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 $m \leq 200$ 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 $m \leq 200$, 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 $(a_0, a_1, \ldots, a_{m-1})$, where

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

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 $m \leq 200$, and as a consequence have the following result:

Theorem. If $p$ and $q = mp + 1$ are odd primes with $m \leq 200$, 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 $m \leq 110$ 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

$$ 10^{-1/3} m^{2/3} < |W_m| < 10^{1/3} m^{2/3}, $$

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).

©1991 American Mathematical Society
0025-5718/91 $1.00 + .25 per page

839
where \( \log \lambda := \frac{2}{3} \int_0^{\pi/3} \log(2 \cos \theta) \, d\theta \approx 0.323 \ldots \). (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,

\[
W_m = \prod_{\zeta^m = 1} g_m(\zeta),
\]

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 \( m \)th roots of unity \( \zeta \), 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

\[
N(1 + \zeta^i + \zeta^j) \quad \text{with} \quad 0 \leq i, j \leq m - 1 \quad \text{and} \quad i \neq m/3 \text{ or } 2m/3,
\]

where \( \zeta := \exp(2i\pi/m) \) and \( N(\cdot) \) is the norm taken over the field extension \( \mathbb{Q}(\zeta)/\mathbb{Q} \). 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 \( \mathbb{Z}[\zeta] \) \((\cong \mathbb{Z}[X]/\phi_m(X))\) 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 \( \mathbb{Q}(\zeta)/\mathbb{Q} \). If \( t \) is a positive integer with \( |N| < \phi_m(t)/2 \) (where \( \phi_m(X) \) is the \( m \)th cyclotomic polynomial), then \( N \) is the least residue, in absolute value, of

\[
A := \prod_{k=1}^{m} (1 + t^j + t^k) \quad \text{modulo} \quad \phi_m(t).
\]
Note that
\[
(2.4) \quad N(1 + \zeta^i + \zeta^j) = \prod_{\substack{k=1 \\text{mod } m}}^m (1 + \zeta^{ik} + \zeta^{jk}).
\]
As \(|\zeta| = 1\), thus \(|1 + \zeta^{ik} + \zeta^{jk}| \leq 3\), and so \(|N| \leq 3^{\phi(m)}\); therefore, we can take \(t = 4\) in Proposition 1. Actually one can usually take \(t = 2\):

**Proposition 2.** If \(\alpha\) and \(\beta\) are primitive \(a\)th and \(b\)th roots of unity with \(\alpha, \beta\) and \(\alpha \beta \neq 1\), and \(m = [a, b] = \text{lcm}(a, b)\), then
\[
(2.5) \quad |A_{\mathbb{Q}(\zeta)}| = |1 + \alpha + \beta| < \phi_m(2)/2
\]
ext except if \(1 + \alpha + \beta\) is a conjugate or multiple of one of \(1 + \zeta_3 + \zeta_6, 1 + \zeta_4 + \zeta_8, 1 + \zeta_5 + \zeta_{10}, 1 + \zeta_4 + \zeta_6, 1 + \zeta_7 + \zeta_{14}, 1 + \zeta_6 + \zeta_{18}, 1 + \zeta_6 + \zeta_{10}\), 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 \(1 + \lfloor \varphi(m)\log 2/\log 10 \rfloor \leq 29\) digits for \(m \leq 200\)). 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 \(\mathbb{Z}[\zeta]\). However, \(N\) and \(A\) are both integers, by definition. Therefore, as \(t - \zeta\) divides \(N - A\) (in \(\mathbb{Z}[\zeta]\)), 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

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

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 $\frac{1}{12}m(m/\phi(m))\log m$ prime divisors of $W_m$, the largest of which is exponential in $\phi(m)$. 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 $0 \leq i, j \leq m - 1$ 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 $V_m = \lambda^m \prod \mu^{(1-1/p^2)+O(\tau(m))}$, 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

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

$(4.1)$ 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 $n$ (FLTI)$_n$ is said to be true if $\gcd(n, xyz) > 1$ in any integer solution of $(4.1)$. (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 $(m^n - 1)W_m$. 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 $W_m$, (FLTI)$_p$ is true (by using Wieferich’s Theorem [20]—if $p^2$ does not divide $2^p - 2$ then (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
\[
\phi_m(X) = \prod_{d|\gcd(m, X)} (X^d - 1)^{\mu(m/d)},
\]
which may be rewritten as
\[
\left\{ \prod_{n|\gcd(m, X)} (1 - (X^{m/n})^n)^{\mu(n)} \right\}^{\mu(r)},
\]
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 \( \geq 2 \).

We can easily deduce

**Corollary 1.** For any positive integer \( m \) and real number \( x \), with \( m \), \(|x| \geq 2 \),
\[
|\log| \phi_m(x) | - \varphi(m) \log |x| | < \log (|x|/(|x| - 1)).
\]

**Proof of Proposition 3.** We start by noting the inequality
\[
G_n(x) := \prod_{d > n} \left( 1 - \frac{1}{x^d} \right) \geq 1 - \frac{1}{x^n},
\]
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),
\[
\left( \frac{\phi_m(x)}{x^{\varphi(m)}} \right)^{\mu(m)} = \prod_{d|\gcd(m, X)} \left( 1 - \frac{1}{x^d} \right)^{\mu(d)} > \frac{(1 - 1/x)G_p(x)}{1 - 1/x^p} \geq 1 - \frac{1}{x}.
\]
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
\[
\left( \frac{\phi_m(x)}{x^{\varphi(m)}} \right)^{\mu(m)} = \frac{1 - 1/x}{1 - 1/x^p} \rightarrow 1 - \frac{1}{x} \quad \text{as} \quad p \rightarrow \infty.
\]
On the other hand,
\[
\frac{\phi_m(x)/x^{\varphi(m)}\mu(m)}{\Phi(1/x)} = \prod_{d|m} \left(1 - \frac{1}{x^d}\right)^{-\mu(d)} \leq \frac{1 - 1/x^q}{G_q(x)} \leq 1
\]
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),
\[
\frac{\phi_m(x)/x^{\varphi(m)}\mu(m)}{\Phi(1/x)} \geq G_{q-1}(x) \geq 1 - \frac{1}{x^{q-1}} \to 1
\]
as $q \to \infty$ (that is, as $k \to \infty$).

**Proof of Corollary 1.** By taking $n = 1$ in (5.3) we find that $\Phi(1/x) < 1$ for any $x \geq 2$, and so (5.2) holds for $x \geq 2$ 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 $x$, $\phi_m(x) = \phi_m(-x)$ 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
\[
\Phi(X) = X - X + X^2 + X^5 - X^6 + 2X^7 - X^8 + X^9 + X^{11} + X^{13} + 2X^{16} - X^{17} + 2X^{18} + X^{20} + \ldots
\]
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 $\rho(n)$, the number of partitions of $n$, as $\Phi(X)$ is majorized by the power series $\prod_{n \geq 1} (1 - X^n)^{-1}$. 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 $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, and prove Proposition 2. Previous authors have considered improving the (trivial) bound $N \leq 3^{\varphi(m)}$ given in the introduction—the best bound to date is Krasner’s $N \leq 3^{m/4}$ for $m \equiv 2$ or $4 \pmod{6}$, 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 $N \leq 3^{\varphi(m)/2}$ except when $\alpha$, $\beta$, or $\alpha \beta$ is a primitive 6th or 10th root of unity, and a finite number of other exceptional pairs $(\alpha, \beta)$. These bounds may not be improved by too much—by (1.1) we see that a large number of such norms must be $>(\lambda - \epsilon)^{\varphi(m)}$ as $m \to \infty$, and we can easily construct a few norms $>\frac{1}{2} 3^{\varphi(m)/2}$: If $\alpha$ is a primitive 6th root of unity and $\beta$ a primitive $b$th root of unity with $b \equiv 4$ or $8 \pmod{12}$, so that $m = [a, b] = 3b$, then $|N(1+\alpha+\beta)| = \phi_m/3$, 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,
Our starting point is a result of Dénes [4, equation (10)].

**Proposition 4.** Suppose \( \alpha, \beta, \text{ and } \gamma = \alpha \beta \) are given primitive \( a, b, \) and \( c \)th roots of unity, respectively. Let \( m = [a, b] \). Then

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

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

\[
\left| 2 + \alpha \right|^2 \left| 2 + \beta \right|^2 \left| 2 + \gamma \right|^2 = \left| 1 - \alpha \right|^2 \left| 1 - \beta \right|^2 \left| 1 - \gamma \right|^2 + 9\left| 1 + \alpha + \beta \right|^4.
\]

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

We now exclude the first term of the right-hand side of (6.2) and take the norm (in \( \mathbb{Q}(\zeta_m) / \mathbb{Q} \)) 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 \( \alpha, \beta, \gamma, a, b, c, \) and \( m \) be as in Proposition 4. For any fixed \( \epsilon > 0 \), if \( 1/\varphi(a) + 1/\varphi(b) + 1/\varphi(c) < \log(1 + \epsilon)/\log 2 \), then

\[
\left| N(1 + \alpha + \beta) \right| \leq \left( \frac{8(1 + \epsilon)}{3} \right)^{\varphi(m)/2}.
\]

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

Taking \( \epsilon = \frac{1}{8} \) in Corollary 2 gives \( |N| \leq 3^{\varphi(m)/2} \) except if at least one of \( a, b, \) and \( c \) is small. Now, rearrange \( \alpha, \beta, \) and \( \gamma \) so that \( \varphi(a) \leq \varphi(b) \leq \varphi(c) \).

Then, if \( |N| > 3^{\varphi(m)/2} \), we see that

\[
\frac{2}{\varphi(b)} \geq \frac{1}{\varphi(b)} + \frac{1}{\varphi(c)} \geq \frac{\log(9/8)}{\log 2} - \frac{1}{\varphi(a)},
\]

which can occur in only finitely many cases (as \( c \) is determined by \( a \) and \( b \)) unless the right-hand side is \( \leq 0 \). But then \( \varphi(a) \leq 2 \log 2 / \log 9 < 6 \), 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 \( \epsilon > 0 \), we have \( |N| \leq ((\sqrt{5} + 1)/2 + \epsilon)^{\varphi(m)} \) 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 \(\gamma = \alpha \beta\) be a primitive \(c\)th root of unity, and reorder \(\alpha, \beta,\) and \(\gamma\) (taking their conjugates if necessary) so that
\[
|\phi_a(-2)|^{1/\varphi(a)} \geq |\phi_b(-2)|^{1/\varphi(b)} \geq |\phi_c(-2)|^{1/\varphi(c)}.
\]
(Note that \(N(1 + \alpha + \beta) = N(1 + \overline{\alpha} + \overline{\beta}) = N(1 + \overline{\beta} + \gamma)\). Then, by Corollary 1, Proposition 4, and (6.3), we have
\[
(2^{\varphi(m)/2}/\varphi(m))^{2/\varphi(m)} \leq (\phi_m(2)/2)^{2/\varphi(m)}
\]
\[
\leq \frac{1}{\varphi(a)} |\phi_a(-2)|^{1/\varphi(a)} |\phi_b(-2)|^{1/\varphi(b)} |\phi_c(-2)|^{1/\varphi(c)}
\]
\[
\leq \frac{1}{\varphi(a)} |\phi_a(-2)|^{1/\varphi(a)} |\phi_b(-2)|^{2/\varphi(b)}
\]
\[
\leq \frac{1}{\varphi(a)} |\phi_a(-2)|^{3/\varphi(a)} \leq \frac{1}{\varphi(a)} (2^{\varphi(b)/1-2/\varphi(b)})
\]
\[
(6.4)
\]
\[
\leq \frac{1}{\varphi(a)} (2^{\varphi(b)/1-2/\varphi(b)})
\]
\[
(6.5)
\]
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),
\[
\frac{3}{2} \leq 2^{3/\varphi(a)+4/\varphi(m)} \leq 2^{7/\varphi(a)},
\]
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),
\[
3/\varphi(a) \leq 2^{4/\varphi(m)+2/\varphi(b)} \leq 2^{6/\varphi(b)},
\]
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**


Department of Computer Science, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada

E-mail address: gife@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