$$\sum_{i=1}^{m} d_i^2 = 4\sum_{i=1}^{m} \sin^2 \frac{\varphi_i}{2} = 2\sum_{i=1}^{m} (1-\cos\varphi_i) = 2(m-m\bar{r}_1),$$

and $\bar{r}_1$ has the value

$$\bar{r}_1 = 1-\frac{1}{2m}\sum_{i=1}^{m} d_i^2.$$

But this reckoning does not seem to lead to any particularly simple geometric interpretation for $\bar{r}$. It may turn out, in some circumstances at least, that $\bar{r}_1$ is the more significant measure after all.

THE UNIVERSITY OF MINNESOTA

METHODS FOR FINDING FACTORS OF LARGE INTEGERS*

BY H. S. VANDIVER

1. *Introduction.* We shall examine, in this paper, the problem of finding factors of integers beyond the range of Lehmer's factor tables, by methods shorter than that of dividing the integer by all the primes less than its square root.

Three methods will be proposed here. The first two depend on the representation of the integer as a definite quadratic form, and the third on the representation as an indefinite quadratic form. As I hope to devote another paper to the development of the last two methods, only outlines and a few examples will be given in connection with them.

The theory of quadratic forms has been applied in several different ways to the problem.†

In particular, Seelhoff‡ gave an expeditious method with the use of tables, which, however, is limited in application,

* Presented to the Society, September 7, 1923, under the title *A method of finding factors of integers of the form* $8n+1$. The author was enabled to carry out this investigation through a grant from the Heckscher Foundation for the Advancement of Research.

† Dickson, *History of the Theory of Numbers*, vol. 1, pp. 361–66.

‡ AMERICAN JOURNAL, vol. 7, p. 264; vol. 8, p. 26.

since if the integer is composite, it does not always enable us to determine the factors.

The first method explained in the present paper applies only to integers of the form $8n+1$ and $12n+1$ which are the product of two distinct primes. Although the process will always yield the factors in a finite number of steps, it is impracticable on account of its length if the integer is as large as 10^7. *Unlike other methods, however, the particular forms used are always the same.* Hence they lend themselves conveniently to the construction of tables with a view of lessening the amount of computation involved. The theory of indefinite forms has been applied by Tchebycheff* to our problem, but the method is quite different from the one given here which involves indefinite forms.

2. *First Method of Factorization.* Suppose that we have an integer m of the form $8n+1$ which is the product of two distinct prime factors. It is immediately seen that each factor has the same residue modulo 8, otherwise the product would not be of the form $8n+1$. If both are of the form $8n+1$ or both of the form $8n+5$ then m may be presented in more than one way in the form x^2+y^2, x and y prime to each other. Similarly if both are of the form $8n+3$ then m may be represented in more than one way in the form x^2+2y^2, x and y prime to each other. In the case where both are of the form $8n+7$ it will now be shown that m may be represented in at least two different ways in the form $2x^2-y^2$, where x and y are each $<\sqrt{m}$ and prime to each other.

In a paper which appeared in this BULLETIN (vol. 22 (1915), pp. 61–66) I proved that if p is a prime and a is a positive integer prime to p, then there is at least one and not more than two sets (x, y) such that

$$ay \equiv \pm x \pmod{p}$$

when x and y are positive integers prime to each other and $0<x<\sqrt{p}$, $0<y<\sqrt{p}$.

* LIOUVILLE, (1), vol. 16, p. 257.

On page 64 of the same article, I remarked that the existence of at least one set (x, y) satisfying the conditions

$$ay \equiv \pm x \pmod{m} \tag{1}$$

where m is composite followed also from the reasoning used. If two sets $(x_1\ y_1)$ and $(x_2 y_2)$ are regarded as the same if and only if $x_1 y_2 = x_2 y_1$ then for m any integer there are not more than two sets, a fact which was pointed out to me by Dr. C. F. Gummer.

If

$$\begin{cases} kx_1 \equiv y_1 \pmod{m}, \\ kx_2 \equiv y_2 \pmod{m}, \end{cases} \tag{2}$$

where $|x_1|$, $|y_1|$, $|x_2|$ and $|y_2|$ are each $< \sqrt{p}$, then from the first congruence

$$kx_1x_2 \equiv x_2y_1 \pmod{m};$$

and from the second

$$y_2x_1 - x_2y_1 \equiv 0 \pmod{m}.$$

This gives, on account of the range of values for the x's and y's,

$$y_2x_1 - x_2y_1 = \pm m \quad \text{or} \quad y_2x_1 - x_2y_1 = 0,$$

and the last relation can exist only if we regard the sets (x_1, y_1) and (x_2, y_2) as the same. If the first relation holds and therefore the two sets exist, then a third set different from them cannot exist. To show this we note in (2) that we may take both x_1 and x_2 positive, and if this is done then it follows, using the relation $y_2x_1 - x_2y_1 = \pm m$, that y_1 and y_2 have opposite signs. Hence we may write

$$kx_1 \equiv y_1 \pmod{m},$$
$$kx_3 \equiv y_3 \pmod{m},$$

where x_1 and x_3 are positive and y_1 and y_3 have the same sign. It follows as before that

$$y_3x_1 - x_3y_1 = \pm m,$$

and this is impossible since the expression on the left is, in absolute value, less than m.

Now consider the solution of

$$u^2-2 \equiv 0 \pmod{m}, \tag{3}$$

where m is the product of two distinct prime factors each of the form $8n+7$. There are four incongruent roots of the congruence which we will designate by $a, -a, b, -b$, where $a \not\equiv \pm b$. According to the theorem first proved we may write

$$av \equiv w \pmod{m},$$
$$bv_1 \equiv w_1 \pmod{m},$$

where $|v|, |w|, |v_1|, |w_1|$ are each less than $\sqrt{m}$. Squaring and using (3) we have

$$\begin{cases} 2v^2-w^2 \equiv 0 \pmod{m}, \\ 2v_1^2-w_1^2 \equiv 0 \pmod{m}, \end{cases} \tag{4}$$

or,

$$2v^2w_1^2 \equiv 2v_1^2w^2 \pmod{m},$$

and since m is odd,

$$(vw_1-v_1w)(vw_1+v_1w) \equiv 0 \pmod{m}. \tag{5}$$

Also from (4) we have

$$\begin{cases} 2v^2-w^2 = m, \\ 2v_1^2-w_1^2 = m. \end{cases} \tag{6}$$

We shall now show that in (5) one of the factors on the left is divisible by a factor of m but not by m. For if

$$vw_1+v_1w \equiv 0 \pmod{m},$$

then, since v, w, v_1, w_1 are all prime to m, we have, from (4), since m is not divisible by a square,

$$\frac{v}{w} \equiv \frac{-v_1}{w_1} \pmod{m},$$

or

$$a \equiv -b \pmod{m},$$

contrary to hypothesis; and if

$$vw_1-v_1w \equiv 0 \pmod{m},$$

then

$$a \equiv b \pmod{m},$$

which is also contrary to hypothesis.

Consequently, by taking the smallest positive factor in (5), and finding the greatest common divisor of it and m, we obtain a factor of m.

THEOREM. *If a number m of the form $8n+1$ is the product of two distinct primes then it is expressible in at least two different ways by one of the forms x^2+y^2, x^2+2y^2, and $2y^2-x^2$, where x and y are each positive and $<\sqrt{m}$. It is also possible to find two such representations which yield, by a direct process, a factor of m.*

This theorem gives the following scheme for finding a factor of an integer of the form $8n+1$.

(1.) Divide the integer by all primes less than its cube root. If it is divisible by a prime within this limit which is not of the form $8n+1$, the process cannot be carried further. Otherwise we may proceed as follows.

(2.) Extract the square root of the possibly new number m. If it is a perfect square, all the factors of m are known, as it cannot have more than two distinct prime factors other than unity. If m is not a perfect square we proceed to the third step.

(3.) Find by Gauss' method of exclusion all representations of m in the form x^2+y^2. If there is but one representation, then m is prime. If there is more than one, then the factors of m may be found from the several representations. If there are no representations then proceed to the next step.

(4.) Find by the method of exclusion all the representations of m in the form $2y^2-x^2$, where x and y are each $<\sqrt{m}$. It cannot have a unique representation, as it follows from this that m is prime, and this would have been detected in step 3. If there is more than one representation then the factors of m may be found from them. If there are no representations then we use the fifth step.

(5.) Find by the method of exclusion all the representations of m in the form x^2+2y^2. The factors of m are obtained from the several representations.

3. *Example.* Let us show how to factor $532481 = N$. Divide by all the primes <82, since $[\sqrt[3]{N}] = 81$. It is found that N is not divisible by any of these primes. Also N is not a square. Hence it is prime, or is the product of two distinct primes. We seek first all the values x, y, such that

$$x^2+y^2 = N.$$

Either x or y is odd* and each is <730. Suppose x is odd. Also $N \equiv 2 \pmod 3$. This gives $x \equiv \pm 1 \pmod 3$, since if $x \equiv 0 \pmod 3$ we find $y^2 \equiv 2 \pmod 3$, which is impossible. Hence since x is odd, we have $x \equiv \pm 1 \pmod 6$. Now $N \equiv 1 \pmod 5$; and, in a similar way, we find $x \equiv 0, \pm 1 \pmod 5$. Therefore $x \equiv 1, 5, 11, 19, 25, 29 \pmod{30}$. We have $N \equiv 5 \pmod 7$, and $x \equiv \pm 1, \pm 2 \pmod 7$. Modulo 210, x has the possible residues 1, 5, 19, 29, 41, 55, 61, 65, 71, 79, 89, 121, 125, 131, 139, 145, 149, 155, 169, 181, 191, 205, 209. Similarly x has the possible residues $0, \pm 1, \pm 2, \pm 5 \pmod{11}$; and we then set down the least possible residues of x modulo $11 \cdot 210$, which are less than 730. We find 68 numbers. Using the modulus 16, we may exclude numbers of the form 3, 5, 11 and 13, modulo 16. Similarly we may exclude numbers of the form 1, 4, 6, 11, 14, 19, 21, 24, modulo 25, and 3, 4, 5, 10, 11, 12, modulo 13. This leaves 12 possible values for x which we may test directly, and we find none that will give a representation of N in the required form.

We now proceed to step 4 and find all representations of the form

$$2y^2-x^2 = N,$$

where x and y are each $< \sqrt{N}$. In this relation $516 < y < 730$. Also $y \equiv 1 \pmod 2$. Possible values of y satisfy $y \equiv 0, \pm 1 \pmod 5$, $y \equiv 0, \pm 1 \pmod 7$. Modulo 70, y has therefore the possible residues 1, 15, 21, 29, 35, 49, 55, and 69. We find similarly $y \equiv 0, \pm 3, \pm 4 \pmod 9$. We then write down the integers between 516 and 730 having the above properties and find 519, 525, 545, 561, 581, 589, 609, 615, 645, 651, 679, 699, 715.

* The work could have been made shorter here by taking x even and noting that $x \equiv 0 \pmod 4$.

Now y cannot be congruent to 0, 4, 5, 6 or 7 (mod 11), and we may exclude integers of this type from the above set, leaving 519, 525, 581, 615, 651, 679. Actual trial of all these gives only two representations,

$$2 \cdot 525^2 - 137^2 = 2 \cdot 519^2 - 79^2 = N,$$

and

$$525 \cdot 79 - 519 \cdot 137 = 29628.$$

The greatest common divisor of N and 29628 is 823. Hence $N = 823 \cdot 647$, each of which is a prime.

A similar method may be applied to integers of the form $12n+1$. If N is of this form and the product of two distinct primes, then each has the same residue, modulo 12. If both are of the form $12n+1$, or $12n+5$, then N is expressible as the sum of two squares. If each is of the form $12n+7$ then $N = x^2 + 3y^2$. If each is of the form $12n+11$ then it may be shown that $2N = 3y^2 - x^2$, where x and y are each $< \sqrt{N}$. For in case the congruence $u^2 - 3 \equiv 0$ (mod N) is solvable and if a is one of its roots then $ma \equiv k$ (mod N) where m and k are each $< \sqrt{N}$, and therefore $3m^2 - k^2 \equiv 0$ (mod N) and $3m^2 - k^2 = N$ or $2N$. But the first case is impossible, since $N \equiv 1$ (mod 3). We then have all the material necessary to carry through a method for factoring integers of the form $12n+1$ analogous to that described for the case $8n+1$.

4. *Second Method of Factorization.* The second method of factorization is briefly as follows. Find by known methods a negative integer $-a$ which is a quadratic residue of n, the integer to be factored (n not a perfect power). From a known result in the theory of quadratic forms it follows that, corresponding to every root u of the congruence $u^2 \equiv -a \pmod{n}$ there is a set of integers x, y and k such that

$$x^2 + ay^2 = kn, \tag{1}$$

$k < 2\sqrt{a/3}$, x and y prime to each other.* From (1)

* This theorem was used by H. J. S. Smith, WORKS, vol. 1, p. 148 in the solution of the quadratic congruence.

we have $(-a/k_1) = 1$ where k_1 is any divisor of k, and $(kn/a_1) = 1$ where a_1 is any divisor of a. We select the k's satisfying these conditions, and also $k < 2\sqrt{a/3}$ and we find the possible forms

$$x_s^2 + ay_s^2 = k_s n,$$

$s = 1, 2, \ldots, i$. Find by Gauss' method of exclusion or other schemes all actual representations of this type; then all factors of n may be found from them, by known methods.

It is best to select a, if possible, so that it contains several small primes as factors since this will diminish the number of possible values of k.

5. *Example* 1. $n = 532481$. In order to find values of a as described above, expand $\sqrt{n}$ as a continued fraction. We have the corresponding values given in the following table.

Denominator of comp. quotient	Terms in cont. fraction
1	729
$1040 = 5 \cdot 13 \cdot 4^2$	1
419	2
$608 = 4^2 \cdot 2 \cdot 19$	2
$95 = 5 \cdot 19$	14
$1280 = 16^2 \cdot 5$	1
97	14
$160 = 4^2 \cdot 2 \cdot 5$	9
79	18

Hence $-5 \cdot 13$ is a residue of n, $-19 \cdot 2$ is an R (residue), $5 \cdot 19$ is an R, -5 is an R, -10 is an R, whence 2 and 13, -19 and -5 are residues. Also 79 is an R. Hence $-a = -2 \cdot 5 \cdot 13 \cdot 79$ is a residue. Hence

$$x^2 + ay^2 = kn,$$

where $k < 118$. From the relations $p_r^2 - nq_r^2 = \pm d_r$ where p_r/q_r is a convergent and d_r a denominator of comp.

quotient in development of $\sqrt{n}$ we have $(n/13) = (n/79) = (n/5) = 1$. Hence also $(k/5) = (k/13) = (k/79) = 1$. This gives $k \equiv 0, 1, 4 \pmod 5$ and $k \equiv 0, 1, 3, 4, 9, 10, 12 \pmod{13}$. We set down the integers

1	3	4	9	10	12	13
14	16	17	22	23	25	26
27	29	30	35	36	38	39
40	42	43	48	49	51	52
53	55	56	61	62	64	65
66	68	69	74	75	77	78
79	81	82	87	88	90	91
92	94	95	100	101	103	104
105	107	108	113	114	115	117.

We note also that $k \not\equiv 0, 3, 4, 5 \pmod 8$; using this with $k \not\equiv 2$ or $3 \pmod 5$ we have remaining

1	9	10	14	25	26
30	39	49	55	65	
66	74	79	81	90	
94	95	105	114.		

We have

$$\left(\frac{-2\cdot 5\cdot 13\cdot 79}{3}\right) = \left(\frac{-2\cdot 5\cdot 13\cdot 79}{7}\right) = -1.$$

Hence k cannot be a multiple of 3 or 7. Moreover, it is evident that k is not divisible by 5^2. This leaves

1	10	26	55	65
	74	79	94	95.

From $x^2 + ay^2 = 10n$ we have $5x^2 + 2\cdot 13\cdot 79y^2 = 2n$ whence $(13\cdot 79/5) = 1$ which is incorrect; this excludes 10. Similarly 26 is excluded, also 65. We have $(74/79) = -1 = (94/79)$ and these are then excluded leaving 1, 55, 79 and 95 as possible values of k. Let us now examine

$$x^2 + ay^2 = n.$$

Here y ranges from 1 to 7 inclusive, and it must be even, which gives us

$$701^2 + 10270\cdot 2^2 = n.$$

For $k = 55$, we have $5x^2 + 2 \cdot 13 \cdot 79\, y^2 = 11n$. Using Gauss' method of exclusion we have

$$y \equiv \pm 2 \pmod 5, \qquad y \equiv 1 \pmod 2,$$
$$y \not\equiv 0 \pmod 3, \qquad y \not\equiv \pm 2 \pmod 7,$$

whence

$$5 \cdot 1073^2 + 2 \cdot 13 \cdot 79 \cdot 7^2 = 11n$$

and the two representations give $n = 823 \cdot 647$.

6. *Example* 2. $n = 13179643$ (an 8-figure number selected at random, except that it is not divisible by small integers).

Denominator of complete quotient	Term of cont. fraction
1	3630
$2743 = 13 \cdot 211$	2
$13^2 \cdot 3 \cdot 7 = 3549$	1
2906	1
$3 \cdot 17 \cdot 79 = 4029$	1
1303	4
$3 \cdot 11 \cdot 173 = 5709$	1
$2 \cdot 193 = 386$	

Hence we may take $a = 2 \cdot 3 \cdot 7 \cdot 193 = 8106$,

(1) $$x^2 + ay^2 = nk,$$

$k < 2\sqrt{a/3}$ or $k < 104$. Also $(n/3) = (n/7) = (n/193) = 1$ and $(k/3) = (k/7) = (k/193) = 1$. $k \equiv 0$ or $1 \pmod 3$, $k \equiv 0, 1, 2, 4 \pmod 7$; hence, modulo 21, the residues of k are 1, 4, 7, 9, 15, 16, 18, 21, so the values of k may be written

1	4	7	9	15	16	18	21
22	25	28	30	36	37	39	42
43	46	49	51	57	58	60	63
64	67	70	72	78	79	81	84
85	88	91	93	99	100	102.	

Also $k \not\equiv 0, 4, 5, 7, \pmod 8$. Using these conditions together with the methods employed in the last case gives

$$k = 1, 25, 42, 43, 46, 67.$$

Hence the factors of n may be found by using these values of k in (2).

For the same value of n,

$$n = 3630^2 + 13 \cdot 211,$$

we may take $a = 13 \cdot 211$. This gives

$$k = 1, 13, 16, 43, 49, 53, 56.$$

Let $n = 11432767$. Here $n = 3381^2 + 1606$; $1606 = 2 \cdot 11 \cdot 73$ Let us now examine

$$x^2 + 1606\, y^2 = kn.$$

We find $k = 1, 25, 23$ or 38.

Let $n = 236364091$, the numerator of the 12th Bernoulli number; then

$$n = 15374^2 + 4215,$$
$$kn = x^2 + 3 \cdot 5 \cdot 281\, y^2,$$

whence, using previous methods, $k = 1, 16, 31, 39$ or 64.

7. *Case of Periodic Continued Fractions.* In applying the schemes outlined in the second method we may find at the beginning that, after a few operations, we have developed a period of the continued fraction for $\sqrt{n}$. Suppose* that the period has $2r$ terms, say

$$\mu_1, \mu_2, \ldots, \mu_{r-1}, b, \mu_{r-1}, \mu_{r-2}, \ldots, \mu_1, c,$$

then d_r, the denominator of the complete quotient corresponding to b is a divisor of $2n$. Since b is not the last quotient in a period then $(-1)^r d_r \neq 1$, and therefore $(-1)^r d_r = -1, \pm 2$, or some factor of n not unity. Also, if the period has an odd number of terms then $x^2 - ny^2 = -1$ has solutions. It then follows that *either a factor of n has been found, or else n is expressible in one of the forms* $x^2 + y^2$, $x^2 + 2y^2$ *or* $2x^2 - y^2$, x *and* y *each* $< \sqrt{p}$. In cases where the factor is not derived as a divisor of d_r, however, it is more expeditious to expand the square root of some multiple of n as a continued fraction to find suitable values for a.

* Märcker, CRELLE, vol. 20 (1840), pp. 355-59.

8. *Example.* Let us factor $n = 36343817$. A period in the development of $\sqrt{n}$ is 1, 1, 2, 1, 1, 12056, and $d_3 = 4019$, whence $n = 4019 \cdot 9043$.

9. *Third Method of Factorization.* The third method depends on representing the number as an indefinite quadratic form. In a paper already cited I proved that there exists at least one set of positive integers (x, y) such that $ay \equiv \pm x \pmod{m}$ where a is any integer prime to the integer m, x and y each $< \sqrt{m}$. Hence if there exist roots of the quadratic congruence $\mu^2 \equiv a \pmod{n}$ then corresponding to each root μ_1, we have a set (x, y) such that $\mu_1 y \equiv \pm x \pmod{n}$, x and $y < \sqrt{n}$, and we have $ay^2 - x^2 \equiv 0 \pmod{n}$ or $ay^2 - x^2 = kn$ where $0 < k < a$.

10. *Example.* Let us consider $n = 13179643$. The development of $\sqrt{n}$ as a continued fraction (given above) shows that 21 is a quadratic residue of n, and therefore

$$21x^2 - y^2 = kn$$

where $0 < k < 21$, also x and $y < \sqrt{n}$. The continued fraction development gives $(n/7) = 1$, $(n/3) = 1$, hence $(k/7) = -1$, $(k/3) = -1$. Using $(k/3) = -1$ we have as possible values of k

2	3	5	6	8	9
11	12	14	15	17	18

We have $k \not\equiv 1, 2, 4 \pmod{7}$ and $k \not\equiv 0, 2, 6 \pmod{8}$, which leaves 3, 5, 12 and 17 as possible values. Note that $\sqrt{(k+1)n/21} > x > \sqrt{kn/21}$.

Since writing what precedes, I have examined Kraïtchek's *Théorie des Nombres* (Paris, 1922). This book contains tables that are admirably adapted for use in connection with any of the three methods described in this paper. Kraïtchek tabulates the incongruent values of x in $x^2 + Dy^2 \equiv N \pmod{\varrho}$, where ϱ assumes various small values.

CORNELL UNIVERSITY