29, therefore 5 does not divide 371. $N = \begin{vmatrix} 21 & 49 \\ 1 & 20 \end{vmatrix}$. 3 divides 21, 3 does not divide 49, therefore 3 does not divide 371. 7 divides 21, 7 divides 49, therefore 7 divides 371. Hence, $371 = 7\begin{vmatrix} 3 & 7 \\ 1 & 20 \end{vmatrix} = 7(53)$. Now $53 = \begin{vmatrix} 8 & 11 \\ 1 & 8 \end{vmatrix}$. $p_i \leq [8 - \sqrt{11}] = 4$ and the set of p_i's = $\{2, 3\}$. It has already been determined that neither 2 nor 3 divide 371 so neither will divide 53 and 53 is prime. Therefore, 371 = 7(53) is a prime factorization of the given number.

Example II: Let $N = 1001 = \begin{vmatrix} 32 & 23 \\ 1 & 32 \end{vmatrix}$. $p_i \leq [32 - \sqrt{23}] = 27$ and the set of p_i's is $\{2, 3, 5, 7, 11, 13, 17, 19, 23\}$. $1001 = \begin{vmatrix} 32 & 23 \\ 1 & 32 \end{vmatrix}$. 2 divides 32, 2 does not divide 23, therefore 2 does not divide 1001. 23 divides 23, 23 does not divide 32, therefore 23 does not divide 1001. $1001 = \begin{vmatrix} 33 & 55 \\ 1 & 32 \end{vmatrix}$. 3 divides 33, 3 does not divide 55, therefore 3 does not divide 1001. 11 divides 33, 11 divides 55, therefore 11 divides 1001. Hence, $1001 = 11\begin{vmatrix} 3 & 5 \\ 1 & 32 \end{vmatrix} = 11(96 - 50)$ and $1001 = 11(91)$. Now $91 = 10^2 - 3^2 = (10 + 3)(10 - 3)$ and $91 = 13(7)$. $1001 = 7(11)(13)$ which is a prime factorization of 1001.

This method of factoring can be considered an extension of the method of using prime trial divisors. The use of a determinant of a matrix to express N changes the procedure from dividing one number by the prime trial divisors to dividing two considerably smaller numbers by the trial divisors. The line operations of the determinant can be considered as extra manipulations but, by creating multiples of two or more of the trial divisors in the upper left position, two or more trial divisors can be tested with each representation.

CHAPTER V

USES AND APPLICATIONS

The educational uses of the extended methods of factoring are quite varied and occur at several places in the mathematics curriculum of today. Not all of the methods are applicable at all levels but various aspects of the different methods can be used in several levels.

The method using prime trial divisors can be used with the fifth grade material of the School Mathematics Study Group.[9] In the section designated as EB11 the concepts of factors and primes are introduced. Eratosthene's sieve is used to determine the primes less than 100 and the upper bound of $\sqrt{N}$ is also included in an exercise designed to challenge students. The basic concepts necessary to understand this method of factoring are present in this material and could be used to provide a somewhat different approach to factors and primes. The method of factoring by prime trial divisors could also be used as enrichment material for the superior students.

The method of prime trial divisors can also be used with the SMSG material in the text, Mathematics for Junior High School.[10] The treatment of prime and composite numbers in this text is very similar to the treatment in the fifth grade material and the method

[9] SMSG, Mathematics for the Elementary School, New Haven, Connecticut: Yale University, 1961.

[10] SMSG, Mathematics for Junior High Schools, New Haven, Connecticut: Yale University, 1960, Part I, p. 151.

of prime trial divisors could be used in the same way as with the fifth grade material.

Prime and composite numbers are again included in the SMSG First Course in Algebra.[11] The treatment is very similar to the two previously mentioned and the applications are the same. However, since the students at this level should be more mature mathematically, the presentation may be more theoretical.

Factoring as the difference of two squares is introduced in the text.[12] The introduction of this concept would equip the students so they could use the method of Busk and Hudson. This method would be good material for all students at this level and should prove interesting and stimulating to the superior students.

The method of factoring using matrices would be good supplementary material for the students taking a course using the SMSG text, Introduction to Matrix Algebra.[13] Two by two matrices and their determinants are presented in this text and the method of factoring using matrices would be particularly applicable in this material. This method would be an example of how some of the comparatively recent developments in mathematics can be made to apply to older topics.

Another use for the methods of factoring can be found in conjunction with the supplementary material for secondary mathematics. The

[11] SMSG, First Course in Algebra, New Haven, Connecticut: Yale University, 1960, part II, p. 252.

[12] Ibid., p. 325.

[13] SMSG, Introduction to Matrix Algebra, New Haven, Connecticut: Yale University, 1960, p. 77.

SMSG material, Essays on Number Theory,[14] is a good example of supplementary material with which the methods of factoring could be used.

Another use of the methods of factoring would be in the training of secondary mathematics teachers. To present the material on prime and composite numbers, some knowledge of the various methods would be desirable. This knowledge can be acquired in many ways but it would be good to have the material included somewhere in the curriculum required for prospective teachers. Some appropriate courses in which this material could be included are courses in elementary number theory, matrix algebra, modern algebra, and methods of teaching mathematics.

The inclusion of material of this type in the mathematics of the elementary school also means that the elementary teachers must become familiar with the material. Thus, the material should be included in the curriculum of prospective elementary teachers.

Another use for material on factoring numbers is in conjunction with in-service programs for teachers in the field. This material could be used in institutes, extension courses, or any project intended to give help to teachers.

Finally, the extended method of Busk and Hudson is adaptable to programming for a computer. The algorithm has been programmed and tested on the IBM 650. The program and results of the tests are included in appendix II.

[14] SMSG, Essays on Number Theory, New Haven, Connecticut: Yale University, 1960, parts I, II.

BIBLIOGRAPHY

Dickson, L. E., *History of the Theory of Numbers,* Washington: Carnegie Institute, Vol. I, II, III, 1919.

Eves, Howard, *An Introduction to the History of Mathematics,* New York: Rinehart and Company, Inc., 1953.

Eves, Howard and Newsom, Carroll V., *An Introduction to the Foundations and Fundamental Concepts of Mathematics,* New York: Rinehart and Company, Inc., 1958.

Hohn, Franz E., *Elementary Matrix Algebra,* New York: The Macmillan Company, 1958.

Landau, Edmund, *Elementary Number Theory,* New York: Chelsea Publishing Company, 1958.

LeVeque, William J., *Topics in Number Theory,* Reading, Massachusetts: Addison Wesley Publishing Company, Inc., Vol. I, II, 1956.

Mathews, G. B., *Theory of Numbers,* New York: G. E. Stechert and Company, 1927.

Nagell, Trygve, *Introduction to Number Theory,* New York: John Wiley and Sons, Inc., 1951.

Ore, Oystein, *Number Theory and Its History,* New York: McGraw-Hill Book Company, Inc., 1948.

School Mathematics Study Group, *Essays on Number Theory,* New Haven, Connecticut: Yale University, 1960.

School Mathematics Study Group, *First Course in Algebra,* New Haven, Connecticut: Yale University, 1960.

School Mathematics Study Group, *Introduction to Matrix Algebra,* New Haven, Connecticut: Yale University, 1960.

School Mathematics Study Group, *Mathematics for Junior High Schools,* New Haven, Connecticut: Yale University, 1960.

School Mathematics Study Group, *Mathematics for the Elementary School,* New Haven, Connecticut: Yale University, 1961.

Stewart, B. M., *Theory of Numbers,* New York: The Macmillan Company, 1952.

INDEX OF SYMBOLS

APPENDIX I

Twenty-two possible endings for perfect squares:

00
01
04
09
16
21
24
25
29
36
41
44
49
56
61
64
69
76
81
84
89
96

APPENDIX II

Program for the extended method of Busk and Hudson written in Fortran language for the 650 Fortran System.

```
1  READ, N1, N2
   M=N1
   N=N2
2  I=I
   N3=N
3  N3=N3-I
   IF(N3) 4, 5, 6
6  I = I+2
   GO TO 3
4  N=N+4*(M+1)
   NS=N
   M=M+2
   GO TO 2
5  K=(I+1)/2
   L1=M+K
   L2=M-K
   L=L1*L2
   PUNCH, N1, N2, L1, L2, L
   IF (L2-1) 6, 1, 7
7  N=NS
   GO TO 4
   END
```

In this program, $L = N1^2 - N2$ with N1 even or odd according as 3 or 1 Mod 4 and $N1^2 \geq N$ with $N1 = -[-\sqrt{N}]$ or $-[-\sqrt{N}] + 1$.

The program was tested on the IBM 650 by using L = 51 which is composite and L = 31 which is prime. In the case where L = 51 two cards were punched out, one gave 17 and 3 for L1 and L2, the other gave 51 and 1 for L1 and L2. In the case where L = 31 only one card was punched out and this card gave 31 and 1 for L1 and L2.

VITA

Gerald Kenneth Goff

Candidate for the Degree of

Doctor of Education

Thesis: N FACTORABLE OR PRIME

Major Field: Higher Education

Biographical:

Personal Date: Born at Apache, Oklahoma, June 26, 1925, the son of Orville H. and Justin Ruth Goff.

Education: Attended grade school in Apache, Oklahoma; graduated from Apache High School in 1943; received the Bachelor of Arts degree from Phillips University, Enid, Oklahoma, with majors in mathematics and physics, in May, 1950; received the Masters of Education degree from Phillips University in July, 1953.

Professional Experience: Entered the United States Navy in 1943; was discharged in 1946; was employed as a teacher in the high school at Verden, Oklahoma from 1950 to 1955; was high school principal the last two years at Verden; was high school principal at Garber High School, Garber, Oklahoma for the school year 1955-56; was employed at Southwestern State College, Weatherford, Oklahoma in June, 1957 as Assistant Professor of Mathematics and have remained in this position.