MATHEMATICS OF COMPUTATION
Volume 66, Number 219, July 1997, Pages 1353–1365
S 0025-5718(97)00843-0

ON THE p-DIVISIBILITY OF FERMAT QUOTIENTS

R. ERNVALL AND T. METSÄNKYLÄ

ABSTRACT. The authors carried out a numerical search for Fermat quotients $Q_a = (a^{p-1} - 1)/p$ vanishing mod p, for $1 \leq a \leq p-1$, up to $p < 10^6$. This article reports on the results and surveys the associated theoretical properties of Q_a. The approach of fixing the prime p rather than the base a leads to some aspects of the theory apparently not published before.

1. INTRODUCTION

For a fixed odd prime p and for $a \in \mathbb{Z} \setminus p\mathbb{Z}$, the integer

$$Q_a = \frac{a^{p-1} - 1}{p} \tag{1}$$

is called the *Fermat quotient* of a (or with *base* a). This quotient has been extensively studied because of its links to numerous questions in number theory. To mention just one such link underlying several important problems, let ω_a, for $1 \leq a \leq p-1$, denote the p-adic integer which is the $(p-1)$st root of 1 congruent to a mod p. Then, for any $m \geq 1$, one has $\omega_a \equiv a \pmod{p^{m+1}}$ if and only if $Q_a \equiv 0 \pmod{p^m}$ (see §7).

This article reports on our computations of Q_a and reviews the current state of knowledge of the associated properties of this number. The main part of the computations consisted of a systematic search, up to $p < 10^6$, for all integers a in the range $1, \ldots, p-1$ satisfying $Q_a \equiv 0 \pmod{p}$. The results on the whole seem to support the expected behavior of Q_a. On the other hand, several interesting details appear.

The article [3] by Brillhart, Tonascia and Weinberger reports thoroughly on the computations of Q_a, particularly its vanishing mod p, until the end of the sixties. Later computational developments will be briefly summed up below in §8. In all this previous work, Q_a is considered from the point of view of a fixed base a, whereas we have adapted the approach of keeping p fixed.

Theoretical results about Q_a are scattered throughout the literature, many of them appearing in the work concerning Fermat's equation. A first comprehensive study of Q_a was published in 1905 by Lerch [20]. A chronological summary of results prior to 1918 can be found in Dickson's history [6, Part I, Chapter IV] (see also Part II, Chapter XXVI). Many later results are surveyed in Ribenboim's book

Received by the editor March 4, 1996 and, in revised form, May 22, 1996.
1991 *Mathematics Subject Classification.* Primary 11A15, 11Y70; Secondary 11D41, 11R18.
Key words and phrases. Fermat quotients, computation, Fermat's equation, Catalan's equation, cyclotomic fields.

[24]. Granville [10, 11], besides proving new results, provides a review of known facts and open problems.

Our discussion contains a simple result about the vanishing mod p, and more generally mod p^m, of Q_a and Q_{a+1} (§5, §7). There are also some other aspects and observations which may be known but to our knowledge have not been published in this form.

In modern literature, Q_a is usually denoted by q_a. Since we are mostly concerned not with Q_a but with its residue modulo p, we prefer to introduce the notation q_a for the number defined by

$$q_a \equiv Q_a \pmod{p}, \qquad 0 \le q_a < p.$$

2. The Fermat quotient matrix

Since $q_a = q_{p^2 \pm a}$, full information about q_a can be obtained by letting a run through a half-system of reduced residue classes mod p^2, say in the interval $0 < a < p^2/2$. The two tables below show q_a in this range for $p = 11$ and $p = 13$ (in each row a runs through $p-1$ consecutive integers).

0	5	0	10	7	5	2	4	0	1
10	10	7	7	9	3	5	8	6	2
9	4	3	4	0	1	8	1	1	3
8	9	10	1	2	10	0	5	7	4
7	3	6	9	4	8	3	9	2	5
6	8	2	6	6					

0	3	8	6	1	11	9	9	3	4	10	1
12	9	12	9	6	0	7	4	0	0	4	2
11	2	3	12	11	2	5	12	10	9	11	3
10	8	7	2	3	4	3	7	7	5	5	4
9	1	11	5	8	6	1	2	4	1	12	5
8	7	2	8	0	8	12	10	1	10	6	6
7	0	6	11	5	10						

Often it is more illuminating, however, to look at q_a for the whole system $\{a \in \mathbb{Z} \setminus p\mathbb{Z} \mid 0 < a < p^2\}$, and we invite the reader to complete the above tables, simply by reflection, into the $p \times (p-1)$ matrices corresponding to this system. Let us denote this matrix by M_p and call it the *Fermat quotient matrix*.

From (1) it follows that

$$q_{a+kp} \equiv q_a - ka^{-1} \pmod{p} \tag{2}$$

for any $k \in \mathbb{Z}$, where a^{-1} denotes the inverse of a mod p. This gives the elements of each column of the matrix M_p as a function of any single element in that column. The column is a permutation of $0, \dots, p-1$ and it can be easily written down, without calculating a^{-1}, once one element is known.

Another basic property of q_a, an immediate consequence of (1), is the "logarithmic rule"

$$q_{ab} \equiv q_a + q_b \pmod{p}. \tag{3}$$

This together with (2) makes it possible to compile M_p, or its first row, with a minimal (if any) use of the computationally impractical formula (1). We will discuss this question in §8.

The integers $a \in \mathbb{Z} \setminus p\mathbb{Z}$ modulo p^2 may be uniquely represented in the form

$$a \equiv r^u (1+p)^v \pmod{p^2}, \qquad u \bmod p-1, \quad v \bmod p, \tag{4}$$

where r is a fixed primitive root of p such that $q_r = 0$. In fact, r and $1+p \bmod p^2$ generate the cyclic subgroups of order $p-1$ and p, respectively, of $G = (\mathbb{Z}/p^2\mathbb{Z})^\times$ (see [12, Part I, Chapter 4]. For any a satisfying (4),

$$q_a \equiv uq_r + vq_{1+p} \equiv -v \pmod{p}.$$

This shows, once again, that every number $0, \dots, p-1$ occurs $p-1$ times in M_p. Note that all the residue classes $a \bmod p^2$ with $q_a = 0$ constitute the subgroup of order $p-1$ in G, while those with $q_a = t$, for each $t \in \{1, \dots, p-1\}$, form a coset of this subgroup.

The following proposition and its proof show that q_a can be characterized, up to a constant factor, by (3) and the periodicity modulo p^2.

Proposition 1. *If the function $\mathbb{Z} \setminus p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, $a \mapsto x_a$ satisfies the conditions*

$$x_a = x_{a+p^2}, \qquad x_{ab} = x_a + x_b, \qquad x_{1+p} = -1 + p\mathbb{Z},$$

then $x_a = q_a + p\mathbb{Z}$.

Proof. Firstly, $x_1 = 0$. Consider $a \bmod p^2$ in the form (4). Since $r^{p-1} \equiv 1 \pmod{p^2}$, we have $-x_r = x_1 = 0$ and, moreover,

$$x_a = v x_{1+p} = -v + p\mathbb{Z} = q_a + p\mathbb{Z}. \quad \square$$

3. First row of the matrix

Problems related to q_a most typically concern the zeros in the first row of the matrix M_p, that is, for $a \in I_p = \{1, \dots, p-1\}$. More generally, it is natural to ask about the distribution of the values of q_a for $a \in I_p$.

The equal elements in the first row of M_p carry information about all the zeros in M_p in the following sense. Let $a, b \in I_p$ with

$$q_a = q_b, \qquad (a, b) = 1; \tag{5}$$

note that the last condition is no actual restriction. Then, for any integer $k \equiv \frac{a}{b} \pmod{p^2}$, we have $q_k = 0$ and $q_{-k} = 0$. Conversely, for any integer k prime to p with $q_k = 0$ there exist $a, b \in I_p$ satisfying (5) such that

$$k \equiv \frac{a}{b} \quad \text{or} \quad k \equiv -\frac{a}{b} \pmod{p^2}. \tag{6}$$

This was observed by Vandiver [31]. A nice proof can be obtained from Minkowski's theorem on linear forms (consider the forms $p^2x + ky$ and y).

As a first consequence it follows (see [31]) that the number of different elements in the first row of M_p is at most $\left[p - \sqrt{(p-1)/2}\right]$ and at least $[\sqrt{p}]$, where the brackets denote the greatest integer function.

For a given k prime to p, the pair of coprime integers $a, b \in I_p$ satisfying $k \equiv \frac{a}{b} \pmod{p^2}$ is necessarily unique. To see this, simply note that a congruence mod p^2 between two positive integers less than p^2 must be an equality.

It follows that, given k, there are at most two pairs $a, b \in I_p$, with $(a, b) = 1$, such that (6) is true. As remarked by Coppersmith [4], there is only one such pair if one adds the condition $a^2 + b^2 < p^2$. We point out that this is an immediate consequence of Lagrange's identity

$$(ab' + a'b)^2 = (a^2 + b^2)(a'^2 + b'^2) - (aa' - bb')^2.$$

Since the total number of zeros in M_p equals $p-1$, one concludes from the last mentioned results the following: the number of primes $l \in I_p$ with a constant value of q_l is less than $\sqrt{p}$, and in the range $1 < l \le [p/\sqrt{2}]$ this number is even less than $\sqrt{p/2}$.

Leaving out the assumption about the primality of l we have

$$\operatorname{card}\{a \in I_p \mid q_a = t\} \ll p^{\frac{1}{2}+\frac{1}{\log\log p}} \qquad (t = 0, \dots, p-1),$$

where the constant implied by $\ll$ is absolute. A proof can be found in Fouché's article [8]; it combines a variant of the above argument with the prime number theorem.

Granville [10] added some more sophisticated reasoning to prove that

$$\operatorname{card}\left\{l < p^{1/u} \mid l \text{ prime}, \, q_l = 0\right\} < up^{1/2u},$$

where $u = 1, 2, \dots$ and $u^{2u} < p$.

In our computation we found all the zeros in the first row of M_p for every p below 10^6 and also for a few primes above this limit. For a fixed p, let z denote the number of these zeros. As expected, z is much less than $\sqrt{p}$ (except for $p = 11$). In the range $p < 10^6$ the values of z vary from 1 to 9, except that $z = 11$ for $p = 1093$ and $z = 12$ for $p = 3511$. The latter primes are the two *Wieferich primes*, i.e., primes with $q_2 = 0$.

Table I lists the primes $p < 2^{32}$ having a zero in the range $1 < a \leq 10$. We used the table in [23] to complete this list of p and included all these primes in our computation, wishing to find as large sets of zeros,

$$Z = \{a \in I_p \mid q_a = 0\},$$

as possible. The second column of the table gives Z, with the prime factorization of each a (up to some trivial factorizations), and the third column records $z = \operatorname{card} Z$. The value $z = 15$ appearing in the table is the largest z we know.

TABLE I. Vanishing q_a, with some a in $2, \dots, 10$, for $p < 2^{32}$.

p	Z	z
11	3^n, $n = 0, 1, 2$	3
487	10^n, $n = 0, 1, 2$; $175 = 5^2 \cdot 7$; 307	5
1093	2^n, $n = 0, \dots, 10$	11
3511	2^n, $n = 0, \dots, 11$	12
20771	5^n, $n = 0, \dots, 6$	7
40487	5^n, $n = 0, \dots, 6$; $4492 = 2^2 \cdot 1123$; $22460 = 2^2 \cdot 5 \cdot 1123$	9
66161	6^n, $n = 0, \dots, 6$	7
491531	7^n, $n = 0, \dots, 6$; $397783 = 17 \cdot 23399$	8
534851	6^n, $n = 0, \dots, 7$	8
1006003	3^n, $n = 0, \dots, 12$	13
3152573	6^n, $n = 0, \dots, 8$; $1693042 = 2 \cdot 13^2 \cdot 5009$	10
53471161	5^n, $n = 0, \dots, 11$	12
56598313	10^n, $n = 0, \dots, 7$	8
1645333507	5^n, $n = 0, \dots, 13$; $1317772341 = 3^3 \cdot 19 \cdot 2568757$	15

Call a subset Y of $Z \setminus \{1\}$ *independent* if there is no relation $q_a = 0$ with $a \in Y$ following by the logarithmic rule from the other relations $q_a = 0$, $a \in Y$. The largest independent set found by us occurs for $p = 728,471$. For this prime, $z = 9$

and the whole set

$$\begin{aligned} Z \setminus \{1\} =\{&36709,\ 159316 = 2^2 \cdot 39829,\ 241830 = 2 \cdot 3^2 \cdot 5 \cdot 2687,\ 288664 \\ &= 2^3 \cdot 36083,\ 418571 = 223 \cdot 1877,\ 443653 = 7 \cdot 61 \cdot 1039,\ 653451 \\ &= 3 \cdot 67 \cdot 3251,\ 679977 = 3^2 \cdot 75553\} \end{aligned}$$

is independent.

On the other hand, for a set Y *not* to be independent, the most frequent reason is that some element is a power of another. There is only one prime below 10^6 providing a different example: for $p = 40,487$ one may take $Y = \{5,\ 4492,\ 5 \cdot 4492\}$ (see Table I).

4. Equidistribution of Fermat quotients

In a recent work [13], Heath-Brown obtains a result about the distribution of the values of q_a. The idea is to consider the Dirichlet character χ mod p^2 given by $\chi(a) = e^{2\pi i q_a/p}$ (for $p \nmid a$) and to estimate the sum $\sum_{M<a\le M+N} \chi^h(a)$, where $p \nmid h$. By using Burgess' estimate, Heath-Brown proves that

$$\sum_{M<a\le M+N} \chi^h(a) \ll N^{1/2} p^{3/8}$$

uniformly for $M, N \ge 1$. By Weyl's criterion this implies, on summing over primes $p \le X$, that the sequence of the numbers q_a/p with increasing p and $a = 1, \dots, p-1$ is uniformly distributed mod 1. The preceding upper bound can also be generalized to $N^{(s-1)/s} p^{(s+1)/2s^2}$, with any fixed integer $s \ge 2$ (personal communication). Letting $s \to \infty$ one concludes that the finite set

$$\{q_a/p \mid 1 < a \le N\},$$

for any fixed prime p, is approximately uniformly distributed mod 1 if $N \ge p^{\frac{1}{2}+\delta}$ (with $\delta > 0$), the distribution tending closer to uniform as $p \to \infty$.

This means that a set of values of q_a, for $1 < a \le N$, behaves approximately like a set in which each number is randomly distributed in the range $0, \dots, p-1$ (for $N \ge p^{\frac{1}{2}+\delta}$). In particular, the effect of single relations between various q_a is on a large scale negligible.

Let $w_p(n)$ denote the probability that exactly n of $p-2$ independent random choices of integers in $\{0, 1, \dots, p-1\}$ turn out to be 0. Thus $w_p(n)$ is given by the binomial distribution:

$$w_p(n) = \binom{p-2}{n} \left(\frac{1}{p}\right)^n \left(\frac{p-1}{p}\right)^{p-2-n},$$

and approaches $e^{-1}/n!$ as $p \to \infty$. This is the Poisson distribution with mean 1. Now consider $z - 1 = \operatorname{card}\{a \in I_p \mid a > 1,\ q_a = 0\}$. Thinking of the numbers q_a as "random" one may thus conjecture that, for each fixed n, the density of primes p with $z - 1 = n$ is $e^{-1}/n!$. In Table II we compare this conjecture with our computations up to 10^6. The second column of the table gives the number of primes p with a fixed z, denoted by m_z. The total number of odd primes less than 10^6 is 78,497. The observed and expected frequencies are seen to agree excellently. (By excluding the primes below some small bound one could come up with yet slightly better figures.)

The last column in Table II indicates the least p belonging to a given z.

TABLE II. Distribution of primes $p < 10^6$ according to the number of vanishing q_a.

$z = n + 1$	m_z	$m_z/78497$	$1/n!e$	$p_{\min}$
1	28949	.3687...	.3678...	3
2	28936	.3686...	.3678...	29
3	14387	.1832...	.1839...	11
4	4763	.0606...	.0613...	269
5	1178	.0150...	.0153...	487
6	216	.0027...	.0030...	653
7	59	.0007...	.0005...	5107
8	5			103291
9	2			40487
10	0			–
11	1			1093
12	1			3511

TABLE III. Vanishing q_a with $1 < a < \sqrt{p}$ and $1 < a < \sqrt[3]{p}$, respectively.

j	g_j	$(p_{\max}, a)$
1	63	91303, 172
2	21	192047, 141
3	13	291721, 323
4	14	383951, 92
5	15	497557, 525
6	13	598967, 574
7	9	691409, 471
8	8	795071, 465
9	7	880751, 672
10	9	993913, 675

(p, a)	(p, a)	(p, a)
1093, 2	29131, 15	66431, 40
1093, 4	33923, 18	77867, 37
1093, 8	40487, 5	123653, 12
2693, 12	40487, 25	131759, 45
3511, 2	46021, 17	160541, 30
3511, 4	46457, 20	401771, 63
3511, 8	47441, 33	491531, 7
20771, 5	48947, 17	491531, 49
20771, 25	66161, 6	534851, 6
25633, 24	66161, 36	534851, 36
		661049, 76

In our range $p < 10^6$ we recorded the particular cases of $q_a = 0$ with $1 < a < \sqrt{p}$, and also those with $1 < a < \sqrt[3]{p}$. Data about these zeros are shown in Table III. There are 172 primes for which an a of the former kind exists; the first table shows their number, denoted by g_j, in each subinterval $\Delta_j : (j-1)10^5 < p < j \cdot 10^5$ $(j = 1, \ldots, 10)$. The third column exhibits, as a sample, the largest p in each Δ_j together with the corresponding a (which happens to be unique).

The second table lists the pairs (p, a) for which $q_a = 0$ and $1 < a < \sqrt[3]{p}$.

The tendency of a decreasing frequency of primes p in Table III can be explained simply by the fact that the share of these short ranges in the whole I_p tends to zero. In fact we conjecture that for any exponent κ, with $0 < \kappa < 1$, the density of primes p for which there is some vanishing q_a in the range $1 < a < p^\kappa$ is zero. This conjecture is supported by the Poisson model discussed above in connection with Table II and Heath-Brown's equidistribution results.

A main motivation for the study of small $a \in I_p$ with $q_a = 0$ has traditionally been the Fermat equation $x^p + y^p = z^p$. It had been shown that the existence of a solution (x, y, z) with $p \nmid xyz$ would imply that $q_l = 0$ for all primes $l = 2, 3, \ldots, L$,

where the value of L was gradually increased. The latest result, due to Suzuki [28], has $L = 113$.

After this, it is natural to ask what can be said about the least $a > 1$, say $a = d_p$, such that q_a does *not* vanish. Note that d_p is necessarily prime. Granville [10, 11] proved, as a slight improvement upon a result by Lenstra [19], that $d_p < \log^2 p$. The main argument in both authors' works is again the simple fact that the total number of zeros in the matrix M_p is known; in addition, some analytical results about the distribution of prime numbers are required.

Since any $t \in \{0, \dots, p-1\}$ occurs $p-1$ times in M_p, one expects a similar estimate for the number $l_p(t) = \min\{l \mid l \text{ prime}, q_l \neq t\}$. Fouché [8] has indeed proved that $l_p(t) \leq (1+o(1)) \left(\frac{2}{e} \log p\right)^2$ $(p \to \infty)$.

For d_p one could obtain the weaker estimate $d_p < \sqrt{p}$ just by looking at elementary properties of M_p. One proof for this inequality, under the restriction $p \equiv 1 \pmod 4$, is presented in [30].

It is likely that the true values of d_p are much smaller than $\log^2 p$. A computation by Crandall, Dilcher and Pomerance [5] shows that $d_p \leq 3$ up to $p < 4 \cdot 10^{12}$, more precisely, $d_p = 2$ in this whole range apart from the primes 1093 and 3511.

Note also that Johnson [15] derives various conditions on p and a which ensure that $q_a \neq 0$. This gives him an easy way to generate a set of primes for which $q_2 \neq 0$. The largest prime found by him exceeds 22 million. Unfortunately, it is not known whether one could by this method produce infinitely many such primes.

5. Close zeros

If $d_p > 2$, the first row of the matrix M_p begins with two zeros. One may ask, more generally, what are the possibilities for consecutive zeros, or zeros "close" to each other, in the rows of M_p. For a connection between the existence of consecutive zeros (in the first row I_p of M_p) and the theory of cyclotomic units, see [14].

Our computations reveal that for $p < 10^6$ there are no consecutive zeros in I_p other than those with $a = 1$ and $a = 2$ for the two Wieferich primes. For just thirteen primes in this range there are two zeros, say a and a', with $0 < a' - a < 10$. Nine of those primes can be found in Table I. The remaining four primes, together with the corresponding a and a', are the following:

$$(269 : 171, 180),\ (797 : 440, 446),\ (24337 : 20248, 20254),\ (56909 : 10032, 10040).$$

Looking at the entire matrix M_p rather than at its first row, we find that M_p certainly contains consecutive zeros for infinitely many primes. Indeed, we prove that such zeros exist whenever $p \equiv 1 \pmod 3$. This result will be generalized to $Q_a \bmod p^m$ in §7.

Proposition 2. *If $p \equiv 1 \pmod 3$, there exists $a \in \mathbb{Z}$, $1 < a < p^2 - 1$, such that*

$$(a, p) = (a+1, p) = 1, \qquad q_a = q_{a+1} = 0. \tag{7}$$

Proof. Let $r \bmod p^2$ denote a generator of the cyclic subgroup of $(\mathbb{Z}/p^2\mathbb{Z})^\times$ consisting of the solutions of the congruence $x^{p-1} \equiv 1 \pmod{p^2}$ (see §2). Choose a so that

$$a \equiv r^{(p-1)/3} \pmod{p^2}, \qquad 1 \leq a < p^2.$$

Then a is prime to p and $q_a = 0$. Also it follows that $a^3 \equiv 1 \pmod{p^2}$ and $a \not\equiv 1 \pmod{p^2}$. Therefore, $1 < a < p^2 - 1$. Moreover, $a \not\equiv 1 \pmod{p}$, since otherwise the condition $q_a = 0$ would imply that $a = 1$.

From the decomposition $a^3 - 1 = (a-1)(a^2 + a + 1)$ we find that

$$a^2 + a + 1 \equiv 0 \pmod{p^2}. \tag{8}$$

Thus, $a + 1$ is prime to p and $q_{a+1} = q_{-a^2} = q_{a^2} = 0$. □

Unfortunately, we have $a > p$. Indeed, from $a \leq p - 1$ it would follow that $a^2 + a + 1 < p^2$, which contradicts (8).

Along with a, also $p^2 - a - 1$ satisfies (7) and (8).

The equations $q_a = q_{a+1} = 0$ also imply that $q_c = q_{c+1} = 0$, where c is the multiplicative inverse of a mod p^2. This gives us a method for finding new pairs of consecutive zeros: on obtaining the pair $(c, c+1)$, normalized between 0 and p^2, go to $(p^2 - c - 1, p^2 - c)$ and take again the inverse. It is likely that a satisfies some condition making this procedure terminate quickly. For example, if a is the number of the preceding proof, then $c = p^2 - a - 1$ and so no new pairs will turn up.

6. Fermat quotients and Catalan's equation

It has long been known that Fermat quotients are related to the existence of solutions of Catalan's equation

$$x^p - y^q = 1 \qquad (p \text{ and } q \text{ odd primes}). \tag{9}$$

We refer to [25] for a nice treatment of Catalan's equation. A result by Schwarz [27]—in fact, the latest step in a series of similar results—asserts that (9) has no nontrivial integral solution if $p^{q-1} \not\equiv 1 \pmod{q^2}$ and if there is an imaginary subfield of the pth cyclotomic field whose relative class number is prime to q.

Since the roles of p and q can be interchanged, the "hardest" case occurs when p and q satisfy the simultaneous congruences

$$p^{q-1} \equiv 1 \pmod{q^2}, \qquad q^{p-1} \equiv 1 \pmod{p^2}. \tag{10}$$

Our search shows that there are exactly three such pairs (p, q) with p and q below 10^6:

$$(4871, 83), \quad (18787, 2903), \quad (318917, 911).$$

The first pair was found by Aaltonen and Inkeri [1], the two other pairs by Mignotte and Roy [21, 22].

In addition to these examples, the pairs (1006003, 3) and (1645333507, 5) are known to satisfy (10). These were observed in [1] and [23], respectively. Allowing the case $q = 2$ we have one further example in (1093, 2).

It follows from Tijdeman's famous theorem [29] that any possible solution of (9) necessarily has x^p and y^q below an efficiently computable constant C. The currently known value of C is so large, however, that it is of no use in practical calculations.

7. Fermat quotients modulo higher powers of p

For any $m \geq 1$, the congruence

$$x^{p-1} \equiv 1 \pmod{p^{m+1}} \tag{11}$$

has $p-1$ incongruent roots, and these roots are incongruent even mod p. In fact, the roots are $x \equiv a + \sum_{i=1}^{m} a_i p^i \pmod{p^{m+1}}$, with $1 \leq a \leq p-1$, where

$$\omega_a = a + a_1 p + a_2 p^2 + \cdots \qquad (0 \leq a_i \leq p-1)$$

is the unique p-adic integer congruent to a mod p and satisfying $\omega_a^{p-1} = 1$.

Consequently, there are exactly $p-1$ integers $a \in \mathbb{Z} \backslash p\mathbb{Z}$ in the range $0 < a < p^{m+1}$ such that $Q_a \equiv 0 \pmod{p^m}$.

The numbers ω_a are important in many applications of p-adic numbers, particularly in the theory of cyclotomic fields. The next proposition states one basic property of these numbers.

Proposition 3. *Let $1 \leq a \leq p-1$. Then $\omega_a \equiv a \pmod{p^{m+1}}$ if and only if $Q_a \equiv 0 \pmod{p^m}$. In particular, $a_1 \equiv aQ_a \pmod{p}$.*

Proof. Since $\omega_a \equiv a \pmod{p}$ and $\omega_a^p = \omega_a$, we have

$$\omega_a \equiv a^{p^m} \pmod{p^{m+1}}. \tag{12}$$

Thus it suffices to prove that the congruences $a^{p^m} \equiv a \pmod{p^{m+1}}$ and $a^p \equiv a \pmod{p^{m+1}}$ are equivalent. That the latter congruence implies the former, is obvious. The converse implication is verified by raising the former congruence to the pth power and noting that $a^{p^{m+1}-p^m} \equiv 1 \pmod{p^{m+1}}$.

The last assertion of the proposition follows from (12) for $m = 1$. □

The following result, quoted for $m = 1$ in §2, is a consequence of the structure of the group $G = (\mathbb{Z}/p^{m+1}\mathbb{Z})^\times$. The integers $a \in \mathbb{Z} \setminus p\mathbb{Z}$ modulo p^{m+1} may be uniquely represented in the form

$$a \equiv r^u (1+p)^v \pmod{p^{m+1}}, \qquad u \bmod p-1, \quad v \bmod p^m,$$

where r is a fixed primitive root of p such that $Q_r \equiv 0 \pmod{p^m}$. Here r and $1+p$ mod p^{m+1} generate the cyclic subgroups of order $p-1$ and p^m, respectively, of G.

If $p \equiv 1 \pmod{3}$, the group generated by r mod p^{m+1} contains a subgroup of order 3. Let a mod p^{m+1}, with $1 < a < p^{m+1}$, be a generator of this subgroup. Since a is a root of (11), we have $a \not\equiv 1 \pmod{p}$ and an argument similar to that in the proof of Proposition 2 yields

$$Q_a \equiv Q_{a+1} \equiv 0 \pmod{p^m}.$$

We point out that for $m > 1$ it may happen that this particular a can be chosen from the range $1 < a < p^m$. For instance, if $p = 7$ and $m = 2$, the residue class of 18 mod 343 is such a generator.

Specializing to the case $m = 2$ we have the question – interesting in view of Proposition 3, for example – about the solutions of

$$Q_a \equiv 0 \pmod{p^2}, \qquad 1 < a < p. \tag{13}$$

TABLE IV. Pairs (p, a) satisfying (14) with $|k| \leq 5$ or (15) with $0 \leq b \leq 6$, respectively.

(p, a, k)	(p, a, k)	(p, a, k)
$11, 3, 4$	$131, 111, -5$	$1489, 1211, -2$
$11, 9, -3$	$211, 165, 5$	$2777, 59, 4$
$43, 19, -5$	$241, 94, -3$	$3889, 1004, 2$
$71, 26, -2$	$577, 427, -5$	$5857, 3114, 5$
$103, 43, 4$	$641, 340, -3$	$16091, 7560, -5$
$113, 68, 0$	$997, 252, 5$	$63533, 27864, 5$
$131, 58, 1$	$1291, 1148, -1$	

(p, a, b)	(p, a, b)
$11, 3, 1$	$1847, 189, 2$
$11, 9, 6$	$2693, 12, 1$
$29, 14, 6$	$102451, 22174, 3$
$113, 68, 0$	$252209, 219571, 6$
$1601, 1420, 1$	

According to Lenstra [19] one should expect that for a fixed a there be only finitely many primes p satisfying this congruence. Anyway, the occurrences of (13) seem extremely rare. An old example is $p = 113$, $a = 68$. Our computation shows that there are no further examples in the range $p < 10^6$. Montgomery [23], searching through $a = 2, \ldots, 99$ up to $p < 2^{32}$, did not find any new example either.

We extended our numerical study to two kinds of congruences "close" to (13). The first is the congruence

$$Q_a \equiv kp \pmod{p^2} \tag{14}$$

with $1 < a < p$ and with small $|k|$. For $p < 10^6$, twenty pairs (p, a) satisfying this congruence for $|k| \leq 5$ were found, the largest p being 63,533. These are listed in Table IV (first table). It is no surprise that the number of examples is strongly declining as p increases.

Our second study is related to the solutions of the congruence $x^{p-1} \equiv 1 \pmod{p^3}$ satisfying $x \equiv a \pmod{p}$, where $1 < a < p$ and $q_a = 0$. By the last assertion of Proposition 3, such solutions are of the form $x \equiv a + bp^2 \pmod{p^3}$. One verifies easily that $b \equiv aQ_a/p \pmod{p}$. If b can be taken a small positive number, we thus have a "small" positive solution of this special type for our congruence. This motivation leads us to search for pairs (p, a) such that

$$aQ_a \equiv bp \pmod{p^2}, \tag{15}$$

where $b \geq 0$ is small. All the examples of this congruence for $b \leq 6$ and p below 10^6 are presented in Table IV (second table).

Among the few results about Q_a mod p^m with $m > 1$ appearing in the literature, we would like to quote the following. Granville [9] finds a result about the congruences in (13), for a fixed a (prime) and for varying p, under some strong conditions imposed on the corresponding congruences mod p. E. Lehmer's article [18] relates Q_a mod p^2 to Bernoulli numbers by several congruences, with applications. Johnson [16] presents an algorithm for determining the exact power of p dividing Q_a.

8. The computations

The computations were carried out on a Convex C3840 computer at CSC, the Center for Scientific Computing in Finland. The main part of the work, the location (and prime factorization) of all a in the range $2, \ldots, p-1$ with $q_a = 0$, for $p < 10^6$, took about 28 hours CPU time. No use was made of the parallel computing

feature of the machine. The programs were written in the language C. A table containing the complete results is available by anonymous FTP from `ftp.utu.fi` in the directory `pub/fermquot`.

We calculated q_a for every $a = 1, \dots, \frac{p-1}{2}$, recording only the cases with either $q_a = 0$ or $q_{p-a} = 0$. Note that by (2) the latter condition is equivalent to the congruence $aq_a \equiv -1 \pmod p$. To minimize the amount of computation mod p^2 the program proceeded in cycles, passing from q_a to q_{2a} or, if $2a > \frac{p-1}{2}$, to q_{p-2a}. Hence, a computation mod p^2 was required for just the first q_a in each cycle. The number of cycles remains relatively small: it is $\frac{p-1}{d}$ or $\frac{p-1}{2d}$, where d is the order of 2 mod p. We had earlier developed and programmed this method of computing q_a, without explicitly recording the results, as an intermediate step in a computation of cyclotomic invariants. This is described in [7], and the method has been subsequently applied in a computation extending to higher values of p (see [2] for work to $p < 4 \cdot 10^6$).

For the few single primes between 10^6 and 10^8 in Table I, the running time ranged from a few seconds to about an hour. For the largest prime, 1,645,333,507, the computation was arranged slightly differently. It required about 50 minutes, the number of cycles being three.

As a check we verified, for each $p > 3$, the congruence $48 \sum_{a=1}^{(p-1)/2} a^2 q_a \equiv 1 \pmod p$. This known formula follows easily via Bernoulli numbers B_n: first compute

$$\sum_{a=1}^{p-1} a^2 q_a \equiv \frac{1}{p} \sum_{a=1}^{p-1} \left(a^{p+1} - a^2\right) \equiv B_{p+1} - B_2 \equiv -\frac{1}{2} B_2 \equiv -\frac{1}{12} \pmod p,$$

where use was made of the Kummer congruences mod p for B_n, and then pass to the half-sum by using (2).

Once the table of the zeros of q_a was finished, it did not take more than some seconds of machine time to find the "Catalan pairs" (p, q) and the special pairs (p, a) related to the behavior of $Q_a \bmod p^2$.

For a reader interested in computing by hand the Fermat quotient matrix for small p we point out that the above cycle method can then be much improved by a more efficient use of the logarithmic rule. For many primes there is no need at all for computation mod p^2, if one employs the information provided by the first and last columns of M_p, known *a priori*.

There exist numerous previous works tabulating zeros of q_a. The tables typically have a fixed upper bound for a, whereas p may occasionally be very large. The table in [3] covers most of its predecessors; it extends over the range $a < 100$, the upper bound for p varying from 10^6 to $3 \cdot 10^9$. Montgomery [23] completes this table up to $p < 2^{32}$. A part of the new data given by him was earlier found by Keller [17]. For $a \le 150$, there is a table by Riesel [26] extending to $p < 10^4$. A recent work by S. Shepherd settles the range $100 \le a \le 1000$, $p < 10^5$ (personal communication). Aaltonen and Inkeri performed computations for $a < 10^4$, $p < 10^4$, restricting to prime values of a; their article [1] tabulates the results for a below 1000 (the table for $100 < a < 1000$ is reprinted in [24, pp. 348–349]).

When writing the present paper we learned that Mignotte and Roy had computed $q^{p-1} \bmod p^2$ for large sets of primes q and p. Part of their results appears in [21]. Currently they are extending the computation for all primes $q < 10^5$ and for $p < M(q)$, where $M(q)$ depends on q and is anyway to exceed $1000q$.

Acknowledgment

Several colleagues have provided us with information and advice during the work. Our special thanks are due to Karl Dilcher, Andrew Granville, Roger Heath-Brown, Maurice Mignotte, Peter Montgomery and Ray Stewart.

References

1. M. Aaltonen and K. Inkeri, *Catalan's equation $x^p - y^q = 1$ and related congruences*, Math. Comp. **56** (1991), 359–370. MR **91g:**11025
2. J. Buhler, R. Crandall, R. Ernvall and T. Metsänkylä, *Irregular primes and cyclotomic invariants to four million*, Math. Comp. **61** (1993), 151–153. MR **93k:**11014
3. J. Brillhart, J. Tonascia and P. Weinberger, *On the Fermat quotient*, Computers in Number Theory (ed. by Atkin and Birch), Academic Press, London and New York, 1971, pp. 213–222. MR **47:**3288
4. D. Coppersmith, *Fermat's Last Theorem (Case 1) and the Wieferich criterion*, Math. Comp. **54** (1990), 895–902. MR **90h:**11024
5. R. Crandall, K. Dilcher and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. **66** (1997), 433–449. CMP 96:07
6. L. E. Dickson, *History of the Theory of Numbers, I-II*, Carnegie Institution of Washington, Washington, 1919-1920; reprint, Chelsea, New York, 1952.
7. R. Ernvall and T. Metsänkylä, *Cyclotomic invariants for primes between* 125000 *and* 150000, Math. Comp. **56** (1991), 851–858. MR **91h:**11157
8. W. L. Fouché, *On the Kummer–Mirimanoff congruences*, Quart. J. Math., Oxford, II Ser., **37** (1986), 257–261. MR **88a:**11022
9. A. Granville, *Refining the conditions on the Fermat quotient*, Math. Proc. Cambr. Phil. Soc. **98** (1985), 5–8. MR **86g:**11016
10. A. Granville, *Diophantine Equations with Varying Exponents* (doctoral thesis), Queen's University, Kingston, Ontario, Canada, 1987.
11. A. Granville, *Some conjectures related to Fermat's Last Theorem*, Number Theory (Banff, AB, 1988), de Gruyter, Berlin, 1990, pp. 177–192. MR **92k:**11036
12. H. Hasse, *Zahlentheorie*, 3rd ed., Akademie-Verlag, Berlin, 1969; English translation: *Number Theory*, Springer, Berlin–New York, 1980. MR **81c:**12001b
13. R. Heath-Brown, *An estimate for Heilbronn's exponential sum*, Analytic Number Theory: Proc. Conference in honor of Heini Halberstam, Birkhäuser, Boston, to appear in 1996.
14. C. Helou, *Norm residue symbol and cyclotomic units*, Acta Arith. **73** (1995), 147-188. CMP 96:03
15. W. Johnson, *On the nonvanishing of Fermat quotients* $\pmod p$, J. Reine Angew. Math. **292** (1977), 196–200. MR **56:**8489
16. W. Johnson, *On the p-divisibility of the Fermat quotients*, Math. Comp. **32** (1978), 297–301. MR **57:**3053
17. W. Keller, *New prime solutions p of $a^{p-1} \equiv 1 \pmod{p^2}$* (preliminary report), Abstracts Amer. Math. Soc. **9** (1988), 503.
18. E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. (2) **39** (1938), 350–360.
19. H. W. Lenstra, Jr., *Miller's primality test*, Inform. Process. Lett. **8** (1979), 86–88. MR **80c:**10008
20. M. Lerch, *Zur Theorie des Fermatschen Quotienten* $\frac{a^{p-1}-1}{p} = q(a)$, Math. Annalen **60** (1905), 471–490.
21. M. Mignotte and Y. Roy, *l'Equation de Catalan*, Prépubl. l'Inst. Rech. Math. Avancée 513/P-299 (1992), 1–44.
22. M. Mignotte and Y. Roy, *Catalan's equation has no new solution with either exponent less than* 10651, Experiment. Math. **4** (1995), 259–268. CMP 96:12
23. P. Montgomery, *New solutions of $a^{p-1} \equiv 1 \pmod{p^2}$*, Math. Comp. **61** (1993), 361–363. MR **94d:**11003
24. P. Ribenboim, *The New Book of Prime Number Records*, 3rd ed., Springer, New York, 1996. CMP 96:09

25. P. Ribenboim, *Catalan's Conjecture*, Academic Press, New York and London, 1994. MR **95a:**11029
26. H. Riesel, *Note on the congruence* $a^{p-1} \equiv 1 \pmod{p^2}$, Math. Comp. **18** (1964), 149–150. MR **28:**1156
27. W. Schwarz, *A note on Catalan's equation*, Acta Arith. **72** (1995), 277–279. MR **96f:**11048
28. J. Suzuki, *On the generalized Wieferich criteria*, Proc. Japan Acad., Ser. A **70** (1994), 230–234. MR **95j:**11026
29. R. Tijdeman, *On the equation of Catalan*, Acta Arith. **29** (1976), 197–209. MR **53:**7941
30. N. Tzanakis, *Solution to problem E 2956*, Amer. Math. Monthly **93** (1986), 569.
31. H. S. Vandiver, *An aspect of the linear congruence with applications to the theory of Fermat's quotient*, Bull. Amer. Math. Soc. **22** (1915), 61–67.

Forssa Institute of Technology, Saksankatu 46, FIN-30100 Forssa, Finland

Department of Mathematics, University of Turku, FIN-20014 Turku, Finland
E-mail address: taumets@sara.cc.utu.fi