A PRIMITIVE TRINOMIAL OF DEGREE 6972593

RICHARD P. BRENT, SAMULI LARVALA, AND PAUL ZIMMERMANN

Abstract. The only primitive trinomials of degree 6972593 over GF(2) are $x^{6972593} + x^{3037958} + 1$ and its reciprocal.

1. Introduction

This note extends the computation [2], to which we refer for motivations, definitions, historical comments and additional references. All polynomials are assumed to be in $Z_2[x]$. When considering trinomials $T(x) = x^r + x^s + 1$, we assume that $1 \le s \le \lfloor r/2 \rfloor$, so we disregard the reciprocal trinomial $x^r T(1/x) = x^r + x^{r-s} + 1$.

We restrict our attention to Mersenne exponents r, for which $2^r - 1$ is prime. Trinomials $x^r + x^s + 1$ whose degree is a Mersenne exponent $r \le 3021377$ are considered in [2, 3, 4]. Here we consider the next Mersenne exponent $r = 6972593$. According to the GIMPS project [7], 6972593 is the only Mersenne exponent in the interval $(3021377, 10^7)$.

2. Computational results

Using the algorithm of [2, §4], a search for irreducible trinomials of degree $r = 6972593$ was started in February 2001 and completed in July 2003. Sieving eliminated all but 236244 (6.78%) of the $\lfloor r/2 \rfloor = 3486296$ candidate trinomials and took about 5% of the total time. In most cases we sieved up to degree 26.

For the 236244 candidate trinomials $T(x)$ not eliminated by sieving, we computed $x^{2^r} \bmod T(x)$: since r is prime, $T(x)$ is irreducible iff $x^{2^r} = x \bmod T(x)$. In some cases we tested the reciprocal of $T(x)$ instead of $T(x)$, see [2, Thm. 2 & §4].

One primitive trinomial,

$$T(x) = x^{6972593} + x^{3037958} + 1,$$

was found on August 31, 2002. Our computations show that this is the only primitive trinomial of degree 6972593, apart from its reciprocal.

The computation was performed on an average of about 300 processors and took approximately 230000 Mips-years (17.8 times as long as for $r = 3021377$).

3. Checking the results

It is important to check the results of such a long computation to detect human, software and/or hardware errors [4, 5, 7]. Most software that can be used to compute irreducible/primitive trinomials is impractical for degrees as large as

1991 *Mathematics Subject Classification.* Primary 11B83; Secondary 11-04, 11N35, 11R09, 11T06, 11Y55, 12-04.

Key words and phrases. Irreducible trinomials, primitive trinomials, Mersenne numbers.

Version of 5 October 2003. To appear in *Mathematics of Computation.*

6972593 because of inefficient use of memory or non-optimized algorithms. NTL [6] is the only general-purpose package that we have found capable of checking the irreducibility of a trinomial of degree 6972593 over Z_2, and NTL takes three times longer than our program `irred` (13 hours versus 4.33 hours on an 833 Mhz Alpha EV68 to verify our primitive trinomial).

The log files for $r = 6972593$ and other Mersenne exponents less than 10^7 are available on our web site [1], along with details of the checks performed. Any discrepancies found during checking will be reported there.

Acknowledgements. The following institutions and individuals contributed to the computing task (approximate percentages in parentheses): Centre Informatique National de l'Enseignement Supérieur (30%); Oxford Supercomputing Centre (26%); Oxford Centre for Computational Finance (19%); Oxford University Computing Laboratory (14%); Australian Partnership for Advanced Computing, courtesy of Brendan McKay (9%); Juan Luis Varona (1.3%); Barry Mead (0.4%); Nicolas Daminelli (0.2%); and Nate Begeman (0.1%). Nate also ported our program to the Mac G4, using Motorola's AltiVec ISA extension to the PowerPC processor. We thank Philippe Falandry for assistance in compiling our program on the IBM SP in 64-bit mode, Julian Seward and Andrew Tridgell for their assistance in running the `valgrind` simulator, Victor Shoup for his NTL package [6], George Woltman and the GIMPS project [7] for providing information on Mersenne exponents, and an anonymous referee for encouraging us to make the text more succinct. The first author acknowledges the support of EPSRC Grant GR/N35366/01.

References

[1] R. P. Brent, Search for primitive trinomials, `http://www.comlab.ox.ac.uk/oucl/work/richard.brent/trinom.html`.

[2] R. P. Brent, S. Larvala and P. Zimmermann, A fast algorithm for testing reducibility of trinomials mod 2 and some new primitive trinomials of degree 3021377, *Math. Comp.* **72** (2003), 1443–1452. MR 1972745.

[3] R. P. Brent and P. Zimmermann, Algorithms for finding almost irreducible and almost primitive trinomials, in *Primes and Misdemeanours: Lectures in Honour of the Sixtieth Birthday of Hugh Cowie Williams*, Fields Institute, Toronto, 2004, to appear.

[4] 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), 811–814. MR **2000i:**11183. Corrigenda: *ibid* **71** (2002), 1337–1338. MR **2003c:**11153.

[5] T. J. Nicely, Enumeration to 10^{14} of the twin primes and Brun's constant, *Virginia Journal of Science* **46** (1995), 195–204. MR **97e:**11014.

[6] V. Shoup, NTL: A library for doing number theory (version 5.3.1), `http://www.shoup.net/ntl/`.

[7] G. Woltman *et al.*, GIMPS, The Great Internet Mersenne Prime Search, `http://www.mersenne.org/`.

Oxford University Computing Laboratory, Oxford OX1 3QD, UK
E-mail address: `trinomials@rpbrent.co.uk`

Helsinki University of Technology, Espoo, Finland
E-mail address: `slarvala@cc.hut.fi`

LORIA/INRIA Lorraine, 615 rue du jardin botanique, BP 101, F-54602 Villers-lès-Nancy, France
E-mail address: `Paul.Zimmermann@loria.fr`