TESTS FOR PRIMALITY

By B. W. Brewer

1. **Introduction.** Practical tests for the primality of certain integers of the form $A2^n - 1$ have been given. There is the well-known theorem, due in substance to Lucas [4] and based on the series 4, 14, 194, $\cdots$, giving a necessary and sufficient condition for the primality of the Mersenne numbers $2^n - 1$ (n an odd prime). Though Lucas never published a complete proof of this theorem, proofs have been given by D. H. Lehmer [2, 3], Western [5], and Kaplansky [1]. Lehmer obtained his first proof as a by-product of an extended theory of Lucas functions and indicated other series that might be used to test the Mersenne numbers for primality. His second proof is based on quite elementary properties of the Lucas functions and is self-contained. Kaplansky defined a function related to those of Lucas and proved a theorem which includes Lucas' theorem as a special case. His theorem indicates other series that might be used to test the Mersenne numbers for primality, and his proof is modeled on Lehmer's second proof. Western's proof is based on the theory of algebraic numbers. Lehmer also applied his extended theory of Lucas functions to obtain necessary and sufficient conditions for the primality of integers of the form $A2^n - 1$ (A odd, $A < 2^n$).

It is the purpose of this paper to develop primality tests for certain integers of the form $A2^n - 1$, basing the development on the theory of Galois fields. We obtain a proof of Lucas' test for the primality of $2^n - 1$, and develop a test for $A2^n - 1$ (A odd, $A < 2^{n+1}$) similar to those given by Lehmer. In addition, we obtain tests for $2p - 1$ (Lucas), $4p - 1$, $8p - 1$, $2p^2 - 1$, $8p^2 - 1$, and $p^2 \pm p - 1$ for certain odd primes p. All of these tests state divisibility conditions on certain Lucas functions.

2. **Tests for primality.** Let P and Q be coprime integers and α, β be the roots of the quadratic $x^2 - Px + Q$ over the rational number field. Then the Lucas functions are defined by

$$U_n = (\alpha^n - \beta^n)/(\alpha - \beta), \qquad V_n = \alpha^n + \beta^n,$$

where n is a positive integer. It follows from the definitions that U_n and V_n are integers for every n, and

$$U_{n+2} = PU_{n+1} - QU_n, \qquad V_{n+2} = PV_{n+1} - QV_n, \tag{1}$$

$$U_{2n} = U_nV_n, \qquad V_{2n} = V_n^2 - 2Q^n. \tag{2}$$

Received May 23, 1951.