TEN NEW PRIMITIVE BINARY TRINOMIALS

RICHARD P. BRENT AND PAUL ZIMMERMANN

ABSTRACT. We exhibit ten new primitive trinomials over GF(2) of record degrees 24 036 583, 25 964 951, 30 402 457, and 32 582 657. This completes the search for the currently known Mersenne prime exponents.

Primitive trinomials of degree up to 6 972 593 were previously known [4]. We have completed a search for all known Mersenne prime exponents [7]. Ten new primitive trinomials were found. Our results are summarized in the following theorem:

Theorem 1. For the integers $r$ listed in Table 1, the primitive trinomials $x^r + x^s + 1$ of degree $r$ over GF(2) are exactly those given in Table 1, and the corresponding reciprocal trinomials $x^r + x^{r-s} + 1$.

Proof. From the GIMPS Project [7], the integers $r$ listed in Table 1 are exponents of Mersenne primes $2^r - 1$. Thus, irreducible trinomials of degree $r$ are necessarily primitive. Irreducibility of the trinomials listed in Table 1 follows from the authors’ computations, using the new algorithm described in [5, 6] (verified using the algorithm of [3] and independently verified by Allan Steel using Magma). Finally, the fact that no irreducible trinomials were missed during the search, for those degrees $r$, follows from the certificates given on the authors’ web pages [1].

Remarks. The integers $r$ listed in Table 1 are the known Mersenne exponents of the form $r = \pm 1 \mod 8$ in the interval [100 000, 32 582 657]. For smaller exponents, omitted to save space, see [10] or our web site [4]. According to the GIMPS Project [7], the list is complete for $r \leq 16 300 000$. Known Mersenne exponents of the form $r = \pm 3 \mod 8$ for $r > 5$ cannot be the degrees of irreducible trinomials due to Swan’s theorem [12]; the possibility $x^r + x^2 + 1$ permitted by Swan’s theorem is easily ruled out in all known cases with $r > 5$; see the authors’ web site [4].

Our search used a new algorithm [5, 6] relying on fast arithmetic in GF(2)[x], whose details are given in [1]. Another significant improvement over previous work is that certificates were produced; this enables one to check easily that the claimed nonprimitive trinomials are indeed reducible. A certificate is simply an encoding of a nontrivial factor of smallest degree. A 2.4Ghz Intel Core 2 takes only 15 minutes to check the certificates of all 16 291 325 reducible trinomials ($s \leq r/2$) of degree $r = 32 582 657$ with our check-ntl program based on NTL [1].

Received by the editor April 15, 2008.

2000 Mathematics Subject Classification. Primary 11B83, 11Y16; Secondary 11-04, 11T06, 11Y55, 12-04.

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

©2008 American Mathematical Society
Reverts to public domain 28 years from publication
Table 1. Known primitive trinomials \( x^r + x^s + 1 \) whose degree is a Mersenne exponent \( r \geq 100000 \), for \( s \leq r/2 \).

<table>
<thead>
<tr>
<th>( r )</th>
<th>( s )</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>110503</td>
<td>25230, 53719</td>
<td>Heringa et al. [8]</td>
</tr>
<tr>
<td>132049</td>
<td>7000, 33912, 41469, 52549, 54454</td>
<td>Heringa et al. [8]</td>
</tr>
<tr>
<td>756839</td>
<td>215747, 267428, 279695</td>
<td>Brent et al. [9]</td>
</tr>
<tr>
<td>859433</td>
<td>170340, 288477</td>
<td>Brent et al. [3], Kumada et al. [9]</td>
</tr>
<tr>
<td>3021377</td>
<td>361604, 1010202</td>
<td>Brent et al. [3]</td>
</tr>
<tr>
<td>6972593</td>
<td>307958</td>
<td>Brent et al. [4]</td>
</tr>
<tr>
<td>24036583</td>
<td>8412642, 8755528</td>
<td>Brent and Zimmermann, 2007</td>
</tr>
<tr>
<td>25964951</td>
<td>880890, 4627670, 4830131, 6383880</td>
<td>Brent and Zimmermann, 2007</td>
</tr>
<tr>
<td>30402457</td>
<td>2162059</td>
<td>Brent and Zimmermann, 2007</td>
</tr>
<tr>
<td>32582657</td>
<td>5110722, 5552421, 7545455</td>
<td>Brent and Zimmermann, 2008</td>
</tr>
</tbody>
</table>

Acknowledgements

The authors thank Allan Steel, who independently verified (with Magma) the ten new primitive trinomials, and the authors of the Magma and NTL software tools that were used to check reducibility of the other trinomials. Part of the computations reported in this paper were carried out using the Grid’5000 experimental testbed, an initiative of the French Ministry of Research through the ACI GRID incentive action, INRIA, CNRS and RENATER and other contributing partners (see https://www.grid5000.fr). The work of the first author was supported by the Australian Research Council.

References


[10] Y. Kurita and M. Matsumoto, Primitive t-nomials (\( t = 3, 5 \)) over GF(2) whose degree is a Mersenne exponent \( \leq 44497 \), 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@loria.fr