positive integers $x$ such that $n - g(x) > 0$ and by $P(n)$ the number of $x$'s such that all numbers $f_1(x), f_2(x), \cdots, f_k(x)$ and $n - g(x)$ are primes. Then for large $n$ we have

$$(3) \qquad P(n) \sim \frac{N}{\log^{k+1} N} (h_0 h_1 \cdots h_k)^{-1} \prod_p \left(1 - \frac{\omega(p)}{p}\right)\left(1 - \frac{1}{p}\right)^{-k-1}$$

where $h_0$ is the degree of $g$ and $\omega(p)$ is the number of solutions of the congruence $f(x)(n - g(x)) \equiv 0 (\mathrm{mod}\, p)$.

Conjectures C, G, L and therefore also A, H, I are particular cases of formula (3). To see this, as far as C is concerned, one should put

$$f_1(x) = bx + l, \qquad g(x) = ax, \qquad n = \frac{k - al}{b},$$

where $l$ is an integer such that $al \equiv k(\mathrm{mod}\, b)$, $-b < l \leqq 0$. Conjecture A has been extensively verified [3, p. 37]. I have had no possibility to verify by computation the agreement of formula (3) with reality in other cases. For such comparisons one should replace $N(\log N)^{-k-1}$ by $\int_2^N (\log u)^{-k-1} du$, as is pointed out in [3].

I conclude with expressing my thanks to the referee for his valuable suggestions.

Mathematics Institute PAN
Sniadeckich 8, Warsaw 1
Poland

1. P. T. Bateman & R. A. Horn, "A heuristic asymptotic formula concerning the distribution of prime numbers," *Math. Comp.*, v. 16, 1962, p. 363–367.

2. S. Chowla, "The representation of a number as a sum of four squares and a prime," *Acta Arith.*, v. 1, 1935, p. 115–122.

3. G. H. Hardy & J. E. Littlewood, "Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes," *Acta Math.*, v. 44, 1923, p. 1–70.

4. Ju. V. Linnik, "An asymptotic formula in an additive problem of Hardy-Littlewood," (Russian), *Izv. Akad. Nauk SSSR. Ser. Mat.*, v. 24, 1960, p. 629–706.

# Some Miscellaneous Factorizations

By John Brillhart

**1. Introduction.** The factorizations presented here have accumulated in the author's files for several years and have not heretofore appeared in print. Twenty-five contain new prime factors (designated by an asterisk), while twenty-one, listed as complete, possess a cofactor that is prime. Included are the complete factorizations of four Mersenne numbers and twelve Fibonacci numbers. Further results include a second factor of the Mersenne number $M_{191}$ and of the Fermat number $F_{10}$, as well as the least prime factor of $M_{271}$. These new results relating to Mersenne numbers supplement an earlier tabulation by G. D. Johnson and the author [1].

The factorizations, with the exception of those numbered (6)–(9), inclusive, were obtained by the author on various IBM computers at the University of California at Berkeley and at Los Angeles. The factorizations (6)–(9) of certain alge-

Received January 3, 1963, revised March 12, 1963.

braic factors of the Aurifeuillian numbers $2^{162} + 1$, $2^{222} + 1$, $2^{230} + 1$, and $2^{282} + 1$ were discovered by K. R. Isemonger, with whose kind permission they are included here. It should be noted in (9) that the factor 7484047069 does not appear with an asterisk, inasmuch as it is a known prime factor [2] of the algebraic factor

$$2^{47} + 2^{24} + 1 \text{ of } 2^{141} - 2^{71} + 1.$$

The factors in (30) and (31) were discovered in examining the numbers

$$\tfrac{1}{9}(10^p - 1),$$

$p$ a prime $\leqq 109$, for factors $< 10^6$ in the cases where no factor was known ($p = 37, 47, 59, 67, 71, 73, 83, 89, 97, 101, 109$) [3]. These numbers, as well as the cofactors in (30) and (31), were also tested by the contra-positive of Fermat's Theorem: "If $a^{N-1} \not\equiv 1 (\text{mod } N)$ and $(a, N) = 1$, then $N$ is composite," and were all found to be composite. Thus, for $p \leqq 109$, the only primes of this form are $\tfrac{1}{9}(10^2 - 1)$, $\tfrac{1}{9}(10^{19} - 1)$ and $\tfrac{1}{9}(10^{23} - 1)$.

**2. Primality Testing.** The primality of the cofactors in factorizations (2), (5) and (10)–(21), inclusive, was determined by showing that each cofactor possesses no factor less than its square root. In particular, by this procedure the Fibonacci number $U_{83}$ was identified as a prime. (The standard notation for such numbers is used here, in that $U_n$ is defined by the linear recurrence $U_n = U_{n-1} + U_{n-2}$, for $n = 2, 3, 4, \cdots$, with $U_0 = 0$ and $U_1 = 1$.)

In factorizations (1), (3), and (4), whose cofactors were too large to be tested for primality by this method, recourse was taken to the well-known theorem of Lehmer [4]: "If $a^x \equiv 1 (\text{mod } N)$ for $x = N - 1$, but not for $x$ a quotient of $N - 1$ on division by any of its prime factors, then $N$ is prime."

Inasmuch as the hypothesis of this theorem requires the complete factorization of $N - 1$, as well as a suitable choice of the integer $a$, a preliminary investigation was performed, with the following results. For (1) and (3), respectively, $N - 1 = 2^3 \cdot 3 \cdot 103 \cdot 149 \cdot 4657 \cdot 71429 \cdot 32456563$, with $a = 5$; and

$$N - 1 = 2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 41 \cdot 163 \cdot 179 \cdot 643 \cdot 919 \cdot 43399 \cdot 1071379 \cdot 23262667 \cdot 1159540629640123,$$

with $a = 19$.

A different situation was encountered in examining the cofactor in (4), where

$$N - 1 = 2 \cdot 5 \cdot 181 \cdot 4377829335516737914555053958986007 = 2 \cdot 5 \cdot 181 \cdot M,$$

with $a = 17$. To show that this factorization is complete, the theorem was applied to $M$ itself. This application was possible because of the fortunate factorization:

$$M - 1 = 2 \cdot 3 \cdot 47 \cdot 253567 \cdot 811039 \cdot 2293751 \cdot 32910082955041,$$

with $a = 13$.

**3. Complete Factorizations.**

(1) $2^{103} - 1 = 2550183799^* \cdot 3976656429941438590393^*$

(2) $2^{163} - 1 = 150287 \cdot 704161 \cdot 110211473 \cdot 27669118297^* \cdot$
$36230454570129675721^*$

(3) $2^{179} - 1 = 359 \cdot 1433 \cdot$
$1489459109360039866456940197095433721664951999121$

(4) $2^{181} - 1 = 43441 \cdot 1164193 \cdot 7648337 \cdot$
$7923871097285295625344647665764672671$

(5) $2^{165} + 1 = 3^2 \cdot 11^2 \cdot 67 \cdot 331 \cdot 683 \cdot 2971 \cdot 20857 \cdot 48912491 \cdot$
$415365721^* \cdot 2252127523412251^*$

(6) $2^{81} + 2^{41} + 1 = 5 \cdot 109 \cdot 246241 \cdot 106979941^* \cdot 168410989^*$

(7) $2^{111} + 2^{56} + 1 = 5 \cdot 149 \cdot 3109 \cdot 184481113 \cdot 1398316729^* \cdot 4345052821^*$

(8) $2^{115} + 2^{58} + 1 = 41 \cdot 277 \cdot 30269 \cdot 15096281^* \cdot 1021622741^* \cdot$
$7834788541^*$

(9) $2^{141} - 2^{71} + 1 = 5 \cdot 1129 \cdot 3761 \cdot 1768141^* \cdot 54865357^* \cdot 7484047069 \cdot$
$180846660913^*$

(10) $U_{71} = 6673^* \cdot 46165371073^*$

(11) $U_{79} = 157 \cdot 92180471494753$

(12) $U_{83} = 99194853094755497$

(13) $U_{89} = 1069 \cdot 1665088321800481$

(14) $U_{91} = 13^2 \cdot 233 \cdot 741469^* \cdot 159607993^*$

(15) $U_{93} = 2 \cdot 557 \cdot 2417 \cdot 4531100550901$

(16) $U_{95} = 5 \cdot 37 \cdot 113 \cdot 761 \cdot 29641^* \cdot 67735001^*$

(17) $U_{97} = 193 \cdot 389 \cdot 3084989^* \cdot 361040209^*$

(18) $U_{101} = 743519377^* \cdot 770857978613^*$

(19) $U_{103} = 519121^* \cdot 5644193^* \cdot 512119709^*$

(20) $U_{107} = 1247833^* \cdot 8242065050061761^*$

(21) $U_{109} = 827728777^* \cdot 32529675488417^*$

## 4. Some Prime Factors.

(22) $93507247^* \mid 2^{171} - 1$

(23) $60816001^* \mid 2^{175} - 1$

(24) $7068569257^* \mid 2^{191} - 1$

(25) $121793911^* \mid 2^{203} - 1$

(26) $634569679^* \mid 2^{207} - 1$

(27) $731516431^* \mid 2^{215} - 1$

(28) $15242475217^* \mid 2^{271} - 1$

(29) $395937 \cdot 2^{14} + 1 = 6487031809^* \mid 2^{2^{10}} + 1$

(30) $493121^* \mid 10^{67} - 1$

(31) $497867^* \mid 10^{89} - 1$

It should be remarked that the prime in (29) is the last "small" factor of the early Fermat numbers $F_m (= 2^{2^m} + 1)$ to be discovered, since all factors $< 2^{35}$ for $1 \leqq m \leqq 19$ are now known [5].

**5. Acknowledgments.** The author would like to thank the directors of the computer centers at the University of California at Berkeley and at Los Angeles for their generous support of the projects that have produced the above results. He would also like especially to thank John Selfridge and Vance Vaughan for their considerable efforts in his behalf. Finally, he would like to express his gratitude to

R. M. Robinson, whose IBM 701 program produced the factorization (5), and to D. H. Lehmer, whose suggestions have materially assisted in the planning of this work.

University of San Francisco
San Francisco, California

1. John Brillhart & G. D. Johnson, "On the factors of certain Mersenne numbers," *Math. Comp.*, v. 14, 1960, p. 365–369.
2. John Brillhart, "Concerning the numbers $2^{2p} + 1$, $p$ prime," *Math. Comp.*, v. 16, 1962, p. 424–430. (Reference is there made to the earlier table by M. Kraitchik.)
3. A. J. C. Cunningham & H. J. Woodall, *Factorizations of* $(y^n \mp 1)$, Hodgson, London, 1925, p. 19.
4. D. H. Lehmer, "Tests for primality by the converse of Fermat's theorem," *Bull., Amer. Math. Soc.*, v. 33, 1927, p. 327–340.
5. R. M. Robinson, "A report on primes of the form $k \cdot 2^n + 1$ and on factors of Fermat numbers," *Proc., Amer. Math. Soc.*, v. 9, 1958, p. 673–681.

EDITORIAL NOTE: Rudolph Ondrejka has shown that $10^{37} - 1$ is divisible by 2028119. (*Recreational Math. Mag.*, Feb. 1962, p. 47.)

# A Note on Octic Permutation Polynomials

**By S. R. Cavior**

**1. Introduction.** A polynomial $f(x)$ with coefficients in the finite field $GF(q)$, $q = p^n$, is called a permutation polynomial if the set $\{f(a): a \in GF(q)\}$ is a permutation of $GF(q)$. The object of this paper is to extend some known results about permutation polynomials of even degree over fields with odd characteristic $p$.

We shall frequently use the following theorem which is given by Dickson [1, p. 77].

Theorem. *If $f(x)$ is a polynomial of degree $m$ over $GF(q)$, and if $m \mid q - 1$, then $f(x)$ does not permute $GF(q)$.*

To begin our discussion, we note immediately, by the Theorem, that a quadratic polynomial cannot permute $GF(q)$. Dickson, in [1], showed that a quartic cannot permute $GF(q)$ for $q > 7$ (although two do for $q = 7$), and that a sextic cannot permute $GF(q)$ for $q > 11$ (although several do for $q = 11$.) A natural question to ask, then, is whether there is an upper bound for the order of a finite field which an octic can permute.

The present investigation, however, is restricted to the following special octics:

$$f(x) = x^8 + ax^t \qquad t = 1, 3, 5, 7; a \in GF(q). \tag{1}$$

The case $t = 7$ can be settled at once, for if $f(x) = x^8 + ax^7$, where $a \in GF(q)$, then $f(-a) = f(0) = 0$. That is, $f(x)$ is not a permutation polynomial. With the aid of a computer it was discovered that the only polynomials of the form (1) which permute $GF(p)$ for $p < 500$ are

$$x^8 + ax \qquad a = \pm 4, \pm 10; p = 29 \tag{2}$$

Received October 12, 1962, revised April 26, 1963. This research was supported in part by National Science Foundation. The computations involved were carried out in the Duke University Computing Laboratory, which is supported in part by National Science Foundation.