Primitive Polynomials (Mod 2)

By E. J. Watson

The following list contains one example of a primitive polynomial (mod 2) for each degree n, $1 \leqq n \leqq 100$. It was compiled with the aid of the Mercury computer at Manchester University by the following method.

The polynomials $P_n(x)$ (mod 2) of degree n were tested in their natural order until a primitive polynomial was found. The test comprised three stages. In the first stage the small primes, of degree up to 9, were tried as possible factors (mod 2) of P_n. If no factor was found P_n went forward to the second stage, which tested whether P_n divides $x^N - 1$, where $N = 2^n - 1$. If it does, and N is prime (a Mersenne prime), this suffices to prove that P_n is primitive. If N is composite, however, P_n might divide $x^M - 1$, where M is a factor of N, and then P_n would not be primitive. The third stage was, therefore, a trial of this possibility, in which M took the values N/p, where p runs through the prime factors of N.

The two latter stages were carried out by a process in which the computer repeated the operations of squaring, possibly multiplying by x (depending on the binary representation of M), then dividing by P_n. The prime factors of N were taken from the tables of Kraïtchik [1], supplemented by Robinson's [2] further decomposition of $2^{95} - 1$. If any more of these 'prime' factors should turn out to be composite, doubt would be cast on the corresponding P_n. Mersenne polynomials for $n = 107$ and 127 are also given. The prime $x^{127} + x + 1$ was found by Zierler [3]. Its nature follows from the general result that if $\Sigma a_n x^n$ divides $\Sigma c_n x^n$ (mod p), then

$$\Sigma a_n x^{p^n} \quad \text{divides} \quad \Sigma c_n x^{p^n} \qquad (\text{mod } p).$$

The primitive character of each polynomial $P_n(x)$ listed has been checked by a repetition of the second and third stages on the conjugate polynomial $x^n P_n(x^{-1})$. In the list only the degrees of the separate terms in P_n are given, thus

$$127 \quad 1 \quad 0 \qquad \text{stands for} \qquad x^{127} + x + 1.$$

Department of Mathematics
University of Manchester

1. M. Kraïtchik, *Introduction à la Théorie des Nombres*, Gauthier-Villars, Paris, 1952.
2. R. M. Robinson, "Some factorizations of numbers of the form $2^n \pm 1$," *MTAC*, v. 11, 1957, p. 265–268.
3. N. Zierler, "Linear recurring sequences," *J. Soc. Indust. Appl. Math.*, v. 7, 1959, p. 31–48.

Received December 18, 1961.

Primitive Polynomials (mod 2)

1	0						51	6	3	1	0		
2	1	0					52	3	0				
3	1	0					53	6	2	1	0		
4	1	0					54	6	5	4	3	2	0
5	2	0					55	6	2	1	0		
6	1	0					56	7	4	2	0		
7	1	0					57	5	3	2	0		
8	4	3	2	0			58	6	5	1	0		
9	4	0					59	6	5	4	3	1	0
10	3	0					60	1	0				
11	2	0					61	5	2	1	0		
12	6	4	1	0			62	6	5	3	0		
13	4	3	1	0			63	1	0				
14	5	3	1	0			64	4	3	1	0		
15	1	0					65	4	3	1	0		
16	5	3	2	0			66	8	6	5	3	2	0
17	3	0					67	5	2	1	0		
18	5	2	1	0			68	7	5	1	0		
19	5	2	1	0			69	6	5	2	0		
20	3	0					70	5	3	1	0		
21	2	0					71	5	3	1	0		
22	1	0					72	6	4	3	2	1	0
23	5	0					73	4	3	2	0		
24	4	3	1	0			74	7	4	3	0		
25	3	0					75	6	3	1	0		
26	6	2	1	0			76	5	4	2	0		
27	5	2	1	0			77	6	5	2	0		
28	3	0					78	7	2	1	0		
29	2	0					79	4	3	2	0		
30	6	4	1	0			80	7	5	3	2	1	0
31	3	0					81	4	0				
32	7	5	3	2	1	0	82	8	7	6	4	1	0
33	6	4	1	0			83	7	4	2	0		
34	7	6	5	2	1	0	84	8	7	5	3	1	0
35	2	0					85	8	2	1	0		
36	6	5	4	2	1	0	86	6	5	2	0		
37	5	4	3	2	1	0	87	7	5	1	0		
38	6	5	1	0			88	8	5	4	3	1	0
39	4	0					89	6	5	3	0		
40	5	4	3	0			90	5	3	2	0		
41	3	0					91	7	6	5	3	2	0
42	5	4	3	2	1	0	92	6	5	2	0		
43	6	4	3	0			93	2	0				
44	6	5	2	0			94	6	5	1	0		
45	4	3	1	0			95	6	5	4	2	1	0
46	8	5	3	2	1	0	96	7	6	4	3	2	0
47	5	0					97	6	0				
48	7	5	4	2	1	0	98	7	4	3	2	1	0
49	6	5	4	0			99	7	5	4	0		
50	4	3	2	0			100	8	7	2	0		
107	7	5	3	2	1	0	127	1	0				