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.