MATHEMATICS OF COMPUTATION
VOLUME 57, NUMBER 196
OCTOBER 1991, PAGES 839–848

THE PRIME FACTORS OF WENDT'S BINOMIAL CIRCULANT DETERMINANT

GREG FEE AND ANDREW GRANVILLE

ABSTRACT. Wendt's binomial circulant determinant, W_m, is the determinant of an m by m circulant matrix of integers, with (i, j)th entry $\binom{m}{|i-j|}$ whenever 2 divides m but 3 does not. We explain how we found the prime factors of W_m for each even $m \le 200$ by implementing a new method for computations in algebraic number fields that uses only modular arithmetic. As a consequence we prove that if p and $q = mp + 1$ are odd primes, 3 does not divide m, and $m \le 200$, then the first case of Fermat's Last Theorem is true for exponent p.

1. INTRODUCTION

For a given positive even integer m, define W_m to be the determinant of the m by m circulant matrix with top row $(a_0, a_1, \dots, a_{m-1})$, where

$$g_m(X) := \sum_{i=0}^{m-1} a_i X^i := \begin{cases} (X+1)^m - X^m & \text{if 6 does not divide } m, \\ \dfrac{(X+1)^m - X^m}{(X^2+X+1)} & \text{if 6 divides } m. \end{cases}$$

When 6 does not divide m, the (i, j)th entry is $\binom{m}{|i-j|}$, and this matrix is given the name in the title. There are a variety of applications of W_m in number theory, in particular to Fermat's Last Theorem. In this paper we will explain how we computed the prime factors of W_m for each even $m \le 200$, and as a consequence have the following result:

Theorem. *If p and $q = mp + 1$ are odd primes with $m \le 200$, then the first case of Fermat's Last Theorem is true for exponent p if 6 does not divide m, and for exponent p^2 if 6 does divide m.*

Previous results of this type have had the restriction that 6 does not divide m (which we remove as a consequence of [10]). Such a theorem has been proved for all $m \le 110$ in [4], and W_m has been computed as far as $m = 50$ in [6].

In [1], Boyd did an analytic investigation of the size of W_m and showed that if 6 does not divide m, then

$$10^{-1/3}\lambda^{m^2} < |W_m| < 10^{1/3}\lambda^{m^2}, \tag{1.1}$$

Received February 5, 1990; revised August 22, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11Y40; Secondary 11C20, 11D41, 11R18.
The second author was supported, in part, by the National Science Foundation (grant number DMS-8610730).

where $\log\lambda := \frac{2}{\pi}\int_0^{\pi/3}\log(2\cos\theta)\,d\theta$ $(\approx 0.323\ldots)$. (Alternatively, we can define $\log\lambda := (3\sqrt{3}/4\pi)L(2,\chi)$, where $L(s,\chi)$ is the Dirichlet L-function for the quadratic character $\chi(\cdot)$ of conductor 3.)

2. Our computational method

There are many ways to determine the value of W_m. The most obvious is to simply compute the determinant of the matrix above; unfortunately, this is extremely costly for, say, $m = 100$.

A beautiful theorem of Stern [17] states that the determinant of a circulant matrix with top row $(b_0, b_1, \ldots, b_{m-1})$ is equal to the resultant of $X^m - 1$ with the polynomial $b(X) := \sum_{i=0}^{m-1} b_i X^i$. Thus,

$$W_m = \prod_{\zeta^m=1} g_m(\zeta), \tag{2.1}$$

and it is this formula that forms the basis for our computational method. Now $g_m(X) = \prod(1 + X - \zeta X)$, where the product is over all mth roots of unity ζ, except primitive cube roots of unity. Combining this with (2.1), we see that the set of prime divisors of W_m is given by the set of prime divisors of

$$N(1 + \zeta^i + \zeta^j) \quad \text{with } 0 \le i, j \le m-1 \text{ and } i \ne m/3 \text{ or } 2m/3, \tag{2.2}$$

where $\zeta := \exp(2i\pi/m)$ and $N(\cdot)$ is the norm taken over the field extension $\mathbf{Q}(\zeta)|\mathbf{Q}$. We shall compute these norms.

There are a few different ways to compute such norms in algebraic number fields. The first is to approximate the complex numbers $(1 + \zeta^i + \zeta^j)$ to many significant digits and then to multiply them together, being careful with rounding errors. As the product (that is, the norm) is an integer, we need only enough significant digits to ensure that we can determine which integer it is. This approach will be very costly for large m.

A second approach is to treat complex numbers in $\mathbf{Z}[\zeta]$ $(\cong \mathbf{Z}[X]/\phi_m(X))$ as polynomials in X, where we may replace X to any power (say p) greater than m, by X^{p-m}. Thus, as we multiply together conjugates, we work with m-vectors of integers and so avoid rounding errors. However, the necessary vector manipulations now become quite costly when m is large.

Our approach borrows the idea of 'single point evaluation' from the methods of symbolic computation [2], to compute these norms rather more efficiently. The main idea that we use is summed up by

Proposition 1. *Let N be the norm of $1+\zeta^i+\zeta^j$ over $\mathbf{Q}(\zeta)|\mathbf{Q}$. If t is a positive integer with $|N| < \phi_m(t)/2$ (where $\phi_m(X)$ is the mth cyclotomic polynomial), then N is the least residue, in absolute value, of*

$$A := \prod_{\substack{k=1\\(k,m)=1}}^{m} (1 + t^{ik} + t^{jk}) \quad \textit{modulo } \phi_m(t). \tag{2.3}$$

Note that

$$N(1+\zeta^i+\zeta^j)=\prod_{\substack{k=1\\(k,m)=1}}^{m}(1+\zeta^{ik}+\zeta^{jk}). \tag{2.4}$$

As $|\zeta|=1$, thus $|1+\zeta^{ik}+\zeta^{jk}|\le 3$, and so $|N|\le 3^{\varphi(m)}$; therefore, we can take $t=4$ in Proposition 1. Actually one can usually take $t=2$:

Proposition 2. *If α and β are primitive ath and bth roots of unity with α, β and $\alpha\overline{\beta}\neq 1$, and $m=[a,b]$ $(=\operatorname{lcm}[a,b])$, then*

$$|N_{\mathbf{Q}(\zeta)|\mathbf{Q}}(1+\alpha+\beta)|<\phi_m(2)/2 \tag{2.5}$$

except if $1+\alpha+\beta$ is a conjugate or multiple of one of $1+\zeta_3+\zeta_6$, $1+\zeta_4^3+\zeta_8$, $1+\zeta_5^2+\zeta_{10}$, $1+\zeta_4+\zeta_6$, $1+\zeta_7^2+\zeta_{14}$, $1+\zeta_6+\zeta_{18}$, $1+\zeta_6+\zeta_{10}$, where $\zeta_n=\exp(2i\pi/n)$.

Thus, to compute N, we had only to compute the product in (2.3) (with $t=2$), in modular arithmetic, a relatively inexpensive task with a multi- or arbitrary precision package (we used 'C'): Not much is lost here (in terms of the number of digits) as we know that 'on average' (multiplicatively) our norms are exponential in $\varphi(m)$ by (1.1).

The method used here is applicable to a wide range of computations in algebraic number fields (as may be discerned from the proof of Proposition 1 below); for instance, the same idea was used in [7] to compute the class numbers of prime cyclotomic fields, for all primes up to 3000.

In our computations we went up to $m=200$, although we could have gone much further (the modulus in (2.3) has no more than $1+[\varphi(m)\log 2/\log 10]\le 29$ digits for $m\le 200$). The difficulty in our method (or indeed any method), as m grows large, is the factorization of the norms: up to $m=200$ we used Pollard's $p-1$ algorithm [15] and Morrison and Brillhart's continued fraction algorithm [14], but for $m=1000$, say, no known factoring algorithm would help!

Proof of Proposition 1. By comparing the terms of the products in (2.3) and (2.4) we see that $N\equiv A$, modulo the ideal $(t-\zeta)$ of the ring $\mathbf{Z}[\zeta]$. However, N and A are both integers, by definition. Therefore, as $t-\zeta$ divides $N-A$ (in $\mathbf{Z}[\zeta]$), thus each conjugate of $t-\zeta$ does, and so their product, $\phi_m(t)$, divides $N-A$.

Now $|N|<\phi_m(t)/2$ and $N\equiv A \pmod{\phi_m(t)}$, and so can only be the least residue, in absolute value, of $A \pmod{\phi_m(t)}$. □

3. Some results and heuristics

We present, in Table I, a sample of our computations. We give the number of primes dividing each W_m (other than the prime factors of m itself) and the largest of these primes.

TABLE 1

Some statistics on the prime divisors of Wendt determinants

m	Number of primes dividing W_m	Largest prime dividing W_m
10	3	31
20	4	61
30	7	331
40	11	61681
50	17	6101
60	17	4561
80	32	4278255361
100	40	8976001
120	54	4562284561
140	70	175480061
150	86	1133836730401
160	95	44479210368001
180	114	183717901
200	122	31211252919601

The largest prime that we found was 618,970,019,642,690,137,449,562,111, which divides W_{178}. All but a few small prime divisors are $\equiv 1 \pmod{m}$, in each case, which is why Pollard's $p-1$ algorithm was an extremely effective tool in factoring.

When examining the statistics in Table I we noticed that there seem to be around $\frac{1}{32}m(m/\phi(m))\log m$ prime divisors of W_m, the largest of which is exponential in $\varphi(m)$. We now give some rough heuristic arguments to support these observations.

For each m, define $V_m := \prod(1+\zeta^i+\zeta^j)$, where $\zeta = \exp(2i\pi/m)$ and the product is over values of i and j with $0 \le i, j \le m-1$ and $(i, j, m) = 1$. Clearly, $W_m = \prod_{d|m} V_d$, and so $V_m = \prod_{d|m} W_d^{\mu(m/d)}$ for each m. By (1.1) we see that $V_m = \lambda^{m^2 \prod_{p|m}(1-1/p^2)+O(\tau(m))}$, where $\tau(m)$ denotes the number of

divisors of m. We also note that V_m is the product of $m\prod_{p|m}(1+1/p)$ norms. Now as each such norm is $\leq 3^{\varphi(m)}$, and their multiplicative average is $> \lambda^{\varphi(m)}$, we see that some positive proportion of them is $> \lambda^{\varphi(m)/2}$. Thus, if we admit that a randomly chosen integer n is prime with probability $1/\log n$, then we should expect

$$\gg \left\{ m \prod_{p|m} \left(1+\frac{1}{p}\right) \right\} \frac{1}{\varphi(m)} \gg \left(\frac{m}{\varphi(m)}\right)^2$$

of these 'large' norms to be prime.

Now Hardy and Ramanujan [11] showed that almost all integers n have $\{1+o(1)\}\log\log n$ distinct prime factors. So, if we admit that our 'large' norms behave like randomly chosen integers, then we can deduce that their product has

$$\asymp m \prod_{p|m} \left(1+\frac{1}{p}\right) \log\log(\lambda^{\varphi(m)/2}) \asymp m \left(\frac{m}{\varphi(m)}\right) \log m$$

distinct prime factors (where the notation $x \asymp y$ means that $x = O(y)$ and $y = O(x)$).

Both heuristics essentially support our observations.

4. The first case of Fermat's Last Theorem

Fermat's Last Theorem is the following conjecture: For any integer $n \geq 3$, there do not exist nonzero integers x, y, z for which

$$x^n + y^n = z^n \quad \text{with } \gcd(x, y, z) = 1. \tag{4.1}$$

(4.1) is known to have no solutions for any $n \leq 150,000$ [18]; and only finitely many solutions for any given n [5]. The first case of Fermat's Last Theorem for exponent n $(\text{FLTI})_n$ is said to be true if $\gcd(n, xyz) > 1$ in any integer solution of (4.1). $(\text{FLTI})_n$ is known to be true for any $n \leq 7.57 \times 10^{17}$ [3].

In 1823, Sophie Germain [13] showed that if (4.1) has solutions and $q = mn + 1$ is prime, where $m \equiv 2$ or $4 \pmod 6$, then either $\gcd(n, xyz) > 1$ or q divides $(m^m - 1)W_m$. Various authors have modified Sophie Germain's criteria and, most recently, the following result was given in [10] for prime power exponents in (4.1):

Lemma 1. *If p and $q = mp + 1$ are odd primes, q does not divide W_m, and p does not divide m, then the first case of Fermat's Last Theorem is true for exponent p if $6 \nmid m$, and for exponent p^2 if $6|m$.*

We computed the prime divisors of W_m for each even $m \leq 200$ and verified that, for all exponents p for which p divides m or q divides W_m, $(\text{FLTI})_p$ is true (by using Wieferich's Theorem [20]—if p^2 does not divide $2^p - 2$ then $(\text{FLTI})_p$ is true). Thus, we obtained the theorem in §1. Notice that, in many

cases, this theorem provides an easily verified criterion to prove that the first case of Fermat's Last Theorem is true for exponent p.

5. Bounding the values taken by cyclotomic polynomials

Define the power series

$$\Phi(X) = \prod_{n\geq 1}(1 - X^n)^{\mu(n)},$$

which is easily shown to converge absolutely for $|X| < 1$. This power series can be seen to be related to any given cyclotomic polynomial from the well-known formula

$$\phi_m(X) = \prod_{d|m}(X^d - 1)^{\mu(m/d)}, \tag{5.1}$$

which may be rewritten as

$$\left\{\prod_{n|r}(1 - (X^{m/r})^n)^{\mu(n)}\right\}^{\mu(r)},$$

where r is the largest squarefree divisor of m. We shall prove

Proposition 3. *For any $x \geq 2$, $1 - 1/x$ and $\Phi(1/x)$ are, respectively, the infimum and supremum of the set of values taken by $(\phi_m(x)/x^{\varphi(m)})^{\mu(m)}$ with m squarefree and ≥ 2.*

We can easily deduce

Corollary 1. *For any positive integer m and real number x, with $m, |x| \geq 2$,*

$$|\log|\phi_m(x)| - \varphi(m)\log|x|| < \log(|x|/(|x| - 1)). \tag{5.2}$$

Proof of Proposition 3. We start by noting the inequality

$$G_n(x) := \prod_{d>n} 1 - \frac{1}{x^d} \geq 1 - \frac{1}{x^n}, \tag{5.3}$$

which holds for any $n \geq 1$ and $x \geq 2$ (this is easily proved by taking logarithms of both sides and comparing terms).

Let p and q be the smallest primes that do/do not divide m, respectively. Then, by (5.1) and (5.3),

$$\left(\frac{\phi_m(x)}{x^{\varphi(m)}}\right)^{\mu(m)} = \prod_{d|m}\left(1 - \frac{1}{x^d}\right)^{\mu(d)} > \frac{(1 - 1/x)G_p(x)}{1 - 1/x^p} \geq 1 - \frac{1}{x}.$$

Thus, $1 - 1/x$ is a lower bound on our set of values; that it is the infimum comes from noting that if $m = p$ is prime, then

$$\left(\frac{\phi_m(x)}{x^{\varphi(m)}}\right)^{\mu(m)} = \frac{1 - 1/x}{1 - 1/x^p} \hookrightarrow 1 - \frac{1}{x} \quad \text{as } p \hookrightarrow \infty.$$

On the other hand,

$$\frac{(\phi_m(x)/x^{\varphi(m)})^{\mu(m)}}{\Phi(1/x)} = \prod_{d\nmid m}\left(1-\frac{1}{x^d}\right)^{-\mu(d)} < \frac{1-1/x^q}{G_q(x)} \le 1$$

by (5.3). Thus, $\Phi(1/x)$ is an upper bound; we see that it is the supremum by taking m to be the product of the first k primes, so that, by (5.3),

$$\frac{(\phi_m(x)/x^{\varphi(m)})^{\mu(m)}}{\Phi(1/x)} \ge G_{q-1}(x) \ge 1-\frac{1}{x^{q-1}} \hookrightarrow 1$$

as $q \hookrightarrow \infty$ (that is, as $k \hookrightarrow \infty$). □

Proof of Corollary 1. By taking $n = 1$ in (5.3) we find that $\Phi(1/x) < 1$ for any $x \ge 2$, and so (5.2) holds for $x \ge 2$ and m squarefree, by Proposition 3. Now, if r is the largest squarefree divisor of m, then $\phi_m(x) = \phi_r(x^{m/r})$ by (5.1), and so (5.2) follows for m from (5.2) for r. Finally, note that for any x, $\phi_m(x) = \phi_{2m}(-x)$ for m odd and $\phi_m(x) = \phi_m(-x)$ if m is divisible by 4 by (5.1), so (5.2) for $x < -2$ follows from (5.2) for $x > 2$. □

Remark. The power series

$$\Phi(X) = 1 - X + X^2 + X^5 - X^6 + 2X^7 - X^8 + X^9 + X^{11} + X^{13} + 2X^{16} - X^{17} + 2X^{18} + X^{20} + \cdots$$

may well prove of further interest because of its close connection to cyclotomic polynomials. The growth of the coefficients of the cyclotomic polynomials has received much attention; we observe here that the coefficient of X^n in $\Phi(X)$ is bounded above by $p(n)$, the number of partitions of n, as $\Phi(X)$ is majorized by the power series $\prod_{n\ge1}(1-X^n)^{-1}$. It would be interesting to obtain a better bound.

6. Bounding the sum of three roots of unity

In this section we show how to obtain strong bounds on $N(1+\alpha+\beta)$, where N is the norm over the field extension $\mathbf{Q}(\zeta_m)|\mathbf{Q}$, and prove Proposition 2. Previous authors have considered improving the (trivial) bound $N \le 3^{\varphi(m)}$ given in the introduction—the best bound to date is Krasner's $N \le 3^{m/4}$ for $m \equiv 2$ or 4 (mod 6), except in finitely many cases, which was obtained by consideration of circulants [12]. We shall improve Krasner's bound—for instance we will show that $N \le 3^{\varphi(m)/2}$ except when α, β, or $\alpha\overline{\beta}$ is a primitive 6th or 10th root of unity, and a finite number of other exceptional pairs (α, β). These bounds may not be improved by too much—by (1.1) we see that a large number of such norms must be $> (\lambda-\varepsilon)^{\varphi(m)}$ as $m \to \infty$, and we can easily construct a few norms $> \frac{1}{2}3^{\varphi(m)/2}$: If α is a primitive 6th root of unity and β a primitive bth root of unity with $b \equiv 4$ or 8 (mod 12), so that $m = [a, b] = 3b$, then $|N(1+\alpha+\beta)| = \phi_{m/2}(3)$, which is $> \frac{1}{2}3^{\varphi(m)/2}$ by Corollary 1. (Note that $\alpha^{m/2+1} = \alpha$ and $\beta^{m/2+1} = -\beta$, and $(1+\alpha+\beta)(1+\alpha-\beta) = 3\alpha - \beta^2$. Thus,

$N(1+\alpha+\beta)^2 = N(3-\overline{\alpha}\beta^2) = \phi_{m/2}(3)^2$, as $\overline{\alpha}\beta^2$ is a primitive $(m/2)$th root of unity.)

Our starting point is a result of Dénes [4, equation (10)].

Proposition 4. *Suppose* α, β, *and* $\gamma = \alpha\overline{\beta}$ *are given primitive* a, b, *and* cth *roots of unity, respectively. Let* $m = [a, b]$. *Then*

$$|N(1+\alpha+\beta)|^{2/\varphi(m)} \le \tfrac{1}{3}|\phi_a(-2)|^{1/\varphi(a)}|\phi_b(-2)|^{1/\varphi(b)}|\phi_c(-2)|^{1/\varphi(c)}. \tag{6.1}$$

Our derivation of (6.1) is rather different from that of Dénes: We start from the identity

$$|2+\alpha|^2|2+\beta|^2|2+\gamma|^2 = |1-\alpha|^2|1-\beta|^2|1-\gamma|^2 + 9|1+\alpha+\beta|^4. \tag{6.2}$$

(This is easily proved by noting that the right-hand side of (6.2) is the difference of the two squares $(3(1+\alpha+\beta)(1+\overline{\alpha}+\overline{\beta}))^2 - ((1-\alpha)(1-\overline{\beta})(1-\overline{\gamma}))^2$, and the corresponding factors are $(2+\overline{\alpha})(2+\beta)(2+\gamma)$ and its conjugate.)

We now exclude the first term of the right-hand side of (6.2) and take the norm (in $\mathbf{Q}(\zeta_m)|\mathbf{Q}$) of both sides, obtaining the inequality in (6.1).

As an immediate consequence of Proposition 4 and Corollary 1 we can obtain

Corollary 2. *Let* α, β, γ, a, b, c, *and* m *be as in Proposition* 4. *For any fixed* $\varepsilon > 0$, *if* $1/\varphi(a) + 1/\varphi(b) + 1/\varphi(c) < \log(1+\varepsilon)/\log 2$, *then*

$$|N(1+\alpha+\beta)| \le (8(1+\varepsilon)/3)^{\varphi(m)/2}.$$

For instance, this holds if $a, b, c > (4\log 2/\varepsilon)^2$ *and* $\varepsilon \le \frac{1}{2}$.

Taking $\varepsilon = \frac{1}{8}$ in Corollary 2 gives $|N| \le 3^{\varphi(m)/2}$ except if at least one of a, b, and c is small. Now, rearrange α, β, and γ so that $\varphi(a) \le \varphi(b) \le \varphi(c)$. Then, if $|N| > 3^{\varphi(m)/2}$, we see that

$$\frac{2}{\varphi(b)} \ge \frac{1}{\varphi(b)} + \frac{1}{\varphi(c)} \ge \frac{\log(9/8)}{\log 2} - \frac{1}{\varphi(a)},$$

which can occur in only finitely many cases (as c is determined by a and b) unless the right-hand side is ≤ 0. But then $\varphi(a) \le \log 2/\log\frac{9}{8} < 6$, and so $a = 1, 2, 3, 4, 5, 6, 8, 10$, or 12, and we can use (6.1) to further eliminate values of a.

In certain special cases we can improve somewhat on Corollary 2. For instance, we can show that for any $\varepsilon > 0$, we have $|N| \le ((\sqrt{5}+1)/2 + \varepsilon)^{\varphi(m)}$ provided that a is sufficiently large and that there is a sufficiently large prime dividing m that does not divide a.

A sketch of the proof of Proposition 2. We shall show that there are only finitely many possible values of a and b for which (2.5) fails; it thus requires a small amount of computation (for instance, by using Proposition 1 with $t = 4$) to verify the result (alternatively, one can use a lengthy case analysis; see [9] for details).

So suppose (2.5) fails, that is $|N| \geq \phi_m(2)/2$. Let $\gamma = \alpha\overline{\beta}$ be a primitive cth root of unity, and reorder α, β, and γ (taking their conjugates if necessary) so that

$$|\phi_a(-2)|^{1/\varphi(a)} \geq |\phi_b(-2)|^{1/\varphi(b)} \geq |\phi_c(-2)|^{1/\varphi(c)}. \tag{6.3}$$

(Note that $N(1+\alpha+\beta) = N(1+\overline{\alpha}+\overline{\gamma}) = N(1+\overline{\beta}+\gamma)$.) Then, by Corollary 1, Proposition 4, and (6.3), we have

$$\begin{aligned}
(2^{\varphi(m)-2})^{2/\varphi(m)} &\leq (\phi_m(2)/2)^{2/\varphi(m)} \\
&\leq \tfrac{1}{3}|\phi_a(-2)|^{1/\varphi(a)}|\phi_b(-2)|^{1/\varphi(b)}|\phi_c(-2)|^{1/\varphi(c)} \\
&\leq \tfrac{1}{3}|\phi_a(-2)|^{1/\varphi(a)}|\phi_b(-2)|^{2/\varphi(b)} \qquad (6.4) \\
&\qquad (\leq \tfrac{1}{3}|\phi_a(-2)|^{1/\varphi(a)}(2^{\varphi(b)+1})^{2/\varphi(b)}) \\
&\leq \tfrac{1}{3}|\phi_a(-2)|^{3/\varphi(a)} \leq \tfrac{1}{3}(2^{\varphi(a)+1})^{3/\varphi(a)}. \qquad (6.5)
\end{aligned}$$

Now a and b both divide m, so that $1/\varphi(a)$ and $1/\varphi(b)$ are both $\geq 1/\varphi(m)$. Therefore, by (6.5),

$$\tfrac{3}{2} \leq 2^{3/\varphi(a)+4/\varphi(m)} \leq 2^{7/\varphi(a)},$$

and so $\varphi(a) \leq 7\log 2/\log\frac{3}{2}$, which gives a finite number of possibilities for a. Then by (6.4),

$$3/|\phi_a(-2)|^{1/\varphi(a)} \leq 2^{4/\varphi(m)+2/\varphi(b)} \leq 2^{6/\varphi(b)},$$

and so, as $|\phi_a(-2)| < 3^{\varphi(a)}$ for $a > 1$ (by Corollary 1),

$$\varphi(b) \leq 6\log 2/\left\{\log 3 - \frac{1}{\varphi(a)}\log|\phi_a(-2)|\right\},$$

which gives a finite number of possibilities for b. □

Acknowledgment

We would like to thank the referee for his or her careful reading of this paper.

Bibliography

1. D. W. Boyd, *The asymptotic behaviour of the binomial circulant determinant*, J. Math. Anal. Appl. **86** (1982), 30–38.
2. B. W. Char, K. O. Geddes, and G. H. Gonnet, *GCDHEU: Heuristic polynomial GCD algorithm based on integer GCD computation*, Proc. Internat. Sympos. Symbolic and Algebraic Manipulation (J. Fitch, ed.), Lecture Notes in Comput. Sci., vol. 174, Springer-Verlag, Berlin and New York, 1984, pp. 285–296.
3. D. Coppersmith, *Fermat's Last Theorem (case* I*) and the Wieferich criterion*, Math. Comp. **54** (1990), 895–902.
4. P. Dénes, *An extension of Legendre's criterion in connection with the first case of Fermat's Last Theorem*, Publ. Math. Debrecen **2** (1951), 115–120.
5. G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

6. J. S. Frame, *Factors of the binomial circulant determinant*, Fibonacci Quart. **18** (1980), 9–23.
7. G. Fung, A. Granville, and H. C. Williams, *Computations on the first factor of the class number of cyclotomic fields*, J. Number Theory (to appear).
8. P. Furtwängler, *Letzter Fermatscher Satz und Eisensteinsches Reziprozitätsprinzip*, Sitzungsber. Akad. Wiss. Wien. Abt. IIa **121** (1912), 589–592.
9. A. Granville, *Diophantine equations with varying exponents (with special reference to Fermat's Last Theorem)*, Doctoral thesis, Queen's University, Kingston, Ontario, 1987.
10. A. Granville and B. Powell, *On Sophie Germain type criteria for Fermat's Last Theorem*, Acta Arith. **50** (1988), 265–277.
11. G. H. Hardy and S. Ramanujan, *The normal number of prime factors of a number* n, Quart. J. Math. **48** (1917), 76–92.
12. M. Krasner, *A propos du critère de Sophie Germain–Furtwängler pour le premier cas du théorème de Fermat*, Mathematica Cluj **16** (1940), 109–114.
13. A. M. Legendre, *Recherches sur quelques objets d'analyse indéterminée et particulièrement sur le théorème de Fermat*, Mém. Acad. Sci. Inst. France **6** (1823), 1–60.
14. M. Morrison and J. Brillhart, *A method of factoring and the factorization of* $F7$, Math. Comp. **29** (1975), 183–205.
15. J. M. Pollard, *Theorems on factorization and primality testing*, Proc. Cambridge Philos. Soc. **76** (1974), 521–528.
16. P. Ribenboim, 13 *lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.
17. M. A. Stern, *Einige Bemerkungen über eine Determinante*, J. Reine Angew. Math. **73** (1871), 379–380.
18. J. Tanner and S. S. Wagstaff, Jr., *New congruences for the Bernoulli numbers*, Math. Comp. **48** (1987), 341–350.
19. E. Wendt, *Arithmetische Studien über den letzten Fermatschen Satz, welcher aussagt, dass die Gleichung* $a^n = b^n + c^n$ *für* $n > 2$ *in ganzen Zahlen nicht auflösbar ist*, J. Reine Angew. Math. **113** (1894), 335–347.
20. A. Wieferich, *Zum letzten Fermat'schen Theorem*, J. Reine Angew. Math. **135** (1909), 293–302.

Department of Computer Science, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada
E-mail address: gjfee@daisy.waterloo.edu

School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540
Current address: Department of Mathematics, University of Georgia, Athens, Georgia 30602
E-mail address: andrew@joe.math.uga.edu