SOME NEW FACTORIZATIONS OF $2^n \pm 1$

BY D. H. LEHMER

1. *Introduction.* The purpose of this note is to announce five new factorizations of $2^n \pm 1$. The results are due directly and indirectly to the writer's new number theoretic machine.* In fact the large primes quoted below would have remained undiscovered by the writer had he not been in possession of the means of factoring numbers of this size without difficulty. The actual factorizations quoted below are the result of a month's experiment with the machine. As a matter of fact the machine ran only a few hours altogether. When some permanent location has been found for the apparatus, it is hoped to consider much more difficult problems.

2. *Theorem for Large Primes.* We begin with the large primes. These primes were identified with the help of the following theorem.†

THEOREM A. *If the integer N divides $\alpha^{N-1}-1$, but is prime to $\alpha^{(N-1)/p}-1$, p a prime, then all the factors of N are of the form $px+1$.*

If a large enough prime factor p of $N-1$ is known, this theorem so restricts the factors of N, that the primality of N follows almost at once.

3. *Factorization of* $2^{73}+1$. The number N in this case is

$$N = \frac{2^{73}+1}{3 \cdot 1753} = 1795\ 91803\ 87410\ 70627.$$

It was found that $N-1$ is divisible by $p=811$, and that the hypothesis of Theorem A is satisfied for $\alpha=3$. Hence every factor of N is of the form $811x+1$, as well as $73x+1$ and $8x+1$, 3. Writing $N=a^2-b^2$, we deduce at once

$$a = 28039961672k + 244363342366.$$

* This Bulletin, vol. 38 (1932), p. 635.

† This theorem is a special case of Theorem 3, of the writer's article published in this Bulletin, vol. 33 (1932), p. 331.

Since the smallest factor of N is known to exceed 300000, we find

$$a \leqq 2993196881235,$$

so that $k \leqq 107$. These few values of k are easily disposed of using small moduli $\leqq 19$. Hence N is a prime and we have

$$2^{73} + 1 = 3 \cdot 1753 \cdot 1795\ 91803\ 87410\ 70627.$$

4. *Factorization of* $2^{85}-1$. The number N under consideration here is

$$N = \frac{2^{85} - 1}{(2^{17} - 1)(2^5 - 1)} = 9520\ 97280\ 63337\ 58431.$$

Here $N-1$ is divisible* by $p=257$. The hypothesis of Theorem A is shown to be satisfied with $\alpha=3$, and the primality of N follows easily as before. Hence

$$2^{85} - 1 = 31 \cdot 131071 \cdot 9520\ 97280\ 63337\ 58431.$$

5. *Factorization of* $2^{95}+1$. The number N in this case is

$$N = \frac{(2^{95} + 1)(2 + 1)}{(2^{19} + 1)(2^5 + 1)(2281)} = 3011\ 34747\ 96142\ 49131.$$

It was found that N divides $3^{N-1}-1$, but no large prime factor of $N-1$ was immediately available. In fact

$$N - 1 = 2 \cdot 3 \cdot 5 \cdot 19 \cdot 5\ 28306\ 57537\ 09209.$$

It thus became necessary to examine the large factor M of $N-1$. By expanding $M^{1/2}$ in a regular continued fraction it was found that -7 is a quadratic residue of M. Hence if M is composite we may expect at least two representations of M by the form x^2+7y^2. The machine gave them in less than half an hour as follows:

$$N = 40923451^2 + 7 \cdot 22704112^2 = 66855539^2 + 7 \cdot 10779628^2.$$

This gives us the decomposition

$$M = 59957 \cdot 88114244437.$$

This last factor we proved to be a prime by applying Theorem

* One may easily show in general that any prime factor of $a^{p-1}-1$ not dividing a^q-1, divides $[(a^{pq}-1)(a-1)]/[(a^p-1)(a^q-1)]-1$.

A using the factor $p=2489947$ of 88114244436. Armed with this large factor of $N-1$, the application of Theorem A to N was soon completed, and it resulted that N is a prime. Hence

$$2^{95}+1 = 3\cdot 11\cdot 2281\cdot 174763\cdot 3011\ 34747\ 96142\ 49131.$$

This proof for primality is a positive proof, although it may seem round about. The machine could have been easily set to search directly for the factors of N, but its failure to find a factor might not have been acceptable to the reader as a proof of primality.

6. *Factorization of* $2^{93}+1$. The number under discussion here is

$$N = \frac{(2^{93}+1)(2+1)}{(2^{31}+1)(2^3+1)} = 1537\ 22867\ 20933\ 01419.$$

Since each factor of N is of the form $93x+1$ and $8x+1$, 3 we find easily that if $N=a^2-b^2$, then a is of the form $69192k+1239854518$. The smallest factor of N exceeds 300000 so that

$$a \leqq 2562047936822, \text{ or } k \leqq 37010176.$$

The machine was set to exclude values of k. It ran only a few seconds, and delivered the value $k=6886$. This gives us

$$a = 1716310630, \text{ and } b = 1186799691.$$

Hence

$$N = 529510939\cdot 2903110321.$$

It is easily seen that both factors are primes, hence

$$2^{93}+1 = 3^2\cdot 529510939\cdot 715827883\cdot 2903110321.$$

7. *Factorization of* $2^{79}-1$. We are concerned in this case with

$$N = (2^{79}-1)/2687 = 2\ 24958\ 286426\ 02584\ 99201.$$

Since the factors of N are of the forms $79x+1$, $8x\pm 1$, it follows that if $N=a^2-b^2$, a will have the forms

$$a = 6241x+159,\ 3x+0,\ 512x\pm 63,\ 97,\ 159,\ 191.$$

Combining these forms we get

$$a = 9586176k+159,\ 1610337,\ 4793247,\ 6403425,$$
$$6590655,\ 7002561,\ 8987199,\ 9399105.$$

Since $a \leqq 374930473917097$, we have in each case $k \leqq 39111579$. Thus the problem of representing N as the difference of squares was split into 8 parts. The first two parts were covered by the machine without any result. On the third run, however, the machine stopped almost at once at $x = 58088$. This gives

$$a = 556846584735, \quad b = 556644555032.$$

Hence we have the factorization

$$2^{79} - 1 = 2687 \cdot 202029703 \cdot 1113491139767.$$

It is not difficult to show that the factors are primes. This is the 13th composite Mersenne number to be completely factored. The author's recent report* on Mersenne numbers should be changed accordingly.

PASADENA, CALIFORNIA

MATRICES WHOSE sTH COMPOUNDS ARE EQUAL

BY JOHN WILLIAMSON

If A is a matrix of m rows and n columns and s is any positive integer less than or equal to the smaller of n and m, from A can be formed a new matrix A_s of ${}_mC_s$ rows and ${}_nC_s$ columns, the elements in the tth row of A_s being the ${}_nC_s$ determinants of order s that can be formed from the t_1th, $\cdots$, t_sth rows of A, and the elements in the tth column being the ${}_mC_s$ determinants of order s that can be formed from the t_1th, $\cdots$, t_sth columns of A. The matrix A_s, so defined, is called the sth compound matrix of A. In the following note we discuss the necessary and sufficient conditions under which the sth compounds of two matrices are equal. We shall require the following lemmas.

LEMMA I. *The rank of the sth compound of a matrix A, whose rank is r, is ${}_rC_s$ if $r \geqq s$ and is zero if $s > r$.*†

---

* This Bulletin, vol. 38 (1932), p. 384. Dr. N. G. W. H. Beeger has kindly called my attention to the fact that $2^{233}-1$ has two known prime factors and should be classified accordingly.

† Cullis, *Matrices and Determinoids*, vol. 1, p. 289.