JOURNAL OF NUMBER THEORY **66**, 29–50 (1997)
ARTICLE NO. NT972162

Fermat Quotients for Composite Moduli

Takashi Agoh*

Department of Mathematics, Science University of Tokyo, Noda, Chiba 278, Japan

Karl Dilcher†

Department of Mathematics, Statistics and Computing Science, Dalhousie University, Halifax, Nova Scotia, Canada B3H 3J5

and

Ladislav Skula‡

Department of Mathematics, Faculty of Science, Masaryk University, 66295 Brno, Czech Republic

Communicated by A. Granville

Received April 12, 1996; revised January 21, 1997

Analogues of Fermat quotients for a composite modulus $m \geqslant 2$ are investigated, with special emphasis on various congruences. In particular, the numbers m for which $a^{\psi(m)} \equiv 1 \pmod{m^2}$, where $\gcd(a, m) = 1$, ("Wieferich numbers with base a") are completely characterized in terms of the Wieferich primes with base a.

1. INTRODUCTION

One of the most classical and celebrated theorems in elementary number theory is Fermat's little theorem (see, e.g., [5] or [13]).

* Supported in part by a grant of the Ministry of Education, Science and Culture of Japan. E-mail: agoh@ma.noda.sut.ac.jp.

† Supported by NSERC of Canada. E-mail: dilcher@cs.dal.ca.

‡ Supported by the Grant Agency of the Czech Republic, "Number Theory, its Algebraic Aspects and its Relationship to Computer Science," No. 201/93/2/22. E-mail: skula@math.muni.cz.

0022-314X/97 $25.00

THEOREM 1.1 (Fermat's little theorem). *If p is a prime and a is an integer not divisible by p, then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

This gives rise to a class of special quotients which are integers.

DEFINITION 1.1. Let p be a prime and a an integer not divisible by p. The quotient

$$q_p(a) = \frac{a^{p-1} - 1}{p}$$

is called the *Fermat quotient* of p with base a.

These objects have been investigated by many authors (see, e.g., [5, 8, 11, or 13]). In particular, the Fermat quotient with base 2 was used by Wieferich [17] in his celebrated theorem concerning the first case of Fermat's last theorem.

THEOREM 1.2 (Wieferich). *Let p be an odd prime, and x, y, z be integers, not divisible by p, satisfying the equation*

$$x^p + y^p + z^p = 0.$$

Then

$$2^{p-1} \equiv 1 \pmod{p^2}.$$

Odd primes satisfying this last congruence or, equivalently, the congruence $q_p(2) \equiv 0 \pmod{p}$, are called *Wieferich primes*. At present only two such primes are known: 1093, discovered by Meissner (1913), and 3511, discovered by Beeger (1922); see, e.g., [13]. According to the computations of D. H. Lehmer [10] there are no other Wieferich primes less than 6×10^9. These computations were recently extended to 4×10^{12} by Crandall, Dilcher, and Pomerance [4]; again, no other Wieferich prime was found. Computations concerning Fermat quotients with other bases were carried out by several authors (see [13] or [14]), the most recent being Montgomery [12]. (Here we would like to point out that several pairs (a, p) with $q_p(a) \equiv 0 \pmod{p}$, claimed to be new in [12], were in fact discovered earlier by Keller [7].)

In 1905, Lerch [8, pp. 484–487] introduced and studied a generalization of the Fermat quotient for composite modulus m (m odd, $m > 1$). It is based on the following well-known extension of Fermat's little theorem.

THEOREM 1.3 (Euler's theorem). *Let m and a be two relatively prime integers, $m \geqslant 2$. Then*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

In a subsequent paper [9], Lerch extended his definition of generalized Fermat quotients to arbitrary integers $m \geqslant 2$; we propose to call them *Euler quotients*. Apart from Lerch's work, they have not been studied in any great detail.

DEFINITION 1.2. Let a and $m \geqslant 2$ be relatively prime integers. The quotient

$$q(a, m) = \frac{a^{\phi(m)} - 1}{m}$$

will be called the Euler quotient of m with base a.

To continue the analogy with the case of prime moduli, we generalize the concept of a Wieferich prime as follows.

DEFINITION 1.3. Let $m \geqslant 2$ and a be relatively prime integers. We say that m is a *Wieferich number* with base a if

$$q(a, m) \equiv 0 \pmod{m}.$$

We note that the term "Wieferich number" was recently also introduced in [6] to denote a different generalization of a Wieferich prime. We do not believe that there is much danger of confusion.

The purpose of this paper is twofold. First, we undertake a careful study of Euler quotients, generalizing many of the properties of the Fermat quotients discovered by Lerch [8] and E. Lehmer [11]. This is done in Sections 2 through 4. Then, in Section 5, we give a characterization for an integer $m \geqslant 2$ to be a Wieferich number. Our main result is Theorem 5.5 which shows that the Wieferich numbers to a given base are completely determined by the corresponding Wieferich *primes* to this base (i.e., primes p for which $q_p(a) \equiv 0 \pmod{p}$). As corollaries we obtain the simple facts that (given a fixed base a) the largest prime factor of a Wieferich number is always a Wieferich prime, and that the product of two relatively prime Wieferich numbers is again a Wieferich number. By means of Theorem 5.5 and the known Wieferich primes all the Wieferich numbers with base 2 up to a certain limit are listed in Section 6. In that last section we give two more examples and list in Table I the numbers of Wieferich numbers to bases less than 100.

TABLE I

Number of m for Which $q(a, m) \equiv 0 \pmod{m}$

a	$N_1(a)$	$N_2(a)$	a	$N_1(a)$	$N_2(a)$	a	$N_1(a)$	$N_2(a)$
2	104	63	39	79	18	70	65	8
3	341	21	40	357	105	71	471	390
5	*	92	41	*	58	72	0	0
6	*	21	42	6	6	73	4	4
7	1473	144	43	56	56	74	1	1
10	688	12	44	114	78	75	851	184
11	30	30	45	*	73	76	*	167
12	35	8	46	5	5	77	101	37
13	*	72	47	0	0	78	*	116
14	7	7	48	3	3	79	*	759
15	22	12	50	2	2	80	99	85
17	*	238	51	23	23	82	7	7
18	*	104	52	*	9	83	*	150
19	*	1119	53	1483	797	84	54	25
20	*	14	54	5	5	85	65	58
21	0	0	55	1651	144	86	26	15
22	*	25	56	351	12	87	214	54
23	*	66	57	*	120	88	*	1
24	8	8	58	357	11	89	21	21
26	*	29	59	70	16	90	0	0
28	31	31	60	2	2	91	43	43
29	0	0	61	0	0	92	*	38
30	22	11	62	231	159	93	*	210
31	*	866	63	*	265	94	*	84
33	433	87	65	108	108	95	340	111
34	0	0	66	36	3	96	1848	18
35	416	174	67	*	135	97	*	75
37	*	11	68	461	259	98	1371	22
38	15	15	69	*	172	99	398	381

Finally we note that the related Wilson quotients, which are based on the well-known theorem of Wilson (see, e.g., [13]) can also be extended to composite moduli, and one can study composite analogues of Wilson primes. This is the subject of a separate paper [2]. It is also worth mentioning that Fermat quotients and Fermat primes have recently been extended to function fields; see [15].

2. EULER QUOTIENTS; GENERAL DISCUSSION

We begin by stating two fundamental congruences for the Euler quotients (see [8]; part (b) is easily generalized for $\alpha \geqslant 1$). Fix $m \geqslant 2$.

PROPOSITION 2.1. (a) *If a and b are integers with $(a, m) = (b, m) = 1$, then*

$$q(ab, m) \equiv q(a, m) + q(b, m) \pmod{m}$$

(*the "logarithmic property"*).

(b) *If c, k are integers, c, m are relatively prime, and α is a positive integer, then*

$$q(c + km^{\alpha}, m) \equiv q(c, m) + \frac{\phi(m)\, k}{c}\, m^{\alpha - 1} \pmod{m^{\alpha}}.$$

Next we present some relationships between various $q(a, m)$ with fixed base a and different moduli m. The proofs are quite straightforward.

PROPOSITION 2.2. (a) *If a and mn are relatively prime and if $m, n \geqslant 2$ then*

$$q(a, m) \mid nq(a, mn).$$

(b) *If a, m, and n are positive integers with $(a, mn) = (m, n) = 1$, then*

$$q(a, mn) \equiv \frac{\phi(n)}{n}\, q(a, m) \pmod{m},$$

and similarly with m and n interchanged.

The following theorem was first proved by Lerch [8] in a special case, and then, again, [9] in general. It generalizes a congruence that was used by Lerch [8] and E. Lehmer [11] to derive numerous other congruences which were useful, in part, as criteria for the first case of Fermat's last theorem. For the sake of completeness, we will present a proof (based on Lerch's paper [9]).

THEOREM 9.3 (Lerch). *If a and $m \geqslant 2$ are relatively prime integers, then*

$$q(a, m) \equiv \sum_{\substack{r = 1 \\ (r, m) = 1}}^{m} \frac{1}{ar} \left[\frac{ar}{m} \right] \pmod{m},$$

where $[x]$ denotes the greatest integer $\leqslant x$.

Proof. We write $ra \equiv c \pmod{m}$, with $1 \leqslant c \leqslant m$, $(c, m) = 1$. Then $ra = km + c$ for some integer k, and so $k = [ra/m]$. We use the fact that as c goes through all integers between 1 and m and relatively prime to m, then

so does r. Let P denote the product of all such integers. If the products and sums are understood to be taken over all r with $1 \leqslant r \leqslant m$ and $(r, m) = 1$, we get

$$P = \prod \left(ar - m \left[\frac{ar}{m} \right] \right) = a^{\phi(m)} P \prod \left(1 - \frac{m}{ar} \left[\frac{ar}{m} \right] \right);$$

i.e.,

$$1 = a^{\phi(m)} \prod \left(1 - \frac{m}{ar} \left[\frac{ar}{m} \right] \right) \equiv a^{\phi(m)} \left(1 - m \sum \frac{1}{ar} \left[\frac{ar}{m} \right] \right) \pmod{m^2},$$

or

$$a^{\phi(m)} - 1 \equiv a^{\phi(m)} m \sum \frac{1}{ar} \left[\frac{ar}{m} \right] \pmod{m^2}.$$

The result now follows if we divide both sides of the congruence by m and note that $a^{\phi(m)} \equiv 1 \pmod{m}$. ∎

THEOREM 2.4 (Baker; Lerch). *Let $a \geqslant 1$ and $m \geqslant 2$ be relatively prime integers. Then*

$$q(a, m) \equiv \sum_{\substack{r=1 \\ (r, m)=1}}^{m} \frac{\lambda(r)}{r} \pmod{m},$$

where $\lambda(r)$ denotes the least nonnegative residue of $-r/m \pmod{a}$.

Proof. We will actually show that this result and Theorem 2.3 are equivalent in the sense that each can be obtained from the other. With the notations of the proof of Theorem 2.3 we have

$$k = \left[\frac{ra}{m} \right] = \frac{ra - c}{m} \equiv -\frac{c}{m} \pmod{a}.$$

Then $0 \leqslant k < a$, since otherwise we would have $ra = km + c > km \geqslant am$, contradicting $r \leqslant m$. Hence, $[ar/m] = \lambda(c)$. We are done once we note that $ar \equiv c \pmod{m}$, and that c traverses a reduced residue system modulo m as r does. ∎

Historical remarks. In his paper [8] (1905) Lerch proved Theorem 2.3 for $m = p$ (an odd prime) in formula (8) and for odd m with $(m, \phi(m)) = 1$ in the same paper, formula (36). It was mentioned again, with proof, in his later paper [9] (1906, formula (2)). This time the only restriction was $a > 0$, but Lerch's proof works also for general a.

Also in 1906, Baker [3 (Feb. 8), p. 132] and Lerch [9 (Jan. 2), Eq. (3)] independently published Theorem 2.4. Its origins can be found in Sylvester's work [16] (1861), for the case where a and m are different primes. But Baker had only the condition $1 \leqslant a < m$ and Lerch did not give a proof.

3. EULER QUOTIENTS AND BERNOULLI POLYNOMIALS

In this section we will derive a variety of identities and congruences for Euler quotients involving Bernoulli polynomials and sums of powers of consecutive integers. The most important results, generalizing known congruences, are Theorems 3.2 and 3.6.

The Bernoulli polynomials $B_n(x)$, $n \geqslant 0$, can be defined by

$$B_n(x) = \sum_{r=0}^{n} \binom{n}{r} B_r x^{n-r}, \tag{3.1}$$

where the Bernoulli numbers B_r are defined by the generating function

$$\frac{t}{e^t - 1} = \sum_{r=0}^{\infty} \frac{B_r}{r!} t^r.$$

We will make repeated use of the following well-known connection between Bernoulli polynomials and sums of powers: For integers $k \geqslant 1$,

$$\sum_{j=1}^{n-1} j^k = \frac{1}{k+1} (B_{k+1}(n) - B_{k+1}). \tag{3.2}$$

THEOREM 3.1. *Let $a \geqslant 1$ and $m \geqslant 2$ be relatively prime integers. Then*

$$aq(a, m) = -\frac{a^{\phi(m)}}{mB_{\phi(m)}} \sum_{j=1}^{a-1} \left(B_{\phi(m)}\left(\frac{j}{a}\right) - B_{\phi(m)} \right).$$

Proof. The well-known relation

$$a^k \sum_{j=1}^{a-1} B_k\left(\frac{j}{a}\right) = (a - a^k)\, B_k$$

for $k \geqslant 2$ (see, e.g., [1, p. 804]) gives

$$a^k \sum_{j=1}^{a-1} \left(B_k\left(\frac{j}{a}\right) - B_k \right) = a(1 - a^k)\, B_k.$$

Setting $k = \phi(m)$ and using the definition of $q(a, m)$ we obtain the theorem. ∎

For another expression for the Euler quotient, we introduce the following.

Notation. Let $m \geqslant 2$ be an integer. For a real number $X \geqslant 1$, put

$$S^*(X) = \sum_{\substack{x=1 \\ (x,m)=1}}^{[X]} x^{\phi(m)-1}, \qquad S(X) = \sum_{x=1}^{[X]} x^{\phi(m)-1}.$$

Lerch's Theorem 2.3 can now be reformulated as follows.

THEOREM 3.2. *Let $a \geqslant 1$ and $m \geqslant 2$ be relatively prime integers. Then*

$$aq(a, m) \equiv -\sum_{k=1}^{a-1} S^*\left(\frac{km}{a}\right) \pmod{m}.$$

Notice that for $a = 1$ the right-hand side of this congruence is zero, by convention.

Proof. For $m = 2$, the left-hand side is $(a-1)\,a/2$, and since a is odd, $S^*(km/a) = 1$ for $(a+1)/2 \leqslant k \leqslant a-1$ and 0 otherwise. Hence, the right-hand side is $(a-1)/2$; therefore both sides have the same parity. Now suppose $m \geqslant 3$. Then $S^*(m) \equiv 0 \pmod{m}$ and for any integer $x (1 \leqslant x \leqslant m, (x, m) = 1)$ and $k_0 = [ax/m] + 1$ we have $ax/m < k_0 < ax/m + 1$; therefore $x < k_0 m/a < x + m/a$, which implies that $[(k_0 - 1)\,m/a] < x \leqslant [k_0 m/a]$. Hence

$$\begin{aligned}
\sum_{k=1}^{a-1} S^*\left(\frac{km}{a}\right) &\equiv \sum_{k=1}^{a} S^*\left(\frac{km}{a}\right) \pmod{m} \\
&= \sum_{k=1}^{a} \sum_{\substack{x=1 \\ (x,m)=1}}^{[km/a]} x^{\phi(m)-1} \\
&= \sum_{\substack{x=1 \\ (x,m)=1}}^{m} \sum_{\substack{k=1 \\ x \leqslant [km/a]}}^{a} x^{\phi(m)-1} \\
&= \sum_{\substack{x=1 \\ (x,m)=1}}^{m} \left(a - \left[\frac{ax}{m}\right]\right) x^{\phi(m)-1} \\
&\equiv -\sum_{\substack{r=1 \\ (r,m)=1}}^{m} \frac{1}{r}\left[\frac{ar}{m}\right] \pmod{m},
\end{aligned}$$

which, according to Lerch's Theorem 2.3, proves the result. ∎

THEOREM 3.3. *Let $m = p^\alpha$, where p is a prime and α is a positive integer. Let a and b be positive integers such that $(m, a) = 1$ and $ab \equiv 1 \pmod m$. If $m = 4$, $a \equiv b \equiv 3 \pmod 4$ and $a \not\equiv b \pmod 8$, put $\varepsilon = 2$; otherwise set $\varepsilon = 0$. Then*

$$aq(a, m) \equiv -\frac{1}{\phi(m)} \sum_{j=1}^{a-1} (B_{\phi(m)}(jb) - B_{\phi(m)}) + \varepsilon \pmod m.$$

Proof. (i) Using the identity $B_1(x) - B_1 = x$ we easily get the theorem for $m = 2$. Let $m = 4$. Then a and b are odd, $aq(a, m) = a(a^2 - 1)/4$, and $B_2(x) - B_2 = x^2 - x$. We can also suppose $a \geqslant 3$. So

$$\begin{aligned} -\frac{1}{\phi(m)} \sum_{j=1}^{a-1} (B_{\phi(m)}(jb) - B_{\phi(m)}) &= -\frac{1}{2} \sum_{j=1}^{a-1} (bj)^2 + \frac{1}{2} \sum_{j=1}^{a-1} (bj) \\ &= -\frac{1}{2} b^2 \frac{a(a-1)(2a-1)}{6} + \frac{1}{2} b \frac{a(a-1)}{2} \\ &= -ba \frac{a-1}{2} \cdot \frac{1}{3} \left(ba - \frac{b+3}{2} \right) \\ &\equiv -\frac{a-1}{2} \frac{b+1}{2} \pmod 4. \end{aligned}$$

When $a \equiv b \equiv 1 \pmod 4$, we write $a = 1 + 4u$, $b = 1 + 4v$ $(u, v \in \mathbb{Z})$, and we have $aq(a, 4) \equiv 2u \pmod 4$ and $-((a-1)/2)((b+1)/2) = -2u(1 + 2v) \equiv 2u \pmod 4$. If $a \equiv b \equiv 3 \pmod 4$, we write $a = 3 + 4u$, $b = 3 + 4v (u, v \in \mathbb{Z})$, and have $aq(a, 4) \equiv 2 + 2u \pmod 4$ and $-((a-1)/2)((b+1)/2) = -(1 + 2u) \times (2 + 2v) \equiv 2 + 2v \pmod 4$, which implies the theorem for $m = 4$.

(ii) Let $m = p^\alpha$, where p is a prime and α is a positive integer, $m \neq 2, 4$. Since $ba \equiv 1 \pmod m$, there exists a positive integer v with $ba = mv + 1$. Let $1 \leqslant j, k \leqslant a - 1$ be integers such that $jv \equiv k \pmod a$. Then $jv = k + T(j)a$, where $T(j)$ is some nonnegative integer. We have now

$$\begin{aligned} \frac{km}{a} &= \frac{m(jv - T(j)\, a)}{a} = \frac{jvm}{a} - mT(j) \\ &= \frac{abj - j}{a} - mT(j) = bj - mT(j) - \frac{j}{a}, \end{aligned}$$

or

$$\left[\frac{km}{a} \right] = bj - mT(j) - 1.$$

Since $\phi(m)-1=p^{\alpha-1}(p-1)-1\geqslant\alpha$ and $S(tm)\equiv 0 \pmod m$ for positive integers t, we have

$$S^*\left(\frac{km}{a}\right)\equiv S\left(\frac{km}{a}\right)=S(bj-1-mT(j))\equiv S(bj-1) \pmod m.$$

Therefore by Theorem 3.2,

$$aq(a, m)\equiv -\sum_{j=1}^{a-1} S(bj-1) \pmod m.$$

Using identity (3.2), we get

$$\frac{1}{\phi(m)}\sum_{j=1}^{a-1}(B_{\phi(m)}(jb)-B_{\phi(m)})=\sum_{j=1}^{a-1} S(bj-1),$$

and we are done. ∎

COROLLARY 3.4. *Let $m=p^{\alpha}$, where p is a prime and α a positive integer. Let a be a positive integer not divisible by p, and let X be a p-integral rational number satisfying $Xa\equiv 1 \pmod m$ unless $m=4$ and $a\equiv 3 \pmod 4$ in which case we suppose that $Xa\equiv 1 \pmod 8$. Then*

$$aq(a, m)\equiv -\frac{1}{\phi(m)}\sum_{j=1}^{a-1}(B_{\phi(m)}(jX)-B_{\phi(m)}) \pmod m,$$

or, equivalently,

$$aq(a, m)\equiv -\frac{1}{\phi(m)}\sum_{j=1}^{a-1}\left(B_{\phi(m)}\left(\frac{j}{a}\right)-B_{\phi(m)}\right) \pmod m.$$

Proof. For a positive real number x, define the functions

$$F(x)=-\frac{1}{\phi(m)}\sum_{j=1}^{a-1}\sum_{r=0}^{\phi(m)-1}\binom{\phi(m)}{r}B_r\, j^{\phi(m)-r}x^{\phi(m)-r};$$

$$G(x)=-\frac{1}{\phi(m)}\sum_{j=1}^{a-1}\sum_{r=0}^{\phi(m)-1}\binom{\phi(m)}{r}(\phi(m)-r)\,B_r\, j^{\phi(m)-r}x^{\phi(m)-r-1}.$$

Put

$$w=\begin{cases}2 & \text{when} \quad m=4;\ a\equiv 3 \pmod 4,\\ 1 & \text{otherwise.}\end{cases}$$

Let b be a positive integer such that $ba \equiv 1 \pmod{wm}$. By Theorem 3.3 we have

$$aq(a, m) \equiv F(b) \equiv F(b + wm) \pmod{m}.$$

There exists a p-integral number Y such that $X = b + wmY$. Since for $1 \leqslant j \leqslant a-1$, $0 \leqslant r \leqslant \phi(m) - 1$ we have

$$\begin{aligned}(jX)^{\phi(m)-r} &= (jb + jwmY)^{\phi(m)-r} \\ &\equiv (jb)^{\phi(m)-r} + (\phi(m) - r)\, j^{\phi(m)-r} b^{\phi(m)-r-1} wmY \pmod{m^2},\end{aligned}$$

the number $wmG(b)$ is p-integral and

$$F(X) \equiv F(b) + wmG(b)\, Y \pmod{m}.$$

Setting $X = b + wm$, we get

$$F(b) \equiv F(b + wm) \equiv F(b) + wmG(b) \pmod{m};$$

hence $wmG(b) \equiv 0 \pmod{m}$ and we are done. ∎

To obtain an expression for $aq(a, m)$ for a general modulus m we use another statement of Lerch [9, (5)].

PROPOSITION 3.5 (Lerch). *Let $m = m_1 \cdots m_k$, where $k \geqslant 1$ and $m_1 \geqslant 2, \ldots, m_k \geqslant 2$ are pairwise relatively prime integers, and let a be an integer with $(a, m) = 1$. For $1 \leqslant r \leqslant k$ let $n_r = m/m_r$ and $n'_r \in \mathbb{Z}$ such that $n_r^2 n'_r \equiv 1 \pmod{m_r}$. Then*

$$q(a, m) \equiv \sum_{r=1}^{k} n_r n'_r \phi(n_r)\, q(a, m_r) \pmod{m}.$$

This statement and Corollary 3.4 give us the following result.

THEOREM 3.6. *Let $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be the prime factorization of an integer $m \geqslant 2$, and let a be a positive integer, $(m, a) = 1$. Then*

$$aq(a, m) \equiv -\phi(m) \sum_{r=1}^{k} \frac{n_r n'_r}{\phi(m_r)^2} \sum_{j=1}^{a-1} \left(B_{\phi(m_r)}\left(\frac{j}{a}\right) - B_{\phi(m_r)} \right) \pmod{m},$$

where $m_r = p_r^{\alpha_r}$, $n_r = m/m_r$, and $n'_r \in \mathbb{Z}$ such that $n_r^2 n'_r \equiv 1 \pmod{m_r}$ $(1 \leqslant r \leqslant k)$.

4. FURTHER CONGRUENCES FOR EULER QUOTIENTS

In this section we will use Lerch's Theorem 2.3 to generalize a congruence of E. Lehmer [11, (45)] for base 2. This is done in Proposition 4.3. As important ingredients in the proof we require congruences for Euler quotients and sums of powers that are of independent interest. The properties (3.2) and (3.1) of the Bernoulli numbers and polynomials are again used as essential tools.

PROPOSITION 4.1. *Let p be a prime, $a, n \in \mathbb{Z}$, $n \geqslant 1$, and $p \nmid a$. Then we have*

(a) *for $p = 2$,*

$$q(a, 2^{n+1}) = q(a, 2^n) + 2^{n-1} q(a, 2^n)^2;$$

(b) *for $p = 3$,*

$$q(a, 3^{n+1}) = q(a, 3^n) + 3^n q(a, 3^n)^2 + 3^{2n-1} q(a, 3^n)^3;$$

(c) *for $p \geqslant 5$,*

$$q(a, p^{n+1}) \equiv q(a, p^n) + p^n \frac{p-1}{2} q(a, p^n)^2 \pmod{p^{2n}}.$$

Proof. Suppose $p \geqslant 5$. Put $x = a^{p^{n-1}(p-1)}$ and $q = q(a, p^n)$. Then $x = 1 + qp^n$ and $x^r \equiv 1 + rp^n q + (r(r-1)/2)\, p^{2n} q^2 \pmod{p^{2n+1}}$ for $0 \leqslant r \leqslant p-1$. Hence, $\sum_{r=0}^{p-1} x^r \equiv p + (p(p-1)/2)\, p^n q \pmod{p^{2n+1}}$. We have now

$$p^{n+1} q(a, p^{n+1}) = x^p - 1 = (x-1) \sum_{r=0}^{p-1} x^r = qp^n \sum_{r=0}^{p-1} x^r.$$

Consequently,

$$q(a, p^{n+1}) \equiv q + p^n \frac{p-1}{2} q^2 \pmod{p^{2n}}.$$

The equalities (a) and (b) can be shown in a similar way. ∎

LEMMA 4.2. *Let p be an odd prime and n a positive integer. Put $c = p^n(p-1) - 1$ and*

$$S = \sum_{\substack{y=1 \\ p \nmid y}}^{(p^{n+1}-1)/2} y^c, \qquad \sigma = \sum_{\substack{y=1 \\ p \nmid y}}^{(p^n-1)/2} y^c.$$

Then

$$S \equiv \sigma \pmod{p^{2n}} \qquad \textit{when} \quad p \geqslant 5,$$

$$S \equiv \sigma + p^{2n-1} \pmod{p^{2n}} \qquad \textit{when} \quad p = 3.$$

Proof. First we show

$$\sum_{x=1}^{p^n-1} x^c \equiv \begin{cases} 0 \pmod{p^{2n}}, & \text{if} \quad p \geqslant 5, \\ p^{2n-1} \pmod{p^{2n}}, & \text{if} \quad p = 3. \end{cases} \tag{4.1}$$

Using identities (3.2), (3.1), and the von Staudt–Clausen theorem, we have

$$\begin{aligned} \sum_{x=1}^{p^n-1} x^c &= \frac{1}{c+1} \sum_{j=0}^{c} \binom{c+1}{j} B_j (p^n)^{c+1-j} \\ &\equiv \frac{1}{c+1} \left[\binom{c+1}{c} B_c p^n + \binom{c+1}{c-1} B_{c-1} p^{2n} \right. \\ &\quad \left. + \binom{c+1}{c-2} B_{c-2} p^{3n} \right] \pmod{p^{2n}} \\ &= \frac{c}{2} B_{c-1} p^{2n}; \end{aligned}$$

the last equality follows from the fact that c is odd and $c \geqslant 5$. For $p \geqslant 5$ we have $c-1 \not\equiv 0 \pmod{p-1}$, so the congruence (4.1) is valid. For $p = 3$, $pB_{c-1} \equiv -1 \pmod{p}$ by the von Staudt–Clausen theorem; hence,

$$\frac{c}{2} B_{c-1} p^{2n} \equiv p^{2n-1} \pmod{p^{2n}}.$$

Now we show that with the exception of the case $p = 3$, $n = 1$,

$$\sum_{\substack{x=1 \\ p \nmid x}}^{p^n-1} x^{c-1} \equiv 0 \pmod{p^n}. \tag{4.2}$$

Let r be a primitive root mod p^n. Since $\phi(p^n) = p^{n-1}(p-1)$ does not divide $c-1$, we have

$$\sum_{\substack{x=1 \\ p \nmid x}}^{p^n-1} x^{c-1} \equiv \sum_{j=0}^{\phi(p^n)-1} (r^{c-1})^j = \frac{(r^{c-1})^{\phi(p^n)} - 1}{r^{c-1} - 1} \equiv 0 \pmod{p^n}.$$

Since $c-1$ is even, this gives

$$\sum_{\substack{x=1\\ p\nmid x}}^{(p^n-1)/2} x^{c-1} \equiv \begin{cases} 1 \pmod{p^{2n}}, & \text{for } p=3;\ n=1,\\ 0 \pmod{p^{2n}}, & \text{otherwise.}\end{cases} \tag{4.3}$$

We obtain from (4.1), (4.2), and (4.3) for $p \geqslant 5$,

$$\begin{aligned} S &= \sum_{k=0}^{(p-3)/2} \sum_{\substack{x=1\\ p\nmid x}}^{p^n-1} (x+kp^n)^c + \sum_{\substack{x=1\\ p\nmid x}}^{(p^n-1)/2} \left(x+\frac{p^n(p-1)}{2}\right)^c \\ &\equiv \sum_{k=0}^{(p-3)/2} \sum_{\substack{x=1\\ p\nmid x}}^{p^n-1} (x^c + cx^{c-1}kp^n) + \sum_{\substack{x=1\\ p\nmid x}}^{(p^n-1)/2} \left(x^c + cx^{c-1}\frac{p^n(p-1)}{2}\right) \\ &\equiv \sigma \pmod{p^{2n}}. \end{aligned}$$

Analogously for $p=3$ and $n \neq 1$,

$$S \equiv p^{2n-1} + \sigma \pmod{p^{2n}}.$$

The case $p=3, n=1$ can be calculated separately. This proves the lemma. ∎

Using Lerch's Theorem 3.2 for base $a=2$, we have for an odd prime p and a positive integer n,

$$2q(2, p^{n+1}) \equiv -S \pmod{p^{n+1}}.$$

With Proposition 4.1 and Lemma 4.2 we now obtain the following generalization of congruence (45) in Emma Lehmer's paper [11].

PROPOSITION 4.3. *Let p be an odd prime and n a positive integer. Then*

$$\sum_{\substack{x=1\\ p\nmid x}}^{(p^n-1)/2} \frac{1}{x} \equiv -2q(2, p^n) + p^n q(2, p^n)^2 \pmod{p^{n+1}}.$$

Now we investigate the image $q((\mathbb{Z}/m^2\mathbb{Z})^\times)$ under the homomorphism $q: (\mathbb{Z}/m^2\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z}, +)$ induced by the Euler quotient $q(x, m)$ (see Proposition 2.1(b) with $\alpha=2$).

PROPOSITION 4.4. *let* $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ *be the prime factorization of the integer* $m \geqslant 2$ *and* q *the homomorphism from* $(\mathbb{Z}/m^2\mathbb{Z})^\times$ *into* $(\mathbb{Z}/m\mathbb{Z}, +)$ *induced by the Euler quotient of* m. *For* $1 \leqslant r \leqslant k$ *put* $m_r = p_r^{\alpha_r}$ *and*

$$d_r = \begin{cases} (m_r, 2\prod_{j=1}^{k}(p_j - 1)), & \text{when} \quad m_r = 2^{\alpha_r};\ \alpha_r \geqslant 2, \\ (m_r, \prod_{j=1}^{k}(p_j - 1)), & \text{otherwise.} \end{cases}$$

Let $d = \prod_{r=1}^{k} d_r$. *Then the image* $q((\mathbb{Z}/m^2\mathbb{Z})^\times)$ *equals* $\{td + m\mathbb{Z}\colon\ 0 \leqslant t \leqslant (m/d) - 1\}$; *it is therefore isomorphic to* $(\mathbb{Z}/(m/d)\,\mathbb{Z}, +)$ *for* $m > 2$.

Proof. I. First we prove the proposition for the case $m = p^\beta$, where p is a prime and β is a positive integer.

(a) Suppose $p = 2$. Since $q(3, 2) = 1$ we may assume $\beta \geqslant 2$. Let a be an odd integer. Then $a = 2k + 1$ for some $k \in \mathbb{Z}$ and $q(a, 4) = k(k+1) \equiv 0 \pmod 2$. Using Proposition 4.1(a) and induction on β, we have proven that $q(a, 2^\beta)$ is even.

We show by induction that, given a $\beta \geqslant 2$, there exists an odd integer a with $q(a, 2^\beta) \equiv 2 \pmod{2^\beta}$. This is true for $\beta = 2$ since $q(3, 4) = 2$. Assuming it holds for some β, we use Proposition 4.1(a) to obtain $q(a, 2^{\beta+1}) \equiv 2 \pmod{2^\beta}$. Hence $(q(a, 2^{\beta+1}), 2^{\beta+1}) = 2$ and there exists a positive integer n with the property $nq(a, 2^{\beta+1}) \equiv 2 \pmod{2^{\beta+1}}$. Finally, using the logarithmic property (Proposition 2.1(a)) we obtain $q(a^n, 2^{\beta+1}) \equiv 2 \pmod{2^{\beta+1}}$.

(b) Suppose p is odd. Then $q(p+1, p) \equiv -1 \pmod p$, therefore $p \nmid q(p+1, p)$. Assume that there exists an integer a, $p \nmid a$, with $p \nmid q(a, p^\beta)$. By Proposition 4.1(b), (c) we have $p \nmid q(a, p^{\beta+1})$, so there exists a positive integer n with $nq(a, p^{\beta+1}) \equiv 1 \pmod{p^{\beta+1}}$. According to the logarithmic property (Proposition 2.1(a)) we have now $q(a^n, p^{\beta+1}) \equiv 1 \pmod{p^{\beta+1}}$.

II. For $1 \leqslant r \leqslant k$ we set $n_r = m/m_r$ and $n_r' \in \mathbb{Z}$ with $n_r^2 n_r' \equiv 1 \pmod{m_r}$.

(a) Let $a \in \mathbb{Z}$, $(a, m) = 1$, and let $1 \leqslant w \leqslant k$. If $1 \leqslant r \leqslant k$, $r \neq w$, then $m_w \mid n_r$, so $d_w \mid n_r n_r' \phi(n_r)$. If p_w is odd, or $p_w = 2$ and $\alpha_w = 1$, then $d_w \mid \phi(n_w)$. If $p_w = 2$ and $\alpha_w \geqslant 2$, then according to I, $q(a, m_w)$ is even and $d_w \mid n_w n_w' \phi(n_w)\, q(a, m_w)$. So in all cases we have $d_w \mid q(a, m)$ by Lerch's Proposition 3.5, and hence $d \mid q(a, m)$.

(b) Denote by $\bar{d}$ the greatest common divisor of $\{n_r n_r' \phi(n_r)\colon\ 1 \leqslant r \leqslant k\} \cup \{m\}$. Then there exist integers X_r such that

$$\sum_{r=1}^{k} n_r n_r' \phi(n_r)\, X_r \equiv \bar{d} \pmod m.$$

We have now three cases:

(i) There exists $1 \leqslant w \leqslant k$ such that $2 = p_w$, $\alpha_w \geqslant 2$ and

$$2^{\alpha_w} \nmid \prod_{j=1}^{k} (p_j - 1).$$

(ii) There exists $1 \leqslant w \leqslant k$ such that $2 = p_w$, $\alpha_w \geqslant 2$ and

$$2^{\alpha_w} \mid \prod_{j=1}^{k} (p_j - 1).$$

(iii) All other cases (i.e., $4 \nmid m$).

In cases (ii) and (iii) we have $d = \bar{d}$, and in case (i), $d = 2\bar{d}$.

According to I there exist integers, a_r, $p_r \nmid a_r$, for $1 \leqslant r \leqslant k$ with the properties

$$q(a_r, m_r) \equiv \begin{cases} X_r & \text{in case (iii)} \\ 2X_r & \text{in case (i)} \\ & \\ X_r & \text{in case (ii) for } r \neq w \\ 0 & \text{in case (ii) for } r = w \end{cases} \pmod{m_r}.$$

Let $a \in \mathbb{Z}$, $a \equiv a_r \pmod{m_r^2}$ for each $1 \leqslant r \leqslant k$. By Proposition 2.1(b) we have $q(a, m_r) \equiv q(a_r, m_r) \pmod{m_r}$ and according to Lerch's Proposition 3.5 we get $q(a, m) \equiv d \pmod{m}$, which completes the proof. ∎

COROLLARY 4.4. *The map* $q: (\mathbb{Z}/m^2\mathbb{Z})^\times \to \mathbb{Z}/m\mathbb{Z}$ *induced by the Euler quotient has kernel of order* $d\phi(m)$.

5. WIEFERICH NUMBERS

The aim of this final section is to characterize all Wieferich numbers $m \geqslant 2$ for a fixed base $a (a \in \mathbb{Z}, (a, m) = 1)$. This will be done by means of Wieferich primes. We begin by introducing two lemmas.

LEMMA 5.1. *Let* p *be a prime and* x, N *integers,* $N \geqslant 0$. *Let* $x \equiv 1 \pmod{p}$ *if* p *is odd and* $x \equiv 1 \pmod{4}$ *if* $p = 2$. *Then*

$$\operatorname{ord}_p(x^{p^N} - 1) = \operatorname{ord}_p(x - 1) + N.$$

Proof. It suffices to prove the statement for $N=1$; the general case follows by an easy induction on N. If p is odd, there exists an integer z such that $x=1+zp$, and then $x^r \equiv 1+rzp \pmod{p^2}$ for $0 \leqslant r \leqslant p-1 (r \in \mathbb{Z})$. Therefore,

$$\sum_{r=0}^{p-1} x^r \equiv p \pmod{p^2},$$

and the congruence is satisfied also for $p=2$. Now since

$$x^p - 1 = (x-1) \prod_{r=0}^{p-1} x^r,$$

we have

$$\operatorname{ord}_p(x^m - 1) = \operatorname{ord}_p(x-1) + 1$$

and the result follows. ∎

COROLLARY 5.2. *Let $n \geqslant 1$ and a be integers, p be a prime with $p \nmid a$, and in the case $p=2$ let $a \equiv 1 \pmod 4$. Then*

$$\operatorname{ord}_p q(a, p^n) = \operatorname{ord}_p q(a, p).$$

In particular, p^n is a Wieferich number with base a if and only if $\operatorname{ord}_p q(a, p) \geqslant n$.

Proof. Using Lemma 5.1 we obtain

$$\begin{aligned} \operatorname{ord}_p q(a, p^n) &= \operatorname{ord}_p(a^{p^{n-1}(p-1)} - 1) - n \\ &= \operatorname{ord}_p(a^{p-1} - 1) - 1 = \operatorname{ord}_p q(a, p). \end{aligned}$$ ∎

LEMMA 5.3. *Let x and N be integers, $N \geqslant 1$, $x \equiv 3 \pmod 4$. Then*

$$\operatorname{ord}_2(x^{2^N} - 1) = \operatorname{ord}_2(x+1) + N.$$

Proof. Obviously $\operatorname{ord}_2(x-1) = \operatorname{ord}_2(x^{2^n}+1) = 1$ for each positive integer n. For $N=1$ the lemma is valid. Now let $N \geqslant 2$ and suppose that the statement holds for $N-1$. Since

$$x^{2^N} - 1 = (x^{2^{N-1}} - 1)(x^{2^{N-1}} + 1),$$

we have

$$\begin{aligned} \operatorname{ord}_2(x^{2^N} - 1) &= \operatorname{ord}_2(x^{2^{N-1}} - 1) + \operatorname{ord}_2(x^{2^{N-1}} + 1) \\ &= \operatorname{ord}_2(x+1) + (N-1) + 1. \end{aligned}$$ ∎

Notation. Let p be a prime and a an integer with $p \nmid a$. Put

$$\sigma(a, p) = \operatorname{ord}_p q(a, p) = \operatorname{ord}_p(a^{p-1} - 1) - 1 \qquad \text{if} \quad p \text{ is odd},$$

$$\sigma(a, 2) = \begin{cases} \operatorname{ord}_2 q(a, 2) = \operatorname{ord}_2(a-1) - 1 & \text{if} \quad a \equiv 1 \pmod 4, \\ \operatorname{ord}_2 \dfrac{a+1}{2} = \operatorname{ord}_2(a+1) - 1 & \text{if} \quad a \equiv 3 \pmod 4. \end{cases}$$

PROPOSITION 5.4. *Let m and a be relatively prime integers, $m \geqslant 3$, and $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be the prime factorization of m. Let $1 \leqslant j \leqslant k$ and $p = p_j$. Then*

$$\operatorname{ord}_p q(a, m) = \operatorname{ord}_p \left(\prod_{i=1}^{k} (p_i - 1) \right) + \sigma(a, p).$$

Proof. Put $\pi = \operatorname{ord}_p(\prod_{i=1}^{k} (p_i - 1))$, $\alpha = \alpha_j$, $b = a^{p^\pi \phi(p^\alpha)} = a^{\phi(p^{\alpha+\pi})}$. Then $\phi(m) = p^\pi \phi(p^\alpha) X$, where X is a positive integer with $p \nmid X$. Since

$$a^{\phi(m)} - 1 = b^X - 1 = (b-1) \sum_{r=0}^{X-1} b^r,$$

$b \equiv 1 \pmod p$ and $\sum_{r=0}^{X-1} b^r \equiv X \not\equiv 0 \pmod p$, we have

$$\operatorname{ord}_p(a^{\phi(m)} - 1) = \operatorname{ord}_p(b-1) = \sigma(a, p) + \alpha + \pi,$$

according to Lemmas 5.1 and 5.3. (Put $x = a^{p-1}$ and $N = \alpha + \pi - 1$). Therefore,

$$\operatorname{ord}_p q(a, m) = \operatorname{ord}_p(a^{\phi(m)} - 1) - \alpha = \sigma(a, p) + \pi$$

and we are done. ∎

The next theorem, our main criterion for a number m being a Wieferich number, is an easy consequence of Proposition 5.4.

THEOREM 5.5. *Let m and a be relatively prime integers, $m \geqslant 3$, and $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be the prime factorization of m. Then the following statements are equivalent*:

(a) *m is a Wieferich number with base a*;

(b) $\operatorname{ord}_{p_j} \prod_{i=1}^{k} (p_i - 1) + \sigma(a, p_j) \geqslant \alpha_j$ *for all* $1 \leqslant j \leqslant k$.

The following assertion is clear.

PROPOSITION 5.6. *The integer $m=2$ is a Wieferich number with base a (a odd) if and only if $a \equiv 1 \pmod 4$.*

Now we state some corollaries to Theorem 5.5.

COROLLARY 5.7. *Let p be an odd prime, n a positive integer, and a an integer not divisible by p. If p^n is a Wieferich number with base a then p^r is also a Wieferich number with base a for $1 \leqslant r \leqslant n$.*

COROLLARY 5.8. *Let a be an odd integer and n a positive integer. Put*

$$\varepsilon = \begin{Bmatrix} 1, & \text{if} \quad a \equiv 1 \pmod 4 \\ 2, & \text{if} \quad a \equiv 3 \pmod 4 \end{Bmatrix}; \qquad \beta = \operatorname{ord}_2((a+(-1)^{\varepsilon})/2).$$

Then 2^n is a Wieferich number with base a if and only if $\varepsilon \leqslant n \leqslant \beta$.

COROLLARY 5.9. *Let a and m be relatively prime integers, $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ the prime factorization of m, $k \geqslant 2$, and $p_j < p_k$ for all $1 \leqslant j \leqslant k-1$. If m is a Wieferich number with base a, then p_k^n is a Wieferich number with base a for each integer n, $1 \leqslant n \leqslant \alpha_k$.*

This implies, in particular, that the largest prime factor of a Wieferich number (with base a) must be a Wieferich prime (with base a).

COROLLARY 5.10. *Let m_1 and m_2 be relatively prime Wieferich numbers with base a ($a \in \mathbb{Z}$, $(a, m_1 m_2) = 1$). Then $m_1 m_2$ is a Wieferich number with base a.*

6. EXAMPLES

1. We will list all known Wieferich numbers with base 2 by means of the two known Wieferich primes 1093 and 3511.

Let $P = 1093$ and $Q = 3511$. For these primes we have

$$\operatorname{ord}_P q(2, P) = \operatorname{ord}_Q p(2, Q) = 1,$$

$$P - 1 = 2^2 \cdot 3 \cdot 7 \cdot 13; \qquad Q - 1 = 2 \cdot 3^3 \cdot 5 \cdot 13.$$

According to Theorem 5.5, the following integers are Wieferich numbers with base 2:

$$P,\ 3\cdot P,\ 3^i\cdot 7\cdot P,\ 3^i\cdot 13\cdot P \qquad (0\leqslant i\leqslant 2),$$

$$3^j\cdot 7\cdot 13\cdot P,\ 3^j\cdot Q,\ 3^j\cdot 5\cdot Q \qquad (0\leqslant j\leqslant 3),$$

$$3^k\cdot 13\cdot Q,\ 3^k\cdot 5\cdot 13\cdot Q,\ 3^k\cdot P\cdot Q,\ 3^k\cdot 5\cdot P\cdot Q \qquad (0\leqslant k\leqslant 4),$$

$$3^l\cdot 7\cdot P\cdot Q,\ 3^l\cdot 5\cdot 7\cdot P\cdot Q \qquad (0\leqslant l\leqslant 5),$$

$$3^l\cdot 13^n\cdot P\cdot Q,\ 3^l\cdot 5\cdot 13^n\cdot P\cdot Q \qquad (0\leqslant l\leqslant 5,\ 1\leqslant n\leqslant 2),$$

$$3^m\cdot 7\cdot 13^n\cdot P\cdot Q,\ 3^m\cdot 5\cdot 7\cdot 13^n\cdot P\cdot Q \qquad (0\leqslant m\leqslant 6,\ 1\leqslant n\leqslant 2).$$

These are altogether 104 Wieferich numbers with base 2; there can be no others less than the next Wieferich prime.

2. According to Montgomery's table in [12], only two pairs (a, p) have the property

$$a^{p-1}\equiv 1 \pmod{p^3}$$

for primes $11\leqslant p<2^{32}$ and integers $2\leqslant a\leqslant 99$ with $p\nmid a$. These pairs are (42, 23) and (68, 113). We therefore choose the bases 42 and 68 as our next examples.

2.1. For base $a=42$ only $p=23$ is known to have the property $q(a, p)\equiv 0 \pmod{p}$. Therefore the only Wieferich numbers with base 42 below 2^{32} are

$$23,\ 23^2,\ 11\cdot 23,\ 11\cdot 23^2,\ 5\cdot 11\cdot 23,\ 5\cdot 11\cdot 23^2.$$

2.2. For $a=68$ the primes below 2^{32} satisfying $q(a, p)\equiv 0 \pmod{p}$ are 5, 7, 19, 113, and 2741. So in this case there will be essentially more Wieferich numbers. We use again Theorem 5.5. First observe that 5 has the same property as 113, namely $q(68, 5)\equiv 0 \pmod{25}$, so that

$$\sigma(68, p)=\begin{cases}1 & \text{for } p=7, 19, 2741,\\ 2 & \text{for } p=5, 113.\end{cases}$$

Also

$$112=2^4\cdot 7, \qquad 2740=2^2\cdot 5\cdot 137, \qquad 136=2^3\cdot 17,$$

but $17\mid 68$, so the prime 17 will not occur in the construction. Denote by M the set of integers

$$3^i\cdot 7,\ 3^j\cdot 19,\ 113^x,\ 3^k\cdot 7\cdot 19,\ 3^i\cdot 7^y\cdot 113^x,$$

$$3^j\cdot 19\cdot 113^x,\ 3^k\cdot 7^y\cdot 19\cdot 113^x,$$

where $0 \leqslant i \leqslant 1$, $0 \leqslant j \leqslant 2$, $0 \leqslant k \leqslant 3$, $1 \leqslant x, y \leqslant 2$. The set M contains 41 integers ($\geqslant 7$). Further, set $A = \{5, 5^2\}$ and $B = \{2741, 2741 \cdot 137\}$. Then

$$a, b, m, ab, am, bm, abm, 5^3 b, \qquad \text{and} \qquad 5^3 bm$$

($a \in A$, $b \in B$, $m \in M$) are Wieferich numbers with base 68. The largest one among these is

$$3^3 \cdot 5^3 \cdot 7^2 \cdot 19 \cdot 113^2 \cdot 137 \cdot 2741 = 15,066,415,764,437,625.$$

There can be no other Wieferich numbers with base 68 below the next prime p (after 2^{32}) satisfying $q(68, p) \equiv 0 \pmod{p}$.

3. For the remaining nonpower bases a, $2 \leqslant a \leqslant 99$, we list in Table I the numbers $N_1(a)$ of all Wieferich numbers generated by the corresponding Wieferich primes to base a (taken from [12]), if this was possible with a reasonable amount of computing time and memory (otherwise, an asterisk is shown). In the third columns, $N_2(a)$ denotes the number of those that are less than 4×10^9: this was done to allow a comparison of the counts in a fixed interval.

ACKNOWLEDGMENTS

We thank Andrew Granville for his helpful remarks and for giving the present proof of Theorem 2.4. We also thank Chris Turner for constructing an algorithm and for computing the entries of Table I. Most of this work was prepared while the second and third authors were visiting the Science University of Tokyo in Noda, Chiba, Japan, in the Spring of 1994. They thank the Department of Mathematics for the support and hospitality received.

REFERENCES

1. M. Abramowitz and I. A. Stegun, "Handbook of Mathematical Functions," National Bureau of Standards, Washington, 1964.
2. T. Agoh, K. Dilcher, and L. Skula, Wilson quotients for composite moduli, *Math. Comp.*, to appear.
3. H. F. Baker, Remark on the Eisenstein–Sylvester extension of Fermat's theorem, *Proc. London Math. Soc. (2)* **4** (1906), 131–135.
4. R. E. Crandall, K. Dilcher, and C. Pomerance, A search for Wieferich and Wilson primes, *Math. Comp.* **66** (1997), 433–449.
5. L. E. Dickson, "History of the Theory of Numbers. Vol 1. Divisibility and Primality," Chelsea, New York, 1962.
6. Z. Franco and C. Pomerance, On a conjecture of Crandall concerning the $qx + 1$ problem, *Math. Comp.* **64** (1995), 1333–1336.
7. W. Keller, New prime solutions p of $a^{p-1} \equiv 1 \pmod{p^2}$, *AMS Abstracts* **9**, No. 6 (1988), 503.

8. M Lerch, Zur Theorie des Fermatschen Quotienten $(a^{p-1}-1)/p = q(a)$, *Math. Ann.* **60** (1905), 471–490.
9. M. Lerch, Sur les théorèmes de Sylvester concernant le quotient de Fermat, *C. R. Acad. Sci. Paris* **142** (1906), 35–38.
10. D. H. Lehmer, On Fermat's quotient, base two, *Math. Comp.* **36** (1981), 289–290.
11. E. Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, *Ann. of Math.* **39** (1938), 350–360.
12. P. L. Montgomery, New solutions of $a^{p-1} \equiv 1 \pmod{p^2}$, *Math. Comp.* **61** (1993), 361–363.
13. P. Ribenboim, "The Book of Prime Number Records," Springer-Verlag, New York, 1988.
14. P. Ribenboim, "The Little Book of Big Primes," Springer-Verlag, New York, 1991.
15. J. Sauerberg and L. Shu, Fermat quotients over function fields, preprint, 1995.
16. J. J. Sylvester, Sur une propriété des nombres premiers qui se rattache au théorème de Fermat, *C. R. Acad. Sci. Paris* **52** (1861), 161–163.
17. A. Wieferich, Zum letzten Fermat'schen Theorem, *J. Reine Angew. Math.* **136** (1909), 293–302.