Twelve new primitive binary trinomials
Richard P Brent, Paul Zimmermann

To cite this version:
Richard P Brent, Paul Zimmermann. Twelve new primitive binary trinomials. 2016. hal-01378493

HAL Id: hal-01378493
https://inria.hal.science/hal-01378493
Preprint submitted on 10 Oct 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
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).

<table>
<thead>
<tr>
<th>$r$</th>
<th>$s$</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>42 643 801</td>
<td>55981, 3706066, 3896588, 12899278, 20150445</td>
<td>Brent and Zimmermann, 2009</td>
</tr>
<tr>
<td>43 112 609</td>
<td>3569337, 4463337, 17212521, 21078848</td>
<td>Brent and Zimmermann, 2009</td>
</tr>
<tr>
<td>57 885 161</td>
<td>none</td>
<td>Brent and Zimmermann, 2013</td>
</tr>
<tr>
<td>74 207 281</td>
<td>9156813, 9999621, 30684570</td>
<td>Brent and Zimmermann, 2016</td>
</tr>
</tbody>
</table>

Table 1. New primitive trinomials $x^r+x^s+1$ of degree a Mersenne exponent $r$, for $s \leq r/2$. 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 ($s \leq r/2$) 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.


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


[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)


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