MATHEMATICS OF COMPUTATION, VOLUME 32, NUMBER 141
JANUARY 1978, PAGES 297–301

On the p-Divisibility of the Fermat Quotients

By Wells Johnson*

Abstract. Upper bounds for the power of p which divides the Fermat quotient $q_a = (a^{p-1} - 1)/p$ are obtained, and conditions are given which imply that $q_a \not\equiv 0 \pmod{p}$. The results are in terms of the number of steps in a simple algorithm which determines the semiorder of $a \pmod{p}$.

1. Introduction. If p is an odd prime and $p \nmid a$, the Fermat quotient is defined by $q_a = q_a(p) = (a^{p-1} - 1)/p$. It is known that if the Fermat equation $x^p + y^p = z^p$ has a solution in the first case (with $p \nmid xyz$), then $q_a \equiv 0 \pmod{p}$ for $2 \leqslant a \leqslant 31$. In an earlier paper [2], we gave certain conditions on p and a which ensure that $q_a \not\equiv 0 \pmod{p}$. In view of the importance of this for the first case of Fermat's Last Theorem it seems desirable to continue the study.

In this paper we present an elementary algorithm and derive from it an upper bound for the power of p which divides q_a. The algorithm is generally much less efficient than the squaring algorithm normally used to determine computationally whether $q_a \equiv 0 \pmod{p}$. For a discussion and summary of the extensive computational results already known on this question, see Brillhart et al. [1]. We have not used the present algorithm to obtain additional computational results, but rather, we show how it can lead to some interesting theoretical consequences, particularly in cases where a and the order of $a \pmod{p}$ are relatively small. The algorithm does have the advantage that in order to determine whether $q_a \equiv 0 \pmod{p}$, it is only necessary to do the computations $\pmod{p}$.

For simplicity, we restrict our attention to cases where $1 < a < p$. For more general cases, we can use the congruence $q_{a+p} \equiv q_a - a^{-1} \pmod{p}$. For any integer $n \geqslant 2$, we let $e_p(n)$ denote the exponent of p in the prime factorization of n. If $p \nmid a$, we define the *semiorder* of $a \pmod{p}$ to be the smallest positive integer d such that $a^d \equiv \pm 1 \pmod{p}$, and we denote it by $\operatorname{sord}_p a$. We always have that $\operatorname{sord}_p a \leqslant (p-1)/2$, and that $\operatorname{sord}_p a$ is equal to either the order of $a \pmod{p}$ or one-half the order of $a \pmod{p}$, depending upon the parity of the latter. In any case, $\operatorname{sord}_a p$ divides $p - 1$. As usual, we denote the greatest integer function with square brackets.

2. The Algorithm. We begin with an odd prime p and an integer a, $1 < a < p$. Since $q_{p-1} \equiv 1 \pmod{p}$ (in fact $\pmod{p^2}$), it is no loss of generality to assume that $a < p - 1$. We define four sequences $\{a_n\}$, $\{e_n\}$, $\{b_n\}$, and $\{Q_n\}$ inductively as follows:

Received April 1, 1977.
AMS (MOS) subject classifications (1970). Primary 10A10; Secondary 10A30, 10B15.
Key words and phrases. Fermat quotients, Fermat's Last Theorem, Wieferich's criterion.
*Supported by a grant from the Vaughn Foundation Fund.

$a_0 = 1$,
e_n is the unique exponent satisfying $a^{e_n - 1} a_n < p - 1 \leqslant a^{e_n} a_n$, $n \geqslant 0$,
$b_n = [a^{e_n} a_n / p]$, $n \geqslant 0$,
$a_{n+1} = a^{e_n} a_n - b_n p$, $n \geqslant 0$,
$Q_0 = b_0$, $Q_n = a^{e_n} Q_{n-1} + b_n$, $n \geqslant 1$.

Clearly, $e_n \geqslant 1$ for all $n \geqslant 0$. We halt the algorithm at step k if either $a^{e_k} a_k = p - 1$ or if $a_{k+1} = 1$. We are simply looking at the least positive residues of successive powers of a (mod p), and stopping when this power is equal to $\operatorname{sord}_p a$. The sequence $\{a_n\}$ gives the least positive residues of $a^{e_0 + e_1 + \cdots + e_n}$, and we have that

$$e_0 + e_1 + \cdots + e_k = \operatorname{sord}_p a.$$

In the case that $a^{e_k} a_k = p - 1$, we define $b_k = 1$ (and Q_k accordingly), so that at the last step we always have $a^{e_k} a_k = \pm 1 + b_k p$. We call k the *number of reductions* of a (mod p).

The final expression for Q_k is

$$Q_k = \sum_{i=0}^{k-1} a^{e_{i+1} + \cdots + e_k} b_i + b_k.$$

Starting with the equation $a^{e_k} a_k = \pm 1 + b_k p$, and unravelling the algorithm by substituting for $a_k, a_{k-1}, \ldots, a_1$ successively, we see that

$$a^{e_0 + e_1 + \cdots + e_k} = a^{\operatorname{sord}_p a} = \pm 1 + p Q_k.$$

Since $e_n \geqslant 1$ and the definition of e_n implies that $b_n < a$, it follows that Q_k is nothing more than the a-adic expansion of the quotient $(a^{\operatorname{sord}_p a} \mp 1)/p$.

THEOREM. $e_p(q_a) = e_p(Q_k)$.

Proof. If $s = \operatorname{sord}_p a$, then $a^s = \pm 1 + p Q_k$. If $d = (p-1)/s$, then d is even and $a^{p-1} = (\pm 1 + p Q_k)^d = 1 \pm d p Q_k + \binom{d}{2} p^2 Q_k^2 \pm \cdots$, implying that $q_a = Q_k(\pm d + \binom{d}{2} p Q_k \pm \cdots)$. Since $p \nmid d$, the last term is relatively prime to p and the result follows.

We note in passing that the actual value of q_a (mod p) or (mod p^n) can be determined by the algorithm if that is desired.

To illustrate the algorithm and the Theorem, take $p = 11$, $a = 3$. In this example, $k = 2$ and the algorithm reads

$$3^3 = 5 + 2p, \qquad Q_0 = 2,$$
$$3 \cdot 5 = 4 + p, \qquad Q_1 = 1 + 3 \cdot 2 = 7,$$
$$3 \cdot 4 = 1 + p, \qquad Q_2 = 1 + 3 \cdot 7 = 2p.$$

In this case $\operatorname{sord}_{11} 3 = 3 + 1 + 1 = 5$, and $3^5 = 243 = 1 + 2p^2$. Hence $3^{10} = (1 + 2p^2)^2$, so that $q_3 = 4p(1 + p^2)$. We thus have $e_p(q_3) = e_p(Q_2) = 1$.

If $k = 0$, then $Q_k = b_0 < a < p$, so that the Theorem implies that $q_a \not\equiv 0$ (mod p), and this is established with a minimum amount of computation. This is the case when $a = 2$ and p is a Fermat or Mersenne prime, giving a result of Mirimanoff [4] and Perisastri [5]. Additional examples for which $k = 0$ include $p = 313$, $a = 5$; $p = 37$,

$a = 6$; $p = 101$, $a = 10$; and $p = 1093$, $a = 3$. Thus we easily establish that $q_3 \not\equiv 0 \pmod{1093}$, a fact which is not without significance for the first case of Fermat's Last Theorem, since $p = 1093$ is one of the rare primes for which $q_2 \equiv 0 \pmod{p}$.

3. Upper Bounds for $e_p(q_a)$. The Theorem enables us to obtain upper bounds on $e_p(q_a)$ in terms of k.

COROLLARY 1. *Let p be a prime and suppose $1 < a < p - 1$. If k represents the number of reductions of $a \pmod{p}$ and $N_k = [(k+1)/[\log_a p]]$, then*

$$e_p(q_a) \leqslant \operatorname{Min}\{2k,\ k + N_k\}.$$

In the case that $k \geqslant 1$ and $b_0 = b_1 = \cdots = b_k$,

$$e_p(q_a) \leqslant \operatorname{Min}\{2k - 1,\ k + N_k\}.$$

Proof. For $1 \leqslant j \leqslant k$, $a^{e_j - 1} \leqslant a^{e_j - 1} a_j < p$, so that $a^{e_j} < ap$. Since $b_j < a$ for $1 \leqslant j \leqslant k$, it follows that

$$Q_k < a^{e_1 + e_2 + \cdots + e_k + 1} < a^{k+1} p^k < p^{2k+1}.$$

Hence by the Theorem, $e_p(q_a) = e_p(Q_k) \leqslant 2k$.

The bound $k + N_k$ is an improvement over the bound $2k$ if $k > 1$ and $a^2 < p$, or if $k = 1$ and $a^3 < p$. For $k \geqslant 1$, $a^{e_0 - 1} < p < a^{e_0}$, so that $e_0 - 1 = [\log_a p]$. By the definition of N_k, we have that $a^{k+1} < p^{N_k + 1}$, so that $Q_k < p^{k + N_k + 1}$ and $e_p(q_a) = e_p(Q_k) \leqslant k + N_k$.

If $b_0 = b_1 = \cdots = b_k = b$, then $Q_k = b(1 + \Sigma_{i=0}^{k-1} a^{e_{i+1} + \cdots + e_k})$. Since $b < a$, we have that $p \nmid b$ and hence $e_p(q_a) = e_p(Q_k/b)$. But

$$Q_k/b \leqslant (a^{e_1 + \cdots + e_k + 1} - 1)/(a - 1) < (a^{k+1} p^k - 1)/(a - 1).$$

Hence, to establish the bound $e_p(q_a) \leqslant 2k - 1$, it suffices to show that, for $k \geqslant 1$,

$$a^{k+1} p^k < p^{2k}(a - 1) \quad \text{or} \quad a^{k+1} < p^k(a - 1).$$

Since $a < p$, it is enough to consider the case $k = 1$ and prove that $a^2 < p(a - 1)$ for $1 < a < p - 1$. For fixed p, we see that the function $f(a) = a^2 - pa + p$ is a parabola whose minimum occurs at $a = p/2$. Since we may exclude the case $p = 3$, we have that $f(2) = f(p - 2) = 4 - p < 0$, so that $f(a) < 0$ for $2 \leqslant a \leqslant p - 2$, as desired.

If $a = 2$, then we always have the added restriction that $b_0 = b_1 = \cdots = b_k = 1$. In this case, however, stronger bounds for $e_p(q_2)$ can be obtained as follows.

COROLLARY 2. *Let p be a prime and let k denote the number of reductions of $2 \pmod{p}$. Then*

$$e_p(q_2) \leqslant k - 1 \quad \textit{for } k \geqslant 3, \textit{ and}$$

$$e_p(q_2) = 0 \qquad \textit{for } 0 \leqslant k \leqslant 2.$$

Proof. For $k \geqslant 1$ and $0 \leqslant j \leqslant k$, we have that $2^{e_j} a_j = a_{j+1} + p \leqslant 2p - 1 < 2^{e_0 + 1}$, so that $2^{e_j} < 2^{e_0 + 1}/a_j$. Hence,

$$Q_k < 2^{e_1 + \cdots + e_k + 1} < 2^{k(e_0 + 1) + 1}/a_1 a_2 \cdots a_k.$$

But none of the distinct, odd, positive integers $a_1, \ldots, a_k$ can be 1. Thus,

$$Q_k < 2^{2k+1}p^k/3 \cdot 5 \cdot 7 \cdots (2k+1).$$

For $k \geqslant 4$, $Q_k < p^k$ so that $e_p(q_2) = e_p(Q_k) \leqslant k-1$, as desired. If $k = 3$ and $a_1 \geqslant 9$, then $Q_k < p^k$ also. Hence, we may assume that $k = 3$ and $a_1 \leqslant 7$, in which case $2^{e_0} \leqslant p + 7$, so that $2^{e_0-1} \leqslant (p+7)/2$. Hence,

$$Q_3 < 2^7((p+7)/2)^3/3 \cdot 5 \cdot 7 < p^3 \quad \text{for } p \geqslant 11.$$

For $p < 11$, k is never 3.

If $k = 0$, then $e_p(q_2) = 0$ by Corollary 1. If $k = 1$, then $Q_k = 1 + 2^{e_1}$. Since $2^{e_1} < 2^{e_0+1}/a_1 \leqslant 2^{e_0+1}/3 < 2^{e_0}$, we have that $e_1 \leqslant e_0 - 1$. Hence,

$$Q_k = 1 + 2^{e_1} \leqslant 1 + 2^{e_0-1} < p,$$

so that $e_p(q_2) = e_p(Q_k) = 0$.

Finally, suppose $k = 2$, so that $Q_k = 1 + 2^{e_2} + 2^{e_1+e_2}$. Then if $p \mid q_2$, we have by the Theorem that $2^{e_2}(1 + 2^{e_1}) \equiv -1 \pmod{p}$. But $2^{e_2}a_2 \equiv \pm 1 \pmod{p}$, so that $(1 + 2^{e_1}) \equiv \mp a_2 \pmod{p}$. As above, $1 + 2^{e_1} < p$ and hence $1 + 2^{e_1} = a_2$ or $p - a_2$. Since $e_1 \geqslant 1$ and a_2 is odd, the latter choice cannot hold. The algorithm gives $2^{e_0} = a_1 + p$ and $2^{e_1}a_1 = a_2 + p$. Combining these with $1 + 2^{e_1} = a_2$, we have $2^{e_0+e_1} = a_2(p+1)$, and hence a_2 must be a power of 2, a contradiction.

Thus $q_2 \not\equiv 0 \pmod{p}$ for primes p of the form $(2^r \pm 1)/D$ where $D = 1$ $(k = 0)$, $D = 1 + 2^s$ $(k = 1)$, or $D = 1 + 2^s + 2^{s+t}$ $(k = 2)$. By the Wieferich criterion, this establishes the first case of Fermat's Last Theorem for such primes. The cases $k = 0, 1$ are included in the results of [2]. The case $k = 0$ corresponds to the Mersenne and Fermat primes. We have $k = 1$ for $p = 11, 13, 43, 241, 683, 2731, 43691, 61681$ and 174763, and $k = 2$ for $p = 41, 73$, and 113.

The example $p = 11$, $a = 3$ provides an instance where $k = 2$ and $q_a \equiv 0 \pmod{p}$. The final result of Corollary 2 and its proof can be generalized to the case of arbitrary a, however, under certain restrictions.

COROLLARY 3. *Let p be a prime and suppose $1 < a < p - 1$. Let k denote the number of reductions of $a \pmod{p}$. Then $q_a \not\equiv 0 \pmod{p}$ under any one of the following conditions*:

(a) $k = 0$,

(b) $k = 1$ *and* $b_0 = b_1$,

(c) $k = 2$, $b_0 = b_1 = b_2$, *and* $a \nmid p - 2$.

Proof. (a) if $k = 0$, the result follows from Corollary 1. Directly, we have that $Q_k = b_0 < a < p$, so that $p \nmid Q_k$ and hence $p \nmid q_a$ by the Theorem.

(b) If $k = 1$ and $b_0 = b_1 = b$, then $Q_k = b(1 + a^{e_1})$. Since $p \nmid b$, it suffices to prove that $p \nmid (1 + a^{e_1})$. We have that $a^{e_1-1}a_1 < p - 1 < a^{e_0}$, so that $e_1 \leqslant e_0$. If $e_1 < e_0$, then $a^{e_1} \leqslant a^{e_0-1} < p - 1$ so that $1 + a^{e_1} < p$, which is sufficient. Hence it remains to exclude the case $e_1 = e_0$. Since $k = 1$, $e_1 = e_0$ implies that $a^{2e_0} \equiv \pm 1 \pmod{p}$ and $\operatorname{sord}_p a = 2e_0$. If the top sign holds, then $a^{e_0} \equiv \pm 1 \pmod{p}$, contradicting the definition of $\operatorname{sord}_p a$. Hence $a^{2e_0} \equiv -1 \pmod{p}$, and $a^{2e_0} + 1 = pb(a^{e_0} + 1)$.

But then $a^{e_0} + 1 \mid a^{2e_0} \pm 1$, so that $a^{e_0} + 1 \mid 2$, a contradiction.

(c) If $k = 2$ and $b_0 = b_1 = b_2 = b$, then $Q_k = b(1 + a^{e_2} + a^{e_1+e_2})$. If $q_a \equiv 0 \pmod{p}$, then, by the Theorem,

$$a^{e_2}(1 + a^{e_1}) \equiv -1 \pmod{p}.$$

Since $a^{e_2}a_2 \equiv \pm 1 \pmod{p}$, it follows that $(1 + a^{e_1}) \equiv \mp a_2 \pmod{p}$. As in the proof of (b), we have that $e_1 \leqslant e_0$. If $e_1 = e_0$, the first two steps of the algorithm imply that

$$a^{2e_0} = a_2 + bp(a^{e_0} + 1).$$

Since $a^{e_0} + 1 \mid a^{2e_0} - 1$, it follows that $a^{e_0} + 1 \mid a_2 - 1$. But $a_2 < p < 1 + a^{e_0}$, so that $a_2 = 1$. But this means that $k = 1$, a contradiction.

Thus $e_1 < e_0$ and hence $1 + a^{e_1} < p$. We thus have that $1 + a^{e_1} = a_2$ or $p - a_2$. If $1 + a^{e_1} = a_2$, then the first two steps of the algorithm give that $a_2 \mid a^{e_0+e_1}$. But a and $a_2 = 1 + a^{e_1} > 1$ are relatively prime, which gives a contradiction. If $1 + a^{e_1} = p - a_2$, $a_2 \equiv p - 1 \pmod{a}$. The three steps of the algorithm show that $a_1 \equiv a_2 \equiv 1 \pmod{a}$, so that $p \equiv 2 \pmod{a}$, concluding the proof.

We have already given examples for (a) with $a > 2$ at the end of the previous section. The examples $a = 3$ and $p = 61$ and $p = 73$ illustrate (b).

We can also prove an old theorem originally due to Meissner [3] using these techniques.

COROLLARY 4 (MEISSNER). *If p is a prime, $1 < a < p$, and the order of a* (mod p) *is* 2, 3, 4, *or* 6, *then* $q_a \not\equiv 0 \pmod{p}$.

Proof. The hypothesis implies that $\operatorname{sord}_p a \leqslant 3$. Since $e_0 \geqslant 2$ and $e_0 + e_1 + \cdots + e_k \leqslant 3$, we must have that $k = 0$ or $k = 1$. If $k = 0$, use Corollary 1. In the remaining case, we have $k = 1$, $e_0 = 2$, $e_1 = 1$, so that

$$Q_k = ab_0 + b_1 = (a \mp 1)b_0 \pm b_0 + b_1.$$

Since $a^3 = \pm 1 + pQ_k$, we have that $(a \mp 1) \mid (\pm b_0 + b_1)$. If the bottom signs hold, then since $1 \leqslant b_0, b_1 < a$, we must have that $b_0 = b_1$, and we can apply Corollary 3. Otherwise, $a - 1 \mid b_0 + b_1$ and $Q_k = (a - 1)(b_0 + u)$, where $1 \leqslant u \leqslant 2$ since $b_0 + b_1 < 2a$. But $p \nmid a - 1$ and $b_0 + u < a + 2 \leqslant p$ implies that $p \nmid Q_k$, so that $p \nmid q_a$, by the Theorem.

Department of Mathematics
Bowdoin College
Brunswick, Maine 04011

1. J. BRILLHART, J. TONASCIA & P. WEINBERGER, "On the Fermat quotient," *Computers in Number Theory* (A. O. L. Atkin & B. J. Birch, Editors), Academic Press, New York, 1971, pp. 213–222. MR 47 #3288.

2. W. JOHNSON, "On the nonvanishing of Fermat quotients (mod p)," *J. Reine Angew. Math.*, v. 292, 1977, pp. 196–200.

3. W. MEISSNER, "Uber die Lösungen der Kongruenz $x^{p-1} \equiv 1 \bmod p^m$ und ihre Verwertung zur Periodenbestimmung mod p^x," *Sitzungsber. Berlin Math. Gesell.*, v. 13, 1914, pp. 96–107.

4. D. MIRIMANOFF, *Comptes Rendus Paris*, v. 150, 1910, pp. 204–206.

5. M. PERISASTRI, "On Fermat's Last Theorem. II," *J. Reine Angew. Math.*, v. 265, 1974, pp. 142–144. MR 49 #2531.