On computing factors of cyclotomic polynomials*†

Richard P. Brent
Computer Sciences Laboratory
Australian National University
Canberra, ACT 0200
rpb@cslab.anu.edu.au

Report TR-CS-92-13
September 1992

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.

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.

*To appear in *Mathematics of Computation* D. H. Lehmer memorial issue, 1993.
 rpb135 typeset using LaTeX

1 Introduction

For integer $n > 0$ let $\Phi_n(x)$ denote the cyclotomic polynomial

$$\Phi_n(x) = \prod_{\substack{0<j\le n \\ (j,n)=1}} (x - \zeta^j), \tag{1}$$

where ζ is a primitive n-th root of unity. Clearly

$$x^n - 1 = \prod_{d|n} \Phi_d(x), \tag{2}$$

and the Möbius inversion formula [13] gives

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}. \tag{3}$$

Equation (1) is useful for theoretical purposes, but (3) is more convenient for computation as it leads to a simple algorithm for computing the coefficients of $\Phi_n(x)$ or evaluating $\Phi_n(x)$ at integer arguments using only integer arithmetic. If n is square-free the relations

$$\Phi_n(x) = \begin{cases} x - 1, & \text{if } n = 1; \\ \Phi_{n/p}(x^p)/\Phi_{n/p}(x), & \text{if } p|n,\ p \text{ prime}; \end{cases} \tag{4}$$

give another convenient recursion for computing $\Phi_n(x)$.

Although $\Phi_n(x)$ is irreducible over Z (see for example [29]), $\Phi_n(x)$ may be reducible over certain quadratic fields. For example,

$$4\Phi_5(x) = (2x^2 + x + 2)^2 - 5x^2, \tag{5}$$

so $\Phi_5(x)$ has factors $x^2 + \left(\frac{1\pm\sqrt{5}}{2}\right) x + 1$ whose coefficients are algebraic integers in $Q[\sqrt{5}]$.

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

$$4\Phi_n(x) = A_n^2 - (-1)^{(n-1)/2} n B_n^2. \tag{6}$$

Gauss [12] proved (6) for odd prime n; the generalization to other odd square-free n is due to Dirichlet [11]. Related identities of Aurifeuille and Le Lasseur [2] are

$$\Phi_n((-1)^{(n-1)/2} x) = C_n^2 - n x D_n^2 \tag{7}$$

for odd square-free n, and

$$\Phi_{n/2}(-x^2) = C_n^2 - n x D_n^2 \tag{8}$$

for even square-free $n > 2$. For a proof, see Lucas [22] or Schinzel [26].

In (6–8), $A_n(x), \ldots, D_n(x)$ are polynomials with integer coefficients, and without loss of generality we can assume that $A_n(x)/2$, $B_n(x)$, $C_n(x)$ and $D_n(x)$ are monic. In Section 3 we show how the coefficients of $A_n, \ldots, D_n$ can be computed by simple algorithms which require $O(n^2)$ arithmetic operations and work entirely over the integers.

In Section 1.1 we summarize our notation for future reference. Some numerical examples are given in Sections 1.2–1.3, and Newton's identities are discussed in Section 1.4. Then, in Section 2, we discuss the theoretical basis for the algorithms. The results for A_n and B_n are known (though perhaps forgotten) – they may be found in Dirichlet [11]. We present them in Section 2.2 for the sake of completeness and to aid the reader in understanding the results for C_n and D_n.

The algorithms are presented in Section 3. The algorithm (Algorithm D) for computing A_n and B_n is essentially due to Dirichlet [11], who illustrated it with some numerical examples but did not state it in general terms. The algorithm (Algorithm L) for computing C_n and D_n appears to be new. In Section 3.3 we comment briefly on Stevenhagen's algorithm [27] and compare it with Algorithm L.

Finally, in Section 4 we give some explicit formulas for $A_n(x), \ldots, D_n(x)$. These may be regarded as generating functions if x is an indeterminate, or may be used to compute $A_n(x), \ldots, D_n(x)$ for given argument x. In the special case $x = 1$ the results for $A_n(1), B_n(1)$ reduce to known formulas involving the class number of the quadratic field $Q[\sqrt{\pm n}]$.

One application of cyclotomic polynomials is to the factorization of integers of the form $a^n \pm b^n$: see for example [6, 7, 8, 9, 15, 16, 24, 26, 27]. If $x = m^2 n$ for any integer m, then (7–8) are differences of squares, giving rational integer factors of $x^n \pm 1$. Examples may be found in Section 4.4. For the reader interested in integer factorization, our most significant results are Algorithm L of Section 3.2 and Theorem 3 of Section 4.4.

1.1 Notation

Unless qualified by "algebraic", the term "integer" means a rational integer. x usually denotes an indeterminate, occasionally a real or complex variable.

$\mu(n)$ denotes the Möbius function, $\phi(n)$ denotes Euler's totient function, and (m, n) denotes the greatest common divisor of m and n. For definitions and properties of these functions, see for example [13]. Note that $\mu(1) = \phi(1) = 1$.

$(m|n)$ denotes the Jacobi symbol[1] except that, as is usual for the Kronecker symbol[2], $(m|n)$ is defined as 0 if $(m, n) > 1$. Thus, when specifying a condition such as $(m|n) = 1$ we may omit the condition $(m, n) = 1$.

n denotes a positive integer (square-free from Section 2.2 on). For given n, we define integers n', s and s' as follows:

$$n' = \begin{cases} n, & \text{if } n = 1 \bmod 4; \\ 2n, & \text{otherwise.} \end{cases}$$

$$s = \begin{cases} -1, & \text{if } n = 3 \bmod 4; \\ +1, & \text{otherwise.} \end{cases}$$

$$s' = \begin{cases} -1, & \text{if } n = 5 \bmod 8; \\ +1, & \text{otherwise.} \end{cases}$$

It is convenient to write g_k for (k, n) and g'_k for (k, n').

Define

$$F_n(x) = \begin{cases} \Phi_n(sx), & \text{if } n \text{ is odd;} \\ (-1)^{\phi(n/2)}\Phi_{n/2}(-x^2), & \text{if } n \text{ is even.} \end{cases} \tag{9}$$

Thus we can write (7–8) as

$$F_n(x) = C_n^2 - nxD_n^2. \tag{10}$$

The factor $(-1)^{\phi(n/2)}$ in the definition of F_n is only relevant if $n = 2$, and ensures that (10) is valid for $n = 2$ (with $C_2(x) = x + 1$, $D_2(x) = 1$). The Aurifeuillian factors of $F_n(x)$ are

$$F_n^+(x) = C_n(x) + \sqrt{nx}\,D_n(x)$$

and

$$F_n^-(x) = C_n(x) - \sqrt{nx}\,D_n(x).$$

[1]See, for example, Riesel [24]. To avoid ambiguity, we *never* write the Jacobi symbol as $\left(\frac{m}{n}\right)$. Note that $m|n$ without parentheses means that m divides n.

[2]See, for example, Landau [18].

From (10) we have $F_n(x) = F_n^-(x)F_n^+(x)$. We may write $F_n^\pm$ for one of F_n^+, F_n^-.

We sometimes need to specify a particular complex square root. If $m < 0$ then $\sqrt{m}$ means $i\sqrt{|m|}$.

d is usually the degree of a polynomial, while D is the discriminant of a quadratic form. For odd square-free n we always have $D = sn$, so $D = 1 \bmod 4$.

Some additional notation is introduced in Section 1.4.

1.2 Examples

Taking $n = 15$, we have

$$\Phi_{15}(x) = \frac{(x^{15}-1)(x-1)}{(x^5-1)(x^3-1)} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1,$$

$$A_{15}(x) = 2x^4 - x^3 - 4x^2 - x + 2,$$

$$B_{15}(x) = x^3 - x,$$

$$C_{15}(x) = x^4 + 8x^3 + 13x^2 + 8x + 1,$$

$$D_{15}(x) = x^3 + 3x^2 + 3x + 1,$$

and the reader may easily verify that (6) and (7) are satisfied. As an example of (8), for $n = 14$ we have

$$F_{14}(x) = \Phi_7(-x^2) = \frac{x^{14}+1}{x^2+1} = x^{12} - x^{10} + x^8 - x^6 + x^4 - x^2 + 1,$$

$$C_{14}(x) = x^6 + 7x^5 + 3x^4 - 7x^3 + 3x^2 + 7x + 1,$$

and

$$D_{14}(x) = x^5 + 2x^4 - x^3 - x^2 + 2x + 1.$$

1.3 The identities of Beeger and Schinzel

Taking $n = 5$ in (7) we obtain

$$\Phi_5(x) = (x^2 + 3x + 1)^2 - 5x(x+1)^2,$$

so $\Phi_5(x^2)$ has factors $x^4 + 3x^2 + 1 \pm \sqrt{5}(x^3 + x)$ in $Q[\sqrt{5}]$. Replacing x by x^3 we obtain factors of $\Phi_5(x^6)$. Now

$$\Phi_{15}(x^2) = \Phi_5(x^6)/\Phi_5(x^2),$$

and by division (taking the factors with opposite signs of $\sqrt{5}$) we obtain factors

$$x^8 + 2x^6 + 3x^4 + 2x^2 + 1 \pm \sqrt{5}(x^7 + x^5 + x^3 + x)$$

of $\Phi_{15}(x^2)$. Thus

$$\Phi_{15}(x) = (x^4 + 2x^3 + 3x^2 + 2x + 1)^2 - 5x(x^3 + x^2 + x + 1)^2. \tag{11}$$

This is not of the form (10) because it gives a factorization of $\Phi_{15}(\pm x)$ over $Q[\sqrt{\pm 5}]$ instead of $Q[\sqrt{\mp 15}]$. Instead, (11) is an example of the more general identities of Beeger [3] and Schinzel [26]. These identities can all be obtained in a similar manner from (10), so in the application to integer factorization they do not give any factors which could not be found from several applications of (10) and some greatest common divisor calculations. For this reason we have restricted our attention to identities of the form (6) and (10).

1.4 Newton's identities

Let

$$P(x) = \prod_{j=1}^{d}(x - \xi_j) = \sum_{j=0}^{d} a_j x^{d-j}$$

be a polynomial of degree d with arbitrary roots ξ_j and coefficients $a_0 = 1, a_1, \ldots, a_d$.

For $k > 0$, define

$$p_k = \sum_{j=1}^{d} \xi_j^k. \tag{12}$$

Newton (1707)[3] showed how to express the elementary symmetric functions $a_1, a_2, \ldots$ in terms of the sums of powers $p_1, p_2, \ldots$

We may find $a_1, \ldots, a_d$ by solving a lower triangular linear system of special form [28]. Writing the solution explicitly in the form of a linear recurrence, we have

$$ka_k = -\sum_{j=0}^{k-1} p_{k-j} a_j \tag{13}$$

for $k = 1, \ldots, d$. An alternative expression for a_k as a determinant may be obtained by applying Cramer's rule to the lower triangular system. However, for computational purposes (13) is more convenient.

In Section 4 we use the following generating function [25] for $(a_0, a_1, \ldots)$:

$$x^d P(1/x) = \sum_{j=0}^{d} a_j x^j = \exp\left(-\sum_{j=1}^{\infty} p_j x^j / j\right) \tag{14}$$

Differentiating both sides of (14) and equating coefficients shows that (13) and (14) are formally equivalent. An independent proof of (14) is the following: for sufficiently small x we have

$$\ln(x^d P(1/x)) = \sum_{k=1}^{d} \ln(1 - \xi_k x) = -\sum_{k=1}^{d}\sum_{j=1}^{\infty} \xi_k^j x^j / j = -\sum_{j=1}^{\infty}\left(\sum_{k=1}^{d} \xi_k^j\right) x^j / j = -\sum_{j=1}^{\infty} p_j x^j / j.$$

In all our applications of (14) the p_j are bounded, so the infinite series converges for $|x| < 1$.

In the following, p_j and a_j are not fixed, but depend on the particular polynomial under consideration at the time. This should not cause any confusion.

2 Theoretical Basis for the Algorithms

Our idea is to compute sums of powers of certain roots of the polynomials occurring on the left side of (6) and (10), and then use Newton's identities in the form (13) to compute the coefficients of $A_n, \ldots, D_n$.

2.1 Cyclotomic polynomials

First consider the computation of the coefficients of the cyclotomic polynomial $\Phi_n(x)$ for $n > 1$. This is presented to illustrate a simple case of the technique; in practice it is more efficient to compute $\Phi_n(x)$ from (3).

[3] See Turnbull [28], where the notation s_k is used in place of our p_k. It would be confusing to use Turnbull's notation because we have used s and s' for other purposes. Note that our p_k are *not* generally prime numbers.

Let ζ be a primitive n-th root of unity. To apply Newton's identities we need to evaluate

$$p_k = \sum_{\substack{0<j<n \\ (j,n)=1}} \zeta^{jk} \tag{15}$$

for $k = 1, 2, \ldots, \phi(n)$. This problem is well-known[4].

If n is prime the problem is easy: from

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{n-1} = \frac{1-\zeta^n}{1-\zeta} = 0,$$

we have $p_1 = -1$. Moreover, for any k with $(k,n) = 1$, the map $z \mapsto z^k$ merely permutes $\{\zeta, \ldots, \zeta^{n-1}\}$, so $p_k = p_1$.

Now consider the general case, n not necessarily prime. From (3) it is clear that $p_1 = \mu(n)$. Let $g_k = (k,n)$. If $g_k = 1$ then the same argument as before shows that $p_k = p_1$. If $g_k > 1$ then the sum (15) defining p_k consists of $\phi(n)/\phi(n/g_k)$ copies of a sum of primitive (n/g_k)-th roots of unity. Thus, the result is

$$p_k = \frac{\mu(n/g_k)\phi(n)}{\phi(n/g_k)}. \tag{16}$$

Using (16) the coefficients $a_1, \ldots, a_{\phi(n)}$ of $\Phi_n(x)$ may be evaluated from the recurrence (13).

As an application of (14) and (16) we prove two Lemmas which give upper bounds on $|\Phi_n(x)|$ and $|F_n(x)|$ for complex x outside the unit circle. Here $F_n(x)$ is the modified cyclotomic polynomial defined by (9). Lemma 2 is used in Section 4.4.

Lemma 1 *If $|x| \ge R > 1$ then*

$$|\Phi_n(x)| < R^{\phi(n)} \exp\left(\frac{1}{R-1}\right).$$

Proof

Let $d = \phi(n)$. From (14) with x replaced by $1/x$, we have

$$\Phi_n(x)/x^d = \exp\left(-\sum_{j=1}^{\infty} p_j x^{-j}/j\right),$$

but from (16) we have

$$|p_j| \le g_j \le \min(j, n),$$

so

$$|\Phi_n(x)/x^d| < \exp\left(\sum_{j=1}^{\infty} R^{-j}\right) = \exp\left(\frac{1}{R-1}\right).$$

This completes the proof. $\square$

Lemma 2 *If $n > 1$ is square-free and $|x| \ge R > 1$ then*

$$|F_n(x)| < R^{\phi(2n)} \exp\left(\frac{1}{R-1}\right).$$

[4] If $\zeta = e^{2\pi i/n}$ then our p_k is "Ramanujan's sum" $c_n(k)$, in the notation of Ramanujan [23] or Chapter 26 of Davenport [10].

Proof

From the definition (9) of $F_n(x)$,

$$\deg\, F_n = \begin{cases} \phi(n), & \text{if } n \text{ is odd;} \\ 2\phi(n/2), & \text{if } n \text{ is even;} \end{cases}$$

so it is easy to see that

$$\deg\, F_n = \phi(2n)$$

in both cases. The bound on $|F_n(x)|$ follows from Lemma 1 applied to $\Phi_n(\pm x)$ if n is odd, and from Lemma 1 applied to $\Phi_{n/2}(-x^2)$ if n is even. □

2.2 The identity of Gauss

From now on we assume that $n > 1$ is square-free. In this subsection we also assume that n is odd. Consider the polynomial

$$G_n(x) = \prod_{\substack{0<j<n \\ (j|n)=1}} (x - \zeta^j) \tag{17}$$

of degree $\phi(n)/2$, where $\zeta = e^{2\pi i/n}$ is a primitive n-th root of unity. The particular choice of primitive root is only significant for the sign of the square root of sn appearing in the equations below.

From Dirichlet [11],

$$2G_n(x) = A_n(x) - \sqrt{sn}B_n(x), \tag{18}$$

where A_n and B_n are as in (6), and s is defined in Section 1.1. Since n is odd, we have $s = (-1|n) = (-1)^{(n-1)/2}$.

Define

$$2\tilde{G}_n(x) = A_n(x) + \sqrt{sn}B_n(x), \tag{19}$$

so Gauss's identity (6) may be written as

$$\Phi_n(x) = G_n(x)\tilde{G}_n(x). \tag{20}$$

The sums of k-th powers of roots of $G_n(x)$ are

$$p_k = \sum_{\substack{0<j<n \\ (j|n)=1}} \zeta^{jk}. \tag{21}$$

Let $g_k = (k, n)$. Then

$$2p_k = \begin{cases} \mu(n) + (k|n)\sqrt{sn}, & \text{if } g_k = 1; \\ \mu(n/g_k)\phi(g_k), & \text{otherwise.} \end{cases} \tag{22}$$

The result (22) is essentially due to Dirichlet [11], but we sketch a proof. If $g_k = 1$, then (22) follows from the discussion in Section 2.1 (where p_k has a different meaning!) and the classical result that the Gaussian sum

$$\sum_{0<j<n} (j|n)\zeta^j$$

is $\sqrt{sn}$. On the other hand, if $g_k > 1$, observe that $(g_k, n/g_k) = 1$ because n is square-free. Thus, we can write the summation index j in (21) in the form $j = j_0 g_k + j_1(n/g_k)$, and $(j|n) = (j_1|g_k)(j_0|(n/g_k))$. Since $jk = j_0 g_k k \bmod n$, ζ^{jk} is independent of j_1, and it follows that the sum (21) defining p_k consists of $\phi(g_k)/2$ copies of a complete sum of primitive (n/g_k)-th roots of unity. Thus, (22) follows as in the proof of (16).

Although (22) has been written with two cases for the sake of clarity, our convention that $(k|n) = 0$ if $(k, n) > 1$ implies that the expression

$$2p_k = \mu(n/g_k)\phi(g_k) + (k|n)\sqrt{sn} \tag{23}$$

is valid in both cases. Similarly for $\tilde{G}_n(x)$, with the sign of $\sqrt{sn}$ in (23) reversed.

Observe that $p_k \in Q[\sqrt{n}]$ is real if $n = 1 \bmod 4$, but $p_k \in Q[\sqrt{-n}]$ is complex if $g_k = 1$ and $n = 3 \bmod 4$.

Using (22), the coefficients of $G_n(x)$, and hence of $A_n(x)$ and $B_n(x)$, may be evaluated from the recurrence (13). Moreover, it is possible to perform the computation using only integer arithmetic. Details are given in Section 3.

2.3 The identities of Aurifeuille, Le Lasseur and Lucas

Here we assume that $n > 1$ is square-free, but not necessarily odd. Recall the definitions of n', s and s' from Section 1.1.

Let $\zeta = e^{\pi i/n'}$ be a primitive $2n'$-th root of unity. The particular choice of primitive root is only significant for the sign of the square root in (29). Consider the polynomial

$$L_n(x) = \prod_{j \in S_n} (x - \zeta^j), \tag{24}$$

where

$$S_n = \begin{cases} \{j \mid 0 < j < 2n',\ (j, n') = 1,\ (j|n) = (-1)^j\}, & \text{if } n = 1 \bmod 4; \\ \\ \{j \mid 0 < j < 2n',\ (j, n') = 1,\ (n|j) = 1\}, & \text{otherwise.} \end{cases} \tag{25}$$

Observe that $L_n(x)$ has degree $\phi(n') = \phi(2n)$. Also, $j \in S_n$ iff $2n' - j \in S_n$, so the coefficients of $L_n(x)$ are real. In fact, from (29) below, they are in $Q[\sqrt{n}]$. We later use the fact that $L_n(x)$ is symmetric.

Schinzel [26] essentially shows (with a different notation) that

$$L_n(x) = C_n(x^2) - s'x\sqrt{n}D_n(x^2) \tag{26}$$

where $C_n(x)$ and $D_n(x)$ are the polynomials of (10). Define

$$\tilde{L}_n(x) = L_n(-x) = C_n(x^2) + s'x\sqrt{n}D_n(x^2), \tag{27}$$

so after a change of variable (10) may be written as

$$F_n(x^2) = L_n(x)\tilde{L}_n(x). \tag{28}$$

Clearly $F_n^-(x) = L_n(s'\sqrt{x})$ and $F_n^+(x) = \tilde{L}_n(s'\sqrt{x})$.

Let $g'_k = (k, n')$. The sums p_k of k-th powers of roots of $L_n(x)$ are

$$p_k = \begin{cases} (n|k)s'\sqrt{n}, & \text{if } k \text{ is odd;} \\ \mu(n'/g'_k)\phi(g'_k)\cos\left((n-1)k\pi/4\right), & \text{if } k \text{ is even.} \end{cases} \tag{29}$$

Observe that the cosine in (29) is 0 or ± 1, and depends only on $n \bmod 4$ and $k/2 \bmod 4$. The proof of (29) is similar to that of (22), but tedious because of the number of cases to be considered. Thus, we omit the details.

Using (29), the coefficients of $L_n(x)$, and hence of $C_n(x)$ and $D_n(x)$, may be evaluated from the recurrence (13). Details are given in Section 3.

3 Algorithms

In this section we use the analytic results of Section 2 to derive efficient algorithms for computing the coefficients of the polynomials $A_n, \ldots, D_n$.

3.1 An algorithm for computing A_n and B_n

Consider the computation of A_n and B_n for odd square-free n. Our notation is the same as in Section 2.2. Write

$$A_n(x) = \sum_{j=0}^{d} \alpha_j x^{d-j},$$

$$B_n(x) = \sum_{j=0}^{d} \beta_j x^{d-j},$$

where $d = \phi(n)/2$, $\alpha_0 = 2$, $\beta_0 = 0$, $\beta_1 = 1$.

Recall the definition (21) of p_k. For $k > 0$ we have, from (23),

$$2p_k = q_k + r_k\sqrt{sn},$$

where q_k and r_k are integers given by

$$q_k = \mu(n/g_k)\phi(g_k) \tag{30}$$

and

$$r_k = (k|n). \tag{31}$$

Using (13) and (18), we obtain the recurrences

$$\alpha_k = \frac{1}{2k}\sum_{j=0}^{k-1}(snr_{k-j}\beta_j - q_{k-j}\alpha_j) \tag{32}$$

and

$$\beta_k = \frac{1}{2k}\sum_{j=0}^{k-1}(r_{k-j}\alpha_j - q_{k-j}\beta_j) \tag{33}$$

for $k = 1, 2, \ldots, d$. The algorithm is now clear:

Algorithm D (for Dirichlet)

1. Evaluate q_k and r_k for $k = 1, \ldots, d$ using (30–31).
2. Set $\alpha_0 \leftarrow 2$ and $\beta_0 \leftarrow 0$.
3. Evaluate α_k and β_k for $k = 1, \ldots, d$ using (32–33).

Comments on Algorithm D

1. (32–33) should give exact integer results; in practice a sum not divisible by $2k$ is a symptom of integer overflow.
2. The operation count can be reduced by a factor of close to four if advantage is taken of the following properties of A_n and B_n:

A_n is anti-symmetric if its degree $d = \phi(n)/2$ is odd, otherwise A_n is symmetric (except for the trivial case $A_3(x) = 2x + 1$). Thus, we may use

$$\alpha_k = (-1)^d \alpha_{d-k}$$

if $2k > d$ and $n > 3$.

B_n/x is antisymmetric if n is composite and $n = 3 \bmod 4$, otherwise B_n/x is symmetric. Thus, we may use

$$\beta_k = \begin{cases} \beta_{d-k}, & \text{in the symmetric case;} \\ -\beta_{d-k}, & \text{in the anti-symmetric case.} \end{cases}$$

Using these properties, the recurrences (32–33) need only be applied for $k \le \max(1, \lfloor d/2 \rfloor)$.

Example

Consider the case $n = 15$ as in Section 1.2. We have $s = -1$, $d = \phi(15)/2 = 4$. Thus

$$q_1 = q_2 = q_4 = \mu(15)\phi(1) = 1,\ q_3 = \mu(5)\phi(3) = -2,$$

$$r_1 = (1|15) = 1,\ r_2 = (2|15) = (2|3)(2|5) = 1,\ r_3 = (3|15) = 0,\ r_4 = (4|15) = 1.$$

q_3, q_4, r_3, and r_4 are not required if we use symmetry.

The initial conditions are $\alpha_0 = 2$ and $\beta_0 = 0$. The recurrences (32–33) give

$$\alpha_1 = (-15 r_1 \beta_0 - q_1 \alpha_0)/2 = -1,$$

$$\beta_1 = (r_1 \alpha_0 - q_1 \beta_0)/2 = 1,$$

$$\alpha_2 = (-15 r_2 \beta_0 - 15 r_1 \beta_1 - q_2 \alpha_0 - q_1 \alpha_1)/4 = -4,$$

$$\beta_2 = (r_2 \alpha_0 + r_1 \alpha_1 - q_2 \beta_0 - q_1 \beta_1)/4 = 0.$$

Using symmetry of $A_n(x)$ and anti-symmetry of $B_n(x)/x$, or continuing with the recurrences (32–33), we obtain $\alpha_3 = \alpha_1 = -1$, $\beta_3 = -\beta_1 = -1$, $\alpha_4 = \alpha_0 = 2$, $\beta_4 = -\beta_0 = 0$. Thus $A_{15}(x) = 2x^4 - x^3 - 4x^2 - x + 2$ and $B_{15}(x) = x^3 - x$, as expected.

3.2 An algorithm for computing C_n and D_n

Consider the computation of C_n and D_n for square-free $n > 1$. Define n', s, s' and L_n as in Section 2.3, and $d = \phi(n')/2$. Thus $\deg L_n = 2d$, $\deg C_n = d$, and $\deg D_n = d - 1$. From (26) it is enough to compute the coefficients a_k of $L_n(x)$. In order to work over the integers, we define

$$q_k = \begin{cases} s' p_k/\sqrt{n}, & \text{if } k \text{ is odd;} \\ p_k, & \text{if } k \text{ is even;} \end{cases}$$

where p_k is the sum of k-th powers of roots of $L_n(x)$. Thus, from (29),

$$q_k = \begin{cases} (n|k), & \text{if } k \text{ is odd;} \\ \mu(n'/g'_k)\phi(g'_k)\cos\left((n-1)k\pi/4\right), & \text{otherwise.} \end{cases} \qquad (34)$$

If

$$C_n(x) = \sum_{j=0}^{d} \gamma_j x^{d-j}$$

and

$$D_n(x) = \sum_{j=0}^{d-1} \delta_j x^{d-1-j},$$

then, from (26),

$$\gamma_k = a_{2k}$$

and

$$\delta_k = -s' a_{2k+1}/\sqrt{n}.$$

In particular, $\gamma_0 = \delta_0 = 1$. Using (13) we obtain

$$\gamma_k = \frac{1}{2k} \sum_{j=0}^{k-1} (n q_{2k-2j-1} \delta_j - q_{2k-2j} \gamma_j) \tag{35}$$

and

$$\delta_k = \frac{1}{2k+1} \left(\gamma_k + \sum_{j=0}^{k-1} (q_{2k+1-2j} \gamma_j - q_{2k-2j} \delta_j) \right) \tag{36}$$

for $k = 1, 2, \ldots$

We may use the fact that $C_n(x)$ and $D_n(x)$ are symmetric to reduce the number of times the recurrences (35–36) need to be applied. An algorithm which incorporates this refinement is:

Algorithm L (for Lucas)

1. Evaluate q_k for $k = 1, \ldots, d$ using (34).
2. Set $\gamma_0 \leftarrow 1$ and $\delta_0 \leftarrow 1$.
3. Evaluate γ_k for $k = 1, \ldots, \lfloor d/2 \rfloor$ and δ_k for $k = 1, \ldots, \lfloor (d-1)/2 \rfloor$ using (35–36).
4. Evaluate γ_k for $k = \lfloor d/2 \rfloor + 1, \ldots, d$ using $\gamma_k = \gamma_{d-k}$.
5. Evaluate δ_k for $k = \lfloor (d+1)/2 \rfloor, \ldots, d-1$ using $\delta_k = \delta_{d-1-k}$.

Example

Consider the case $n = 15$ as in Section 1.2. We have $n' = 2n = 30$, $s' = 1$, $d = \phi(30)/2 = 4$. Thus

$$q_1 = (15|1) = 1,$$

$$q_2 = \mu(15)\phi(2)\cos(7\pi) = -1,$$

$$q_3 = (15|3) = 0,$$

$$q_4 = \mu(15)\phi(2)\cos(14\pi) = 1.$$

The initial conditions are $\gamma_0 = \delta_0 = 1$. The recurrences (35–36) give

$$\gamma_1 = (15 q_1 \delta_0 - q_2 \gamma_0)/2 = 8,$$

$$\delta_1 = (\gamma_1 + q_3 \gamma_0 - q_2 \delta_0)/3 = 3,$$

$$\gamma_2 = (15 q_3 \delta_0 + 15 q_1 \delta_1 - q_4 \gamma_0 - q_2 \gamma_1)/4 = 13.$$

Using symmetry we obtain $\gamma_3 = \gamma_1 = 8$, $\gamma_4 = \gamma_0 = 1$, $\delta_2 = \delta_1 = 3$, and $\delta_3 = \delta_0 = 1$. Thus $C_{15}(x) = x^4 + 8x^3 + 13x^2 + 8x + 1$ and $D_{15}(x) = x^3 + 3x^2 + 3x + 1$, as expected.

3.3 Stevenhagen's algorithm

Stevenhagen [27] gives an algorithm for computing the polynomials $C_n(x)$ and $D_n(x)$. His algorithm depends on the application of the Euclidean algorithm to two polynomials with integer coefficients and degree $O(n)$. $C_n(x)$ and $D_n(x)$ may be computed as soon as a polynomial of degree $\le \phi(n)/2$ is generated by the Euclidean algorithm. Thus, the algorithm requires $O(n^2)$ arithmetic operations, the same order[5] as our Algorithm L.

Unfortunately, Stevenhagen's algorithm suffers from a well-known problem of the Euclidean algorithm [14] – although the initial and final polynomials have small integer coefficients, the intermediate results grow exponentially large. When implemented in 32-bit integer arithmetic we found that Stevenhagen's algorithm failed due to integer overflow for $n = 35$.

Algorithm L does not suffer from this problem. It is easy to see from the recurrences (35–36) that intermediate results can grow only slightly larger than the final coefficients γ_k and δ_k. A straightforward implementation of Algorithm L can compute C_n and D_n for all square-free $n < 180$ without encountering integer overflow in 32-bit arithmetic. When it does eventually occur, overflow is easily detected because the division by $2k$ in (35) or by $2k+1$ in (36) gives a non-integer result.

4 Explicit expressions for $A_n, \ldots, D_n$

We now use (14) to give generating functions for the coefficients of $A_n, \ldots, D_n$. The generating functions can be used to evaluate the coefficients of $A_n(x), \ldots, D_n(x)$ in $O(n \log n)$ arithmetic operations, via the fast power series algorithms of Section 5 of Brent and Kung [5]. Also, where the generating functions converge, they give explicit formulas which can be used to compute $A_n(x), \ldots, D_n(x)$ at particular arguments x. However, it is often more efficient to compute the coefficients of the polynomials by the algorithms of Section 3 and then evaluate the polynomials by Horner's rule.

The generating functions may be written in terms of certain analytic functions f_n and g_n, which we now define.

4.1 The analytic functions f_n and g_n

For odd square-free $n > 1$ and $|x| \le 1$, define

$$f_n(x) = \sum_{j=1}^{\infty} (j|n) \frac{x^j}{j}. \tag{37}$$

Similarly, for square-free $n > 1$ and $|x| \le 1$, define

$$g_n(x) = \sum_{j=0}^{\infty} (n \mid 2j+1) \frac{x^{2j+1}}{2j+1}. \tag{38}$$

Observe that $g_n(x)$ is an odd function, so $g_n(-x) = -g_n(x)$.

It follows from (46) and (57) below that $\exp(\sqrt{sn} f_n(x))$ and $\exp(2\sqrt{n} g_n(x))$ are rational functions with zeros and poles at certain roots of unity. From these representations it follows that the analytic continuations outside the unit circle are given by

$$\begin{cases} f_n(x) = f_n(1/x), & \text{if } n = 1 \bmod 4; \\ f_n(x) + f_n(1/x) = 2f_n(1), & \text{if } n = 3 \bmod 4; \end{cases} \tag{39}$$

[5]The complexity of both algorithms can be reduced to $O(n(\log n)^2)$ arithmetic operations by standard "divide and conquer" techniques [1, 4], but this is not of practical significance.

and

$$g_n(x) = g_n(1/x). \tag{40}$$

The functions $f_n(x)$ and $g_n(x)$ are closely related. For example, taking the odd terms in the sum (37) and using the law of quadratic reciprocity, we obtain

$$f_n(x) - f_n(-x) = 2g_n(x\sqrt{s})/\sqrt{s}.$$

Such identities are a consequence of relationships between the polynomials $G_n(x)$ and $L_n(x)$.

$f_n(1)$ is related to the class number $h(D)$ of the quadratic field $Q[\sqrt{D}]$ with discriminant $D = sn$. In the notation of Davenport [10], $f_n(1) = L_{-1}(1) = L(1) = L(1, \chi)$, where $\chi(j) = (j|n)$ is the real, nonprincipal Dirichlet character appearing in (37). Known results [10, 18, 19, 30] in the case $n = 3 \bmod 4$ (so $D = -n$) are

$$f_n(1) = \frac{-\pi}{n^{3/2}} \sum_{j=1}^{n-1} (j|n)j = \frac{\pi}{(2-(2|n))\sqrt{n}} \sum_{j=1}^{(n-1)/2} (j|n) = \frac{2\pi}{w\sqrt{n}} h(-n) > 0. \tag{41}$$

Here

$$w = \begin{cases} 6, & \text{if } n = 3; \\ 2, & \text{if } n = 3 \bmod 4,\ n > 3 \end{cases}$$

is the number of roots of unity in $Q[\sqrt{D}]$. Since $h(-n)$ is an integer and $h(-3) = 1$, we have

$$\exp(2i\sqrt{n} f_n(1)) = \begin{cases} (-1+\sqrt{-3})/2, & \text{if } n = 3; \\ 1, & \text{if } n = 3 \bmod 4,\ n > 3. \end{cases} \tag{42}$$

In the case $n = 1 \bmod 4$, we have $D = n$, and

$$f_n(1) = \frac{\ln \varepsilon}{\sqrt{n}} h(n). \tag{43}$$

Here ε is the "fundamental unit", i.e. $\varepsilon = (|u| + \sqrt{n}|v|)/2$, where (u, v) is a minimal nontrivial solution of $u^2 - nv^2 = 4$. For example, if $n = 5$ then $\varepsilon = (3 + \sqrt{5})/2$, $h(5) = 1$ and $f_5(1) = (\ln \varepsilon)/\sqrt{5} = 0.4304\ldots$

4.2 The polynomials A_n and B_n

Let $n > 3$ be odd and square-free. We exclude $n = 3$ to avoid the special case in (42), but the results apply with minor modifications when $n = 3$. Let s, G_n, $\tilde{G}_n$ be as in Section 2.2, and $d = \phi(n)/2$. Recall that

$$G_n(x) = \prod_{\substack{0<j<n \\ (j|n)=1}} (x - \zeta^j) \tag{44}$$

and

$$\tilde{G}_n(x) = \prod_{\substack{0<j<n \\ (j|n)=-1}} (x - \zeta^j). \tag{45}$$

From (14) and (23), we have

$$\tilde{G}_n(1/x)/G_n(1/x) = \exp(\sqrt{sn} f_n(x)). \tag{46}$$

Also, from (44),

$$(-x)^d G_n(1/x) = \prod_{\substack{0<j<n \\ (j|n)=1}} (\zeta^j x - 1) = \prod_{\substack{0<j<n \\ (j|n)=1}} \zeta^j (x - \zeta^{-j}), \tag{47}$$

so

$$G_n(1/x)/\tilde{G}_n(1/x) = \zeta^\sigma \prod_{j=1}^{n-1} (x - \zeta^{-j})^{(j|n)}, \tag{48}$$

where

$$\sigma = \sum_{j=1}^{n-1} (j|n) j. \tag{49}$$

If $n = 1 \bmod 4$ then by grouping the terms for j and $n - j$ ($j < n/2$) in (49) we have $n|\sigma$. If $n = 3 \bmod 4$ then, from (41), we have $\sigma = -nh(-n)$ so again $n|\sigma$. Thus, in both cases $\zeta^\sigma = 1$, and from (48) we have

$$G_n(1/x)/\tilde{G}_n(1/x) = \begin{cases} G_n(x)/\tilde{G}_n(x), & \text{if } n = 1 \bmod 4; \\ \tilde{G}_n(x)/G_n(x), & \text{if } n = 3 \bmod 4. \end{cases} \tag{50}$$

It follows from (46) that

$$\tilde{G}_n(x)/G_n(x) = \exp(s\sqrt{sn} f_n(x)). \tag{51}$$

We see from (46) or (51) that, as claimed above, $\exp(\sqrt{sn} f_n(x))$ is a rational function. It has zeros at ζ^j, $(j|n) = -s$; and poles at ζ^j, $(j|n) = +s$. From (20) and (51), taking a square root, we obtain

$$G_n(x) = \sqrt{\Phi_n(x)} \exp\left(\frac{-s\sqrt{sn}}{2} f_n(x)\right) \tag{52}$$

If (52) is interpreted as a generating function for $G_n(x)$ then $\sqrt{\Phi_n(x)}$ and $f_n(x)$ should be interpreted as power series in x, and the correct sign of the square root is positive. On the other hand, if (52) is regarded as an exact expression for $G_n(x)$, then the sign of the square root is positive for real x, because $G_n(x)$ and $\Phi_n(x)$ have no real roots, and the exponential never vanishes, so a change in sign would contradict the continuity of $G_n(x)$. An extension of this argument shows that the same branch of the square root must be taken in any simply-connected, closed region which does not contain any of the zeros of $\Phi_n(x)$. (We omit similar comments below.)

From (52) we easily deduce the corresponding expressions for $A_n(x) = G_n(x) + \tilde{G}_n(x)$ and $B_n(x) = (\tilde{G}_n(x) - G_n(x))/\sqrt{sn}$. We state the results as a Theorem:

Theorem 1 *For odd, square-free $n > 3$, the polynomials $A_n(x)$ and $B_n(x)$ occurring in Gauss's identity* (6) *are*

$$A_n(x) = 2\sqrt{\Phi_n(x)} \cosh\left(\frac{\sqrt{sn}}{2} f_n(x)\right) \tag{53}$$

and

$$B_n(x) = 2\sqrt{\frac{\Phi_n(x)}{sn}} \sinh\left(\frac{\sqrt{sn}}{2} f_n(x)\right). \tag{54}$$

Remark

If $n = 3 \bmod 4$, so $s = -1$, then it is natural to replace $\cosh(iz)$ by $\cos(z)$ in (53) and $\sinh(iz)$ by $i\sin(z)$ in (54), giving

$$A_n(x) = 2\sqrt{\Phi_n(x)} \cos\left(\frac{\sqrt{n}}{2} f_n(x)\right) \tag{55}$$

and

$$B_n(x) = 2\sqrt{\frac{\Phi_n(x)}{n}} \sin\left(\frac{\sqrt{n}}{2} f_n(x)\right). \tag{56}$$

Example

Consider the case $n = 15$. We expand the right side of (55) as a power series in x, keeping enough terms to find $A_{15}(x)$ without using symmetry. From Section 1.2 we have

$$\Phi_{15}(x) = 1 - x + x^3 - x^4 + x^5 - x^7 + x^8,$$

so

$$\sqrt{\Phi_{15}(x)} = 1 - \frac{x}{2} - \frac{x^2}{8} + \frac{7x^3}{16} - \frac{37x^4}{128} + \cdots$$

Also,

$$f_{15}(x) = x + \frac{x^2}{2} + \frac{x^4}{4} - \frac{x^7}{7} + \cdots$$

so

$$\cos\left(\frac{\sqrt{15}}{2} f_{15}(x)\right) = 1 - \frac{15x^2}{8} - \frac{15x^3}{8} + \frac{15x^4}{128} + \cdots$$

and

$$2\sqrt{\Phi_{15}(x)}\cos\left(\frac{\sqrt{15}}{2} f_{15}(x)\right) = 2 - x - 4x^2 - x^3 + 2x^4 + \cdots,$$

which is $A_{15}(x) + O(x^5)$ as expected. We can ignore the $O(x^5)$ term (which in fact vanishes) since we know that $\deg A_{15}(x) = \phi(15)/2 = 4$.

A reader who attempts similar computations for larger n will soon be convinced that Algorithm D of Section 3.1 is more convenient, if only because all intermediate results are integers and there is an easy check on the accuracy of the inner product accumulations.

Using (41–43) and the fact (an immediate consequence of (4)) that

$$\Phi_n(1) = \begin{cases} n, & \text{if } n \text{ is prime;} \\ 1, & \text{for other square-free } n > 1; \end{cases}$$

we can verify that (46) and (51–56) give sensible results in the case $x = 1$. For example, we have $h(-15) = 2$, so $f_{15}(1) = 2\pi/\sqrt{15}$ and $\cos(\frac{\sqrt{15}}{2} f_{15}(1)) = \cos(\pi) = -1$. Thus (55) gives the correct value -2 of $A_{15}(1)$.

4.3 The polynomials C_n and D_n

We now consider the analogues of (53–54) for the Lucas polynomials C_n and D_n. The argument is similar to that of Section 4.2, but simpler because the polynomial $L_n(x)$ is symmetric, which leads to the simple functional equation (40) for $g_n(x)$.

Assume that $n > 1$ is square-free, and adopt the notation of Section 2.3. Using (29) in the generating function (14), we have

$$\tilde{L}_n(1/x)/L_n(1/x) = \exp\left(2s'\sqrt{n}g_n(x)\right). \tag{57}$$

This shows that $\exp(2\sqrt{n}g_n(x))$ is a rational function. From

$$\tilde{L}_n(1/x)/L_n(1/x) = \tilde{L}_n(x)/L_n(x)$$

we deduce the functional equation (40), which gives the analytic continuation of $g_n(x)$ outside the unit circle. We may also write (57) more simply as

$$\tilde{L}_n(x)/L_n(x) = \exp\left(2s'\sqrt{n}g_n(x)\right). \tag{58}$$

From (28) and (58), taking a square root, we obtain

$$L_n(x) = \sqrt{F_n(x^2)}\exp\left(-s'\sqrt{n}g_n(x)\right). \tag{59}$$

Theorem 2 *Let $n > 1$ be square-free. The Aurifeuillian factors $F_n^{\pm}(x) = C_n(x) \pm \sqrt{nx}D_n(x)$ of $F_n(x)$ are given by*

$$F_n^{\pm}(x) = \sqrt{F_n(x)}\exp\left(\pm\sqrt{n}g_n(\sqrt{x})\right). \tag{60}$$

Also,

$$C_n(x) = \sqrt{F_n(x)}\cosh\left(\sqrt{n}g_n(\sqrt{x})\right) \tag{61}$$

and

$$D_n(x) = \sqrt{\frac{F_n(x)}{nx}}\sinh\left(\sqrt{n}g_n(\sqrt{x})\right). \tag{62}$$

Proof

Recall that the Aurifeuillian factors $F_n^{\pm}(x) = C_n(x) \pm \sqrt{nx}D_n(x)$ of $F_n(x)$ are $L_n(\pm\sqrt{x})$. Thus (60) follows from (59). Since

$$L_n(x) + L_n(-x) = 2C_n(x^2)$$

and

$$L_n(x) - L_n(-x) = -2s'x\sqrt{n}D_n(x^2),$$

we easily deduce (61–62). □

4.4 Application to integer factorization

In this section we illustrate how the results of Sections 3.2 and 4.3 can be used to obtain factors of integers of the form $a^n \pm b^n$. Our examples are for illustrative purposes, so are small enough to be verified by hand. Many larger examples can be found in [6, 7].

As usual, $n > 1$ is a square-free integer. Recall the definition of $F_n(x)$ from Section 1.1. Note that the polynomial $F_n(x)$ is a factor of $x^n \pm 1$ (where the sign is "$-$" if $n = 1 \bmod 4$, and "$+$" otherwise).

If x has the form m^2n, where m is a positive integer, then $\sqrt{nx} = mn$ is an integer, and the Aurifeuillian factors $F_n^{\pm}(x) = C_n(x) \pm mnD_n(x)$ give integer factors of $F_n(x)$, and hence of $x^n \pm 1 = m^{2n}n^n \pm 1$. For example, if $m = n^k$, we obtain factors of $n^{(2k+1)n} \pm 1$.

More generally, if $m = p/q$ is rational, we obtain rational factors of $x^n \pm 1 = p^{2n}q^{-2n}n^n \pm 1$, and thus integer factors of $p^{2n}n^n \pm q^{2n}$. We consider one example later, but for the moment we continue to assume that m is an integer.

Before giving numerical examples, we state explicitly how the results of Section 4.3 can be used to compute $F_n^{\pm}(m^2n)$.

Theorem 3 *Let m, n be positive integers, $n > 1$ square-free, $x = m^2n$, and $\lambda = \phi(2n)/2$. Then the Aurifeuillian factors $F_n^{\pm}(x)$ of $F_n(x)$ are given by*

$$F_n^-(x) = \lfloor \hat{F} + 1/2 \rfloor$$

and

$$F_n^+(x) = F_n(x)/F_n^-(x),$$

where

$$\hat{F} = \sqrt{F_n(x)}\exp\left(-\frac{1}{m}\sum_{j=0}^{\lambda-1}\frac{(n \mid 2j+1)}{(2j+1)x^j}\right).$$

Proof

From (60), using the functional equation (40) and the power series (38) for $g_n(1/\sqrt{x})$, we have

$$F_n^-(x) = \sqrt{F_n(x)}\exp\left(-\frac{1}{m}\sum_{j=0}^{\infty}\frac{(n \mid 2j+1)}{(2j+1)x^j}\right).$$

Thus, we only have to show that the error incurred by truncating the power series after λ terms is less than $1/2$ in absolute value, i.e. that $|\hat{F} - F_n^-| < 1/2$.

If $x < 5$ we must have $m = 1$, $n = 2$ or 3, $x = n$, $\lambda = 1$. In both cases $F_n^-(n) = 1$ and it is easy to verify that $1/2 < \hat{F} < 3/2$. Thus, from now on we assume that $x \geq 5$.

Let

$$t = \frac{1}{m}\sum_{j=\lambda}^{\infty}\frac{(n \mid 2j+1)}{(2j+1)x^j}.$$

Since $m \geq 1$, $\lambda \geq 1$, $x \geq 5$, and the Jacobi symbol is 0 or ± 1, we have

$$|t| \leq \sum_{j=\lambda}^{\infty}\frac{x^{-j}}{(2j+1)} \leq \left(\frac{1}{3} + \frac{1}{5\cdot 5} + \frac{1}{7\cdot 5^2} + \cdots\right)x^{-\lambda}$$

so

$$|t| \leq 5\left(\sqrt{5}\,\ln\left(\frac{1+\sqrt{5}}{2}\right) - 1\right)x^{-\lambda} < 0.3802x^{-\lambda}. \tag{63}$$

In particular, $|t| < 0.3802/x < 0.08$, so

$$|\exp(t) - 1| < \frac{|t|}{1 - |t|/2} < \frac{0.3802x^{-\lambda}}{0.96} < 0.4x^{-\lambda}. \tag{64}$$

Now $\hat{F} = F_n^- \exp(t)$, so

$$|\hat{F} - F_n^-| = F_n^-|\exp(t) - 1|. \tag{65}$$

Applying Lemma 2 of Section 2.1 with $R = 5$ gives

$$F_n(x) < \exp(1/4)x^{\phi(2n)},$$

but $\phi(2n) = 2\lambda$ and F_n^- is the smaller factor of F_n, so

$$F_n^-(x) \leq \sqrt{F_n(x)} < \exp(1/8)x^{\lambda}. \tag{66}$$

From (64–66) we finally obtain the bound

$$|\hat{F} - F_n^-| < 0.4\exp(1/8) < 0.5,$$

which completes the proof. $\square$

Since the argument of the exponential in Theorem 3 is $-1/m + O(1/n)$ as $n \to \infty$, we have the following result, which sheds some light on the ratio of the Aurifeuillian factors. (The Corollary strictly follows from Theorem 3 only if m is an integer, but from the proof of Theorem 3 it is clear that the Corollary is also valid for rational m.)

Corollary 1 *Let $x = m^2 n$ where $m > 0$ is rational $n > 1$ is an integer. Consider m fixed as $n \to \infty$ through square-free values. Then the Aurifeuillian factors $F_n^{\pm}(x)$ of $F_n(x)$ satisfy*

$$F_n^+(x)/F_n^-(x) = \exp(2/m) + O(1/n).$$

Examples

1. To start with a simple example, consider $n = 2$, $m = 2$, so $x = m^2 n = 8$ and $\lambda = 1$. In Theorem 3 we have $F_2(x) = x^2 + 1 = 65$,

$$\hat{F} = \sqrt{F_2(x)}\exp(-1/m) = \sqrt{65}\exp(-1/2) = 4.89\cdots$$

and rounding to the nearest integer gives the factor 5 of 65.

2. A similar but less trivial example is $n = 2$, $m = 2^5$, $x = m^2 n = 2^{11}$. Here $F_2(x) = x^2 + 1 = 2^{22} + 1$ and

$$\hat{F} = \sqrt{F_2(x)}\exp(-1/m) = \sqrt{2^{22}+1}\exp(-2^{-5}) = 1984.98\cdots$$

which on rounding gives the factor $F_2^- = 1985$ of $2^{22} + 1$. By division we find $F_2^+ = 2113$, so the complete factorization is $2^{22} + 1 = 5 \cdot 397 \cdot 2113$.

3. Now consider $n = 5$, $m = 3$, so $x = m^2 n = 45$ and $\lambda = \phi(10)/2 = 2$. In this case

$$F_5(x) = \Phi_5(x) = (x^5 - 1)/(x - 1) = 4193821,$$

$$\hat{F} = \sqrt{F_5(x)}\exp\left(-\frac{1}{m} + \frac{1}{3m^3 n}\right) = \sqrt{4193821}\exp(-134/405) = 1470.99924\cdots$$

and rounding to the nearest integer gives the factor 1471 of $F_5(x)$. By division we obtain the other factor 2851. In this example, but not in general, the Aurifeuillian factors are prime.

4. Now consider a composite n, say $n = 15$. To keep the arithmetic easy we take $m = 1$, so $x = 15$ and

$$F_{15}(x) = \Phi_{15}(-x) = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1 = 2732936641.$$

The example in Section 3.2 shows how we can use Algorithm L to compute

$$C_{15}(x) = x^4 + 8x^3 + 13x^2 + 8x + 1$$

and

$$D_{15}(x) = x^3 + 3x^2 + 3x + 1.$$

Evaluating the polynomials, we find

$$C_{15}(15) = 80671, \quad D_{15}(15) = 4096,$$

so the Aurifeuillian factors of $F_{15}(15)$ are $80671 \pm 15 \cdot 4096$. This gives 19231 and 142111, which can easily be verified to be factors of $15^{15} + 1$. The "algebraic" factors $(15^3 + 1)/16$ and $(15^5 + 1)/16$ allow us to complete the factorization:

$$15^{15} + 1 = 2^4 \cdot 31 \cdot 211 \cdot 1531 \cdot 19231 \cdot 142111$$

Alternatively, instead of evaluating $C_{15}(15)$ and $D_{15}(15)$, we can use Theorem 3. We have $\lambda = \phi(15)/2 = 4$. Since $(15|3) = (15|5) = 0$ and $(15|7) = 1$, the computation gives

$$\hat{F} = \sqrt{F_{15}(x)}\exp\left(-1 - \frac{1}{7n^3}\right) = 19231.00217\cdots$$

and rounding to the nearest integer gives the factor 19231 of $F_{15}(15)$.

5. To conclude, we give an example where $m = p/q$ is rational but not an integer. Consider $n = 7$, $p = 2$, $q = 5$, so $x = p^2n/q^2 = 28/25$ and $\sqrt{nx} = pn/q = 14/5$. We have

$$F_7(x) = \Phi_7(-x) = \frac{x^7+1}{x+1} = \frac{28^7+25^7}{53 \cdot 25^6}$$

Theorem 3 is not applicable. Because x is close to 1, the series for $g_7(1/\sqrt{x})$ converges rather slowly, and we need to take at least 35 terms to obtain sufficient accuracy. However, using Algorithm L we easily find that

$$C_7(x) = x^3 + 3x^2 + 3x + 1, \quad D_7(x) = x^2 + x + 1,$$

so Horner's rule gives

$$C_7(x) = 148877/5^6, \quad D_7(x) = 2109/5^4,$$

and $C_7(x) \pm \sqrt{nx}D_7(x)$ gives $296507/5^6$ and $1247/5^6$. Thus, we have obtained factors 296507 and 1247 of $(25^7 + 28^7)/53$. The larger factor is prime, so it is easy to deduce the complete factorization

$$25^7 + 28^7 = 29 \cdot 43 \cdot 53 \cdot 296507$$

Acknowledgements

Thanks are due to Brendan McKay for suggesting the use of the generating function (14), to Emma Lehmer and an anonymous referee for helpful comments on the exposition, to Hans Riesel for his kind assistance with the solution of exercise A6.2 of [24], and to Sam Wagstaff and Hugh Williams for providing copies of several references which were difficult to find in Australia.

References

[1] A. V. Aho, J. E. Hopcroft and J. D. Ullman, *The Design and Analysis of Computer Algorithms*, Addison-Wesley, Menlo Park, Calif., 1974, Chapter 8.

[2] A. Aurifeuille and H. Le Lasseur, see [20], page 276, or [21], page 785.

[3] N. G. W. H. Beeger, "On a new quadratic form for certain cyclotomic polynomials", *Nieuw Arch. Wisk.* (2), 23 (1951), 249-252.

[4] R. P. Brent, F. G. Gustavson and D. Y. Y. Yun, "Fast solution of Toeplitz systems of equations and computation of Padé approximants", *J. Algorithms* 1 (1980), 259-295.

[5] R. P. Brent and H. T. Kung, "Fast algorithms for manipulating formal power series", *J. ACM* 25 (1978), 581-595.

[6] R. P. Brent and H. J. J. te Riele, *Factorizations of* $a^n \pm 1$, $13 \le a < 100$, Report NM-R9212, Department of Numerical Mathematics, Centrum voor Wiskunde en Informatica, Amsterdam, June 1992.

[7] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman and S. S. Wagstaff, Jr., *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers*, second edition, American Mathematical Society, Providence, Rhode Island, 1988.

[8] A. J. C. Cunningham, "Factorisation of $N = y^y \mp 1$ and $x^{xy} \mp y^{xy}$", *Messenger of Math.* (2), 45 (1915), 49-75.

[9] A. J. C. Cunningham and H. J. Woodall, *Factorisation of* $y^n \mp 1$, $y = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers* (n), Hodgson, London, 1925.

[10] H. Davenport, *Multiplicative Number Theory*, second edition (revised by H. L. Montgomery), Springer-Verlag, New York, 1980.

[11] P. G. Lejeune Dirichlet, *Vorlesungen über Zahlentheorie*, fourth edition, Friedr. Vieweg & Sohn, Braunschweig, 1894, Chapter 5 and Supplement 7.

[12] C. F. Gauss, *Disquisitiones Arithmeticæ*, G. Fleischer, Leipzig, 1801, Art. 356-357. Reprinted in *Carl Friedrich Gauss Werke*, Band 1, Georg Olms Verlag, Hildesheim, 1981.

[13] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, fifth edition, Clarendon Press, Oxford, 1984, Ch. 16.

[14] D. E. Knuth, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms* (second edition), Addison-Wesley, Menlo Park, 1981, Chapter 3.

[15] M. Kraitchik, "Décomposition de $a^n \pm b^n$ en facteurs dans le cas où nab est un carré parfait avec une table des décompositions numériques pour toutes les valeurs de a et b inférieures à 100", Gauthiers-Villars, Paris, 1922.

[16] M. Kraitchik, *Recherches sur la Théorie des Nombres*, Volume 1, Gauthiers-Villars, Paris, 1924.

[17] M. Kraitchik, *Introduction à la Théorie des Nombres*, Gauthiers-Villars, Paris, 1952.

[18] Edmund Landau, *Vorlesungen über Zahlentheorie*, Band 1(1): *Aus der elementaren und additiven Zahlentheorie*, Leipzig, 1927. English translation: *Elementary Number Theory*, Chelsea, New York, 1958.

[19] Serge Lang, *Cyclotomic Fields I and II*, combined second edition, Graduate Texts in Mathematics 126, Springer-Verlag, New York, 1990.

[20] E. Lucas, "Théorèmes d'arithmétique", *Atti. R. Acad. Sc. Torino* 13 (1877-8), 271-284.

[21] E. Lucas, "Sur la série récurrente de Fermat", *Bull. Bibl. Storia Sc. Mat. e Fis.* 11 (1878), 783-789.

[22] E. Lucas, "Sur les formules de Cauchy et de Lejeune-Dirichlet", *Ass. Française pour l'Avanc. des Sci., Comptes Rendus* 7 (1878), 164-173.

[23] S. Ramanujan, "On certain trigonometrical sums and their applications in the theory of numbers", *Trans. Cambridge Philos. Soc.* 22, 13 (1918), 259-276. Reprinted in *Collected Papers of Srinivasa Ramanujan* (edited by G. H. Hardy, P. V. Seshu Aiyar and B. M. Wilson), Cambridge Univ. Press, 1927.

[24] Hans Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, Boston, 1985.

[25] John Riordan, *An Introduction to Combinatorial Analysis*, Princeton University Press, New Jersey, 1978, Ch. 2, exercise 27.

[26] A. Schinzel, "On the primitive prime factors of $a^n - b^n$", *Proc. Cambridge Philos. Soc.* 58 (1962), 555-562. MR 26#1280

[27] Peter Stevenhagen, "On Aurifeuillian factorizations", *Nederl. Akad. Wetensch. Indag. Math.* 49 (1987), 451-468. MR 89a:11015

[28] H. W. Turnbull, *Theory of Equations* (fifth edition), Oliver and Boyd, Edinburgh, 1952, Sec. 32.

[29] B. L. van der Waerden, *Algebra*, Vol. 1 (English translation by Fred Blum, fifth edition), Frederick Ungar, New York, 1953, Ch. 7.

[30] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics 83, Springer-Verlag, New York, 1982.