MATHEMATICS OF COMPUTATION
Volume 71, Number 237, Pages 415–427
S 0025-5718(00)01292-8
Article electronically published on October 18, 2000

UPPER BOUNDS FOR THE PRIME DIVISORS OF WENDT'S DETERMINANT

ANASTASIOS SIMALARIDES

Abstract. Let $c \geq 2$ be an even integer, $(3,c)=1$. The resultant W_c of the polynomials t^c-1 and $(1+t)^c-1$ is known as Wendt's determinant of order c. We prove that among the prime divisors q of W_c only those which divide 2^c-1 or $L_{c/2}$ can be larger than $\theta^{c/4}$, where $\theta = 2.2487338$ and L_n is the nth Lucas number, except when $c=20$ and $q=61$. Using this estimate we derive criteria for the nonsolvability of Fermat's congruence.

1. Introduction

Let $c \geq 2$ be an even integer. Given two polynomials $f(t)$ and $g(t)$ denote by $R(f(t), g(t))$ their resultant. The integer

$$W_c = R(t^c - 1, (1+t)^c - 1)$$

is known as Wendt's determinant. The prime divisors of W_c are of importance because of the following result of Wendt [16].

Theorem 1. *Let p, q be odd primes such that $q = 1 + cp$, $(3,c)=1$. Then, Fermat's congruence*

$$x^p + y^p + z^p \equiv 0 \pmod{q} \tag{1}$$

has a nontrivial solution (that is, a solution (x,y,z) such that $xyz \not\equiv 0 \pmod{q}$) if and only if q divides W_c.

Although Fermat's Problem has been solved completely, some questions concerning congruence (1) (or, equivalently, the number W_c) remain still unanswered (cf. Section 5).

Since $W_c = 0$ if and only if $(3,c) > 1$, we shall assume through the paper that $(3,c)=1$. The quantity $|W_c|$ grows rapidly with c; Boyd [1] proved that

$$10^{-1/3}\lambda^{c^2} < |W_c| < 10^{1/3}\lambda^{c^2},$$

where $\log\lambda = \frac{2}{\pi}\int_0^{\pi/3}\log(2\cos\theta)d\theta = 0.323\ldots$. In the Table 1 below we list the first few values of $|W_c|$. Several authors carried out the complete factorization of W_c for $c \leq c_0$: Frame [8] for $c_0 = 50$; Fee and Granville [6] for $c_0 = 200$; Ford and Jha [7] for $c_0 = 500$.

Received by the editor April 13, 1999 and, in revised form, February 24, 2000.
2000 *Mathematics Subject Classification.* Primary 11C20; Secondary 11Y40, 11D79.
Key words and phrases. Wendt's determinant, Fermat's congruence.

TABLE 1. The values of $|W_c|$ for $c \leq 20$

c	$\|W_c\|$	c	$\|W_c\|$
2	3	14	$2^{24} \cdot 3 \cdot 29^6 \cdot 43^3 \cdot 127^3$
4	$3 \cdot 5^3$	16	$3^7 \cdot 5^3 \cdot 7^6 \cdot 17^{15} \cdot 257^3$
8	$3^7 \cdot 5^3 \cdot 17^3$	20	$3 \cdot 5^{24} \cdot 11^9 \cdot 31^3 \cdot 41^9 \cdot 61^6$
10	$3 \cdot 11^9 \cdot 31^3$		

By the well-known factorizations (cf. [8])

$$\begin{aligned} W_c &= \prod_{a=1}^{c}\prod_{b=1}^{c}(1+\zeta^a+\zeta^b) \\ &= \prod_{a=1}^{c}\prod_{b=1}^{c}(1-\zeta^a-\zeta^b), \quad \zeta = e^{2\pi i/c}, \end{aligned} \tag{2}$$

of W_c, it follows immediately that the integer $2^c - 1$ divides W_c. It follows also in an analogous way (cf. Section 2) that $L_{c/2}$ divides W_c (L_n is the nth Lucas number), in case $c \equiv 2 \pmod 4$.

Such nice factors of W_c are called *principal factors*. Further information on the principal factors of W_c can be found in E. Lehmer [11], Frame [8] and Ribenboim [12]; for a recent result see Helou [9]. The factorization of the principal factors

$$2^c - 1, \quad L_{c/2}, \tag{3}$$

is of special importance, because the greatest prime divisor of W_c divides often one of the numbers (3). The extensive tables by Brillhart et al. [2], contain all the known factorizations of the numbers $2^c - 1$ for $c \leq 2400$; other tables by Brillhart et al. [3] contain all the known factorizations of the Lucas numbers L_n for $n \leq 500$. Unfortunately, no complete factorization of W_c is known that involves only simple principal factors.

Upper bounds for the prime divisors of W_c are obtained in the following way. Let q be a prime divisor of W_c, which does not divide c. It follows by (2) that a prime ideal divisor of q in $\mathcal{Q}(\zeta)$ divides a trinomial cyclotomic integer $1+\zeta^a+\zeta^b$. In consequence, q divides both the norm

$$N = N(a,b) = N_{\mathcal{Q}(\zeta)/\mathcal{Q}}(1+\zeta^a+\zeta^b)$$

of $1+\zeta^a+\zeta^b$ and the resultant

$$R = R(a,b) = R(1+t^a+t^b, t^{c/2}+1)$$

of the polynomials $1+t^a+t^b$ and $t^{c/2}+1$; in consequence, it suffices to estimate one of the numbers $|N|$ and $|R|$. Bounds which arise from the estimation of $|N|$ have their origin in Vandiver [15], who first noticed and used the simplest possible estimate $|N| \leq 3^{\phi(c)}$ of this type (ϕ is Euler's function). Improved bounds of this type were proved and used by Denes [5], Simalarides [13], and, Fee and Granville [6]. Bounds that arise from the estimation of $|R|$ have their origin in Krasner [10], who proved that $q \leq 3^{c/4}$ for every prime divisor q of W_c such that $2^c \not\equiv 1 \pmod q$ and $q = 1 + cp$, where p is a prime. The author [14] improved upon Krasner's result by proving that $q \leq 3 + (2.618\ldots)^{c/4}$, under the same conditions. In the same paper, it was also proved that $q \leq 2.459^{c/4}$ under the additional condition that q does not divide the numbers $1+(-1)^{c/2} \pm L_{c/2}$. The results in [10] and [14] were not formulated explicitly as results concerning the resultant W_c, but rather, as results concerning the first case of Fermat's Last Theorem.

We generalize and improve all these previous results as follows.

Theorem 2. *Let $c \geq 2$ be an even integer such that $(3,c)=1$. If a prime divisor q of W_c satisfies the inequality*

$$q > \theta^{c/4}, \quad \text{where} \quad \theta = 2.2487338, \tag{4}$$

then at least one of the following is true: (i) $c=20$ *and* $q=61$*;* (ii) q *is a divisor of* 2^c-1*;* (iii) $c \equiv 2 \pmod 4$ *and q is a divisor of* $L_{c/2}$.

The proof of Theorem 2 will be given in Section 3.

In case $c \equiv 0 \pmod 4$ the number 2^c-1 admits the obvious factorization

$$2^c-1=(2^{c/4}-1)(2^{c/4}+1)(2^{c/2}+1),$$

while in case $c \not\equiv 0 \pmod 8$, it can be factored further (Aurifeuillian factorization) as follows:

$$2^c-1=(2^{c/4}-1)(2^{c/4}+1)(2^{c/4}-2^{(c+4)/8}+1)(2^{c/4}+2^{(c+4)/8}+1).$$

In view of these factorizations, Theorem 2 can be written in the following sharper form.

Theorem 3. *Let $c \geq 2$ be an even integer such that $(3,c)=1$. Then, among the prime divisors q of W_c, only those which divide either*

$$2^c-1 \quad \text{or} \quad L_{c/2}, \quad \text{in case} \quad c \equiv 2 \pmod 4,$$

or

$$2^{c/2}+1, \quad \text{in case} \quad c \equiv 0 \pmod 8,$$

can be larger than $\theta^{c/4}$, where $\theta = 2.2487338$, except when

$$(c,q) \in \{(4,3),(4,5),(20,61)\}.$$

2. Preliminaries concerning Fibonacci and Lucas numbers

The formulae

$$L_{2n}=L_n^2-2(-1)^n, \quad 4+L_{2n-1}^2=5F_{2n-1}^2, \quad n \geq 1, \tag{5}$$

are immediate consequences of the standard expresssions

$$L_n=\omega_1^n+\omega_2^n, \qquad F_n=\frac{\omega_2^n-\omega_1^n}{\omega_2-\omega_1}, \quad n \geq 1$$

for the nth Lucas and Fibonacci numbers, respectively, where $\omega_1=(1-\sqrt{5})/2$, $\omega_2=(1+\sqrt{5})/2$, are the roots of the polynomial t^2-t-1. Define

$$u_c=R(t^2+t-1,\ t^c-1).$$

The following lemma shows that u_c is a principal factor of W_c.

Lemma 1. *Let $c \geq 2$ be an even integer such that $(3, c) = 1$. Then the following hold true:*
(i) *The integer u_c is a divisor of W_c.*
(ii) *We have*

$$\begin{aligned} u_c &= 2 - L_c = 2 + 2(-1)^{c/2} - L_{c/2}^2 \\ &= \begin{cases} \left(2 - L_{\frac{c}{4}}\right)\left(2 + L_{\frac{c}{4}}\right) L_{\frac{c}{4}}^2 & \textit{if } c \equiv 0 \pmod 8, \\ -5F_{\frac{c}{4}}^2 L_{\frac{c}{4}}^2 & \textit{if } c \equiv 4 \pmod 8, \\ -L_{\frac{c}{2}}^2 & \textit{if } c \equiv \pm 2 \pmod 8). \end{cases} \end{aligned}$$

(iii) *If a prime divisor $q \neq 5$ of u_c is larger than $\theta^{c/4}$, then $c \equiv 2 \pmod 4$ and q is a divisor of $L_{c/2}$.*

Proof. (i) Immediate in view of (2) and the fact that

$$u_c = \prod_{a=1}^{c} (\zeta^{2a} + \zeta^a - 1).$$

(ii) We have

$$\begin{aligned} u_c = (\omega_1^c - 1)(\omega_2^c - 1) &= (\omega_1\omega_2)^c - (\omega_1^c + \omega_2^c) + 1 \\ &= 2 - L_c. \end{aligned}$$

Applying formulae (5) we obtain the rest of the result sought.
(iii) Immediate in view of (ii) and of the obvious bounds

$$L_n \leq 1 + \omega_2^n = 1 + (1.618\ldots)^n, \qquad F_n \leq \frac{\omega_2^n + 1}{\sqrt{5}} = \frac{(1.618\ldots)^n + 1}{\sqrt{5}},$$

where $n \geq 1$.

3. Proof of Theorem 2

First of all, Theorem 2 is true for $c \leq 20$, so we can assume that $c \geq 22$. Assume that there is a prime divisor q of W_c which satisfies the inequality (4). Assume also that q is neither a divisor of $2^c - 1$, nor a divisor of $L_{c/2}$ in case $c \equiv 2 \pmod 4$. We shall prove that this assumption leads to a contradiction. Hypothesis (4) implies that $q > c$, so q does not divide c; it follows that

$$1 + \zeta^a + \zeta^b \equiv 0 \pmod{\mathbf{q}}, \tag{6}$$

where $\mathbf{q}$ is a prime ideal divisor of q in $\mathcal{Q}(\zeta)$, and a, b are two integers such that

$$a \not\equiv 0, \quad b \not\equiv 0, \quad a \not\equiv b \pmod c$$

(the last three relations are immediate consequences of the hypothesis $2^c \not\equiv 1 \pmod q$).

Since $\zeta^{c/2} + 1 = 0$, the resultant $R(a, b)$ of the polynomials $1 + t^a + t^b$, $t^{c/2} + 1$ satisfies the congruence

$$R(a, b) \equiv 0 \pmod q. \tag{7}$$

We can assume that $q \equiv 1 \pmod c$; otherwise would have $R(a, b) \equiv 0 \pmod{q^2}$, and in consequence $q < 3^{c/8}$, which would contradict hypothesis (4).

The integer $R(a,b)$ admits the following representation:

$$\begin{aligned} R(a,b) &= \prod_{i=1}^{c/2}\left[1+\zeta^{(2i-1)a}+\zeta^{(2i-1)b}\right] \\ &= \prod_{i=1}^{c_1}\left[3+2\cos\frac{2\pi a}{c}(2i-1)\right. \\ &\qquad \left. +2\cos\frac{2\pi b}{c}(2i-1)+2\cos\frac{2\pi(a-b)}{c}(2i-1)\right] d, \end{aligned}$$

where

$$c_1 = \begin{cases} \frac{c}{4} & \text{if } c \equiv 0 \pmod 4, \\ \frac{c}{4}-\frac{1}{2} & \text{if } c \not\equiv 0 \pmod 4, \end{cases}$$

and

$$d = \begin{cases} 1 & \text{if } c \equiv 0 \pmod 4, \\ 1+(-1)^a+(-1)^b & \text{if } c \not\equiv 0 \pmod 4. \end{cases}$$

We have $R(a,b) \neq 0$ because of the relation $(3,c)=1$. Introducing the abbreviation

$$A_i = \cos\frac{2\pi a}{c}(2i-1)+\cos\frac{2\pi b}{c}(2i-1)+\cos\frac{2\pi(a-b)}{c}(2i-1),$$

we obtain

$$\log|R(a,b)| = \sum_{i=1}^{c_1}\log(3+2A_i)+\log|d|,$$

where evidently $-1.5 < A_i \leq 3$. We have

$$\log(3+2z) < \sum_{j=0}^{4}\alpha_j z^j, \quad \text{for } -1.5 < z \leq 3,$$

where $\alpha_0 = 1.166985006, \alpha_1 = 0.76146, \alpha_2 = -0.295509605, \alpha_3 = 0.0523446$, $\alpha_4 = 0.0014453$. This implies that

$$\log|R(a,b)| < \sum_{i=1}^{c_1}\sum_{j=0}^{4}\alpha_j A_i^j+\log|d| = \sum_{j=0}^{4}\alpha_j\sum_{i=1}^{c_1}A_i^j+\log|d|. \tag{8}$$

Given two variables x,y, consider the function

$$[\cos x+\cos y+\cos(x-y)]^n, \quad n \geq 0,$$

and its Fourier expansion

$$[\cos x+\cos y+\cos(x-y)]^n = \sum_{r=0}^{\infty}\sum_{s=-\infty}^{\infty}c_{r,s}^{(n)}\cos(rx+sy);$$

the set

$$\mathcal{A}_n = \left\{(r,s)\in\mathbb{Z}\times\mathbb{Z}; c_{r,s}^{(n)} \neq 0\right\}$$

is finite. We have trivially $\mathcal{A}_0 = \{(0,0)\}$ and $c_{0,0}^{(0)} = 1$. It is easily seen that

$$\mathcal{A}_n \subset \mathcal{A}_{n+1}, \quad \text{for } n = 1,2,3,\dots.$$

We can write

$$[\cos x + \cos y + \cos (x-y)]^n = \sum_{(r,s)\in\mathcal{A}_n} c_{r,s}^{(n)} \cos (rx+sy),$$

or more simply

$$[\cos x + \cos y + \cos (x-y)]^n = \sum_{r,s} c_{r,s}^{(n)} \cos (rx+sy).$$

Estimate (8) then takes the form

$$\log|R(a,b)| < \sum_{j=0}^{4} \alpha_j \sum_{r,s} c_{r,s}^{(j)} \sum_{i=1}^{c_1} \cos \frac{2\pi(ra+sb)}{c}(2i-1) + \log|d|. \tag{9}$$

We also have

(10)

$$\sum_{i=1}^{c_1} \cos \frac{2\pi(ra+sb)}{c}(2i-1) = \begin{cases} c_1(-1)^{2(ra+sb)/c} & \text{if } ra+sb \equiv 0 \pmod{\frac{c}{2}}; \\ 0 & \text{if } ra+sb \not\equiv 0 \pmod{\frac{c}{2}} \\ & \text{and } c \equiv 0 \pmod 4; \\ -\frac{1}{2}\cos (ra+sb)\pi & \text{if } ra+sb \not\equiv 0 \pmod{\frac{c}{2}} \\ & \text{and } c \not\equiv 0 \pmod 4. \end{cases}$$

The next lemma guarantees that $ra+sb \not\equiv 0 \pmod{\frac{c}{2}}$ for all $(r,s)\in\mathcal{A}_4$ with at most two exceptions. We denote by (a,b) any solution of the congruence

$$1+\zeta^A+\zeta^B \equiv 0 \pmod{\mathbf{q}},\ A\not\equiv 0,\ B\not\equiv 0,\ A\not\equiv B \pmod c; \tag{11}$$

the numbers a,b are determined mod$c$. Relation (6) says that the set of the solutions to (11) is nonempty by hypothesis.

Lemma 2. *Let $\mathcal{A} = \{(2,-4),(4,-2),(2,2)\}$. Then the following hold true:*
(I) *The pairs $(b,a),(-a,b-a)$ are also solutions of (11).*
(II) *The congruence*

$$ra+sb \equiv 0 \pmod{\frac{c}{2}} \tag{12}$$

is impossible for $(r,s)\in\mathcal{A}_4-\mathcal{A}-\{(0,0)\}$.
(III) *If $c\not\equiv 0 \pmod 4$, then congruence (12) is impossible for $(r,s)\in\mathcal{A}_4-\{(0,0)\}$, while if $c\equiv 0 \pmod 4$, then congruence (12) can be satisfied by at most one $(r,s)\in\mathcal{A}$ and in this case $2(ra+sb)/c$ is odd.*

Proof. The first assertion of the lemma is obvious.

(II) We have $\mathcal{A}_1 = \{(1,-1),(1,0),(0,1)\}$ and

$$\begin{aligned} \mathcal{A}_2 &= \mathcal{A}_1 \cup \{(0,0),(1,-2),(2,-2),(2,-1),(2,0),(1,1),(0,2)\}, \\ \mathcal{A}_3 &= \mathcal{A}_2 \cup \{(1,-3),(2,-3),(3,-3),(3,-2),(3,-1),(3,0),(2,1),(1,2),(0,3)\}, \\ \mathcal{A}_4 &= \mathcal{A}_3 \cup \{(1,-4),(2,-4),(3,-4),(4,-4),(4,-3), \\ &\qquad (4,-2),(4,-1),(4,0),(3,1),(2,2),(1,3),(0,4)\}. \end{aligned}$$

Obviously, the set $\mathcal{A}_4-\mathcal{A}-\{(0,0)\}$ consists of 27 elements.

Consider the transformations τ_0,τ_1,τ_2 defined by

$$\tau_0(a,b)=(a,b),\quad \tau_1(a,b)=(b,a),\quad \tau_2(a,b)=(-a,b-a).$$

All these transformations are of the form

$$\tau_i(a,b) = \left(a_{11}^{(i)}a + a_{12}^{(i)}b, a_{21}^{(i)}a + a_{22}^{(i)}b\right), \quad i = 0,1,2, \tag{13}$$

or in matrix notation

$$\tau_i(a,b)^T = \begin{pmatrix} a_{11}^{(i)} & a_{12}^{(i)} \\ a_{21}^{(i)} & a_{22}^{(i)} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}, \quad a_{kl} \in \mathbb{Z}.$$

The image $\tau_i(a,b)$ is also a solution of (11) for $i = 0,1,2$ because of the part (I) of the lemma. For this reason, if

$$r_1 a + s_1 a \not\equiv 0 \pmod{\frac{c}{2}}, \tag{14}$$

for some $(r_1, s_1) \in \mathcal{A}_4 - \mathcal{A} - \{(0,0)\}$ and for every solution (a,b) of (11), then also

$$r_1\left(a_{11}^{(i)}a + a_{12}^{(i)}b\right) + s_1\left(a_{21}^{(i)}a + a_{22}^{(i)}b\right) \not\equiv 0 \pmod{\frac{c}{2}} \tag{15}$$

for every $i = 0,1,2,3$. Since the left member of (15) is equal to

$$\left(r_1 a_{11}^{(i)} + s_1 a_{21}^{(i)}\right)a + \left(r_1 a_{12}^{(i)} + s_1 a_{22}^{(i)}\right)b,$$

it follows that if (14) is true for some $(r_1, s_1) \in \mathcal{A}_4 - \mathcal{A} - \{(0,0\}$ and for every solution (a,b), then the relation $ra + sb \not\equiv 0 \pmod{c/2}$ is also true for the pair (r,s), where

$$\begin{pmatrix} r \\ s \end{pmatrix} = \begin{pmatrix} a_{11}^{(i)} & a_{21}^{(i)} \\ a_{12}^{(i)} & a_{22}^{(i)} \end{pmatrix} \begin{pmatrix} r_1 \\ s_1 \end{pmatrix}, \quad i = 0,1,2. \tag{16}$$

A subset $\mathcal{B}$ of $\mathcal{A}_4 - \mathcal{A} - \{(0,0)\}$ is called *fundamental*, if, for every pair $(r,s) \in \mathcal{A}_4 - \mathcal{A} - \{(0,0)\}$, the equality

$$\begin{pmatrix} r \\ s \end{pmatrix} = \pm T \begin{pmatrix} r_1 \\ s_1 \end{pmatrix}$$

holds true for some $(r_1, s_1) \in \mathcal{B}$ and for some transformation T composed of the transformations (16).

The final conclusion of the above discussion is the following: To prove part (II) of Lemma 2, it suffices to prove that the congruence (12) is impossible for all $(r,s) \in \mathcal{B}$, where $\mathcal{B}$ is a fundamental subset of $\mathcal{A}_4 - \mathcal{A} - \{(0,0)\}$. A simple calculation shows that a fundamental subset of $\mathcal{A}_4 - \mathcal{A} - \{(0,0)\}$ is the following

$$\mathcal{B} = \{(1,0),(2,0),(3,0),(4,0),(1,1),(1,-3),(1,-4)\}.$$

We distinguish two cases (A), (B).

(A) $(r,s) \in \{(1,0),(2,0),(3,0),(4,0)\}$; we have to prove that

$$a \not\equiv 0, 2a \not\equiv 0, 2^2 a \not\equiv 0, 3a \not\equiv 0 \pmod{\frac{c}{2}}.$$

We prove the first three relations by induction on the exponents of the powers $1, 2, 2^2$. The first relation is true by hypothesis. Assuming that $2^j a \not\equiv 0 \pmod{c/2}$, let us prove that $2^{j+1}a \not\equiv 0 \pmod{c/2}$. Indeed, the contrary hypothesis $2^{j+1}a \equiv 0 \pmod{c/2}$ implies that $2^{j+1}a = k(c/2)$, where k is an integer. The number k is odd, because if k were even, then this fact would vitiate the induction hypothesis;

in consequence, c is divisible by 4 and so $a = k(c/2^{j+2})$. Then $\zeta^a = \xi$, where ξ is a primitive 2^{j+2}-th root of unity, and congruence (6) becomes

$$1 + \xi \equiv -\zeta^b \pmod{\mathbf{q}}. \tag{17}$$

Congruence (17) implies then $(1+\xi)^c \equiv 1 \pmod{\mathbf{q}}$ and taking norms we conclude that $2^c \equiv 1 \pmod{q}$, which is impossible by hypothesis.

It remains to prove that $3a \not\equiv 0 \pmod{c/2}$; indeed, if were $3a \equiv 0 \pmod{c/2}$ this would imply (since $(3, c) = 1$) that $a \equiv 0 \pmod{c/2}$, which is impossible by hypothesis.

(B) $(r, s) \in \{(1, 1), (1, -3), (1, -4)\}$; assume that the congruence (12) holds true for such a pair (r, s). We shall prove that this leads to a contradiction. We have by hypothesis

$$\zeta^{ra} \equiv \pm\zeta^{-sb} \pmod{\mathbf{q}}, \quad 1 + \zeta^a + \zeta^b \equiv 0 \pmod{\mathbf{q}}. \tag{18}$$

It follows that at least one of the polynomials

$$f^{\pm}_{r,s}(t) = \begin{cases} (1+t)^r \pm t^{-s} & \text{if } s < 0, \\ \\ t^s(1+t)^r \pm 1 & \text{if } s > 0, \end{cases} \tag{19}$$

has a common root $\bmod q$ with the polynomial $t^c - 1 = (t^{c/2} - 1)(t^{c/2} + 1)$. This implies that at least one of the congruences

$$R\left(f^{\pm}_{r,s}(t), t^{c/2} + (-1)^n\right) \equiv 0 \pmod{q} \tag{20}$$

holds true for every $n \in \{1, 2\}$. If $d^{\pm}_{r,s}$ are the degrees of the polynomials (19) and $\rho^{\pm}_1, \rho^{\pm}_2, \ldots,$ their roots, then

$$R\left(f^{\pm}_{r,s}(t), t^{c/2} + (-1)^n\right) = \prod_{i=1}^{d^{\pm}_{r,s}} \left[\rho_i^{c/2} + (-1)^n\right].$$

We have to distinguish between two cases (a) and (b):
(a) $(r, s) = (1, 1)$; we have

$$f^{\pm}_{1,1}(t) = t^2 + t \pm 1,$$

$$0 < \left|R\left(t^2 + t + 1, t^{c/2} + (-1)^n\right)\right| \leq 4, \tag{21}$$

$$\begin{aligned} R\left(t^2 + t - 1, t^{c/2} + (-1)^n\right) &= \left[(-\omega_1)^{\frac{c}{2}} + (-1)^n\right] \cdot \left[(-\omega_2)^{\frac{c}{2}} + (-1)^n\right] \\ &= 1 + (-1)^{c/2} + (-1)^{n+\frac{c}{2}} L_{c/2} \neq 0. \end{aligned} \tag{22}$$

Relation (21) contradicts hypothesis (4). Each of the numbers (22) divides by part (ii) of Lemma 1 the number u_c for $n = 1, 2$. Congruence (20) leads then, in view of part (iii) of Lemma 1, to a contradiction.
(b) $(r, s) \in \{(1, -3), (1, -4)\}$; we have

$$f_{1,-3}(t) = \pm t^3 + t + 1 \quad \text{and} \quad f_{1,-4}(t) = \pm t^4 + t + 1.$$

For $c \geq 22$, a simple calculation shows that

$$0 < \left|R\left(f^{\pm}_{r,s}(t), t^{c/2} + (-1)^n\right)\right| < \theta^{c/4}$$

for $(r, s) \in \{(1, -3), (1, -4)\}$, which contradicts, in view of (20), hypothesis (4).

(III) If two of the congruences

$$2a-4b\equiv 0,\ 4a-2b\equiv 0,\ 2a+2b\equiv 0 \pmod{\frac{c}{2}}, \tag{23}$$

were true, then for these two congruences, say for the first and for the second, we would have

$$\begin{aligned} 0 \quad \equiv \quad & (2a-4b)+(4a-2b)\equiv 6a-6b \pmod{\frac{c}{2}} \Rightarrow 6a-6b=k\frac{c}{2} \\ & \Rightarrow 2a-2b=k_1\frac{c}{2} \quad (\text{because } c\not\equiv 0 \pmod 3) \\ & \Rightarrow 2a-2b\equiv 0 \pmod{\frac{c}{2}}, \end{aligned}$$

which is absurd, since $(2,-2)\in\mathcal{A}_4-\mathcal{A}-\{(0,0)\}$. If one of the congruences (23) is true, this means that

$$2a-4b\equiv 0 \ \text{ or } \ 4a-2b\equiv 0 \ \text{ or } \ 2a+2b\equiv 0 \pmod{\frac{c}{2}},$$

or equivalently

$$2a-4b=k_1\frac{c}{2} \ \text{ or } \ 4a-2b=k_2\frac{c}{2} \ \text{ or } \ 2a+2b=k_3\frac{c}{2}. \tag{24}$$

The integers k_1,k_2,k_3 cannot be even; otherwise this would imply that

$$a-2b\equiv 0 \ \text{ or } \ 2a-b\equiv 0 \ \text{ or } \ a+b\equiv 0 \pmod{\frac{c}{2}},$$

which is absurd, because $(1,-2),(2,-1),(1,1)\in\mathcal{A}_4-\mathcal{A}-\{(0,0)\}$. In case $c\not\equiv 0 \pmod 4$ the equalities (24) are all impossible because the right members are odd numbers.

We then turn to the proof of theorem. We distinguish two cases (A) and (B).
(A) $c\equiv 0 \pmod 4$; then $c_1=\frac{c}{4}$ and $d=1$. In case the congruence $ra+sb\equiv 0 \pmod{\frac{c}{2}}$ holds true for one (and only one) $(r,s)\in\mathcal{A}$, it follows by Lemma 2 and relations (9), (10) that

$$\log|R(a,b)|<\left[\alpha_0c_{0,0}^{(0)}+\alpha_1c_{0,0}^{(1)}+\alpha_2c_{0,0}^{(2)}+\alpha_3c_{0,0}^{(3)}+\alpha_4(c_{0,0}^{(4)}-c_{r,s}^{(4)})\right]\frac{c}{4}.$$

Since

$$c_{0,0}^{(0)}=1, c_{0,0}^{(1)}=0, c_{0,0}^{(2)}=\frac{3}{2}, c_{0,0}^{(3)}=\frac{3}{2}, c_{0,0}^{(4)}=\frac{45}{8},$$

and

$$c_{r,s}^{(4)}=\frac{3}{4} \ \text{ for } \ (r,s)\in\mathcal{A},$$

we obtain the estimate

$$\log|R(a,b)|<(0.809283336\ldots)\frac{c}{4}<\frac{c}{4}\log\theta. \tag{25}$$

In case the congruence $ra+sb\equiv 0 \pmod{\frac{c}{2}}$ is impossible for all $(r,s)\in\mathcal{A}$, Lemma 2, together with the relations (9), (10), imply the estimate

$$\log|R(a,b)|<\left[\sum_{j=0}^{4}\alpha_jc_{0,0}^{(j)}\right]\frac{c}{4}=\frac{c}{4}\log\theta. \tag{26}$$

Both estimates (25) and (26) contradict, by (7), hypothesis (4).

(B) $c \not\equiv 0 \pmod 4$; then $c_1 = \frac{c}{4} - \frac{1}{2}$, $d = 1 + (-1)^a + (-1)^b$, and it follows by Lemma 2 and relations (9), (10) that

$$\begin{aligned}
\log|R(a,b)| &< \sum_{j=0}^{4} \alpha_j \left[\frac{c_1}{4} c_{0,0}^{(j)} - \frac{1}{2} \sum_{\substack{r,s \\ (r,s)\neq(0,0)}} c_{r,s}^{(j)} \cos(ra+sb)\pi \right] + \log|d| \\
&= \sum_{j=0}^{4} \alpha_j \left[\frac{c}{4} c_{0,0}^{(j)} - \frac{1}{2} \sum_{r,s} c_{r,s}^{(j)} \cos(ra+sb)\pi \right] + \log|d| \\
&= \left[\sum_{j=0}^{4} \alpha_j c_{0,0}^{(j)} \right] \frac{c}{4} - \frac{1}{2} \sum_{j=0}^{4} \alpha_j \left[(-1)^a + (-1)^b + (-1)^{a-b} \right]^j + \log|d|.
\end{aligned}$$

Hence

$$\log|R(a,b)| < \begin{cases} \dfrac{c}{4} \log\theta + \log|d| - 0.01889 & \text{if } a, b \text{ are both even,} \\[2ex] \dfrac{c}{4} \log\theta - 0.4103 & \text{otherwise,} \end{cases}$$

which by (7) contradicts hypothesis (4), since q cannot divide the integer d.

4. The large prime divisors of W_c

Let $c \geq 2$ be an integer such that $(3,c) = 1$. A prime divisor q of W_c is called *large* if $q > \theta^{c/4}$. Denote by $\mathcal{P}_c$ the set of large prime divisors of W_c; denote also by P_c, Q_c, U_c (or, for simplicity, by P, Q, U) the largest prime divisor of the numbers $2^{c/2} - 1$, $2^{c/2} + 1$, $L_{c/2}$, respectively. The set $\mathcal{P}_c$ is empty in case $c \equiv 4 \pmod 8$, except when $c = 20$. We can easily determine the set $\mathcal{P}_c$ using Theorem 3 in combination with the tables in [2] and [3]. Thus, in Table 2 below we list the large prime divisors of W_c for all $c \leq 662$, such that $c \not\equiv 0 \pmod 3$ and $c \not\equiv 4 \pmod 8$ (the case $c = 20$ is also included). We did not try to extend Table 2 beyond the value $c = 662$, because for $c > 662$, in the tables in [2] and [3] appear incomplete factorizations of the numbers (3), involving composite factors whose prime factors are unknown. We found that all the numbers in Table 2 are congruent to $1 \pmod c$. We also found that for $c \leq 662$, and $q \in \mathcal{P}_c$, the number $(q-1)/c$ is always composite except when

$$(c,q) \in \{(10,31),\ (20,61),\ (22,683)\}.$$

The verification of the last assertion has been carried out without much difficulty because in almost all cases, the numbers $(q-1)/c$ were found to have a small prime divisor. The only difficulties arose from the numbers $P_{482}, Q_{362}, Q_{454}$. Indeed we found that the least prime divisor of the numbers $(P_{482}-1)/482$ and $(Q_{362}-1)/362$ is 21221 and 412987, respectively, while the converse of Fermat's Theorem with base 2 showed that the number

$$(Q_{454} - 1)/454 = 15\ 4145\ 7503\ 4860\ 2301\ 1302\ 1485\ 7398\ 0441\ 2137\ 3127$$

is composite (with unknown factors).

TABLE 2. The large prime divisors of W_c for $c \le 662$

c	$\mathcal{P}_c$	c	$\mathcal{P}_c$	c	$\mathcal{P}_c$	c	$\mathcal{P}_c$
2	Q U	166	P	334	P Q	502	Q
8	Q	170	P Q	338	P	506	$\varnothing$
10	P Q U	176	$\varnothing$	344	$\varnothing$	512	Q
14	P Q U	178	P Q U	346	$\varnothing$	514	$\varnothing$
16	Q	182	$\varnothing$	350	$\varnothing$	518	P
20	61	184	Q	352	Q	520	$\varnothing$
22	P Q U	190	Q	358	P Q	526	Q
26	P Q U	194	P Q	362	P Q	530	$\varnothing$
32	Q	200	$\varnothing$	368	$\varnothing$	536	Q
34	P Q U	202	Q	370	Q	538	P Q
38	P Q U	206	P Q	374	P Q	542	P
40	Q	208	Q	376	$\varnothing$	544	$\varnothing$
46	P Q	214	P Q	382	Q	550	Q
50	$\varnothing$	218	P Q	386	$\varnothing$	554	Q
56	Q	224	$\varnothing$	392	$\varnothing$	560	$\varnothing$
58	Q	226	U	394	P	562	P Q
62	P Q U	230	$\varnothing$	398	P Q	566	P Q
64	Q	232	Q	400	$\varnothing$	568	Q
70	$\varnothing$	238	$\varnothing$	406	P	574	P
74	P Q U	242	P Q U	410	Q	578	P
80	Q	248	$\varnothing$	416	$\varnothing$	584	Q
82	P Q U	250	$\varnothing$	418	$\varnothing$	586	P U
86	Q	254	P Q	422	P	590	Q
88	Q	256	$\varnothing$	424	$\varnothing$	592	Q
94	Q U	262	P Q	430	Q	598	Q
98	P Q U	266	P Q	434	Q	602	Q
104	$\varnothing$	272	$\varnothing$	440	$\varnothing$	608	$\varnothing$
106	Q U	274	$\varnothing$	442	P Q	610	$\varnothing$
110	$\varnothing$	278	P Q	446	Q U	614	P U
112	Q	280	Q	448	$\varnothing$	616	Q
118	P	286	$\varnothing$	454	P Q	622	P Q U
122	P Q U	290	P Q	458	Q U	626	Q U
128	Q	296	Q	464	Q	632	Q
130	P	298	Q	466	P Q	634	Q
134	P Q	302	Q	470	$\varnothing$	638	P
136	Q	304	$\varnothing$	472	Q	640	$\varnothing$
142	Q U	310	$\varnothing$	478	P Q	646	P
146	P Q	314	$\varnothing$	482	P Q	650	P
152	Q	320	Q	488	$\varnothing$	656	$\varnothing$
154	P	322	Q	490	P	658	P Q
158	Q U	326	$\varnothing$	494	Q	662	P
160	$\varnothing$	328	Q	496	Q		

5. APPLICATIONS TO FERMAT'S CONGRUENCE

Let p, q be odd primes. It is easy to prove that Fermat's congruence (1) has a nontrivial solution if $q \not\equiv 1 \pmod{p}$ or $(3, c) > 1$. However, the case $q \equiv 1 \pmod{p}$,

$(3, c) = 1$ involves many difficult and still unsolved problems. Combining together Theorems 1 and 3 we obtain the following main result.

Theorem 4. *Let p, q be odd primes such that $(p, q) \neq (3, 61)$. Then Fermat's congruence*

$$x^p + y^p + z^p \equiv 0 \pmod{q} \tag{27}$$

has only trivial solutions (that is, solutions (x, y, z) such that $xyz \equiv 0 \pmod{q}$) provided that:
(i) $q = 1 + cp$ *and* $(3, c) = 1$;
(ii) $2^c \not\equiv 1 \pmod{q}$, *or* $c \equiv 0 \pmod{4}$;
(iii) $L_{c/2} \not\equiv 0 \pmod{q}$, *or* $c \equiv 0 \pmod{4}$;
(iv) $q > \theta^{c/4}$.

The stronger condition $c \equiv 0 \pmod{4}$ in (ii) instead of $c \equiv 0 \pmod{8}$, is due to the fact that the number $2^{c/2} + 1$ does not have prime divisors of the form $q \equiv 1 \pmod{8}$; this has been proved in [14, p. 170]. Theorem 4 improves upon the previous results of Vandiver [15], Krasner [10] and the author [14].

The numerical evidence indicates that the conditions

$$2^c \not\equiv 1 \pmod{q} \quad \text{and} \quad L_{c/2} \not\equiv 0 \pmod{q}$$

are almost always superfluous; more precisely:

Proposition 1. *Let p, q be odd primes. Then, congruence* (27) *has only trivial solutions for every prime exponent*

$$p \leq \frac{\theta^{166} - 1}{664} = (3.9769287\ldots)10^{55},$$

provided that $q = 1 + cp$, $(3, c) = 1$, $q > \theta^{c/4}$ and that

$$(p, q) \neq (3, 31), (3, 61), (31, 683).$$

Proof. Assume that the pair (p, q) contradicts the truth of the proposition. Then, necessarily, $q \in \mathcal{P}_c$. By the results in Section 4 (last paragraph) it follows that $c \geq 664$. In consequence

$$p > \frac{\theta^{c/4} - 1}{c} \geq \frac{\theta^{166} - 1}{664},$$

which is impossible by hypothesis.

Proposition 1 leads naturally to the following conjecture.

Conjecture 1. Let p, q be odd primes. Then, congruence (27) has only trivial solutions provided that $q = 1 + cp$, $(3, c) = 1$, $q > \theta^{c/4}$ and that $(p, q) \neq (3, 31)$, $(3, 61)$, $(31, 683)$.

It is important to note that inequality $q > \theta^{c/4}$ is equivalent to

$$\begin{aligned} q &< \frac{4}{\log \theta} p \log p + \frac{4}{\log \theta} p \log g \log p \\ &= (4.936\ldots) p \log p + (4.936\ldots) p \log \log p \end{aligned}$$

(in fact, the last inequality is a bit weaker). According to a classical result of Dickson, congruence (27) has nontrivial solutions if

$$q > (p-1)^2 (p-2)^2 + 6p - 2.$$

Chowla [4] conjectured that the stronger inequality $q > p^2$ holds true for sufficiently large p.

Acknowledgment

I would like to express my thanks to the referee for valuable suggestions.

References

[1] D.W. Boyd, *The asymptotic behaviour of the circulant determinant*, J. Math. Appl. 86 (1982), 30–38. MR **83f:**10007

[2] 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*, Contemporary Mathematics 22, American Mathematical Society, Providence, 1988. MR **90d:**11009

[3] J. Brillhart, P.L. Montgomery and R.D. Silverman, *Tables of Fibonacci and Lucas Factorizations*, Math. Comp. 50 (1988), 251–260. MR **89h:**11002

[4] S. Chowla, *Some conjectures in elementary number theory*, Norske Vid. Selsk. Forh. (Trondheim) 35 (1962), 13. MR **25:**2995

[5] 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. MR **13:**822h

[6] G. Fee and A. Granville, *The prime factors of Wendt's binomial circulant determinant*, Math. Comp. 57 (1991), 839–848. MR **92f:**11183

[7] D. Ford and V. Jha, *On Wendt's Determinant and Sophie Germain's Theorem*, Experimental Math. 2 (1993), 113–119. MR **95b:**11029

[8] J.S. Frame, *Factors of the binomial circulant determinant*, Fibonacci Quart. 18 (1980), 9–23. MR **81j:**11007

[9] C. Helou, *On Wendt's determinant*, Math. Comp. 66 (1997), 1341–1346. MR **97j:**11014

[10] M. Krasner, *A propos du critère de Sophie Germain – Furtwängler pour le premier cas du théorèm de Fermat*, Mathematica Cluj. 16 (1940), 109–114. MR **1:**291k

[11] E. Lehmer, *On a resultant connected with Fermat's Last Theorem*, Bull. Amer. Math. Soc. 41 (1935), 864–867.

[12] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer, New York, 1979. MR **81f:**10023

[13] A. Simalarides, *Applications of the theory of cyclotomic field to Fermat's equation and congruence*, Ph.D. Thesis, Athens University, Athens 1984.

[14] A. Simalarides, *Sophie Germain's Principle and Lucas numbers*, Math. Scand. 67 (1990), 167–176. MR **92c:**11026

[15] H.S. Vandiver, *Some theorems in finite field theory with applications to Fermat's Last Theorem*, Proc. Nat. Acad. Sci. U.S.A. 30 (1944), 362–367. MR **6:**117e

[16] 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.

T.E.I. of Chalcis, Psahna 34400, Euboea, Greece