Twelve new primitive binary trinomials

Richard Brent, Paul Zimmermann

TWELVE NEW PRIMITIVE BINARY TRINOMIALS

RICHARD P. BRENT AND PAUL ZIMMERMANN

Abstract. We exhibit twelve new primitive trinomials over GF(2) of record degrees 42 643 801, 43 112 609, and 74 207 281. In addition we report the first Mersenne exponent not ruled out by Swan's theorem [10] — namely 57 885 161 — for which none primitive trinomial exists. This completes the search for the currently known Mersenne prime exponents.

Primitive trinomials of degree up to 32 582 657 were reported in [5]. We have completed a search for all new Mersenne prime exponents found by the GIMPS project [7]. Twelve new primitive trinomials were found (see Table 1).

r	s	Notes
42 643 801	55981, 3706066, 3896488, 12899278, 20150445	Brent and Zimmermann, 2009
43 112 609	3569337, 4463337, 17212521, 21078848	Brent and Zimmermann, 2009
57 885 161	none	Brent and Zimmermann, 2013
74 207 281	9156813, 9999621, 30684570	Brent and Zimmermann, 2016

Table 1. New primitive trinomials x^r+x^s+1 of degree a Mersenne exponent r, for $s \le r/2$. For smaller exponents, see references in [5] or our web site [1].

Our search used the new algorithm [4] relying on fast arithmetic in GF(2)[x], whose details are given in [2]. For the squaring of polynomials over GF(2)[x], we used the new `_pdep_u64` Intel intrinsic, which gave a speedup of a factor about 2.5 over the algorithm described in [3, §4]. On a 3.3Ghz Intel Core i5-4590, together with improvements in the `gf2x` library, we were able to square a degree-74 207 280 polynomial in about 2 milliseconds, and to multiply two such polynomials in about 700 milliseconds. As in [5], we produced certificates for non-primitive trinomials, which were checked independently with Magma and NTL (a certificate is simply an encoding of a nontrivial factor of smallest degree). A 3.3Ghz Intel Core i5-4590 takes only 22 minutes to check the certificates of all 37 103 637 reducible trinomials ($s \le r/2$) of degree $r = 74\,207\,281$ with our `check-ntl` program based on NTL [9], the largest factor having degree 19 865 299 for $s = 9\,788\,851$.

Acknowledgements. The authors thank Allan Steel, who independently verified with Magma the twelve new primitive trinomials, and Grégoire Lecerf who verified with Mathemagix the three primitive trinomials of degree 74 207 281. Part of the computations reported in this paper were carried out using a cluster funded by the French ANR CatRel.

1991 *Mathematics Subject Classification.* Primary 11B83, 11Y16; Secondary 11-04, 11N35, 11R09, 11T06, 11Y55, 12-04.

Key words and phrases. GF(2)[x], trinomials, irreducible polynomials, primitive polynomials, Mersenne numbers.

References

[1] Richard P. Brent, *Search for primitive trinomials (mod 2)*, `http://wwwmaths.anu.edu.au/~brent/trinom.html`, 2008.

[2] Richard Brent, Pierrick Gaudry, Emmanuel Thomé, and Paul Zimmermann, *Faster multiplication in* GF(2)[x], Proc. of the 8th International Symposium on Algorithmic Number Theory (ANTS VIII), *Lecture Notes in Computer Science* **5011**, Springer-Verlag, 2008, 153–166.

[3] Richard P. Brent, Samuli Larvala, and Paul 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. MR1972745 (2004b:11161)

[4] Richard Brent and Paul Zimmermann, *A multi-level blocking distinct degree factorization algorithm*, Contemporary Mathematics **461** (2008), 47–58.

[5] ———, *Ten new primitive trinomials*, Math. Comp. **78** (2008), 1197–1199.

[6] ———, *The Great Trinomial Hunt*, Notices of the AMS **58:2** (2011), 233–239.

[7] The Great Internet Mersenne Prime Search, `mersenne.org`.

[8] Y. Kurita and M. Matsumoto, *Primitive t-nomials* ($t = 3, 5$) *over* GF(2) *whose degree is a Mersenne exponent* ≤ 44497, Math. Comp. **56** (1991), 817–821. MR1068813 (91h:11138)

[9] Victor Shoup, *NTL: A library for doing number theory*, `http://www.shoup.net/ntl/`, 2016.

[10] R. G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. **12** (1962), 1099–1106. MR0144891 (26 #2432)

Australian National University, Canberra, Australia
E-mail address: `trinomials@rpbrent.com`

Inria Nancy - Grand Est, Villers-lès-Nancy, France
E-mail address: `Paul.Zimmermann@inria.fr`