MATHEMATICS OF COMPUTATION
VOLUME 64, NUMBER 209
JANUARY 1995, PAGES 363–392

A NEW CRITERION FOR THE FIRST CASE OF FERMAT'S LAST THEOREM

KARL DILCHER AND LADISLAV SKULA

Dedicated to Paulo Ribenboim

ABSTRACT. It is shown that if the first case of Fermat's last theorem fails for an odd prime l, then the sums of reciprocals modulo l, $s(k, N) = \sum 1/j$ $(kl/N < j < (k+1)l/N)$ are congruent to zero mod l for all integers N and k with $1 \le N \le 46$ and $0 \le k \le N-1$. This is equivalent to $B_{l-1}(k/N) - B_{l-1} \equiv 0 \pmod{l}$, where B_n and $B_n(x)$ are the nth Bernoulli number and polynomial, respectively. The work can be considered as a result on Kummer's system of congruences.

1. INTRODUCTION

The first case of Fermat's last theorem (FLT I) for the prime l is a conjecture stating that there are no integers x, y, and z with the property $x^l + y^l + z^l = 0$ provided $l \nmid xyz$.

Many criteria, going in various directions, concerning (FLT I) have been established; see, e.g., Ribenboim's book [21]. One of these directions deals with the Fermat quotients

$$q_l(p) = \frac{p^{l-1} - 1}{l}.$$

In his famous paper [32], Wieferich showed that if (FLT I) fails for the prime l, then $q_l(2) \equiv 0 \pmod{l}$. This result was extended to other primes p, most recently to all primes p up to 89 by Granville and Monagan [12].

The aim of this article is to replace the notion of the Fermat quotient by special sums $s(k, N)$ defined by

$$s(k, N) = \sum_{j=[kl/N]+1}^{[(k+1)l/N]} j^{l-2} \tag{1.1}$$

for integers N and k with $1 \le N \le l-1$ and $0 \le k \le N-1$. According to Fermat's little theorem we have

$$s(k, N) \equiv \sum_{j=[kl/N]+1}^{[(k+1)l/N]} \frac{1}{j} \pmod{l}. \tag{1.2}$$

Received by the editor April 20, 1992 and, in revised form, October 19, 1993.
1991 *Mathematics Subject Classification.* Primary 11D41; Secondary 11B68, 15A15, 11Y40.

0025-5718/95 $1.00 + $.25 per page

These sums are linked to the Fermat quotients by a theorem of Lerch [17, equation (8)], which we state in the following equivalent form:

$$Nq_l(N) \equiv \sum_{k=0}^{N-1} ks(k, n) \pmod{l}. \tag{1.3}$$

The Fermat quotient $q_l(N)$ is therefore a "linear combination" of the sums $s(k, N)$. The results quoted above, together with the "logarithmic property" of the Fermat quotients (see (2.1) below), show that if (FLT I) is false for the prime l, then the left-hand side of (1.3) is zero (modulo l) for all $N < l$ with prime divisors of at most 89.

In this paper we shall prove the following somewhat surprising result:

Main Theorem. *If the first case of Fermat's last theorem fails for the prime l, then*

$$s(k, N) \equiv 0 \pmod{l} \tag{1.4}$$

for all $1 \leq N \leq 46$ and $0 \leq k \leq N-1$.

We note that in view of (1.2) and some basic properties of the Bernoulli polynomials $B_m(x)$ we can rewrite (1.4) as

$$B_{l-1}\left(\frac{k}{N}\right) - B_{l-1} \equiv 0 \pmod{l}; \tag{1.5}$$

here, B_m is the mth Bernoulli number.

The proof of our main theorem is based on the main result in [25] (see Theorem 4.6 below), which was formulated in a more abstract form. The hypotheses of this result are verified through extensive calculations, thus leading to our main theorem.

Closely related to the main theorem is the following result of Cikánek [7]: There exists an integer L such that for every prime $l > L$ for which $(\text{FLT I})_l$ fails, we have $s(k, N) \equiv 0 \pmod{l}$ for all $2 \leq N \leq 94$ and $0 \leq k \leq N-1$.

In §2 we quote some results on Fermat quotients. Section 3 contains some earlier results related to the main theorem, and in §4 we quote results from the literature necessary for our proofs. Section 5 contains the central part of the proof of the main theorem. Section 6 deals with a sequence of determinants and associated polynomials, which are central to this paper, and in §§7 and 8 we give details of the computations. Based on the main theorem, we make some probability considerations in §9. In §10, finally, we state some consequences of our main theorem, partly based on further computations.

In view of the latest developments concerning Fermat's last theorem, we wish to point out that the greater part of this paper is of independent interest. In fact, our main theorem can be stated as a result on Kummer's system of congruences, without reference to FLT I:

Theorem 1.2. *If τ and $1-\tau$ are nontrivial solutions (i.e., $\not\equiv 0, \pm 1 \pmod{l}$) of order greater than 16 of the system $(K)_l$ of congruences, then*

$$s(k, N) \equiv 0 \pmod{l}$$

for all $1 \leq N \leq 46$ and $0 \leq k \leq N-1$.

For references concerning $(K)_l$, see §4. Remarks on the proof of Theorem 1.2 can be found in §5.3.

2. Fermat quotient criteria

Throughout this paper, l denotes an odd prime. We also use the notation $(\text{FLT I})_l$ for the first case of Fermat's last theorem for the prime l.

We recall that for integers a not divisible by l, the Fermat quotient $q_l(a)$ of l with base a is defined to be the integer

$$q_l(a) = \frac{a^{l-1} - 1}{l}.$$

The following "logarithmic property" was first observed by Eisenstein [10, p. 41; Werke, p. 710]: If a and b are integers not divisible by l, then

$$q_l(ab) \equiv q_l(a) + q_l(b) \pmod{l}. \tag{2.1}$$

Wieferich [32] was the first to use Fermat quotients in a criterion for (FLT I); he proved the following celebrated result.

Theorem 2.1 (Wieferich, 1909). *If* $(\text{FLT I})_l$ *is false, then* $q_l(2) \equiv 0 \pmod{l}$.

This theorem was extended by Mirimanoff [18] and Vandiver [29].

Theorem 2.2 (Mirimanoff, 1910). *If* $(\text{FLT I})_l$ *is false, then* $q_l(3) \equiv 0 \pmod{l}$.

Theorem 2.3 (Vandiver, 1914). *If* $(\text{FLT I})_l$ *is false, then* $q_l(5) \equiv 0 \pmod{l}$ *and*

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{[l/5]} \equiv 0 \pmod{l}.$$

These results have since been further extended by several authors (see [21]). More recently, the following result was proved in [12].

Theorem 2.4 (Granville and Monagan, 1988). *If* $(\text{FLT I})_l$ *is false, then* $q_l(p) \equiv 0 \pmod{l}$ *for all primes* $p \leq 89$.

Using their result together with a method proposed by Gunderson [14], Granville and Monagan [12] show that $(\text{FLT I})_l$ is true for all odd primes up to 7×10^{14} and a little beyond. Still using Theorem 2.4, but now by improving Gunderson's method, Tanner and Wagstaff [28] got a new bound larger than 1.56×10^{17}, and then Coppersmith [8] made significant changes in Gunderson's method to get the following result:

Theorem 2.5 (Coppersmith, 1990). *If* $(\text{FLT I})_l$ *is false, then*

$$l > 7.568 \times 10^{17}. \tag{2.2}$$

3. Related results

We assume throughout that N is an integer, $1 \leq N \leq l - 1$. First we show that the cases $1 \leq N \leq 6$ of the main theorem are easy consequences of the results quoted in the previous section. Indeed, we note that for all odd primes l we have

$$s(0, 1) \equiv 0 \pmod{l}; \tag{3.1}$$

this follows easily from the fact that the summands in (1.2) run through the sequence $1, 2, \dots, l-1 \pmod{l}$. It is also easy to see from (1.2) that for $0 \le k \le N-1$ we have

$$s(k, N) \equiv -s(N-1-k, N) \pmod{l}; \tag{3.2}$$

we note that (3.1) is an immediate consequence of (3.2).

Taking into account these relations as well as Lerch's formula (1.3) and the "logarithmic property" (2.1), we obtain from the theorems of Wieferich, Mirimanoff, and Vandiver the following result.

Theorem 3.1. *If* $(\text{FLT I})_l$ *is false, then* $s(k, N) \equiv 0 \pmod{l}$ *for* $1 \le N \le 6$ *and* $0 \le k \le N-1$.

Remarks. (a) This result was observed for $N = 2, 3, 4$, and 6 by Emma Lehmer in 1938 [16] in her investigations of $q_l(2)$ and $q_l(3)$ modulo l^2.

(b) Lerch's formula (1.3) for $N = 2$ can be easily obtained from the following formula observed by Eisenstein (1850) ([9, p. 21], or Math. Werke, p. 710):

$$2q_l(2) \equiv 1 - \frac{1}{2} + \frac{1}{3} - \cdots + \frac{1}{l-2} - \frac{1}{l-1} \pmod{l}. \tag{3.3}$$

A further result in the direction of our main theorem is due to the second author [25, Theorem 5.5].

Theorem 3.2 (Skula). *If* $(\text{FLT I})_l$ *is false, then* $s(k, N) \equiv 0 \pmod{l}$ *for* $N \in \{2, 3, \dots, 10\} \cup \{12\}$ *and* $0 \le k \le N-1$.

In [25] a theory concerning the sums $s(k, N)$ was developed; the Main Theorem (4.14) there (see Theorem 4.6 below) was used to prove the above result. The necessary calculations were done "by hand". In the present paper we use the same theorem from [25], amended by a more recent result of Granville [13], to prove our main theorem; here the calculations were done with computers.

Next we prove a representation of $s(k, N)$ as sums of inverses modulo l that differs from (1.2). For any integer n we denote by $\eta(n)$ the least positive residue $n/l \pmod{N}$.

Proposition 3.3. *For* $1 \le v \le N$ *we have*

$$s(\eta(v) - 1, N) \equiv -N \sum \frac{1}{n} \pmod{l}, \tag{3.4}$$

where the sum runs through all n, $1 \le n \le l-1$, *with* $n \equiv v \pmod{N}$.

Proof. (i) Let $L = \{1, 2, \dots, l-1\}$ and

$$A(v) = \{n \in L \mid n \equiv v \pmod{N}\},$$
$$B(v) = \{j \in \mathbb{Z} \mid (\eta(v) - 1)l/N < j < \eta(v)l/N\}.$$

For $n \in A(v)$, let $\psi(n)$ denote the least positive residue of $-n/N \pmod{l}$. Clearly, ψ is an injection from $A(v)$ to L. We show that ψ is a bijection from $A(v)$ onto $B(v)$. Put

$$w = \begin{cases} q & \text{for } v < \rho, \\ q-1 & \text{for } v \ge \rho, \end{cases}$$

where $l = Nq + \rho$, q and ρ are integers, $1 \leq \rho \leq N-1$. Then for $n \in A(v)$ we have $n = v + hN$, where $0 \leq h \leq w$. Since

$$n \equiv N\left(h + \frac{v - \eta(v)\rho}{N} - \eta(v)q\right) \pmod{l},$$

we have

$$\psi(n) \equiv -nN^{l-2} \equiv \eta(v)q - h + \frac{\eta(v)\rho - v}{N} \pmod{l}.$$

Therefore,

$$\psi(n) \equiv \frac{l}{N}\eta(v) - h - \frac{v}{N} \pmod{l}.$$

Since

$$\frac{l}{N}(\eta(v) - 1) < \frac{l}{N}\eta(v) - w - \frac{v}{N} \leq \frac{l}{N}\eta(v) - h - \frac{v}{N} < \frac{l}{N}\eta(v),$$

we get $\psi(n) \in B(v)$. The identities

$$\bigcup_{v=1}^{N} A(v) = \bigcup_{v=1}^{N} B(v) = L$$

now imply that ψ is a bijection from $A(v)$ to $B(v)$.

(ii) We have now

$$-N \sum_{\substack{n=1 \\ n \equiv v \pmod{N}}}^{l-1} \frac{1}{n} = -N \sum_{n \in A(v)} \frac{1}{n} \equiv \sum_{n \in A(v)} \frac{1}{\psi(n)} \pmod{l}$$

$$= \sum_{x \in B(v)} \frac{1}{x} \equiv s(\eta(v) - 1, N) \pmod{l}.$$

This completes the proof. □

By means of the identity (3.4) and Lerch's formula (1.3) we can express the Fermat quotient as follows.

Corollary 3.4. *For* $2 \leq N \leq l-1$ *we have*

$$q_l(N) \equiv -\sum_{n=1}^{l-1} \frac{\eta(n)}{n} \pmod{l}.$$

This congruence was stated (without proof) by Sylvester [27] for the case where N is a prime different from l. In general, it is in fact due to Glaisher [11].

4. Summary of known results

In this section we shall state the known results that will be used in the proof of our main theorem. Concepts that are not needed will not be explained here; the reader may wish to consult the original papers.

1. One of the cornerstones in the study of the first case of Fermat's last theorem is the "Kummer system of congruences" $(K)_l$ introduced by Kummer [15] in his work on (FLT I). This system can be formulated as follows:

$$(K)_l \qquad B_{2j}\varphi_{l-2j}(t) \equiv 0 \pmod{l}, \qquad 1 \le j \le \frac{l-3}{2},$$

where B_{2j} is the $(2j)$th Bernoulli number and $\varphi_i(t)$ the Mirimanoff polynomial (see, e.g., [21, p. 139 ff.]). In the same article [15], Kummer stated his famous criterion:

Theorem 4.1 (Kummer, 1857). *If x, y, and z are relatively prime integers, if l does not divide xyz, and if $x^l + y^l + z^l = 0$, then any integer $-\tau$ with the property $x\tau \equiv -y \pmod{l}$ is a solution of $(K)_l$. (We may also add that $-\tau$ is a solution of $\varphi_{l-1}(t) \equiv 0 \pmod{l}$).*

2. Pollaczek [20] also made important contributions in this area. He proved the following for the integer τ from Kummer's theorem 4.1 (see [12, §4]).

Theorem 4.2 (Pollaczek, 1917). *Let i, j, and k be the orders $\pmod{l}$ of τ, $1-\tau$, and $\tau/(\tau-1)$, respectively. Then none of the numbers ij, ik, jk is less than $3(\log l)/(\log \alpha)$, where $\alpha = (1+\sqrt{5})/2$.*

In his paper [20], Pollaczek used a special matrix $A_n(t)$ (in the notation of [12]) of size $2\varphi(n) \times \varphi(n)$, for integers $n \ge 2$. The entries of $A_n(t)$ are powers of t. Let $\rho(n, t)$ denote the rank of $A_n(t)$ for an integer t, considered over the Galois field $\mathbb{Z}/l\mathbb{Z}$. Then $\rho(n, t) \le \varphi(n)$. In [12, §§8, 9] this matrix was replaced by a new matrix $A_n^*(t)$, and the rank of $A_n^*(t)$ was calculated. From the definition of $A_n^*(t)$ in [9] it can be deduced that if $A_n^*(t)$ has full rank modulo l, then $A_n(t)$ has full rank modulo l, or $t^d - 1 \equiv 0 \pmod{l}$ for certain t (see also [25, (5.1.1)], where these numbers d are explicitly determined). In summary, we have

Proposition 4.3. *Let t be an integer, not divisible by l, with order greater than 16. Then $\rho(n, t) = \varphi(n)$ for $2 \le n \le 18$ and $n = 20, 22$. Furthermore, $\rho(19, t) = \varphi(19)$, with the possible exception of those t that have order 17 and 18, and $\rho(21, t) = \varphi(21)$, with the possible exception of t with order 17, 19, or 20.*

3. In order to formulate the main result from [25], which will be needed for our goals, we have to introduce a special matrix $D_N(t)$ from [25, equation 4.13]:

Definition 4.4. Let N be an integer, $N \ge 3$. For integers μ and ν with $\gcd(\mu, N) = \gcd(\nu, N) = 1$, let $r(\mu, \nu)$ denote the least positive residue of $\nu/\mu \pmod{N}$; i.e., $r(\mu, \nu)$ is the integer with $0 < r(\mu, \nu) < N$ and $\mu r(\mu, \nu) \equiv \nu \pmod{N}$. Then for a variable t, define the matrix $D_N(t)$ by

$$D_N(t) = [t^{r(\mu,\nu)-1} + t^{N-1-r(\mu,\nu)}]$$

$(1 \le \mu, \nu < N/2, \gcd(\mu, N) = \gcd(\nu, N) = 1)$. Note that $D_N(t)$ is a square matrix of order $\varphi(N)/2$; here, φ denotes the Euler totient function.

We can now state the main theorem from [25], which will be the central ingredient in the proof of our main theorem. It was originally stated and proved for another system of congruences introduced in [24], equivalent in a certain sense to the Kummer system $(K)_l$.

Theorem 4.5 (Skula). *Let N be an integer with $N \geq 2$ and $(N-2)(N-1)/2 \leq l$, and let $-\tau$ be a solution of the system $(K)_l$ and of the congruence $\varphi_{l-1}(t) \equiv 0 \pmod{l}$, $\tau \not\equiv 0 \pmod{l}$. Assume that the following conditions are satisfied:*

(a) $\det D_M(\tau) \not\equiv 0 \pmod{l}$ *for each integer M with $M \geq 3$ and $M|N$;*

(b) $\rho(n, \tau) = \varphi(n)$ *for each integer n, $2 \leq n < N/2$.*

Then $s(k, N) \equiv 0 \pmod{l}$ for each $0 \leq k \leq N-1$.

Remark. Using a different method, Granville [13] proved this result with condition (a) replaced by

(a′) $\det D_N(\tau) \not\equiv 0 \pmod{l}$.

This will simplify our calculations for certain N in §§7 and 8.

5. Proof of the Main Theorem

1. Suppose that $(\text{FLT I})_l$ is false. Then there exist integers x_1, x_2, x_3 such that

$$x_1^l + x_2^l + x_3^l = 0 \quad \text{and} \quad l \nmid x_1 x_2 x_3 . \tag{5.1}$$

By Coppersmith's result (Theorem 2.5) we may assume that $l > 7.568 \times 10^{17}$. For $1 \leq i, j \leq 3$ and $i \neq j$, let τ_{ij} be an integer with the property

$$x_i \tau_{ij} \equiv -x_j \pmod{l}. \tag{5.2}$$

Then it is easy to see from (5.2) that

$$\tau_{ij}\tau_{ji} \equiv 1 \pmod{l}, \tag{5.3}$$

$$\tau_{ij} + \tau_{ik} \equiv 1 \pmod{l} \qquad (j \neq k), \tag{5.4}$$

$$\tau_{ij} \not\equiv 0 \pmod{l} \quad \text{and} \quad \tau_{ij} \not\equiv 1 \pmod{l}. \tag{5.5}$$

Lemma 5.1. *There exist different pairs a and b of integers $i \neq j$, $1 \leq i, j \leq 3$, such that the orders of τ_a and τ_b are greater than 16 and*

$$\tau_b \equiv 1 - \tau_a \pmod{l}. \tag{5.6}$$

Proof. With (5.3) and (5.4) we see that τ_{21}, τ_{23}, and τ_{31} can be written in the form τ, $1-\tau$, and $\tau/(\tau-1)$. Lemma 4.2 now implies that at least two of them have orders not less than $(3(\log l)/(\log \alpha))^{1/2}$, which means orders greater than 16, by (2.2). The same is true for the triple τ_{12}, τ_{13}, and τ_{32}; i.e., at least two of them have order greater than 16. In summary, out of the three possible values of the index i there will always be one for which (5.4) holds, such that the orders of τ_{ij} and τ_{ik} are greater than 16. This proves the lemma. □

2. By Kummer's criterion (Theorem 4.1) and the discussion in subsection 1, $-\tau_a$ and $-\tau_b$ are solutions of the system $(K)_l$ of congruences and of the congruence $\varphi_{l-1}(t) \equiv 0 \pmod{l}$.

Hence, by Theorem 4.5 and the remark following it, the proof is complete if we can verify conditions (a′) and (b). Condition (b) is satisfied by Lemma 5.1 and Proposition 4.3, unless

$$\begin{aligned} &t^d \equiv 1 \pmod{l} \quad \text{for } d = 17 \text{ or } 18 \text{ and } N = 39, \ldots, 42, \text{ or} \\ &t^d \equiv 1 \pmod{l} \quad \text{for } d = 17, 18, 19 \text{ or } 20 \text{ and } N = 43, \ldots, 46. \end{aligned} \tag{5.7}$$

For condition (a′) we will try to show that either $l \nmid \det D_N(t)$ or $l \nmid \det D_N(1-t)$ for all $t \in \mathbb{Z}$. Hence, if there is a nonzero integer c such that

$$u(t) \det D_N(t) + v(t) \det D_N(1-t) = c, \tag{5.8}$$

where u and v are polynomials with integer coefficients, then the proof is complete, with the possible exception of those l which divide c.

However, as N gets larger, the constant c becomes increasingly difficult or impossible to factor. To deal with these cases, we note that it is apparent from the proof of Theorem 4.5 (i.e., Theorem 4.14 in [25]) that what is really needed is that the matrix $\widetilde{D}_N(t)$, formed by stacking $D_N(t)$ on top of $D_N(1-t)$, have maximum rank modulo l, namely, rank $\varphi(N)/2$ (see also [13]). Thus, we can choose one or more $\varphi(N)/2 \times \varphi(N)/2$ submatrices of $\widetilde{D}_N(t)$ different from $D_N(t)$ and $D_N(1-t)$ and find a new constant c' (and, if necessary, a third one, c'') by combining a new pair of determinants according to (5.8). The actual exceptional primes are then only the prime divisors of $\gcd(c, c')$ (or of $\gcd(c, c', c'')$).

It turns out that the determinant of $D_N(t)$ has particularly nice, and for computational purposes useful, properties. The next section, therefore, is devoted to studying the polynomials $\det D_N(t)$.

3. We now wish to show that Theorem 1.2 does not depend on the assumption that $(\text{FLT I})_l$ is false. This result follows again from Theorem 4.5. Lemmas 5.1 and 4.2 are not needed because of the assumption that τ and $1-\tau$ have orders greater than 16. An important computational tool throughout this paper is the Wieferich test, which is normally stated as a criterion for (FLT I) (see Theorem 2.1). However, Skula [23] proved the following version:

If there exists a solution τ of the system $(K)_l$ such that $\varphi_{l-1}(\tau) \equiv 0 \pmod{l}$ and $\tau \not\equiv 0, 1 \pmod{l}$, then $q_l(2) \equiv 0 \pmod{l}$.

Hence we may continue to use the Wieferich test. In other places we deal with certain exceptional primes by simply stating that they are smaller than the Coppersmith bound (Theorem 2.5); these primes can also be dealt with using the Wieferich test.

Finally, we have to explain the absence of the congruence $\varphi_{l-1}(\tau) \equiv 0 \pmod{l}$ in Theorem 1.2. This is due to the following result of Agoh [1, Theorem 1]:

If we omit one congruence from the system of congruences $(K)_l$ augmented by $\varphi_{l-1}(\tau) \equiv 0 \pmod{l}$, then we obtain an equivalent system of congruences.

In particular, we may omit the congruence in question. We thus have to add the hypothesis $\tau \not\equiv -1 \pmod{l}$ (-1 is never a solution of $\varphi_{l-1}(\tau) \equiv 0 \pmod{l}$, but counts as "trivial solution" of $(K)_l$).

6. The polynomials $F_N(t)$

1. Theorem 4.5 and §5 indicate that the determinant of the matrix $D_N(t)$ plays an essential role in the proof of our main theorem. We begin with a definition.

Definition 6.1. For an integer $N \geq 3$, put $F_N(t) = \det D_N(t)$, with $D_N(t)$ as in Definition 4.4.

It is clear that $F_N(t)$ is a polynomial in t with integer coefficients. We derive now some further properties.

Proposition 6.2. (a) *The polynomial $F_N(t)$ has leading coefficient* 1 *and degree* $(N-2)\varphi(N)/2$.

(b) *$F_N(t)$ is a reciprocal polynomial.*

Proof. (a) The entries on the main diagonal of $D_N(t)$ are all equal to $t^{N-2}+1$; they have the highest degree of all the entries of $D_N(t)$. This implies (a).

(b) We have

$$t^{(N-2)\varphi(N)/2}F_N\left(\frac{1}{t}\right) = \det t^{N-2}[t^{1-r(\mu,\nu)} + t^{1+r(\mu,\nu)-N}]_{\mu,\nu}$$

$$= \det[t^{N-1-r(\mu,\nu)} + t^{r(\mu,\nu)-1}]_{\mu,\nu} = F_N(t). \quad \square$$

Proposition 6.3. *The polynomial $F_N(t)$ is divisible in $\mathbb{Z}[t]$ by the following polynomials:*

(a) $(t-1)^{\varphi(N)-2}$;

(b) $(t+1)^{\varphi(N)-2}$ *if N is even,*

(c) $(t+1)^{\varphi(N)/2}$ *if N is odd.*

Proof. (a) We subtract the first row from the others. Then the (μ, ν)-entry has the form $\psi(t) = t^{r(\mu,\nu)-1} + t^{N-1-r(\mu,\nu)} - t^{\nu-1} - t^{N-1-\nu}$ $(\mu > 1)$. This polynomial is divisible by $(t-1)^2$; therefore $(t-1)^{\varphi(N)-2} | F_N(t)$.

(b) If N is even, we consider again the polynomial $\psi(t)$ from (a). We may suppose that $r(\mu, \nu) = z > \nu$. Then

$$\psi(t) = t^{\nu-1}(t^{z-\nu}-1) - t^{N-1-z}(t^{z-\nu}-1) = (t^{z-\nu}-1)(t^{\nu-1} - t^{N-1-z}).$$

Since z and ν are both odd, we have $\nu - 1 \equiv N-1-z \pmod 2$, and therefore $(t+1)^2 | \psi(t)$; hence $(t+1)^{\varphi(N)-2} | F_N(t)$.

(c) If N is odd, the sum of exponents of t in each entry of $D_N(t)$ is odd; therefore $t+1$ divides each entry, and the result follows. $\square$

Remark. We can see from Table 1 (next page) that the powers in Proposition 6.3 of the factors $t-1$ and $t+1$ are the exact powers for $3 \le N \le 46$. Also, Proposition 6.3 is closely related to Theorem 6.4 below.

2. For the next result we introduce the following notation. Let E denote the group of even Dirichlet characters modulo N. For $\chi \in E$, put

$$F_\chi(t) = \sum_{\substack{j=1 \\ (j,N)=1}}^{N-1} \chi(j) t^{j-1}. \tag{6.1}$$

Define the matrix $B = [\chi(\nu)]_{\nu,\chi}$, where $1 \le \nu < N/2$ with $\gcd(\nu, N) = 1$, and $\chi \in E$. Then B is a square matrix of order $\varphi(N)/2$, and it is easy to see that $\det B \neq 0$ (see, e.g., [5, p. 420, Problem 5]; as domain for each even Dirichlet character mod N consider the quotient group $(\mathbb{Z}/N\mathbb{Z})^*/\{-1, 1\}$).

Theorem 6.4. *There holds*

$$F_N(t) = \prod_{\chi \in E} F_\chi(t). \tag{6.2}$$

Proof. Fix $\chi \in E$ and $1 \le \mu < N/2$ with $\gcd(\mu, N) = 1$. Then, since $r = r(\mu, \nu)$ runs through a reduced residue system modulo N as ν does, we have

$$\sum_{\substack{\nu=1 \\ (\nu,N)=1}}^{N/2} (t^{r(\mu,\nu)-1} + t^{N-1-r(\mu,\nu)})\chi(\nu) = \chi(\mu) \sum_{\substack{r=1 \\ (r,N)=1}}^{N/2} (t^{r-1} + t^{N-1-r})\chi(r)$$

$$= \chi(\mu) F_\chi(t);$$

TABLE 1. The polynomials $F_N(t)$

N	d	cd	nd	degrees of noncyclotomic irreducible factors	cyclotomic factors
7	15	11	4	4	$(t^6-1)(t^2-1)^2(t-1)$
8	12	12	0	/	$(t^8-1)(t^4-1)$
9	21	17	4	4	$(t^9-1)(t^3-1)(t^2-1)^2(t+1)$
10	16	16	0	/	$(t^{12}-1)(t^4-1)$
11	45	21	24	24	$(t^{10}-1)(t^2-1)^4(t-1)^3$
12	20	20	0	/	$(t^{12}-1)(t^8-1)$
13	66	26	40	16, 16, 8	$(t^{12}-1)(t^2-1)^5(t-1)^4$
14	36	20	16	8, 8	$(t^8+1)(t^6-1)(t^2-1)^3$
15	52	32	20	8, 6, 6	$(t^8-1)(t^5-1)^2(t^3-1)^3(t^2+1)$ $(t+1)^3$
16	56	48	8	8	$(t^{16}-1)^2(t^8-1)(t^4-1)(t^2-1)^2$
17	120	36	84	48, 24, 12	$(t^{16}-1)(t^2-1)^7(t-1)^6$
18	48	32	16	16	$(t^{18}-1)(t^6-1)(t^4+1)(t^2-1)^2$
19	153	41	112	84, 28	$(t^{18}-1)(t^2-1)^8(t-1)^7$
20	72	64	8	8	$(t^{20}-1)^2(t^{12}-1)(t^4-1)^3$
21	114	46	68	28, 16, 16, 8	$(t^7-1)^3(t^6-1)(t^3-1)^4(t^2-1)^2$ $(t+1)^3$
22	100	36	64	64	$(t^{12}+1)(t^{10}-1)(t^2-1)^7$
23	231	51	180	180	$(t^{22}-1)(t^2-1)^{10}(t-1)^9$
24	88	88	0	/	$(t^{24}-1)^2(t^{12}-1)^2(t^8-1)^2$
25	230	102	128	64, 64	$(t^{25}-1)^2(t^5-1)^6(t^4-1)(t^2-1)^9$
26	144	48	96	40, 40, 16	$(t^{14}+1)(t^{12}-1)(t^6-1)(t^2-1)^8$
27	225	137	88	84, 4	$(t^{27}-1)^3(t^9-1)^4(t^3-1)(t^2-1)^8$ $(t+1)$
28	156	124	32	16, 8, 8	$(t^{28}-1)^3(t^{12}-1)(t^8+1)(t^4-1)^4$ $(t^2-1)^2$
29	378	66	312	144, 144, 24	$(t^{28}-1)(t^2-1)^{13}(t-1)^{12}$
30	112	88	24	24	$(t^{24}-1)(t^{20}-1)^2(t^{12}-1)(t^6-1)^2$
31	435	71	364	208, 104, 52	$(t^{30}-1)(t^2-1)^{14}(t-1)^{13}$
32	240	184	56	48, 8	$(t^{32}-1)^4(t^{16}-1)^2(t^8-1)(t^4-1)$ $(t^2-1)^6$
33	310	108	202	104, 64, 22, 12	$(t^{11}-1)^5(t^{10}-1)(t^6-1)(t^3-1)^9$ $(t^2-1)^2(t+1)^6$
34	256	68	188	112, 48, 28	$(t^{18}+1)(t^{16}-1)(t^6-1)^2(t^2-1)^{11}$
35	396	144	252	80, 52, 40, 40, 22, 18	$(t^{12}-1)(t^8-1)(t^7-1)^9(t^5-1)^{10}$ $(t^2-1)(t+1)^9$
36	204	172	32	16, 16	$(t^{36}-1)^4(t^{12}-1)(t^8-1)(t^2-1)^4$
37	630	86	544	192, 192, 64, 64, 32	$(t^{36}-1)(t^2-1)^{17}(t-1)^{16}$
38	324	68	256	192, 64	$(t^{20}+1)(t^{18}-1)(t^2-1)^{15}$
39	444	148	296	80, 64, 64, 32, 32, 32	$(t^{13}-1)^6(t^{12}-1)(t^6-1)^2(t^4+1)$ $(t^3-1)^{10}(t^2-1)^3(t+1)^6$
40	304	248	56	24, 12, 12, 8	$(t^{40}-1)^4(t^{20}-1)^2(t^{12}-1)(t^8-1)^3$ $(t^6-1)(t^2-1)^3$
41	780	96	684	288, 144, 144, 72, 36	$(t^{40}-1)(t^2-1)^{19}(t-1)^{18}$
42	240	100	140	64, 40, 20, 16	$(t^{14}-1)^3(t^{12}+1)(t^8+1)(t^6-1)^6$ (t^2-1)
43	861	101	760	456, 228, 76	$(t^{42}-1)(t^2-1)^{20}(t-1)^{19}$
44	420	276	144	64, 64, 16	$(t^{44}-1)^5(t^{12}+1)(t^{10}-1)(t^4-1)^5$ $(t^2-1)^7$
45	516	324	192	80, 52, 40, 8, 6, 6	$(t^{45}-1)^4(t^{15}-1)^4(t^9-1)^3(t^8-1)$ $(t^6+t^3+1)^3(t^5-1)^2(t^4-1)(t^2-1)^7$
46	484	84	400	400	$(t^{24}+1)(t^{22}-1)(t^2-1)^{19}$

here we used the fact that $\mu r \equiv \nu \pmod{N}$ implies $\chi(\mu)\chi(r) = \chi(\nu)$. Therefore,

$$D_N(t)B = [\chi(\mu)F_\chi(t)]_{\mu,\chi},$$

where $1 \le \mu < N/2$, $\gcd(\mu, N) = 1$, and $\chi \in E$. Hence,

$$F_N(t)\det B = \det B \prod_{\chi \in E} F_\chi(t),$$

and the proof is complete. (See also [5, p. 421] and [31, Lemma 5.26(a)]). □

Remarks. (1) Among the polynomials $F_\chi(t)$ (for a given N) there is at least one with rational integer coefficients. Indeed, if $\chi = \chi_0$ is the principal character, then

$$F_{\chi_0}(t) = \sum_{\substack{i=1 \\ (j,N)=1}}^{N-1} t^{j-1}.$$

Furthermore, if χ is an even quadratic character, then $F_\chi(t)$ has only coefficients ± 1. For instance, if N is an odd prime $p \equiv 1 \pmod 4$, then

$$F_\chi(t) = \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) t^{j-1},$$

where (j/p) is the Legendre symbol. Polynomials of this kind (with χ not necessarily an even character) are known as Fekete polynomials; see, e.g., [4].

We also note that the $F_\chi(t)$ have other interesting properties which depend on the structure of the character group modulo N. A detailed study is not needed here.

(2) A summary of the properties of $F_N(t)$, $7 \le N \le 46$, is given in Table 1. There, d stands for the degree of $F_N(t)$, cd for the total degree of its cyclotomic factors, and nd for the total degree of its noncyclotomic factors.

3. The following result shows that $F_M(t)$ is a divisor of $F_N(t)$ for certain pairs (M, N).

Proposition 6.5. *Let $M, N \ge 3$ be integers with the same prime divisors, and suppose that $M|N$. Then $F_M(t)|F_N(t)$ in $\mathbb{Z}[t]$.*

Proof. We denote $K := N/M$, $\overline{M} := \{j \in \mathbb{Z} | 1 \le j \le M,\ (j, M) = 1\}$, and $\overline{N} := \{i \in \mathbb{Z} | 1 \le i \le N,\ (i, N) = 1\}$. Then we can rewrite $\overline{N} = \{j + kM | j \in \overline{M},\ 0 \le k \le K - 1\}$. Now we note that an even character χ modulo M can be extended to an even character χ_N modulo N by setting

$$\chi_N(j + kM) = \chi(j) \qquad (j \in \overline{M},\ 0 \le k \le K - 1).$$

Then by (6.1) we have

$$F_{\chi_N}(t) = \sum_{i \in \overline{N}} \chi_N(i) t^{i-1} = \sum_{j \in \overline{M}} \sum_{k=0}^{K-1} \chi(j) t^{j+kM-1}$$

$$= \sum_{j \in \overline{M}} \chi(j) t^{j-1} \sum_{k=0}^{K-1} t^{kM} = F_\chi(t) \frac{t^N - 1}{t^M - 1}.$$

The result now follows from (6.2). □

4. In view of the polynomials (6.1) we need some information on the structure of Dirichlet characters. For details, see, e.g., [30, Chapter 7]. We write N in its canonical representation

$$N = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} .$$

For the sake of simplicity we first assume that $\alpha = 0$ or 1; this is sufficient for our purposes. For $j = 1, \ldots, k$ define

$$c_j := \varphi(p_j^{\alpha_j}) = (p_j - 1) p_j^{\alpha_j - 1} ,$$

and let g_j be the smallest primitive root modulo $p_j^{\alpha_j}$. Furthermore, let ε_j, $1 \le j \le k$, be any (not necessarily primitive) c_jth root of unity. Then

$$\chi(a) = \begin{cases} \varepsilon_1^{\nu_1} \varepsilon_2^{\nu_2} \cdots \varepsilon_k^{\nu_k} & \text{if } (a, m) = 1 , \\ 0 & \text{if } (a, m) > 1 , \end{cases} \tag{6.3}$$

where $\nu_1, \nu_2, \ldots, \nu_k$ are defined by

$$a \equiv g_1^{\nu_1} \pmod{p_1^{\alpha_1}}, \ldots, a \equiv g_k^{\nu_k} \pmod{p_k^{\alpha_k}}, \tag{6.4}$$

is a Dirichlet character modulo N. Conversely, any Dirichlet character modulo N is of the above form.

Now, for the character χ in (6.3) to be even, we need $\chi(-1) = 1$. By (6.4), $a = -1$ corresponds to

$$\nu_j = \frac{1}{2} \varphi(p_j^{\alpha_j}), \qquad j = 1, \ldots, k .$$

But then, with (6.3) we see that only an *even* number of the ε_j, $j = 1, \ldots, k$, can be primitive c_jth roots of unity; the others have to be $(c_j/2)$th roots of unity.

5. Finally, suppose that $N = 2^{\alpha}$, $\alpha \ge 2$. Let $\varepsilon = 1$ or -1, and ε_0 any $(2^{\alpha-2})$th root of unity (not necessarily primitive). Then the function

$$\chi(a) = \begin{cases} \varepsilon^{\nu} \varepsilon_0^{\nu_0} & \text{if } (a, N) = 1 , \\ 0 & \text{if } (a, N) > 1 , \end{cases} \tag{6.5}$$

where ν and ν_0 are (uniquely) defined by

$$a \equiv (-1)^{\nu} 5^{\nu_0} \pmod{2^{\alpha}}, \tag{6.6}$$

is a Dirichlet character modulo $N = 2^{\alpha}$. Conversely, any Dirichlet character modulo 2^{α} $(\alpha \ge 2)$ is of the above form.

Again, for the character χ in (6.5) to be even, we need $\chi(-1) = 1$. By (6.6), $a = -1$ corresponds to $\nu = 1$, $\nu_0 = 0$, and by (6.5) we have $\chi(-1) = \varepsilon = 1$. Hence the *even* characters modulo $N = 2^{\alpha}$ $(\alpha \ge 2)$ are given by

$$\chi(a) = \begin{cases} \varepsilon_0^{\nu_0} & \text{if } (a, N) = 1 , \\ 0 & \text{if } (a, N) > 1 , \end{cases}$$

with ε_0 and ν_0 as before.

7. The computations, Part I. ($N = 11, 13, 14, 15, 16, 18, 20, 21, 24, 28, 30, 36, 40$)

1. The possible exceptional primes l can be calculated in two ways:

(i) by finding the constants c in equation (5.8);

(ii) by using the polynomial factorization in Theorem 6.4 and evaluating resultants, and using, if necessary, other submatrices of $\widetilde{D}_N(t)$.

In this section we shall deal with those cases for which method (i) is practicable. First we note that if we have

$$u_{ij}(t)F_i(t) + v_{ij}(t)G_j(t) = c_{ij}, \qquad 1 \le i \le m,\ 1 \le j \le n, \tag{7.1}$$

with $u_{ij}, v_{ij} \in \mathbb{Z}[t]$ and $c_{ij} \in \mathbb{Z}$, then there are polynomials $u, v \in \mathbb{Z}[t]$ such that

$$u(t)\prod_{i=1}^{m} F_i(t) + v(t)\prod_{j=1}^{n} G_j(t) = \prod_{i=1}^{m}\prod_{j=1}^{n} c_{ij}. \tag{7.2}$$

Indeed, if

$$u(t)F(t) + v_j(t)G_j(t) = c_j, \qquad j = 1, 2,$$

then by multiplying these two equations together we get

$$(u^2F + uv_2G_2 + uv_1G_1)F + (v_1v_2)G_1G_2 = c_1c_2.$$

The assertion (7.2) is now obtained by induction.

By (7.2) it suffices to consider pairs of factors of the polynomials $F_N(t)$, $F_N(1-t)$. Also, by Lemma 5.1, cyclotomic factors of order ≤ 16 can be disregarded.

2. As an example, we describe in detail the calculations for the case $N = 14$. We have

$$D_{14}(t) = \begin{pmatrix} 1+t^{12} & t^2+t^{10} & t^4+t^8 \\ t^4+t^8 & 1+t^{12} & t^2+t^{10} \\ t^2+t^{10} & t^4+t^8 & 1+t^{12} \end{pmatrix},$$

and

$$\begin{aligned} F_{14}(t) &= \det D_{14}(t) \\ &= 1 - 2t^6 - 3t^{10} + 4t^{12} + 3t^{16} - 6t^{18} + 3t^{20} + 4t^{24} - 3t^{26} - 2t^{30} + t^{36} \\ &= (t-1)^4(t+1)^4(1+t+t^2)(1-t+t^2)(1+t^8)f_1(t)f_2(t), \end{aligned}$$

where

$$f_1(t) = 1 + t^2 + 2t^4 + 2t^6 + t^8, \qquad f_2(t) = 1 + 2t^2 + 2t^4 + t^6 + t^8.$$

We note that the cyclotomic factors of $F_{14}(t)$ all have order ≤ 16, so they can be ignored in what follows. We compute now $g_j(t) := f_j(1-t)$:

$$\begin{aligned} g_1(t) &= 7 - 30t + 71t^2 - 104t^3 + 102t^4 - 68t^5 + 30t^6 - 8t^7 + t^8, \\ g_2(t) &= 7 - 26t + 57t^2 - 84t^3 + 87t^4 - 62t^5 + 29t^6 - 8t^7 + t^8. \end{aligned}$$

Using an algorithm for finding the g.c.d. of $f_1(t)$ and $g_1(t)$ (e.g., the routine "gcdex" on MAPLE), we now determine polynomials $u_{11}, v_{11} \in \mathbb{Z}[t]$ such that

$$u_{11}(t)f_1(t) + v_{11}(t)g_1(t) = c_{11}.$$

We get

$$u_{11}(t) = -205242 + 1215982t - 2545873t^2 + 3059783t^3 - 2336540t^4 + 1139405t^5 - 328485t^6 + 43798t^7,$$

$$v_{11}(t) = 42838 + 9854t + 809t^2 - 70943t^3 - 33840t^4 - 88257t^5 - 21899t^6 - 43798t^7,$$

and

$$c_{11} = 94582 = 2 \times 19^2 \times 131.$$

Similarly, we find u_{12}, v_{12}, u_{22}, v_{22}, and

$$c_{12} = 688383001 = 43 \times 181 \times 241 \times 367, \qquad c_{22} = 58519 = 139 \times 421.$$

Now, the exceptional primes are the factors of the c_{ij}, namely, 2, 19, 43, 131, 139, 181, 241, 367, 421. But (FLT I) is certainly true for these prime exponents (e.g., since they are all below the bound (2.2)). This concludes the proof of the main theorem for $N = 14$.

3. We dealt with the other cases for N (namely, 11, 13, 15, 16, 18, 20, 21, 24, 28, 30, 36, 40) in exactly the same way. The symbolic manipulation package MAPLE was used to evaluate the determinants, to do the polynomial calculations, and to factor the numbers c_{ij}. Most prime factors are less than the bound (2.2). Those larger than that bound are listed in Table 2; for these primes l we checked that the Fermat quotient $q_l(2) \not\equiv 0 \pmod{l}$. This completes the proof of our main theorem for the N under consideration in this section, with the exception of $N = 40$.

TABLE 2. Exceptional primes

N	exceptional primes
13	1938181974650674321837
	1919161201375463453526 1
	1997528240063703162013213
17	518306729572832193774907228949910023 6729
19	186753445089142195483237
	400443742545087272981932335515915819000633984233 21
21	1591527325421298297187
	279467626079514592617511
	52444347498467623057551343
	291909291277221022866974626 99
	55281209602509156697788324469
22	138201523840689613021
	4962117726750564486679765262032 21
25	3382717282842812911
	1126441906701735542398248 1
	4716909569298617563477046743185373 1
26	1558482696940606437939347755803338623072153
	5529415957782663330858444568572985814525443

TABLE 2 (continued)

27	8369570580199826563
	447188548098899056249
	22436394034386081908398006877782601066 59
28	7165864476521984353
29	1407041578912351747
	161116934598291994141
	72337923395894981717109479 93
	16474862057340134605674539552845938468575009603
	p194, p238
32	8857981054094232409
	172638455754479209193
	282845710352878213354031
	20456704623491742790395 1873
	12559086499354376212375694 09
	36039036700301240842104507 53
35	39867644621631498545512 3
	64618453953282251628471635368241821
	11023482621077961007075050457019523 73
	11674513443951972931250312022805887230114781826869045784609
38	112212614137195861183
	16828933323639940515090132748894291 69
	p113, p339
41	17096818297220038291908 1
43	74139191281466608291
	204571727151308695753
	2634070735318559967109
	1278405528360764121347
	29379961454664251289579673618989913 9
	81382952490730746402310717889745964057
	11681277008957350992192583814684956295599117
	p202
45	573133270034835821071
	11481509342383088945915281
	81761558598048047482289918427906071686 93
	65134317787788214600157847398128834527 01
	47316028049620874729081544400383811900383955925825774932811557482892 9
46	33029556661758142729
	83074579099762209433276 3631

4. For $N = 40$ we have to exclude the cases listed in equation (5.7). This is done by taking the resultants of $t^{17} - 1$ and $t^{18} - 1$ with the noncyclotomic polynomial factors of $F_{40}(1-t)$ and with the cyclotomic factors of order > 16. These resultants are easy to factor, and all prime factors are less than Coppersmith's bound (2.2). This takes care of condition (a′) of Theorem 4.5. To deal with condition (b), we assume that t has order 17 or 18. The case that

$1-t$ has also order 17 or 18 will be excluded by taking the resultants of $t^{17}-1$ and $(1-t)^{17}-1$, of $t^{17}-1$ and $(1-t)^{18}-1$, and of $t^{18}-1$ and $(1-t)^{18}-1$ (or by finding the corresponding numbers c in (5.8)). Only with respect to the prime divisors of these numbers are the orders of both t and $1-t$ possibly less than 19; but these primes are easy to determine and to exclude, using the Wieferich test. This completes the proof for $N = 40$.

5. One other detail remains to be discussed. The prime factors obtained in most factorization algorithms are only "probable primes". Although they are extremely likely to be primes, we need to address the possibility that they are composite. The following proposition shows that this eventuality poses no probelm if instead of the "straight" Wieferich test (i.e., testing for $q_l \not\equiv 0 \pmod{l}$) we check whether $\gcd(l, q_l(2)) = 1$, for a "probable prime" l.

Proposition 7.1. *Let n be a pseudoprime to base 2 (i.e., a composite number such that $2^{n-1} \equiv 1 \pmod{n}$) and p a prime divisor of n. If $q_n(2) \not\equiv 0 \pmod{p}$, then also $q_p(2) \not\equiv 0 \pmod{p}$.*

Proof. Write $n = mp^k$, where $p \nmid m$, $k \geq 1$. By Fermat's (little) theorem we have

$$2^{p^k} = 2^{p^{k-1}+\varphi(p^k)} = 2^{p^{k-1}}(1+bp^k)$$

for some integer b. Then

$$2^{n-1} = 2^{mp^k-1} = 2^{mp^{k-1}-1}(1+bp^k)^m.$$

Since n is a pseudoprime to base 2, the left-hand side of this last equation is $\equiv 1 \pmod{n}$ and therefore also modulo p. The second term on the right-hand side is also $\equiv 1 \pmod{p}$; hence,

$$2^{mp^{k-1}-1} = 1 + ap \tag{7.3}$$

for some $a \in \mathbb{Z}$. Now we rewrite

$$2^{n-1} = 2^{mp^k-1} = 2^{p-1}(2^{mp^{k-1}-1})^p. \tag{7.4}$$

To obtain a contradiction, suppose that $q_p(2) \equiv 0 \pmod{p}$; i.e., $2^{p-1} = 1+cp^2$ for some $c \in \mathbb{Z}$. Then with (7.3) and (7.4) we get

$$2^{n-1} = (1+cp^2)(1+ap)^p = 1+dp^2$$

for some $d \in \mathbb{Z}$. This contradicts the hypothesis, and the proof is complete. □

Remark. In computing $2^{l-1} \pmod{l^2}$ for the Wieferich test, straightforward exponentiation should be avoided because of the large size of the primes l. (MAPLE, e.g., has a "smart" modular exponentiation routine.)

8. The computations, Part II. ($N = 17, 19, 22, 23, 25, 26, 27, 29, 31$–$35, 37, 38, 39, 41$–$46$)

1. From the discussion in §5.2 it is clear that we have to show that the matrix $\widetilde{D}_N(t)$ has maximal rank $\pmod{l}$. To do this, it suffices to exhibit two submatrices of $\widetilde{D}_N(t)$ such that the resultant of their determinants is not divisible by l. If this resultant is easy to factor, then the prime factors are considered exceptional primes and can be eliminated by applying the Wieferich test. The

computations are done in three main steps:

(a) Because of the convenient factorization (6.2), we first choose the two submatrices $D_N(t)$ and $D_N(1-t)$.

(b) If any resultants from (a) remain unfactored, we combine $D_N(t)$ with the "next easiest" submatrix of $\widetilde{D}_N(t)$ obtained by taking $D_N(t)$ and replacing its first row by the first row of $D_N(1-t)$. Only the prime factors of the gcd of the resultants from (a) and (b) remain exceptional primes.

(c) If this gcd cannot be factored, we combine $D_N(t)$ with some other $\varphi(N)/2 \times \varphi(N)/2$ submatrix of $\widetilde{D}_N(t)$, and take the gcd of this resultant with the unfactored numbers from (b). In some cases, this step may have to be repeated with a different submatrix if the gcd is still too large.

The details follow in the remainder of this section.

2. It is clear from Proposition 6.3 or from (6.1) (using basic properties of Dirichlet characters) that the polynomials $F_\chi(t)$ have some cyclotomic factors. We clear the $F_\chi(t)$ of all cyclotomic polynomials of orders ≤ 16 and rewrite (6.2) as

$$F_N(t) = \widetilde{F}_N(t) \prod_{j=1}^{\varphi(N)/2} f_{N,j}(t) = \widetilde{F}_N(t) F_N^*(t), \tag{8.1}$$

where the $f_{N,j}(t)$ are the corresponding $F_\chi(t)$ cleared of cyclotomic factors of order ≤ 16, and $\widetilde{F}_N(t)$ is the product of all these factors. Then by the discussion at the beginning of §7 it suffices to determine the constants c obtained from

$$u(t)F_N^*(t) + v(t)F_N^*(1-t) = c. \tag{8.2}$$

3. By [12, Lemma 20] the constant c in (8.2) divides the resultant of $F_N^*(t)$ and $F_N^*(1-t)$. By (8.1) and multiplicativity of the resultant we have

$$R_t(F_N^*(t), F_N^*(1-t)) = \prod_{i=1}^{\varphi(N)/2} \prod_{j=1}^{\varphi(N)/2} R_t(f_{N,i}(t), g_{N,j}(t)), \tag{8.3}$$

where $g_{N,j}(t) := f_{N,j}(1-t)$. Since the f's and g's do not, in general, have integer coefficients (but have coefficients in the $(\varphi(N)/2)$th cyclotomic field; see subsection 6 below), we take the norm on both sides of (8.3) and obtain

$$N[R_t(F_N^*(t), F_N^*(1-t))] = \prod\prod N[R_t(f_{N,i}(t), g_{N,j}(t))], \tag{8.4}$$

where the double product is as in (8.3), and the norm is understood as the norm in the $(\varphi(N)/2)$th cyclotomic field. We note that the left-hand side of (8.4) is the $(\varphi(\varphi(N)/2))$th power of the left-hand side of (8.3), since the latter is already a rational integer; however, this is of no further consequence. The factors on the right-hand side of (8.4) are now rational integers, and it is clear that each prime factor of c in (8.2) is a prime factor of some term

$$N[R_t(f_{N,i}(t), g_{N,j}(t))]. \tag{8.5}$$

Hence, it suffices to compute these terms and their factors.

4. Next we note that different terms (8.5) may have identical values. Since $R_t(f(t), g(t))$ and $R_t(g(t), f(t))$ differ at most in sign, it suffices to consider the cases $1 \leq i \leq \varphi(N)/2$ and $i \leq j \leq \varphi(N)/2$. Furthermore, the resultant is

an algebraic integer in the $(\varphi(N))$th cyclotomic field (or in a cyclotomic field of smaller order), as is clear from §§6.3, 6.4. Then the norm, as product of this algebraic integer and its conjugates, will usually coincide with other terms (8.5). Details of this will be given in the discussions of the individual cases.

5. A special case occurs when in §5.1 we have $\tau \equiv 2 \pmod{l}$; in this case the set $\{\tau_{ij} | 1 \leq i, j \leq 3, i \neq j\}$ consists of only three distinct $(\mathrm{mod}\, l)$ elements, namely $\{2, -1, 1/2\}$. Although this case is included in all previous discussions, it will sometimes be useful to treat it separately. It is responsible for some of the smaller factors of the constant c and can therefore be used in the necessary factorization (see Step 15 in the next subsection).

6. For the actual computations, we distinguish between three different cases:
(i) $N = p^\alpha$ or $N = 2p^\alpha$, $\alpha \geq 1$, $p \geq 3$. This covers $N = 17, 19, 22, 23, 25, 26, 27, 29, 31, 34, 37, 38, 41, 43, 46$.
(ii) $N = 2^\alpha$, $\alpha \geq 2$. This covers $N = 32$.
(iii) The remaining cases $N = 33, 35, 39, 42, 44$, and 45.
We begin with case (i); fix such an N. By §6.4 we have

$$\chi(a) = \begin{cases} \varepsilon^{2\nu} & \text{if } (a, m) = 1, \\ 0 & \text{if } (a, m) > 1, \end{cases} \tag{8.6}$$

where ε is a dth root of unity (not necessarily primitive), $d := (p-1)p^{\alpha-1}$, and ν is given by

$$a \equiv g^\nu \pmod{p^\alpha},$$

with g a primitive root (say, the smallest one) modulo p^α. The definition of ν can be rewritten in index notation (see, e.g., [30]) as

$$\nu = \mathrm{ind}_g\, a \pmod{p^\alpha},$$

so that with (6.1) and (8.6) we obtain

$$F_\chi(t) = \sum_{\substack{j=1 \\ (j,N)=1}}^{N-1} \varepsilon^{2\,\mathrm{ind}_g\, j \pmod{p^\alpha}} t^{j-1}. \tag{8.7}$$

Now, as ε runs through all dth roots of unity (d of them), χ runs twice through all even characters modulo N. A convenient way of creating the relevant dth roots of unity is to fix one *primitive* dth root of unity ε and to take $\varepsilon^2, \varepsilon^4, \ldots, \varepsilon^d = 1$. This also gives us a way of numbering the even characters and thus the polynomials (8.7). We denote now

$$F_k(t) := \sum_{\substack{j=1 \\ (j,N)=1}}^{N-1} \varepsilon^{2k\,\mathrm{ind}_g\, j \pmod{p^\alpha}} t^{j-1}, \qquad k = 1, 2, \ldots, d, \tag{8.8}$$

where ε is a fixed primitive dth root of unity. (Note that this is different from $F_N(t)$, as defined in Definition 6.1.) For the computations it is important to note that one can avoid complex arithmetic (and the explicit use of, say, $\varepsilon = e^{2\pi i/d}$) by doing all computations symbolically and reducing modulo $\phi_d(\varepsilon)$ the polynomials in ε that arise, where ϕ_d is the dth cyclotomic polynomial.

We are now ready to summarize the algorithm used.

1. Given N of the form p^α or $2p^\alpha$, determine the smallest primitive root $g \pmod{p^\alpha}$, $d = (p-1)p^{\alpha-1}$, and $\phi_d(\varepsilon)$.
2. Compute the polynomials $F_k(t)$ according to (8.8), $k = 1, 2, \ldots, d/2$.
3. Reduce these polynomials modulo $\phi_d(\varepsilon)$.
4. Divide the polynomials by all cyclotomic factors (in t) of order ≤ 16; let $f_k(t)$, $k = 1, \ldots, d/2$, be the polynomials thus cleared of small cyclotomic factors.
5. Determine $g_k(t)$, $k = 1, \ldots, d/2$.
6. For $j = 1, \ldots, d/2$ and $k = j, \ldots, d/2$, compute the resultants $R_t(f_j(t), g_k(t))$; before this is done, it should be determined which sets of pairs (j, k) would give identical norms of the corresponding resultants (see §§8.3 and 8.6). Denote $r_{j,k}(\varepsilon) := R_t(f_j(t), g_k(t))$; they are polynomials in ε.
7. Reduce the $r_{jk}(\varepsilon)$ modulo $\phi_d(\varepsilon)$ to obtain $\overline{r_{j,k}}(\varepsilon)$; these are polynomials in ε of degree at most $\varphi(d) - 1$.
8. Find the norms of the $\overline{r_{j,k}}(\varepsilon)$. This is best done by computing the resultants $R_\varepsilon(\overline{r_{j,k}}(\varepsilon), \phi_d(\varepsilon))$.
9. Try to factor these last numbers; the prime factors are the exceptional primes, or possible factors of the constant c in (5.8).
10. If Step 9 is successful, apply the Wieferich test to all prime factors exceeding Coppersmith's bound. This completes only the cases $N = 17$ and $N = 26$.
11. In all other cases, compute the noncyclotomic factors with rational integer coefficients of $F_N(t)$ by multiplying together appropriate factors $F_k(t)$ (in (8.8)) and reducing modulo $\phi_d(\varepsilon)$. Include cyclotomic factors of order > 16, and denote them by $\psi_1(t), \ldots, \psi_s(t)$. (Their degrees are listed in Table 1.)
12. Set up the matrix obtained from $D_N(t)$ by replacing its first row by the first row of $D_N(1-t)$; evaluate its determinant and remove small cyclotomic factors.
13. Evaluate the resultants $\rho_1, \ldots, \rho_s$ of the polynomial in Step 12 with the polynomials $\psi_1(t), \ldots, \psi_s(t)$.
14. Find $\gcd(\rho_i, \overline{r_{j,k}}(\varepsilon))$ for all appropriate triples (i, j, k). It turns out that most of these numbers, except at most s of them, are very small.
15. Try to factor the numbers obtained in Step 14. (After dividing by an appropriate $\psi_i(2)$, $i = 1, \ldots, s$, most are squares.)
16. If Step 15 is successful, enter the primes exceeding Coppersmith's bound into Table 2 and apply the Wieferich test. This completes the cases $N = 19, 22, 25, 27, 29, 38$. For $N = 43$, go to Step 20. (Although the cases $N = 17$ and $N = 26$ were already settled in Step 10, we carried out Steps 11–16 for these cases as well; this reduced the number of exceptional primes in Table 2).
17. If Step 15 is not successful for N, choose another $\varphi(N)/2 \times \varphi(N)/2$ submatrix of $\tilde{D}_N(t)$ and compute its determinant. To label these, denote by $D_N(a_1, a_2, \ldots, a_{\varphi(N)/2})$ the matrix whose jth row is the jth row of $D_N(t)$ if $a_j = 1$ and is the jth row of $D_N(1-t)$ if $a_j = 2$. Remove small cyclotomic factors.

18. As in Step 13, evaluate the resultants $\rho_1^*, \dots, \rho_s^*$ of the determinant in Step 17 with the polynomials $\psi_1(t), \dots, \psi_s(t)$ of Step 11.
19. Take the gcd of the resultants ρ_j^* with the numbers obtained in Step 14. We are done if the gcd is 1 or a small prime. We first tried the matrix $D_N(1, 2, 1, 2, \dots)$ in Steps 17–19; this was successful in the cases $N = 23, 31, 37$, and 41. In the remaining cases we had to try again with different matrices. Successful choices were $D_{34}(2, 1, 2, 1, 2, 1, 2, 2)$ and $D_{46}(1, 2, 2, 1, 1, 1, 2, 2, 2, 2, 1)$.
20. For $N = 41, 43$, and 46 we have to take equation (5.7) into account; see also §7.4. This leads to 1, 6, and 2 new exceptional primes exceeding the bound (2.2), respectively. They are also entered in Table 2, and the Wieferich test is applied.

7. One may ask why the above method was not used also for the cases covered by §7. The reason lies in the fact that the resultant in (8.3) is often vastly larger than the constant c in (8.2). For the same reason, in some cases in this section a mixed approach was chosen. It can be described as follows:

1. To avoid the evaluation of the determinant $\det D_N(t)$ and the factoring of the polynomial $F_N(t)$, equations (6.2) and (6.1) (or, in practice, (8.8)) were used to obtain $F_N(t)$ and, by combining appropriate factors $F_\chi(t)$, the irreducible (over $\mathbb{Q}$) factors were found.
2. As far as practicable, the MAPLE routine "gcdex" was used to find the constants c_{ij}, as in §7.
3. Now the method described in the previous subsection was employed to find the terms (8.5).
4. By taking the gcd's of pairs of numbers c_{ij} and numbers of the type (8.5), factors of the c_{ij} are sometimes found, which may lead to a complete or almost complete factorization.

This approach will be illustrated in the next subsection.

8. As an example, we treat the case $N = 22$ in some greater detail. First we note that $d = 10$, $\phi_d(\varepsilon) = \varepsilon^4 - \varepsilon^3 + \varepsilon^2 - \varepsilon + 1$, and $g = 2$ (see also Table 3). We can now compute from (8.8) the polynomials $F_k(t)$, $k = 1, \dots, 5$. For example,

$$F_1(t) = 1 + \varepsilon^8 t^2 + \varepsilon^4 t^4 + \varepsilon^2 t^6 + \varepsilon^6 t^8 + \varepsilon^6 t^{12} + \varepsilon^2 t^{14} + \varepsilon^4 t^{16} + \varepsilon^8 t^{18} + t^{20}.$$

Since ε satisfies $\phi_d(\varepsilon) = 0$, we reduce modulo $\phi_d(\varepsilon)$ and obtain

$$\begin{aligned} F_1(t) = 1 &- \varepsilon^3 t^2 + (-1 + \varepsilon - \varepsilon^2 + \varepsilon^3) t^4 + \varepsilon^2 t^6 - \varepsilon t^8 - \varepsilon t^{12} + \varepsilon^2 t^{14} \\ &+ (-1 + \varepsilon - \varepsilon^2 + \varepsilon^3) t^{16} - \varepsilon^3 t^{18} + t^{20}; \end{aligned}$$

similarly for $F_2(t), \dots, F_5(t)$. Here $F_5(t)$ has only rational integer coefficients, as expected. Now we factor the $F_k(t)$, and get

$$\begin{aligned} F_1(t) = (t-1)^2(t+1)^2\{1 &+ (2 - \varepsilon^3) t^2 + (2 + \varepsilon - \varepsilon^2 - \varepsilon^3) t^4 \\ &+ (2 + 2\varepsilon - \varepsilon^2 - \varepsilon^3) t^6 + (2 + 2\varepsilon - \varepsilon^2 - \varepsilon^3) t^8 \\ &+ (2 + 2\varepsilon - \varepsilon^2 - \varepsilon^3) t^{10} + (2 + \varepsilon - \varepsilon^2 - \varepsilon^3) t^{12} \\ &+ (2 - \varepsilon^3) t^{14} + t^{16}\}; \end{aligned}$$

TABLE 3. Distinct resultants

N	d	$\phi_d(\varepsilon)$	g	distinct resultants
17	16	ε^8+1	3	$(1,1)(1,2)(1,3)^2(1,4)(1,5)^2(1,6)(1,7)^2$ $(1,8)(2,2)^2(2,4)^2(2,6)^4(2,8)^2(4,4)^4$ $(4,8)^4(8,8)^4$
19	18	$\varepsilon^6-\varepsilon^3+1$	2	$(1,1)(1,2)(1,3)(1,4)(1,6)(1,8)^2(1,9)$
22	10	$\varepsilon^4-\varepsilon^3+\varepsilon^2-\varepsilon+1$	2	$(3,3)^3(3,6)^6(3,9)^3(9,9)^6(1,1)(1,2)(1,4)^2$ $(1,5)(5,5)^4$
23	22	$\varepsilon^{10}-\varepsilon^9+\cdots-\varepsilon+1$	5	$(1,1)(1,2)(1,3)(1,5)(1,7)(1,10)^2(1,11)$ $(11,11)^{10}$
25	20	$\varepsilon^8-\varepsilon^6+\varepsilon^4-\varepsilon^2+1$	2	$(1,1)\cdots(1,6)(1,8)(1,9)^2(1,10)(2,2)(2,4)$ $(2,5)(2,8)^2(2,10)(5,5)^4(5,10)^4(10,10)^4$
26	12	$\varepsilon^4-\varepsilon^2+1$	2	$(1,1)\cdots(1,4)(1,5)^2(2,2)(2,3)(2,4)^2(3,3)^2$
27	18	$\varepsilon^6-\varepsilon^3+1$	2	– as for $N=19$ –
29	28	$\varepsilon^{12}-\varepsilon^{10}+\cdots-\varepsilon^2+1$	2	$(1,1)\cdots(1,4)(1,6)\cdots(1,10)(1,12)(1,13)^2$ $(1,14)(2,2)(2,4)(2,6)(2,7)(2,12)^2(2,14)$ $(7,7)^6(7,14)^6(14,14)^6$
31	30	$\varepsilon^8+\varepsilon^7-\varepsilon^5-\varepsilon^4-\varepsilon^3$ $+\varepsilon+1$	3	$(1,1)\cdots(1,3)(1,4)^2(1,5)\cdots(1,7)(1,9)$ $(1,10)(1,11)^2(1,12)(1,14)^2(1,15)(3,3)^2$ $(3,5)(3,6)^2(3,12)^4(3,15)^2(5,5)^4(5,10)^8$ $(5,15)^4(15,15)^8$
32	16	ε^8+1	-	– as for $N=17$ –
34	16	ε^8+1	3	– as for $N=17$ –
37	36	$\varepsilon^{12}-\varepsilon^6+1$	2	$(1,1)\cdots(1,10)(1,12)(1,14)(1,15)(1,16)$ $(1,17)^2(1,18)(2,2)(2,3)(2,4)(2,6)(2,8)$ $(2,9)(2,12)(2,15)(2,16)^2(2,18)(3,3)^3$ $(3,6)^3(3,9)^3(3,12)^3(3,15)^3(3,18)^3(6,6)^3$ $(6,12)^6(6,18)^3(9,9)^6(9,18)^6(18,18)^6$
38	18	$\varepsilon^6-\varepsilon^3+1$	2	– as for $N=19$ –
41	40	$\varepsilon^{16}-\varepsilon^{12}+\varepsilon^8-\varepsilon^4+1$	6	$(1,1)\cdots(1,6)(1,8)(1,9)^2(1,10)(1,11)^2$ $(1,12)\cdots(1,16)(1,18)(1,19)^2(1,20)(2,2)^2$ $(2,4)^2(2,5)(2,6)^2(2,8)^2(2,10)^2(2,16)^2$ $(2,18)^4(2,20)^2(4,4)^2(4,5)(4,8)^2(4,10)^2$ $(4,16)^4(4,20)^2(5,5)^4(5,10)^4(5,15)^8(5,20)^4$ $(10,10)^8(10,20)^8(20,20)^8$
43	42	$\varepsilon^{12}+\varepsilon^{11}-\varepsilon^9-\varepsilon^8+\varepsilon^6$ $-\varepsilon^4-\varepsilon^3+\varepsilon+1$	3	$(1,1)\cdots(1,7)(1,8)^2(1,9)(1,10)(1,12)$ $(1,13)^2(1,14)(1,15)(1,18)(1,20)(1,21)$ $(3,3)^2(3,6)^2(3,7)(3,9)^2(3,18)^4(3,21)^2$ $(7,7)^6(7,14)^{12}(7,21)^6(21,21)^{12}$
46	22	$\varepsilon^{10}-\varepsilon^9+\varepsilon^8-\cdots-\varepsilon+1$	5	– as for $N=23$ –

similarly for $F_2(t), F_3(t), F_4(t)$. Let $f_k(t)$, $k=1,\ldots,4$, be the respective terms in braces. We also get

$$F_5(t)=(1+t+t^2+t^3+t^4)(1-t+t^2-t^3+t^4)(1+t^4)(1-t^4+t^8).$$

The four factors are cyclotomic polynomials of order 5, 10, 8, and 24, respectively. The first three factors may be disregarded (since the orders are ≤ 16); we set

$$f_5(t)=1-t^4+t^8.$$

Next we determine $g_k(t) = f_k(1-t)$, $k = 1, \ldots, 5$. For example,

$$g_1(t) = (16 + 8\varepsilon - 5\varepsilon^2 - 7\varepsilon^3) + (-128 - 64\varepsilon + 40\varepsilon^2 + 56\varepsilon^3)t + \cdots + (122 - \varepsilon^3)t^{14} - 16t^{15} + t^{16}.$$

Before computing the various terms of type (8.5), we determine which sets of pairs (j, k) would give identical values. We introduce the following notation:

$$[j, k] := R_t(f_j(t), g_k(t)), \qquad N(j, k) := N([j, k]).$$

From the fact that ε^2, ε^4, ε^6, and ε^8 are all primitive 5th roots of unity, while $\varepsilon^{10} = 1$, we find with (8.8) and the definition of the norm in the cyclotomic field of order 5 that

$$N(1, 1) = [1, 1][2, 2][3, 3][4, 4],$$

and therefore

$$N(1, 1) = N(2, 2) = N(3, 3) = N(4, 4).$$

Similarly, we have $N(1, 2) = [1, 2][2, 4][3, 1][4, 3]$, which implies $N(1, 2) = N(1, 3) = N(2, 4) = N(3, 4)$; $N(1, 4) = [1, 4][2, 3][3, 2][4, 1]$, hence $N(1, 4) = N(2, 3)$, and we expect this number to be a square; $N(1, 5) = [1, 5][2, 5][3, 5][4, 5]$, hence $N(1, 5) = N(2, 5) = N(3, 5) = N(4, 5)$. Finally, $N(5, 5) = [5, 5]^4$; i.e., $N(5, 5)$ is a fourth power. This covers all $N(j, k)$ with $1 \le j \le k \le 5$, so we have to compute only a set of representatives, say $N(1, 1)$, $N(1, 2)$, $N(1, 4)$, $N(1, 5)$, and $N(5, 5)$. This is denoted in Table 3 as $(1, 1)(1, 2)(1, 4)^2(1, 5)(5, 5)^4$; here, $(i, j)^k$ means that $N(i, j)$ is a kth power of an integer.

The resultants $[j, k]$ were computed using MAPLE. For example, $R_t(f_1(t), g_1(t))$ is a polynomial in ε of degree 87, namely,

$$r_{1,1}(\varepsilon) = 923093284287916500122098117549805625 + \cdots - 523398183742251345117184\varepsilon^{87}.$$

Reduced modulo $\phi_5(\varepsilon)$, this is

$$\overline{r_{1,1}}(\varepsilon) = 187861240755070540672588378908420225 + \cdots - 455396484434167522733374972091035660\varepsilon^3.$$

Finally, to find the norm, we compute $R_\varepsilon(\overline{r_{j,k}}(\varepsilon), \phi_5(\varepsilon))$. This is a number of 143 digits. The numbers $N(1, 2)$, $N(1, 4)$, and $N(1, 5)$ have 140, 139, and 70 digits, respectively. $N(5, 5)$ was not computed, but rather $R_t(f_5(t), g_5(t)) = N(5, 5)^{1/4}$. In a first attempt at factoring, using the MAPLE routine "ifactor" with the "easy" option, we obtained

$$\begin{aligned} N(1, 1) &= 5^6 \times 61^2 \times 191^2 \times 55681^2 \times C_{121}, \\ N(1, 2) &= 5^6 \times C_{136}, \\ N(1, 4)^{1/2} &= 2^6 \times 5^3 \times C_{66}, \\ N(1, 5) &= 5^4 \times 37441 \times 241561 \times P_{62}, \\ N(5, 5)^{1/4} &= 2^8 \times 3^4 \times 5^2 \times 7^2 \times 241, \end{aligned}$$

where C_n, resp. P_n, denotes a composite number, resp. a prime, of n digits.

Using the method described in subsection 7, we have further factored C_{121}, yielding a composite C_{71}. The cofactor C_{61} can be discarded since it is a factor of the resultant in (8.3) but not of the essential constant c in (8.2). Then the elliptic curve method was used to attempt factoring C_{66}, C_{71}, and C_{136}. After using several curves, the first two numbers were completely factored, while only a prime factor P_{11} of C_{136} was found, leaving the composite cofactor C_{125} still unfactored. Hence, we continue with Step 11 of subsection 6.

The polynomial $F_{22}(t)$ has only one noncyclotomic factor in $\mathbb{Z}[t]$, namely, the product $\psi_1(t) = F_1(t) \cdots F_4(t)$. There is also a cyclotomic factor of order 24. Hence,

$$\psi_1(t) = 1 + 7t^2 + 28t^4 + 84t^6 + \cdots + 84t^{58} + 28t^{60} + 7t^{62} + t^{64},$$
$$\psi_2(t) = \phi_{24}(t) = t^8 - t^4 + 1.$$

The determinant in Step 12 is a polynomial of degree 100. We clear it of the factors $(t^2 - 1)^6$ and obtain

$$2 - 20t + 200t^2 - 1240t^3 + \cdots - 1260t^{85} + 196t^{86} - 20t^{87} + t^{88}.$$

The resultant ρ_1 (Step 13) has 228 digits, while $\rho_2 = 2^8 \times 3^6 \times 5^4 \times 7^2 \times 11^8 \times 73 \times 241 \times 2521 \times 963121$. We now evaluate $\gcd(\rho_1, N(i, j))$, $j = 1, 2, 4, 5$. For $j = 2, 4$, and 5 this is very small. For $j = 1$ it turns out that the gcd is divisible by

$$\psi_1(2) = 138\ 201\ 523\ 840\ 689\ 613\ 021$$

and that the quotient is a square. The square root is then easy to factor:

$$\left(\frac{\gcd(\rho_1, N(1, 1))}{\psi_1(2)}\right)^{1/2}$$
$$= 5^3 \times 61 \times 191 \times 55681 \times 2292221 \times 127238511434 \times P_{33},$$

where P_{33} is a prime of 33 digits. $\psi_1(2)$ is also a prime. This completes the proof of the main theorem for $N = 22$, with the possible exception of these two primes which are entered in Table 2 and eliminated by applying the Wieferich test.

9. Case (ii) of subsection 6, i.e., the case $N = 32$, is very similar to Case (i); only the remarks in §6.4 have to be taken into account when setting up the polynomials corresponding to (8.7). The mixed approach discussed in subsection 7 was used; the norms of the resultants were used to factor the numbers obtained by the method of §7.

10. Now we consider the case (iii) of the beginning of subsection 6, i.e., $N = 33, 35, 39, 42, 44$, and 45. There are no entries in Table 3 for these N since the polynomials $F_\chi(t)$ cannot be numbered as in (8.8).

If $N = 33$, we have $p_1 = 3$, $p_2 = 11$, $c_1 = 2$, $c_2 = 10$, ε_1 is a "second root of unity" (± 1), and ε_2 is a 10th root of unity. It follows from §6.3 that

(i) if $\varepsilon_1 = 1$, then ε_2 must be a 5th root of unity;

(ii) if $\varepsilon_1 = -1$, then ε_2 must be a primitive 10th root of unity.

Similarly, for $N = 35$ we have $c_1 = 4$, $c_2 = 6$, ε_1 is a 4th root of unity, and ε_2 is a 6th root of unity. Then

(i) if $\varepsilon_1 = 1$ or -1, then ε_2 must be a 3rd root of unity;
(ii) if $\varepsilon_1 = i$ or $-i$, then ε_2 must be a primitive 6th root of unity.

The remaining cases are set up in a similar manner. In practice, the polynomials $F_\chi(t)$ in all these cases are computed similarly to (8.7), but taking the above remarks and (6.3) into account. From these one can proceed almost exactly as before.

The cases $N = 33, 35,$ and 45 are completed in Step 16. For $N = 39, 42,$ and 44 we have to continue to Step 19, using the matrices $D_{39}(1, 1, 1, 2, 2, 2, 1, 1, 1, 2, 1, 1)$, $D_{42}(2, 1, 1, 2, 2, 2)$, and $D_{44}(1, 2, 1, 2, 1, 2, 1, 2, 1, 1)$, respectively. Step 20 for $N = 39, 42, 44$, and 45 yields only small additional exceptional primes, i.e., primes below Coppersmith's bound (2.2).

9. Probability considerations

1. The main result in [12] (see Theorem 2.4 above) is an extremely restrictive condition on a prime l for which $(\text{FLT I})_l$ fails. This fact was translated into a probability statement in [12, §11]. Similarly, we will use our main theorem to derive an improved (heuristic) probability result for (FLT I) to fail.

We assume in this section that $l > 7.568 \times 10^{17}$ (see (2.2)), and that $1 \le N \le 46$. Our main assumption is that the values of the $s(k, N)$, $0 \le k \le N-1$, are randomly distributed $(\mathrm{mod}\, l)$, subject to the three conditions (3.2), (1.3), and (2.1). For example, (3.2) implies with $N = 1$ and $k = 0$ that $s(0, 1) \equiv 0 \pmod{l}$. With $N = 2$ and $k = 0$ we have $s(0, 2) \equiv -s(1, 2) \pmod{l}$.

2. We will calculate the probability $\beta(N)$ of the statement "$s(k, N) \equiv 0 \pmod{l}$ for each $0 \le k \le N-1$ provided that $s(k, M) \equiv 0 \pmod{l}$ for each integer M, $1 \le M < N$, $M \mid N$, and for each $0 \le k \le M-1$".

Since there are l residue classes $(\mathrm{mod}\, l)$, we have

$$\beta(N) = l^{-b(N)}, \tag{9.1}$$

where $b(N)$ is a nonnegative integer. By the remarks at the end of the previous subsection, we clearly have $b(1) = 0$ and $b(2) = 1$. If N is an odd prime, $N = p$, then conditions (1.3) and (2.1) pose no further restrictions. Hence,

$$b(p) = \frac{1}{2}(p-1) = \frac{1}{2}\varphi(p) \tag{9.2}$$

for an odd prime p.

If N is composite, then the situation is a little more complicated. According to condition (3.2) we need to consider only the sums $s(k, N)$ for $0 \le k < (N-1)/2$. Let $k_0 = 0$, and $1 < k_1 < k_2 < \cdots < k_m < N$ be integers with $\gcd(k_i, N) > 1$ (then $m = N - 1 - \varphi(N)$).

If N is even, then we have the following homogeneous system of linear congruences with unknowns $s(k, N)$:

$$\sum_{k=k_i}^{k_{i+1}-1} s(k, N) \equiv 0 \pmod{l}, \qquad 0 \le i \le \frac{N}{2} - \frac{\varphi(N)}{2} - 1;$$

$$\sum_{k=0}^{N/2-1} (N - 2k - 1)s(k, N) \equiv 0 \pmod{l}$$

and similarly when n is odd. The first system (N even) has $\frac{1}{2}\varphi(N) - 1$ free unknowns, and the other one (N odd) has $\frac{1}{2}\varphi(N) - 2$ free unknowns. This, together with (9.2), gives $b(1) = 0$, $b(2) = 1$, and for $N > 2$

$$b(N) = \begin{cases} \frac{1}{2}\varphi(N) & \text{if } N \text{ is prime,} \\ \frac{1}{2}\varphi(N) - 1 & \text{if } N \text{ is even,} \\ \frac{1}{2}\varphi(N) - 2 & \text{if } N \text{ is odd, composite.} \end{cases} \tag{9.3}$$

3. Let $p(N)$ denote the probability of the assertion "$s(k, M) \equiv 0 \pmod{l}$ for all $1 \leq M \leq N$ and for all $0 \leq k \leq M - 1$". Then we have with (9.1),

$$p(N) = \prod_{M=1}^{N} \beta(M) = l^{-\gamma(N)}, \qquad \gamma(N) = \sum_{M=1}^{N} b(M). \tag{9.4}$$

With (9.3) we now compute $\gamma(46) = 284$.

Let B be an integer larger than all exceptional primes for $1 \leq N \leq 46$. Then the probability that $(\text{FLT I})_l$ fails for at least one $l > B$ is

$$\sum_{l>B} l^{-284} < \int_B^{\infty} x^{-284}\, dx = \frac{1}{283} B^{-283}.$$

Here we can clearly take $B = 7.568 \times 10^{17}$ (Coppersmith's bound), and we obtain a probability of less than 0.7×10^{-5062} for $(\text{FLT I})_l$ to fail for a prime l. This probability is essentially lower than what one can obtain by means of Fermat quotients. For instance, Granville and Monagan's result (Theorem 2.4) gives the term l^{-24}.

10. Concluding remarks

1. The criterion (1.5) can be rewritten in terms of generalized Bernoulli numbers. Indeed, let $B_{\chi,n}$ be the nth generalized Bernoulli number belonging to the residue class character χ modulo N. Then the well-known connection with the ordinary Bernoulli polynomials gives

$$B_{\chi,l-1} = N^{l-2} \sum_{k=0}^{N-1} \chi(k) B_{l-1}\left(\frac{k}{N}\right). \tag{10.1}$$

Since $\sum_{k=0}^{N-1} \chi(k) = 0$, we have

$$B_{\chi,l-1} = N^{l-2} \sum_{k=0}^{N-1} \chi(k) \left\{ B_{l-1}\left(\frac{k}{N}\right) - B_{l-1} \right\} \equiv 0 \pmod{l}$$

by (1.5). Hence we have

Corollary 10.1. *If* $(\text{FLT I})_l$ *fails, then we have* $B_{\chi,l-1} \equiv 0 \pmod{l}$ *for all nontrivial Dirichlet characters* χ *modulo* N, $3 \leq N \leq 46$.

Remarks. (1) Since $B_{\chi,n} = 0$ for odd characters χ and even numbers n, Corollary 10.1 is meaningful only for even characters χ.

(2) Corollary 10.1 is in fact true for the wider class of generalized Bernoulli numbers belonging to a periodic arithmetic function f with period N and

satisfying $f(1)+\cdots+f(N)=0$. These numbers can be defined by (10.1), with f in place of χ.

2. Eisenstein's formula (3.3) and the Wieferich criterion (Theorem 2.1) imply that if $(\text{FLT I})_l$ is false, then the alternating sum on the right-hand side of (3.3) is congruent to zero $(\text{mod}\, l)$. The following corollary can be considered as a generalization; it follows immediately from Proposition 3.3 and the main theorem.

Corollary 10.2. *If* $(\text{FLT I})_l$ *fails, then*

$$\sum_{n=1}^{l-1} \frac{f(n)}{n} \equiv 0 \ (\text{mod}\, l)$$

for all periodic arithmetic functions f *with period* N, $1 \le N \le 46$.

3. In view of the criteria of Wieferich and others (see §2), the Fermat quotients $q_l(a)$ (with $l \nmid a$) have been studied quite extensively, mainly in connection with the congruence $q_l(a) \equiv 0 \ (\text{mod}\, l)$. In the remainder of this section we will discuss some computations done with the sums $s(k, N)$, in relation to Fermat quotients.

First we consider the case $a = 2$. An odd prime l with the property $q_l(2) \equiv 0 \ (\text{mod}\, l)$ is called a Wieferich prime. At present, only two such primes are known: $l = 1093$ and $l = 3511$.

Lerch's congruence (1.3) shows a close relationship between the Fermat quotients and the sums $s(k, N)$. We can use this to prove the following

Proposition 10.3. *Let* l *be an odd prime. Then the following are equivalent*:

(a) l *is a Wieferich prime*;
(b) $s(0, 2) \equiv 0 \ (\text{mod}\, l)$;
(c) $s(0, 4) \equiv 0 \ (\text{mod}\, l)$;
(d) $s(1, 4) \equiv 0 \ (\text{mod}\, l)$;
(e) $s(1, 6) \equiv 0 \ (\text{mod}\, l)$.

Proof. From (1.3) we get, with $N = 2$,

$$s(1, 2) \equiv 2q_l(2) \ (\text{mod}\, l), \tag{10.2}$$

and (3.2) gives

$$s(0, 2) \equiv -2q_l(2) \ (\text{mod}\, l). \tag{10.3}$$

Now we consider $N = 4$. First, by definition of the $s(k, N)$ we have $s(0, 2) = s(0, 4) + s(1, 4)$, and therefore, with (10.3),

$$s(0, 4) + s(1, 4) \equiv -2q_l(2) \ (\text{mod}\, l). \tag{10.4}$$

Furthermore, by (3.2) we have $s(2, 4) \equiv -s(1, 4) \ (\text{mod}\, l)$ and $s(3, 4) \equiv -s(0, 4) \ (\text{mod}\, l)$; hence (1.3) with $N = 4$ gives

$$3s(0, 4) + s(1, 4) \equiv -4q_l(4) \equiv -8q_l(2) \ (\text{mod}\, l), \tag{10.5}$$

where we have used the logarithmic property (2.1). By subtracting (10.4) from (10.5) we obtain

$$s(0, 4) \equiv -3q_l(2) \ (\text{mod}\, l), \tag{10.6}$$

and with (10.4) we get

$$s(1, 4) \equiv q_l(2) \pmod{l}. \tag{10.7}$$

Next we consider $N = 6$. The congruences (1.3) and (3.2) give

$$5s(0, 6) + 3s(1, 6) + s(2, 6) \equiv -6q_l(6) \equiv -6q_l(2) - 6q_l(3) \pmod{l}. \tag{10.8}$$

We rewrite (10.3) as

$$s(0, 6) + s(1, 6) + s(2, 6) \equiv -2q_l(2) \pmod{l}, \tag{10.9}$$

subtract (10.9) from (10.8), and divide by 2, to get

$$2s(0, 6) + s(1, 6) \equiv -2q_l(2) - 3q_l(3) \pmod{l}. \tag{10.10}$$

Now (1.3) and (3.2) with $N = 3$ give

$$2s(0, 3) \equiv -3q_l(3) \pmod{l}, \tag{10.11}$$

which can be rewritten as $2s(0, 6) + 2s(1, 6) \equiv -3q_l(3) \pmod{l}$. Subtracting (10.10) from this, we finally obtain

$$s(1, 6) \equiv 2q_l(2) \pmod{l}. \tag{10.12}$$

This completes the proof, with (10.3), (10.6), and (10.7). □

Remark. With (10.11) we see that Proposition 10.3 has an obvious analogue connecting the "Mirimanoff primes" (see Theorem 2.2) with $s(0, 3)$.

For a Wieferich prime l we also have

$$q_l(8) \equiv q_l(16) \equiv q_l(32) \equiv 0 \pmod{l}.$$

In [24] it was mentioned that for the two known Wieferich primes we have

$$s(k, 8) \not\equiv 0 \pmod{l}, \qquad 0 \le k \le 3.$$

By computer calculations we found that the same is true also for $N = 16$ $(0 \le k \le 7)$ and $N = 32$ $(0 \le k \le 15)$. In fact, we found that among the sums $s(k, N)$, $2 \le N \le 46$, $0 \le k < (N - 1)/2$, only the cases mentioned in Proposition 10.3 are congruent to zero (mod 1093), while for $l = 3511$ we have in addition $s(9, 33) \equiv 0 \pmod{3511}$.

4. Apart from the two Wieferich primes, we investigated the known pairs (N, l) for which $q_l(N) \equiv 0 \pmod{l}$ with $3 \le N \le 46$ and $N < l$. A table of such pairs, where N is prime, is given in [22] (p. 276; also with references to the sources). A similar table for composite N can be found in [6] and in the recent update [19].

According to these tables we have $q_l(3) \equiv 0 \pmod{l}$ for $l = 11$ and $l = 1006003$; therefore, by (10.11), $s(0, 3) \equiv 0 \pmod{l}$ for these two primes. However, no other sums $s(k, N)$ $(0 \le k < (N - 1)/2, N \le 46)$ were found to be congruent to zero (mod l) for any pair (N, l) from the tables, although $q_l(N) \equiv 0 \pmod{l}$.

5. The sums $s(k, N)$, $2 \le N \le 46$, $0 \le k < (N - 1)/2$, were computed for all odd primes $l < 2000$ $(N < l)$. For each such N, with the exception

of $N = 5$, there exist $0 \le k < (N-1)/2$ and a prime $l < 2000$, $N < l$, such that $s(k, N) \equiv 0 \pmod{l}$. On the other hand, we found only three instances where for the same l and N two sums are $0 \pmod{l}$. These are: $s(3, 40) \equiv s(9, 40) \equiv 0 \pmod{131}$; $s(0, 24) \equiv s(4, 24) \equiv 0 \pmod{137}$; and $s(1, 17) \equiv s(5, 17) \pmod{1381}$.

6. We call a prime $l \ge 7$ a Vandiver prime (see Theorem 2.3) if $s(0, 5) \equiv 0 \pmod{l}$ or $s(1, 5) \equiv 0 \pmod{l}$, i.e., if

$$\sum_{j=1}^{[l/5]} \frac{1}{j} \equiv 0 \pmod{l} \quad \text{or} \quad \sum_{j=[l/5]+1}^{[2l/5]} \frac{1}{j} \equiv 0 \pmod{l}.$$

We also note that according to the main result in [26], we have for $l > 5$

$$\frac{2}{5} s(1, 5) \equiv \frac{1}{l} F_{l-(5/l)} \pmod{l},$$

where F_n is the nth Fibonacci number ($F_0 = 0$, $F_1 = 1$, $F_{n+2} = F_{n+1} + F_n$ for $n \ge 0$) and $(5/l)$ is the Legendre symbol.

P. L. Montgomery [19] reports no solution of $F_{l-(5/l)} \equiv 0 \pmod{l^2}$ with $l < 2^{32}$. We inspected $s(0, 5) \pmod{l}$ and $s(1, 5) \pmod{l}$ with $l < 200000$; no solution of $s(1, 5) \equiv 0 \pmod{l}$ was found. The values $\pmod{l}$ appear to be randomly distributed. A curious case occurs at $l = 24179$, where $s(0, 5) \equiv 1 \pmod{l}$. (In this case, $s(1, 5) \equiv 11776 \pmod{l}$.)

7. Next we derive a result, similar to our main theorem, which involves a substantially shorter interval of summation.

Proposition 10.4. *If* $(\text{FLT I})_l$ *fails, then*

$$\sum_{j=[l/46]+1}^{[l/45]} \frac{1}{j} \equiv 0 \pmod{l}. \tag{10.13}$$

Proof. By the main theorem we have $s(0, 45) \equiv s(0, 46) \equiv 0 \pmod{l}$ if $(\text{FLT I})_l$ fails. The sum (10.13) is the difference of these two sums and is therefore congruent to zero $\pmod{l}$ as well.

We computed the sums (10.13) for all primes $l < 2 \times 10^6$; note that even the largest primes in this range have less than 1000 terms in the corresponding sums. Also, the sum cannot be zero unless it has at least three terms; i.e., $[l/45] - [l/46] \ge 3$. This is certainly true when $l/45 - l/46 \ge 2$, i.e., $l \ge 4140$. Hence it is sufficient to begin with the following prime, $l = 4153$. No zero sum was found. □

8. Finally in this section, we remark that the numbers $B_{l-1}(k/N) - B_l B_{l-1}$ in (1.5) have recently been subject to some investigation; see [2] and [3]. In [3], for example, a von Staudt-Clausen type result is derived. It should be noted, however, that these results concern the denominators of the numbers in question, while (1.5) is a condition concerning the numerators.

On the other hand, some remarkable congruence results for the left-hand side of (1.5), involving linear recurrence sequences, were discovered very recently; see [33].

ACKNOWLEDGMENTS

The authors gratefully acknowledge the advice and encouragement of Andrew Granville who, among other things, drew our attention to the decomposition (6.2) and suggested Proposition 7.1. Also, without his advice we would have obtained only a weaker version of our main theorem.

The numerical results would have been less complete without the help and advice from Samuel S. Wagstaff, Jr., who factored a number of integers for us. In particular, he used his "multiple polynomial quadratic sieve" program to factor two "difficult" composites of 78 and 85 digits, belonging to the cases $N = 35$ and $N = 17$, respectively.

The majority of large integers were factored with the elliptic curve method, using a program of Peter Montgomery.

This work was begun while the second author visited the Department of Mathematics, Statistics and Computing Science of Dalhousie University, partially supported by NSERC of Canada.

BIBLIOGRAPHY

1. T. Agoh, *On the Kummer-Mirimanoff congruences*, Acta Arith. **60** (1990), 141–156.
2. G. Almkvist and A. Meurman, *Values of Bernoulli polynomials and Hurwitz's zeta function at rational points*, C. R. Math. Rep. Acad. Sci. Canada **13** (1991), 104–108.
3. K. Bartz and J. Rutkowski, *On the von Staudt-Clausen theorem*, C. R. Math. Rep. Acad. Sci. Canada **15** (1993), 46–48.
4. P. T. Bateman, G. B. Purdy, and S. S. Wagstaff, Jr., *Some numerical results on Fekete polynomials*, Math. Comp. **29** (1975), 7–23.
5. Z. I. Borevich and I. R. Shafarevich, *Number theory*, Academic Press, New York, 1966.
6. J. Brillhart, J. Tonascia, and P. Weinberger, *On the Fermat quotient*, Computers in Number Theory, Academic Press, London and New York, 1971, pp. 213–222.
7. P. Cikánek, *A special extension of Wieferich's criterion*, Math. Comp. **62** (1994), 923–930.
8. D. Coppersmith, *Fermat's last theorem (case 1) and the Wieferich criterion*, Math. Comp. **54** (1990), 895–902.
9. L. E. Dickson, *History of the theory of numbers*, Vol. 1, Divisibility and Primality, Chelsea, New York, 1962.
10. G. Eisenstein, *Eine neue Gattung zahlentheoretischer Funktionen welche von zwei Elementen abhängen und durch gewisse lineare Funktional-Gleichungen definiert werden*, Bericht über die zur Bekanntmachung geeigneten Verhandlungen der Königl. Preuss. Akademie der Wissenschaften zu Berlin (1850), 36–42. (See also Mathematische Werke, 2nd ed., Gotthold Eisenstein, Band II, Chelsea, New York, 1989, pp. 705–711.)
11. J. W. L. Glaisher, *On the residues of r^{p-1} to modulus p^2, p^3 etc.*, Quart. J. Math. **32** (1901), 1–27.
12. A. Granville and M. B. Monagan, *The first case of Fermat's last theorem is true for all prime exponents up to* 714,591,416,091,389, Trans. Amer. Math. Soc. **306** (1988), 329–359.
13. A. Granville, *The Kummer-Wieferich-Skula approach to the first case of Fermat's Last Theorem*, Advances in Number Theory (F. Q. Gouvêa and N. Yui, eds.), (Proc. Third Conference of the Canadian Number Theory Assoc., August 18–24, 1991, Queen's University at Kingston), Clarendon Press, Oxford, 1993, pp. 479–497.
14. N. G. Gunderson, *Derivation of criteria for the first case of Fermat's last theorem and the combination of these criteria to produce a new lower bound for the exponent*, Thesis, Cornell University, 1948.

15. E. E. Kummer, *Einige Sätze über die aus den Wurzeln der Gleichung* $\alpha^\lambda = 1$ *gebildeten complexen Zahlen für den Fall, dass die Klassenanzahl durch* λ *theilbar ist, nebst Anwendung derselben auf einen weiteren Beweis des letzten Fermat'schen Lehrsatzes*, Math. Abh. Königl. Akad. Wiss. zu Berlin (1857), pp. 41–74. (Collected Papers, Vol. I, Springer-Verlag, Berlin and New York, 1975, pp. 639–692.)
16. E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. (2) **39** (1938), 350–360.
17. M. Lerch, *Zur Theorie des Fermatschen Quotienten* $(a^{p-1} - 1)/p = q(a)$, Math. Ann. **60** (1905), 471–490.
18. D. Mirimanoff, *Sur le dernier théorème de Fermat*, C. R. Acad. Sci. Paris **150** (1910), 204–206.
19. P. L. Montgomery, *New solutions of* $a^{p-1} \equiv 1 \pmod{p^2}$, Math. Comp. **61** (1993), 361–363.
20. F. Pollaczek, *Über den grossen Fermat'schen Satz*, Akad. Wiss. Wien, Abt. IIa **126** (1917), 45–49.
21. P. Ribenboim, 13 *lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.
22. ———, *The book of prime number records*, Springer-Verlag, New York, 1988.
23. L. Skula, *On the Kummer's system of congruences*, Comment. Math. Univ. St. Paul. **35** (1986), 137–163.
24. ———, *Some consequences of the Kummer system of congruences*, Comment. Math. Univ. St. Paul. **39** (1990), 19–40.
25. ———, *Fermat's last theorem and the Fermat quotients*, Comment. Math. Univ. St. Paul. **41** (1992), 35–54.
26. Zhi-Hong Sun and Zhi-Wei Sun, *Fibonacci numbers and Fermat's Last Theorem*, Acta Arith. **60** (1992), 371–388.
27. 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; also in The Collected Mathematical Papers, Vol. II, Chelsea, New York, 1973, pp. 229–231.
28. J. W. Tanner and S. S. Wagstaff, Jr., *New bound for the first case of Fermat's last theorem*, Math. Comp. **53** (1989), 743–750.
29. H. S. Vandiver, *Extension of the criteria of Wieferich and Mirimanoff in connection with Fermat's last theorem*, J. Reine Angew. Math. **144** (1914), 314–318.
30. I. M. Vinogradov, *Elements of number theory*, Dover, New York, 1954.
31. L. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York, 1982.
32. A. Wieferich, *Zum letzten Fermat'schen Theorem*, J. Reine Angew. Math. **136** (1909), 293–302.
33. A. Granville and Zhi-Wei Sun, *Values of Bernoulli polynomials*, Pacific J. Math. (to appear).

Department of Mathematics, Statistics and Computing Science, Dalhousie University, Halifax, Nova Scotia B3H 3J5, Canada
E-mail address: dilcher@cs.dal.ca

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