If p occurs in the set (12), $p-8$ is not in it except for $p=232, 240, 472, 480$. For these four, $p-8\cdot 2^4$ is not in the set (12). This proves Theorem 4.

9. Corresponding results for cubes are obtained in the writer's paper in the American Mathematical Monthly for April, 1927. Assistance has been provided by the Carnegie Institution for the more elaborate investigation of fifth and higher powers.

THE UNIVERSITY OF CHICAGO

TESTS FOR PRIMALITY BY THE CONVERSE OF FERMAT'S THEOREM*

BY D. H. LEHMER

There are, generally speaking, two distinct methods for determining the primality of a large integer without trying possible divisors. Up to this time the method which goes by the name of Lucas' test† has yielded the most results. It is particularly well adapted to the investigation of Mersenne numbers and has consequently led to the identification of the three largest primes heretofore known, namely, $2^{89}-1$, $2^{107}-1$ and $2^{127}-1$. The other method is based on the converse of Fermat's theorem. It is the purpose of this paper to discuss certain improvements in this method, and to apply it to some numbers of the form $10^n \pm 1$.

It has long been known that the simple converse of Fermat's theorem, namely: *If* $a^x \equiv 1 \pmod N$ *for* $x=N-1$, *then* N *is a prime*, is *not* true, as is shown by the simple example: $4^{14} \equiv 1 \pmod{15}$. A true converse of this theorem was first given by Lucas‡ in 1876: *If* $a^x \equiv 1 \pmod N$ *for* $x=N-1$, *but not for* $x<N-1$, *then* N *is a prime.* In 1891 he proved the following theorem.§

---

* Presented to the Society, San Francisco Section, April 2, 1927.

† American Journal, vol. 1 (1878), pp. 184–220.

‡ Lucas, loc. cit., p. 302.

§ *Théorie des Nombres*, 1891, pp. 423, 441.

THEOREM 1. *If* $a^x \equiv 1 \pmod{N}$ *for* $x = N-1$, *but not for* x *a proper divisor of* $N-1$, *then* N *is a prime.*

When applied to a particular N, this theorem exhibits three defects. In the first place, the complete factorization of $N-1$ must be known. Secondly, the number of values of x which must be tried in order to show that the second part of the hypothesis is fulfilled, may be impossibly large. Thirdly, the condition for primality is sufficient but not necessary. If, however, N is of the form 2^n+1, the first two defects vanish; for in this case all the divisors of $N-1$ are powers of 2, so that in testing for the first part of the hypothesis, the second part is automatically taken care of in the successive squarings of the residues modulo N. Unfortunately the only numbers of the form 2^n+1 that have any chance to be primes are the Fermat numbers in which n is a power of 2. The numbers $2^{128}+1$ and $2^{256}+1$ have been tested in this way by Morehead and A. E. Western,* and both numbers were found to be composite. The next such number awaiting investigation is $2^{1024}+1$, a number of 309 digits. A skillful computer could test this number in about ten years. As far as is known to the present author, no prime above the range of ordinary methods of factorization has ever been identified by the converse of Fermat's theorem.† It is clear that Theorem 1 must be improved before further results are possible.

The first defect has to do with the factorization of $N-1$, and is difficult to overcome in case N is a number of unknown form. In many cases it is no easier to factor $N-1$ completely than to factor N. If, however, N is the maximum algebraically prime factor of a number of the form $y^n \pm 1$, it is usually

* This Bulletin, vol. 11 (1905), pp. 543; and vol. 16 (1909), pp. 1–6.

† An attempt to establish the primality of $2^{61}-1$ was made by Seelhoff (Zeitschrift für Mathematik und Physik, vol. 31 (1886), pp. 174–178) using methods depending on the converse of Fermat's theorem. The proof is invalid, as was pointed out by Cole. It depends upon the false proposition that if a divides b and also c, then either b divides c or else c divides b. Despite this obvious error, the proof of the primality of $2^{61}-1$ is invariably attributed to Seelhoff.

possible to decompose $N-1$ into algebraic factors as is shown in the following examples:

$$\frac{y^n \pm 1}{y \pm 1} - 1 = \frac{y}{y \pm 1}(y^{n-1} - 1),$$

$$\frac{y^{4n+2} \pm 1}{y^2 \pm 1} - 1 = \frac{y^2}{y^2 \pm 1}(y^{4n} - 1),$$

$$\frac{y^{4n} \pm 1}{y^4 \pm 1} - 1 = \frac{y^4}{y^4 \pm 1}(y^{4n-4} - 1),$$

$$\frac{y^{8n} \pm 1}{y^8 \pm 1} - 1 = \frac{y^8}{y^8 \pm 1}(y^{8n-8} - 1),$$

$$\frac{y^{n^2} \pm 1}{y^n \pm 1} - 1 = \frac{y^n}{y^n \pm 1}(y^{n^2-n} - 1),$$

. . . . . .

The large factors on the right are differences of squares. Thus the factors of $N-1$ are made to depend upon factorizations of $y^n \pm 1$ for much smaller values of n. These may be taken from tables* previously computed. In case $N-1$ cannot be expressed in some such form as the above, one can always be assured of having n as a factor of $N-1$. If a small factor of N is known (as it often is from congruence tables) and if N' is the residuary factor, the factorization of $N'-1$ is again very difficult. In this case, however, we have n as a factor, but it is of little use except in reducing the size of the number to be factored. We shall see later that it is not necessary to know the complete factorization of $N-1$.

The next improvement in Theorem 1 that suggests itself is the reduction of the number of values of x to be tried. In the following theorem this number is reduced from the number of divisors of $N-1$ to the number of its prime factors.

---

* Cunningham and Woodall, *Factorization of* $y^n \pm 1$, London, 1925.

THEOREM 2. *If* $a^x \equiv 1 \pmod{N}$ *for* $x = N-1$, *but not for* x *a quotient of* $N-1$ *on division by any of its prime factors, then* N *is a prime.*

Let

$$N - 1 = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_t^{\alpha_t} = m_i p_i, \qquad (i = 1,2,3, \cdots, t).$$

Then we have for an hypothesis:

$$a^{N-1} \equiv 1 \pmod{N} \tag{1}$$

$$a^{m_i} \not\equiv 1 \pmod{N}, \qquad (i = 1,2,3, \cdots, t). \tag{2}$$

Now let ϵ be the smallest value of x satisfying $a^x \equiv 1 \pmod{N}$. Then ϵ divides $N-1$. For, if not, let $N-1 = n\epsilon + \delta$. Then since

$$a^{N-1} = a^{n\epsilon+\delta} \equiv 1 \pmod{N},$$

it follows that $a^\delta \equiv 1 \pmod{N}$, which is impossible, since $\delta < \epsilon$. But ϵ does not divide m_i, for if it did, we would have $a^{m_i} \equiv 1 \pmod{N}$. Now let us write

$$\epsilon = n p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t},$$

where β_i may be zero and n is free of p_i. Consider the quotient

$$\frac{N-1}{\epsilon} = \frac{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}}{n p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t}}.$$

Since $N-1$ is divisible by ϵ, we see that $n = 1$, and further,

$$\beta_1 \leqq \alpha_1, \ \beta_2 \leqq \alpha_2, \ \cdots, \ \beta_t \leqq \alpha_t.$$

Now the quotient

$$\frac{m_1}{\epsilon} = \frac{p_1^{\alpha_1 - 1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}}{p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t}}$$

is not an integer, but it is identical with the preceding quotient except for the p_1's, so that we can write $\beta_1 > \alpha_1 - 1$, and in general $\beta_i > \alpha_i - 1$. But we have seen that $\beta_i \leqq \alpha_i$. Hence $\beta_i = \alpha_i$ and $\epsilon = N-1$. Finally let $\phi(N)$ be the totient of N. Then $a^{\phi(N)} \equiv 1 \pmod{N}$. Now if N were composite,

we would have $\phi(N) < N-1$. But this is impossible since $N-1=\epsilon$, and this is the smallest value of x satisfying $a^x \equiv 1 \pmod{N}$. Hence N is a prime.

Although this theorem is an improvement on Theorem 1, it still has the third defect of that theorem; that is, it tells us nothing of the character of a number N which satisfies the first part of the hypothesis but not the second. We have this situation, for example, whenever a is a quadratic residue of the prime N. It is clear that this defect cannot be eliminated by any theorem having the general form of Theorems 1 and 2. With this in mind we change our point of attack, and, by introducing a new element in the hypothesis, arrive at the following theorem.

THEOREM 3. *If* $a^x \equiv 1 \pmod{N}$ *for* $x = N-1$ *and if* $a^x \equiv r > 1$ *for* $x = (N-1)/p$, *and if* $r-1$ *is prime to* N, *then all the prime factors of* N *are of the form* $np^\alpha + 1$, *where* α *is the highest power to which the prime* p *occurs as a divisor of* $N-1$.

Let $N-1 = qp^\alpha = mp$. Then we have for an hypothesis:

$$a^{N-1} \equiv 1 \pmod{N}, \tag{1}$$

$$a^m \equiv r \pmod{N}, \tag{2}$$

$$r - 1 \text{ is prime to } N. \tag{3}$$

Now let κ be any prime factor of N and let ξ be the smallest value of x such that $a^x \equiv 1 \pmod{\kappa}$. Then since $a^{N-1} \equiv 1 \pmod{\kappa}$, we can show as in the preceding theorem that ξ divides $N-1$. Also by Fermat's theorem $a^{\kappa-1} \equiv 1 \pmod{\kappa}$. Hence ξ divides $\kappa - 1$. But ξ does not divide m, for if it did we would have $a^m \equiv 1 \pmod{\kappa}$, which would imply that $r-1$ is divisible by κ. But $r-1$ is prime to N, and hence is prime to κ. Let us write $\xi = n_1 p^\beta$, where n_1 is prime to p, and β may be zero. Consider the quotient

$$\frac{N-1}{\xi} = \frac{qp^\alpha}{n_1 p^\beta}.$$

Since q is also prime to p, we have $\beta \leqq \alpha$. Now the quotient

$$\frac{m}{\xi} = \frac{qp^{\alpha-1}}{n_1 p^{\beta}}$$

is not an integer, since m is not divisible by ξ. Hence $\beta > \alpha - 1$. That is, $\beta = \alpha$ and $\xi = n_1 p^{\alpha}$. But since ξ divides $\kappa - 1$, we have $\kappa - 1 = n_2 \xi = n_1 n_2 p^{\alpha}$. Hence $\kappa = np^{\alpha} + 1$.

This theorem is the basis of a method given by Pocklington,* the importance of which seems to have escaped attention. In order to remove the final defect of Theorem 1, we must discuss the cases in which the various parts of the hypothesis are not fulfilled. If $a^{N-1} \not\equiv 1 \pmod{N}$, then N is composite, and its factors are not obtainable by this method. If $a^m \equiv 1 \pmod{N}$, all the factors of N divide the number $a^m - 1$, whose primitive factors are of the form $2nm+1$. It is usually too troublesome, however, to try to show that N is a primitive factor. In practice, it is better to take m/p_2 or m/p_1^2 for a new value of m. If then $a^m \not\equiv 1$, all the factors of N are of the form $np_2^{\alpha_2}+1$ or $np_1^{\alpha_1-1}+1$, respectively. If $p_1 = 2$, this last case may be investigated without further calculation. However, this failure of the second part of the hypothesis is very rare, especially when care is taken in choosing the base a. Finally, if $r-1$ is not prime to N, their G.C.D. will be a factor of N.

Suppose that we have applied Theorem 3 to a particular N and we find that $\kappa = np_1^{\alpha_2} + 1$. Then N is a prime if $p^{\alpha_1} > N^{1/2}$. If on the other hand $p_1^{\alpha_1}$ is too small, other factors of $N-1$ may be dealt with in the same manner, so that we obtain $\kappa = np_1^{\alpha_1} p_2^{\alpha_2} \cdots + 1$, a form sufficiently exclusive to meet our needs. Suppose we have found in this way that $\kappa = nP + 1$, where P is the product of certain odd prime factors of $N-1$. Our first inclination is to let n take on successive integral values, beginning with unity, and then try as divisors of N the prime values of κ. If $N^{1/2} > 10^7$ however, κ will run above the present limit of the list of primes, and we must

* Proceedings of the Cambridge Philosophical Society, vol. 18 (1914–16), p. 29.

try composite values of κ as well. Of course, about 5/6 of these are easily seen to be multiples of small primes; as for the others, it is easier actually to try them as divisors. All this may entail considerable labor, which may, for the most part, be obviated by seeking to express N as the difference of two squares. If every factor of $N=a^2-b^2$ is of the form $nP+1$, where P is odd, it follows that*

$$a^2 \equiv N \pmod{P^2}, \tag{1}$$

$$a \equiv 1 \pmod{P}. \tag{2}$$

One of the two values of a involved in (1) is eliminated by (2) so that a is restricted to one case in P^2. In fact, if

$$N \equiv 1 + kP \pmod{P^2},$$

then

$$a \equiv 1 + \frac{k}{2} P \pmod{P^2},$$

where, if k is odd, $k/2$ is taken modulo P. If the factors of N are, at the same time, of the form $n2^\lambda+1$, a similar restriction may be set up modulo $2^{2\lambda-1}$, which may be useful when λ is large. Suppose it is known that no factor of N is less than some limit W. Then a has the following range of values:

$$N^{1/2} < a < \frac{1}{2}\left(W + \frac{N}{W}\right).$$

In our case W is at least as large as $2P$, so that we have

$$N^{1/2} < a < \left(P + \frac{N}{4P}\right).$$

Although a has a greater range than κ, the possible values of a are more restricted especially when P is large. When P is small, so that there are a great number of values of either a or κ to be tried, use can be made of the "movable strip" method† of combining linear forms, which again favors the

* Lawerence, Quarterly Journal, vol. 28 (1896), pp. 285–311. Kraitchik, *Théorie des Nombres*, Paris, 1922, p. 146.

† Kraitchik, loc. cit., Chapter 2; also see Lawerence, loc. cit.

search for a. It is sometimes advantageous to use both methods. The direct method may be used to increase the limit W, thus decreasing the range for a, so that the work may be easily finished by the difference of squares.

Of the numbers $y^n \pm 1$, those for which $y=2$ have been most extensively investigated. Perhaps $y=10$ comes second in importance. If the results with 10^n-1 are comparatively few, it is not to be attributed to lack of interest, but rather to the lack of adequate methods with which to deal with these larger numbers. The preceding theory is most easily applied to divisors of $10^n \pm 1$, because of the ease with which the calculations may be performed.

Instead of employing the modulus N in our work, we may use any multiple of N; and, having found the residue of a^{N-1} modulo kN, we have only to divide the result by N to obtain the desired result. If N is a divisor of $10^n \pm 1$, we may choose k such that $10^n \pm 1 = kN$. The advantage in using the modulus $10^n \pm 1$ is that the division by this modulus may be performed by a single subtraction or addition. To cast 10^n+1 out of a number of $2n$ digits, we separate it into periods of n digits each, beginning at the right, and subtract the second period from the first. For 10^n-1, we simply add the two periods. An added advantage in using a composite modulus is that it provides an easy method of checking the work. We may select some small divisor of k, such as δ, and then construct an auxiliary table of $a^x \pmod{\delta}$, containing at most $\phi(\delta)$ entries. This table enables us to predict what any particular residue of $a^x \pmod{kN}$ should be congruent to $\pmod{\delta}$, by finding what x is congruent to $\pmod{\phi(\delta)}$. The calculation of the residue of a^{N-1} may be most easily performed as follows. We first make a table of exponents beginning with $n-1$, in which each entry is obtained by writing in the greatest integer in half the entry just above. This table has roughly $3 \log_{10} N$ entries, the final one being unity. Starting now at the bottom, we make a table of powers of a, each line being obtained by taking the square of the preceding entry, modulo $10^n \pm 1$, and multiplying this result

by a, whenever the desired entry corresponds to an odd exponent. On arriving at the top of the table, we cast N out of the final result and obtain $a^{N-1} \pmod N$. Of course the same procedure applies to the calculation of the residue of a^m.

Below are the results of applying Theorem 3 to seven divisors of $10^n \pm 1$ for $n = 19$, 20, 23, 24, 27, and 31. Besides the check already mentioned, every step in the following work has been verified by casting out multiples of 1001. It is confidently believed that, in those cases where $a^{N-1} \not\equiv 1$, this result is not due to a slip in the computation. However, the actual residues are given in hopes that they may prove useful to future workers who may wish to verify the results obtained.

1. *Example* 1. $N = 440,334,654,777,631$.

This number is the residuary factor of $10^{27}-1$. In fact

$$10^{27}-1 = 3^5 \cdot 37 \cdot 757 \cdot 333667 \cdot N.$$

The discovery of the factors 3 and 757 by congruence tables makes the factorization of $N-1$ a rather serious problem. At first sight we have

$$N-1 = 2 \cdot 3^3 \cdot 5 \cdot 1,630,869,091,769.$$

The first two factors are of no use, since we know in advance that every factor of N is of the form $54n+1$. After examining the large factor for divisors less than 1000 without result, 5 was chosen as p^α; it was found that

$$3^{(N-1)/5} = 3^m \equiv 31343325933897 = r \pmod N,$$

and further that

$$r^5 \equiv 3^{N-1} \equiv 1 \pmod N,$$

$r-1$ being prime to N. Every factor of N is then of the form $5n+1$. It was next decided to undertake the arduous though not impossible task of seeking to represent N as the difference of two squares, taking for W the limit 120,000 set by congruence tables. Before actually starting the work, however, a further attempt to factor the number 1,630,869,091,769

was made by means of the "factor stencils" of D. N. Lehmer,* which, though still incomplete, are fortunately available to the present author. Although this number of unknown form is nearly 1000 times larger than the intended limit of the stencils, it was found without great difficulty that

$$1,630,869,091,769 = 31249 \cdot 52,189,481.$$

Choosing 52189481 as a new value of p^α, it was easily found that

$$3^m \equiv 78533825886276 = r \pmod{N},$$

$r-1$ being prime to N. The factors of N are then of the form $52189481n+1$. But $N^{1/2}$ is less than 20984153. Hence N is a prime and we have the complete factorization

$$10^{27} - 1 = 3^5 \cdot 37 \cdot 757 \cdot 333667 \cdot 440334654777631.$$

2. *Example* 2. $N = 9,999,000,099,990,001.$

This number is $(10^{20}+1)/(10^4+1.)$ It was found that

$$3^{N-1} \equiv 3703264653988674 \pmod{N}.$$

Hence N is composite. This number has been examined for factors less than its cube root without success. It is therefore the product of two primes.

3. *Example* 3. $N = 9,999,999,900,000,001.$

This number is $(10^{24}+1)/(10^8+1)$. In this case we have

$$N - 1 = \frac{10^{24}+1}{10^8+1} - 1 = \frac{10^8}{10^8+1}(10^{16} - 1)$$
$$= 2^8 \cdot 5^8 \cdot 3^2 \cdot 11 \cdot 73 \cdot 101 \cdot 137.$$

The divisors 2^8 and 5^8 were chosen as values of p^α and tested in one operation as follows. It was first found that

$$7^{(N-1)/10} \equiv 7128121476353673 = r \pmod{N}.$$

Then

$$r^2 \equiv 7^{(N-1)/5} \equiv 428233546143224 \pmod{N},$$

* Proceedings of the National Academy, vol. 11 (1925), p. 97.

and finally

$$r^5 \equiv -1 \quad \text{and} \quad r^{10} \equiv 1 \pmod{N}.$$

Since r^2-1 is prime to N, it follows that every factor of N is of the form 5^8n+1 and also of the form 2^8n+1. But $N^{1/2}<10^8$, so that N is a prime and we have the complete factorization:

$$10^{24}+1 = 17 \cdot 5882353 \cdot 9999999900000001.$$

4. *Example* 4. $N = 909,090,909,090,909,091.$

This number is $(10^{19}+1)/11$. It was found that

$$3^{N-1} \equiv 1 \pmod{N}.$$

Now we have

$$N-1 = \frac{10^{19}+1}{10+1} - 1 = \frac{10}{11}(10^{18}-1)$$
$$= 2 \cdot 3^4 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \cdot 52579 \cdot 333667.$$

Choosing as p the number 333667, we obtain

$$3^m \equiv 314776999832050172 = r \pmod{N},$$

$r-1$ being prime to N. Every factor of N is then of the form $333667n+1$, and also $19n+1$; or, in other words, $6339673n+1$. Using this restriction, we might test directly for the factors of N with n ranging from 1 to 150. About 125 of these values of κ might be ruled out as being multiples of small primes. The remaining 25 would have to be tested. Instead, let us write $N=a^2-b^2$. Then since

$$N \equiv 1 + 56743 \cdot 6339673 \pmod{(6339673)^2},$$

it follows that

$$a \equiv 1+3202708 \cdot 6339673 \pmod{(6339673)^2},$$

or

$$a = 4019453746929n + 20304121434485. \tag{1}$$

Taking $2P$ or 12679346 as a value of W, we find that a has the following range:

$$933462589 < a < 35855622005. \tag{2}$$

The smallest value of a allowed by (1) is more than 500 times larger than the largest value allowed by (2). Hence a does not exist and N is a prime. We then have the complete factorization

$$10^{19} + 1 = 11 \cdot 909090909090909091.$$

5. *Example* 5. $N = 999,999,999,000,000,001.$

This number is $(10^{27}-1)/(10^9-1)$. In this case it was found that

$$3^{N-1} \equiv 437299180785434949 \pmod{N};$$

N is therefore composite. This number and the third one examined above fill in two entries in the following rather curious table:

91	Composite
9901	Prime
999001	Composite
99990001	Prime
9999900001	Composite
999999000001	Prime
99999990000001	Composite
9999999900000001	Prime
999999999000000001	Composite

Unfortunately, the next entry in this table is composite.

6. *Example* 6. $N = 11,111,111,111,111,111,111,111.$

This number is $(10^{23}-1)/9$. It was found that

$$3^{N-1} \equiv 1268486354649455149380 \pmod{N}.$$

Hence we know that N is composite. This number is listed as a prime in a table of divisors of $10^n \pm 1$ given by Loof.* In a French edition† of this table is given the curious entry: $11111 \cdot 11111$? Bickmore‡ marks this number as a prime

* Archiv der Mathematik und Physik, vol. 16 (1851), pp. 54–57.

† Nouvelles Annales, vol. 14 (1855), pp. 115–117. Compare Messenger of Mathematics, vol. 33 (1903–04), p. 96.

‡ Nouvelles Annales, (3), vol. 15 (1896), p. 222.

on the authority of Loof. The character of $(10^{23}-1)/9$ as revealed for the first time by the above result will be settled once and for all only when the factors are discovered. The numbers made up entirely of the digit 1 are of interest on account of the rarity of primes among them. Only those numbers that have a prime number of digits have any chance to be primes, and this set may be said to correspond to the Mersenne numbers. Besides the obvious cases 1 and 11, this former set contains but one other prime less than the limit $(10^{37}-1)/9$. This prime is $(10^{19}-1)/9$ and was examined independently by Hoppe and Kraitchik by the difference of two squares. By way of comparison with the Mersenne numbers, it is found that there are no less than 9 primes less than $2^{37}-1$. The numbers $10^{2^n}+1$, which correspond to the Fermat numbers, also show a scarcity of primes. The only primes that have been found in this set are 11 and 101, up to the limit $10^{64}+1$.

7. *Example* 7. $N = 909,090,909,090,909,090,909,090,909,091.$

This number is $(10^{31}+1)/11$. In this case it was found that

$$3^{N-1} \equiv 1 \pmod{N}.$$

Now we have

$$N - 1 = \frac{10^{31}+1}{10+1} - 1 = \frac{10}{11}(10^{30}-1)$$

$$= 2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 31 \cdot 37 \cdot 41 \cdot 211 \cdot 241 \cdot 271 \cdot 2161 \cdot 9091 \cdot 2906161.$$

Here $N-1$ breaks up into so many small factors that no single one used for p gives sufficient restriction. Selecting $p_1 = 2906161$ and $p_2 = 9091$, it was found that

$$3^{m_1} \equiv 40421597451230127 5864167721473 = r_1 \pmod{N},$$

and

$$3^{m_2} \equiv 55433011245022437 2250010348117 = r_2 \pmod{N},$$

r_1-1 and r_2-1 being prime to N. Hence the factors of N belong to the forms

$$\left.\begin{matrix} 31n+1 \\ 9091n+1 \\ 2906161n+1 \end{matrix}\right\} \text{ or } 819017199181n+1.$$

Now $N^{1/2}=953462589245592$. To test directly for the factors of N would require 1164 values of n. Instead, we find that

$$N \equiv 1 + 645945952735 \cdot 819017199181 \pmod{(819017199181)^2},$$

so that

$$a \equiv 1 + 732481575958 \cdot 819017199181 \pmod{(819017199181)^2}$$

or

$$(1) \qquad a = 670789172554289827070761n + 599915008792806066890399.$$

To find the range for a, we let $W=2P=1638034398362$ and obtain

$$(2) \qquad 953462589245592 < a < 554988900110999445.$$

We see that the smallest value of a in (1) is more than a million times larger than the largest value in (2). Hence a does not exist and N is a prime. We then have the complete factorization

$$10^{31}+1 = 11 \cdot 909090909090909090909090909091.$$

The author's acknowledgements are due to Miss E. M. Trotskaia for help in carrying out the above calculations.

THE UNIVERSITY OF CALIFORNIA