MATHEMATICS OF COMPUTATION, VOLUME 28, NUMBER 127, JULY 1974, PAGES 847-850

On Multiple Prime Divisors of Cyclotomic Polynomials

By Wayne L. McDaniel

Abstract. Let q be a prime < 150 and F_n be the cyclotomic polynomial of order n. All triples (p, n, q) with p an odd prime $< 10^6$ when $q < 100$ and $p < 10^4$ when $100 < q < 150$ are given for which $F_n(q)$ is divisible by p^t $(t > 1)$.

1. Introduction. The cyclotomic polynomial F_n of order n is defined by

$$F_n(x) = \prod_k (x - e^{2\pi ik/n}), \tag{1}$$

where the index k ranges over the integers relatively prime to n. A basic formula relating $x^n - 1$ to the cyclotomic polynomials [3, Chapter 8] is

$$x^n - 1 = \prod_{d|n} F_d(x). \tag{2}$$

Certain investigations, such as, for example, those concerned with odd perfect numbers and amicable numbers draw upon a knowledge of the prime divisors of $F_n(q)$, for q prime; frequently, a knowledge of whether $F_n(q)$ is free of relatively small factors of multiplicity greater than one is helpful. We present in this paper all triples (p, n, q) with p an odd prime less than L (L defined below), q a prime less than 150 and n any positive integer, for which a power of p greater than the first divides $F_n(q)$.

We have made extensive use of the tables of solutions of $a^{p-1} \equiv 1 \pmod{p^2}$ presented in papers by Brillhart, Tonascia and Weinberger [1], and Riesel [4]. Our search limits for p are those given in these papers; if q is a prime < 150, then $p < L$ for L defined as follows:

$q = 2$	$L = 3 \cdot 10^9$
$q = 3$	$L = 2^{30}$
$q = 5$	$L = 2^{29}$
$q = 7, 11, 13, 29, 49$	$L = 2^{28}$
$q = 17, 19$	$L = 2^{27}$
$q = 23$	$L = 2^{26}$
$q = 61, 73, 89, 97$	$L = 2^{25}$
$q = 31, 37, 41, 43, 53, 59, 67, 71, 79, 83$	$L = 10^6$
$100 < q < 150$	$L = 10^4$

Received August 27, 1973.

AMS (MOS) subject classifications (1970). Primary 10A25; Secondary 10A40.

Key words and phrases. Cyclotomic polynomial, sum of divisors.

2. The Approach. That starting with the available solutions of the congruence $a^{p-1} \equiv 1 \pmod{p^2}$ leads to a most efficient means of finding the multiple odd prime factors of $F_n(a)$, for *any* positive integer n, is based on the following reasoning: It is well known (see [2, pp. 164, 166]) that $F_n(a)$ has as possible divisors the largest prime factor of n (but not its square if $n > 2$) and numbers of the form $1 + kn$. If, now, p^t $(t > 1)$ is an odd prime power divisor of $F_n(a)$, n any positive integer, then $p - 1 = kn$ for some integer k; since, by (2), $F_n(a)$ divides $a^n - 1$, it is clear that p^t divides $a^n - 1$, and, therefore, $a^{p-1} \equiv 1 \pmod{p^t}$. It follows that the only possible odd prime power divisors p^t $(t > 1)$ of $F_n(a)$, for $p < L$ and $a < 150$, are those primes p listed in the tables of [1] and [4].

We have restricted our investigation to $F_n(a)$ for a a *prime* largely because interest in the multiplicity of divisors of cyclotomic polynomials frequently occurs in connection with their appearance as factors of the sum-of-divisors function σ. Since σ is a multiplicative function and, for q prime,

$$\sigma(q^{n-1}) = (q^n - 1)/(q - 1) = \prod_{d|n} F_d(q), \quad d \neq 1, \tag{3}$$

it is sufficient to confine one's attention to $F_n(a)$ for a a prime.

Our calculation, carried out on the University of Missouri's IBM 360, was shortened through application of the following extension of Theorem 4 in [1]:

THEOREM. *Let a, r and m be positive integers with $(m, \varphi(m)) = 1$. If a belongs to $e \pmod{m}$ and $a^{\varphi(m)} \equiv 1 \pmod{m^r}$, then a belongs to $e \pmod{m^r}$.*

Proof. The proof is by mathematical induction on r. The theorem is trivially true when $r = 1$. If the theorem is assumed to be true for $r = t$, then $a^e = 1 + km^t$ for some positive integer k. Now, when $r = t + 1$,

$$\begin{aligned} 1 \equiv a^{\varphi(m)} &\equiv (a^e)^{\varphi(m)/e} = (1 + km^t)^{\varphi(m)/e} \\ &\equiv 1 + km^t\varphi(m)/e \pmod{m^{t+1}}, \end{aligned}$$

from which it follows that $m|k$. Hence, $a^e \equiv 1 \pmod{m^{t+1}}$. No smaller power of a is congruent to $1 \pmod{m^{t+1}}$, since a belongs to $e \pmod{m}$.

We immediately have this

COROLLARY. *If, for some odd prime p and positive integers a and r, a belongs to the exponent $e \pmod{p}$ and $a^{p-1} \equiv 1 \pmod{p^r}$, then $p^r | F_e(a)$.*

Proof. Since, by the Theorem, p^r divides $a^e - 1$, $p | F_d(a)$ for some divisor d of e, by (2). But then, $p | a^d - 1$, so $d = e$. Since $d = e$ is the only divisor of e for which $p | F_d(a)$, p^r divides $F_e(a)$.

The obvious implication of the Corollary, with respect to the problem of finding p, n and q $(p < L, q < 150)$ such that $p^t | F_n(q)$, is that, for each pair p and q such that $q^{p-1} \equiv 1 \pmod{p^t}$ $(t = 2$ or $3)$ in the tables of [1] and [4], one need only find the smallest factor n of $p - 1$ for which $p | q^n - 1$. It follows that p^t divides $F_n(q)$.

Our procedure, then, was straightforward; the exponent to which q belongs $\pmod{p}$ was found in the usual way. Only four values of $F_n(q)$ are divisible by p^3 for $p < L$, $q < 150$, and these are marked with an asterisk in the table. No $F_n(q)$ is divisible by the fourth power of an odd prime for p and q in our ranges.

We are indebted to the referee for pointing out that the entry $a = 23$, $p = 1370377$ in Table I of [1] should have been $a = 23$, $p = 13703077$. Subsequently, we checked all values of a and p listed in the tables of both [1] and [4], and the triples in our own table, and found all entries to be correct with the one exception noted above.

All primes p *and* q, $2 < p < L$, $q < 150$,
and integers n *for which* $p^2 \mid F_n(q)$.

p	n	q	p	n	q
1093	$2^2 \cdot 7 \cdot 13$	2	*3	2	53
3511	$3^3 \cdot 5 \cdot 13$	2	47	23	53
11	5	3	59	29	53
1006003	$2 \cdot 3^2 \cdot 55889$	3	97	$2^4 \cdot 3$	53
20771	$5 \cdot 31 \cdot 67$	5	2777	$2^2 \cdot 347$	59
40487	$2 \cdot 31 \cdot 653$	5	7	3	67
53471161	$2 \cdot 3^2 \cdot 5 \cdot 148531$	5	47	$2 \cdot 23$	67
5	2^2	7	268573	$2 \cdot 3 \cdot 22381$	67
491531	$5 \cdot 13 \cdot 19 \cdot 199$	7	3	2	71
71	$2 \cdot 5 \cdot 7$	11	47	23	71
863	$2 \cdot 431$	13	331	$3 \cdot 5 \cdot 11$	71
1747591	$3 \cdot 5 \cdot 13 \cdot 4481$	13	3	1	73
3	2	17	7	3	79
46021	$2 \cdot 5 \cdot 13 \cdot 59$	17	263	$2 \cdot 131$	79
48947	24473	17	3037	$2^2 \cdot 3 \cdot 11 \cdot 23$	79
3	1	19	4871	487	83
*7	$2 \cdot 3$	19	13691	$5 \cdot 37^2$	83
13	$2^2 \cdot 3$	19	3	2	89
43	$2 \cdot 3 \cdot 7$	19	13	$2^2 \cdot 3$	89
137	$2^2 \cdot 17$	19	7	2	97
63061489	$2^4 \cdot 3^2 \cdot 7 \cdot 73 \cdot 857$	19	5	1	101
13	$2 \cdot 3$	23	*3	2	107
2481757	$2^2 \cdot 206813$	23	5	2^2	107
13703077	$2^2 \cdot 3^2 \cdot 380641$	23	97	$2^5 \cdot 3$	107
7	$2 \cdot 3$	31	*3	1	109
79	$3 \cdot 13$	31	3	1	127
6451	$3 \cdot 5^2 \cdot 43$	31	19	$2 \cdot 3^2$	127
3	1	37	907	$2 \cdot 3 \cdot 151$	127
77867	$2 \cdot 38933$	37	17	2^4	131
29	2^2	41	29	$2^2 \cdot 7$	137
1025273	$2^3 \cdot 128159$	41	59	29	137
5	2^2	43	6733	$2^2 \cdot 3 \cdot 11 \cdot 17$	137
103	$2 \cdot 3 \cdot 17$	43	5	2	149

We remark that one can readily infer that if q is a prime < 150 and n is any positive integer > 1, then $\sigma(q^{n-1})$ is square-free of prime divisors $p < L$, $p \nmid n$, except in those cases where p, n and q are listed in our table. This is a consequence of (3) and a theorem due to Sylvester [5] which states, essentially, that if $F_r(a)$ and $F_s(a)$ are distinct divisors of $(a^n - 1)/(a - 1)$, then, except for divisors of r and s, $F_r(a)$ and $F_s(a)$ are relatively prime.

Department of Mathematics
University of Missouri-St. Louis
St. Louis, Missouri 63121

1. J. BRILLHART, J. TONASCIA & P. WEINBERGER, "On the Fermat quotient," *Proceedings of the 1969 Atlas Symposium on Computers in Number Theory* (Oxford, 1969), pp. 213-222.

2. T. NAGELL, *Introduction to Number Theory*, Wiley, New York, 1951. MR **13**, 207.

3. H. RADEMACHER, *Lectures on Elementary Number Theory*, Blaisdell, Waltham, Mass., 1964. MR **30** #1079.

4. H. RIESEL, "Note on the congruence $a^{p-1} \equiv 1 \pmod{p^2}$," *Math. Comp.*, v. 18, 1964, pp. 149-150. MR **28** #1156.

5. J. J. SYLVESTER, "On the divisors of the sum of a geometrical series whose first term is unity and common ratio any positive or negative number," *Nature*, v. 37, 1888, pp. 417-418; *Collected Mathematical Papers*, v. 4, 1912, pp. 625-629.