# On Wendt's Determinant and Sophie Germain's Theorem

David Ford and Vijay Jha

**CONTENTS**



Research supported by the Natural Sciences and Engineering Research Council (Canada) and Fonds pour la Formation de Chercheurs et l'Aide à la Recherche (Quebec).

Some results in section 3 of this work are taken from Jha's Ph.D. thesis [Jha 1992].

After a brief review of partial results regarding Case I of Fermat's Last Theorem, we discuss the relationship between the number of points on Fermat's curve modulo a prime and the resultant $R_n$ of the polynomials $X^n - 1$ and $(-1 - X)^n - 1$, called Wendt's determinant. The investigation of a conjecture about essential prime factors of $R_n$ (Conjecture 1.3) leads to a proof that Case I of Fermat's Last Theorem holds for any prime exponent $p > 2$ such that $np + 1$ is prime for some integer $n \leq 500$ not divisible by 3.

EDITOR'S NOTE: In addition to providing insight into Wendt's determinant, an object of interest in its own right, this paper belongs to a continuing line of investigations that may prove fruitful in spite of the recent announcement by Wiles of his proof of Fermat's Last Theorem. It is not unreasonable to hope for a more elementary proof than Wiles'.

## 1. INTRODUCTION

Case I of Fermat's Last Theorem for an odd prime $p$ is the statement that $x^p + y^p + z^p = 0$ has no integer solutions with $p \nmid xyz$. Throughout this paper, we will refer to it simply as "Case I". See [Ribenboim 1979; 1987] for references and a detailed history.

In 1823 Sophie Germain showed that Case I is true for any odd prime $p$ such that $2p+1$ is prime. In general, if $n$ is an integer not divisible by 3, Case I is true for all primes $p > 2$ such that $np+1$ is prime, with possibly a finite number of exceptions. Thus Germain's result was that the exceptional set is empty for $n = 2$. Legendre extended this to $n = 4, 8, 10, 14, 16$ (only even values of $n$ are interesting because of the condition that $np + 1$ be a prime).


1058-6458/96 \$0.50 per page

Denote by $E_n$ the exceptional set for the integer $n$, that is, let

$$E_n = \left\{ \begin{array}{r} p : p > 2 \text{ is prime, } np+1 \text{ is prime,} \\ \text{and Case I fails for } p. \end{array} \right\}$$

An important result of Furtwängler [1912] implies that:

**Theorem 1.1.** *If $n$ is any integer and $p \in E_n$, either $p$ divides $n$ or $np+1$ divides Wendt's determinant $R_n$.*

Wendt's determinant [Wendt 1894] can be defined as the resultant of the polynomials $X^n - 1$ and $(-1-X)^n - 1$. The finiteness of $E_n$ when $3 \nmid n$ follows from Theorem 1.1 and from the fact that $R_n \neq 0$ in this case. (When $n$ divides 3 we have $R_n = 0$, so no information on $E_n$ is gained.)

For any particular value of $n$, we can attempt to show that $E_n = \varnothing$ by using various criteria (discussed in more detail in Section 2) to eliminate the possible candidates allowed by Theorem 1.1. As we shall see, this strategy is particulary useful when we work successively with increasing values of $n$, for then we can use previously obtained information to account for most prime factors of $R_n$. Indeed, suppose we have proved that $E_m = \varnothing$ for all $m < n$ with $3 \nmid m$. Then, if $p \in E_n$ is exceptional, it follows that $mp+1$ is composite for all $m < n$ with $3 \nmid m$ (otherwise we would have $p \in E_m$). It also follows, by Theorem 1.1, that either

(a) $p \leq n$, or
(b) $p > n$ and $np+1$ divides $R_n$.

Possibility (b) leads to the following definition:

**Definition 1.2.** A prime divisor $q$ of $R_n$ is *essential* if $q = np+1$ for some prime $p > n$ such that $mp+1$ is composite for all $m < n$ with $3 \nmid m$.

The essential prime factors of $R_n$ seem to be quite scarce. For $n \leq 500$, with $3 \nmid n$, there are only two such primes. This suggests the following conjecture:

**Conjecture 1.3.** *The set of essential factors of $R_n$, for all $n$ not dividing 3, had natural density zero:*

$$\lim_{x\to\infty} \frac{\#\{p : p \leq x, p \text{ essential factor of some } R_n\}}{\#\{p : p \leq x, p \text{ prime}\}} = 0.$$

One can show that this conjecture implies that Case I holds for a set of prime exponents of natural density one. We apply these ideas, as explained below, to obtain the following extension of Germain's theorem:

**Theorem 1.4.** *$E_n$ is empty for all $n \leq 500$ such that $3 \nmid n$.*

This improves on the previous result in this direction [Fee and Granville 1991], where the bound is $n \leq 200$. As we shall see in Section 2, our approach differs from that of previous authors in that we do not use any criteria (like that of Wieferich) based upon Kummer–Mirimonoff congruences.

The rest of this paper has the following outline. Section 2 gives more details on the work that we build on. In Section 3 we study the set of points on Fermat's curve modulo $q$, establish a bijection between $(\mathbf{Z}/p\mathbf{Z})^2$-equivalence classes of nontrivial points and the set of algebraic factors of $R_n$ that are divisible by $q$, and describe explicitly some nonessential factors of $R_n$. In Section 4 we describe in some detail the computational procedure used in proving Theorem 1.4, and particularly in factorizing the $R_n$, the most computationally intensive step.

## 2. BACKGROUND

Of the classical attempts to prove that Case I holds for every odd prime $p$, we consider three categories. The first is based on the Kummer–Mirimonoff congruences and their consequences, and include Wieferich's criterion [Wieferich 1909]:

**Theorem 2.1.** *Case I holds for every $p$ such that $2^p \not\equiv 2 \pmod{p^2}$.*

Other examples are Mirimonoff's criterion [Ribenboim 1979], and Eichler's and Brückner's theorems

[Jha 1993]. These theorems reduce the task of verifying Case I to the verification of certain congruences modulo $p$, and have been used to establish Case I for a large number of primes [Coppersmith 1990].

The second approach originated with Germain, whose ideas Legendre used to prove the following:

**Theorem 2.2.** *Let $p$ and $q$ be distinct odd primes such that*

(a) $xyz \equiv 0 \pmod q$ *whenever* $x^p + y^p + z^p \equiv 0 \pmod q$, *and*
(b) *$p$ is not congruent to a $p$-th power modulo $q$.*

*Then Case I holds for the exponent $p$.*

Taking the special case $q \equiv 1 \pmod p$ we have a theorem of an entirely different nature from the ones in the first category; here congruences are modulo primes of the form $np + 1$. To establish that $E_n = \varnothing$ for a given $n$ (see the Introduction for the notation), it suffices to check conditions (a) and (b) of Theorem 2.2 for prime $p$ and $q$ with $q = np + 1$. One can show that, if $q = np + 1$, condition (a) holds if and only if $q \nmid R_n$.

The third category of criteria is represented by the result of Furtwängler alluded to in the Introduction, which says that if Case I fails with integers $x, y, z$ and exponent $p$, and if $q$ is a prime dividing $xyz$, then $q^p \equiv q \pmod{p^2}$. A simple reasoning shows that this result, together with the remark in the preceding paragraph, implies Theorem 1.1.

Theorem 1.1 is very convenient because it depends only on $p$ and not on the hypothetical solution $(x, y, z)$. Dénes [1951] used it, together with his observation that $R_n$ is the product of norms of elements of $\mathbf{Q}(\zeta_n)$, where $\zeta_n$ is a primitive $n$-th root of unity, to prove that $E_n = \varnothing$ for all $n \le 110$ with $3 \nmid n$. Recently Fee and Granville [1991] extended this to all $n \le 200$ with $3 \nmid n$, working according to the following plan:

(a) Express $R_n$ as the product of norms of certain elements of $\mathbf{Q}(\zeta_n)$, and factorize these norms completely.
(b) Establish Case I for all $p$ such that $np + 1$ is prime and divides $R_n$. (In this range it is known that the other possibility for elements of $E_n$—namely, $p$ dividing $n$ and such that $np + 1$ is prime—cannot occur.)

These authors, like Dénes, used Wieferich's criterion (Theorem 2.1) to carry out step (b) of this scheme. But the use of such criteria obscures the power of the criteria implicit in the knowledge that $E_n = \varnothing$. It is true that, for each $n$, this knowledge seems to yield less information than do criteria based on Kummer–Mirimonoff congruences. For example, Lehmer showed that the Wieferich criterion fails for only two primes under $6 \times 10^9$ [Ribenboim 1987]; whereas, for $p = 197$, we have $np + 1$ composite for all $n < 38$ with $3 \nmid n$, so the fact that $E_n =$ for these values of $n$ is of no benefit in proving that Case I holds for $p$. However, as first observed in [Adleman and Heath-Brown 1985], the condition $E_n = \varnothing$ is very effective when applied collectively for a sequence of values of $n$.

We have, therefore, taken a different approach, avoiding the use of criteria based on Kummer–Mirimonoff congruences, and working by induction on $n$. Assuming that $E_m = \varnothing$ for each $m < n$ with $3 \nmid m$, we must do two things in order to prove that $E_n = \varnothing$:

(a) Verify that Case I is satisfied for odd primes $p \le n$ with $np + 1$ prime.
(b) Find the essential prime divisors $q$ of $R_n$ (Definition 1.2), and verify that Case I is satisfied for the values of $p$ such that $q = np + 1$.

In practice, the primes in (a) are small and easily accounted for. Indeed, for each odd prime $p \le 500$, it is easy to find an integer $m < p$ with $mp+1$ prime and $3 \nmid m$. We have $m < n$, so by the induction assumption $E_m = \varnothing$ and $p$ is not excpetional.

As to the primes in (b), they usually form an empty set, as we remarked in the Introduction. For more details, see Section 4.

We conclude this section with some remarks on the density of primes for which Case I holds. Note that, by Theorem 1.1, we have $\#E_n < \omega(n) + \omega(R_n)$, where $\omega(u)$ denotes the number of distinct prime divisors of the integer $u$. Since $\log R_n < cn^2$ for some constant $c > 0$, we get a bound for $\#E_n$. Adleman and Heath-Brown [1985] used this bound to show that, for $\frac{1}{2} \le \tau < 1$, the sum

$$\Sigma_\tau = \sum \# \left\{ \begin{array}{r} q : q \le x,\ q \equiv 1 \pmod p), \\ q \equiv 2 \pmod 3) \end{array} \right\},$$

taken over odd primes $p \in (x^\tau, x]$ for which Case I fails, satisfies

$$\Sigma_\tau \le \sum_{\substack{n < x^{1-\tau} \\ 3 \nmid n}} \#E_n \le \sum_{n < x^{1-\tau}} cn^2 = O(x^{3(1-\tau)}).$$

They also applied sieve methods to estimate this sum in a different way. Fouvry [1985] then showed that there exists $\tau > \frac{2}{3}$ such that $\Sigma_\tau > F(\tau)\,\mathrm{Li}(x)$, where $F(\tau) > 0$. In this way they proved that the number of primes $\le x$ for which Case I is true is at least of the order of $x^{2/3}$.

As remarked before, the criteria $E_n = \varnothing$ are fruitful when considered collectively and independent of any other type of criteria. One motivation to use only these criteria (rather than Wieferich and the like) is to measure their power from the point of view of strengthening Adleman, Heath-Brown, and Fouvry's theorems.

## 3. FERMAT'S CURVE MODULO q AND WENDT'S DETERMINANT

In this section, unless we say otherwise, $p$ is a positive integer and $q \equiv 1 \pmod p$ is a prime power such that $3 \nmid (q-1)/p$.

Let $\mathfrak{C}$ be the projective Fermat's curve of exponent $p$ in the finite field $\mathbf{F}_q$ of $q$ elements. We call two points $(x, y)$ and $(x', y')$ on $\mathfrak{C}$ *equivalent* if there exist $p$-th roots of unity $a$ and $b$ in $\mathbf{F}_q$ such that $x' = ax$ and $y' = by$. A point $(x, y)$ is *trivial* if $x = 0$ or $y = 0$. There are two classes of trivial points, each with $p$ elements; all other classes contain $p^2$ elements each. Thus the number of points on $\mathfrak{C}$ is $kp^2 + 2p$, where $k$ is the number of equivalence classes of nontrivial points.

Let $\zeta_n$ be a primitive $n$-th root of unity, and let $\mathfrak{N}$ be the norm map from $\mathbf{Q}(\zeta_n)$ to $\mathbf{Q}$. Wendt's determinant $R_n$ is the product of the elements $1 + \zeta_n^i + \zeta_n^j$, for $i, j \in \mathbf{Z}/n\mathbf{Z}$ [Dénes 1951; Ribenboim 1989]. We call two pairs $(i, j)$ and $(i', j')$ in $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ *equivalent* if there is a unit $t \in \mathbf{Z}/n\mathbf{Z}$ such that $i' = ti$ and $j' = tj$ in $\mathbf{Z}/n\mathbf{Z}$. Let $T_n$ be the set of these equivalence classes. It is clear that $R_n$ is the product of norms $\mathfrak{N}(1 + \zeta_n^i + \zeta_n^j)$, where $(i, j)$ runs over a set of representatives of distinct classes from $T_n$.

Let $Q$ be a prime ideal of the field $\mathbf{Q}(\zeta_n)$ lying above $q$, and fix an isomorphism between $\mathbf{Z}[\zeta_n]/Q$ and $\mathbf{F}_q$. Let $\omega$ be the image of $\zeta_n$ in $\mathbf{F}_q$. Then $\omega$ is a primitive $n$-th root of unity in $\mathbf{F}_q$, so it has a $p$-th root $\alpha \in \mathbf{F}_q$. One easily shows that $q$ divides $\mathfrak{N}(1 + \zeta_n^i + \zeta_n^j)$ if and only if the pair $(\alpha^i, \alpha^j)$ lies on the Fermat's curve $\mathfrak{C}$ in $\mathbf{F}_q$. Thus the correspondence

$$(\alpha^i, \alpha^j) \mapsto (i, j)$$

defines an injective map $\mathfrak{C} \mapsto T_n$, whose image consists of all those classes of $(i, j)$ such that $q$ divides $\mathfrak{N}(1 + \zeta_n^i + \zeta_n^j)$.

Now consider the maps

$$(i, j) \mapsto (j, i) \quad \text{and} \quad (i, j) \mapsto (j, j - i)$$

of $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ onto itself. These maps factor with respect to the equivalence relation defined above, to yield bijections of $T_n$ that we call $f$ and $g$. We have $f^2 = g^3 = 1$. We further quotient $T_n$ by the action of the group

$$\{1,\ f,\ g,\ fg,\ g^2,\ fg^2\} \tag{3.1}$$

generated by $f$ and $g$, obtaining a set $\bar{T}_n$. Then $\mathfrak{N}(1 + \zeta_n^i + \zeta_n^j)$ only depends on the class of $(i, j)$ in $\bar{T}_n$. Let $k_{ij}$ be the number of elements of $T_n$ in the class of $(i, j)$ in $\bar{T}_n$. Then $R_n$ is the product of $\mathfrak{N}(1 + \zeta_n^i + \zeta_n^j)^{k_{ij}}$, where $(i, j)$ varies over a set of representatives of distinct classes of $\bar{T}_n$. A priori, $k_{ij}$ can take the values 1, 2, 3 and 6, but it is easy to see that $k_{ij} = 1$ does not occur, and the condition $3 \nmid (q-1)/p$ excludes the case $k_{ij} = 2$. Hence the possible values for $k_{ij}$ are 3 and 6. One can verify that $k_{ij} = 3$ for some $(i, j)$ if and only if $q$ divides $2^n - 1$. We have proved the following:

**Proposition 3.1.** *Let $T_{n,q}$ be the subset of $T_n$ consisting of those classes of $(i, j)$ such that $q$ divides $\mathfrak{N}(1 + \zeta_n^i + \zeta_n^j)$. Then there is a bijection between $T_{n,q}$ and the set of equivalence classes of nontrivial points on Fermat's curve $\mathfrak{C}$. Further,*

$$N(p, q) - 2p = kp^2,$$

*where $N(p, q)$ is the number of points on $\mathfrak{C}$ and $k = \#T_{n,q}$ is the number of distinct norms appearing in $R_n$ that are divisible by $q$. Moreover, $k \equiv 0 \pmod 3$, and if $k$ is odd then $q$ divides $2^n - 1$.*

**Remark 3.2.** This shows that most of the norms dividing $R_n$ (namely, those not dividing $2^n - 1$) divide it to the sixth power. Thus we can reduce the number of norms to be computed in the calculation of $R_n$ by almost six times. We also conclude that there exist integers $a_n$, $b_n$ such that $R_n = a_n^3 b_n^6$.

Now we describe some nonessential factors of the resultant $R_n$.

**Proposition 3.3.** *Let $n \in \mathbf{Z}^+$, let $q$ be an odd prime coprime to $n$, and let $f$ be the order of $q$ in the group of units of $\mathbf{Z}/n\mathbf{Z}$. Then*

(i) *Let $m = (q^f - 1)/n$. If $\gcd(q - 1, m) = 1$ then $q^f$ divides $R_n$.*
(ii) *Let $q \equiv 1 \pmod n$ and $q < n^{4/3}$. Then $q^k$ divides $R_n$, where $k$ is given by Proposition 3.1.*
(iii) *Let $q - 1$ divide $n$. Then $q^{f(q-2)}$ divides $R_n$.*

*Proof.* (i) Since $\gcd(q-1, m) = 1$, the map $x \mapsto x^m$ is a bijection of $\mathbf{F}_q$. Hence the equation $x^m + y^m + 1 \equiv 0$ has a solution in $\mathbf{F}_q$ with $xy \not\equiv 0 \pmod q$. Then $x^m$ is a common root of the polynomials $X^m - 1$ and $(-1 - X)^m - 1$ in $\mathbf{F}_q$. This shows that the resultant is zero, that is $q$ divides $R_n$.

If $Q$ is a prime ideal in $\mathbf{Q}(\zeta_n)$ lying above $q$, we have $\mathfrak{N}(Q) = q^f$. Using the decomposition of $R_n$ as a product of algebraic integers $1 + \zeta_n^i + \zeta_n^j$, we see that there exist $i, j \in \mathbf{Z}/n\mathbf{Z}$ such that $Q$ divides $1+\zeta_n^i+\zeta_n^j$. Hence $\mathfrak{N}(Q)$ divides $q^f = \mathfrak{N}(1+\zeta_n^i+\zeta_n^j)$, and $q^f$ divides $R_n$.

(ii) Let $p = (q-1)/n$. It follows from [Lang 1990, § 6], the number of finite points on the projective Fermat's curve in $\mathbf{F}_q$ is

$$N(p, q) - 2p = q + 1 - 3p + r(p, q),$$

where $r(p, q)$ is an error term not exceeding

$$(p - 1)(p - 2)q^{1/2}.$$

Thus, for $q > p^4$ this curve always has finite points. Exactly as in the proof of Proposition 3.1, we conclude that $q$ divides $k$ distinct norms appearing in $R_n$.

(iii) For $p = 1$, the projective Fermat equation with exponent $p$ has $q-2$ finite points in $\mathbf{F}_q$. Hence it has at least $q - 2$ solutions in the finite field $\mathbf{F}_r$, where $r = q^f$. As in Proposition 3.1, $q$ divides at least $q-2$ distinct norms appearing in $R_n$. However then, as shown in the proof of part (i), $q^f$ divides all these norms dividing $R_n$. □

**Remark 3.4.** The sum of the nonessential factors of $R_n$ described by (iii), for $n \leq x$, is at least of the order of $x^2$, even without counting the orders $f$.

## 4. COMPUTATIONS

This section elaborates on the implementation of the inductive procedure outlined in Section 2 to prove Theorem 1.4.

The first step of the procedure, for each $n$ of interest ($n \leq 500$ even with $3 \nmid n$), is the factorization of $R_n$. As observed in [Fee and Granville 1991], this is the step most likely to constitute an obstacle in terms of computational power. The obvious idea is to compute the norms $\mathfrak{N}(1+\zeta_n^i+\zeta_n^j)$ for all $i, j \in \mathbf{Z}/n\mathbf{Z}$, and factorize these integers. However, as already observed in the preceding section, $\mathfrak{N}(1 + \zeta_n^i + \zeta_n^j)$ does not change when we multiply both $i$ and $j$ by the same unit in $\mathbf{Z}/n\mathbf{Z}$, or when we replace $(i, j)$ by its image under one of the transformations of the group (3.1). In other words, we need only take one representative $(i, j)$ from each element of $\bar{T}_n$.

Another shortcut comes from the fact that $R_m$ divides $R_n$ whenever $m$ divides $n$, so $q$ is a prime divisor of $R_n$ if and only if it is a prime divisor of $\mathfrak{N}(1+\zeta_d^i+\zeta_d^j)$ for some $d \mid n$ with $\gcd(i,j,d)=1$. Thus we economize by computing $\mathfrak{N}(1+\zeta_d^i+\zeta_d^j)$ only when $\gcd(i,j,n)=1$ (but note that then we are forced to make the computations also for odd $n \le 250$ with $3 \nmid n$). The property $\gcd(i,j,n)=1$ depends only on the class of $(i,j)$ in $\bar{T}_n$, so this simplification does not interfere with the one mentioned in the previous paragraph.

For each of the necessary pairs $(i,j)$, the norm $\mathfrak{N}(1+\zeta_n^i+\zeta_n^j)$ is easy to compute as the resultant of the $n$-th cyclotomic polynomial $\Phi_n(X)$ with the polynomial $1+X^i+X^j$. This part of the computation was performed in ALGEB [Ford 1978], and required 5.21 CPU hours. (Computations were performed on a VAX 6510 system and a VAXstation 4000 at Concordia University.)

We completed the factorization of the $R_n$ in several steps. Two cases must be distinguished: that of the factors $\mathfrak{N}(1+\zeta_n^i+\zeta_n^j)$ with $i,j \ne 0$, and that of the factors $\mathfrak{N}(2+\zeta_n)$.

There were 12859 distinct nontrivial norms of the first type. The Maple `ifactor` procedure [Char et al. 1991], with the `easy` option, reduced this to a set of 2323 composite values in 1.22 CPU hours. An ALGEB implementation of the Pollard rho method reduced this to 64 composite values in 48.50 CPU hours. An ALGEB implementation of the Lenstra elliptic curve method completely factorized the remaining values in 9.10 CPU hours.

The factorizations of the (249 distinct nontrivial) norms of the form $\mathfrak{N}(2+\zeta_n)$ are considerably more difficult; fortunately they can be derived from the factorizations of $(-2)^n+1$, which for $n \le 500$ are given in [Brillhart et al. 1988].

Next we eliminated the factors of $R_n$ that were not of the form $q = np+1$ with $p$ prime. The sizes of the remaining sets are shown in Table 1. Then, for each $n$, we constructed the set of essential factors of $R_n$ by discarding the factors $q = np+1$ such that $mp+1$ is prime for some $m < n$ with $3 \nmid m$. The resulting sets were empty, except for

| $n$ | $w_n$ | $n$ | $w_n$ | $n$ | $w_n$ | $n$ | $w_n$ |
|---|---|---|---|---|---|---|---|
| 2 | 0 | 128 | 3 | 254 | 10 | 380 | 14 |
| 4 | 0 | 130 | 8 | 256 | 11 | 382 | 13 |
| 8 | 0 | 134 | 5 | 260 | 15 | 386 | 6 |
| 10 | 1 | 136 | 8 | 262 | 8 | 388 | 7 |
| 14 | 1 | 140 | 7 | 266 | 8 | 392 | 16 |
| 16 | 0 | 142 | 9 | 268 | 4 | 394 | 18 |
| 20 | 1 | 146 | 8 | 272 | 10 | 398 | 11 |
| 22 | 2 | 148 | 4 | 274 | 5 | 400 | 22 |
| 26 | 2 | 152 | 6 | 278 | 8 | 404 | 19 |
| 28 | 1 | 154 | 9 | 280 | 16 | 406 | 16 |
| 32 | 2 | 158 | 5 | 284 | 9 | 410 | 11 |
| 34 | 2 | 160 | 7 | 286 | 9 | 412 | 15 |
| 38 | 3 | 164 | 7 | 290 | 15 | 416 | 14 |
| 40 | 1 | 166 | 4 | 292 | 10 | 418 | 14 |
| 44 | 2 | 170 | 10 | 296 | 5 | 422 | 17 |
| 46 | 2 | 172 | 3 | 298 | 7 | 424 | 9 |
| 50 | 3 | 176 | 4 | 302 | 9 | 428 | 15 |
| 52 | 3 | 178 | 5 | 304 | 12 | 430 | 17 |
| 56 | 5 | 182 | 10 | 308 | 13 | 434 | 21 |
| 58 | 1 | 184 | 5 | 310 | 12 | 436 | 11 |
| 62 | 3 | 188 | 7 | 314 | 12 | 440 | 18 |
| 64 | 5 | 190 | 6 | 316 | 9 | 442 | 13 |
| 68 | 1 | 194 | 8 | 320 | 15 | 446 | 13 |
| 70 | 6 | 196 | 5 | 322 | 11 | 448 | 15 |
| 74 | 4 | 200 | 6 | 326 | 15 | 452 | 12 |
| 76 | 2 | 202 | 6 | 328 | 13 | 454 | 10 |
| 80 | 4 | 206 | 9 | 332 | 11 | 458 | 14 |
| 82 | 3 | 208 | 4 | 334 | 7 | 460 | 25 |
| 86 | 5 | 212 | 13 | 338 | 14 | 464 | 11 |
| 88 | 4 | 214 | 7 | 340 | 13 | 466 | 15 |
| 92 | 5 | 218 | 6 | 344 | 13 | 470 | 15 |
| 94 | 7 | 220 | 9 | 346 | 11 | 472 | 14 |
| 98 | 5 | 224 | 10 | 350 | 18 | 476 | 24 |
| 100 | 4 | 226 | 11 | 352 | 10 | 478 | 14 |
| 104 | 5 | 230 | 10 | 356 | 15 | 482 | 14 |
| 106 | 3 | 232 | 8 | 358 | 6 | 484 | 23 |
| 110 | 8 | 236 | 7 | 362 | 19 | 488 | 17 |
| 112 | 4 | 238 | 15 | 364 | 12 | 490 | 24 |
| 116 | 6 | 242 | 12 | 368 | 9 | 494 | 22 |
| 118 | 7 | 244 | 8 | 370 | 16 | 496 | 13 |
| 122 | 5 | 248 | 8 | 374 | 18 | 500 | 13 |
| 124 | 6 | 250 | 8 | 376 | 10 | | |

**TABLE 1.** Number $w_n$ of prime factors of $R_n$ of the form $pn+1$, for $p$ an odd prime.

two, which had one element each, given by $np+1$ with

$$n = 292, \quad p = 5907553471801 \quad \text{and}$$
$$n = 388, \quad p = 68115914363248623814719 1.$$

To prove that these values of $p$ are not exceptional, it is enough by Theorem 1.1 to find $n'$ with $n'p+1$ prime, $p \nmid n'$ and $n'p+1 \nmid R_{n'}$. We can take $n' = 316$ and $n' = 430$, respectively. This takes care of (b) in the procedure outlined in Section 2, near the bottom of page 115. We saw there how to take care of (a).

The elimination of nonessential factors of $R_n$ was programmed in ALGEB. The proof that they are not exceptional was done with simple Maple programs (the computation of $R_m$ mod $q$ being very quick). These steps took only a few minutes of CPU time.

## ACKNOWLEDGEMENT

The authors wish to acknowledge the valuable assistance of Peter Montgomery.

## REFERENCES

[Adleman and Heath-Brown 1985] L. M. Adleman and D. R. Heath-Brown, "The first case of Fermat's Last Theorem", *Invent. Math.* **79** (1985), 409–416.

[Boyd 1982] D. W. Boyd, "The asymptotic behavior of the binomial circular determinant", *J. Math. Anal. Appl.* **86** (1982), 30–38.

[Brillhart et al. 1988] J. Brillhart et al., *Factorization of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to High Powers* (2nd ed.), Contemporary Mathematics **22**, American Mathematical Society, Providence, 1988.

[Char et al. 1991] B. W. Char et al., *Maple V Language Reference Manual*, Springer-Verlag, New York, 1991.

[Coppersmith 1990] D. Coppersmith, "Fermat's Last Theorem (case I) and the Wieferich criterion", *Math. Comp.* **54** (1990), 895–902.

[Dénes 1951] 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.

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

[Ford 1978] D. Ford, "On the computation of the maximal order in a Dedekind domain", Ph.D. Dissertation, Ohio State University, 1978.

[Fouvry 1985] E. Fouvry, "Theoreme de Brun–Titshmarsh; application au Theoreme de Fermat", *Invent. Math.* **79** (1985), 383–407.

[Furtwängler 1912] P. Furtwängler, "Letzter Fermatscher Satz und Eisensteinsches Reziprozitätsprinzip", *Sitzungsber. Akad. Wiss. Wien, Math.-Naturwiss. Abt. 2a* **121** (1912), 589–592.

[Jha 1992] V. Jha, "The Stickelberger ideal in the spirit of Kummer and the first case of Fermat's Last Theorem", Ph.D. thesis, Panjab University, Chandigarh, India, 1992,. Also published as Queen's Papers in Pure and Applied Math. **93**, Queen's University, Kingston, Ont., 1993.

[Lang 1990] S. Lang, *Cyclotomic Fields I and II* (combined 2nd ed.), Springer-Verlag, New York, 1990.

[Ribenboim 1979] P. Ribenboim, *Thirteen Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.

[Ribenboim 1987] P. Ribenboim, "Recent results about Fermat's Last Theorem", *Expositiones Math.* **5** (1987), 75–90.

[Ribenboim 1989] P. Ribenboim, *The Book of Prime Number Records* (2nd ed.), Springer-Verlag, New York, 1989.

[Wendt 1984] E. Wendt, "Arithmetische Studien über den letzten Fermatschen Satz", *J. Reine Angew. Math.* **113** (1894), 335–347.

[Wieferich 1909] A. Wieferich, "Zum letzten Fermat'schen Theorem", *J. Reine Angew. Math.* **136** (1909), 293–302.

David Ford, Centre Interuniversitaire en Calcul Mathématique Algébrique, Department of Computer Science, Concordia University, Montréal, Québec, Canada (ford@abacus.concordia.ca)

Vijay Jha, Centre Interuniversitaire en Calcul Mathématique Algébrique, Department of Computer Science, Concordia University, Montréal, Québec, Canada (jha@abacus.concordia.ca)

Received May 17, 1993; accepted in revised form August 19