MATHEMATICS OF COMPUTATION, VOLUME 27, NUMBER 124, OCTOBER 1973

Primitive Binary Polynomials

By Wayne Stahnke

Abstract. One primitive polynomial modulo two is listed for each degree n through $n = 168$. Each polynomial has the minimum number of terms possible for its degree. The method used to generate the list is described.

Introduction. The accompanying table contains one primitive polynomial modulo two for each degree n, $1 \leqq n \leqq 168$. Since the number of physical logic elements required to implement a given polynomial is a function of the number of terms in that polynomial, each entry has as few terms as possible for polynomials of its degree.

Each polynomial listed for $n > 1$ is of one of two forms. If there exist one or more primitive trinomials $f(x) = x^n + x^k + 1$ the trinomial with the smallest k is listed. If no primitive trinomials exist, the polynomial given is of the form $g(x) = x^n + x^{b+a} + x^b + x^a + 1$, with $0 < a < b < n - a$. For these polynomials, a is as small as possible, and for the a listed, b is as small as possible. This form was chosen because it corresponds to the configuration of logic elements introduced by Scholefield [1], which implements the reciprocal polynomial $x^n g(x^{-1})$ using only n unit-delay elements and two two-input modulo-two adders. The conventional shift-register configuration [2] can also implement $g(x)$ or $x^n g(x^{-1})$, at the expense of one additional two-input modulo-two adder.

In the table, only the degrees of the individual terms of the primitive polynomials are listed, so that for example

$$125, 108, 107, 1, 0 \quad \text{represents} \quad g(x) = x^{125} + x^{108} + x^{107} + x + 1.$$

The only similar table known to the author is Watson's [3] which lists one primitive polynomial for each degree n through $n = 100$, and also for $n = 107$ and $n = 127$. The entries in Watson's table are not of any particular form, and many of them do not have the minimum possible number of terms.

The Test for Primitivity. The test for primitivity consists of four stages. The first two stages, which are used because of their relatively high speed, eliminate all of the reducible polynomials. The last two stages form a necessary and sufficient test for primitivity.

In the first stage, the trial polynomial $p(x)$ is rejected as reducible (and therefore not primitive) if each one of its terms is an even power of x, since in that case the polynomial is a square.

Received October 11, 1972.

AMS (MOS) subject classifications (1970). Primary 12C05, 12C10.

Key words and phrases. Primitive polynomials, finite field, Mersenne numbers, shift-register sequences.

In the second stage, the greatest common divisor of $p(x)$ and $x^{2^m} + x$ is calculated for each m, $1 \leqq m \leqq [n/2]$, using the Euclidean algorithm. The trial polynomial is rejected as reducible if the result is not equal to 1 for each m. This stage forms a necessary and sufficient test for the irreducibility of $p(x)$ since every irreducible polynomial of degree m is a factor of $x^{2^m} + x$ [4, p. 103].

Exponents of Terms of Primitive Binary Polynomials

1	0				41	3	0		
2	1	0			42	23	22	1	0
3	1	0			43	6	5	1	0
4	1	0			44	27	26	1	0
5	2	0			45	4	3	1	0
6	1	0			46	21	20	1	0
7	1	0			47	5	0		
8	6	5	1	0	48	28	27	1	0
9	4	0			49	9	0		
10	3	0			50	27	26	1	0
11	2	0			51	16	15	1	0
12	7	4	3	0	52	3	0		
13	4	3	1	0	53	16	15	1	0
14	12	11	1	0	54	37	36	1	0
15	1	0			55	24	0		
16	5	3	2	0	56	22	21	1	0
17	3	0			57	7	0		
18	7	0			58	19	0		
19	6	5	1	0	59	22	21	1	0
20	3	0			60	1	0		
21	2	0			61	16	15	1	0
22	1	0			62	57	56	1	0
23	5	0			63	1	0		
24	4	3	1	0	64	4	3	1	0
25	3	0			65	18	0		
26	8	7	1	0	66	10	9	1	0
27	8	7	1	0	67	10	9	1	0
28	3	0			68	9	0		
29	2	0			69	29	27	2	0
30	16	15	1	0	70	16	15	1	0
31	3	0			71	6	0		
32	28	27	1	0	72	53	47	6	0
33	13	0			73	25	0		
34	15	14	1	0	74	16	15	1	0
35	2	0			75	11	10	1	0
36	11	0			76	36	35	1	0
37	12	10	2	0	77	31	30	1	0
38	6	5	1	0	78	20	19	1	0
39	4	0			79	9	0		
40	21	19	2	0	80	38	37	1	0

Exponents of Terms of Primitive Binary Polynomials

81	4	0		
82	38	35	3	0
83	46	45	1	0
84	13	0		
85	28	27	1	0
86	13	12	1	0
87	13	0		
88	72	71	1	0
89	38	0		
90	19	18	1	0
91	84	83	1	0
92	13	12	1	0
93	2	0		
94	21	0		
95	11	0		
96	49	47	2	0
97	6	0		
98	11	0		
99	47	45	2	0
100	37	0		
101	7	6	1	0
102	77	76	1	0
103	9	0		
104	11	10	1	0
105	16	0		
106	15	0		
107	65	63	2	0
108	31	0		
109	7	6	1	0
110	13	12	1	0
111	10	0		
112	45	43	2	0
113	9	0		
114	82	81	1	0
115	15	14	1	0
116	71	70	1	0
117	20	18	2	0
118	33	0		
119	8	0		
120	118	111	7	0
121	18	0		
122	60	59	1	0
123	2	0		
124	37	0		
125	108	107	1	0
126	37	36	1	0
127	1	0		
128	29	27	2	0
129	5	0		
130	3	0		
131	48	47	1	0
132	29	0		
133	52	51	1	0
134	57	0		
135	11	0		
136	126	125	1	0
137	21	0		
138	8	7	1	0
139	8	5	3	0
140	29	0		
141	32	31	1	0
142	21	0		
143	21	20	1	0
144	70	69	1	0
145	52	0		
146	60	59	1	0
147	38	37	1	0
148	27	0		
149	110	109	1	0
150	53	0		
151	3	0		
152	66	65	1	0
153	1	0		
154	129	127	2	0
155	32	31	1	0
156	116	115	1	0
157	27	26	1	0
158	27	26	1	0
159	31	0		
160	19	18	1	0
161	18	0		
162	88	87	1	0
163	60	59	1	0
164	14	13	1	0
165	31	30	1	0
166	39	38	1	0
167	6	0		
168	17	15	2	0

If the trial polynomial is irreducible, the test goes forward to the third stage, which verifies that $p(x)$ divides $x^{2^n} + x$, which is equivalent to saying that the period of $p(x)$ divides $2^n - 1$. This must be true since it has already been established that $p(x)$ is irreducible, so this stage checks for possible machine errors of certain types in the second stage.

If $2^n - 1$ is prime, the trial polynomial is primitive. If $2^n - 1$ is composite, however, the period of $p(x)$ may be a factor of $2^n - 1$. This possibility is tried in the fourth stage in which $x^{(2^n-1)/q} \bmod p(x)$ is calculated for each prime factor q of $2^n - 1$. If the result is 1 for any q, the trial polynomial is not primitive.

If the trial polynomial survives all four stages of the test, it is primitive, which is checked by repeating the third and fourth stages of the test on the reciprocal polynomial $x^n p(x^{-1})$.

The program was run on the IBM 360/67 at Fairchild Semiconductor. At the beginning of each computer run, the factors of $2^n - 1$ were multiplied together for each n and it was verified that their product was actually $2^n - 1$. No machine errors were encountered in any of the computer runs. All of the trinomials were checked against the list of Zierler and Brillhart [5], and all of the polynomials of degree $n \leqq 19$ were checked against Marsh's list [6]. There were no discrepancies.

The factors of $2^n - 1$ were taken from Riesel [7] and checked against other sources in the literature ([8], [9], [10], [11], [12], [13], [14]) with a few exceptions. The factorizations for n = 125, 137, 139, 141, 143, 145, 149, 157, 161 and 167 were furnished by John Brillhart, with whose kind permission they were used to complete the preparation of the table.

Fairchild Semiconductor
464 Ellis Street
Mountain View, California 94040

1. P. H. R. Scholefield, "Shift registers generating maximum-length sequences," *Electronic Technology*, v. 37, 1960, pp. 389–394.

2. S. W. Golomb, *Shift Register Sequences*, Holden-Day, San Francisco, Calif., 1967. MR **39** #3906.

3. E. J. Watson, "Primitive polynomials (Mod 2)," *Math. Comp.*, v. 16, 1962, pp. 368–369. MR **26** #5764.

4. E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968. MR **38** #6873.

5. N. Zierler & J. Brillhart, "On primitive trinomials (Mod 2)," *Information Control*, v. 13, 1968, pp. 541–554; II, v. 14, 1969, pp. 566–569. MR **38** #5750; MR **39** #5521.

6. R. W. Marsh, *Table of Irreducible Polynomials Over GF*(2) *Through Degree* 19, Office of Technical Services, Department of Commerce, Washington, D. C., October 24, 1957.

7. H. Riesel, *En Bok om Primtal* [*A Book on Prime Numbers*], Studentlitteratur, Lund, 1968. (Swedish) MR **42** #4507.

8. J. Brillhart, "Some miscellaneous factorizations," *Math. Comp.*, v. 17, 1963, pp. 447–450.

9. J. Brillhart & J. L. Selfridge, "Some factorizations of $2^n \pm 1$ and related results," *Math. Comp.*, v. 21, 1967, pp. 87–96. MR **37** #131.

10. K. R. Isemonger, "Complete factorization of $2^{159} - 1$," *Math. Comp.*, v. 15, 1961, pp. 295–296. MR **23** #A1577.

11. K. R. Isemonger, "Some additional factorizations of $2^n \pm 1$," *Math. Comp.*, v. 19, 1965, pp. 145–146. MR **30** #1081.

12. M. Kraitchik, *Introduction à la Théorie des Nombres*, Gauthier-Villars, Paris, 1952. MR **14**, 535.

13. M. Kraitchik, "On the factorization of $2^n \pm 1$," *Scripta Math.*, v. 18, 1952, pp. 39–52. MR **14**, 121.

14. R. M. Robinson, "Some factorizations of numbers of the form $2^n \pm 1$," *MTAC*, v. 11, 1957, pp. 265–268. MR **20** #832.