A SPECIAL EXTENSION OF WIEFERICH'S CRITERION

PETR CIKÁNEK

Abstract. The following theorem is proved in this paper: "If the first case of Fermat’s Last Theorem does not hold for sufficiently large prime \( l \), then

\[ \sum_{x} x^{l-2} \left[ \frac{kl}{N} < x < \left( \frac{k+1}{N} \right) \right] \equiv 0 \pmod{l} \]

for all pairs of positive integers \( N, k, N \leq 94, 0 < k < N - 1 \)." The proof of this theorem is based on a recent paper of Skula and uses computer techniques.

0. Introduction

The first case of Fermat’s Last Theorem states that for each odd prime \( l \) the equation

\[ x^l + y^l + z^l = 0 \]

has no integral solution \( x, y, z \) with \( l \nmid xyz \).

One of many methods investigating this problem was introduced by A. Wieferich. This method is connected with the Fermat quotients \( q_l(a) \),

\[ q_l(a) = \frac{a^{l-1} - 1}{l} , \]

defined for each integer \( a \) such that \( a \) is not divisible by \( l \).

Let us assume in this paragraph that \( l \) is an odd prime which does not satisfy the first case of Fermat’s Last Theorem.

In 1909, Wieferich [7] published the following important result:

\[ q_l(2) \equiv 0 \pmod{l}. \]

Many mathematicians have extended this Wieferich criterion. The latest result is due to A. Granville and B. Monagan [1] and states \( q_l(p) \equiv 0 \pmod{l} \) for each prime \( p \) such that \( p \leq 89 \).

These considerations have been generalized by L. Skula. He studied the sums

\[ s(k, N) = \sum_{x} x^{l-2} \left[ \frac{kl}{N} < x < \left( \frac{k+1}{N} \right) \right] \]

Received by the editor May 6, 1991 and, in revised form, November 25, 1991 and November 5, 1992.

1991 Mathematics Subject Classification. Primary 11D41.

Key words and phrases. The first case of Fermat’s Last Theorem, Fermat quotient, Bernoulli numbers, Bernoulli polynomials.
for integers \( N, k, 1 \leq N \leq l - 1, 0 \leq k \leq N - 1 \). These sums are connected with the Fermat quotients by a formula introduced essentially by M. Lerch [2]:

\[
q_l(N) \equiv N^{l-2} \sum_{k=0}^{N-1} k s(k, N) \pmod{l}.
\]

Skula [4] proved

\[
s(k, N) \equiv 0 \pmod{l}, \quad 0 \leq k \leq N - 1,
\]

for each \( N \in \{2, 3, \ldots, 10\} \cup \{12\} \).

In this paper, Skula’s result is improved for integers \( N \leq 94 \) (Main Theorem 3.2), but only for sufficiently large primes \( l \).

**Remark.** It is easy to prove that the statement

\[
s(k, N) \equiv 0 \pmod{l}, \quad 0 \leq k \leq N - 1,
\]

is equivalent to the statement

\[
B_{l-1} \left( \frac{j}{N} \right) - B_{l-1} \equiv 0 \pmod{l}, \quad 0 \leq j \leq N,
\]

where \( B_n, B_n(x) \) are the \( n \)th Bernoulli number and Bernoulli polynomial, respectively. Therefore, our result implies that the polynomial \( B_{l-1}(t) - B_{l-1} \) has at least \( 1 + \sum_{N=1}^{94} \varphi(N) = 2703 \) distinct zeros modulo \( l \) for sufficiently large prime \( l \), where \( l \) does not satisfy the first case of Fermat’s Last Theorem.

### 1. Basic notions and assertions

We will assume in this section that there is an odd prime \( l \) which does not satisfy the first case of Fermat’s Last Theorem, briefly (FLTI) \( l \) fails; i.e., there exist integers \( x, y, z \) such that

\[
x^l + y^l + z^l = 0, \quad l \nmid xyz.
\]

1.1. **Definition.** Let \( \tau_1, \ldots, \tau_6 \) denote the integers satisfying

\[
x\tau_1 \equiv -y \pmod{l}, \quad x\tau_3 \equiv -z \pmod{l}, \quad y\tau_5 \equiv -z \pmod{l},
\]

\[
y\tau_2 \equiv -x \pmod{l}, \quad z\tau_4 \equiv -x \pmod{l}, \quad z\tau_6 \equiv -y \pmod{l}.
\]

The definition of \( \tau_1, \ldots, \tau_6 \) implies

1.2. **Lemma.** The integers \( \tau_1, \ldots, \tau_6 \) satisfy the following congruences:

\[
\tau_1\tau_2 \equiv \tau_3\tau_4 \equiv \tau_5\tau_6 \equiv 1 \pmod{l},
\]

\[
\tau_1 + \tau_3 \equiv \tau_2 + \tau_5 \equiv \tau_4 + \tau_6 \equiv 1 \pmod{l},
\]

\[
0 \nmid \tau_i \neq 1 \pmod{l}, \quad 1 \leq i \leq 6.
\]

According to the results of Pollaczek ([3], See [1, Lemma 15]) we have

1.3. **Lemma.** Let \( r_1, \ldots, r_6 \) denote the orders of the integers \( \tau_1, \ldots, \tau_6 \) mod \( l \). Then \( r_1 = r_2, r_3 = r_4, r_5 = r_6 \), and each of the products \( r_1r_3, r_3r_5, r_1r_5 \) is greater than or equal to

\[
\frac{3 \log(l)}{\log \left( \frac{1 + \sqrt{5}}{2} \right)}.
\]
1.4. **Definition.** Pollaczek introduced a matrix $A_s(t)$ of size $2\phi(s) \times \phi(s)$ ($\phi$ Euler's function) for integers $s \geq 2$ and variable $t$ in [3]. Let $r(s, t)$ denote the rank of the matrix $A_s(t)$ over the finite $\mathbb{Z}/l\mathbb{Z}$.

According to the results from [1, Table 1] (see also [4, 5.1.1]) we obtain

1.5. **Lemma.** Let $s, t$ be integers, $2 \leq s \leq 46$ and the order of $t$ modulo $l$ be greater than $44$. Then $r(s, t) = \phi(s)$.

1.6. **Definition.** Skula ([4, Definition 4.13]) has introduced the following square matrix $D_N = D_N(t)$ of order $\phi(N)/2$ for integers $N \geq 3$ and variable $t$ by the formula

$$D_N = D_N(t) = [t^{z(u,v)-1} + t^{N-1-z(u,v)}],$$

where $1 \leq u, v \leq \frac{N}{2}$, $\gcd(u, N) = \gcd(v, N) = 1$.

Let us denote $d_N(t) = \det D_N(t)$.

The next theorem follows from Skula's results ([4, Main Theorem 4.14, 5.4.2]).

1.7. **Theorem.** Let $N$ be an integer, $N \geq 2$, $\frac{N-2}{2} < l$, and $\tau_1, \ldots, \tau_6$ be the integers from 1.1. Assume that there exists $1 \leq a \leq 6$ such that the following conditions are satisfied:

(a) $d_M(\tau_a) \equiv 0 \pmod{l}$ for each integer $M \geq 3, M \nmid N$;

(b) $r(s, \tau_a) = \phi(s)$ for each integer $s, 2 \leq s < \frac{N}{2}$.

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

2. **Some auxiliary statements**

2.1. **Lemma.** Let $p$ be a prime, $f(t), g(t)$ be polynomials over $\mathbb{Z}$, the leading coefficients of which are not divisible by $p$. If $f, g$ are relatively prime over the finite field $\mathbb{Z}/p\mathbb{Z}$, then $f$, $g$ are relatively prime over $\mathbb{Q}$.

**Proof.** It is sufficient to prove that $\gcd(f, g)$ over $\mathbb{Z}$ is a constant. Assume on the contrary that there exist polynomials $h, u, v$ over $\mathbb{Z}$ such that

$$f = hu, \quad g = hv, \quad \deg(h) > 0. \tag{1}$$

We can consider $f, g, h, u, v$ as polynomials over $\mathbb{Z}/p\mathbb{Z}$. Their degrees do not change because $p$ does not divide the leading coefficients of these polynomials. Then the equation (1) holds also over $\mathbb{Z}/p\mathbb{Z}$, and this is a contradiction. $\Box$

2.2. **Theorem.** Let $m$ be a positive integer. There is an integer $L_0 = L_0(m)$ with the following property:

Let $l > L_0$ be a prime for which $(FLT)_l$ fails. Then there exist two different integers $a, b, 1 \leq a, b \leq 6$, such that

$$\tau_a + \tau_b \equiv 1 \pmod{l}, \quad r_a > m, r_b > m,$$

where $r_a, r_b$ are the orders of the integers $\tau_a, \tau_b$ modulo $l$. 
Proof. Let \( L_0 \) be the smallest integer greater than
\[
\left( \frac{1 + \sqrt{5}}{2} \right)^{m^2/3}.
\]
The proof then easily follows from Pollaczek's Lemmas 1.3. and 1.2. \( \square \)

2.3. Theorem. Let \( N \) be an integer, \( 2 \leq N \leq 94 \), \( d(t) \) be any common multiple of the polynomials \( d_M(t) \), \( 3 \leq M \), \( M \mid N \). Let \( g(t) \) be a polynomial such that:

(a) \( g(t) \) is a product of some cyclotomic polynomials,
(b) \( g(t) \mid d(t) \) over the ring \( \mathbb{Z}[t] \) \( \) (we allow \( g(t) = 1 \)).

Let the polynomial \( f(t) = \frac{d(t)}{g(t)} \) satisfy

(2) \[ \gcd(f(t), f(1-t)) = 1 \quad \text{over } \mathbb{Q}. \]

Then there exists a positive integer \( L \) such that

\[ s(k, N) \equiv 0 \pmod{l}, \quad 0 < k < N - 1, \]

for each prime \( l > L \) for which \( (FLT)_{\ell} \) fails.

Proof. Suppose \( f(t), f(1-t) \) are relatively prime over the field \( \mathbb{Q} \). Then there exist an integer \( c \) and integral polynomials \( u(t), v(t) \) such that

(3) \[ f(t)u(t) + f(1-t)v(t) = c. \]

Let \( c \) be the smallest integer with this property.

Let us put \( n_0 = \max\{n, \Phi_n(t)\mid g(t)\} \) \( \) \( \) \( \Phi_n \) is the \( n \)th cyclotomic polynomial, \( m = \max\{n_0, 45\} \), \( L_0 = L_0(m) \) the integer from 2.2.

Let \( l \) be a prime, \( l > L_0 \), \( l \mid c \), for which \( (FLT)_l \) fails. According to 2.2 there exist different integers \( a, b, 1 < a, b < 6 \), such that

\[ \tau_a + \tau_b \equiv 1 \pmod{l}, \quad r_a > m, r_b > m. \]

By (3) we have \( f(\tau_a) \neq 0 \pmod{l} \) or \( f(\tau_b) \neq 0 \pmod{l} \). Therefore, we can assume

(4) \[ f(\tau_a) \neq 0 \pmod{l}. \]

Since \( r_a > m \geq n_0 \), we have

\[ \Phi_n(\tau_a) \neq 0 \pmod{l}, \quad 1 \leq n \leq n_0, \]

and it follows that

(5) \[ g(\tau_a) \neq 0 \pmod{l}. \]

Putting (4) and (5) together, we obtain

\[ f(\tau_a)g(\tau_a) = d(\tau_a) \neq 0 \pmod{l}; \]

therefore,

\[ d_M(\tau_a) \neq 0 \pmod{l} \]

for all integers \( M \), \( 3 \leq M \leq N \), \( M \mid N \).

We can see that the integer \( a \) satisfies the first condition of Theorem 1.7. The second condition is satisfied according to 1.5. The proof now immediately follows from Theorem 1.7. \( \square \)
What follows is useful for practical computer calculation. Instead of dealing with polynomials \( d_M(t) = \det D_M(t) \), it allows to work with polynomials of lower degrees. These assertions follow from Washington's book [6, (4.5.26)]. For the convenience of readers we include proofs of these assertions.

Let \( \chi \) be an even Dirichlet's character \( \mod M \). Let \( f_\chi(t) \) be a polynomial of form
\[
f_\chi(t) = \sum_i \chi(i) t^{i-1}, \quad 1 \leq i \leq M, \ \gcd(i, M) = 1.
\]

2.4. **Lemma.** Let \( M \) be an integer, \( M \geq 3 \). Then
\[
\det D_M(t) = \pm \prod_\chi f_\chi(t),
\]
where the product is over all even Dirichlet's characters \( \mod M \).

**Proof.** Let \( \langle \alpha \rangle \) denote the fractional part of a real number \( \alpha \). It is easy to see that
\[
\chi \equiv M \left\langle \frac{x}{M} \right\rangle \pmod M
\]
for each integer \( x \).

According to 1.6 we have
\[
D_M(t) = \left[ t^{z(u,v)} + t^{M-z(u,v)} \right]_{v,u}, \quad 1 \leq u, \ v \leq \frac{M}{2},
\]
\[
\gcd(u, M) = \gcd(v, M) = 1, \quad 1 \leq z(u,v) \leq M - 1, \quad v \equiv uz(u,v) \pmod M.
\]

Putting \( i \equiv \pm u^{-1} \pmod l \), so that \( 1 \leq i \leq \frac{M}{2} \), we get
\[
d_M(t) = \pm t^{-\varphi(M)/2} \det A,
\]
where \( A \) is a matrix of the form
\[
A = \left[ t^{M(iv/M)} + t^{M(-iv/M)} \right]_{i,v}, \quad 1 \leq i, \ v \leq \frac{m}{2}, \ \gcd(i, M) = \gcd(v, M) = 1.
\]

Now it is sufficient to show that
\[
\det A = \pm t^{\varphi(M)/2} \prod_\chi f_\chi(t),
\]
where the product is over all even characters \( \mod M \).

Let \( B \) be the square matrix
\[
B = [\chi(i)]_{x,i},
\]
\( \chi \) an even Dirichlet's character \( \mod M \), \( 1 \leq i \leq M/2 \), \( \gcd(i, M) = 1 \). It is easy to prove that this matrix is nonsingular (see, e.g., Van der Waerden [5, §§124–126]), and we have
\[
BA = \left[ \sum_i \chi(i) t^{M(iv/M)} \right] = \left[ \chi^{-1}(v) \sum_i \chi(i) t^{i} \right]_{x,v},
\]
\[
(1 \leq i \leq M, \ \gcd(i, M) = 1);
\]
hence
\[
\det B \det A = \pm t^{\varphi(M)/2} \left( \prod_\chi f_\chi(t) \right) \det B.
\]

This completes the proof. \( \square \)
2.5. **Lemma.** Let \( \chi \) be an even character mod M of order \( n \geq 1 \). Then the polynomial

\[
F_\chi(t) = \prod_{a} f_{\chi^a}(t), \quad 1 \leq a \leq n, \quad \gcd(a, n) = 1,
\]

is a polynomial with integer coefficients.

**Proof.** The polynomial \( f_{\chi}(t) \) is polynomial over the field \( \mathbb{Q}(\xi_n), \, \xi_n = e^{2\pi i/n} \).

Let us consider the Galois group \( G \) of the extension \( \mathbb{Q}(\xi_n)/\mathbb{Q} \). It is well known that

\[
G = \{ \sigma_s, \, s \in \mathbb{Z}, \, 1 \leq s \leq n, \, \gcd(s, n) = 1, \, \sigma_s(\xi_n) = \xi_n^s \}.
\]

Every isomorphism \( \sigma_s \) can be extended in the natural way on the ring \( \mathbb{Q}(\xi_n)[t] \), and obviously

\[
\sigma_s(F_\chi(t)) = F_\chi(t).
\]

Since \( F_\chi(t) \) is an element of \( \mathbb{Z}(\xi_n)[t] \), we have \( F_\chi(t) \in \mathbb{Z}[t] \). \( \square \)

3. **Main results**

Let \( N \) be an integer, \( 3 \leq N \leq 94 \). By 2.4, 2.5 we can express the polynomial \( d_N(t) \) as a product of integers polynomials \( F_\chi(t) \). Let \( K_N \) denote the number of these polynomials. We will enumerate them (for example according to the values of their degrees) and add the index \( N \) so we have

\[
d_N(t) = \prod_{i=1}^{K_N} F_{N,i}(t).
\]

Let \( g_{N,i} \) be the product of all cyclotomic polynomials dividing \( F_{N,i} \), and put \( f_{N,i} = F_{N,i}/g_{N,i} \) for each \( 1 \leq i \leq K_N \). According to 2.1 the condition (2) holds if we find a prime \( p = p(L, M, i, j) \) for each set of integers \( L, M, i, j, \, 3 \leq L, M, \, L|N, M|N, \, 1 \leq i \leq K_L, \, 1 \leq j \leq K_M \) such that

\[
gcd(f_L,i(t), f_M,j(1 - t)) = 1 \quad \text{over } \mathbb{Z}/p\mathbb{Z}.
\]

This was done using a personal computer. In most cases, (6) holds for polynomials \( F_{L,i}(t), \, F_{M,j}(1 - t) \), and some prime \( p \leq 17 \), so it is sufficient to compute only polynomials \( F_{N,i}(t), \, F_{N,i}(1 - t) \) modulo small primes. The calculation of polynomials \( F_{N,i}(t), g_{N,i}(t), \, f_{N,i}(t), \, f_{N,i}(1 - t) \) over \( \mathbb{Z} \) is necessary only in a few cases (for example, if \( \Phi_3(t) || F_{N,i}(t) \), because \( \Phi_3(t) = \Phi_3(1 - t) \)). The relation (6) also holds in these cases for some prime \( p, \, p \leq 17 \).

Therefore, from our computation we obtain the following lemma.

3.1. **Lemma.** Let \( L, M, i, j \) be integers, \( 3 \leq L, M, \, \text{lcm}[L, M] \leq 94, \, 1 \leq i \leq K_L, \, 1 \leq j \leq K_M \). Then there exists a prime \( p \in \{ 2, 3, 5, 7, 11, 17 \} \) such that the polynomials \( f_{L,i}(t), \, f_{M,j}(1 - t) \) are relatively prime over \( \mathbb{Z}/p\mathbb{Z} \).

The Main Theorem follows now immediately from 3.1, 2.6, 2.1, and 1.6.
3.2. **Theorem.** Let \( N \) be an integer, \( 2 \leq N \leq 94 \). There exists an integer \( L \) such that

\[
s(k, N) \equiv 0 \pmod{l}, \quad 0 \leq k \leq N - 1,
\]

for each prime \( l > L \) for which the first case of Fermat's Last Theorem is false for prime exponent \( l \).

3.3. **Remark.** Let us try to find a value for the number \( L \) in the last theorem. In our calculations we shall suppose that the polynomials \( g_{n,i} \) have not been divided by cyclotomic polynomials \( \Phi_n(t), n > 45 \). According to the proofs of 2.3 and 2.2, the first condition for the number \( L \) is that

\[
L > \left( \frac{1 + \sqrt{5}}{2} \right)^{45^2/3}.
\]

The second condition is that \( L \) is greater than the largest prime dividing the number \( c \) in (3). This certainly holds if \( L \) is greater than the resultant of the polynomials \( f(t), f(1 - t) \) (it is known that the number \( c \) divides this resultant—see [1, Lemma 20]).

We will find the rough upper bound of this resultant for the cases \( N \) being a prime. In these cases we have

\[
f(t) = \frac{d_N(t)}{g(t)},
\]

\[k = \deg f(t) = \deg f(1 - t) \deg d_N(t) = \frac{\phi(N)(N - 2)}{2} = \frac{(N - 1)(N - 2)}{2}.
\]

Let \( f(t) = (t - \alpha_1) \cdots (t - \alpha_k) \) over the field of complex numbers.

Each complex number \( \alpha_j \) is a root of some polynomial \( f_x(t) \), so we have

\[|\alpha_j|^{N-2} \leq \sum_{i=0}^{N-3} |\alpha_j|^i;
\]

hence \( |\alpha_j| < 2 \).

It follows that

\[R(f(t), f(1 - t)) = \prod_{i,j} (\alpha_i - (1 - \alpha_j)) < 5^{k^2} \leq 5^{(N-1)^2(N-2)^2/4}.
\]

We have proved the next theorem.

3.4. **Theorem.** Let \( N \) be a prime, \( 11 \leq N \leq 89 \). Then

\[
s(k, N) \equiv 0 \pmod{l}, \quad 0 \leq k \leq N - 1,
\]

for each prime \( l > 5^{(N-1)^2(N-2)^2/4} \) for which the first case of Fermat's Last Theorem is false for prime exponent \( l \).

**Bibliography**


2. M. Lerch, *Zur Theorie des Fermatschen Quotienten* \( \frac{a^{p-1} - 1}{p} = q(a) \), Math. Ann. 60 (1905), 471–490.


Družba 1289, 768 24 Hulin, Czech Republic