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 elsewhere.

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

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

and the Möbius inversion formula [9] gives

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}. \tag{2}$$

Equation (1) is useful for theoretical purposes, but (2) 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

$$\Phi_n(x) = \begin{cases} x - 1 & \text{if } n = 1,\\ \Phi_{n/p}(x^p)/\Phi_{n/p}(x) & \text{if } p \text{ is prime and } p|n, \end{cases} \tag{3}$$

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

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.

To appear in *Proceedings of a Conference on Computational Algebra and Number Theory* (held at the University of Sydney, November 1992). This paper is a preliminary report and introduction to [1].

rpb127 typeset using $\mathcal{A}\mathcal{M}\mathcal{S}$-LaTeX

In this preliminary report we omit proofs, and assume from now on that

$$n > 1 \text{ is square-free and } n = 1 \bmod 4. \tag{4}$$

The results can be generalized to other square-free n, and similar results hold for the identities of Gauss and Dirichlet. The interested reader is referred to [1] for details.

$\Phi_n(x)$ satisfies an identity

$$\Phi_n(x) = C_n(x)^2 - nxD_n(x)^2 \tag{5}$$

of Aurifeuille, Le Lasseur and Lucas[1]. For a proof, see Lucas [15] or Schinzel [17]. Here $C_n(x)$ and $D_n(x)$ are symmetric, monic polynomials with integer coefficients. For example, if $n = 5$, we have

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1 = (x^2 + 3x + 1)^2 - 5x(x + 1)^2,$$

so

$$C_5(x) = x^2 + 3x + 1 \quad \text{and} \quad D_5(x) = x + 1. \tag{6}$$

In Section 1.1 we summarize our notation. Then, in Section 2, we outline the theoretical basis for our algorithm for computing $C_n(x)$ and $D_n(x)$. The algorithm (Algorithm L) is presented in Section 3. Algorithm L appears to be new, although the key idea (using Newton's identities to evaluate polynomial coefficients) is due to Dirichlet [8]. A different algorithm, due to Stevenhagen [18], is discussed in Section 3.1.

In Section 4 we give explicit formulas for $C_n(x)$, $D_n(x)$ etc. These may be regarded as generating functions if x is an indeterminate, or may be used to compute $C_n(x)$ and $D_n(x)$ for given argument x. In the special case $x = 1$ there is an interesting connection with Dirichlet L-functions and the theory of class numbers of quadratic fields.

One application of cyclotomic polynomials is to the factorization of integers of the form $a^n \pm b^n$: see for example [3, 4, 5, 6, 11, 12, 16]. If $x = m^2 n$ for any integer m, then (5) is a difference of squares, giving integer factors $C_n(x) \pm mnD_n(x)$ of $x^n \pm 1$. Examples are given in Sections 3–4.

1.1. Notation. For consistency we follow the notation of [1] where possible, although there are simplifications due to our assumption (4).

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 [9]. Note that $\mu(1) = \phi(1) = 1$.

$(m|n)$ denotes the Jacobi symbol[2] except that $(m|n)$ is defined as 0 if $(m, n) > 1$. Thus, when specifying a condition such as $(m|n) = 1$ we may omit the condition $(m, n) = 1$. As usual, $m|n$ without parentheses means that m divides n.

n denotes a positive integer satisfying (4), which implies that $(-1|n) = 1$. It is convenient to write g_k for (k, n).

For given n, we define $s' = (2|n)$. In view of (4), the following are equivalent:

$$s' = (2|n) = (-1)^{(n^2-1)/8} = (-1)^{(n-1)/4} = \begin{cases} +1 & \text{if } n = 1 \bmod 8, \\ -1 & \text{if } n = 5 \bmod 8. \end{cases}$$

[1]Lucas [13, page 276] states "Les formules et les conséquences précédentes sont dues à la collaboration de M. Aurifeuille, ancien Professeur au lycée de Toulouse, actuellement décédé, et de M. Le Lasseur, de Nantes". See also [14, page 785].

[2]See, for example, Riesel [16]. To avoid ambiguity, we *never* write the Jacobi symbol as $\left(\frac{m}{n}\right)$.

The Aurifeuillian factors of $\Phi_n(x)$ are

$$F_n^+(x) = C_n(x) + \sqrt{nx}D_n(x) \quad \text{and} \quad F_n^-(x) = C_n(x) - \sqrt{nx}D_n(x).$$

From (5) we have $\Phi_n(x) = F_n^-(x)F_n^+(x)$.

1.2. Acknowledgements. Thanks are due to Emma Lehmer, Brendan McKay, Hans Riesel, Sam Wagstaff, and Hugh Williams for their comments and assistance.

2. Theoretical results

In this section we summarise some theoretical results which form the basis for Algorithm L. 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 (9). Consider the polynomial

$$L_n(x) = \sum_{\substack{0<j<n \\ (j|n)=(-1)^j}} (x - \zeta^j)(x - \zeta^{-j}),$$

which we may write as

$$L_n(x) = \sum_{\substack{0<j<n \\ (j|n)=(-1)^j}} \left(x^2 - 2\left(\cos\frac{\pi j}{n}\right)x + 1\right). \tag{7}$$

$L_n(x)$ has degree $\phi(n)$. Also, from (7), $L_n(x)$ is symmetric and has real coefficients. Schinzel [17] shows that

$$L_n(x) = C_n(x^2) - s'x\sqrt{n}D_n(x^2) \tag{8}$$

where $C_n(x)$ and $D_n(x)$ are the polynomials of (5), and $s' = (2|n)$ as usual. Clearly $F_n^-(x) = L_n(s'\sqrt{x})$ and $F_n^+(x) = L_n(-s'\sqrt{x})$.

For example, suppose $n = 5$. Then (7) gives

$$L_5(x) = \left(x^2 - 2\left(\cos\frac{3\pi}{5}\right)x + 1\right)\left(x^2 - 2\left(\cos\frac{4\pi}{5}\right)x + 1\right),$$

but $\cos 3\pi/5 = (1-\sqrt{5})/4$ and $\cos 4\pi/5 = -(1+\sqrt{5})/4$, so it is easily verified that

$$L_5(x) = x^4 + \sqrt{5}x^3 + 3x^2 + \sqrt{5}x + 1 = C_5(x^2) + x\sqrt{5}D_5(x^2),$$

where $C_5(x)$ and $D_5(x)$ are as in (6).

Let $g_k = (k, n)$. It may be shown that the Gaussian sums p_k of k-th powers of roots of $L_n(x)$ are

$$p_k = \begin{cases} (n|k)s'\sqrt{n} & \text{if } k \text{ is odd,} \\ \mu(n/g_k)\phi(g_k) & \text{if } k \text{ is even.} \end{cases} \tag{9}$$

3. An algorithm for computing C_n and D_n

In this section we consider the computation of C_n and D_n. Define $d = \phi(n)/2$. Thus $\deg L_n = 2d$, $\deg C_n = d$, and $\deg D_n = d - 1$. From (8) it is enough to compute the coefficients a_k of $L_n(x)$. Using (9), the coefficients of $L_n(x)$, and hence of $C_n(x)$ and $D_n(x)$, may be evaluated from Newton's identities. 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 (9),

$$q_k = \begin{cases} (n|k) & \text{if } k \text{ is odd,} \\ \mu(n/g_k)\phi(g_k) & \text{if } k \text{ is even.} \end{cases} \tag{10}$$

If

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

then, from (8),

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

In particular, $\gamma_0 = \delta_0 = 1$. Using Newton's identities, we obtain the recurrences

$$\gamma_k = \frac{1}{2k} \sum_{j=0}^{k-1} (n q_{2k-2j-1}\delta_j - q_{2k-2j}\gamma_j) \tag{11}$$

and

$$\delta_k = \frac{1}{2k+1} \left(\gamma_k + \sum_{j=0}^{k-1} (q_{2k+1-2j}\gamma_j - q_{2k-2j}\delta_j) \right) \tag{12}$$

for $k > 0$.

We can use the fact that $C_n(x)$ and $D_n(x)$ are symmetric to reduce the number of times the recurrences (11)–(12) need to be applied. An algorithm which incorporates this refinement is:

Algorithm L

1. Evaluate q_k for $k = 1, \ldots, d$ using the definition (10).
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 equations (11)–(12).
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 $\delta_k = \delta_{d-1-k}$.

Examples.

1. Consider the case $n = 5$. We have $s' = (2|5) = -1$, $d = \phi(5)/2 = 2$. Thus

$$q_1 = (5|1) = 1 \quad \text{and} \quad q_2 = \mu(5)\phi(1) = -1.$$

The initial conditions are $\gamma_0 = \delta_0 = 1$. The recurrence (11) gives

$$\gamma_1 = (5q_1\delta_0 - q_2\gamma_0)/2 = 3.$$

Using symmetry we obtain $\gamma_2 = \gamma_0 = 1$ and $\delta_1 = \delta_0 = 1$. Thus

$$C_5(x) = x^2 + 3x + 1, \qquad D_5(x) = x + 1,$$

and it is easy to verify that $\Phi_5(x)^2 = C_5(x)^2 - 5xD_5(x)^2$, as expected from (5).

2. Now consider $n = 33$. We have $s' = (2|33) = 1$, $d = \phi(33)/2 = 10$. Thus

$$\begin{aligned}
q_1 &= (33|1) = 1, & q_2 &= \mu(33)\phi(1) = 1,\\
q_3 &= (33|3) = 0, & q_4 &= \mu(33)\phi(1) = 1,\\
q_5 &= (33|5) = -1, & q_6 &= \mu(11)\phi(3) = -2,\\
q_7 &= (33|7) = -1, & q_8 &= \mu(33)\phi(1) = 1,\\
q_9 &= (33|9) = 0, & q_{10} &= \mu(33)\phi(1) = 1.
\end{aligned}$$

The initial conditions are $\gamma_0 = \delta_0 = 1$. The recurrences (11)–(12) give

$$\begin{aligned}
\gamma_1 &= (33q_1\delta_0 - q_2\gamma_0)/2 = 16,\\
\delta_1 &= (\gamma_1 + q_3\gamma_0 - q_2\delta_0)/3 = 5,\\
\gamma_2 &= (33q_3\delta_0 - q_4\gamma_0 + 33q_1\delta_1 - q_2\gamma_1)/4 = 37,\\
\delta_2 &= (\gamma_2 + q_5\gamma_0 - q_4\delta_0 + q_3\gamma_1 - q_2\delta_1)/5 = 6,\\
\gamma_3 &= (33q_5\delta_0 - q_6\gamma_0 + 33q_3\delta_1 - q_4\gamma_1 + 33q_1\delta_2 - q_2\gamma_2)/6 = 19,\\
\delta_3 &= (\gamma_3 + q_7\gamma_0 - q_6\delta_0 + q_5\gamma_1 - q_4\delta_1 + q_3\gamma_2 - q_2\delta_2)/7 = -1,\\
\gamma_4 &= (33q_7\delta_0 - q_8\gamma_0 + \cdots + 33q_1\delta_3 - q_2\gamma_3)/8 = -32,\\
\delta_4 &= (\gamma_4 + q_9\gamma_0 - q_8\delta_0 + \cdots + q_3\gamma_3 - q_2\delta_3)/9 = -9,\\
\gamma_5 &= (33q_9\delta_0 - q_{10}\gamma_0 + \cdots + 33q_1\delta_4 - q_2\gamma_4)/10 = -59.
\end{aligned}$$

Using symmetry, we obtain

$$C_{33}(x) = x^{10} + 16x^9 + 37x^8 + 19x^7 - 32x^6 - 59x^5 - 32x^4 + 19x^3 + 37x^2 + 16x + 1$$

and

$$D_{33}(x) = x^9 + 5x^8 + 6x^7 - x^6 - 9x^5 - 9x^4 - x^3 + 6x^2 + 5x + 1.$$

From the recurrence (3),

$$\Phi_{33}(x) = \Phi_3(x^{11})/\Phi_3(x) = \frac{x^{22} + x^{11} + 1}{x^2 + x + 1},$$

and it is straightforward to verify that $\Phi_{33}(x) = C_{33}(x)^2 - 33xD_{33}(x)^2$.

3.1. Stevenhagen's algorithm. Stevenhagen [18] gives a different 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 at most $\phi(n)/2$ is generated by the Euclidean algorithm. Thus, the algorithm requires $O(n^2)$ arithmetic operations, the same order[3] as our Algorithm L.

Unfortunately, Stevenhagen's algorithm suffers from a well-known problem of the Euclidean algorithm [10] – although the initial and final polynomials have small integer coefficients, the intermediate results grow exponentially large. When implemented in 32-bit integer arithmetic, Stevenhagen's algorithm fails due to integer overflow for $n \geq 35$.

Algorithm L does not suffer from this problem. It is easy to see from the recurrences (11)–(12) 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 $n < 180$ without

[3]The complexity of both algorithms can be reduced to $O(n(\log n)^2)$ arithmetic operations by standard "divide and conquer" techniques.

encountering integer overflow in 32-bit arithmetic. When it does eventually occur, overflow is easily detected because the division by $2k$ in (11) or by $2k+1$ in (12) gives a non-integer result.

4. Explicit expressions for C_n and D_n

In this section we give generating functions for the coefficients of C_n and D_n. These generating functions seem to be new. They can be used to evaluate the coefficients of $C_n(x)$ and $D_n(x)$ in $O(n \log n)$ arithmetic operations, via the fast power series algorithms of [2, Section 5]. Also, where they converge, they give explicit formulas which can be used to compute $C_n(x)$ and $D_n(x)$ at particular arguments x. However, it may be more efficient to compute the coefficients of the polynomials using Algorithm L, and then evaluate the polynomials by Horner's rule.

The generating functions may be written in terms of an analytic function g_n, which we now define. We continue to assume that (4) holds.

4.1. The analytic functions f_n and g_n. In this subsection x is a complex variable. For x inside the unit circle, and on the boundary $|x| = 1$ where the series converge, define

$$f_n(x) = \sum_{j=1}^{\infty} (j|n) \frac{x^j}{j} \tag{13}$$

and

$$g_n(x) = \sum_{j=0}^{\infty} (n|2j+1) \frac{x^{2j+1}}{2j+1}. \tag{14}$$

Observe that $g_n(x)$ is an odd function, so $g_n(-x) = -g_n(x)$. Our assumption (4) implies that $(n|2j+1) = (2j+1|n)$, so

$$2g_n(x) = f_n(x) - f_n(-x). \tag{15}$$

Also, since $(2j|n) = (2|n)(j|n) = s'(j|n)$, it is easy to see that

$$f_n(x) + f_n(-x) = s' f_n(x^2). \tag{16}$$

In [1] it is shown that analytic continuations of $f_n(x)$ and $g_n(x)$ outside the unit circle are given by the simple functional equations

$$f_n(x) = f_n(1/x), \qquad g_n(x) = g_n(1/x).$$

$f_n(1)$ is related to the class number $h(n)$ of the quadratic field $Q[\sqrt{n}]$ with discriminant n. In the notation of Davenport [7], $f_n(1) = L_{-1}(1) = L(1) = L(1, \chi)$, where $\chi(j) = (j|n)$ is the real, nonprincipal Dirichlet character appearing in (13). Thus, using well-known results,

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

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 we have $f_5(1) = (\ln \varepsilon)/\sqrt{5} = 0.4304\ldots$

Using (15)–(16), we obtain a simple relation between $g_n(1)$ and $f_n(1)$:

$$g_n(1) = \left(1 - \frac{s'}{2}\right) f_n(1).$$

Thus, in our example, $g_5(1) = 3f_5(1)/2$.

4.2. Generating functions. In [1] it is shown that

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

This leads to the following theorem. As usual, we continue to assume that n satisfies (4).

Theorem 1. *The Aurifeuillian factors $F_n^{\pm}(x) = C_n(x) \pm \sqrt{nx}D_n(x)$ of $\Phi_n(x)$ are given by*

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

Also,

$$C_n(x) = \sqrt{\Phi_n(x)}\cosh\left(\sqrt{n}g_n(\sqrt{x})\right)$$

and

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

4.3. Application to integer factorization. In this section we illustrate how the results of Sections 3 and 4.2 can be used to obtain factors of integers of the form $a^n \pm b^n$. Other examples can be found in [1, 3, 4].

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 $\Phi_n(x)$, and hence of $x^n - 1 = m^{2n}n^n - 1$. For example, if $m = n^k$, we obtain factors of $n^{(2k+1)n} - 1$.

Before giving numerical examples, we state explicitly how Theorem 1 can be used to compute $F_n^{\pm}(m^2n)$ with a finite number of arithmetic operations. The following theorem shows how many terms have to be taken in the infinite series (14) defining g_n. Because there is a little slack in the proof of the theorem, there is no practical difficulty in evaluating the exponential and square root to sufficient accuracy.

Theorem 2. *Let m, n be positive integers, $n > 1$ square-free, $n = 1 \bmod 4$, $x = m^2n$, and $\lambda = \phi(n)/2$. Then the Aurifeuillian factors of $\Phi_n(x)$ are*

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

and

$$F_n^{+}(x) = \Phi_n(x)/F_n^{-}(x),$$

where

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

Examples.

3. Consider $n = 5$, $m = 3$, so $x = m^2n = 45$ and $\lambda = \phi(5)/2 = 2$. Thus

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

$$\widehat{F} = \sqrt{\Phi_5(x)}\exp\left(-\frac{1}{m} + \frac{1}{3m^3n}\right) = \sqrt{4193821}\exp(-134/405) = 1470.99924\ldots$$

and rounding to the nearest integer gives the factor 1471 of $\Phi_5(x)$. By division we obtain the other factor 2851. Thus

$$45^5 - 1 = 44\Phi_5(x) = 2^2 \cdot 11 \cdot 1471 \cdot 2851.$$

In this example the Aurifeuillian factors are prime.

TABLE 1. Some Aurifeuillian factorisations

a^n	$a^n - 1$
21^{189}	$2^2 \cdot 5 \cdot 43 \cdot 109 \cdot 127 \cdot 163 \cdot 379 \cdot 463 \cdot 631 \cdot 757 \cdot 3319 \cdot 4789 \cdot$ $6427 \cdot 51787 \cdot 4779433 \cdot 85775383 \cdot 227633407 \cdot 4167831781 \cdot$ $22125429901 \cdot 7429452749713 \cdot 27186384126763 \cdot$ $100595851688887003 \cdot 5595292262076879253511 \cdot$ $592823611828574163154462624637481670158792334981 \cdot P_{60}$
33^{99}	$2^5 \cdot 37 \cdot 67 \cdot 199 \cdot 991 \cdot 1123 \cdot 2113 \cdot 19009 \cdot 90619 \cdot$ $34905511 \cdot 91402147 \cdot 747487377451 \cdot 4098986195943739 \cdot$ $9878399619525368754006622104322228 99 \cdot P_{46}$
33^{165}	$2^5 \cdot 31 \cdot 67 \cdot 331 \cdot 1123 \cdot 1321 \cdot 2113 \cdot 4951 \cdot 8581 \cdot 9241 \cdot 39451 \cdot$ $90619 \cdot 9540301 \cdot 91402147 \cdot 204970261 \cdot 275465191 \cdot 10125617371 \cdot$ $47284185301 \cdot 180115639771 \cdot 747487377451 \cdot 4098986195943739 \cdot$ $111935606239801921 51 \cdot 10761419445492388495462 21 \cdot$ $1423360768655377015279057937915830 51 \cdot P_{44}$
77^{77}	$2^2 \cdot 19 \cdot 23 \cdot 617 \cdot 757 \cdot 25411 \cdot 52344007 \cdot 278949511 \cdot 6165802127 \cdot$ $1241612324726802397 7 \cdot 188456985084507821054922117467601 79 \cdot P_{53}$
97^{97}	$2^5 \cdot 3 \cdot 389 \cdot 363751 \cdot 684640163 \cdot 11943728733741294764390602153 \cdot$ $549180361199324724418373466271912931710271534073773 \cdot P_{95}$
101^{101}	$2^2 \cdot 5^2 \cdot 607 \cdot 1213 \cdot 5657 \cdot 157561 \cdot$ $9931988588681 \cdot 102208068907493 \cdot 393101595766008847 \cdot$ $1260296562653610987238421629708576030882329452274601 7 \cdot P_{89}$
105^{105}	$2^3 \cdot 13 \cdot 151 \cdot 211 \cdot 421 \cdot 631 \cdot 1009 \cdot 1201 \cdot 1621 \cdot 2731 \cdot 11131 \cdot 102181 \cdot$ $485689 \cdot 18416161 \cdot 1340912959 \cdot 59785910251 \cdot 3662332210521480889 \cdot$ $2396546294931397077 1 \cdot 4974399548014294337472227709 1 \cdot$ $5384579552746854831338204156683983031 \cdot P_{43}$

4. Consider $n = 5$, $m = 40$, so $x = m^2 n = 8000$ and $x^n - 1 = 20^{15} - 1$. We have

$$\begin{aligned} \widehat{F} &= \sqrt{\Phi_5(x)} \exp\left(-\frac{1}{m} + \frac{1}{3m^3 n}\right) \\ &= 64004000.37\ldots \times 0.9753109279\ldots = 62423800.99\ldots \end{aligned}$$

and rounding to the nearest integer gives an Aurifeuillian factor $F_5^- = 62423801$ of $\Phi_5(x)$. By division we obtain the other Aurifeuillian factor $F_5^+ = 65624201$. Alternatively, we can find the same factors from (6) by evaluating $C_5(x)$ and $D_5(x)$. Neither of the Aurifeuillian factors is prime, but $20^{15} - 1$ also has "algebraic" factors $20^3 - 1 = 19 \cdot 421$ and $20^5 - 1 = 11 \cdot 19 \cdot 61 \cdot 251$. Thus, it is easy to find that $F_5^- = 11 \cdot 19 \cdot 61 \cdot 3001$, $F_5^+ = 251 \cdot 261451$, and

$$20^{15} - 1 = 11 \cdot 19 \cdot 31 \cdot 61 \cdot 251 \cdot 421 \cdot 3001 \cdot 261451.$$

5. For an example with larger λ, consider $m = 1$, $n = 13$, so $x = m^2n = 13$, $x^n - 1 = 13^{13} - 1$, and $\lambda = \phi(13)/2 = 6$. Theorem 2 gives

$$\begin{aligned}
\widehat{F} &= \sqrt{\Phi_{13}(13)}\exp\left(-\sum_{j=0}^{5}\frac{(13|2j+1)}{(2j+1)13^j}\right)\\
&= \sqrt{\frac{13^{13}-1}{13-1}}\exp\left(-1-\frac{1}{3\cdot 13}+\frac{1}{5\cdot 13^2}+\frac{1}{7\cdot 13^3}-\frac{1}{9\cdot 13^4}+\frac{1}{11\cdot 13^5}\right)\\
&= 5023902.0906\ldots \times 0.3590131665\ldots = 1803646.998\ldots,
\end{aligned}$$

and rounding to the nearest integer gives an Aurifeuillian factor $F_{13}^{-} = 1803647$ of $\Phi_{13}(13)$. The same factor could have been found from the polynomials

$$C_{13}(x) = x^6 + 7x^5 + 15x^4 + 19x^3 + 15x^2 + 7x + 1$$

and

$$D_{13}(x) = x^5 + 3x^4 + 5x^3 + 5x^2 + 3x + 1.$$

It is easy to deduce that

$$13^{13} - 1 = 2^2 \cdot 3 \cdot 53 \cdot 264031 \cdot 1803647.$$

6. An illustrative sample of other factorisations which can be obtained from Algorithm L or Theorem 2, and would have been difficult to obtain in any other way, is given in Table 1. The factors given explicitly in Table 1 are prime. As usual, large k-digit primes are written as P_k if they can be found by division.

References

1. R. P. Brent, "On computing factors of cyclotomic polynomials", *Mathematics of Computation*, D. H. Lehmer memorial issue, 1993, to appear. Preprint available by anonymous ftp from `dcssoft.anu.edu.au` (`rpb135.dvi.Z` in directory `pub/Brent`).
2. R. P. Brent and H. T. Kung, "Fast algorithms for manipulating formal power series", *J. ACM* 25 (1978), 581-595.
3. 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. Available by anonymous ftp from `dcssoft.anu.edu.au` (`rpb134.*.Z` in directory `pub/Brent`).
4. 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.
5. 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.
6. 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.
7. H. Davenport, *Multiplicative Number Theory*, second edition (revised by H. L. Montgomery), Springer-Verlag, New York, 1980.
8. P. G. Lejeune Dirichlet, *Vorlesungen über Zahlentheorie*, fourth edition, Friedr. Vieweg & Sohn, Braunschweig, 1894, Chapter 5 and Supplement 7.
9. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, fifth edition, Clarendon Press, Oxford, 1984, Ch. 16.
10. D. E. Knuth, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms* (second edition), Addison-Wesley, Menlo Park, 1981, Chapter 3.
11. 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.

12. M. Kraitchik, *Recherches sur la Théorie des Nombres*, Volume 1, Gauthiers-Villars, Paris, 1924.
13. E. Lucas, "Théorèmes d'arithmétique", *Atti. R. Acad. Sc. Torino* 13 (1877-8), 271-284.
14. E. Lucas, "Sur la série récurrente de Fermat", *Bull. Bibl. Storia Sc. Mat. e Fis.* 11 (1878), 783-789.
15. E. Lucas, "Sur les formules de Cauchy et de Lejeune-Dirichlet", *Ass. Française pour l'Avanc. des Sci., Comptes Rendus* 7 (1878), 164-173.
16. Hans Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, Boston, 1985.
17. A. Schinzel, "On the primitive prime factors of $a^n - b^n$", *Proc. Cambridge Philos. Soc.* 58 (1962), 555-562.
18. Peter Stevenhagen, "On Aurifeuillian factorizations", *Nederl. Akad. Wetensch. Indag. Math.* 49 (1987), 451-468.

Computer Sciences Lab, Australian National University, Canberra, ACT 0200
E-mail address: rpb@cslab.anu.edu.au