ON COMPUTING FACTORS OF CYCLOTOMIC POLYNOMIALS

RICHARD P. BRENT

In memory of
Derrick H. Lehmer
1905–1991

Abstract

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

$$4\Phi_n(x) = A_n^2 - (-1)^{(n-1)/2} n B_n^2.$$

A similar identity of Aurifeuille, Le Lasseur and Lucas is

$$\Phi_n((-1)^{(n-1)/2} x) = C_n^2 - nxD_n^2$$

or, in the case that n is even and square-free,

$$\pm\Phi_{n/2}(-x^2) = C_n^2 - nxD_n^2.$$

Here $A_n(x), \ldots, D_n(x)$ are polynomials with integer coefficients. We show how these coefficients can be computed by simple algorithms which require $O(n^2)$ arithmetic operations and work over the integers. We also give explicit formulae and generating functions for $A_n(x), \ldots, D_n(x)$, and illustrate the application to integer factorization with some numerical examples.

Comments

Only the Abstract is given here. The full paper will appear as [2]. For a preliminary report and additional numerical examples, see [1].

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, ACT 0200
E-mail address: rpb@cslab.anu.edu.au

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

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

rpb135a typeset using $\mathcal{AMS}$-LaTeX.