

# Primitive Polynomials (Mod 2)

By E. J. Watson

The following list contains one example of a primitive polynomial (mod 2) for each degree  $n$ ,  $1 \leq n \leq 100$ . 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 Kraitchik [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  $\sum a_n x^n$  divides  $\sum c_n x^n$  (mod  $p$ ), then

$$\sum a_n x^{pn} \text{ divides } \sum c_n x^{pn} \pmod{p}.$$

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

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

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.

