BINARY BBP-FORMULAE FOR LOGARITHMS AND GENERALIZED GAUSSIAN-MERSENNE PRIMES

Marc Chamberland

Department of Mathematics and Computer Science

Grinnell College

Grinnell, IA, 50112

E-mail: chamberl@math.grinnell.edu

Abstract.

Constants of the form

$$C = \sum_{k=0}^{\infty} \frac{p(k)}{q(k)b^k}$$

where p and q are integer polynomials, $\deg p < \deg q$, and $p(k)/q(k)$ is non-singular for non-negative k and $b \geq 2$, have special properties. The nth digit (base b) of C may be calculated in (essentially) linear time without computing its preceding digits, and constants of this form are conjectured to be either rational or normal to base b.

This paper constructs such formulae for constants of the form $\log p$ for many primes p. This holds for all Gaussian-Mersenne primes and for a larger class of "generalized Guassian-Mersenne primes." Finally, connections to Aurifeuillian factorizations are made.

AMS (MOS) subject classification : 11Y05 (11A41, 11B99, 11T22, 11Y60).

Keywords: primes, Gaussian-Mersenne, BBP, Aurifeuillian.

1   Introduction

The 1997 paper of Bailey, Borwein and Plouffe[2] heralded a new era for the computation of various transcendental constants. For formulae such as the alluring

$$\pi = \sum_{k=0}^{\infty} \frac{1}{16^k} \left(\frac{4}{8k+1} - \frac{2}{8k+4} - \frac{1}{8k+5} - \frac{1}{8k+6} \right)$$

and more generally

$$C = \sum_{k=0}^{\infty} \frac{p(k)}{q(k)b^k}$$

where p and q are integer polynomials, $\deg p < \deg q$, and $p(k)/q(k)$ is non-singular for non-negative k and $b \in \mathbf{Z}^+$, they showed that the nth digit (base b) may be calculated in (essentially) linear time without computing its preceding digits. Moreover, constants of this form are conjectured to be either rational or normal to base b; see Bailey and Crandall[3]. Bailey[1] has recently catalogued a collection of these BBP-formulae.

Curiously, these formulae intersect with the search for prime numbers. Recall that the Gaussian-Mersenne primes (Sloane A057429) are the primes p such that $((1+i)^p - 1)((1-i)^p - 1)$ is prime. Not only will we see that $\log q$ has a BBP-formula for every Gaussian-Mersenne prime q, but also for a much broader sequence of "generalized Gaussian-Mersenne primes."

Section 2 shows how evaluating cyclotomic polynomials at particular complex values yields new BBP-formulae, which in turn is used to motivate the definition of generalized Gaussian-Mersenne primes. In performing such calculations, certain redundancies keep cropping up, shown to be related to Aurifeuillian identities. Section 3 shows how the cyclotomic polynomials can be used to construct such formulae.

2 Cyclotomic Polynomials and Generalized Gaussian-Mersenne Primes

Perhaps the simplest BBP-formula for logarithms is the classical

$$\log 2 = \sum_{k=1}^{\infty} \frac{1}{k2^k}.$$

Bailey *et al.*[2] sought to determine all integers m such that $\log m$ has a *binary* BBP-formula, that is, where $b = 2^l$. Bailey and Crandall noted that the space of constants which admit a binary BBP-formula is linear; if C_1 has such a formula with base 2^{l_1} and C_2 has a formula with base 2^{l_2}, then $C_1 + C_2$ has a formula with base $2^{\mathrm{lcm}(l_1,l_2)}$. Since

$$\log(2^n - 1) - n \log 2 = \log\left(1 - \frac{1}{2^n}\right) = -\sum_{k=1}^{\infty} \frac{1}{k2^{kn}},$$

$\log(2^n - 1)$ has a binary BBP-formula, subsequently yielding formulae for $\log(2^n + 1)$ and the natural logarithm of any integer of the form

$$\frac{(2^{a_1} - 1)(2^{a_2} - 1)\cdots(2^{a_h} - 1)}{(2^{b_1} - 1)(2^{b_2} - 1)\cdots(2^{b_j} - 1)}. \tag{1}$$

The paper [2] gave a list of some primes which have this form. Bailey [1] extended this list by using the expression

$$\mathrm{Re}\left(\log\left(1 \pm \frac{(1+i)^k}{2^n}\right)\right) \tag{2}$$

suggested by R. Harley and J. Borwein. This expression has a binary BBP-formula since, for example,

$$
\begin{aligned}
\log\left(1 - \frac{1+i}{2^n}\right) &= -\sum_{j=1}^{\infty} \left(\frac{1+i}{2^n}\right)^j \frac{1}{j} \\
&= -\sum_{j=0}^{\infty} \sum_{k=1}^{8} \left(\frac{1+i}{2^n}\right)^{8j+k} \frac{1}{8j+k} \\
&= -\sum_{j=0}^{\infty} \frac{1}{2^{(8n-4)j}} \sum_{k=1}^{8} \left(\frac{1+i}{2^n}\right)^k \frac{1}{8j+k}.
\end{aligned}
$$

A crucial tool for factoring numbers of the form $b^n - 1$ is the classical theory of cyclotomic polynomials:

$$b^n - 1 = \prod_{d|n} \Phi_d(b) \tag{3}$$

where $\Phi_d(x)$, the dth cyclotomic polynomial, is defined as

$$\Phi_d(x) = \prod_{j=1}^{\phi(d)} (x - \zeta_j).$$

The terms ζ_j are the primitive d^{th} roots of unity and $\phi(\cdot)$ is the Euler totient function. Alternatively, a well-known identity for these polynomials derived using Möbius inversion is

$$\Phi_d(x) = \prod_{k|d} (1 - x^{d/k})^{\mu(k)} \tag{4}$$

where $\mu(\cdot)$ is the Möbius function.

In conjunction with expression (1), Bailey $et\ al.$ state that $\log \Phi_m(2)$ admits a binary BBP-formula for all positive integers m. One may easily extend this to

$$\log\ \Phi_m(2^k) \tag{5}$$

for all integers k. However, the cyclotomic polynomials may be used to obtain many other values. Using the Möbius formula (4) with $x = (\pm 1 + i)/2^n$ yields

$$\mathrm{Re}\left(\log\ \Phi_m\left(\frac{\pm 1 + i}{2^n}\right)\right) = \sum_{d|m} \mu(d)\mathrm{Re}\left(\log\left(1 - \left(\frac{\pm 1 + i}{2^n}\right)^{m/d}\right)\right). \tag{6}$$

As in the consideration of the expression (2), the right side is a binary BBP-formula. Though it is simply a linear combination of expressions of the form (2), the advantage here is that implicitly some cancellation may take place. For example, we have

$$\mathrm{Re}\left(\log \Phi_6\left(\frac{1 + i}{16}\right)\right) = \frac{1}{2}\left[\log 14449 - 14 \log 2\right],$$

hence 14449 joins the list. Similarly, one may use the Möbius formula (4) with $x = (\pm 1 + \sqrt{3}i)/2^n$ to obtain

$$
\text{Re}\left(\log \; \Phi_m \left(\frac{\pm 1 + \sqrt{3}i}{2^n} \right) \right) = \sum_{d|m} \mu(d) \text{Re}\left(\log \left(1 - \left(\frac{\pm 1 + \sqrt{3}i}{2^n} \right)^{m/d} \right) \right),
$$

(7)

again producing binary BBP-formulae. An example here is

$$
\text{Re}\left(\log \; \Phi_5 \left(\frac{1 + \sqrt{3}i}{4} \right) \right) = \frac{1}{2}\left[\log 331 - 8 \log 2 \right],
$$

so 331 comes onto the list. Again, such results are linear combinations of earlier formulae since, for example,

$$
\text{Re}\left(\log \left(1 - \frac{1 + \sqrt{3}i}{2}x \right) \right) = \log(1 - x^3) - \log(1 - x).
$$

Modest calculations with Maple produced the following augmentation of Bailey's list of primes whose logarithm admits a binary BBP-formula (underlined numbers are given by Bailey[1]):

2, 3, 5, 7, 11, 13, 17, 19, 29, 31, 37, 41, 43, 61, 73, 109, 113, 127, 151, 241, 257, 331 , 337, 397, 683, 1321, 1429, 1613, 2113, 2731, 5419, 8191, 14449, 26317, 38737, 43691, 61681, 65537, 87211, 131071, 174763, 246241, 262657, 268501, 279073, 312709, 524287, 525313, 599479, 2796203, 4327489, 7416361, 15790321, 18837001, 22366891, 29247661, 47392381, 107367629, 536903681, 1326700741, 4278255361, 4562284561, 40388473189, 77158673929, 118750098349, 415878438361, 1133836730401, 2932031007403, 3630105520141, 4363953127297, 4432676798593, 4981857697937, 108140989558681, 140737471578113, 1041815865690181, 96076791871613611, 18446744069414584321, 5302306226370307681801, 2048568835297380486760231, 170594105047383239992180849, 84159375948762099254554456081, 134304196845099262572814573351, 19177458387940268116349766612211, 304832756195865229284807891468769, 1339272539833668386958920468400193, 3652124453410972878264128353955921,

17723039943798878297697950773025614516, 611314287240422783484044389824161303296,
14615030311274778250999793695434731225480429568016,
8679885647472749271631248681278986579764893131376395696

Of course, products of two primes, three primes, etc. were found to be on the list. Keeping track of these products of primes helps generate new single primes. For example, since $2^{11} - 1 = 23 \times 89$, the product 23×89 is on the list. In addition, we have

$$\mathrm{Re}\left(\log\ \Phi_6\left(\frac{1+\sqrt{3}i}{2^{12}}\right)\right) = \frac{1}{2}\left[\log 7 + 2\log(23 \times 89) + \log 599479 - 44\log 2\right],$$

so this is how 599479 was obtained. Products of two primes which are on the list include:

23×89, 47×178481, 53×157, 59×3033169, 67×20857, 71×122921, 79×121369,

83×8831418697, 97×673, 101×8101, 137×953, 139×168749965921, 149×184481113, 181×54001,

193×22253377, 197×19707683773, 229×457, 223×616318177, 251×4051, 277×30269,

281×86171, 283×165768537521, 313×1249, 353×2931542417, 571×160465489,

593×231769777, 601×1801, 631×23311, 641×6700417, 1013×1657, 1777×25781083,

3121×21841, 3761×7484047069, 5581×384773, 8681×49477, 10169×43249589,

13367×164511353, 32377×1212847, 92737×649657, 179951×3203431780337,

181549 × 12112549

Note that all the primes up to 101 are on the list, either alone or multiplied by one other prime. Indeed, every odd prime p is on the list, either alone or in some multiple product of primes since $2^{p-1} - 1$ is on the list and $p|(2^{p-1} - 1)$. Carl Pomerance (see [2]) showed that 23 could not be written in the form (1); however, it is still unknown whether $\log 23$ has a binary BBP-formula. Related questions are extensively dealt with by Borwein, Borwein and Galway[4].

An important subclass of binary BBP-formulae concerns the expression

$$\mathrm{Re}\left(\log\ \Phi_m\left(\frac{1+i}{2}\right)\right). \qquad (8)$$

Letting m equal a prime $p = 4k + 1$, we have

$$\begin{aligned}
\Phi_p\left(\frac{1+i}{2}\right) &= 1 + \left(\frac{1+i}{2}\right) + \left(\frac{1+i}{2}\right)^2 + \cdots + \left(\frac{1+i}{2}\right)^{(4k+1)} \\
&= \frac{\left(\frac{1+i}{2}\right)\left(\frac{1+i}{2}\right)^{4k} - 1}{\left(\frac{1+i}{2} - 1\right)} \\
&= 1 + i\left(1 - \left(-\frac{1}{4}\right)^k\right),
\end{aligned}$$

which produces

$$\begin{aligned}
\mathrm{Re}\left(\log\Phi_p\left(\frac{1+i}{2}\right)\right) &= \frac{1}{2}\log\left(1 + \left(1 - \left(-\frac{1}{4}\right)^k\right)^2\right) \\
&= \frac{1}{2}\log\left(2\cdot 4^{2k} - 2(-4)^k + 1\right) - 2k\log 2 \\
&= \frac{1}{2}\log\left((1+i)^{(4k+1)} - 1\right)\left((1-i)^{(4k+1)} - 1\right) - 2k\log 2 \\
&= \frac{1}{2}\log\left((1+i)^p - 1\right)\left((1-i)^p - 1\right) - 2k\log 2 \\
&= \frac{1}{2}\log\left(\frac{\left((1+i)^p - 1\right)\left((1-i)^p - 1\right)}{2^{4k}}\right).
\end{aligned}$$

A similar calculation may be done for primes of the form $p = 4k - 1$. We then have that if q is a Gaussian-Mersenne prime, then $\log q$ admits a binary BBP-formula. This connection implies a larger question: For which positive integers m is the numerator of the rational expression

$$\exp\left(2\mathrm{Re}\left(\log\Phi_m\left(\frac{1+i}{2}\right)\right)\right) \qquad (9)$$

prime? Besides the Gaussian-Mersenne primes, many composite m satisfy this condition. These generalized Gaussian-Mersenne primes, checked for all $m < 3000$, are listed below (the regular Gaussian-Mersenne primes are underlined).

$$2, \underline{3}, 4, \underline{5}, \underline{7}, 9, 10, \underline{11}, 12, 14, 15, 18, \underline{19}, 21, 22, 26, 27, \underline{29}, 30, 33, 34, 35, 42, 45,$$

$\underline{47}, 49, 51, 54, 55, 58, 63, 65, 66, 69, 70, \underline{73}, \underline{79}, 85, 86, 87, 105, 106, 110, 111, \underline{113}, 114,$

$126, 129, 138, 147, \underline{151}, \underline{157}, \underline{163}, \underline{167}, 178, 186, 189, 217, 231, \underline{239}, \underline{241}, 242,$

$\underline{283}, 319, 323, 350, \underline{353}, 363, \underline{367}, 375, \underline{379}, 385, 391, \underline{457}, 462, 522, 543, 566, 602, 621,$

$633, 651, 679, 741, 779, 819, 871, 885, \underline{997}, 1062, 1114, 1126, 1150, 1226, 1275, 1317,$

$1329, \underline{1367}, 1382, 1434, 1477, 1710, 1926, 1970, 2331, 2422, 2446, 2995.$

Some of the primes produced by expression (9) have been put on the previous list of primes. When $m = 2995$, this produces a prime with over 700 digits.

3   Aurifeuillian Factorizations

Since the cyclotomic polynomials are irreducible in $\mathbf{Z}[x]$, it would seem no further factorization of $b^n - 1$ in equation (3) is possible. However, by imposing certain restrictions on x, other factorizations exist. An example is

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

which, upon letting $x = 5^{2k-1}$ and factoring the difference of squares, yields

$$\Phi_5(5^{2k-1}) = [5^{4k-2} + 3 \cdot 5^{2k-1} + 1 - 5^k(5^{2k-1} + 1)][5^{4k-2} + 3 \cdot 5^{2k-1} + 1 + 5^k(5^{2k-1} + 1)].$$

These special polynomial identities were first noted by A. Aurifeuille and subsequently generalized by E. Lucas. References and other examples of Aurifeuillian identities may be found in Brillhart *et al.* [6], as well as their use in factoring. Theorems regarding writing $\Phi_n(x)$ as a difference of squares may be found in Schinzel[7], Stevenhagen[8] and Brent[5].

Earlier we saw that $\log(2^n \pm 1)$ has a binary BBP-formula. Bailey[1]) notes that

$$\mathrm{Re}\left(\log\left(1 \pm \frac{1+i}{2^n}\right)\right) = \left(\frac{1}{2} - n\right)\log 2 + \frac{1}{2}\log\left(2^{2n-1} \pm 2^n + 1\right),$$

so the two expressions $2^{2n-1} \pm 2^n + 1$ come onto the list. However, multiplying these terms gives the classical Aurifeuillian identity

$$2^{4n-2} + 1 = \left(2^{2n-1} + 2^n + 1\right)\left(2^{2n-1} - 2^n + 1\right).$$

This demonstrates why some calculations used in the last section to generate the list of primes were redundant. Indeed, in searching for various families of factors, similar identities arise. We now develop other Aurifeuillian identities, interesting for their own sake, and make connections to expressions used in the last section. Let us start with a general theorem regarding cyclotomic polynomials.

Theorem 3.1 *Let* $m, n \in \mathbf{Z}^+$ *satisfy* $\gcd(m, n) = 1$ *and at least one of* m *or* n *is greater than 2. Then*

$$\Phi_{mn}(x) = \prod_{j=1}^{\phi(m)} \Phi_n(x\zeta_j) \tag{10}$$

where ζ_j *are the primitive* m^{th} *roots of unity.*

Proof: Since the degree of $\Phi_n(x)$ is $\phi(n)$, the degree of the left side polynomial of (10) is $\phi(mn) = \phi(m)\phi(n)$, matching the degree of the right. The left polynomial is monic, while the leading coefficient of the right side is

$$\prod_{j=1}^{\phi(m)} \zeta_j^{\phi(n)} = \left(\prod_{j=1}^{\phi(m)} \zeta_j\right)^{\phi(n)}$$
$$= 1$$

so the right is also monic. It remains to show that the roots of each side are the same.

The roots of $\Phi_{mn}(x)$ are simply $e^{ki2\pi/mn}$ with $\gcd(k, mn) = 1$. We will show that each of these $\phi(mn)$ distinct roots is also a root of the right side. To expand the right side, first note that each ζ_j has the form $e^{li2\pi/m}$ for some l satisfying $\gcd(l, m) = 1$. This combines to give

$$x\zeta_j = e^{(k+ln)i2\pi/mn}$$

so it is suffices to show that for each k there exists an l such that

$$\gcd\left(\frac{k+ln}{m},n\right)=1.$$

Since $\gcd(k,mn)=1$, we have $\gcd(k,n)=1$. This implies that $\gcd(k+ln,n)=1$ and, using the Euclidean algorithm with $\gcd(m,n)=1$, there exists an l such that $k+ln$ is a multiple of m. This completes the proof. $\quad\square$

With the identities

$$\Phi_{2^kn}(x)=\Phi_n\left(-x^{2^{k-1}}\right),\quad n\text{ odd}$$

and

$$\Phi_{pn}(x)=\Phi_n(x^p),\quad p\text{ prime, }p\nmid n,$$

we construct several examples.

Example 3.1 The case $m=4$ was foreshadowed by Schinzel[7, formula (12)]. Letting n be odd in Theorem 3.1 gives

$$\Phi_n(-x^2)=\Phi_{4n}(x)=\Phi_n(ix)\Phi_n(-ix).$$

Replacing x with ix gives

$$\Phi_n(x^2)=\Phi_n(x)\Phi_n(-x).$$

Example 3.2 Letting $m=8$, n odd, we have

$$\Phi_{8n}(x)=\left[\Phi_n\left(x\frac{1+i}{\sqrt{2}}\right)\Phi_n\left(x\frac{1-i}{\sqrt{2}}\right)\right]\left[\Phi_n\left(x\frac{-1+i}{\sqrt{2}}\right)\Phi_n\left(x\frac{-1-i}{\sqrt{2}}\right)\right]. \tag{11}$$

Replacing x with $\sqrt{2}x$ yields

$$\Phi_n(-4x^4)=\Phi_{4n}(2x^2)$$
$$=\left[\Phi_n(x(1+i))\Phi_n(x(1-i))\right]\left[\Phi_n(x(-1+i))\Phi_n(x(-1-i))\right]. \tag{12}$$

If x is real, the two right side expressions must be integer polynomials since they are each the product of complex conjugates. Example subcases with $x=2^k$ are

n=1:

$$2^{4k+2} + 1 = (2^{2k+1} + 2^{k+1} + 1)(2^{2k+1} - 2^{k+1} + 1)$$

n=15:

$$2^{32k+16} + 2^{28k+14} - 2^{20k+10} - 2^{16k+8} - 2^{12k+6} + 2^{4k+2} + 1 = L \cdot R$$

where

$$
\begin{aligned}
L, R \; = \; & 2^{16k+8} \pm 2^{15k+8} + 2^{14k+7} \pm 2^{13k+7} + 2^{12k+7} \pm 2^{11k+7} + 3 \cdot 2^{10k+5} \pm 2^{9k+6} \\
& + 3 \cdot 2^{8k+4} \pm 2^{7k+5} + 3 \cdot 2^{6k+3} \pm 2^{5k+4} + 2^{4k+3} \pm 2^{3k+2} + 2^{2k+1} \pm 2^{k+1} + 1
\end{aligned}
$$

Getting back to the redundancies in our earlier calculations, let $x = 1/2^k$ in (12) to produce

$$\mathrm{Re}\left(\log\ \Phi_{4n}\left(\frac{1}{2^{2k-1}}\right)\right) = 2\left[\mathrm{Re}\left(\log\ \Phi_n\left(\frac{1+i}{2^k}\right)\right) + \mathrm{Re}\left(\log\ \Phi_n\left(\frac{-1+i}{2^k}\right)\right)\right].$$

This shows how terms from (5) and (6) appear in some factorizations.

Example 3.3 Letting $m = 12$ and $2, 3 \nmid n$, we have

$$\Phi_{12n}(x) = \Phi_n\left(x\frac{\sqrt{3}+i}{2}\right)\Phi_n\left(x\frac{\sqrt{3}-i}{2}\right)\Phi_n\left(x\frac{-\sqrt{3}+i}{2}\right)\Phi_n\left(x\frac{-\sqrt{3}-i}{2}\right) \tag{13}$$

Replacing x with $2\sqrt{3}x$ gives

$$\Phi_{6n}(12x^2) = \left[\Phi_n\left(x(3+\sqrt{3}i)\right)\Phi_n\left(x(3-\sqrt{3}i)\right)\right]\left[\Phi_n\left(x(-3+\sqrt{3}i)\right)\Phi_n\left(x(-3-\sqrt{3}i)\right)\right]$$

Again, the two right side expressions must be integer polynomials. Example subcases with $x = 2^{k-1}$ are

n=1:

$$9 \cdot 2^{4k} - 3 \cdot 2^{2k} + 1 = (3 \cdot 2^{2k} - 3 \cdot 2^k + 1)(3 \cdot 2^{2k} + 3 \cdot 2^k + 1)$$

n=5:

$$
\begin{aligned}
& 2^{16k}3^8 + 2^{14k}3^7 - 2^{10k}3^5 - 2^{8k}3^4 - 2^{6k}3^3 + 2^{2k}3 + 1 \\
& \quad (2^{8k}3^4 + 2^{7k}3^4 + 2^{6k+1}3^3 + 2^{5k}3^3 + 2^{4k}3^2 + 2^{3k}3^2 + 2^{2k+1}3 + 2^k3 + 1) \\
& \quad \times (2^{8k}3^4 - 2^{7k}3^4 + 2^{6k+1}3^3 - 2^{5k}3^3 + 2^{4k}3^2 - 2^{3k}3^2 + 2^{2k+1}3 - 2^k3 + 1)
\end{aligned}
$$

To show how equation (13) produces redundancies, replace x with $x(\sqrt{3} + i)/2$ to obtain

$$\Phi_{6n}\left(\frac{1 + \sqrt{3}i}{2}x^2\right) = \Phi_{12n}\left(\frac{\sqrt{3} + i}{2}x\right) = \Phi_n\left(\frac{1 + \sqrt{3}i}{2}x\right)\Phi_n\left(\frac{-1 - \sqrt{3}i}{2}x\right)\Phi_n(x)\Phi_n(-x).$$

With $x = 1/2^{k-1}$ this yields the relationship

$$\begin{aligned}
\mathrm{Re}\left(\log\Phi_{6n}\left(\frac{1 + \sqrt{3}i}{2^{2k-1}}\right)\right) &= \mathrm{Re}\left(\log\Phi_n\left(\frac{1 + \sqrt{3}i}{2^k}\right)\right) + \mathrm{Re}\left(\log\Phi_n\left(\frac{-1 + \sqrt{3}i}{2^k}\right)\right) \\
&\quad + \log\Phi_n\left(\frac{1}{2^{k-1}}\right) + \log\Phi_n\left(\frac{-1}{2^{k-1}}\right).
\end{aligned}$$

This shows how terms from (5) and (7) appear in some factorizations.

References

[1] Bailey, D.H. A Compendium of BBP-Type Formulas for Mathematical Constants. Preprint, http://crd.lbl.gov/~dhbailey/dhbpapers/index.html, (2000).

[2] Bailey, D.H., Borwein, P.B. and Plouffe, S. On the Rapid Computation of Various Polylogarithmic Constants. *Mathematics of Computation*, 66(218):903–913, (1997).

[3] Bailey, D.H., Crandall, R.E. On the random character of fundamental constant expansions. *Experimental Mathematics*, 10(2):175–190, (2001).

[4] Borwein, D., Borwein, J.M., Galway,W.F. Finding and Excluding b-ary Machin-Type BBP Formulae. *Canadian Journal of Mathematics*, submitted, (2003). CECM Preprint 2003:195.

[5] R. Brent. Computing Aurifeuillian factors. *Computational algebra and number theory (Sydney, 1992)*, Mathematics and its Applications, <u>325</u>:201–212, Kluwer, Dordrecht, (1995).

[6] J. Brillhart, D.H. Lehmer, J.L. Selfridge, B. Tuckerman, and S.S. Wagstaff,Jr. *Factorizations of $b^n \pm 1$*. American Mathematical Society, Providence, (1983).

[7] A. Schinzel. On Primitive Prime Factors of $a^n - b^n$. *Proceedings of the Cambridge Philosophical Society*, <u>58</u>(4):555–562, (1962).

[8] P. Stevenhagen. On Aurifeuillian Factorizations. *Proceedings of the Koninklijke Akademie van Wetenschappen*, <u>90</u>(4):451–468, (1987).