COMPUTING AURIFEUILLIAN FACTORS

RICHARD P. BRENT

Abstract

For odd square-free $n > 1$, the cyclotomic polynomial $\Phi_n(x)$ satisfies an identity

$$\Phi_n(x) = C_n(x)^2 \pm nxD_n(x)^2$$

of Aurifeuille, Le Lasseur and Lucas. Here $C_n(x)$ and $D_n(x)$ are monic polynomials with integer coefficients. These coefficients can be computed by simple algorithms which require $O(n^2)$ arithmetic operations over the integers. Also, there are explicit formulas and generating functions for $C_n(x)$ and $D_n(x)$. This paper is a preliminary report which states the results for the case $n = 1 \bmod 4$, and gives some numerical examples. The proofs, generalisations to other square-free n, and similar results for the identities of Gauss and Dirichlet, will appear in [2].

Comments

Only the Abstract is given here. The full paper will appear as [1]. For a more comprehensive (but more difficult) paper, see [2].

References

[1] R. P. Brent, "Computing Aurifeuillian factors" *Proceedings of a Conference on Computational Algebra and Number Theory*, held at Sydney University, November 1992 (edited by W. Bosma and A. van der Poorten), to appear. rpb127.

[2] R. P. Brent, "On computing factors of cyclotomic polynomials", *Mathematics of Computation* (D. H. Lehmer memorial issue), 1993, to appear. rpb135.

Computer Sciences Laboratory, Australian National University, Canberra

E-mail address: `rpb@cslab.anu.edu.au`

1991 *Mathematics Subject Classification.* Primary 12E10; Secondary 05A15, 11-04, 11T06, 11T22, 11T24, 11Y16, 12-04, 12Y05.

Key words and phrases. Aurifeuillian factorization, class number, cyclotomic field, cyclotomic polynomial, exact computation, generating functions, integer factorization, Newton's identities.

rpb127a typeset using $\mathcal{A}\mathcal{M}\mathcal{S}$-LaTeX.