The proof is immediate, for by the Hamilton-Cayley theorem

$$\delta(R(x)) = 0, \qquad \delta'(S(x)) = 0.$$

Since $\mathfrak{A}$ is isomorphic with the algebra of matrices $R(x)$ (or $S(x)$), we have $\delta(x)=0$ (or $\delta'(x)=0$).

For the example of §4 we have

$$\delta(\omega) = \omega^2 - \omega x_1, \qquad \delta'(\omega) = \omega^2 - 2\omega x_1 + x_1^2 .$$

Hence $\delta(x)=0$, while $\delta'(x)=x_1^2-x_1^2e_1-x_1x_2e_2$.

Ohio State University

ON THE NUMBER $(10^{23}-1)/9$

D. H. LEHMER

The purpose of this note is to save any further effort* in trying to factor the number $N=(10^{23}-1)/9=111, 11111, 11111, 11111, 11111$ which in a previous paper was found to be composite.† This assertion was based on a negative result giving $3^{N-1}\not\equiv 1 \pmod N$.

On the basis of this conclusion Kraitchik‡ attempted to factor N arriving at another negative result that N had no factors and therefore was a prime. This conflict of results led us to recompute the value of $3^{N-1} \pmod N$ which shows clearly a mistake in the original calculation arising from the choice of 3 for a base instead of another number prime to $10^{23}-1$. Such another base would have furnished the extra check which would have detected the error.

---

* A recent letter from Mr. R. E. Powers informs us that he has been to the trouble of finding 150 quadratic residues of N.

† This Bulletin, vol. 33 (1927), p. 338.

‡ Mathesis, vol. 42 (1928), p. 386.

The recomputation revealed the following results:

$$3^{N-1} \equiv 1 \pmod{N},$$
$$3^{(N-1)/11} \equiv 14\ 45009\ 64787\ 71867\ 25049 = r_1 \pmod{N},$$
$$3^{(N-1)/4093} \equiv 98\ 37816\ 77563\ 73768\ 37434 = r_2 \pmod{N},$$
$$((r_1 - 1), N) = ((r_2 - 1), N) = 1.$$

By Theorem 3 of my paper cited above, it follows that the factors of N belong to the forms

$$\left.\begin{matrix} 23n + 1 \\ 121n + 1 \\ 4093n + 1 \end{matrix}\right\} 11390819n + 1.$$

If we seek to express N as the difference of squares $(a^2 - b^2)$, we have

$$a = 129750757490761n + 115222895547343.$$

If we restrict a modulo 12 and 25, the smallest admissible value to try is

$$a = 5435003952668544.$$

The total range for a is given by the inequalities

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

where $W = 22781638$, that is,

$$a < 243861122499491.$$

The maximum value of a is less than the smallest possible value; therefore a does not exist and N is a prime.

The results of Kraitchik's investigations will occupy a whole chapter of his forthcoming book.* Those interested in the factorization of large numbers will await with interest the exposition of the method by which Kraitchik was able to identify this sixth largest prime known.

Brown University

* *Recherches sur la Théorie des Nombres*, vol. 2.