

NEW PRIMITIVE t -NOMIALS ($t = 3, 5$) OVER $GF(2)$ WHOSE DEGREE IS A MERSENNE EXPONENT

TOSHIHIRO KUMADA, HANNES LEEB,
YOSHIHARU KURITA, AND MAKOTO MATSUMOTO

ABSTRACT. All primitive trinomials over $GF(2)$ with degree 859433 (which is the 33rd Mersenne exponent) are presented. They are $X^{859433} + X^{288477} + 1$ and its reciprocal. Also two examples of primitive pentanomials over $GF(2)$ with degree 86243 (which is the 28th Mersenne exponent) are presented. The sieve used is briefly described.

1. INTRODUCTION

Primitive t -nomials (t -term polynomials) over $GF(2)$ are useful in applications like random number generation, coding theory, and cryptography. Heringa et al. [H] exhaustively listed all primitive trinomials of Mersenne exponent degree up to the 31st Mersenne exponent 216091. This note is an extension of that work.

Let M_n denote the n th Mersenne exponent (for example, $M_{28} = 86243$ and $2^{M_{28}} - 1$ is known to be a prime). As of November 27, 1998, 37 Mersenne exponents had been found. 3021377 is the greatest of them. An exhaustive primality test of all exponents less than 2000000 has been carried out (it proves that $M_{35} = 1398269$). The known Mersenne exponents greater than 2000000 are 2976221 and 3021377. In this paper, we define $M_{36\#} = 2976221$ and $M_{37\#} = 3021377$. The sharp mark behind 36 and 37 shows that the search for Mersenne exponents p in the interval $2000000 < p < 3021377$ has not been exhaustive. See [HT1, HT2] for information about the current search status of Mersenne exponents.

Table 1 lists all primitive trinomials $X^p + X^q + 1$ over $GF(2)$ with degree $p = M_n$ ($33 \leq n \leq 36\#$), $q \leq \lfloor p/2 \rfloor$. Table 2 lists examples of primitive pentanomials $X^p + X^{q_1} + X^{q_2} + X^{q_3} + 1$ over $GF(2)$ with degree $p = M_{28}$. In Tables 1 and 2, only the exponents of the terms are listed.

2. TEST FOR PRIMITIVITY

2.1. Primitivity of trinomials. Let $f(X) = X^p + X^q + 1$ be a trinomial of degree $p = M_n$. Our aim is to find q such that $X^p + X^q + 1$ is primitive. By considering the reciprocal polynomial, we may assume that $1 \leq q \leq \lfloor p/2 \rfloor$. If $2^p - 1$ is prime, then primitivity is equivalent to irreducibility. The test for primitivity comprises

Received by the editor May 19, 1998.

1991 *Mathematics Subject Classification*. Primary 11-04, 11T06, 12-04, 12E05.

Key words and phrases. Irreducible polynomials, primitive polynomials, finite field, Mersenne exponent.

This research was supported by the Austrian Science Foundation (FWF), project no. P11143-MAT.

the following three sieves. The first two of these are only necessary condition tests, but they reject about 90% of the candidates. The third sieve is a necessary and sufficient test. The third sieve can determine whether $f(X)$ is irreducible or not with an $O(p^2)$ computation.

Let k_n denote $2^n - 1$. Sieves I and II are based on a well-known theorem [L, pp. 48]: if $\phi(X)$ is an irreducible polynomial over $GF(2)$ of degree m , then $\phi(X) | (X^{1+k_n} - X)$ if and only if $m|n$. Thus by computing $\gcd(f(X), X^{k_n} - 1)$, we know whether $f(X)$ has a factor of degree $m|n$.

Sieve I: mod k test. One can determine easily whether $\gcd(f(X), X^k - 1) = 1$ for small k as follows. If it equals 1, then $f(X)$ goes forward to the next sieve. Let k be an odd positive integer. Then

$$\begin{aligned} \gcd(f(X), X^k - 1) &= \gcd(X^p + X^q + 1, X^k - 1) \\ &= \gcd(X^{(p \bmod k)} + X^{(q \bmod k)} + 1, X^k - 1). \end{aligned}$$

So fix p , and put

$$R_k = \{\bar{q} \in \mathbf{Z}/k\mathbf{Z} \mid \gcd(X^{(p \bmod k)} + X^{\bar{q}} + 1, X^k - 1) \neq 1\}.$$

This set can be obtained by exhaustive search for $\bar{q} \in \mathbf{Z}/k\mathbf{Z}$. If for a given q there exists a k with $(q \bmod k) \in R_k$, then $X^p + X^q + 1$ is reducible. We compute R_k for $k = 3, 5, 7, \dots, k_{12} + 2$, and $k = k_{13}, k_{14}, k_{15}$. We reject q if for one of above k we have $(q \bmod k) \in R_k$. This test rejects about 89% of the candidates.

Sieve II: direct gcd test. Let $f(X)$ be a trinomial which passed Sieve I. By computing $\gcd(f(X), X^{k_n} - 1)$ ($n = 16, 17, 18$) we can eliminate some candidates. Sieves I and II reject about 91% of the candidates.

Sieve III is a necessary and sufficient irreducibility test based on Theorem 1 (see below). The following description is quoted from [M].

Let S^∞ denote the $GF(2)$ -vector space of all infinite sequences of zeros and ones. That is,

$$S^\infty := \{\chi = (\dots, x_5, x_4, x_3, x_2, x_1, x_0) \mid x_i \in GF(2)\}.$$

Let D (*delay operator*) and H (*decimation operator*) be linear operators from S^∞ to S^∞ defined by

$$D(\dots, x_4, x_3, x_2, x_1, x_0) = (\dots, x_5, x_4, x_3, x_2, x_1),$$

$$H(\dots, x_4, x_3, x_2, x_1, x_0) = (\dots, x_{10}, x_8, x_6, x_4, x_2, x_0).$$

Let $\varphi(X)$ be the characteristic polynomial of a linear recurrence, and let χ be an element of S^∞ . Then, χ satisfies the recurrence if and only if $\varphi(D)\chi = 0$. Note that $\varphi(D)$ is a linear operator and 0 denotes the zero sequence. It is easy to check that

$$DH = HD^2.$$

Since the coefficients are in $GF(2)$, we have $\varphi(X^2) = \varphi(X)^2$, and thus if $\varphi(D)\chi = 0$ then

$$\varphi(D)H\chi = H\varphi(D^2)\chi = H\varphi(D)^2\chi = 0,$$

i.e., $H\chi$ also satisfies the same recurrence. The following theorem holds [M].

Theorem 1. *Let $\varphi(X)$ be a polynomial over $GF(2)$ whose degree p is a Mersenne exponent. Take $\chi \in S^\infty$ such that $\varphi(D)\chi = 0$ and $H\chi \neq \chi$. Then $\varphi(t)$ is primitive if and only if $H^p\chi = \chi$.*

In the above theorem, put $\varphi(X) := X^p + X^q + 1$. Let $T = (\dots, t_4, t_3, t_2, t_1, t_0)$ be an element of S^∞ such that $\varphi(D)T = 0$, i.e., for all non-negative integers i ,

$$(*) \quad t_{p+i} = t_{q+i} + t_i.$$

Let $Extend : GF(2)^p \rightarrow GF(2)^{2p}$ send the initial vector $T_0 = (t_{p-1}, \dots, t_0)$ to the vector $(t_{2p-1}, t_{2p-2}, \dots, t_0)$ of twice the length generated by the recurrence (*). Let $H' : GF(2)^{2p} \rightarrow GF(2)^p$ be

$$(t_{2p-1}, t_{2p-2}, \dots, t_0) \mapsto (t_{2(p-1)}, t_{2(p-2)}, \dots, t_2, t_0).$$

Since the linear recurrence sequence is determined by its initial vector of length p , computing H is equivalent to computing $H' \circ Extend$.

Sieve III: final test.

- (1) Choose an initial vector $T_0 = (t_{p-1}, \dots, t_i, \dots, t_0)$ so that $H(T_0) \neq T_0$.
- (2) Compute successively the sequences S_i, T_i as follows. $S_i := Extend(T_i)$, $T_{i+1} := H'(S_i)$.
- (3) If T_p equals T_0 , then $f(x)$ is primitive, and otherwise not primitive.

2.2. Primitivity of pentanomials. The necessary and sufficient irreducibility test used for pentanomials is a more naive method than that used for trinomials. Let $f(X) = X^p + X^{q_1} + X^{q_2} + X^{q_3} + 1$ be a pentanomial of Mersenne exponent degree p . We compute $X^N \pmod{f(X)}$, where $N = 2^p - 1$. The pentanomial is irreducible if and only if the result equals 1. $X^N = 1 \pmod{f(X)}$ is equivalent to $X^{N+1} = X \pmod{f(X)}$, because X is an invertible element in the residue ring $GF(2)[X]/(f(X))$. In the actual procedure, we compute successively the sequence X_i from X_0 to X_p , where $X_i = X_{i-1}^2 \pmod{f(X)}$ over $GF(2)$ and $X_0 = X$. See [K] for more information.

3. RESULTS

Concerning the trinomials, we tried searching for primitive trinomials of degree M_{33}, M_{34}, M_{35} and $M_{36\#}$. We did not search for primitive trinomials of degree M_{32} and $M_{37\#}$.

For $p = M_{34}, M_{35}$ and $M_{36\#}$, nonexistence of primitive trinomials is proved as follows: Swan's Corollary [B, p. 170] guarantees that $X^p + X^q + 1$ is reducible over $GF(2)$ if $p = \pm 3 \pmod{8}$ and $q \neq 2$. So we may assume q to be 2 for $p = M_{34}, M_{35}$ and $M_{36\#}$. Then by Sieve III, we show that $X^p + X^2 + 1$ is reducible.

In case of $p = M_{33}$, 40656 candidates passed Sieves I and II. For the computer search, we used an SGI POWER Challenge 10000 GR parallel computer with 20 processors and 2.5 GB RAM. After minor architecture-specific optimizations, we were able to test approximately one candidate parameter per hour. Hence, checking

TABLE 1. Primitive trinomials

n	$M_n \pmod{8}$	$p = M_n$	q
32	-1	756839	the search is not done
33	1	859433	288477
34	3	1257787	none
35	-3	1398269	none
36#	-3	2976221	none
37#	1	3021377	the search is not done

TABLE 2. Primitive pentanomials

n	$p = M_n$	q_1	q_2	q_3
28	86243	62833	50942	11754
		64043	41667	19434

all 40656 candidates consumed a total accumulated time of 4.6 years; using 19 of the available processors, the search was completed in about 3 months.

The non-exhaustive search for primitive pentanomials was done in the AIST computer center (RIPS), Tsukuba. We succeeded in finding two primitive pentanomials whose degree is M_{28} .

ACKNOWLEDGMENTS

We would like to thank Prof. Zinterhof for putting the computing facilities of the University of Salzburg's RIST++ institute at our disposal. We also would like to thank the referee for his(her) careful reading.

REFERENCES

- B. E. R. Berlekamp, *Algebraic coding theory*, McGraw-Hill, New York, 1968. MR **38**:6873
- H. J. R. Heringa, H. W. J. Blöte and A. Compagner, *New primitive trinomials of Mersenne-exponent degrees for random-number generation*, Int. J. Mod. Phys. C vol. 3, No. 3, (1992), 561–564. MR **94a**:11113
- HT1. <http://www.mersenne.org/status.htm>
- HT2. <http://www.utm.edu:80/research/primes/mersenne.shtml>
- K. Y. Kurita and M. Matsumoto, *Primitive t -nomials ($t = 3, 5$) over $GF(2)$ whose degree is a Mersenne exponent ≤ 44497* , Math. Comp. vol. 56, No. 194, April (1991), pp. 817–821. MR **91h**:11138
- L. R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge Univ. Press, Cambridge, 1986. MR **88c**:11073
- M. M. Matsumoto and T. Nishimura, *Mersenne Twister: A 623-dimensionally equidistributed uniform pseudorandom number generator*, ACM Trans. on Modeling and Computer Simulation vol. 8, No. 1, January 1998, pp. 3–30.

DEPARTMENT OF MATHEMATICS, KEIO UNIVERSITY, YOKOHAMA, JAPAN
E-mail address: kumada@math.keio.ac.jp

DEPARTMENT OF STATISTICS, OR AND COMPUTER METHODS, UNIVERSITY OF VIENNA, AUSTRIA
E-mail address: leeb@smc.univie.ac.at

HUNGARIAN PRODUCTIVITY CENTER, BUDAPEST, HUNGARY
E-mail address: ykurit@ibm.net

DEPARTMENT OF MATHEMATICS, KEIO UNIVERSITY, YOKOHAMA, JAPAN
E-mail address: matumoto@math.keio.ac.jp