MATHEMATICS OF COMPUTATION
Volume 67, Number 223, July 1998, Pages 1323–1330
S 0025-5718(98)00982-X

EVERY ODD PERFECT NUMBER HAS A PRIME FACTOR WHICH EXCEEDS 10^6

PETER HAGIS, JR. AND GRAEME L. COHEN

ABSTRACT. It is proved here that every odd perfect number is divisible by a prime greater than 10^6.

1. INTRODUCTION

In what follows, a, b, c, ... will be used to represent non-negative integers, with primes being symbolized by p, q and r. An element of the (possibly empty) set of odd perfect numbers will be denoted by N, so that $\sigma(N) = 2N$ where σ is the familiar sum of divisors function. The dth cyclotomic polynomial will be symbolized by F_d, so that $F_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$. If p and m are relatively prime, $h(p;m)$ will denote the order of p modulo m.

According to Theorem 3.4 in [9],

(1) $\sigma(p^a) = \prod_d F_d(p)$, where $d \mid (a+1)$ and $d > 1$.

From Theorems 94 and 95 in [8],

(2) $q \mid F_m(p)$ if and only if $m = q^b h(p;q)$. If $b > 0$, then $q \parallel F_m(p)$. If $b = 0$, then $q \equiv 1 \pmod{m}$.

It follows from (2) that

(3) if $q \mid F_r(p)$, then either $r = q$ and $p \equiv 1 \pmod{q}$ (and $q \parallel F_r(p)$) or $q \equiv 1 \pmod{r}$;

(4) if $q = 3$ or 5 and $m > 1$ is odd, then $q \mid F_m(p)$ (in fact, $q \parallel F_m(p)$) if and only if $m = q^b$ and $p \equiv 1 \pmod{q}$.

According to a result due to Bang [1],

(5) if p is an odd prime and $m \geq 3$, then $F_m(p)$ has at least one prime factor q such that $q \equiv 1 \pmod{m}$.

It is well known, and easy to prove, that

(6) $N = p_0^{a_0} p_1^{a_1} \dots p_u^{a_u}$, where the p_i are distinct odd primes, $p_0 \equiv a_0 \equiv 1 \pmod{4}$, and $2 \mid a_i$ if $i > 0$. (In this, p_0 is called the *special* prime.)

In [4], it was proved that at least one of the p_i in (6) exceeds 100110. In 1978, Condict [3], in his senior thesis at Middlebury College, improved this bound to 300000, while in 1982 Brandstein [2] announced that at least one of the p_i is greater than 500000. (To the best of our knowledge, however, Brandstein's announcement has never been substantiated by a public proof.) The purpose of the present paper is to improve these results by proving the following

Received by the editor October 24, 1995 and, in revised form, July 10, 1996.
1991 *Mathematics Subject Classification.* Primary 11A25, 11Y70.

Theorem. *If N is odd and perfect, then N has a prime factor which exceeds* 10^6*.*

Our proof will be by contradiction. Thus, we now assume without further explicit mention that $p_i < 10^6$ for every p_i in (6), and shall show that this assumption is untenable.

Since N is perfect, and since σ is multiplicative, it follows from (1) and (6) that

(7) $2N = \prod_{i=0}^{u} \sigma(p_i^{a_i}) = \prod_{i=0}^{u} \prod_d F_d(p_i)$, where $d \mid (a_i+1)$ and $d > 1$ (with $d = 2$ if and only if $i = 0$).

We see immediately that the set of p_i in (6) is identical with the set of odd prime factors of the $F_d(p_i)$ in (7). In particular, recalling our assumption we note that all of the prime factors of each $F_d(p_i)$ must be less than 10^6. Our proof will hinge on the consequence that if r is a prime divisor of $a_i + 1$, then every prime factor of $F_r(p_i)$ must be less than 10^6.

2. Acceptable values of $F_r(p)$

If $p > 2$ and r are primes, we shall say that $F_r(p)$ is *acceptable* if every prime divisor of $F_r(p)$ is less than 10^6. It follows easily from (5) that if $r > 500000$, then $F_r(p)$ is unacceptable for every odd prime p. We shall say that the prime p is *inadmissible* if $F_r(p)$ is unacceptable for every prime r (with $r = 2$ taken into consideration only if it is possible that p is the special prime for N).

An extensive computer search revealed that if $3 \le p < 10^6$ and $r \ge 7$, then $F_r(p)$ is unacceptable except for the 35 pairs of values of p and r listed in Table 1. Details of the search and supporting arguments may be found in an appendix to this paper. At the suggestion of a referee, some of these arguments have been included in Section 7 of the present paper. The complete appendix appears in [5] and is available upon request from the second author.

3. An important set of primes

Our objective in this section is to show that N is not divisible by certain "small" primes.

Lemma 1. *Let X be the set of primes*

$$X = \{3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 43, 61, 127, 131, 151, 1093\}.$$

If $p \in X$, then $p \nmid N$.

The proof proceeds by considering each prime p in X in turn, but in the order

$$1093, 151, 31, 127, 19, 11, 7, 23, 131, 37, 61, 13, 3, 5, 29, 43, 17.$$

We assume $p \mid N$ and find all acceptable values of $F_r(p)$ (with $r = 2$ being considered only if p might be the special prime); from (7), $F_r(p) \mid 2N$ for at least one acceptable $F_r(p)$ and each odd prime divisor of this $F_r(p)$ divides N; from each acceptable $F_r(p)$ a single odd prime divisor, say q, is selected and all of the acceptable values of $F_r(q)$ are determined. This procedure is iterated until an inadmissible prime or some other contradiction is encountered, thus showing that $p \nmid N$. Treating the primes of X in the given order allows those already considered to be used in the elimination of subsequent ones.

We shall illustrate the method by showing that $1093 \nmid N$ and $151 \nmid N$. The complete proof of Lemma 1 is given in the appendix mentioned in Section 2. Hopefully, the nomenclature we use is self-explanatory. We write p^* to imply that p is the

TABLE 1. Acceptable values of $F_r(p)$ for $3 \le p < 10^6$ and $r \ge 7$

p	r	$F_r(p)$
3	7	1093
3	11	$23 \cdot 3851$
3	13	797161
3	17	$1871 \cdot 34511$
3	19	$1597 \cdot 363889$
5	7	19531
7	7	$29 \cdot 4733$
7	11	$1123 \cdot 293459$
11	7	$43 \cdot 45319$
13	11	$23 \cdot 419 \cdot 859 \cdot 18041$
19	7	$701 \cdot 70841$
43	7	$7 \cdot 5839 \cdot 158341$
59	7	$43 \cdot 281 \cdot 757 \cdot 4691$
67	7	$175897 \cdot 522061$
79	7	$281 \cdot 337 \cdot 1289 \cdot 2017$
127	7	$7 \cdot 43 \cdot 86353 \cdot 162709$
131	7	$127 \cdot 189967 \cdot 211093$
191	7	$127 \cdot 197 \cdot 10627 \cdot 183569$
269	7	$43 \cdot 211 \cdot 631 \cdot 2633 \cdot 25229$
359	7	$211 \cdot 449 \cdot 1303 \cdot 4019 \cdot 4327$
389	7	$127 \cdot 337 \cdot 659 \cdot 827 \cdot 148933$
431	7	$29 \cdot 953 \cdot 967 \cdot 1009 \cdot 238267$
2381	7	$7 \cdot 43 \cdot 2689 \cdot 3613 \cdot 72997 \cdot 853903$
2713	7	$29^2 \cdot 43 \cdot 73361 \cdot 258469 \cdot 581729$
3301	7	$29^2 \cdot 911 \cdot 38669 \cdot 186733 \cdot 233941$
3779	7	$197 \cdot 2311 \cdot 23773 \cdot 455407 \cdot 591053$
4327	7	$7 \cdot 3221 \cdot 5503 \cdot 5657 \cdot 92401 \cdot 101221$
8009	7	$7 \cdot 43 \cdot 127 \cdot 491 \cdot 127247 \cdot 305873 \cdot 361313$
9719	7	$281 \cdot 3067 \cdot 8219 \cdot 19937 \cdot 30773 \cdot 193957$
10889	7	$2003 \cdot 22093 \cdot 116341 \cdot 471997 \cdot 686057$
10949	7	$7 \cdot 29 \cdot 197 \cdot 547 \cdot 1009 \cdot 6917 \cdot 25523 \cdot 442177$
27457	7	$29 \cdot 42463 \cdot 65171 \cdot 71261 \cdot 91813 \cdot 816047$
53831	7	$7 \cdot 29 \cdot 39341 \cdot 104651 \cdot 257489 \cdot 269221 \cdot 420001$
191693	7	$7561 \cdot 11887 \cdot 14869 \cdot 16759 \cdot 89839 \cdot 118399 \cdot 208279$
493397	7	$29^2 \cdot 127 \cdot 1163 \cdot 2129 \cdot 4229 \cdot 26041 \cdot 50177 \cdot 71359 \cdot 138349$

special prime. (Of course, two different primes cannot both be special simultaneously.)

A. $1093 \nmid N$.

A, 1093: $F_2(1093) = 2 \cdot 547$; $F_3(1093) = 3 \cdot 398581$.

A, 1093^*, 547: $F_3(547) = 3 \cdot 163 \cdot 613$.

A, 1093^*, 547, 613: $F_3(613) = 3 \cdot 7 \cdot 17923$; $F_5(613) = 131 \cdot 20161 \cdot 53551$.

A, 1093^*, 547, 613, 17923: $F_3(17923) = 3 \cdot 13 \cdot 31 \cdot 265717$.

A, 1093^*, 547, 613, 17923, 265717: 265717 is inadmissible.

A, 1093^*, 547, 613, 20161: 20161 is inadmissible.

A, 1093, 398581: $F_2(398581) = 2 \cdot 17 \cdot 19 \cdot 617$.

A, 1093, 398581^*, 617: $F_3(617) = 97 \cdot 3931$.

A, 1093, 398581^*, 617, 3931: $F_3(3931) = 3 \cdot 7 \cdot 31 \cdot 23743$.

A, 1093, 398581^*, 617, 3931, 23743: 23743 is inadmissible.

B. $151 \nmid N$.

B, 151: $F_3(151) = 3 \cdot 7 \cdot 1093$, contradiction to A.

4. A restriction on the exponents in the prime power decomposition of N

Suppose that $p^a \parallel N$ and $r \mid (a+1)$ where $r > 5$. Then $F_r(p)$ appears in Table 1 and, from (7), $F_r(p) \mid N$. It follows from Table 1 and Lemma 1 that $r = 7$ and $p \in \{67, 79, 359, 3779, 9719, 10889, 191693\}$. Referring to Table 1, we see that if $p = 67$, then $175897 \mid N$. Since $F_r(175897)$ is acceptable only for $r = 2$ and since $F_2(175897) = 2 \cdot 37 \cdot 2377$ (and $37 \nmid N$ from Lemma 1), we conclude that $p \neq 67$. Similarly, if $p = 79$, then $337 \mid N$; only $F_2(337) = 2 \cdot 13^2$ and $F_3(337) = 3 \cdot 43 \cdot 883$ are acceptable and since neither 13 nor 3 divides N we see that $p \neq 79$. If $p = 359$, then $1303 \mid N$; only $F_3(1303) = 3 \cdot 13 \cdot 19 \cdot 2293$ is acceptable and $3 \nmid N$, so $p \neq 359$. If $p = 3779$, then $455407 \mid N$; since 455407 is inadmissible, $p \neq 3779$. If $p = 9719$, then $3067 \mid N$; since only $F_3(3067) = 3 \cdot 127 \cdot 24697$ is acceptable and $3 \nmid N$, we see that $p \neq 9719$. If $p = 10889$, then $471997 \mid N$; but only $F_2(471997) = 2 \cdot 19 \cdot 12421$ is acceptable and $19 \nmid N$, so $p \neq 10889$. Finally, $p \neq 191693$ since otherwise $11887 \mid N$, and 11887 is inadmissible.

We have proved

Lemma 2. *If $p^a \parallel N$ and p is not the special prime p_0, then $a + 1 = 3^b \cdot 5^c$ where $b + c > 0$. If $p_0^{a_0} \parallel N$, then $a_0 + 1 = 2 \cdot 3^b \cdot 5^c$ where $b + c \geq 0$.*

5. Four important sets

Let $S = \{47, 53, 59, \ldots\}$ be the set of all primes p such that $p \not\equiv 1 \pmod 3$, $p \not\equiv 1 \pmod 5$ and $37 < p < 10^6$. It follows from Lemma 2, (7) and (2) that if $p \in S$ and $p \nmid F_2(p_0)$, then $p \nmid N$. (For if $p \mid F_d(p_i)$ and $d \neq 2$ in (7), then either $3 \mid d$ and then $p \equiv 1 \pmod 3$, or $5 \mid d$ and then $p \equiv 1 \pmod 5$; so $p \notin S$.) At most one element of S can divide $F_2(p_0)$. For suppose that $p_i \in S$ and $p_i^{a_i} \parallel N$ and $p_i \mid F_2(p_0)$. Then $p_i^{a_i} \parallel F_2(p_0)$, and if two elements of S were divisors of $F_2(p_0)$ it would follow that $F_2(p_0) = p_0 + 1 \geq 2 \cdot 47^2 \cdot 53^2 > 12 \cdot 10^6$. This is impossible since $p_0 < 10^6$. Note that $p_0 \notin S$ since otherwise $3 \mid F_2(p_0)$, so $3 \mid N$ in contradiction to Lemma 1.

We have proved

Proposition 1. *The number N is divisible by at most one element of S.* (*If there is such an element s, then $s \neq p_0$ and $s \geq 47$.*)

Computer searches showed that S has 29451 elements, and

(8) $S^* = \prod_{p \in S} p/(p-1) > 1.6358.$

Let $T = \{61, 151, 181, \ldots\}$ be the set of all primes p such that $p \equiv 1 \pmod{15}$ and $37 < p < 10^6$. It follows from Lemma 2, (7) and (4) that if $p \in T$ and $p \neq p_0$, then $p \nmid N$. (For if $p_i \in T$ and $p_i^{a_i} \parallel N$ where $i > 0$, then $3 \mid (a_i + 1)$ or $5 \mid (a_i + 1)$, so that $F_3(p_i) \mid N$ and then $3 \mid N$, or $F_5(p_i) \mid N$ and then $5 \mid N$, either of which contradicts Lemma 1.)

We have proved

Proposition 2. *The number N is divisible by at most one element of T.* (*If there is such an element it is p_0, and then $p_0 \geq 61$.*)

Computer searches showed that T has 9806 elements, and

(9) $T^* = \prod_{p \in T} p/(p-1) > 1.1567.$

Now, let $U = \{43, 73, 79, \dots\}$ be the set of all primes p such that $p \equiv 1 \pmod 3$, $p \not\equiv 1 \pmod 5$, $F_5(p)$ has a prime factor which exceeds 10^6, and $37 < p < 10^6$. It follows from Lemma 2, (7) and (4) that if $p \in U$ and $p \neq p_0$, then $p \nmid N$. (For if $p_i \in U$ and $p_i^{a_i} \parallel N$ where $i > 0$, then $3 \mid (a_i + 1)$ and $F_3(p_i) \mid N$ and $3 \mid N$, or $5 \mid (a_i + 1)$ and $F_5(p_i) \mid N$ and N has a prime factor which exceeds 10^6. In either case we have a contradiction.)

We have proved

Proposition 3. *The number N is divisible by at most one element of U.* (*If there is such an element it is p_0, and then $p_0 \geq 73$.*)

Computer searches showed that U has 29115 elements, and

(10) $U^* = \prod_{p \in U} p/(p-1) > 1.4919.$

Finally, let $V = \{1091, 1181, 1811, \dots\}$ be the set of all primes p such that $p \equiv 1 \pmod 5$, $p \not\equiv 1 \pmod 3$, $F_3(p)$ has a prime factor which exceeds 10^6, and $37 < p < 10^6$. If $p \in V$, then $p \neq p_0$, since $3 \mid F_2(p)$, and it follows from Lemma 2, (7) and (4) that $p \nmid N$.

We have proved

Proposition 4. *The number N is not divisible by any element of V.*

Computer searches showed that V has 6719 elements, and

(11) $V^* = \prod_{p \in V} p/(p-1) > 1.0389.$

Note that S, T, U and V are pairwise disjoint.

6. The proof of our theorem

There are 78486 primes p such that $37 < p < 10^6$, and

(12) $P^* = \prod_{41 \leq p < 10^6} p/(p-1) < 3.6597.$

If $p^a \parallel N$, then $1 < \sigma(p^a)/p^a < p/(p-1)$. Since σ is a multiplicative function and $x/(x-1)$ is monotonic decreasing for $x > 1$, it follows from Lemma 1 (using here only that $p \nmid N$ for $p \leq 37$), Propositions 1, 2, 3, 4 and (7), (8), (9), (10), (11), (12) that

$$2 = \frac{\sigma(N)}{N} < \prod_{i=0}^{u} \frac{p_i}{p_i - 1} \leq \frac{47}{46} \frac{61}{60} \frac{P^*}{S^* T^* U^* V^*} < 1.2963.$$

(Note that 47 and 61 appear explicitly due to Propositions 1 and 2.) This contradiction proves our theorem.

7. Some details on the search for acceptable values of $F_r(p)$

As can be seen from Table 1, if $3 \leq p < 10^6$ and $r \geq 7$, only 35 values of $F_r(p)$ are acceptable. (Of course, it follows from (5) that $F_r(p)$ is unacceptable if $r > 500000$.) In establishing this fact it was essential that those $F_r(p)$ be determined which are divisible by at least the second power of a prime. The tables to be found in [6] and [7] were helpful in this regard, but their ranges were much too narrow for most of our searches.

Suppose first that $701 \le r < 500000$ and $10^2 < p < 10^6$. A computer search showed that

(i) if $q < 10^6$, then $q^3 \nmid F_r(p)$ except that $3119^3 \parallel F_{1559}(146917)$;
(ii) there are at most 116 primes q such that $q < 10^6$ and $q \equiv 1 \pmod r$ (and, specifically, there are 116 primes less than 10^6 and congruent to 1 modulo 751), except that there are exactly 122 primes less than 10^6 and congruent to 1 modulo 719 (13 of which, including 1439, are less than 10^5 and 109 of which are between 10^5 and 10^6).

Now suppose that $r \ge 701$, $10^2 < p < 10^6$ and all of the prime factors of $F_r(p)$ are less than 10^6. Then, from (5), $r < 500000$. If $r = 719$, then $F_r(p) > p^{r-1} > (10^2)^{718} = 10^{1436}$; but, from (3), (i) and (ii), $F_{719}(p) < 1439^2((10^5)^2)^{12}((10^6)^2)^{109} < 10^{1435}$. If $r \ne 719$, then $F_r(p) > p^{r-1} > (10^2)^{700} = 10^{1400}$; but, from (3), (i) and (ii), $F_r(p) < ((10^6)^2)^{116} = 10^{1392}$ (where, in particular, $F_{1559}(146917) < 3119^3((10^6)^2)^{56} < 10^{683}$, since there are exactly 57 primes less than 10^6 which are congruent to 1 modulo 1559). These contradictions yield

Proposition 5. *If $r \ge 701$ and $10^2 < p < 10^6$, then $F_r(p)$ has a prime factor which exceeds 10^6.*

Next, suppose that $487 \le r < 701$ and $10^2 < p < 10^6$. A computer search showed that

(iii) if $q < 10^6$, then $q^3 \nmid F_r(p)$ and $q^2 \parallel F_r(p)$ for at most one such q (and a fixed value of p);
(iv) there are at most 163 primes q such that $q < 10^6$ and $q \equiv 1 \pmod r$ (and, specifically, there are 163 primes less than 10^6 and congruent to 1 modulo 499).

Now suppose in addition that all of the prime factors of $F_r(p)$ are less than 10^6. If $r \ge 499$, then $F_r(p) > p^{r-1} > (10^2)^{498} = 10^{996}$; but, from (3), (iii) and (iv), $F_r(p) < (10^6)^2(10^6)^{162} = 10^{984}$. If $r = 487$ or 491 then, since there are exactly 156 primes less than 10^6 and congruent to 1 modulo 487 and exactly 153 primes less than 10^6 and congruent to 1 modulo 491, we see that $F_r(p) > (10^2)^{486} = 10^{972}$ and $F_r(p) < (10^6)^2(10^6)^{155} = 10^{942}$. These contradictions prove

Proposition 6. *If $487 \le r < 701$ and $10^2 < p < 10^6$, then $F_r(p)$ has a prime factor which exceeds 10^6.*

A slightly more complicated argument yields

Proposition 7. *If $7 \le r < 487$ and $10^2 < p < 10^6$, then $F_r(p)$ has a prime factor which exceeds 10^6, except for $r = 7$ and the values of p (exceeding 10^2) listed in Table 1.*

It remains to consider those $F_r(p)$ for which $r \ge 7$ and $p < 10^2$. According to the table in [6], $48947^2 \parallel F_{24473}(17)$, $47^2 \parallel F_{23}(53)$, $59^2 \parallel F_{29}(53)$, $47^2 \parallel F_{23}(71)$ and $4871^2 \parallel F_{487}(83)$; otherwise, if $q^2 \mid F_r(p)$ where $r > 5$ and $p < 10^2$, then $q > 10^6$. In each of the five exceptional cases just mentioned, $F_r(p)$ has a prime factor which exceeds 10^6 and is therefore unacceptable. The study of the remaining cases, in each of which either $F_r(p)$ is divisible by a prime greater than 10^6 or $F_r(p)$ is squarefree, yields the first 15 entries in Table 1 and no other acceptable values of $F_r(p)$. The details of this study are omitted here.

8. Concluding remarks

Let Q be the largest prime factor of the odd perfect number N. We have shown that $Q > 10^6$. A referee has pointed out that our proof could probably be modified so as to improve the lower bound on Q from 10^6 to 10^7. He/she is undoubtedly correct. However, the time and effort to do so seem prohibitive to the present authors at the present time for the following reasons.

Our target of 10^6 in this paper was largely determined by the fact that a list of all 78498 primes up to 10^6 was already available for use in memory in the CYBER 860 at the Temple University Computing Center. Using the procedures of this paper, to show that $Q > 10^7$ would necessitate having in memory a list of all 664579 primes up to 10^7.

Now, let $\pi(x)$ denote the number of primes which do not exceed the real number x. We have $\pi(10^6) = 78498$ and $\pi(5 \cdot 10^5) = 41538$. It follows that, in the construction of Table 1, $78497 \cdot 41535 = 3260372895 = P_1$ values of $F_r(p)$ had to be examined for acceptability (taking $r < 500000$ since otherwise $F_r(p)$ is unacceptable). The searches involved in generating Table 1 of this paper required approximately 450 hours of time on the CYBER 860 and perhaps an additional 250 hours (we did not keep accurate records) of time on a 486 PC. Suppose now that the definition of "acceptability" were changed to: "$F_r(p)$ is acceptable if every prime divisor of $F_r(p)$ is less than 10^7." Since $\pi(10^7) = 664579$ and $\pi(5 \cdot 10^6) = 348513$, if Table 1 were now to be regenerated for $3 \leq p < 10^7$ and $r \geq 7$, then $664578 \cdot 348510 = 231612078780 = P_2$ values of $F_r(p)$ would have to be investigated for acceptability. Each such investigation would require at least as much time as those undertaken in the present paper. Therefore, since $P_2/P_1 > 71$, it seems rather conservative to anticipate spending around 30000 hours of time on the CYBER 860 in the generation of Table 1 if one wished to prove that $Q > 10^7$. This estimate is sufficient to discourage the present authors from making such an attempt.

The same referee has also remarked that the contradictory inequality established in Section 6 is much stronger than is needed and that our theorem could be proved using only the sets S and U. This is true, but we have chosen not to omit the sets T and V from consideration since, as the referee says, "the overkill in the inequality in Section 6 partially substantiates" his/her (and our) feeling that a higher lower bound on Q is achievable by the methods of this paper.

References

1. A. S. Bang, *Taltheoretiske Undersøgelser*, Tidsskrift Math. **5**, **IV** (1886), 70–80, 130–137.
2. M. S. Brandstein, *New lower bound for a factor of an odd perfect number*, Abstracts of the Amer. Math. Soc. **3** (1982), 257.
3. J. T. Condict, *On an Odd Perfect Number's Largest Prime Divisor*, Senior Thesis (Middlebury College), May 1978.
4. P. Hagis, Jr. and W. L. McDaniel, *On the largest prime divisor of an odd perfect number. II*, Math. Comp. **29** (1975), 922–924. MR **51:**8021
5. P. Hagis, Jr. and G. L. Cohen, *Every odd perfect number has a prime factor which exceeds* 10^6 (*with appendix*), Research Report No.93-5 (School of Mathematical Sciences, University of Technology, Sydney), July 1993.
6. W. L. McDaniel, *On multiple prime divisors of cyclotomic polynomials*, Math. Comp. **28** (1974), 847–850. MR **52:**8022
7. P. L. Montgomery, *New solutions of* $a^{p-1} \equiv 1 \pmod{p^2}$, Math. Comp. **61** (1993), 361–363. MR **94d:**11003

8. T. Nagell, *Introduction to Number Theory,* second edition, Chelsea, New York, 1964. MR **30:**4714
9. I. Niven, *Irrational Numbers*, Wiley, New York, 1956. MR **18:**195c

Department of Mathematics, Temple University, Philadelphia, Pennsylvania 19122

School of Mathematical Sciences, University of Technology, Sydney, Broadway, NSW 2007, Australia
E-mail address: g.cohen@maths.uts.edu.au