MATHEMATICS OF COMPUTATION
Volume 71, Number 239, Pages 1337–1338
S 0025-5718(02)01487-4
Article electronically published on April 1, 2002

CORRIGENDA TO "NEW PRIMITIVE t-NOMIALS $(t = 3, 5)$ OVER $GF(2)$ WHOSE DEGREE IS A MERSENNE EXPONENT," AND SOME NEW PRIMITIVE PENTANOMIALS

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

Abstract. We report an error in our previous paper [2], where we announced that we listed all the primitive trinomials over $GF(2)$ of degree 859433, but there is a bug in the sieve. We missed the primitive trinomial $X^{859433} + X^{170340} + 1$ and its reciprocal, as pointed out by Richard Brent et al. We also report some new primitive pentanomials.

1. Corrigendum

In [2, Table 1], we claimed that all primitive trinomials with degree 859433 (32nd Mersenne exponent) over $GF(2)$ are $X^{859433} + X^{288477} + 1$ and its reciprocal, but there was a bug in a code for the sieve. Richard Brent et al. [1] pointed out that there are two more primitive trinomials of this degree: $X^{859433} + X^{170340} + 1$ and its reciprocal, through their complete search for the primitive trinomials of degrees 756839, 859433, and 3021377 [1]. (The primitivity of the above trinomial was confirmed by our corrected code, too.) Their current search is shown on the website

http://web.comlab.ox.ac.uk/oucl/work/richard.brent/trinom.html.

2. New primitive pentanomials

Here we report that the following primitive pentanomials (see Table 1 on the next page) have been found by the method described in [2].

Acknowledgments

We would like to thank Professor R. Brent and his colleagues for pointing out our error.

Received by the editor May 10, 2001.

2000 *Mathematics Subject Classification.* Primary 11-04, 11T06, 12-04, 12E05.

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

TABLE 1. Some of p, q_1, q_2, q_3 for which $X^p + X^{q_1} + X^{q_2} + X^{q_3} + 1$ is primitive over $GF(2)$

p	q_1	q_2	q_3
44497	28473	25357	6183
44497	28927	18413	7668
44497	33021	19223	12151
44497	34275	26980	9923
44497	35043	27313	6311
44497	38802	23900	6536
86243	61388	32606	26237
86243	61995	49334	25248
86243	65723	41510	30407
86243	67935	50330	22621
86243	68677	42129	11704
86243	69017	46561	26682
86243	69098	41740	13977
86243	69453	41544	12701
86243	69615	51770	17232

p	q_1	q_2	q_3
110503	71270	66923	19978
110503	75061	42595	36334
110503	77029	67563	40579
110503	78339	65279	14642
110503	78832	42854	27560
110503	80053	48219	27930
110503	80069	42319	32108
110503	81999	66969	26952
110503	88763	63837	31613
110503	89629	48590	20837
110503	89758	57438	39069
110503	92048	53327	15882
110503	92797	61896	21698
110503	93253	61728	21110
110503	93750	46605	29808
110503	95508	64105	37825

REFERENCES

1. R. P. Brent, S. Larvala and P. Zimmermann, *A fast algorithm for testing irreducibility of trinomials mod* 2 (preliminary report), Report PRG TR-13-00, 30 December 2000. Available from `http://web.comlab.ox.ac.uk/oucl/work/richard.brent/pub/pub199.html`.
2. T. Kumada, H. Leeb, Y. Kurita and M. Matsumoto, *New primitive t-nomials* ($t = 3, 5$) *over* $GF(2)$ *whose degree is a Mersenne exponent*, Math. Comp. **69** (2000), no. 230, 811–814. MR **2000i:**11183

DAIWA INSTITUTE OF RESEARCH LTD. 15-6 FUYUKI, KOTO-KU, TOKYO 135-8460, JAPAN
E-mail address: `t.kumada@dir.co.jp`

INSTITUTE OF STATISTICS, UNIVERSITY OF VIENNA, UNIVERSITAETSSTR. 5, 1010 VIENNA, AUSTRIA
E-mail address: `Hannes.Leeb@univie.ac.at`

NIPPON ELECTRIC CONTROL EQUIPMENT INDUSTRIES ASSOCIATION, 2-1-17 HAMAMATSU-CHO, MINATO-KU, TOKYO 105-0013 JAPAN
E-mail address: `ykurit@attglobal.net`

DIVISION OF MATHEMATICS, INTEGRATED HUMAN STUDIES, KYOTO UNIVERSITY, KYOTO 606-8501 JAPAN
E-mail address: `matumoto@math.h.kyoto-u.ac.jp`