# A Report on Prime Numbers of the Forms $M = (6a + 1)2^{2m-1} - 1$ and $M' = (6a - 1)2^{2m} - 1$

By H. C. Williams and C. R. Zarnke

**1. Introduction.** In 1956 Riesel [1] published a table of all primes of the form $M = (6a + 1)2^n - 1$ and $M' = (6a - 1)2^n - 1$ for $a \leqq 9$ and $1 \leqq n \leqq 150$ (in the cases $6a \pm 1 = 5, 7$, or 11 the range is $1 \leqq n \leqq 250$). The purpose of this paper is to extend that table for values of $a \leqq 25$ and $1 \leqq n \leqq 1000$.

**2. Method.** These numbers were tested for primality by using a theorem due to Lehmer [2]. We state this theorem in a slightly more general form here. *Let $N = A2^n - 1 \neq 3N'$, where $n > 2$, $(A, 6) = 1$, and $A < 2^n$; also let $R = 3 \cdot 2^{k+1}y^2$, where $k = 0$ or 1 and $y$ is a solution of the Diophantine equation*

$$3 \cdot 2^k y^2 - 2 = t^2 .$$

*Then a necessary and sufficient condition for $N$ to be prime is that $N$ divides the $(n - 1)$th term of the series*

$$S_1, S_2, S_3, \cdots S_i, \cdots \text{ where } S_i = S_{i-1}^2 - 2, \; S_1 = V_{2A}(R, 1) .$$

*Here*

$$V_{2A}(R, 1) = r_1^{2A} + r_2^{2A} ,$$

*where $r_1$ and $r_2$ are the roots of*

$$x^2 - \sqrt{R}\, x + 1 = 0 .$$

A programme which first eliminated, by a preliminary sieving process, values of $M$ and $M'$ with small prime divisors and then applied the above theorem, as a test for primality, on the remaining numbers was written for an IBM 7040 computer. The calculations performed by this routine were verified by running the programme twice; on the first run, the parameter $R$ was set equal to 6; on the second run, $R$ was set equal to 12. The results of each of these two runs were identical and are presented in Table 1. (The primality of the values of $M$ and $M'$, where $6a + 1 > 2^n$, was determined from tables.)

**3. Remarks.** It is interesting to note that if we define a sequence of numbers $\{G_n\}$, where

$$G_n = F_n 2^{F_n - 1} - 1 , \qquad \text{and} \qquad F_n = 2^{2^n} + 1 ,$$

we see that $G_0$, $G_1$, $G_2$ are each prime. It was also verified by the authors that $G_3$ is a prime; $G_3$ is a prime of exactly 80 digits; cf. Sierpiński [3]. This suggests that perhaps $G_4$ might be a prime; however, with our present facilities, the great length of time required to determine the primality of a number the size of $G_4$ is prohibitive.

Received February 3, 1967.

TABLE 1. *List of Primes of the Form* $(6a \pm 1)2^n - 1$

| $6a \pm 1$ | $n$ ($\leqq 1000$) |
|---|---|
| 5 | 2,4,8,10,12,14,18,32,48,54,72,148,184,248,270,274,420 |
| 7 | 1,5,9,17,21,29,45,177 |
| 11 | 2,26,50,54,126,134,246,354,362,950 |
| 13 | 3,7,23,287,291,795 |
| 17 | 2,4,6,16,20,36,54,60,96,124,150,252,356,460,612,654,664,698,702,972 |
| 19 | 1,3,5,21,41,49,89,133,141,165,189,293,305,395,651,665,771,801,923,953 |
| 23 | 4,6,12,46,72,244,264,544,888 |
| 25 | 3,9,11,17,23,35,39,75,105,107,155,215,335,635,651,687 |
| 29 | 4,16,76,148,184 |
| 31 | 1,5,7,11,13,23,33,35,37,47,115,205,235,271,409,739,837,887 |
| 35 | 2,6,10,20,44,114,146,156,174,260,306,380,654,686,702,814,906 |
| 37 | 1 |
| 41 | 2,10,14,18,50,114,122,294,362,554,582,638,758 |
| 43 | 7,31,67,251,767 |
| 47 | 4,14,70,78 |
| 49 | 1,5,7,9,13,15,29,33,39,55,81,95,205,279,581,807,813 |
| 53 | 2,6,8,42,50,62,362,488,642,846 |
| 55 | 1,3,5,7,15,33,41,57,69,75,77,131,133,153,247,305,351,409,471 |
| 59 | 12,16,72,160,256,916 |
| 61 | 3,5,9,13,17,19,25,39,63,67,75,119,147,225,419,715,895 |
| 65 | 4,6,12,22,28,52,78,94,124,162,174,192,204,304,376,808,930,972 |
| 67 | 5,9,21,45,65,77,273,677 |
| 71 | 2,14,410 |
| 73 | 7,11,19,71,79,131 |
| 77 | 2,4,14,26,58,60,64,100,122,212,566,638 |
| 79 | 1,3,7,15,43,57,61,75,145,217,247 |
| 83 | 2,4,8,10,14,18,22,24,26,28,36,42,58,64,78,158,198,206,424,550,676,904 |
| 85 | 5,11,71,113,115,355,473,563,883 |
| 89 | 4,8,12,24,48,52,64,84,96 |
| 91 | 1,3,9,13,15,17,19,23,47,57,67,73,77,81,83,191,301,321,435,867,869,917 |
| 95 | 2,6,26,32,66,128,170,288,320,470 |
| 97 | 1,9,45,177,585 |
| 101 | 10,18,54,70 |
| 103 | 3,7,11,19,63,75,95,127,155,163,171,283,563 |
| 107 | 10,12,18,24,28,40,90,132,214,238,322,532,858,940 |
| 109 | 9,149,177,419,617 |
| 113 | 8,14,74,80,274,334,590,608,614,650 |
| 115 | 1,3,11,13,19,21,31,49,59,69,73,115,129,397,623,769 |
| 119 | 12,16,52,160,192,216,376,436 |
| 121 | 1,3,21,27,37,43,91,117,141,163,373,421 |
| 125 | 2,4,44,182,496,904 |
| 127 | 25,113 |
| 131 | 2,14,34,38,42,78,90,178,778,974 |
| 133 | 3,11,15,19,31,59,75,103,163,235,375,615,767 |
| 137 | 2,18,38,62 |
| 139 | 1,5,7,9,15,19,21,35,37,39,41,49,69,111,115,141,159,181,201,217,487,567, 677,765,811,841,917 |
| 143 | 2,4,6,8,12,18,26,32,34,36,42,60,78,82,84,88,154,174,208,256,366,448,478, 746 |
| 145 | 5,13,15,31,77,151,181,245,445,447,883 |
| 149 | 4,16,48,60,240,256,304 |
| 151 | 5,221,641 |

Mention should also be made of a table given by Robinson [4] of primes of the form $A2^n + 1$. This paper also contains an excellent bibliography on the present topic and related ones.

University of Waterloo
Waterloo, Canada

1. H. RIESEL, "A note on prime numbers of the forms $N = (6a + 1)2^{2n-1} - 1$ and $M = (6a - 1)2^{2n} - 1$," *Ark. Mat.*, v. 3, 1956, p. 253. MR **17**, 945.
2. D. H. LEHMER, "An extended theory of Lucas' functions," *Ann. of Math.* (2), v. 31, 1930, p. 446.
3. W. SIERPIŃSKI, *A Selection of Problems in the Theory of Numbers*, translated from Polish, Macmillan, New York, 1964, p. 28. MR **30** #1078.
4. R. M. ROBINSON, "A report on primes of the form $k2^n + 1$ and on factors of Fermat numbers," *Proc. Amer. Math. Soc.*, v. 9, 1958, pp. 674–675. MR **20** #3097.