

Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

ON THE HISTORY OF THE PROBLEM OF SEPARATING A NUMBER INTO ITS PRIME FACTORS

By Professor D. N. LEHMER

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA

PERHAPS no other branch of mathematics offers to the non-mathematician so many inviting problems as the theory of numbers. The tools it employs are the simplest, and the methods of operation are familiar to every school-boy. It abounds in problems apparently of the greatest simplicity and really of such subtle make-up that they have baffled the efforts of the greatest mathematicians for centuries. There are many properties of numbers which we use daily, and which most of us are willing to take on experimental evidence, which would puzzle the untrained man to account for. What clerk has not used the method of "casting out the nines" to prove his computations—and how many clerks could give a valid reason for the check, and tell what are its limitations, or state the general law of which this is a special case?

Every carpenter has made use of the right triangle whose sides are 3, 4 and 5 with which to lay off a right angle. No doubt this was the practical method of constructing a right angle in the days of the pyramid builders. He would be a stupid carpenter who would never inquire if other triangles of that sort were not obtainable. He might easily find that others were to be had by multiplying the sides of this triangle by any number, but the question would still confront him as to the existence of other such triangles with sides having no common divisor. By experiment, which enters more into the investigation of problems of this sort than many imagine, he would perhaps hit upon the triangle 5, 12, 13, and then upon the triangle 8, 15, 17. He might then, for his own amusement, undertake to make a list of these triangles, arranging them in order according to the magnitude of the largest side. He would be rewarded first of all by the interesting discovery that sometimes two different triangles may have the same hypothenuse! such as 39, 52, 65 and 25, 60, 65. If he were of a statistical turn of mind he might discover that the number of triangles in his list increased with remarkable regularity with the magnitude of

the largest side. The number of triangles with largest side less than N is roughly proportioned to N. At this point in his career he may apply for help to some well-equipped specialist in the theory of numbers, and the result may be that a good carpenter is spoiled to make a trifling mathematician. One such experimenter, to my knowledge, pushed the investigation through till he found that the number of triangles with sides not greater than N is approximately $N/2\pi$ where π is the number 3.1415926 . . . which represents the ratio of the circumference of a circle to its diameter.

But of all the problems that lure the man of the street into the halls of useless but fascinating research none seems to appeal with more potent call than the problem of separating a given number into its prime factors. It is so easy to multiply two numbers together, and so hard to find them again when they have been welded into one! A multiplying machine will furnish the product of two eight-digit numbers in a few minutes. With all the resources of the theory of numbers at my disposal, I have spent I am ashamed to say how many hours in trying to determine whether the number 403,978,495,031 is a prime or not, and the question is still open. Why should I be interested, you ask, in such a problem? The answer to that question is that experimental work in another field is stopped till this vexing matter is settled. The problem of finding the factors of a given number is not only interesting in itself, but is vital for the investigator in many other researches, particularly in the theory of groups.

Perhaps some notion of the immense antiquity of this problem may be gained by observing that it is a problem that freguently suggests itself to children of ten or twelve years of age. When the progress of civilization in any tribe was such that the most thoughtful members were capable of the intellectual effort of a modern boy of fifteen the problem might likely arise. It might easily have attracted the attention of the cave man that six pebbles could be arranged in two ways; ..... and :::, while only one such arrangement could be found for five or seven pebbles. The discovery of the three ways of grouping twelve pebbles must have been as exciting and mystifying to the original researcher as the discovery of the first magic square. No doubt the number twelve gained considerable respect from this mystic property. The number six later enjoyed great prestige, because it was found that the sum of its divisors 1, 2 and 3 is equal to six! Pythagoras is said to have venerated the number 6 on account of the "integrity of its parts and the

agreement existing in it," calling it marriage and health and beauty! According to the early Christians, God created the earth in six days rather than in one because of the perfection of the number six. The entire human race sprang from the eight souls in Noah's Ark, and, as 8 is not so perfect as 6, we have been living under a disadvantage ever since!

Little is known of the assaults of the ancients on our problem. Their clumsy notation would have lent them little aid in their fight. It was a learned man that could perform a simple division even as late as the thirteenth century. Men like Archimedes were needed to get an approximation to a square root. Practical computation was done on the fingers or on the abacus, and perhaps the notation was of little more use than as a means of recording results. Nevertheless, it would be wrong to assume that previous to the invention of the modern method of denoting numbers mankind was not in possession of some of the most beautiful theorems concerning the properties of numbers. Thus Euclid gives a proof of the infinite number of primes, a proof which is found in almost every treatise on numbers to this day; and his process of finding the greatest common divisor, and his formula for perfect numbers are familiar to every student of this subject.

The first practical contribution to the problem of finding the factors of a number comes from another Greek, Eratosthenes, who lived some time in the second or third century B.C. He seems to have been a man of the greatest versatility, and has left his imprint on many different pages of science. He was librarian at the university of Alexandria, and was noted for his athletic achievements as well as for his literary interests. He devised the calendar in which every fourth year is 366 days long. He measured the length of a degree on the earth's surface and got a good approximation for the radius of the earth. In connection with our problem he invented the so-called "sieve" method which is the basis of construction of all the great factor-tables constructed since his day.

The sieve of Eratosthenes is constructed on the following observation: Every other number after 2 is divisible by 2; every third after 3 is divisible by 3; every fifth after 5 is divisible by 5 and so on. If then we write down the successive numbers in a row and erase every other number beginning with 4, and every third number beginning with 9, and every fifth number beginning with 25; and every seventh number beginning with 49, and so on, we shall have in the remaining numbers a list of successive primes. If instead of erasing the num-

bers we write over every other number beginning with 4 the factor 2, over every third number beginning with 9 the factor 3 we shall have for each number its decomposition into prime factors. The process requires no computation, and may be carried out by measurement alone.

Now the writing of a million numbers in a row turns out to be a somewhat tedious undertaking. Moreover, we are not much interested in finding the factors of the even numbers nor of the multiples of 5. If now we group the numbers in lines of ten thus

1, 2, 3, 4, 5, 6, 7, 8, 9, 10
11, 12, 13, 14, 15, 16, 17, 18, 19, 20
21, 22, 23, 24, 25, 26, 27, 28, 29, 30

we see that all the even numbers lie in the same columns and that the same is true of the multiples of 5. We then omit these columns altogether, thus cutting out sixty per cent. of the numbers in our list. This method of shortening the table of factors seems not to have been used till about the middle of the seventeenth century, when Rahn,[1] or Rhonius, gave such a table extending to 24,000, shortly afterwards extended to 100,000 by Thomas Brancker.[2] The tables preceding Rahn's tables were of a very insignificant sort. Thus Leonardo Pisano[3] in 1202 gave a list of the primes from 11 to 97, and the factors of the composite numbers from 12 to 100. Cataldi[4] in 1603 gave a table extending to 800 and Van Schooten[5] (1657) gave a list of primes to 9979.

It was later discovered that the multiples of 3 could be omitted from the table without very great complication. If we group our list of numbers in lines of thirty we see that the multiples of 2, 3 and 5 all appear in certain columns. Omitting those columns, our list of numbers appears thus:

1, 7, 11, 13, 17, 19, 23, 29
31, 37, 41, 43, 47, 49, 53, 59
61, 67, 71, 73, 77, 79, 83, 89

With the table arranged in this way it is easy to show that if a factor p appears in any place it will also appear in that same column p lines farther down. Eratosthenes's sieve method may then be applied to each column, or better by means of a

[1] Rahn, "Algebra," Zurich, 1659.

[2] Brancker, "An Introduction to Algebra," translated out of the High-Dutch [of Rahn's "Algebra"] into English by Thomas Brancker, 1668.

[3] Pisano, "Il Liber Abici di L. Pisano," 1202, revised 1228.

[4] Cataldi, "Trattato de' numeri perfetti," Bologna, 1603.

[5] van Schooten, "Exercitat. Math.," Leiden, 1657.

stencil to all the columns at once, to find the multiples of p. A table in which the multiples of 2, 3 and 5 were omitted was first published in 1728 by Poetius.[6] The invention of the stencil method is to be credited to C. F. Hindenburg,[7] 1776. That same year was published Felkel's[8] table in which the multiples of 2, 3 and 5 were omitted, the extent of the table being 408,000. Felkel made use of the device of designating the numbers by means of letters for the sake of saving space. The manuscript extended to two millions, but the sale was so meager that the entire edition was made into cartridges to use against the Turk. Only a few copies were saved.

In the early nineteenth century, responding to the urgent appeals of men like Gauss and others who were interested in verifying certain curious laws just discovered relating to the distribution of primes, there appeared the great table of Chernac[9] (1811) giving all the prime factors of all numbers not divisible by 2, 3 or 5 up to 1,020,000 containing 1,020 pages. The bulk of a factor table becomes a serious matter when a limit of several million is contemplated. It occurred to Burckhardt[10] that it is sufficient to know the smallest divisor, as the others may be obtained from the quotient. Burckhardt published such a table of the first three millions. Tables modeled after Burckhardt's were afterward published for the 4th, 5th and 6th million by Glaisher,[11] and for the 7th, 8th and 9th, by Dase.[12] The factor tables computed by myself[13] and published by the Carnegie Institution of Washington omit the multiples of 2, 3, 5 and 7 and carry the work up to the limit 10,000,000 (1909). A list of primes based on this factor table was published in 1914.

It should be stated that manuscript tables of factors were computed by a Bohemian named Kulik[14] up to the extraordinary

[6] Poetius, "Anleitung zu der Arith. Wissenschaft vermittelst einer parallel Algebra," 1728.

[7] Hindenberg, "Beschreibung einer ganz neuen Art," Leipzig, 1776.

[8] Felkel, "Tabula omnium factorum simplicium numerorum," 1776.

[9] Chernac, "Cribrum Arithmeticum," 1811.

[10] Burckhardt, "Tables des diviseurs," Paris, 1817, 1814, 1818 (for the respective three millions).

[11] Glaisher, "Factor Tables for the Fourth, Fifth and Sixth Millions," London, 1879, 1880, 1883.

[12] Dase, "Factoren-Tafeln für alle Zahlen der siebenten (1862) der achten (1863) der neunten (1865) Million," Hamburg.

[13] Lehmer, "Factor Table for the First Ten Millions," Carnegie Institution of Washington, 1909.

[14] Kulik. An account of Kulik's table will be found in the introduction to my list of primes. Carnegie Institution of Washington, 1914.

limit of 100 million! They were never published, and are at present, with the exception of one volume which has disappeared, in the library of the Royal Academy at Vienna. The tenth million of this colossal work I examined with great care in comparing it with my own computations and found some 226 errors in this one million. The great work is not accurate enough to warrant publication, but is of the greatest value for purposes of checking. He also represents the prime factors by means of letters, which makes it a little difficult to compare his table with others.

So much for factor-tables and lists of primes. We are still fairly helpless in the presence of a number that exceeds the limit of our tables, but there are certain schemes which avail to shorten the labor of decomposing a number into its factors which are of considerable service, particularly for numbers of certain kinds.

In 1643 Fermat[15] wrote to his friend Mersenne concerning the number 100,895,598,169: "You ask me whether this number is prime or not, and for a method for finding in one day's time whether it is prime or composite. I reply that it is composite and is the product of 898,423 and 112,303." Now this number happens to be associated with certain numbers of the form $2^n - 1$, the factors of which belong, as Fermat was the first to discover, to certain particular arithmetical progressions. If n is prime the factors of $2^n - 1$ are all equal to one plus a multiple of n. Naturally this wonderful theorem relieves one of the necessity of trying as divisors the greater part of the primes less than the square root of the number. Thus the number $2^{11} - 1 = 2047$ can have factors of the form $22n + 1$, so that the only factors we need try are 23 and 45, and the last being composite is also ruled out. By trial 23 is found to be a factor and $2047 = 23 \times 89$. This discovery of Fermat's has delivered into our hands our largest known primes. The largest one known at the present time is, I believe, $2^{127} - 1$, a number of 39 digits examined by Lucas in 1877.

The great Fermat[16] also invented a method of finding factors when nothing is known of the form of the factors which is very effective when the two factors do not differ very greatly from each other. If a square number can be found which when added to the given number produces a square then the given number is at once reduced to the difference of two squares and is the product of the sum and difference of two numbers. Fer-

[15] Fermat, "Œuvres," Tome 2, p. 255.

[16] Fermat, "Œuvres," Tome 2, p. 257.

mat gives the example 2,027,651,281, which he finds by a few trials to be the difference of the two squares 45041^2 and 1020^2. But the difference of these two squares is equal to the product of their sum 46061 by their difference 44021. Fermat was in possession of devices for shortening the labor of finding the two squares, but even with every such device and the help of computing machines, which adapt themselves very well to this method, the process may lead one an interminable chase in finding the factors of some numbers.

A more effective method depends on the theory of quadratic residues, the underlying principles of which may be made clear in a few words. If a number x can be found such that $x^2 - D$ is divisible by a number m then D is said to be a *quadratic residue* of m. D and m are supposed prime to each other. Such a number x is not always obtainable, and if none is to be found D is said to be a *quadratic non-residue* of m. From the definition it follows that if D is a quadratic residue of m it is a quadratic residue of every factor of m, for surely if an x exists such that $x^2 - 1$ is divisible by m then for that same value of x we shall have $x^2 - D$ divisible by every factor of m. The importance of this simple remark arises when we find that the numbers m which have a given D for quadratic residue all fall into certain arithmetical progressions. Thus those numbers which have 2 for a quadratic residue are all multiples of eight plus or minus unity. Those which have 3 for a quadratic residue are all multiples of twelve plus or minus unity, etc. If then it is known by any means that 2 and 3 are residues of a number we know that not only the number itself, but every odd factor of it, belongs to both of these series of numbers, and consequently belongs to the series 1, 25, 49, 73, 97, . . . or to the series 23, 47, 71, 95, . . . or, as we say, is of the form $24n + 1$. This knowledge enables us then to omit from our list of trial divisors all primes which do not fall in these series and the process of searching for factors is notably shortened.

It will at once be observed that the difficulty has only been shifted from one corner to another, and we are still confronted with the serious problem how to obtain quadratic residues small enough to be of service in this connection, for it should be observed that for larger quadratic residues the number of series is increased. Various devices have been invented for finding directly suitable quadratic residues, the best of which seems to be a by-product of the theory of continued fractions. Another is based on the theory of binary quadratic forms. All of these

methods have been in use for over a century, and are to be found in the works of Euler[17] and Legendre.[18] Where nothing is known of the form of the factors of the number these methods are perhaps the most powerful in our possession.

As the matter stands, then, we are complete masters of the situation for numbers up to ten millions, having reliable tables extending so far. There are photographic copies in this country of Kulik's table for the eleventh million, of which I have one. His second volume running from 12,642,600 to 22,852,800 is lost. The remaining volumes carry the table up to a limit of 100,330,201. In spite of their inaccuracy they are of the greatest value for comparison. For numbers beyond the limits of the available tables modern methods can be applied with fair hopes of success up to a limit, perhaps, of a billion. Beyond that limit, except for numbers of special form, the task of finding factors may well daunt the most intrepid of computers. The problem will always confront the human race. The invention of new methods may push off the limits of the unknown a little farther, just as the invention of a new astronomical instrument may push off a little the boundaries of the physical universe; but the unknown regions are infinite, and if we could come back a thousand years from now we should no doubt find workers in the theory of numbers announcing in the journals new schemes and new processes for the resolution of a given number into its factors.[19]

[17] Euler, "Nova Acta Petrop," 13, 1795–6.

[18] Legendre, "Theorie Des Nombres," 1798, pp. 313–320. A more complete bibliography will be found in the forthcoming "History of the Theory of Numbers," by L. E. Dickson, from which many of the above references are obtained.

[19] Since writing the above I have found the number 403,978,495,031 is equal to $6{,}151 \times 65{,}676{,}881$, both factors being primes. By expanding the square root of the number in a continued fraction it was found that the following numbers were quadratic residues: 2, 5, 7, -13, -17, 23, -29, 31, 43. This knowledge enabled me to reduce the number of trials to fifty-five. If the number had been a prime I should have had some seventy-five trials to make instead of over fifty-one thousand to determine the fact. The number is the denominator of the twenty-ninth convergent to the base of Naperian logarithms when that base is expanded in a regular continued fraction.