A PRODUCT FORMULA RELATED TO THE
DIOPHANTINE EQUATION

\[ N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(u + v\zeta) = w_1^p, \quad p \nmid uv(u^2 - v^2) \]

GEORGES GRAS

Villa la Gardette
Chemin Château Gagnière
F-38520 Le Bourg d'Oisans
France
e-mail: g.mn.gras@wanadoo.fr

Abstract

Let \( u, v \) be coprime integers such that \( N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(u + v\zeta) \) is the \( p \)-th power of an integer, where \( \zeta = e^{2\pi i/p} \). Using the Brückner-Vostokov explicit formula, we establish a product formula for the \( p \)-th power residue symbols computed in our article in common with Quême [7]. This product formula is equivalent to the relations

\[ T_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\frac{\zeta_n - \rho}{1 + \zeta_n}) \log(\zeta_n - \rho) \equiv 0 \pmod{p}, \quad \text{for all } n (p \nmid n, n \nmid p - 1), \]

where \( \zeta_n \) is a primitive \( n \)-th root of unity, \( \rho := \frac{v}{u} \), \( \log \) is the \( p \)-adic logarithm. This allows us to verify, for given values of \( p \), the insolubility of the above equation under the assumption \( p \nmid uv(u^2 - v^2) \). This insolubility is then equivalent to the existence of \( n (p \nmid n, n \nmid p - 1) \) such that

\[ \sum_{k=1}^{p-1} \frac{1}{k} \rho^k T_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}\left(\frac{\zeta_n^k}{1 + \zeta_n^p}\right) \not\equiv 0 \pmod{p}, \]

constituting an alternative to Kummer-Mirimanoff congruences without any

2010 Mathematics Subject Classification: 11D41, 11R18, 11R44, 11R45.

Keywords and phrases: Diophantine equations, cyclotomic fields, cyclotomic units, class field theory, reciprocity laws, Fermat’s last theorem, Mirimanoff congruences.

Received March 13, 2012

© 2012 Scientific Advances Publishers
reference to Bernoulli numbers (see Sections 5, 6, 7). For instance, for \( p = 5 \) and the only possible classes \( \rho_0 = 2, 3 \pmod{5} \), the above condition is fulfilled for \( n = 3 \). For \( p = 37 \) and \( n = 8 \), the condition is fulfilled for all \( \rho_0 \).

## 1. Introduction and Recall of the Main Results

Consider the maximal Abelian extension \( \overline{Q}^{nr} \) of \( Q \), unramified at a given prime number \( p > 2 \). From class field theory, \( \overline{Q}^{nr} = \bigcup_{n, p \nmid n} Q(\mu_n) \).

Let \( H_{\overline{Q}^{nr}}[p] \) be the maximal \( p \)-elementary extension of \( \overline{Q}^{nr} \), unramified outside \( p \). This extension is equal to \( \bigcup_{n, p \nmid n} H_{Q(\mu_n)}[p] \), where \( H_{Q(\mu_n)}[p] \) is the maximal \( p \)-elementary extension of \( Q(\mu_n) \), unramified outside \( p \).

Set \( \zeta := e^{2\pi i/p} \), \( K := Q(\zeta) \), \( p := (\zeta - 1)\mathbb{Z}[\zeta] \). We have shown in [7] that each nontrivial solution \((u, v)\) of the equation in coprime integers \( u, v \),

\[(u + v\zeta)\mathbb{Z}[\zeta] = p^\delta w_1^p,\]

where \( \delta \) is any integer \( \geq 0 \) and \( w_1 \) is any integer ideal of \( K \) (the condition \( \gcd(u, v) = 1 \) implies \( \delta \in \{0, 1\} \) and \( p \nmid w_1 \)), defines some constraints on the law of decomposition, in \( H_{\overline{Q}^{nr}}[p] / \overline{Q}^{nr} \), of each prime number \( q \neq p, q \nmid uv \). The conjectural property that this equation has no nontrivial solutions for \( p > 3 \) is called the strong Fermat last theorem (SFLT).

This writing is equivalent to \( N_{K/Q}(u + v\zeta) = p^\delta w_1^p \) with \( w_1 = N_{K/Q}(w_1) \equiv 1 \pmod{p} \), which leads to a link with Fermat’s equation corresponding to the case, where \( u + v = w_0^p \) if \( \delta = 0 \), or is of the form \( p^{vp-1}w_0^p \) if \( \delta = 1 \) (see [7, Section 2], [6], and [17] for the classical interpretations by means of the arithmetic of the field \( K \); see [4, 11, 12, 13, 14] and many others for similar context).
The nonspecial cases of SFLT (i.e., \( u + v \not\equiv 0 \pmod{p} \)) imply the two cases of Fermat’s last theorem (FLT) since a solution \((a, b, c)\) of the FLT equation, with \( p \nmid ab \), gives, for instance, the solutions \((u, v) = (a, c)\) and \((u, v) = (b, c)\). For \( p > 3 \), we can assume that \( p \nmid (a - c)(b - c) \), hence that \( u - v \not\equiv 0 \pmod{p} \) in the search of solutions of the SFLT equation, in order to disprove FLT. Indeed, the case \( u - v \equiv 0 \pmod{p} \) cannot be avoided in the SFLT case.

So, we can assume that \( p \nmid u^2 - v^2 \) in this study; hence the first case corresponds to \( p \nmid uv \) and the second one for instance to \( p|v \).

In this context, Sitaraman \[12\], using deep \(K\)-theory results of Kurihara \[10\], has proved that if the Bernoulli number \( B_{p-3} \) satisfies the condition \( B_{p-3} \not\equiv 0 \pmod{p^2} \), the first case of FLT holds for \( p \); then Mihăilescu \[11\] has proved that under the same assumption, the SFLT equation has no solutions with \( p \nmid uv(u^2 - v^2) \).

In \[1\], considering the first case of the SFLT equation, Anglès has proved that the theorem of Eichler applies to the conjecture of Terjanian, hence to the Kummer congruences in relation with Bernoulli numbers.

Recall first some definitions about the cyclotomic field \( K \).

**Definition 1.1.** (i) Let \( g := \text{Gal}(K / \mathbb{Q}) \) and let \( \omega \) be the Teichmüller character of \( g \), i.e., the character with values in \( \mu_{p-1}(\mathbb{Q}_p) \) such that for \( s_k \in g \) defined by \( s_k(\zeta) = \zeta^k, k \not\equiv 0 \pmod{p} \), \( \omega(s_k) = \omega(k) \) is the unique \((p - 1)\)-th root of unity of \( \mathbb{Q}_p \) congruent to \( k \) modulo \( p \); \( \omega \) is the character of the \( g \)-module \( \langle \zeta \rangle \).

(ii) The idempotent corresponding to \( \omega \) is \( \mathcal{E}_\omega := \frac{1}{p - 1} \sum_{k=1}^{p-1} \omega^{-1}(k)s_k \in \mathbb{Z}_p[g] \).
(iii) Let $e_\omega$ be a representative in $\mathbb{Z}[g]$ of $\mathcal{E}_\omega$ modulo $p\mathbb{Z}_p[g]$. Put $e_\omega = \sum_{k=1}^{p-1} u_k s_k$, $u_k \in \mathbb{Z}$, $u_k = \frac{k^{-1}}{\mathfrak{p}} \mod p$. Since $\omega^{-1}(s_{p-k}) = -\omega^{-1}(s_k)$, one may assume that $u_{p-k} = -u_k$ for $1 \leq k \leq \frac{p-1}{2}$ so that $e_\omega = (1 - s_\omega) e_\omega^+$ with $e_\omega^+ = \sum_{k=1}^{\frac{p-1}{2}} u_k s_k$.

(iv) For a given primitive $n$-th root of unity $\xi$, with $n \neq 0 \mod p$, we consider the cyclotomic unit $\eta = \eta(\xi) := (1 + \xi \zeta)^{-\frac{1}{2}}$ in $M := LK$, where $L := \mathbb{Q}(\zeta)$. Then we put $\eta_1 := \eta^{e_\omega} = (1 + \xi \zeta)^{\xi_\omega} \zeta^{-\frac{1}{2}} \in M^+$, where $M^+$ is the maximal real subfield of $M$. □

The constraints we have found are made explicit in the nonspecial cases by the following result about the $p$-th power residue symbols of $\eta_1$ (see [7, Theorem 3.3], in the spirit of Vandiver’s papers [15, 16], and its interpretation by means of suitable Frobenius automorphisms in the extensions $H_L[p]/L$, giving [7, Theorem 6.5]).

**Theorem 1.2.** Let $p$ be a prime $> 3$, let $K = \mathbb{Q}(\zeta)$, where $\zeta$ is a primitive $p$-th root of unity, and let $p = (\zeta - 1)E[\zeta]$. Suppose that we have an equality $(u + v\zeta)E[\zeta] = \mathfrak{w}_1^p$ with coprime integers $u, v$, where $\mathfrak{w}_1$ is an integral ideal of $K$ (nonspecial cases $p \nmid u + v$). Let $q \neq p, q \nmid uv$, be a prime such that $\frac{u}{v}$ is of order $n$ modulo $q$, with $p \nmid n$.

Set $\eta := (1 + \xi \zeta)^{-\frac{1}{2}}$ and $\eta_1 := \eta^{e_\omega}$, where $\zeta$ is a primitive $n$-th root of unity. Finally, let $q = (q, u\zeta - v)$ lying above $q$ in $L := \mathbb{Q}(\mu_n)$. Then for all $\Omega \mid q$ in $M := LK$, we have $\left( \frac{\eta_1}{\Omega} \right)_M = \zeta^{-\frac{1}{2} u - v} \kappa_q$, where $\kappa_q := \frac{f_q - 1}{p}$, $f_q$ being the residue degree of $q$ in $K$. □
In this statement, we have used that for any coprime integers \( u, v \), the following two conditions are equivalent (see [7, Lemma 2.6]):

(i) \( q \nmid uv \) \& \( \frac{v}{u} \) is of order \( n \) modulo \( q \);

(ii) for \( \xi \) of order \( n \), \( q := (q, u\xi - v) \) is a prime ideal of \( L := \mathbb{Q}(\xi) \) lying above \( q \) \& \( n \mid q - 1 \).

We shall use the following generalization of this property:

**Lemma 1.3.** For any coprime integers \( u, v \), the following two conditions are equivalent:

(i) \( q \nmid uv \) \& \( \frac{v}{u} \) is of order \( n_0 \) modulo \( q \);

(ii) for \( \xi \) of order \( n = n_0q^r \), \( q \nmid n_0, r \geq 0 \), \( q := (q, u\xi - v) \) is a prime ideal of \( L := \mathbb{Q}(\xi) \) lying above \( q \) \& \( n_0 \mid q - 1 \).

**Proof.** If \( n = n_0q^r, q \nmid n_0, r \geq 0 \), set \( L := \mathbb{Q}(\mu_n), L_0 := \mathbb{Q}(\mu_{n_0}), \mathbb{Q}^r := \mathbb{Q}(\mu_{q^r}) \). Then \( q \) totally ramifies in \( \mathbb{Q}^r / \mathbb{Q} \) and \( L / L_0 \). For \( \xi \) of order \( n \), set \( \xi = \xi_0\psi, \xi_0 \) of order \( n_0, \psi \) of order \( q^r \).

Suppose (i). Since \( \frac{v}{u} \) is of order \( n_0 \) modulo \( q \), the ideal \( q_0 := (q, u\xi_0 - v) \) is (from the previous recalls) a prime ideal lying above \( q \) in \( L_0 \) and \( n_0 \mid q - 1 \); thus \( q_0Z_L \) is of the form \( q_0^{[L:L_0]} \). The unique prime ideal \( q^r \) lying above \( q \) in \( \mathbb{Q}^r \) is such that \( v \equiv 1 \) \( (\mod q^r) \) and we get \( u\xi - v = u\xi_0 - v \) \( (\mod qZ_L) \), hence \( u\xi - v \in q_0Z_L + q^rZ_L = q \). So \( (q, u\xi - v) = q \).

Suppose (ii). If \( q = (q, u\xi - v) \) is a prime ideal of \( L \), then \( q \nmid uv \) (otherwise, \( q \) is the unit ideal). Then \( \xi = \xi_0\psi \equiv \frac{v}{u} \) \( (\mod q) \) gives \( \xi_0 \equiv \frac{v}{u} \) \( (\mod q) \), hence \( \xi_0 \equiv \frac{v}{u} \) \( (\mod q_0) \) for some \( q_0 \) lying above \( q \) in \( L_0 \). Thus \( \frac{v}{u} \) is of order \( n_0 \) modulo \( q \) since \( n_0 \mid q - 1 \). \( \square \)
In practice, this generalization avoids to assume that \( q \nmid n \) and more precisely to assume that, for \( \xi \) of order \( n \), \((u\xi - v)\) is prime to \( n \), which is not effective.

If \( q \mid n \) and if \( \Omega \mid q \) in \( M = L\)K, we note, from \( \xi = \xi_0p \) as above, that

\[
\eta_1 = (1 + \xi\xi_0^{v/\xi})^{\frac{1}{p^2}} = (1 + \xi_0\xi)^{v/\xi^{\frac{1}{2}}} =: \eta_1^0 \quad (\text{mod } \Omega),
\]

since \( v = 1 \pmod{q} \). Thus \( \eta_1^0 \in M_0 := L_{0}K \subseteq M \) has the same local properties as \( \eta_1 \) at \( q \). Be careful that the notations \( n_0, \xi_0, L_0, M_0, q_0 \), \( \eta_1^0 \), depend on the prime \( q \) considered. This prime \( q \) totally splits in \( L_0 / \mathbb{Q} \) and totally ramifies in \( L / L_0 \) (hence \( q \) is of degree 1 in \( L / \mathbb{Q} \)); of course, if \( q \nmid n, n_0 = n, L_0 = L \), and so on.

2. Explicit Formula for the \( p \)-th Power

Residue Symbol \( \left( \frac{\eta_1}{(u\xi - v)\mathbb{Z}_M} \right)_M \)

Let \( \xi \) be a primitive \( n \)-th root of unity such that \( p \mid n, L = \mathbb{Q}(\xi), M = L\)K, and let \( u, v \) be any coprime integers. We assume that \( u\xi - v \) is prime to \( p \); this is satisfied if \( p \nmid uv \) or, if not, if \( \frac{v}{u} \) is not of order \( n \) modulo \( p \). If \( u, v \) are not fixed, we must eliminate all the divisors \( n \) of \( p - 1 \). We consider the real cyclotomic unit (see Definition 1.1 (iv))

\[
\eta_1 := (1 + \xi\xi_0^{v/\xi})^{\frac{1}{2}} \in M^+.
\]

Recall that for \( n \leq 2 \), \( \eta_1 = (1 \pm \xi\xi_0^{v/\xi})^{\frac{1}{2}} = \pm 1 \) and the forthcoming computations are not defined, so we assume \( n > 2 \).

If \( d \) is the residue degree of \( p \) in \( L / \mathbb{Q} \), we can write

\[
u\xi - v = (u\xi - v)^{\beta}(1 + p\beta), \quad \beta \text{ } p\text{-integer of } L.
\]
This relation will be interpreted as \( \frac{1}{p} \log (u\xi - v) = \beta \mod p \), where \( \log \) is the \( p \)-adic logarithm (in fact, its class modulo \( p^2 \)).

Set \( \alpha := u\xi - v \). Then using the general \( p \)-th reciprocity law (see, e.g., [5, II.7.4.4]), we obtain, since \( \eta_1 \) is a unit,

\[
\left(\frac{\eta_1}{\alpha}\right)_M = \left(\frac{\eta_1}{\alpha}\right)_M \left(\frac{\alpha}{\eta_1}\right)_M^{-1} = \prod_{\mathfrak{p} \mid p} (\eta_1, \alpha)_{\mathfrak{p}}^{-1} = \prod_{\mathfrak{p} \mid p} (\eta_1, 1 + p\beta)_{\mathfrak{p}}^{-1},
\]

product over the prime ideals \( \mathfrak{p} \) of \( M \) lying above \( p \); since \( M / L \) is totally ramified at \( p \), we shall write by abuse \( (\eta_1, \alpha)_p \) these Hilbert symbols, where \( p \mid p \) in \( L \), knowing that they are defined on \( M^\times / M^{\times p} \times M^\times / M^{\times p} \) with values in \( \langle \zeta \rangle \) (in the literature, two definitions are possible, which give the Hilbert symbol or its inverse; this is the case with the reference [9] used below, by comparison with ours, see, e.g., [5, II.7.3.1]).

We now refer to the Brückner-Vostokov explicit formula [3] explained by Koch in [9, 6.2, Theorem 2.99], by giving some details for the convenience of the reader.

Consider the uniformizing parameter \( \pi := \zeta - 1 \) of the completions \( M_\mathfrak{p} \) of \( M \) at \( \mathfrak{p} \mid p \mid p \). The inertia field is \( L_p \). We need the formal series \( t(x) := 1 - (1 + x)^p \), such that \( t(\pi) = 0 \), for which \( t(x)^{-1} \) is the Laurent series

\[
- \frac{1}{x^p} \left( 1 - p \left( \frac{c_1}{x} + \cdots + \frac{c_{p-1}}{x^{p-1}} \right) + p^2 \left( \frac{c_1}{x} + \cdots + \frac{c_{p-1}}{x^{p-1}} \right)^2 - \cdots \right),
\]

where the \( c_i \) are integers.

We associate with \( \eta_1 \equiv 1 + \theta_1 \mod \pi^2 \), where \( \theta = \frac{1}{2} \frac{\xi - 1}{\xi + 1} \) for \( n \geq 2 \) (see [7, Subsection 4.1]), and \( 1 + p\beta \), the series with coefficients in \( \mathbb{Z}_p[\xi] \).
such that $F(\pi) \equiv \eta_1 \pmod{\pi^2}$ and $G(\pi) = 1 + p\beta$. Recall that log is the $p$-adic logarithm and dlog is the logarithmic derivative; so $d\log(G) = 0$ giving

$$
(F, G) := \left( \frac{1}{p} \log \frac{F^p}{\sigma_p(F)} \right) d\log(G) - \left( \frac{1}{p} \log \frac{G^p}{\sigma_p(G)} \right) \frac{1}{p} d\log \sigma_p(F)
$$

$$= - \left( \frac{1}{p^2} \cdot \log \frac{G^p}{\sigma_p(G)} \right) \cdot d\log(\sigma_p(F)),
$$

where $\sigma_p$ is the Frobenius automorphism in $L_p / \mathbb{Q}_p$ extended to series by putting $\sigma_p(x) := x^p$. Thus $\sigma_p(G) = 1 + p\sigma_p(\beta)$, $\sigma_p(F) = 1 + \sigma_p(\theta)x^p \pmod{(x^{2p})}$, giving

$$
\log \left( \frac{G^p}{\sigma_p(G)} \right) \equiv -p\sigma_p(\beta) \pmod{p^2},
$$

$$d\log(\sigma_p(F)) \equiv p\sigma_p(\theta)x^{p-1} \pmod{(x^{2p}, px^{2p-1})},
$$

and finally, $(F, G) \equiv \sigma_p(\theta)x^{p-1} \pmod{(px^{p-1}, x^{2p-1}, x^{2p} / p)}$. Then the residue of $t(x)^{-1}(F, G)$ is that of

$$
- \frac{1}{x^p} \sigma_p(\theta)x^{p-1} = - \frac{1}{x} \sigma_p(\theta) \in \mathrm{mod}\left( \frac{p}{x^{p-1}}, \frac{x^p}{p} \right),
$$

hence it is $-\sigma_p(\theta \pmod{p})$ since the generator $\frac{x^p}{p}$ of the above ideal gives rise to a residue only with a term of the form $\frac{c_0}{x^{p+1}}$ of $t(x)^{-1}$ (to give $\frac{c_0}{px}$) in which case $c_0$ is a multiple of $p^2$ (see the expression of $t(x)^{-1}$).
A PRODUCT FORMULA RELATED TO THE ...

To conclude we have to take the absolute local trace, which eliminates the action of the Frobenius automorphism and gives

\[ \text{Tr}_{\mathbb{F}_p}/\mathbb{Q}_p (\theta \beta) = (p - 1) \text{Tr}_{\mathbb{L}/\mathbb{Q}_p} (\theta \beta) \equiv \text{Tr}_{\mathbb{L}/\mathbb{Q}_p} (\theta \beta) \pmod{p}. \]

Then \((\eta_1, \alpha)_p = \zeta^{\text{Tr}_{\mathbb{L}/\mathbb{Q}_p} \left( \frac{1}{2} \frac{\xi - 1}{\xi + 1} \beta \right)}\), because of our definition of the Hilbert symbol, and \(\prod_p (\eta_1, \alpha)_p = \zeta^{-\sum_p \text{Tr}_{\mathbb{L}/\mathbb{Q}_p} \left( \frac{1}{2} \frac{\xi - 1}{\xi + 1} \beta \right)} = \zeta^{\text{Tr}_{\mathbb{L}/\mathbb{Q}} \left( \frac{1}{2} \frac{1 - \xi}{1 + \xi} \beta \right)}\), the global trace being the sum of the local ones. We have obtained the following explicit formula:

**Proposition 2.1.** Let \(u, v\) be any coprime integers, let \(\xi\) be a primitive \(n\)-th root of unity, \(n > 2\), \(p \nmid n\), and \(L = \mathbb{Q} (\xi)\). We assume that \(u\xi - v\) is prime to \(p\) (i.e., \(p \mid uv\) or, if not, \(\frac{v}{u}\) is not of order \(n\) modulo \(p\)).

Put \(\eta_1 := (1 + \xi \zeta)^{v} \zeta^{-\frac{1}{2}}\). Then in \(M := LK\), we have

\[ \left( \frac{\eta_1}{(u\xi - v)Z_M / M} \right) = \zeta^{\text{Tr}_{\mathbb{L}/\mathbb{Q}} \left( \frac{1}{2} \frac{1}{1 + \xi} \frac{1}{p} \log(u\xi - v) \right)}, \]

where \(\log\) is the \(p\)-adic logarithm\(^1\) and where \(\text{Tr}_{\mathbb{L}/\mathbb{Q}}\) is the absolute trace in \(L / \mathbb{Q}\).

\[\square\]

\(^1\) The \(p\)-adic logarithm, defined on the group of elements \(\alpha \in L^\times\) prime to \(p\), is a homomorphism of \(\text{Gal}(L / \mathbb{Q})\)-modules. Its computation modulo \(p^2\) comes from the relation \(\alpha = \alpha^{p^d} (1 + p\beta)\), where \(d\) is the residue degree of \(p\) in \(L / \mathbb{Q}\). Such logarithms are related to deep properties of Fermat quotients of the algebraic numbers \(\alpha\) (see, for instance, Hatada [8] for general studies).
3. A Product Formula for the $p$-th Power

Residue Symbols $\left( \frac{\eta}{\Omega} \right)_M$

Let $n > 2$ be such that $p \nmid n$. Let $\xi$ be a primitive $n$-th root of unity and $L := \mathbb{Q}(\xi)$. For any coprime integers $u, v$, we consider $\Phi_n(u, v) := \prod_{\xi \text{ of order } n} (u\xi^r - v) = N_{L/\mathbb{Q}}(u\xi - v)$. We assume that $p \nmid \Phi_n(u, v)$; as we have seen, this is equivalent for $p$ to be a divisor of $uv$ or, if not, to be such that $\frac{v}{u}$ is not of order $n$ modulo $p$. In practice, we shall assume that $n \nmid p - 1$, which implies $n > 2$.

We set $\Phi_n(u, v) = \prod_{q \text{ prime}} q^{m_q}$. For each $q$ dividing $\Phi_n(u, v)$, we note that necessarily $q \nmid uv$ since $\Phi_n(u, v)$ is homogeneous of the form $u^{\phi(n)} + \cdots + v^{\phi(n)}$ ($\phi$ is the Euler totient function); since $q \nmid N_{L/\mathbb{Q}}(u\xi - v)$, the ideal $(q, u\xi - v)$ is a prime ideal of degree 1 lying above $q$ in $L$ (even if $n = n_0q^r$, $q \nmid n_0$, $r \geq 1$, in which case $n_0 \mid q - 1$ is the order of $\frac{v}{u}$ modulo $q$, and $q$ is ramified in $L$, but has residue degree 1 in $L/\mathbb{Q}$; see Lemma 1.3).

This ideal $(q, u\xi - v)$ is denoted $q_{\rho, \xi}$, where $\rho := \frac{v}{u}$; it only depends on $\xi$ and on the class of $\rho$ modulo $q$.

As soon as $u\xi - v \equiv 0 \pmod{q}$ for $q \mid q$ in $L$, the congruence $u\xi - v \equiv 0 \pmod{q'}$, for $t \in \text{Gal}(L/\mathbb{Q})$, implies $q^t = (q, u\xi - v) = q_{\rho, \xi}$.

We then have

$$(u\xi - v)^{Z_L} = \prod_q q_{\rho, \xi}^{m_q}, \text{ with } q_{\rho, \xi} := (q, u\xi - v). \quad (1)$$
3.1. General results and a product formula

Now, we consider the real cyclotomic unit

\[ \eta_1 := (1 + \xi \zeta)^{\rho_0} \zeta^{-\frac{1}{2}} \in M = LK \]

(see Definition 1.1 (iv)).

We have, for each fixed \( q = q_0, \xi \mid q \) in \( L \), where \( f_q \) is the residue degree of \( q \) in \( K / Q \),

\[
\left( \frac{\eta_1}{q^Z_M} \right)_M = \left( \prod_{\Omega \mid q} \left( \frac{\eta_1}{\Omega} \right)_M \right) = \prod_{\Omega \mid q} \left( \frac{\eta_1}{\Omega} \right)_M = \left( \frac{\eta_1}{\Omega} \right)_M^{p-1} \left( \frac{\eta_1}{\Omega} \right)_M^{p-1},
\]

for any choice of \( \Omega \) lying above \( q \) in \( M \) since the symbol of \( \eta_1 \) does not depend on this choice.\(^2\)

For this prime \( q \), set \( n = n_0 q^r, q \mid n_0, r \geq 0 \), as above; put \( \xi = \xi_0 \psi \) (\( \xi_0 \) of order \( n_0, \psi \) of order \( q^r \)). Hence, we have \( q_0 Z_L = (q, u \xi_0 - v) Z_L = q^{[L : L_0]} \). From the congruence,

\[ \eta_1 = (1 + \xi \zeta)^{\rho_0} \zeta^{-\frac{1}{2}} = (1 + \xi_0 \zeta)^{\rho_0} \zeta^{-\frac{1}{2}} =: \eta_1^0 \pmod{\Omega}, \]

for any \( \Omega \mid q \) in \( M \), the \( p \)-th power residue symbols \( \left( \frac{\eta_1}{\Omega} \right)_M \) and \( \left( \frac{\eta_1^0}{\Omega} \right)_M \) are equal. So, we can compute these symbols in \( M_0 := L_0 K \subseteq M \), where \( L_0 := Q(\xi_0) \), since the residue fields of \( \Omega \) and \( \Omega_0 := \Omega \cap Z_{M_0} \) coincide. We obtain from (1) and (2),

\[^2 \text{If } s \in g = \text{Gal}(M / L), \left( \frac{\eta_1}{\Omega} \right)_M^{o(s)} = s \left( \frac{\eta_1}{\Omega} \right)_M = \left( \frac{s \eta_1}{s \Omega} \right)_M = \left( \frac{\eta_1^{o(s)}}{s \Omega} \right)_M = \left( \frac{\eta_1^0}{s \Omega} \right)_M, \]

hence \( \left( \frac{\eta_1}{\Omega} \right)_M = \left( \frac{\eta_1^0}{s \Omega} \right)_M. \)
$$\left( \frac{\eta_1}{(u^\xi - v)Z_M} \right)_M = \prod_q \left( \frac{\eta_1}{\Omega} \right)_q^{p^{-1}m_q} = \prod_q \left( \frac{n_1^0}{\Omega_0} \right)_q^{p^{-1}m_q},$$

where the objects with index 0 depend on $q$.

Then using Proposition 2.1, we obtain in $L$ the general product formula

$$\left( \frac{\eta_1}{(u^\xi - v)Z_M} \right)_M = \zeta T_{L/F} \left( \frac{1}{2^{1+\xi}} \frac{1}{p} \log(u^\xi - v) \right) = \prod_q \left( \frac{n_1^0}{\Omega_0} \right)_q^{p^{-1}m_q}.$$

(3)

### 3.2. Application to the SFLT equation

Now, we assume that the coprime integers $u, v$ are solution of the SFLT equation in the nonspecial cases for $p > 3$. Under this assumption, we have in the relation (3) a more precise expression of $\prod_q \left( \frac{n_1^0}{\Omega_0} \right)_q^{p^{-1}m_q}$ using, for each $q$, Theorem 1.2 for $n_1^0$ instead of $n_1$ to express the symbols of this product.

Let $\kappa_q := \frac{q^f_q - 1}{p}$. The integer $\bar{\kappa}_q := \frac{q^{p-1} - 1}{p}$ is the Fermat quotient of $q$ and we have the relation $\bar{\kappa}_q = \frac{p-1}{f_q} \kappa_q = -\frac{1}{p} \log(q)$ (mod $p$), hence we will have, in the exponent of $\zeta$, the factor

$$\sum_q \frac{p-1}{f_q} \kappa_q m_q = -\sum_q \frac{1}{p} \log(q^{m_q}) = -\frac{1}{p} \log(\Phi_n(u, v)) \pmod{p}$$

multiplied by $\frac{1}{2} \frac{u - v}{u + v}$; consequently, we get from (3)

$$\left( \frac{\eta_1}{(u^\xi - v)Z_M} \right)_M = \zeta T_{L/F} \left( \frac{1}{2^{1+\xi}} \frac{1}{p} \log(u^\xi - v) \right) = \frac{1}{2} \frac{u - v}{u + v} \frac{1}{p} \log(\Phi_n(u, v)).$$

(4)

We obtain, from (4) and obvious calculations, the following necessary conditions:
Proposition 3.1. Let $n$ be such that $p \nmid n$ and $n \mid p - 1$. Let $\xi$ be a primitive $n$-th root of unity and $L := \mathbb{Q}(\xi)$. For any solution in coprime integers $u, v$ of the SFLT equation for $p > 3$ in the nonspecial cases $u + v \equiv 0 \pmod{p}$, we consider $\Phi_n(u, v) := N_{L/\mathbb{Q}}(u \xi - v)$. From $\log(\Phi_n(u, v)) = \text{Tr}_{L/\mathbb{Q}}(\log(u \xi - v))$, we obtain the congruence

$$\text{Tr}_{L/\mathbb{Q}}\left(\frac{u \xi - v}{1 + \xi} - \frac{1}{p} \log(u \xi - v)\right) \equiv 0 \pmod{p}.$$  

Recall that the assumption $n \mid p - 1$ implies $p \mid \Phi_n(u, v)$.

Proposition 3.2. Let $(u, v)$ be a solution of the SFLT equation such that $p \nmid uv(u^2 - v^2)$. Then $\frac{1}{p} \log(u) \equiv \frac{1}{p} \log(v) \equiv 0 \pmod{p}$. Hence $u^{p-1} \equiv v^{p-1} \equiv 1 \pmod{p^2}$.

Proof. This follows from the generalization to the SFLT equation of the first theorem of Furtwängler proved in [7, Corollary 2.10].

3.3. Study of the nonspecial cases

We have from Proposition 3.1 the necessary condition, for any $n$ with $p \nmid n$ & $n \mid p - 1$, where $\xi$ is any primitive $n$-th root of unity,

$$\text{Tr}_{L/\mathbb{Q}}\left(\frac{u \xi - v}{1 + \xi} - \frac{1}{p} \log(u \xi - v)\right) \equiv 0 \pmod{p}.$$  

Using complex conjugation, we get $\text{Tr}_{L/\mathbb{Q}}\left(\frac{u \xi^{-1} - v}{1 + \xi^{-1}} - \frac{1}{p} \log(u \xi^{-1} - v)\right) \equiv 0 \pmod{p}$ (mod $p$) giving easily the symmetrical formula $\text{Tr}_{L/\mathbb{Q}}\left(\frac{u - v \xi}{1 + \xi} - \frac{1}{p} \log(u - v \xi)\right) = 0 \pmod{p}$. So, we can assume $u$ prime to $p$ (i.e., $p \mid v$ in the second case). With $\rho := \frac{v}{u}$, we obtain from (5) after division by $u$ and using Proposition 3.2,
We have proved the following “product formula” in additive form:

**Theorem 3.3.** Let \( p \) be a prime \( > 3 \). Suppose given a solution, in coprime integers \( u, v, u \neq 0 \mod p \), \( u + v \neq 0 \mod p \), of the SFLT equation for \( p \). Set \( \rho := \frac{u}{v} \). Then for all \( n \) such that \( p \nmid n \) and \( n \nmid p - 1 \), we have the congruence

\[
\text{Tr}_{L/Q}\left( \frac{\xi - \rho}{1 + \xi \rho} \log(u \xi - up) \right) = \text{Tr}_{L/Q}\left( \frac{\xi - \rho}{1 + \xi \rho} \left( \frac{1}{p} \log(u) + \frac{1}{p} \log(\xi - \rho) \right) \right) = \text{Tr}_{L/Q}\left( \frac{\xi - \rho}{1 + \xi \rho} \log(\xi - \rho) \right) = 0 \mod p.
\]

where \( \xi \) is a primitive \( n \)-th root of unity and \( L = \mathbb{Q}(\xi) \).

**Remark 3.4.** In the context of Theorem 3.3, the solution \((u, v)\) is of course fixed, but to get a contradiction, we can hope that \( u \) (unknown) being fixed, none of the values of \( v \) (i.e., of \( \rho \)), modulo a power of \( p \) to be precised, agree with the congruences of the theorem. For arbitrary rationals \( \rho \), the expression

\[
\mathcal{M}_n(\rho) := \text{Tr}_{L/Q}\left( \frac{\xi - \rho}{1 + \xi \rho} \log(\xi - \rho) \right) \mod p,
\]

is only constant on the class of \( \rho \) modulo \( p^2 \) (because of the logarithm of \( \xi - \rho \)); thus, it is a priori sufficient to study this expression for the \( p(p - 1) \) values modulo \( p^2 \) of \( \rho - 1 \mod p \). In fact, we can significantly reduce this number. See Sections 4 and 5 for general results in the first case with \( u - v \neq 0 \mod p \), hence \( \rho \neq 0, 1, -1 \mod p \), giving by a suitable symmetry \( \frac{p - 3}{2} \) conditions to be satisfied to get a contradiction to the existence of the solution \((u, v)\).
Remark 3.5. We shall need the traces $T := \text{Tr}_L/Q\left(\frac{1}{1 + \xi}\right)$ and $T' := \text{Tr}_L/Q\left(\frac{\xi}{1 + \xi}\right)$. We compute that $T' = \text{Tr}_L/Q\left(\frac{\xi^{-1}}{1 + \xi^{-1}}\right) = \text{Tr}_L/Q\left(\frac{1}{1 + \xi}\right) - T$. Then $T' = \text{Tr}_L/Q\left(\frac{1 + \xi^{-1}}{1 + \xi}\right) = \phi(n) - T$, giving $T = \frac{\phi(n)}{2}$.

4. Analysis and Simplification of the General Condition

Let $p > 3$. We assume that $p \nmid n$ and $n \nmid p - 1$. Set, for any rational $\rho := \frac{u}{v}$, $\rho \neq 0, 1, -1 \pmod{p}$ (first case of SFLT with the condition $u - v \neq 0 \pmod{p}$),

$$M_n(\rho) := \text{Tr}_L/Q\left(\frac{\xi - \rho}{1 + \xi} \frac{1}{p} \log(\xi - \rho)\right)$$ (see Theorem 3.3 and Remark 3.4).

Since the class modulo $p$ of $M_n(\rho)$ is constant on the class modulo $p^2$ of $\rho$, we look at $M_n(\rho_0 + \lambda p) = \text{Tr}_L/Q\left(\frac{\xi - \rho_0 - \lambda p}{1 + \xi} \frac{1}{p} \log(\xi - \rho_0 - \lambda p)\right)$, where $\rho_0$ is the representative in $[2, p - 2]$ of the class modulo $p$ of $\rho$ and $\lambda$ any integer modulo $p$. Thus,

$$M_n(\rho_0 + \lambda p) = \text{Tr}_L/Q\left(\frac{\xi - \rho_0}{1 + \xi} \frac{1}{p} \log(\xi - \rho_0)\right) + \text{Tr}_L/Q\left(\frac{\xi - \rho_0}{1 + \xi} \frac{1}{p} \log(1 - \frac{\lambda p}{\xi - \rho_0})\right)$$

$$- \text{Tr}_L/Q\left(\frac{\lambda p}{1 + \xi} \frac{1}{p} \log(\xi - \rho_0)\right) - \text{Tr}_L/Q\left(\frac{\lambda p}{1 + \xi} \frac{1}{p} \log(1 - \frac{\lambda p}{\xi - \rho_0})\right)$$

$$= M_n(\rho_0) - \lambda T_{L/Q}\left(\frac{1}{1 + \xi}\right) = M_n(\rho_0) - \lambda \frac{\phi(n)}{2} \pmod{p}.$$
As a consequence, we note that if $\phi(n) \not\equiv 0 \pmod{p}$, there is a unique value of $\lambda$ modulo $p$ such that $\mathcal{M}_n(\rho_0 + \lambda p)$ is in a given class modulo $p^2$. If $\phi(n) \equiv 0 \pmod{p}$, we have $\mathcal{M}_n(\rho_0 + \lambda p) \equiv \mathcal{M}_n(\rho_0) \pmod{p}$ for all $\lambda$ modulo $p$. In fact, we shall see in Section 5 that, in that case, $\mathcal{M}_n(\rho_0) \equiv 0 \pmod{p}$ for all $\rho_0 \in [2, p-2]$.

**Theorem 4.1.** Let $(u, v)$ be a solution of the SFLT equation in the first case for $p > 3$; we assume that $u - v \not\equiv 0 \pmod{p}$. Let $\rho_0$ be the representative in $[2, p-2]$ of the class modulo $p$ of $\rho := \frac{v}{u}$; set $\rho \equiv \rho_0 + \lambda_0 p \pmod{p^2}$. Let $(n, m)$ be any pair of integers such that $p \nmid nm$, $n \nmid p - 1$, and $m \nmid p - 1$.

Then the conditions $\mathcal{M}_n(\rho_0 + \lambda p) \equiv 0 \pmod{p}$ and $\mathcal{M}_m(\rho_0 + \lambda p) \equiv 0 \pmod{p}$ are incompatible for the class of $\rho_0$ modulo $p^2$ (i.e., for all $\lambda$ modulo $p$, hence for the right $\rho := \rho_0 + \lambda_0 p$) as soon as $\phi(m)\mathcal{M}_n(\rho_0) \not\equiv \phi(n)\mathcal{M}_m(\rho_0) \pmod{p}$.

**Proof.** From Theorem 3.3, we have $\mathcal{M}_n(\rho_0 + \lambda_0 p) \equiv 0 \pmod{p}$ and, in the same way, $\mathcal{M}_m(\rho_0 + \lambda_0 p) \equiv 0 \pmod{p}$.

From the relations $\mathcal{M}_n(\rho_0 + \lambda p) \equiv \mathcal{M}_n(\rho_0) - \lambda \frac{\phi(n)}{2}$ and $\mathcal{M}_m(\rho_0 + \lambda p) \equiv \mathcal{M}_m(\rho_0) - \lambda \frac{\phi(m)}{2} \pmod{p}$ for any $\lambda$ modulo $p$, multiplying by $\phi(m)$ and $\phi(n)$, respectively, we obtain the result, which only depends on $\rho_0$. \( \square \)

In other words, to get a contradiction, it is sufficient to check the condition for the $p - 3$ classes modulo $p$ instead of the $p(p-3)$ classes modulo $p^2$. In fact, we need the verification only for $\frac{p-3}{2}$ values of $\rho_0$, chosen up to inversion modulo $p$ (see Remark 5.4 (ii)).
Corollary 4.2. The first case of SFLT under the condition \( u - v \neq 0 \pmod{p} \) (as well as the first case of Fermat’s last theorem) holds for \( p > 3 \) as soon as for each of the \( \frac{p - 3}{2} \) values \( \rho_0 = 2, \ldots, p - 2 \) (chosen up to inversion modulo \( p \)), there exists a pair \((n, m)\) of integers (\( n \) and \( m \) coprime to \( p \), not dividing \( p - 1 \)) such that \( \phi(n)M_m(\rho_0) \neq \phi(m)M_n(\rho_0) \pmod{p} \), where \( M_n(\rho_0) \) (resp., \( M_m(\rho_0) \)) is equal to \( \text{Tr}_{L/Q} \left( \frac{\xi - \rho_0}{1 + \xi} \frac{1}{p} \log(\xi - \rho_0) \right) \) for \( \xi \) of order \( n \) (resp., \( m \)).

We shall prove Theorem 5.5 giving an important simplification from some insights in the computation of the \( M_n(\rho_0) \), by showing that \( M_n(\rho_0) = 0 \pmod{p} \) for all \( \rho_0 \in [2, p - 2] \) occurs for some specific integers \( n_0 \) (which is stronger than the existence of \( n_0 \) depending on \( \rho_0 \)).

5. Expression of the Necessary Condition by Means of Canonical Traces

5.1. Explicit calculation of \( M_n(\rho) := \text{Tr}_{L/Q} \left( \frac{\xi - \rho}{1 + \xi} \frac{1}{p} \log(\xi - \rho) \right) \pmod{p} \), \( p > 3 \)

We return to the general necessary condition of Theorem 3.3 for the existence of a solution \((u, v)\) of the SFLT equation in the case \( uv(u^2 - v^2) \neq 0 \pmod{p} \)

\[ \text{Tr}_{L/Q} \left( \frac{\xi - \rho}{1 + \xi} \frac{1}{p} \log(\xi - \rho) \right) = 0 \pmod{p} \), for all \( n(p \nmid n, n \nmid p - 1) \),

where \( \rho := \frac{v}{u} \), \( \xi \) is a primitive \( n \)-th root of unity, and \( L = \mathbb{Q}(\xi) \). We have

\[ \frac{1}{p} \log(\xi - \rho) = \frac{1}{p} (1 - (\xi - \rho)^p - 1) \pmod{p} , \]
$d$ being the residue degree of $p$ in $L/\mathbb{Q}$ (note that $d \geq 2$ since $n \nmid p - 1$).

So,

$$
\frac{\xi - \rho}{1 + \frac{1}{\xi}} \frac{1}{p} \log(\xi - \rho) = \frac{\xi - \rho}{1 + \frac{1}{\xi}} \frac{1}{p} (1 - (\xi - \rho)^{p^d - 1})
$$

$$
= \frac{1}{1 + \frac{1}{\xi}} \frac{1}{p} (\xi - \rho - (\xi - \rho)^{p^d}) \pmod{p}.
$$

The computation of $(a + b)^{p^d} \pmod{p^2}$ is given as follows:

From $(a + b)^p = a^p + b^p + p \sum_{k=1}^{p-1} c_p^k a^{p-k} b^k$, where the $c_p^k := \frac{1}{p} \cdot \xi_p^k$

are integers, we get

$$(a + b)^{p^d} = a^{p^d} + b^{p^d} + p \sum_{k=1}^{p-1} c_p^k A^{p-k} B^k \pmod{p^2},$$

where $A := a^{p^{d-1}}$, $B := b^{p^{d-1}}$. Since $\xi^{p^d} = \xi$ by definition and since for a rational $r$, $r^{p^d} \equiv r^p \pmod{p^2}$, we obtain the expression $(A = \xi^{p^{d-1}}$, $B = -\rho^d$)

$$(\xi - \rho)^{p^d} \equiv \xi - \rho^p + p \sum_{k=1}^{p-1} (-1)^k c_p^k (\rho^p)^k \xi^{1-kp^{d-1}} \pmod{p^2}.$$ 

Then this yields

$$\frac{1}{p} (\xi - \rho - (\xi - \rho)^{p^d}) = \frac{1}{p} (\rho^p - \rho) - \sum_{k=1}^{p-1} (-1)^k c_p^k (\rho^p)^k \xi^{1-kp^{d-1}} \pmod{p}.$$ 

From Proposition 3.2 and from the congruence $c_p^k = \frac{(p-1)\cdots(p-(k-1))}{1\cdots(k-1)k} \equiv (-1)^{k-1} \frac{1}{k} \pmod{p}$, we obtain $\frac{1}{p} (\rho^p - \rho) = 0 \pmod{p}$ and
\[
\frac{1}{1 + \xi} \frac{1}{p} (\xi - p - (\xi - p)^p) \equiv \sum_{k=1}^{p-1} \frac{1}{k} p^k \frac{\xi^{1-kp^d-1}}{1 + \xi} \quad \text{(mod } p)\].

We have, using the Frobenius automorphism of \( p \) and complex conjugation

\[
\text{Tr}_{L/Q}\left(\frac{\xi^{1-kp^d-1}}{1 + \xi}\right) = \text{Tr}_{L/Q}\left(\frac{\xi^{p-k}}{1 + \xi^p}\right) = \text{Tr}_{L/Q}\left(\frac{\xi^{-k}}{1 + \xi^{-p}}\right) = \text{Tr}_{L/Q}\left(\frac{\xi^k}{1 + \xi^p}\right),
\]

giving the necessary condition for the nonspecial cases of the SFLT equation

\[
\mathcal{M}_n(p) \equiv \sum_{k=1}^{p-1} \frac{1}{k} p^k \text{Tr}_{L/Q}\left(\frac{\xi^k}{1 + \xi^p}\right) = 0 \quad \text{(mod } p)\]

The knowledge, for \( k = 1, \ldots, p-1 \), of the traces (where \( 1/p \) is seen in \((\mathbb{Z}/n\mathbb{Z})^\times\))

\[
t_{n,k} := \text{Tr}_{L/Q}\left(\frac{\xi^k}{1 + \xi^p}\right) = \text{Tr}_{L/Q}\left(\frac{\xi^{kp}/p}{1 + \xi}\right) \quad \text{(mod } p),
\]

will be used for numerical proof of the first case of SFLT with \( u - v \neq 0 \) (mod \( p \)), using Theorem 5.5 below. We can use the obvious symmetry \( t_{n,p-k} = t_{n,k} \).

5.2. Some exceptional values of the traces \( t_{n,k} \)

We have obtained some informations by systematic numerical calculations. In particular, we have found the following surprising result of nullity of these traces in some circumstances:

**Theorem 5.1.** Let \( p \) be a prime \( \geq 3 \). Let \( \ell \neq p, \ell \nmid p-1 \), be an odd prime. For any rational \( \frac{a}{b} \) with \( \ell \nmid b \), let \( \left\lfloor \frac{a}{b} \right\rfloor_\ell \) be the representative in \([0, \ell - 1]\) of \( \frac{a}{b} \) modulo \( \ell \).
(i) Then $t_{\ell,k} := \text{Tr}_{L/Q} \left( \frac{\zeta^{k/p}}{1 + \zeta} \right) = \frac{\epsilon_k \ell - 1}{2}$, where $\epsilon_k = (-1)^{\left\lfloor \frac{-k}{p} \right\rfloor}$ for all $k \in [1, p-1]$.

(ii) If $\ell \equiv \epsilon \pmod{p}$, where $\epsilon \equiv \pm 1$, then $t_{\ell,k} = \frac{\epsilon \ell - 1}{2} \equiv 0 \pmod{p}$, for all $k \in [1, p-1]$.

**Proof.** We have the identity $X^\ell - 1 = (1 + X)(1 - X + X^2 - \cdots + X^{\ell-1}) - 2$, hence $\frac{2}{1+X} = 1 - X + X^2 - \cdots + X^{\ell-1} \pmod{\Phi_\ell(X)}$, and, for $k \in [1, p-1],$

$$2\text{Tr}_{L/Q} \left( \frac{\zeta^{k/p}}{1 + \zeta} \right) = \sum_{i=0}^{\ell-1} (-1)^i \text{Tr}_{L/Q} \left( \zeta^{i+k/p} \right) = \sum_{i=0}^{\ell-1} (-1)^i \text{Tr}_{L/Q} \left( \zeta^{ip+k} \right).$$

The trace of $\zeta^{ip+k}$ is $-1$ except for the solutions $i_k$ of the congruence $ip + k \equiv 0 \pmod{\ell}$ in the interval $[0, \ell-1]$, in which case we obtain the trace $\ell - 1$. The congruence has, for each fixed $k$, a unique solution $i_k = \left\lfloor \frac{-k}{p} \right\rfloor$ in this interval.

We then have $2t_{\ell,k} = \sum_{i=0}^{\ell-1} (-1)^i (-1) - (-1)^{i+k}(-1) + (-1)^i(\ell - 1)$. This proves the first point of the theorem since when $i_k$ is odd, we find $t_{\ell,k} = -\frac{\ell + 1}{2}$, otherwise $t_{\ell,k} = \frac{\ell - 1}{2}$.

Now suppose that $\ell = \epsilon + \mu p$, $\epsilon = \pm 1$, $\mu \geq 2$. For $\epsilon = 1$, we get $i_k = \mu k$, which is even since $\mu$ is even; moreover, we have $\mu k = \frac{\ell - 1}{p} < \ell - 1$; so

$$t_{\ell,k} = \frac{\ell - 1}{2} \equiv 0 \pmod{p}.$$ If $\epsilon = -1$, we get $i_k = -1 + \mu(p-k) \in [0, \ell - 1]$, which is odd; thus $t_{\ell,k} = -\frac{\ell + 1}{2} \equiv 0 \pmod{p}$. □
The property is proved in the prime case \((n_0 = \ell \equiv \pm 1 \pmod{p})\), but clearly numerical calculations show that the general statement may be the following:

If \(n_0 = \ell m, \ell \equiv \epsilon \pmod{p}, \ell \text{ prime, } m \neq 2, p \nmid m\), then \(t_{n_0,k} \equiv 0 \pmod{p}\) for all \(k \in [1, p-1]\).

**Corollary 5.2.** *In the case \(\ell \equiv -1 \pmod{p}\), \(n_0 = \ell m\) is such that \(\phi(n_0)\) is prime to \(p\) as soon as there is no prime \(\ell' \equiv 1 \pmod{p}\) dividing \(n_0\). Thus, there exist infinitely many \(n_0\) such that \(\phi(n_0) \neq 0 \pmod{p}\) and \(t_{n_0,k} \equiv 0 \pmod{p}\), for all \(k \in [1, p-1]\).*

We can restrict ourselves to \(n_0 = \ell \equiv -1 \pmod{p}\) prime, so that \(\phi(n_0) \equiv -2 \pmod{p}\).

### 5.3. General statement in the first case

Recall first the results of Subsection 5.1 in the following statement restricted to the first case with \(u - v \neq 0 \pmod{p}\), i.e., \(\rho_0 \neq 0, 1, p - 1\):

**Proposition 5.3.** *Let \(p\) be a prime \(> 3\). Suppose given a solution, in coprime integers \(u, v\), of the first case of the SFLT equation for \(p\) with \(u - v \neq 0 \pmod{p}\). Set \(\rho := \frac{v}{u}\) and let \(\rho_0\) be the representative in \([2, p - 2]\) of the class modulo \(p\) of \(\rho\).*

*For any \(n > 2\), let \(\xi\) be a primitive \(n\)-th root of unity, \(L = \mathbb{Q}(\xi)\), and \(t_{n,k} := \text{Tr}_{L/\mathbb{Q}}\left(\frac{\xi^k}{1 + \xi^p}\right)\) for \(k = 1, \ldots, p - 1\). Then for all \(n\) such that \(p \nmid n\) and \(n \nmid p - 1\), we have the congruence

\[
\mathcal{M}_n(\rho_0) := \sum_{k=1}^{p-1} \rho_0^k t_{n,k} \equiv 0 \pmod{p}.
\]

**Remark 5.4.** *(i)* We have \(\mathcal{M}_n(\rho_0) = \sum_{k=1}^{p-1} \omega^{-1}(k)\rho_0^k t_{n,k} \pmod{p}\); the notation \(\mathcal{M}\) is used by analogy with that of the Mirimanoff polynomials...
\[ M_{\omega} (Z) := \sum_{k=1}^{p-1} \omega^k Z^k, \] also denoted \( M_{p-h} (Z) \) in the literature, defined for any \( h \in [0, p-1] \) (see [6, Subsection 3.1] and Section 6).

(ii) If \( \rho_0^* \in [2, p-2] \) is inverse modulo \( p \) of \( \rho_0 \), we have

\[ \rho_0^{-1} \mathcal{M}_n (\rho_0^*) = \sum_{k=1}^{p-1} \frac{1}{k} \rho_0^{*k-1} t_{n,k} = \sum_{k=1}^{p-1} \frac{1}{k} \rho_0^{1-k} t_{n,k} \pmod{p}. \]

Set \( k = p - j \); then since \( \rho_0^{p-1} = 1 \pmod{p} \), we obtain \( \rho_0^{-1} \mathcal{M}_n (\rho_0^*) = -\sum_{j=1}^{p-1} \frac{1}{j} \rho_0^j t_{n,j} = -\mathcal{M}_n (\rho_0) \pmod{p} \). So \( \mathcal{M}_n (\rho_0^*) = -\rho_0 \mathcal{M}_n (\rho_0) \). Thus, we can restrict ourselves to the \( \frac{p-3}{2} \) values of \( \rho_0 \) chosen up to inversion modulo \( p \).

From Corollary 5.2, giving infinitely many \( n_0 \) such that \( \phi(n_0) \neq 0 \pmod{p} \) and \( \mathcal{M}_{n_0} (\rho_0) : = \sum_{k=1}^{p-1} \frac{1}{k} \rho_0^k t_{n_0,k} = 0 \pmod{p} \) for all \( \rho_0 \in [2, p-2] \) (because of the nullity of all the traces \( t_{n_0,k} \)), we have obtained

**Theorem 5.5.** Let \( p \) be a prime > 3. For any \( n > 2 \), let \( \xi \) be a primitive \( n \)-th root of unity, \( L = \mathbb{Q}(\xi) \), and \( t_{n,k} := \text{Tr}_{L/\mathbb{Q}} \left( \frac{\xi^k}{1 + \xi^p} \right) \), \( k = 1, \ldots, p-1 \).

The first case of SFLT under the condition \( u - v \neq 0 \pmod{p} \) (as well as the first case of FLT) holds for \( p \) as soon as for each \( \rho_0 \in [2, p-2] \) (chosen up to inversion modulo \( p \)), there exists an integer \( n \) \((p \nmid n, n \nmid p-1)\) such that \( \mathcal{M}_n (\rho_0) : = \sum_{k=1}^{p-1} \frac{1}{k} \rho_0^k t_{n,k} \neq 0 \pmod{p} \).

**Remark 5.6.** If we take into account the symmetry of the coefficients \( t_{n,k} \), and the relation \( \frac{1}{p-k} = \frac{-1}{k} \pmod{p} \), a contradiction is given as soon as for each \( \rho_0 \in [2, p-2] \) (chosen up to inversion), there exists \( n \) \((p \nmid n, n \nmid p-1)\) such that
$$\mathcal{M}_n(\rho) = \sum_{k=1}^{(p-1)/2} \frac{1}{k} (\rho^k_0 - \rho_0^{p-k}) t_{n,k} \not\equiv 0 \pmod{p}.$$ 

Note that $\rho^k_0 - \rho_0^{p-k} \equiv 0 \pmod{p}$ is equivalent to $\rho_0^{2k-1} \equiv 1 \pmod{p}$ since $\rho_0 \neq 0$, and the solutions $k$ depend on the order of $\rho_0$ modulo $p$. But not all the coefficients $\rho^k_0 - \rho_0^{p-k}$ can be trivial modulo $p$ since $\rho_0 \neq 0, 1$.

So, the relation $\sum_{k=1}^{(p-1)/2} \frac{1}{k} (\rho^k_0 - \rho_0^{p-k}) t_{n,k} \equiv 0 \pmod{p}$ defines a hyperplane $\mathcal{H}_{\rho_0}$ of $\mathbb{F}_p^2$ and a proof of SFLT in the first case with $u - v \neq 0 \pmod{p}$ would result of the fact that not all the vectors $(t_{n,1}, \ldots, t_{n,(p-1)/2}) \pmod{p}$ are in this hyperplane as $n$ varies. 

**Example 5.7.** For $p = 5(n = 3), p = 7(n = 4), p = 11(n = 3), p = 13(n = 5), p = 17(n = 3), p = 19(n = 4), p = 23(n = 3), p = 29(n = 3)$, the value 0 never occurs for $\mathcal{M}_n(\rho_0) \pmod{p}$ for $\rho_0 \in [2, p - 2]$.

The first case giving $\mathcal{M}_n(\rho_0) \equiv 0 \pmod{p}$ for some $\rho_0$ takes place for $p = 31(n = 4)$ with $\rho_0 = 10$ and its inverse 28; but with $n = 7$, all the results are nonzero modulo $p$ (of course, this sufficient condition is not necessary since it is required to find some $n$ such that $\mathcal{M}_n(\rho_0) \not\equiv 0 \pmod{p}$ for the above critical values of $\rho_0$).

For the other values of $p < 100$, we give the minimal allowed $n (p \nmid n, n \nmid p - 1)$, the values of $\rho_0$ such that $\mathcal{M}_n(\rho_0) \equiv 0 \pmod{p}$ (if any), then we look at the increasing values of $n$ which, in general, leads to the conclusion after few tests; for instance, for $p = 59$, the minimal value giving the response is $n = 4$, and for $p = 97$, the minimal value is $n = 7$. Then we give the least $n$ (written $(n)$) such that $\mathcal{M}_n(\rho_0) \not\equiv 0 \pmod{p}$ for all $\rho_0$. Of course, the existence of such an universal $n$ for $p$ is a very strong condition, which is not required for the conclusion.
For all these examples, we have proved the first case of SFLT (under the condition \( u - v \equiv 0 \pmod{p} \)) and of course unconditionally the first case of FLT, in a new numerical setting.
5.4. Study of the $t_{n,k} := \text{Tr}_{L/Q}\left(\frac{\xi^{k/p}}{1+\xi}\right) = \text{Tr}_{L/Q}\left(\frac{\xi^k}{1+\xi^{p}}\right)$, $k = 1, \ldots, p-1$

We give some explicit computations for particular values of $n$. We always assume that $p \nmid n$ and $n \nmid p - 1$. We first give a general formula, which may be convenient for numerical calculations. For any rational $\frac{a}{b}$, with $b$ prime to $n$, we denote by $[\frac{a}{b}]_n$ the representative in $[0, n-1]$ of $\frac{a}{b} \pmod{n}$.

We have $t_{n,k} := \text{Tr}_{L/Q}\left(\frac{\xi^{k/p}}{1+\xi}\right) = \text{Tr}_{L/Q}\left(\frac{\xi^h}{1+\xi}\right)$, where $h = h_k := \left[\frac{k}{p}\right]_n$. Then this yields

$$\frac{\xi^h}{1+\xi} = \frac{\xi^h - (-1)^h}{1+\xi} + \frac{(-1)^h}{1+\xi} = \xi^{-h-1} - \xi^{-h-2} + \cdots + (-1)^h \xi^{-h} + \frac{(-1)^h}{1+\xi}.$$ 

Hence, we obtain

$$t_{n,k} = (-1)^{h+1}\left(\sum_{j=0}^{h-1} (-1)^j \text{Tr}_{L/Q}\left(\xi^j\right) - \frac{\phi(n)}{2}\right),$$

with $h = \left[\frac{k}{p}\right]_n$ and the usual formula $\text{Tr}_{L/Q}\left(\xi^j\right) = \mu\left(\frac{n}{d_j}\right) \frac{\phi(n)}{d_j}$, where $\mu$ is the Moebius function and $d_j = \gcd(j, n)$, $j = 0, \ldots, h-1$.

5.4.1. Case $n$ odd. We then have the identity $(1 + X)(1 - X + \cdots + X^{n-1}) = 2 + X^n - 1$, giving $\frac{\xi^{k/p}}{1+\xi} = \frac{1}{2} \sum_{i=0}^{n-1} (-1)^i \xi^{i+k/p}$, hence $t_{n,k} = \text{Tr}_{L/Q}\left(\frac{\xi^{k/p}}{1+\xi}\right) = \frac{1}{2} \sum_{i=0}^{n-1} (-1)^i \text{Tr}_{L/Q}(\xi^{ip+k})$. Let $d_{i,k} := \gcd(ip + k, n)$.
and let $I_{d,k}^n := \{ i \in [0, n-1], \text{g.c.d.}(ip + k, n) = d \}$ for any divisor $d$ of $n$.

Then $t_{n,k} = \frac{1}{2} \sum_{d \mid n} \sum_{i \in I_{d,k}^n} (-1)^j \text{Tr}_{L/\mathbb{Q}}(\zeta^d)$, hence

$$t_{n,k} = \frac{1}{2} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \frac{\phi(n)}{\phi(n/d)} \sum_{i \in I_{d,k}^n} (-1)^j, \quad k = 1, \ldots, p-1.$$

5.4.2. Case $n = 2m$, with $m > 1$ odd. For $\xi'$ of order $m$, we have $\zeta = -\zeta'$ so that $t_{2m,k} = \text{Tr}_{L/\mathbb{Q}}\left(\frac{\xi'^{kp^{**}}}{1 + \xi'}\right)$, where $p^{**}$ is inverse of $p$ modulo $n$ ($\xi \mapsto \xi^{p^{**}}$ must be the inverse of the Frobenius automorphism of $p$ in $L/\mathbb{Q}$), so that $p^{**}$ is odd and $t_{2m,k} = \text{Tr}_{L/\mathbb{Q}}\left(\frac{(-\xi')^{kp^{**}}}{1 - \xi'}\right) = (-1)^k \text{Tr}_{L/\mathbb{Q}}\left(\frac{\xi^{kp^{**}}}{1 - \xi'}\right)$, $p^*$ being the inverse of $p$ modulo $m$ in $[1, m-1]$. Then we have obtained $t_{2m,k} = (-1)^k \text{Tr}_{L/\mathbb{Q}}\left(\frac{\xi^{h}}{1 - \xi'}\right)$, where $h = h_k := \left\lfloor \frac{k}{Lp} \right\rfloor$.

We have

$$\text{Tr}_{L/\mathbb{Q}}\left(\frac{\xi^{h}}{1 - \xi'}\right) = \text{Tr}_{L/\mathbb{Q}}\left(\frac{\xi^{h-1} + 1}{1 - \xi'}\right) = -\text{Tr}_{L/\mathbb{Q}}(1 + \xi' + \ldots + \xi'^{h-1}) + \frac{\phi(m)}{2} \quad \text{since} \quad \frac{1}{1 - \xi'} = \frac{1}{1 + \xi'} \quad \text{and} \quad \phi(n) = \phi(m), \quad \text{which gives}$$

$$t_{2m,k} = (-1)^{k+1} \left\{ \text{Tr}_{L/\mathbb{Q}}(1 + \xi' + \ldots + \xi'^{\left\lfloor \frac{k}{Lp} \right\rfloor m - 1}) - \frac{\phi(m)}{2} \right\}, \quad k = 1, \ldots, p-1,$$

with the usual calculation of the $\text{Tr}_{L/\mathbb{Q}}(\xi'^j)$ as in 5.4.1.
5.4.3. Case \( n = 2\ell \), with \( \ell > 2 \) prime. The above computation for \( m = \ell \) prime gives
\[
t_{2\ell, k} = (-1)^{k+1} \left( \ell - 1 - (h-1) - \frac{\ell - 1}{2} \right) = (-1)^{k+1} \left( \ell + 1 - \left\lfloor \frac{k}{p} \right\rfloor \right), \quad k = 1, \ldots, p-1.
\]

5.4.4. Case \( n = 2^r \), \( r \geq 2 \). We have the identity \((1 + X)(X^{2^{r-1}} - X^{2^{r-1}-2} + \cdots + 1) + 2 = X^{2^{r-1}} + 1\), hence \( \frac{2}{1+X} = \sum_{i=0}^{2^{r-1}-1} (-1)^i X^i \) (mod \( X^{2^{r-1}} + 1 \)), giving
\[
t_{2^r, k} = \frac{1}{2} \sum_{i=0}^{2^{r-1}-1} (-1)^i \text{Tr}_{L/Q}(\zeta^{i+k}/p) = \frac{1}{2} \sum_{i=0}^{2^{r-1}-1} (-1)^i \text{Tr}_{L/Q}(\zeta^{i+k}p).
\]

The traces \( \text{Tr}_{L/Q}(\zeta^{i+k}p) \) are zero except when \( \zeta^{i+k} = \pm 1 \), hence when \( i + k = 0 \) (mod \( 2^{r-1} \)); this congruence admits exactly one solution \( i_k = \left\lfloor \frac{-k}{p} \right\rfloor \) in \( [0, 2^{r-1} - 1] \). From the relation \( i_k p + k = : \lambda_k 2^{r-1} \), we note that \( i_k \) and \( k \) have same parity and that \( \lambda_k < p \); hence \( \lambda_k = \left\lfloor \frac{k}{2^{r-1}} \right\rfloor \). Since \( \zeta^{i_k p+k} = (-1)^{\lambda_k} \), we get
\[
t_{2^r, k} = (-1)^{k+1} \left\lfloor \frac{k}{2^{r-1}} \right\rfloor, \quad k = 1, \ldots, p-1.
\]

5.4.5. Case \( n = 2^{(p+1)/2} \). Now, we suppose that \( r = \frac{p+1}{2} \) in the previous computations. Let \( i_k p + k = : \lambda_k 2^{(p-1)/2} \), \( \lambda_k \geq 1 \). We have \( k = \lambda_k \epsilon \) (mod \( p \)), where \( \epsilon = \pm 1 \) and \( \lambda_k < p \), so that \( \lambda_k = k \), if \( \epsilon = 1 \) and \( \lambda_k = p - k \), if \( \epsilon = -1 \). Moreover, \( i_k \) and \( k \) have the same parity. We have \( \zeta^{i_k p+k} = (-1)^{\lambda_k} \) and whatever the case, we obtain
\[ t_{g(p+1)/2, k} = \frac{1}{2} (-1)^k (-1)^{\lambda_k} 2^{(p-1)/2} = \frac{1}{2} (-1)^k (-1)^{\lambda_k} \equiv \frac{1}{2} \pmod{p}. \]

This case leads to check \( M_\rho(p_0) = \sum_{k=1}^{p-1} \frac{1}{k} p_0^k \) modulo \( p \) for \( p_0 \in [2, p-2] \) (up to inversion), not to be confused with \( M_\omega(-\rho_0) \equiv 0 \pmod{p} \) (see Section 6, (ii)); the critical values of \( \rho_0 \) come from the roots in \( F_p \setminus \{0, 1, -1\} \) of the Mirimanoff polynomial \( M_\omega \).

5.4.6. Case \( n = \ell^r, \ell > 2 \text{ prime}, r \geq 1 \). We consider the identity

\[ X^{\ell^r} - 1 = (1 + X)(1 - X + \cdots - X^{\ell^r-2} + X^{\ell^r-1}) \]

\( X^i \pmod{X^{\ell^r} - 1} \), hence \( t_{\ell^r, k} = \frac{1}{2} \sum_{i=0}^{\ell^r-1} (-1)^i \). The traces

\( Tr_{L/\mathbb{Q}}(\xi^{ip+k}) \) are zero except when \( \xi^{ip+k} \) is of order 1 or \( \ell \), hence when \( ip + k \equiv 0 \pmod{\ell^r-1} \). Let \( i^0_k = \left\lceil \frac{-k}{\ell^r-1} \right\rceil \). Then we get the \( \ell \) solutions, with alternating parities, \( i^0_k + \nu \ell^{r-1}, 0 \leq \nu \leq \ell - 1 \), among which we have a unique value \( \nu = \nu_k \in [0, \ell - 1] \) such that \( i^0_k \ell \equiv 0 \pmod{\ell^r-1} \).

In general, \( (-1)^{\nu_k} Tr_{L/\mathbb{Q}}(\xi^{i_k^{\nu_k}p+k}) \) is equal to \( (-1)^{i_k^{\nu_k}} \cdot (-1)^{\nu_k} \cdot \ell^{r-1} \) and for \( \nu = \nu_k \), we obtain the expression \( (-1)^{i^0_k} \cdot (-1)^{\nu_k} \cdot \ell^{r-1} \) with \( i^0_k = \left\lceil \frac{-k}{\ell^r-1} \right\rceil \). Carrying the summation of the traces, we obtain easily

\[ t_{\ell^r, k} \equiv \ell^{r-1} \cdot \frac{(-1)^{\nu_k} \ell - (-1)^{\nu_k} \ell^{r-1}}{2} \pmod{p}. \]

For \( r = 1 \), we find again \( t_{\ell, k} \equiv \frac{(-1)^{\nu_k} \ell - (-1)^{\nu_k} \ell^{-1}}{2} \pmod{p} \) (see Theorem 5.1).
5.4.7. Case \( n = \ell^p, \ell > 2 \) prime. If \( r = p \), then \( i_k^0 = \left\lfloor \frac{-k}{p} \right\rfloor_{\ell^p-1} \)

\[
k\frac{\ell^{p-1}-1}{p}
\]
is even, and

\[
t_{p,k} = \frac{(-1)^{\left\lfloor \frac{-k}{p} \right\rfloor_p} \cdot \ell - 1}{2} = \frac{(-1)^{\left\lfloor \frac{-k}{p} \right\rfloor_p} \cdot \ell - 1}{2} = t_{\ell,k} \mod p.
\]

**Remark 5.8.** We have for any \( p \), any \( n \geq 1 \), and any \( k \in [1, p - 1] \), the relation \(\left\lfloor \frac{-k}{p} \right\rfloor_p \cdot p + k = \left\lfloor \frac{k}{n} \right\rfloor_p \cdot n\). This can be useful in the previous formulas (the proof is left to the reader).

\[
\square
\]

6. A Possible Curious Link with Mirimanoff Congruences

Let \( V := \mathbb{F}_p^{p-1} \) and let \( c \) be the complex conjugation. We define the action of the group \( \{1, c\} \) on \( V \) as follows: If \( (a_1, \ldots, a_{p-1}) \in V \), then \( c(a_1, \ldots, a_{p-1}) = (a_{p-1}, \ldots, a_1) \). We have \( V = V^+ \oplus V^- \), where \( V^+ := \frac{1+c}{2} V \) and \( V^- := \frac{1-c}{2} V \); \( V^+ \) and \( V^- \) have dimensions \( \frac{p-1}{2} \).

For instance, the vectors traces \( T_n := (t_{n,1}, \ldots, t_{n,p-1})(p \nmid n, n \nmid p - 1) \)

are elements of \( V^+ \). Let \( \rho_0 \in [2, p - 2] \) be the representative of \( \rho = \frac{v}{u} \)
corresponding to a solution \((u, v)\) of the SFLT equation with \( p \nmid uv \)
\((u^2 - v^2)\). Consider a character \( \omega^h \) of \( g = \text{Gal}(K / \mathbb{Q}) \), \( h \in [0, p - 1] \).

The Mirimanoff sum associated with \( \omega^h \) and \( \rho_0 \) is

\[
M_{\omega^h}(-\rho_0) := \sum_{k=1}^{p-1} \omega^{-h}(k)(-\rho_0)^k = \sum_{k=1}^{p-1} \frac{(-1)^k}{k^h} \rho_0^k \mod p,
\]

written
$$M_{\omega^h}(-\rho_0) = \sum_{k=1}^{p-1} \frac{\rho_0^k}{k} (-1)^k \frac{(-1)^k}{k^{h-1}} \mod p,$$

by analogy with

$$M_n(\rho_0) = \sum_{k=1}^{p-1} 1 \rho_0^k t_{n,k}, \text{ for all integers } n(p \nmid n, n \nmid p - 1).$$

Put $t_{h,k} := \frac{(-1)^k}{k^{h-1}}$; then $t_{h,p-k} = \frac{(-1)^{p-k}}{(p-k)^{h-1}} = (-1)^h \frac{(-1)^k}{k^{h-1}} = (-1)^h t_{h,k}$ (mod $p$). So the vector $T'_h := (t_{h,1}, \ldots, t_{h,p-1})$ is in $V^+$, if $h$ is even and in $V^-$ if not. Thus, the vectors $T_n := (t_{n,1}, \ldots, t_{n,p-1})$ and $T_{2m} := (t'_{2m,1}, \ldots, t'_{2m,p-1})$ are in the subspace $V^+$.

In the same way, the vectors $T_n := (\frac{1}{k} t_{n,k})_{k=1,\ldots,p-1}$ and $T'_{2m} := (\frac{1}{k} t'_{2m,k})_{k=1,\ldots,p-1}$ are in $V^-$. The properties of the systems of vectors $T_n$ and $T_n$ are similar, as well as that of $T'_{2m}$ and $T'_{2m}$; so we shall focus especially on the systems $T_n$ and $T'_{2m}$.

**Lemma 6.1.** The $\frac{p-1}{2}$ vectors $T'_{2m} = (t'_{2m,1}, \ldots, t'_{2m,p-1})$ for $2m \in [0, p-1]$, where $t'_{2m,k} = \frac{(-1)^k}{k^{2m-1}}$ for $k = 1, \ldots, p-1$, are independent over $\mathbb{F}_p$.

**Proof.** We can consider instead $(-1)^k \cdot k \cdot t'^{-1}_{2m,k} = k^{2m}$ in $\mathbb{F}_p$, to compute the rank of the system of vectors $T'_{2m}$. Then the $\frac{p-1}{2} \times (p-1)$-matrix $(k^{2m})_{2m,k}$ is a submatrix of the $(p-1) \times (p-1)$-matrix $(k^j)_{j,k}$, where $j \in [0, p-1], k \in [1, p-1]$. The classical expression of the Vandermonde determinant $|k^j|_{j,k}$ proves the lemma. \qed
Let $I_p := \{2m \in \{0, p - 1\}, B_{2m} = 0 \text{ (mod } p)\}$, where $B_{2m}$ is the $2m$-th Bernoulli number (see [17, Tables, 2]); recall that $B_{2m} = 0$ (mod $p$) is equivalent to $b_{o_{1-2m}} = 0$ (mod $p$) in terms of generalized Bernoulli numbers, then to $|C_{o_{1-2m}}| = 0$ (mod $p$) in terms of $p$-class groups of $K$ (see, e.g., [6, Theorem 2.8] and also Granville [4], where many formal computations can enlighten the subject).

We have the following formulas for the representative $\rho_0$ of $\rho = \frac{v}{u}$ (use [6, Subsection 3.1] with appropriate modifications making true the statements of Theorems 3.7 and 3.9 for the SFLT equation):

(i) $M_1(-\rho_0) = \sum_{k=1}^{p-1} \frac{1}{k} \rho_0^k (-1)^k k = 0 \text{ (mod } p) \text{ since } \rho_0 \neq p - 1.$

(ii) $M_{o_h}(-\rho_0) = \sum_{k=1}^{p-1} \frac{1}{k} \rho_0^k (-1)^k = 0 \text{ (mod } p).$

(iii) $M_{o_h}(-\rho_0) \cdot M_{o_{1-h}}(-\rho_0) = 0 \text{ (mod } p) \text{ for all } h \in \{0, p - 1\} \text{ (Mirimanoff congruences).}$

(iv) $b_{o_{1-2m}} \cdot M_{o_{2m}}(-\rho_0) = 0 \text{ (mod } p) \text{ for all } 2m \in \{0, p - 1\} \text{ (Kummer congruences).}$

Let $E_p := \{2m \in \{0, p - 1\}, 2m \notin I_p\}$, so that $|E_p| = \frac{p - 1}{2} - i_p,$ where $i_p := |I_p|$ is the index of irregularity of $p$. Then from (iv), we get $M_{o_{2m}}(-\rho_0) = 0 \text{ (mod } p) \text{ for all } 2m \in E_p.$ This gives $\frac{P - 1}{2} - i_p$ independent vectors $T_{2m} \in V^+ := \frac{1}{2}(1 + c) \cdot \mathbb{F}_p^{p-1}$, because of Lemma 6.1, hence the vectors $T_n(p \uparrow n, n \uparrow p - 1)$ and $T_{2m}(B_{2m} \neq 0 \text{ (mod } p))$ are in the hyperplane $\mathcal{H}_{\rho_0}$ of $V^+ \simeq \mathbb{F}_p^{(p-1)/2}$ defined by $\sum_{k=1}^{(p-1)/2} \frac{1}{k} (\rho_0^k - \rho_0^{p-k}) x_k = 0,$ $x^+ := \frac{1}{2}(x_k + x_{p-k}).$
It appears, from numerical computations, that the subspace $W$ generated by the vectors $T_n(p \nmid n, n \nmid p - 1)$, is a subspace of $V^+$ of dimension $\frac{p-1}{2} - i_p$ and is equal to the subspace $W'$ generated by the $\frac{p-1}{2} - i_p$ independent vectors $T'_{2m}, 2m \in E_p$. This has been verified by Quème for all $p$ up to 500, hence especially for the irregular primes 37, 59, 67, 101, 103, 131, 149 ($i_p = 1$), then 157, 353, 379, 467 ($i_p = 2$), and 491 ($i_p = 3$).

The most tricky situation should be that the following conjecture be true.

**Conjecture 6.2.** The subspace of $V^+$ generated by the vectors $T'_n := (t_{n,k})_{k=1,\ldots,p-1}$, for all the integers $n (p \nmid n, n \nmid p - 1)$, is equal to the subspace generated by the $\frac{p-1}{2} - i_p$ independent vectors $T''_{2m} := ((-1)^k k^{p-2m})_{k=1,\ldots,p-1}$, for all the even indices $2m \in [0, p-1]$ such that $p$ does not divide the Bernoulli number $B_{2m}$.

Of course, if this conjecture is true, when $i_p = 0$, the above subspaces $W$ and $W'$ of dimensions $\frac{p-1}{2}$ are equal to $V^+$, which implies that not all the vectors $T_n$ are in the hyperplane $\mathcal{H}_{p_0}$ of $V^+$, proving the studied case of SFLT in the regular case. In a numerical point of view, if using suitable integers $n$, we find that the $\mathbb{F}_p$-dimension of $W$ is $\frac{p-1}{2}$, we have proved that $p$ is regular. It will be interesting to use the $t_{n,k}$ to find a lower bound of this dimension.
Remark 6.3. Under the conjecture, the necessary conditions
\[ \sum_{k=1}^{p-1} \frac{1}{k} \rho_0^k t_{n,k} \equiv 0 \pmod{p} \]
can be considered as a refinement of Mirimanoff congruences with coefficients \( t_{n,k} \), for all \( n (p \nmid n, n \nmid p-1) \), instead of coefficients \( (-1)^k k^{p-2m} \). Obviously, using small even indices \( 2m = 2, 4, \ldots \), since the Bernoulli numbers \( B_{2m} \) are not divisible by \( p \), we can obtain contradictions. For instance, for \( p = 29 \) and \( 2m = 2 \), we get \( M_{\omega^2}(-10) = M_{\omega^2}(-3) \equiv 0 \pmod{29} \); but for \( 2m = 4 \), we get the other critical values \( M_{\omega^4}(-26) = M_{\omega^4}(-22) = M_{\omega^4}(-19) \equiv 0 \pmod{29} \), which provides the contradiction for all \( \rho_0 \in [2, p - 2] \).

Unfortunately, in a theoretical point of view, we are not allowed to use the congruences of Mirimanoff (to obtain contradictions in the SFLT case) as long as the Bernoulli numbers have not been computed. In other words, the advantage of the use of Theorem 5.5 with the coefficients \( t_{n,k} \) is that any \( n \) is suitable, contrary to the use of the Mirimanoff coefficients for which, the knowledge of the noncanonical set \( E_p \) is needed.

7. Numerical Experiments and Perspectives

This section results of the collaboration of the author (using [2]) with Quême (using Maple) to verify, improve, or extend some numerical results illustrating some phenomena that we shall describe now.

Recall, from Theorem 5.5, that for any fixed \( \rho_0 \in [2, p - 2] \), we need to find \( n (p \nmid n, n \nmid p-1) \), such that \( \mathcal{M}_n(\rho_0) \neq 0 \pmod{p} \), where
\[ \mathcal{M}_n(\rho_0) = \sum_{k=1}^{p-1} \frac{1}{k} \rho_0^k t_{n,k} \equiv \sum_{k=1}^{(p-1)/2} \frac{1}{k} (\rho_0^k - \rho_0^{p-k}) t_{n,k} \pmod{p}, \]
where
\[ t_{n,k} = \text{Tr}_{Q(\xi)/Q} \left( \frac{\xi^k}{1 + \xi^p} \right) \]
for a primitive \( n \)-th root of unity \( \xi \).
It may be asked if, for a system of coefficients $a_k \in \mathbb{F}_p$, $k = 1, \ldots, \frac{p-1}{2}$, not all equal to 0, there exists at least an integer $n \ (p \nmid n, n \nmid p-1)$ such that $\sum_{k=1}^{(p-1)/2} a_k t_{n,k} \neq 0$ in $\mathbb{F}_p$.

A sufficient condition is the existence of $\frac{p-1}{2}$ linearly independent vectors of the form $T_n = (t_{n,1}, \ldots, t_{n,p-1})$. Unfortunately, the computation of the maximal rank of these systems of vectors (using any large sets of integers $n$) seems, as we have explained in Section 6, to be $\frac{p-1}{2} - i_p$, where $i_p$ is the index of irregularity of $p$. So, this aspect should be abandoned despite the fact that the hyperplane $H_{\rho_0}$ of $\mathbb{F}_p^{(p-1)/2}$ is not so general, which may be helpful.

Moreover, as Theorem 5.5 shows, this very strong condition of maximal rank $\frac{p-1}{2} - i_p$ is not required for a proof of the first case of SFLT assuming $u-v \not\equiv 0 \pmod{p}$.

Quême has verified the principle of Theorem 5.5 and Example 5.7 for all primes $p$ in the interval $5 \leq p < 1000$ by testing increasing values of $n \ (p \nmid n, n \nmid p-1)$ such that $M_n(\rho_0) := \sum_{k=1}^{p-1} \frac{1}{k} \rho_0^k t_{n,k} \not\equiv 0 \pmod{p}$. The maximal needed $n$ is $n = 9$ for $p = 337, 601, and 673$ (but for these primes, the values $n = 3, 4, 6, 8$ are divisors of $p-1$, as well as 5 for 601 and 7 for 337 and 673); for all the other primes $p < 1000$, $n \in \{3, 4, 5, 6, 7, 8\}$ are sufficient to conclude for each $\rho_0 \in [2, p-2]$.

The minimal value of $n$, giving $M_n(\rho_0) \not\equiv 0 \pmod{p}$ for all $\rho_0 \in [2, p-2]$, seems to exist and is very small regarding $p$ (as above, this stronger condition is not necessary).
One can ask if the maximal rank \( \frac{p-1}{2} - i_p \) may be reached by using essentially prime numbers, since in this case, the traces \( t_{n,k} \) are given by simple formulas. The following two families have some interest, especially, the second one.

(a) **Case** \( n_i = \ell_i, \ell_i \text{ prime} \). Let \( \{\ell_2, \ldots, \ell_{(p-1)/2}\} \) be a set of primes such that \( \ell_i \equiv \pm i \pmod{p} \), \( i = 2, \ldots, \frac{p-1}{2} \) and set \( L_i := T_{\ell_i} \); recall that \( \ell_1 \equiv \pm 1 \pmod{p} \) implies \( L_1 = 0 \) (see Theorem 5.1). An extensive experimentation shows that the rank of the system of vectors \( L_i := (t_{\ell_i,1}, \ldots, t_{\ell_i,(p-1)/2}), i = 2, \ldots, \frac{p-1}{2}, \) is often near from or equal to \( \frac{p-3}{2} - i_p \).

We have computed with Quême the (numerous) counterexamples to maximal rank \( \frac{p-3}{2} - i_p \), the first one being \( p = 17 \) for which the rank is 6 instead of the expected rank 7. We obtain for \( i_p = 0 \), the counterexamples \( p = 17, 31, 43, 73, 89, 97, \ldots \).

For \( i_p = 1 \) \( (p = 37, 59, 67, 101, 103, 131, 149, 233, 257, 263, 271, 283, 293, 307, 311, 347, 389) \), Quême find the rank \( \frac{p-3}{2} - i_p \) except for \( p = 233, 257, 283, 307 \).

It is an exercise to prove that any prime \( \ell \) gives the vector \( L_i \) such that \( \ell \equiv \pm i \pmod{p} \).

(b) **Case** \( n_i = 2\ell_i, \ell_i \text{ prime} \). In this case, \( t_{2\ell_i,k} = (-1)^{k+1} \)

\[
\left( \frac{\ell_i + 1}{2} - \left[ \frac{k}{p \ell_i} \right] \right) \quad \text{(see 5.4.3).} \]

So \( L'_i := (t_{2\ell_i,1}, \ldots, t_{2\ell_i,(p-1)}) = \left( -\left[ \frac{1}{p} \right]_{\ell_i}, \left[ \frac{2}{p} \right]_{\ell_i}, \ldots, \left[ \frac{p-1}{p} \right]_{\ell_i} \right) + \frac{\ell_i + 1}{2} (1, -1, \ldots, 1, -1). \)
Contrary to the Case (a), a set of primes \( \{ \ell_1, \ldots, \ell_{(p-1)/2} \} \) such that \( \ell_i \equiv \pm i \pmod{p}, \quad i = 1, \ldots, \frac{p-1}{2} \), seems sufficient to get the rank \( \frac{p-1}{2} - i_p \) for the system of vectors \( L'_i \). This has been confirmed by Quême for all the primes \( p \) up to 500 (especially for the irregular primes like \( p = 491 \) for which \( i_p = 3 \)).

Thus, this case using prime numbers seems to be equivalent to the general one with arbitrary integers \( n \).

8. Conclusion

These computations with very elementary arithmetic in the fields \( \mathbb{Q}(\mu_n) \), coming essentially from Theorem 5.5, suggest that new insights in the first case of SFLT (assuming \( u - v \neq 0 \pmod{p} \)) and of FLT, can be accessible by means of Diophantine studies of the properties of these vectors traces \( T_n \); indeed, the criterion with the sums \( M_n(\rho_0) \) is free of any condition on Bernoulli numbers (see Remark 6.3).

Of course, the condition of Kurihara-Sitaraman-Mihailescu ([10], [11], [12]), \( B_{p-3} \neq 0 \pmod{p^2} \), gives immediately many more cases of verification. The least prime number such that \( p \mid B_{p-3} \) is \( p = 16843 \) (see [13]) and for this prime Quême has verified that \( n = 4 \) is universal to prove the first case of SFLT (for \( u - v \neq 0 \pmod{p} \)); with \( n = 5 \) only \( \rho_0 = 592 \) and its inverse 15392 are critical, which shows the stability of the test for large primes.

For the second case of SFLT, we refer to the more general constraints given in [7]. These constraints are also much more general for the first case studied here, since the present paper gives a product formula, hence a relation between some more precise informations.
Acknowledgement

I am grateful to Quême for some calculations, with Maple, and for his comments on the manuscript. I would like also to thank Mihăilescu for his interest and some remarks and perspective about this paper.

References


[16] H. S. Vandiver, Application of the Theory of Relative Cyclic Fields to both Cases of Fermat’s Last Theorem, Transaction of the AMS 28 (1926), 554-560; Application of the Theory of Relative Cyclic Fields to both Cases of Fermat’s Last Theorem (second paper), Transactions of the AMS 29 (1927), 154-162.