ANALYSIS OF THE CLASSICAL CYCLOTOMIC APPROACH TO FERMAT′S LAST THEOREM

by

Georges Gras

Abstract. — We give again the proof of several classical results concerning the cyclotomic approach to Fermat′s last theorem using *exclusively* class field theory (essentially the reflection theorems), without any calculations. The fact that this is possible suggests a part of the logical inefficiency of the historical investigations.
We analyze the significance of the numerous computations of the literature, to show how they are probably too local to get any proof of the theorem. However we use the derivation method of Eichler as a prerequisite for our purpose, a method which is also local but more effective.
Then we propose some modest ways of study in a more diophantine context using radicals; this point of view would require further nonalgebraic investigations.

Résumé. — Nous redonnons la preuve de plusieurs résultats classiques concernant l'approche cyclotomique du théorème de Fermat en utilisant *exclusivement* la théorie du corps de classes (notamment les théorèmes de réflexion), sans aucun calcul. Le fait que ceci soit possible suggère une part d'inefficacité logique des investigations historiques.
Nous analysons la signification de nombreux calculs de la littérature, afin de montrer en quoi ils sont probablement trop locaux pour donner une preuve du théorème. Cependant nous utilisons la méthode de dérivation d'Eichler comme préalable à notre démarche, méthode aussi locale, mais plus effective.
Ensuite, nous proposons quelques modestes voies d'étude, dans un contexte plus diophantien, utilisant des radicaux, point de vue qui nécessiterait d'établir de nouvelles propriétés non algébriques.

Introduction and Generalities

The classical approaches to Fermat′s last theorem (FLT) are essentially of a p-adic nature in the pth cyclotomic field; thus these studies turn to be arithmetic modulo p, in which case the distinction between first and second case is necessary but unnatural as Wiles′s proof suggests.

2000 ***Mathematics Subject Classification.*** — 11D41, 11R18, 11R37, 11R29.
Key words and phrases. — Fermat′s last theorem, Class field theory, Cyclotomic fields, Reflection theorems, Radicals, Gauss sums.

The author thanks Christian Maire for his interest and comments concerning this didactic paper, Roland Quême for an observation on Wieferich′s criterion, and the Referee for his valuable help and for the corrections of english.

Even if the starting point is of a global nature (pth powers of ideals, classes, units, logarithmic derivative of Eichler,...), the conclusion of the study is mostly local (congruences modulo p) as we can see for instance in Ribenboim and Washington′s books [R, Wa].

We don′t know (for instance in the first case of FLT) if p-adic investigations (Kummer′s congruences, Mirimanoff or Thaine′s congruences, Wieferich or Wendt′s criteria,...) are able, from a logical point of view, to succeed in proving it. We think that probably not and we think that all these dramatically numerous necessary conditions can, in some sense, be satisfied in a very rare " numerical setting", as for the question of Vandiver′s conjecture for which we have given a probabilistic study in [Gr1, II.5.4.9.2]: the number of favourable primes less than p (for a counterexample) can be of the form $c \,.\log(\log(p))$, $c < 1$.

This is to be relativized with the result of Soulé [S] showing (after that of Kurihara [Ku] for $n = 3$) that for odd n, the real components $\mathcal{C}\ell_{\omega^{p-n}}$ of the p-class group [(1)] are trivial for any large p. This result and the well-known relative case indicate that the probabilities are not uniform in the following way:

For small values of odd n, the real components $\mathcal{C}\ell_{\omega^{p-n}}$ are trivial (deep result of [Ku, S]) and for small values of even m, the relative components $\mathcal{C}\ell_{\omega^{p-m}}$ are trivial (because of the evident nondivisibility by p of the first Bernoulli numbers $B_2, \ldots, B_{m_0}$); so that the real components $\mathcal{C}\ell_{\omega^{p-3}}, \ldots, \mathcal{C}\ell_{\omega^{p-n_0}}$, for a small odd n_0, and the relative components $\mathcal{C}\ell_{\omega^{p-2}}, \ldots, \mathcal{C}\ell_{\omega^{p-m_0}}$, for a small even m_0, are trivial, which implies, by reflection, that the real components $\mathcal{C}\ell_{\omega^2}, \ldots, \mathcal{C}\ell_{\omega^{m_0}}$ are trivial and the cyclotomic units $\eta_{\omega^2}, \ldots, \eta_{\omega^{m_0}}$ are not local pth powers at p. [(2)]

In the particular speculative case of the existence of a solution in the first case of Fermat′s equation, from results of Krasner [Kr], [G2], and many authors, for small values of odd n', the last Bernoulli numbers $B_{p-n'}$ must be divisible by p, say $B_{p-3}, \ldots, B_{p-n'_0}$ for a small odd n'_0, giving the nontriviality of the relative components $\mathcal{C}\ell_{\omega^3}, \ldots, \mathcal{C}\ell_{\omega^{n'_0}}$ and the fact that the cyclotomic units $\eta_{\omega^{p-3}}, \ldots, \eta_{\omega^{p-n'_0}}$ are *local* pth powers (but not global pth powers because of the previous result of Soulé, at least up to $\min(n_0, n'_0)$), which creates a significant defect for the probabilities.

As we see from the classical literature, strong diophantine or analytic arguments are absent, even when the p-rank of the class group is involved since this p-rank is used as a formal variable. Moreover the second case is rarely studied.

Of course a great part of the point of view developped here is not really new (many papers of the early twentieth century, contain overviews of our point of view) but we intend to organize the arguments in a more conceptual and accessible way, mainly to avoid Bernoulli′s numbers considerations, and to suggest forthcoming studies in a more diophantine or analytic context by using radicals instead of ideal classes.

---

(1) Standard definitions with the character of Teichmüller ω and the corresponding eigenspaces $\mathcal{C}\ell_{\omega^i}$, also denoted $\mathcal{C}\ell^{(i)}$, $i = 1, \ldots, p-1$; see Not. 2.7, and Th. 2.8, Subsec. 2.3.

(2) The equivalence between $\mathcal{C}\ell_{\omega^{p-k}} \neq 1$ and η_{ω^k} being a local pth power (k even) is given by the theory of p-adic L-functions or the reflection theorem; see Example 2.9.

We will see on this occasion that class field theory, in its various aspects, allows us to find again *all* classical technical properties, without dreadful computations.

Some papers already go partially in this direction (e.g. Anglès [A2, A3], Granville [G1, G2], Helou [He1, He2], Terjanian [Te], Thaine [Th1, Th2, Th3], and many others).
Finally, we must mention that all these studies strongly depend on the base field (here $\mathbb{Q}$) since it is shown in [A2] that many results or conjectures fail for the Fermat equation over a number field $k \neq \mathbb{Q}$.

In Section 1 we recall some basic facts for the convenience of the reader; they can also be found for instance in Washington′s book [Wa].

In Section 2 we recall some very useful properties of class field theory (notion of p-primarity which avoids painful computations, reflection theorems in the general setting developped in [Gr1, II.5.4]) and we introduce the radical W associated to a solution in any case of the Fermat equation.
Then we explain the insufficiency of the local study of FLT, and we put the bases of a global approach with W which does not separate the first and second cases of FLT. We also examine the influence of a solution of the Fermat equation on other arithmetic invariants.

In Section 3, for the first case of FLT, we study p-adically the radical W, introduced in Section 2, and show how Mirimanoff′s polynomials are related to this radical, without use of Bernoulli′s numbers; moreover we modify these polynomials by introducing the characters of the Galois group, which illuminates the class field theory context.
From this, we show that the classical Kummer and Mirimanoff congruences are directly the expression of reflection theorems.
To be complete, we revisit some p-adic studies, as those of Eichler [E1, E2], covering works of Brückner [Br1, Br2] and Skula [Sk1, Sk2].
We then return to the well-known fact that Wieferich′s criterion is a consequence of reciprocity law and, in an Appendix, we give a proof suggested by Quême; for this simpler proof, we interpret, with current technics, some works of Fueter–Takagi (1922) and Inkeri (1948) (see [R, IX.4]) which do not use reciprocity law.
Finally we give a standard proof of the Germain–Wendt theorem, and introduce some (perhaps new) ideas to compare Mirimanoff′s polynomials and Gauss′s sums, and to study “ Mirimanoff′s sums ” defined as sums of roots of unity.

In Section 4, we give some conclusions and prospectives in various directions.

We are aware of the futility of this attempt, but we believe that it can be helpful (or disappointing) for those who wish to pursue this kind of methodologies.

1. Classical results depending on a solution of Fermat′s equation

Let p be a prime number, $p > 2$. Let a, b, c in $\mathbb{Z}\backslash\{0\}$ be pairwise relatively prime integers, such that $a^p + b^p + c^p = 0$. In the second case of FLT, we suppose that $p \,|\, c$.

We have the identity:

$$a^p + b^p = (a+b)\,\mathrm{N}_{K/\mathbb{Q}}\,(a+b\,\zeta) = -c^p,$$

where ζ is a primitive pth root of unity, $K = \mathbb{Q}(\zeta)$, and $\mathrm{N}_{K/\mathbb{Q}}$ is the norm map in $K/\mathbb{Q}$.
Let $\mathfrak{p}$ be the unique prime ideal $(1-\zeta)\,\mathbb{Z}[\zeta]$ of K dividing p. We have $\mathfrak{p}^{p-1} = p\,\mathbb{Z}[\zeta]$.

Lemma 1.1. — *Let ν be the p-adic valuation of c. If $\nu \geq 1$, then $a+b = p^{\nu p-1} c_0^p$ and $\mathrm{N}_{K/\mathbb{Q}}(a+b\,\zeta) = p\,c_1^p$, with $p \nmid c_0\,c_1$ and $p^\nu c_0\,c_1 = -c$. If $\nu = 0$ then $a+b = c_0^p$ and $\mathrm{N}_{K/\mathbb{Q}}(a+b\,\zeta) = c_1^p$ with $c_0\,c_1 = -c$.*

Proof. — If $p \,|\, c$, there exists i, $0 \leq i \leq p-1$, such that $a + b\,\zeta^i \in \mathfrak{p}$; thus $a + b\,\zeta^j \in \mathfrak{p}$ for all $j = 0, \ldots, p-1$ since $a + b\,\zeta^j \equiv a + b\,\zeta^i \bmod \mathfrak{p}$ for any j.
So $p \,|\, a+b$ and, since $p \nmid b$, the $\mathfrak{p}$-adic valuations of $a+b$ and $b\,(\zeta-1)$ are $\mu(p-1)$ for some $\mu \geq 1$ and 1, respectively.
Since $p > 2$, the $\mathfrak{p}$-adic valuation of $a + b\,\zeta = a + b + b\,(\zeta-1)$ is equal to 1 as well as for the conjugates $a + b\,\zeta^i$, $i = 1, \ldots, p-1$. The $\mathfrak{p}$-valuation of $\mathrm{N}_{K/\mathbb{Q}}(a+b\,\zeta)$ is thus equal to $p-1$ and that of $a+b$ is $\mu(p-1) = (\nu p - 1)(p-1)$, and the lemma follows. □

Lemma 1.2. — *Let $\ell \neq p$ be a prime number dividing c. Then $\ell \,|\, \mathrm{N}_{K/\mathbb{Q}}(a+b\,\zeta)$ if and only if $\ell \nmid a+b$ (i.e., g.c.d.$\,(c_0, c_1) = 1$). Any $\ell \,|\, \mathrm{N}_{K/\mathbb{Q}}(a+b\,\zeta)$ is totally split in $K/\mathbb{Q}$.*

Proof. — If $\ell \,|\, \mathrm{N}_{K/\mathbb{Q}}(a+b\,\zeta)$ we may suppose that $a + b\,\zeta \in \mathfrak{l}$ for a suitable $\mathfrak{l} \,|\, \ell$ so that ζ is congruent modulo $\mathfrak{l}$ to a rational, $\mathfrak{l}$ is totally split in $K/\mathbb{Q}$, thus ℓ is congruent to 1 modulo p.
The case $\ell \nmid a+b$ is clear. If $\ell \,|\, a+b$ and if $\mathfrak{l} \,|\, a+b\,\zeta$ for $\mathfrak{l} \,|\, \ell$, we get $b\,(\zeta-1) \in \mathfrak{l}$ (absurd since $\ell \nmid b$.). Thus $\ell \nmid \mathrm{N}_{K/\mathbb{Q}}(a+b\,\zeta)$. □

Corollary 1.3. — *(i) We have $(a+b\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}\,\mathfrak{c}_1^p$ if $p \,|\, c$, where $\mathfrak{c}_1$ is an integral ideal prime to $\mathfrak{p}$, and $(a+b\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{c}_1^p$ if not. We have $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{c}_1) = c_1$.*
(ii) Moreover $\mathfrak{c}_1 = \prod_{\ell | c_1} \mathfrak{l}^{\nu_\ell}$, $\nu_\ell > 0$, where $\mathfrak{l}$ is, for each $\ell \,|\, c_1$, a suitable (unique) prime ideal above ℓ.

Proof. — We have only to prove that if $\mathfrak{l} \,|\, a+b\,\zeta$, then for any conjugate $\mathfrak{l}_i$ (by mean of the automorphism $\zeta \longrightarrow \zeta^i$, $i \neq 1$), we have $\mathfrak{l}_i \nmid a+b\,\zeta$; indeed, if not we would have $b\,(\zeta^{-i} - \zeta) \in \mathfrak{l}$ (absurd). Thus the ideal $\big(\frac{a+b\,\zeta}{1-\zeta}\big)\,\mathbb{Z}[\zeta]$ or $(a+b\zeta)\,\mathbb{Z}[\zeta]$ is characterized by its norm c_1^p and is a pth power. □

Remark 1.4. — (i) By permutation we have the following, with evident notations:

$$\begin{aligned}
&a+b = p^{\nu p-1} c_0^p \ \text{ or } c_0^p, \quad \mathrm{N}_{K/\mathbb{Q}}(a+b\,\zeta) = p\,c_1^p \ \text{ or } c_1^p, \ \text{ with } -c = c_0\,c_1,\\
&b+c = a_0^p, \quad \mathrm{N}_{K/\mathbb{Q}}(b+c\,\zeta) = a_1^p, \ \text{ with } -a = a_0\,a_1,\\
&c+a = b_0^p, \quad \mathrm{N}_{K/\mathbb{Q}}(c+a\,\zeta) = b_1^p, \ \text{ with } -b = b_0\,b_1,\\
&\text{g.c.d.}\,(a_0, a_1) = \text{g.c.d.}\,(b_0, b_1) = \text{g.c.d.}\,(c_0, c_1) = 1,
\end{aligned}$$

$$(a+b\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}\,\mathfrak{c}_1^p \ \text{ or } \ \mathfrak{c}_1^p, \ \text{ with } \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{c}_1) = c_1,$$
$$(b+c\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{a}_1^p, \ \text{ with } \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}_1) = a_1,$$
$$(c+a\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{b}_1^p, \ \text{ with } \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{b}_1) = b_1.$$

(ii) All the prime numbers dividing $a_1 b_1 c_1$ are totally split in $K/\mathbb{Q}$; thus any (positive) divisor of $a_1 b_1 c_1$ is congruent to 1 modulo p.

These computations and the proofs of FLT in particular cases suggest the following conjecture.

Conjecture 1.5. — *Let p be a prime number, $p > 3$, and $K = \mathbb{Q}(\zeta)$, where ζ is a primitive pth root of unity. Put $\mathfrak{p} := (1-\zeta)\,\mathbb{Z}[\zeta]$.*
Then for $x, y \in \mathbb{Z} \setminus \{0\}$, with g.c.d. $(x, y) = 1$, the equation $(x + y\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}\,\mathfrak{z}^p$ or $\mathfrak{z}^p$ (depending on whether $x + y \equiv 0 \bmod (p)$ or not), where $\mathfrak{z}$ is an ideal of K prime to $\mathfrak{p}$, has no solution except the trivial cases: $x + y\,\zeta = \pm(1-\zeta)$ and $\pm(1+\zeta)$.

In other words, considering the two relations $(a+b\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}\mathfrak{c}_1^p$ (or $\mathfrak{c}_1^p$) and $a + b = p^{\nu p-1} c_0^p$ (or c_0^p), equivalent to the existence of a solution of the Fermat equation, we assert that the second is unnecessary, the first one being equivalent to $\mathrm{N}(a+b\,\zeta) = p\,c_1^p$ (or c_1^p). It is likely that this conjecture has already been stated, but we have found no reference.

2. Algebraic Kummer theory and reflection theorems

This Section is valid for the two cases of FLT.

2.1. p-primarity – local pth powers. — The following Theorem 2.2 will be essential to clarify some aspects of ramification in Kummer cyclic extensions of degree p of K. Let $K_\mathfrak{p}$ be the $\mathfrak{p}$-completion of the field K (see [Gr1, I.6.3] for the classical notion of p-primarity due to Hasse).

Lemma 2.1. — *Let $\alpha \in K^\times$ be prime to p and such that $\alpha\,\mathbb{Z}[\zeta]$ is the pth power of an ideal of K.* (3)
The number α is p-primary (i.e., $K(\sqrt[p]{\alpha}\,)/K$ is unramified at $\mathfrak{p}$) if and only if it is a local pth power (i.e., $\alpha \in K_\mathfrak{p}^{\times p}$). This happens if and only if α is congruent to a pth power modulo $\mathfrak{p}^p = (p)\,\mathfrak{p}$.

Proof. — One direction is trivial. Suppose that $K(\sqrt[p]{\alpha}\,)/K$ is unramified at $\mathfrak{p}$; since α is a pseudo-unit, this extension is unramified as a global extension and is contained in the p-Hilbert class field H of K. The Frobenius automorphism of $\mathfrak{p}$ in H/K depends on the class of $\mathfrak{p}$ which is trivial since $\mathfrak{p} = (1-\zeta)$; so $\mathfrak{p}$ splits totally in H/K, thus in $K(\sqrt[p]{\alpha}\,)/K$, proving the first part of the proposition. The final congruential condition of p-primarity is well known (see e.g. [Gr1, Ch. I, § 6, (b)]).

(3) Such numbers are called *pseudo–units* since units are a particular case; we will use this word to simplify.

Warning: the general condition of p-primarity in K is "α congruent to a pth power modulo $\mathfrak{p}^p = (p)\,\mathfrak{p}$", but the general condition to be a local pth power at $\mathfrak{p}$ in K is "α congruent to a pth power modulo $\mathfrak{p}^{p+1} = (p)\,\mathfrak{p}^2$". The fact that "$\alpha$ is a pseudo-unit of K implies the equivalence" is nontrivial and specific of the pseudo-units of the pth cyclotomic field (such studies are given in [Th3], for special pseudo-units, by means of explicit polynomial computations). $\square$

We have the following consequence, due to Kummer for units, which can be generalized to pseudo-units.

Theorem 2.2. — *Every pseudo-unit η of K, congruent to a rational (respectively to a pth power) modulo p, is p-primary, thus a local pth power at $\mathfrak{p}$. If moreover the p-class group of K is trivial, η is a global pth power.*

Proof. — We have, for a suitable rational ρ, $\eta^{p-1} \equiv \rho^{p-1} \equiv 1 \bmod (p)$ in $\mathbb{Z}_{(p)}[\zeta]$, where $\mathbb{Z}_{(p)}$ is the localization of $\mathbb{Z}$ at p.
Put $\eta^{p-1} = 1 + p\,\delta$, $\delta \in \mathbb{Z}_{(p)}[\zeta]$, and $(\eta) = \mathfrak{n}^p$; taking the norm of the relation $(\eta^{p-1}) = \mathfrak{n}^{(p-1)p}$ we get $\mathrm{N}_{K/\mathbb{Q}}(\eta^{p-1}) = n^{(p-1)p}$ with $n^{p-1} \equiv 1 \bmod (p)$, hence $1 \equiv 1 + p\,\mathrm{Tr}_{K/\mathbb{Q}}(\delta) \bmod (p^2)$ giving $\mathrm{Tr}_{K/\mathbb{Q}}(\delta) \equiv 0 \bmod (p)$, thus $\delta \in \mathfrak{p}$, proving the first part of the theorem (see Lem. 2.1).
If $\eta \equiv u^p \bmod (p)$, $u = \sum u_i\,\zeta^i \in \mathbb{Z}_{(p)}[\zeta]$, then $u^p \equiv \sum u_i^p =: \rho \in \mathbb{Z}_{(p)}$ modulo p; reciprocally, $\eta \equiv \rho \bmod (p)$ implies $\eta \equiv \rho^p \bmod (p)$.
The extension $K(\sqrt[p]{\eta}\,)$ is thus unramified; so if the p-class group of K is trivial, this extension must be trivial, which finishes the proof. $\square$

When the p-class group of K is trivial, K is said to be p-regular (in the Kummer sense), which is here equivalent to its p-rationality; this property implies in general the above result for units. See [MN], [JN], [GJ] for these notions in general, and [AN] where the Kummer property is generalized. See Subsections 2.5, (a) and (b) for the study of the invariants $\mathcal{T}(K)$ and $R_2(K)$ whose triviality characterizes the p-rationality and the p-regularity (in the K-theory sense), respectively.

2.2. Introduction of some radicals. — We begin by the following remarks, from a solution (a, b, c) of the Fermat equation, which are the key of the present study.

Remark 2.3. — (i) We note that we have $(a + b\,\zeta)\mathbb{Z}[\zeta] = \mathfrak{p}\mathfrak{c}_1^p$ or $\mathfrak{c}_1^p$ (see Cor. 1.3, (i), or Rem. 1.4, (i)). This means that the Kummer cyclic extensions (of degree p or 1) $K(\sqrt[p]{a + b\,\zeta^i}\,)/K$, $i = 1, \ldots, p-1$, are p-ramified (i.e. unramified outside p). In the same way, $K(\sqrt[p]{b + c\,\zeta^j}\,)/K$, $K(\sqrt[p]{c + a\,\zeta^k}\,)/K$, $j, k = 1, \ldots, p-1$, are p-ramified cyclic extensions.

(ii) When $p \,|\, c$, the extensions $K(\sqrt[p]{b + c\,\zeta^j}\,)/K$, $j = 1, \ldots, p-1$, are unramified: indeed we have $b + c\,\zeta^j \equiv b \bmod (p)$, hence the conclusion with Theorem 2.2.

But we know that these extensions must split at $\mathfrak{p}$ which implies that necessarily $c \equiv 0 \bmod (p^2)$. [4]

We have $c + a\,\zeta^k = \zeta^k\,(a + c\,\zeta^{-k})$ with $a + c\,\zeta^{-k} \equiv a \bmod (p)$; thus in the compositum $K(\sqrt[p]{\zeta}\,,\ \sqrt[p]{c + a\,\zeta^k}\,)$ (where $K(\sqrt[p]{\zeta}\,)/K$ is also p-ramified) we obtain the unramified extensions $K\big(\sqrt[p]{a + c\,\zeta^{k'}}\,\big)/K$, $k' = 1, \ldots, p-1$, and similarly with $c + b\,\zeta^j$.

(iii) If $p\,|\,c$, then from Corollary 1.3, (i), the pseudo-units $\dfrac{a + b\,\zeta^i}{1 - \zeta^i}$ are such that $\dfrac{a + b\,\zeta^i}{1 - \zeta^i} = \dfrac{a + b}{1 - \zeta^i} - b \equiv -b \bmod (p)$ since $a + b$ is of p-valuation $\nu\,p - 1 \geq 2$. Theorem 2.2 implies that the $\dfrac{a + b\,\zeta^i}{1 - \zeta^i}$ are local pth powers at $\mathfrak{p}$ and that the extensions $K\big(\sqrt[p]{\frac{a+b\,\zeta^i}{1-\zeta^i}}\,\big)/K$ are unramified.

Notation 2.4. — *Let E_p be the group of p-units of K. Then $E_p = \langle\,\zeta,\, 1 - \zeta\,\rangle \oplus E^+$, where E^+ is the group of units of the maximal real subfield K^+ de K. Put $E^+ = \langle\,\varepsilon_i\,\rangle_{i=1,\ldots,\frac{p-3}{2}}$, and for $i, j, k = 1, \ldots, p-1$, put:*

$$\begin{aligned}
\Omega &:= \langle\, a + b\,\zeta^i,\, b + c\,\zeta^j,\, c + a\,\zeta^k\,\rangle,\\
\Gamma &:= \langle \zeta,\ 1 - \zeta,\ \varepsilon_1, \ldots, \varepsilon_{\frac{p-3}{2}},\ a + b\,\zeta^i,\ b + c\,\zeta^j,\ c + a\,\zeta^k\,\rangle \;=\; E_p \oplus \Omega,\\
W_c &:= \langle\, a + b\,\zeta^i\,\rangle_i \,.\, K^{\times p}/K^{\times p},\\
W_a &:= \langle\, b + c\,\zeta^j\,\rangle_j \,.\, K^{\times p}/K^{\times p},\\
W_b &:= \langle\, c + a\,\zeta^k\,\rangle_k \,.\, K^{\times p}/K^{\times p},\\
W &:= \Gamma \,.\, K^{\times p}/K^{\times p}.
\end{aligned}$$

If $p\,|\,c$ (second case of FLT), we introduce the group:

$$\Omega_{\text{prim}} := \langle\, \tfrac{a+b\,\zeta^i}{1-\zeta^i},\, b + c\,\zeta^j,\, a + c\,\zeta^k\,\rangle, \textit{ for which } \Gamma = E_p \oplus \Omega_{\text{prim}}.$$

Remark 2.5. — (i) It is easy to see from Corollary 1.3, (ii), that the $3(p-1) + \frac{p+1}{2}$ elements $\zeta,\ 1 - \zeta,\ \varepsilon_1, \ldots, \varepsilon_{\frac{p-3}{2}},\ a + b\,\zeta^i,\ b + c\,\zeta^j,\ c + a\,\zeta^k,\ i, j, k = 1, \ldots, p-1$, are multiplicatively independent and, due to their particular form, the idea is that they are largely independent in $K^\times/K^{\times p}$ (this is the main diophantine argument).

Unfortunately, this is probably very difficult to prove since it looks like Vandiver's conjecture (which applies to the cyclotomic p-units, generated by $1 - \zeta$ and its conjugates, which are not independent in $K^\times/K^{\times p}$ as soon as Vandiver's conjecture is false). But in fact we will see below that the required condition is not the total independence of the above numbers in $K^\times/K^{\times p}$ because of analytic formulas.

(ii) It is evident that $\zeta, 1 - \zeta, \varepsilon_1, \ldots, \varepsilon_{\frac{p-3}{2}}$ are independent in $K^\times/K^{\times p}$ since it is by definition a $\mathbb{Z}$-basis of E_p.

---

(4) We have $b + c\,\zeta = (b + c)\big(1 + \frac{c}{b+c}\,(\zeta - 1)\big)$ where $b + c = a_0^p$. Let $1 + \frac{c}{b+c}\,(\zeta - 1) = (1 + u\,(\zeta - 1))^p$ locally; if $u \equiv u_0 \bmod \mathfrak{p}$, with $u_0 \in \mathbb{Z}$, then $\zeta^{-u_0}\,(1 + u\,(\zeta - 1)) \equiv 1 \bmod \mathfrak{p}^2$, giving $1 + \frac{c}{b+c}\,(\zeta - 1) \equiv 1 \bmod (p)\,\mathfrak{p}^2$, thus $c \equiv 0 \bmod (p)\,\mathfrak{p}$, hence modulo p^2.

(iii) We have $W = \Gamma\,.\,K^{\times p}/K^{\times p}$ and $E_p\,.\,K^{\times p}/K^{\times p} \simeq E_p/E_p^p$; then:

$$\Gamma\,.\,K^{\times p}/E_p\,.\,K^{\times p} \simeq \Gamma/\Gamma \cap (E_p\,.\,K^{\times p}) \simeq \Omega/\Omega \cap (E_p\,.\,K^{\times p})$$

whose order is the degree $\big[K(\sqrt[p]{\Gamma}\,) : K(\sqrt[p]{E_p}\,)\big]$.

(iv) If $p\,|\,c$, then $K(\sqrt[p]{\Omega_{\rm prim}}\,)/K$ is unramified and $K(\sqrt[p]{\Gamma}\,)/K(\sqrt[p]{E_p}\,)$ is unramified hence $\mathfrak{p}$-split of degree $(\Omega_{\rm prim} : \Omega_{\rm prim} \cap (E_p\,.\,K^{\times p}))$ (nonramification and decomposition propagate by extension), which will be interpreted in Subsection 2.3.

Denote by $K(\sqrt[p]{W}\,)$ the extension $K(\sqrt[p]{\Gamma}\,)$. We conclude (Rem. 2.3) that the extension $K(\sqrt[p]{W}\,)/K$ is a Pl_p-ramified p-elementary abelian extension of K (i.e., abelian of exponent p), where Pl_p is the set of places of K above p (here reduced to the singleton $\{\mathfrak{p}\}$).

2.3. Use of class field theory: abelian Pl_p-ramification. — Let H_{Pl_p} be the maximal Pl_p-ramified abelian pro-p-extension of K, and let $\mathcal{C}\!\ell_{Pl_p}$ be the generalised p-class group of K (i.e., the direct limit of the p-ray class groups modulo rays groups of conductor a power of p); we have:

$$\mathrm{Gal}\,(H_{Pl_p}/K) \simeq \mathcal{C}\!\ell_{Pl_p}.$$

From the general reflection formula proved in [Gr1, II.5.4.1, (iii)] we obtain: (5)

$$\mathrm{rk}_p(\mathcal{C}\!\ell_{Pl_p}) - \mathrm{rk}_p(\mathcal{C}\!\ell^{Pl_p}) = |\,Pl_p\,| + p - 1 - \frac{p-1}{2} = \frac{p+1}{2}.$$

Recall that in this formula, $\mathcal{C}\!\ell^{Pl_p}$ (the Pl_p-class group) is the quotient of the p-class group $\mathcal{C}\!\ell$ by the subgroup generated by the classes of the prime ideals above p, which gives, as we have seen, $\mathcal{C}\!\ell^{Pl_p} = \mathcal{C}\!\ell$.

From the above, since $K(\sqrt[p]{W}\,) \subseteq H_{Pl_p}$, we get:

$$\mathrm{rk}_p(\mathcal{C}\!\ell) = \mathrm{rk}_p(\mathcal{C}\!\ell_{Pl_p}) - \frac{p+1}{2} \geq \mathrm{rk}_p(W) - \frac{p+1}{2}.$$

Now we can prove the following from a solution (a, b, c) of the Fermat equation:

Theorem 2.6. — *Let W be the radical generated, in $K^\times/K^{\times p}$, by the group of p-units E_p and the numbers $a + b\,\zeta^i$, $b + c\,\zeta^j$, $c + a\,\zeta^k$, $i, j, k = 1, \ldots, p-1$.* (6)
Then we have the inequalities $\mathrm{rk}_p(W) \leq \frac{p+1}{2} + \mathrm{rk}_p(\mathcal{C}\!\ell) \leq p$.
If moreover p is regular (i.e., if $\mathcal{C}\!\ell$ is trivial) then $W = E_p/E_p^p$.

Proof. — From many authors (see e.g. [G3] for more history), we know that the relative class number h^-, i.e., the order of the relative class group $C^- := \mathrm{Ker}\big(\mathrm{N}_{K/K^+} : C \longrightarrow C^+ := C_{K^+}\big)$, is such that $\log(h^-) < \frac{p}{4}\log(p)$ which proves that $\mathrm{rk}_p(\mathcal{C}\!\ell^-) \leq \frac{p-1}{4}$. From classical Hecke–Leopoldt reflection theorem, we get $\mathrm{rk}_p(\mathcal{C}\!\ell^+) \leq \mathrm{rk}_p(\mathcal{C}\!\ell^-)$ giving the (very bad) inequality $\mathrm{rk}_p(\mathcal{C}\!\ell) \leq \frac{p-1}{2}$, and the first part of the theorem.

(5) For any abelian group A we denote by $\mathrm{rk}_p(A)$ the $\mathbb{F}_p$-dimension of A/A^p.
(6) In the second case of FLT with $p\,|\,c$, $a + b\,\zeta$ is not a pseudo-unit, but $\frac{a+b\,\zeta}{1-\zeta}$, $b + c\,\zeta$, $c + a\,\zeta$ are pseudo-units; thus W is generated by $1 - \zeta$ and pseudo-units.

If p is regular we get $\mathrm{rk}_p(W) \le \frac{p+1}{2}$; since W contains E_p/E_p^p which is of p-rank $\frac{p+1}{2}$ we have the equality, proving the theorem. □

In the regular case we obtain the following (see Not. 2.4):

(i) *First case of FLT*. From Remark 2.5, (iii), we obtain $\Omega \subset E\,.\,K^{\times p}$ since in the first case the elements of Ω are pseudo-units. Then in that case, all the elements $a + b\,\zeta^i$, $b + c\,\zeta^j$, and $c + a\,\zeta^k$ are of the form $\varepsilon\,.\,\alpha^p$, $\varepsilon \in E$, $\alpha \in \mathbb{Z}[\zeta]$. Of course, one can take for ε a cyclotomic unit since the group of cyclotomic units is of prime to p index in E.

(ii) *Second case of FLT*. From Remark 2.5, (iv), and Theorem 2.2, we obtain $\Omega_{\mathrm{prim}} \subset K^{\times p}$; so in the second case (with $p\,|\,c$), all the elements $\frac{a+b\zeta^i}{1-\zeta^i}$, $b + c\,\zeta^j$, and $a + c\,\zeta^k$ are global pth powers,which can perhaps simplify the usual proof.

From this we obtain easily the classical proofs by Kummer of FLT as those given in [W, Th. 1.1 and Th. 9.3] or in [Hel, Chap. 1, § 8.4].

However, Eichler's theorem [E1, E2] (i.e., $\mathrm{rk}_p(\mathcal{C}\ell^-) \le [\sqrt{p+1} - 1.5\,]$ implies the first case of FLT), that we will discuss and prove later (Th. 3.14), may be considered as a wide generalization of the regular case, but limited to the first case of FLT (see also [W, Th. 6.23] or [R, IX.7] for similar proofs).

In the general case, the unlikely equality $\mathrm{rk}_p(\mathcal{C}\ell^+) = \mathrm{rk}_p(\mathcal{C}\ell^-)$ used for the proof of Theorem 2.6 supposes the following facts (see [Gr1, II.5.4.9.2]) for which we introduce the characters of the Galois group:

Notation 2.7. — *(i) Let $g = \mathrm{Gal}\,(K/\mathbb{Q})$ and let ω be the character of Teichmüller of g (i.e., the character with values in $\mu_{p-1}(\mathbb{Q}_p)$ such that for the $s_k \in g$ defined by $s_k(\zeta) = \zeta^k$, $k = 1, \ldots, p-1$, $\omega(s_k)$ is the unique $(p-1)$th root of unity in $\mathbb{Q}_p$, congruent to k modulo p). We will also write $\omega(k) := \omega(s_k)$.*

(ii) Any irreducible p-adic character of g is of the form $\chi := \omega^m$, for $m \in \{1, \ldots, p-1\}$; we denote by χ_0 the unit character ($m = p-1$).

If χ is any p-adic character of g, we put $\chi^* := \omega\chi^{-1}$ (reflection character).

(iii) The idempotent corresponding to χ is:

$$e_\chi := \frac{1}{p-1} \sum_{s\in g} \chi(s^{-1})\, s = \frac{1}{p-1} \sum_{k=1}^{p-1} \chi^{-1}(k)\, s_k \in \mathbb{Z}_p[g].$$

The action of e_χ on a $\mathbb{Z}_p[g]$-module is well-defined; for a $\mathbb{Z}[g]$-module M, we use instead the $\mathbb{Z}_p[g]$-module $M \otimes_{\mathbb{Z}} \mathbb{Z}_p$ or the $\mathbb{Z}_p[g]$-module $M \otimes_{\mathbb{Z}} \mathbb{F}_p \simeq M/M^p$; by abuse of notation we write $M_\chi := M^{e_\chi}$ for the χ-component of M in the above sense.

For instance, we denote by $\mathrm{rk}_p(\mathcal{C}\ell_\chi)$ the p-rank of the χ-component $\mathcal{C}\ell_\chi$ of the p-class group $\mathcal{C}\ell$ $\big(\mathcal{C}\ell_\chi$ is thus the maximal submodule of $\mathcal{C}\ell$ on which g acts via $c^s = c^{\chi(s)}$ for all $s \in g$ and any class $c \in \mathcal{C}\ell_\chi\big)$.

For the group E of units, $E_\chi := E^{e_\chi}$ must be interpreted in $E \otimes_{\mathbb{Z}} \mathbb{Z}_p$ or E/E^p depending on the context.

(iv) Let K_χ be the subfield of K fixed by $\mathrm{Ker}(\chi)$.

To be self-contained, we recall here the main classical results which will be of constant use.

***Theorem 2.8* (Prerequisites).** — (i) (Kummer duality; see [Gr1, Rem. II.5.4.3]). *Let $H_{[p]}$ be the p-elementary p-Hilbert class field of K, $A := \mathrm{Gal}(H_{[p]}/K)$, and R the radical of $H_{[p]}$ (i.e., $A \simeq \mathcal{C}\ell/\mathcal{C}\ell^p$ and $H_{[p]} = K(\sqrt[p]{R}\,)$).*
For any character χ of g and for $\chi^* := \omega\,\chi^{-1}$ we have the canonical isomorphism of g-modules:

$$\mathrm{Gal}(K(\sqrt[p]{R_{\chi^*}}\,)/K) \simeq A_\chi\,\cdot$$

Then we have $R_{\chi^*} \subset K_{\chi^*}$ and $K(\sqrt[p]{R_{\chi^*}}\,)/K$ splits over $K_\chi\,\cdot$

(ii) (Reflection theorems; see [Gr1, 5.4.9.2, "Analysis of a result of Hecke"]). *For any even character $\chi \neq \chi_0$ and for $\chi^* := \omega\,\chi^{-1}$ we have:*

$$\mathrm{rk}_p((Y/Y_{\mathrm{prim}})_{\chi^*}) = \mathrm{rk}_p(\mathcal{C}\ell_{\chi^*}) - \mathrm{rk}_p(\mathcal{C}\ell_\chi) = 1 - \mathrm{rk}_p((Y/Y_{\mathrm{prim}})_\chi),$$

where Y is the group of pseudo-units of K (elements equal to the pth power of an ideal prime to $\mathfrak{p}$), and where Y_{prim} is the subgroup of p-primary pseudo-units (i.e., local pth powers at $\mathfrak{p}$).

(iii) (Main theorem on cyclotomic fields of Thaine–Ribet–Mazur–Wiles–Kolyvagin; see [W, § 15.4]). *For any even character $\chi \neq \chi_0$ and for $\chi^* := \omega\,\chi^{-1}$ we have:*

- $|\,\mathcal{C}\ell_\chi\,| = |\,(\langle\,\varepsilon_\chi\,\rangle : \langle\,\eta_\chi\,\rangle)\,|_p^{-1}$, *where ε_χ is a generator of E_χ and $\eta_\chi = (1-\zeta)^{e_\chi}$.*
- $|\,\mathcal{C}\ell_{\chi^*}\,| = |\,b_{\chi^*}\,|_p^{-1}$, *where $b_{\chi^*} := \frac{1}{p}\sum_{k=1}^{p-1} (\chi^*)^{-1}(k)\,k$.*

The use of the deep result (iii) is not really necessary in this paper but it clarifies the reasonings since we are only interested by the logical aspects of the influence of a solution of Fermat′s equation on these invariants and not by an optimization of the statements.

Example 2.9. — If for an even $\chi \neq \chi_0$, the group $\mathcal{C}\ell_{\chi^*}$ is nontrivial, there exists a nontrivial χ^*-pseudo-unit α_{χ^*} (i.e., $\alpha_{\chi^*} \notin K^{\times p}$).

If α_{χ^*} is p-primary then from (i) this defines a χ-unramified cyclic extension of degree p of K_χ; so that $\mathcal{C}\ell_\chi \neq 1$ and $(\langle\,\varepsilon_\chi\,\rangle : \langle\,\eta_\chi\,\rangle) \equiv 0 \bmod (p)$ from (iii) (counterexample to the Vandiver conjecture).

If α_{χ^*} is not p-primary then from (ii) we get $\mathrm{rk}_p((Y/Y_{\mathrm{prim}})_{\chi^*}) = 1$ and $\mathrm{rk}_p((Y/Y_{\mathrm{prim}})_\chi) = 0$ which implies that all the χ-pseudo-units are p-primary, especially ε_χ, hence $\eta_\chi \in \langle\,\varepsilon_\chi\,\rangle$ is also a local pth power at $\mathfrak{p}$. We have obtained a class field theory version of a result given by the following properties of p-adic L-functions:

$$\begin{aligned}
L_p(0,\chi) &\equiv L_p(1,\chi) \bmod (p) \ \ \text{[W, Cor. 5.13]}\,,\\
L_p(0,\chi) &= -b_{\chi^*} \ \ \text{[W, Th. 5.11]}\,,\\
L_p(1,\chi) &= \tfrac{\tau(\chi)}{p}\sum_{k=1}^{p-1}\chi^{-1}(k)\log(1-\zeta^k) = \tfrac{\tau(\chi)}{p}\log(\eta_\chi^{p-1}) \ \ \text{[W, Th. 5.18]}\,,
\end{aligned}$$

where the Gauss sum $\tau(\chi)$ is of $\mathfrak{p}$-valuation $\leq p-2$, giving easily $b_{\chi^*} \equiv 0 \bmod (p)$ if and only if η_χ is a local pth power at $\mathfrak{p}$ (see Subsec. 3.3 and 3.4).

Then from the above, concerning the equality $\mathrm{rk}_p(\mathcal{C}\ell^+) = \mathrm{rk}_p(\mathcal{C}\ell^-)$, we would have, for each even χ such that $\mathrm{rk}_p(\mathcal{C}\ell_{\chi^*}) \geq 1$, the alternative $\mathrm{rk}_p(\mathcal{C}\ell_{\chi^*}) \geq 2$, or $\mathrm{rk}_p(\mathcal{C}\ell_{\chi^*}) = 1$ and in the writing ${}_p\mathcal{C}\ell_{\chi^*} = \langle\, c\ell(\mathfrak{a}_{\chi^*})\,\rangle$ then $\mathfrak{a}_{\chi^*}^p =: (\alpha)$ with α p-primary; all this is of course very strong because of the probabilistic value of $\mathrm{rk}_p(\mathcal{C}\ell^+)$ discussed in " Introduction and Generalities ".

We will return to reflection theorem in the proof of Theorems 3.7 and 3.9.

If we refer to [W, § 6.5], the value of $\mathrm{rk}_p(\mathcal{C}\ell)$ is conjecturally $\mathcal{O}\big(\frac{\log(p)}{\log(\log(p))}\big)$. With such a result, the inequality of Theorem 2.6 would be:

$$\mathrm{rk}_p(W) \leq \frac{p+1}{2} + \mathcal{O}\Big(\frac{\log(p)}{\log(\log(p))}\Big),$$

noting that the principal term $\frac{p+1}{2}$ comes from the p-units; this means, from Remark 2.5, (iii), that most of the elements of Ω (see Not. 2.4) are of the form $\varepsilon\,.\,\alpha^p$, $\varepsilon \in E_p$, $\alpha \in \mathbb{Z}[\zeta]$. In case Vandiver′s conjecture is satisfied, Theorem 2.6 reduces to:

$$\mathrm{rk}_p(W) \leq \frac{p+1}{2} + \frac{p-1}{4}, \ \text{ instead of } \ \leq p.$$

It is implausible that the p-rank of the radical W, generated by the images in $K^\times/K^{\times p}$ of the $3(p-1) + \frac{p+1}{2}$ multiplicatively independent elements of Γ, could be less than p.

2.4. Comparison of the local and global approaches. — Now we intend to show that any restriction to the local case leads to the following fact, where $K_\mathfrak{p}$ is the completion of K at $\mathfrak{p}$:

$$\mathrm{rk}_p\Big(\mathrm{Gal}\,\big(K_\mathfrak{p}(\sqrt[p]{W}\,)/K_\mathfrak{p}\big)\Big) \leq p;$$

in other words, the four radicals W_a, W_b, W_c, E_p/E_p^p become largely dependent by $\mathfrak{p}$-completion of the base field.
More precisely, we have $K_\mathfrak{p}(\sqrt[p]{W}\,) = K_\mathfrak{p}(\sqrt[p]{W_\mathfrak{p}}\,)$, where $W_\mathfrak{p} = \Gamma\,.\,K_\mathfrak{p}^{\times p}/K_\mathfrak{p}^{\times p}$ is the local radical generated by the image in $K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times p}$ of the $3(p-1) + \frac{p+1}{2}$ elements ζ, $1-\zeta$, $\varepsilon_1, \ldots, \varepsilon_{\frac{p-3}{2}}$, $a + b\,\zeta^i$, $b + c\,\zeta^j$, $c + a\,\zeta^k$, $i, j, k = 1, \ldots, p-1$.
For instance, if $p \,|\, c$, $W_\mathfrak{p}$ is the local radical generated by E_p (see Rem. 2.5, (iv)).

Since $\mathfrak{p}$ splits completely in H and is totally ramified in $H_{P\ell_p}/H$, by local class field theory the p-rank of Gal $\big(H_{P\ell_p}/H\big)$ is less than or equal to the p-rank of the inertia group of the maximal $\mathfrak{p}$-ramified abelian pro-p-extension $M_\mathfrak{p}$ of $K_\mathfrak{p} = H_\mathfrak{p}$, equal to the p-rank of the subgroup of units of $K_\mathfrak{p}^\times$, thus equal to p.
Since $K_\mathfrak{p}(\sqrt[p]{W_\mathfrak{p}}\,) = H_\mathfrak{p}(\sqrt[p]{W_\mathfrak{p}}\,) \subseteq M_\mathfrak{p}$, this yields as expected:

$$\mathrm{rk}_p(W_\mathfrak{p}) = \mathrm{rk}_p\Big(\mathrm{Gal}\,\big(K_\mathfrak{p}(\sqrt[p]{W_\mathfrak{p}}\,)/K_\mathfrak{p}\big)\Big) \leq p.$$

Returning to the global situation and using Theorem 2.6, we obtain directly that:

$$\mathrm{rk}_p(W_\mathfrak{p}) \leq \mathrm{rk}_p(W) \leq \frac{p+1}{2} + \mathrm{rk}_p(\mathcal{C}\ell) \leq p,$$

which is surprising since the global inequality is obtained via an approximate analytic formula.

So in the local situation we only have the following informations:

$$\mathrm{rk}_p(W_{\mathfrak p}) \le \frac{p+1}{2} + \mathrm{rk}_p(\mathcal{C}\ell),$$

knowing that (in a "numerical" point of view) $W_{\mathfrak p}$ does not contain more than p independent elements in $K_{\mathfrak p}^{\times}/K_{\mathfrak p}^{\times p}$, to be compared with the global situation:

$$\mathrm{rk}_p(W) \le \frac{p+1}{2} + \mathrm{rk}_p(\mathcal{C}\ell),$$

knowing that the p-rank of W in $K^{\times}/K^{\times p}$ is only limited by $3(p-1) + \frac{p+1}{2}$.

In the two directions (local or global), a contradiction (i.e., a proof of FLT) would be obtained by proving the following inequalities:

(i) *In the local case*:

$$\mathrm{rk}_p(W_{\mathfrak p}) > \frac{p+1}{2} + \mathrm{rk}_p(\mathcal{C}\ell),$$

under the fact that $\mathrm{rk}_p(W_{\mathfrak p})$ is $p-\delta(p)$, where the defect $\delta(p)$, in the first case of FLT, depends essentially of the local properties of Mirimanoff's polynomials (see Th. 3.5 and Th. 3.9), which gives the sufficient condition to be proved:

$$\delta(p) < p - \frac{p+1}{2} - \mathrm{rk}_p(\mathcal{C}\ell) = \frac{p-1}{2} - \mathrm{rk}_p(\mathcal{C}\ell),$$

which is unusable with the analytic inequality $\mathrm{rk}_p(\mathcal{C}\ell) \le \frac{p-1}{2}$ equivalent to $\delta(p) = 0$.(7)
In the second case of FLT, such a proof is also impossible since, as we have seen, $\mathrm{rk}_p(W_{\mathfrak p}) \le \mathrm{rk}_p(E_p) = \frac{p+1}{2}$.

(ii) *In the global case, for the two cases of FLT*:

$$\mathrm{rk}_p(W) > \frac{p+1}{2} + \mathrm{rk}_p(\mathcal{C}\ell),$$

under the fact that $\mathrm{rk}_p(W)$ is $3(p-1) + \frac{p+1}{2} - \Delta(p)$, where the defect $\Delta(p)$ depends on deep diophantine properties, which gives the sufficient condition to be proved:

$$\Delta(p) < 3(p-1) + \frac{p+1}{2} - \frac{p+1}{2} - \mathrm{rk}_p(\mathcal{C}\ell) = 3\,(p-1) - \mathrm{rk}_p(\mathcal{C}\ell),$$

realized as soon as $\Delta(p) < 5\,\frac{p-1}{2}$ with the analytic inequality $\mathrm{rk}_p(\mathcal{C}\ell) \le \frac{p-1}{2}$, which may be provable.

Remark 2.10. — (i) In the previous analysis, one may object that in an evident way, global radicals and class groups give equivalent informations (in spite of the fact that here we consider generalized classes), but we insist on the fact that these radicals, hence the corresponding classes, are of a very special nature (see for instance Conjecture 1.5, specific of this particular case).

(ii) If we replace the fundamental units ε_i by the cyclotomic units, we obtain the radical $\widetilde{W} = \langle\, \zeta, 1-\zeta^n, a+b\,\zeta^i, b+c\,\zeta^j, c+a\,\zeta^k \,\rangle \,.\, K^{\times p}/K^{\times p},\ \ n, i, j, k = 1, \ldots, p-1$, all the elements being of the special form $x + y\,\zeta^q$.

(7) Note that Mirimanoff's congruences tend to yield a large $\delta(p)$.

The radical $\widetilde{W}$ is of p-rank $3(p-1)+\frac{p+1}{2}-\widetilde{\Delta}(p)$, which requires to prove that $\widetilde{\Delta}(p) < 3(p-1)-\mathrm{rk}_p(\mathcal{C}\ell)$, with $\widetilde{\Delta}(p) \geq \Delta(p)$ because of possible cyclotomic units being pth powers of units (defect of Vandiver's conjecture), which seems to be acceptable, even if $\widetilde{\Delta}(p)$ is not so good, to perform $\widetilde{\Delta}(p) < 5\,\frac{p-1}{2}$.

2.5. Links with other invariants. — Since analytic aspects are important to get good upper bounds, it is useful to connect (or replace) the classical class group with other invariants. Moreover, a solution of Fermat's equation has important consequences on any arithmetic invariant, as the following ones.

(a) *Case of the torsion subgroup of* $\mathrm{Gal}\,(H_{Pl_p}/K)$.

Recall that $\mathrm{Gal}\,(H_{Pl_p}/K) \simeq \mathcal{C}\ell_{Pl_p}$ is isomorphic to $\mathbb{Z}_p^{\frac{p+1}{2}} \oplus \mathcal{T}$, where $\mathcal{T}$ is the (finite) p-torsion subgroup. Thus we get $\mathrm{rk}_p(W) \leq \mathrm{rk}_p(\mathcal{C}\ell_{Pl_p}) = \frac{p+1}{2} + \mathrm{rk}_p(\mathcal{T})$, giving $\mathrm{rk}_p(\mathcal{T}) \geq \mathrm{rk}_p(W) - \frac{p+1}{2}$. If $\mathcal{G}$ is the Galois group of the maximal Pl_p-ramified pro-p-extension of K, then the group $\mathcal{G}$ is defined by d generators and r relations, where:

$$\begin{aligned} d &= \mathrm{rk}_p(\mathrm{H}^1(\mathcal{G}, \mathbb{Z}/p\mathbb{Z})) = \mathrm{rk}_p(\mathcal{C}\ell_{Pl_p}) = \frac{p+1}{2} + \mathrm{rk}_p(\mathcal{T}), \\ r &= \mathrm{rk}_p(\mathrm{H}^2(\mathcal{G}, \mathbb{Z}/p\mathbb{Z})), \end{aligned}$$

with the duality $\mathrm{H}^2(\mathcal{G}, \mathbb{Z}/p\mathbb{Z})^* \simeq {}_p\mathcal{T}$ (see for instance [Gr1, App., Th. 2.2]), giving:

$$\mathrm{rk}_p(\mathrm{H}^2(\mathcal{G}, \mathbb{Z}/p\mathbb{Z})) \geq \mathrm{rk}_p(W) - \frac{p+1}{2} = 3(p-1) - \Delta(p).$$

One may expect that there exist some constraints on such cohomology groups.

The field K is said to be p-rationnal (see [MN]) if $\mathcal{T} = 1$, which is equivalent to $\mathcal{C}\ell = 1$ (K is p-regular in the Kummer sense).

From the reflection theorem (see [Gr2, Th. 10.10]), we have for any χ with $\chi^* = \omega\,\chi^{-1}$: (8)

$$\mathrm{rk}_p(\mathcal{T}_\chi) = \mathrm{rk}_p(\mathcal{C}\ell_{\chi^*}).$$

From the interpretation of the reflection principle for the groups $\mathcal{C}\ell_\chi$ recalled in the Theorem 2.8, (ii) (see also [Gr1, II.5.4.9.2]), we obtain a similar result between the groups $\mathcal{T}_\chi$ and $\mathcal{T}_{\chi^*}$:

$$\mathrm{rk}_p((Y/Y_{\mathrm{prim}})_{\chi^*}) = \mathrm{rk}_p(\mathcal{T}_\chi) - \mathrm{rk}_p(\mathcal{T}_{\chi^*}) = 1 - \mathrm{rk}_p((Y/Y_{\mathrm{prim}})_\chi),$$

for any even χ, where Y is the group of pseudo-units and Y_{prim} the subgroup of p-primary pseudo-units.

Hence, for the group $\mathcal{T}$, the " Vandiver conjecture" is $\mathcal{T}^- = 1$.

Let us mention the two relations (equalities up to a p-adic unit):

$$|\,\mathcal{T}^+\,| = |\,\mathcal{C}\ell^+\,|\,.\,\frac{\mathrm{Reg}^+}{\mathrm{Disc}^+}\,, \quad |\,\mathcal{T}^-\,| = \frac{|\,\mathcal{C}\ell^-\,|}{(\mathbb{Z}_p \log(I^-) : \mathbb{Z}_p \log(P^-))}\,,$$

(8) For a direct proof, use the fact that the relative component $\mathcal{C}\ell^-_{Pl_p}$ is the sum of $\mathcal{T}^-$ and of the Galois group of the compositum of the relative $\mathbb{Z}_p$-extensions giving the representation $\mathbb{Z}_p[g]^-$; the real part $\mathcal{C}\ell^+_{Pl_p}$ is the sum of $\mathcal{T}^+$ and of $\mathbb{Z}_p$ with trivial character; so [Gr1, Th. II.5.4.5] gives the formula.

where Reg^+ is the p-adic regulator, Disc^+ the discriminant, of K^+, I the group of ideals prime to p, P the subgroup of principal ideals, of K; if c is the complex conjugation and $\mathfrak{a}$ an ideal of K, let n be such that $\mathfrak{a}^{n\frac{1-c}{2}} = (\alpha)$, then $\log(\mathfrak{a}^{\frac{1-c}{2}}) := \frac{1}{n}\log(\alpha)$ where log is the Iwasawa logarithm for which $\log(p) = 0$ (note that for the minus part, the units do not enter in the use of log; see [Gr1, Cor. III.2.6.1, Rem. III.2.6.5] for more details and references).

As for the class group, the existence of a solution of Fermat′s equation has a great influence on the group $\mathcal{T}$, for instance on the study of the index $\big(\mathbb{Z}_p \log(I^-) : \mathbb{Z}_p \log(P^-)\big)$ regarding the relations $(x + y\,\zeta) = \mathfrak{p}\,\mathfrak{z}_1^p$ or $\mathfrak{z}_1^p$ giving:

$$\log\Big(\mathfrak{z}_1^{\frac{1-c}{2}}\Big) := \frac{1-c}{2}\,\frac{1}{p}\log(x + y\,\zeta) = \frac{1-c}{2}\,\frac{1}{p}\log\Big(1 + \frac{y}{x+y}\,(\zeta - 1)\Big).$$

Mention also the following reasoning giving another interpretation of a result of Iwasawa [Iw], which may have some interest [(9)]:

For an even χ, since $\mathbb{Z}_p \log(P^-) = \log(U^-)$ where U is the group of principal units of $K_{\mathfrak{p}}$, we obtain easily:

$$|\mathcal{T}_{\chi^*}| = \frac{|\mathcal{C}\ell_{\chi^*}|}{\big(e_{\chi^*}\,.\,\mathbb{Z}_p\log(I) : e_{\chi^*}\,.\,\log(U)\big)}\,.$$

The main theorem on cyclotomic fields (see Th. 2.8, (iii)) gives $|\mathcal{C}\ell_{\chi^*}| = |b_{\chi^*}|_p^{-1}$ (the p-part of the corresponding generalized Bernoulli number $b_{\chi^*} \in \mathbb{Z}_p$).

We know that for any prime ideal $\mathfrak{l}$ of K, $\mathfrak{l} \neq \mathfrak{p}$, we have:

$$\mathfrak{l}^{pS} = \mathcal{G}(\mathfrak{l})^p\,\mathbb{Z}[\zeta],$$

where $S := \frac{1}{p}\sum_{k=1}^{p-1} k\,s_k^{-1}$ is the Stickelberger element [(10)] and $\mathcal{G}(\mathfrak{l})$ the Gauss sum:

$$\mathcal{G}(\mathfrak{l}) := -\sum_{t \in F_{\mathfrak{l}}} \psi(t)\,\zeta_\ell^{\mathrm{tr}(t)},$$

where $F_{\mathfrak{l}}$ is the residue field, ψ the canonical character of order p of $F_{\mathfrak{l}}^\times$, ζ_ℓ a primitive ℓth root of unity, and tr the trace in the residual extension $F_{\mathfrak{l}}/\mathbb{F}_\ell$. Thus taking log we obtain for all even χ:

$$e_{\chi^*}\,.\,S\,.\,\log(\mathfrak{l}) = e_{\chi^*}\,.\,b_{\chi^*}\,.\,\log(\mathfrak{l}) = e_{\chi^*}\,.\,\log(\mathcal{G}(\mathfrak{l})).$$

Then $|b_{\chi^*}|_p^{-1}\,e_{\chi^*}\,.\,\mathbb{Z}_p\log(\mathfrak{l}) = e_{\chi^*}\,.\,\mathbb{Z}_p\log(\mathcal{G}(\mathfrak{l}))$, thus:

$$|\mathcal{T}_{\chi^*}| = \frac{|b_{\chi^*}|_p^{-1}}{\Big(\frac{1}{|b_{\chi^*}|_p^{-1}}\,e_{\chi^*}\,.\,\mathbb{Z}_p\log(\mathcal{G}) : e_{\chi^*}\,.\,\log(U)\Big)}\,,$$

where $\mathcal{G}$ is the group generated by all the Gauss sums $\mathcal{G}(\mathfrak{l})$.

---

(9) From a talk given in 1982 in the University Laval, Québec; published in the mathematical series, N°20 (1984), of the department of mathematics.

(10) We have $e_{\chi^*}\,.\,S = b_{\chi^*}\,.\,e_{\chi^*}$; this explains that we use a different definition from that of [W] for the generalized Bernoulli numbers.

So, the Vandiver conjecture for χ even ($\mathcal{C}\ell_\chi = \mathcal{T}_{\chi^*} = 1$) is equivalent to the fact that $e_{\chi^*} . \mathbb{Z}_p \log(\mathcal{G}) = e_{\chi^*} . \log(U)$, and the whole Vandiver conjecture is equivalent to the fact that the images of the Gauss sums in U generate the minus part of this $\mathbb{Z}_p$-module.

(b) *Case of the regular and wild kernels.*

Recall the fundamental diagram of K-theory, in which $\mathrm{WK}_2(K)$ is called the wild kernel and $\mathrm{R}_2(K)$ the regular kernel in the ordinary sense. We specify the diagram recalled in [Gr1, II.7.6] to the case of the cyclotomic field K (h is the Hilbert symbol and h^{reg} the regular Hilbert symbol, which is explicit):

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{WK}_2(K) & \longrightarrow & \mathrm{K}_2(K) & \xrightarrow{h} & \bigoplus_{v \in Pl^{\mathrm{nc}}} \mu(K_v) & \xrightarrow{\pi} & \mu(K) \longrightarrow 1 \\
 & & \| & & \| & & \downarrow & & \downarrow \\
1 & \longrightarrow & \mathrm{R}_2(K) & \longrightarrow & \mathrm{K}_2(K) & \xrightarrow{h^{\mathrm{reg}}} & \bigoplus_{v \in Pl^{\mathrm{nc}}} \mu(K_v)^{\mathrm{reg}} & \longrightarrow & 1\,,
\end{array}$$

since $(\mathrm{R}_2 : \mathrm{WK}_2) = 1$ for $K = \mathbb{Q}(\zeta)$ (use [Gr1, II.7.6.1]).

For R_2 we have a Kummer interpretation, coming from results of Tate [Ta], which is given by the exact sequence:

$$1 \longrightarrow \mu_p \otimes \mathrm{N}_2 \longrightarrow \mu_p \otimes W_{Pl_p} \xrightarrow{\ f\ } {}_p\mathrm{R}_2 \longrightarrow 1,$$

where W_{Pl_p} is the initial radical of H_{Pl_p}/K, f being defined by $f(\zeta \otimes \alpha) := \{\zeta\,,\,\alpha\}$ for all $\alpha \in W_{Pl_p}$, and where $\mathrm{N}_2 := \{\alpha \in K^\times,\ \{\zeta\,,\,\alpha\} = 1\}/K^{\times p}$ (Tate′s kernel) is such that (as g-modules):

$$\mu_p \otimes \mathrm{N}_2 \simeq (\mu_p \otimes \mu_p) \oplus \mu_p^{\frac{p-1}{2}}\,.$$

We then have $\mathrm{rk}_p(\mathrm{R}_2) = \mathrm{rk}_p(W_{Pl_p}) - \frac{p+1}{2} = \mathrm{rk}_p(\mathcal{C}\ell)$ (see [Gr1, II.7.7.2.2]). More precisely, using characters, we have here another principle of reflection, since we must associate χ with $\overline{\chi} := \omega^{-1}\chi = (\chi^*)^{-1}$, giving for all χ:

$$\mathrm{rk}_p(\mathrm{R}_{2,\,\chi}) = \mathrm{rk}_p(\mathcal{C}\ell_{\omega^{-1}\chi}) = \mathrm{rk}_p(\mathcal{T}_{\omega^2\chi^{-1}}).$$

As for the group $\mathcal{T}$, we get for any even χ:

$$\mathrm{rk}_p((Y/Y_{\mathrm{prim}})_{\chi^*}) = \mathrm{rk}_p(\mathrm{R}_{2,\,\omega^2\chi^{-1}}) - \mathrm{rk}_p(\mathrm{R}_{2,\,\omega\chi}) = 1 - \mathrm{rk}_p((Y/Y_{\mathrm{prim}})_\chi),$$

and “ Vandiver′s conjecture” for R_2 is $R_2^- = 1$.
This can be deduced from the above exact sequence by proving that the groups $\langle\,\zeta\,\rangle \otimes_{\mathbb{Z}_p} \mathcal{C}\ell$ and ${}_p\mathrm{R}_2$ are isomorphic g-modules, which is coherent with the above reflection. Another proof uses the isomorphism proved by Jaulent [J] between $\mathrm{WK}_2/(\mathrm{WK}_2)^p$ and $\langle\,\zeta\,\rangle \otimes_{\mathbb{Z}_p} \widetilde{\mathcal{C}\ell}$, where $\widetilde{\mathcal{C}\ell}$ is the logarithmic p-class group, and the isomorphism $\widetilde{\mathcal{C}\ell} \simeq \mathcal{C}\ell$ for K (see [Gr1, Exer. III.7.1]).

The field K is said to be p-regular (in the K-theory sense) if the p-Sylow of the regular kernel R_2 is trivial (see [JN, GJ]); here it is the case if and only if $\mathcal{C}\ell = 1$.

We have here a complete parallelism between regular kernel and class group (with another Galois action), which may be interesting by studying for instance the map f on the elements $x + y\,\zeta$ of the radical $W \subseteq W_{Pl_p}$, and so on.

We know that $\mathrm{R}_2^+ := \mathrm{R}_2(K^+)$ is given by the value at -1 of the Dedekind zeta function ζ_{K^+} of K^+; more precisely, after the proof of Birch–Tate conjecture by Wiles (on this subject, see e.g. Greither [Gre]) we get:

$$|\,\mathrm{R}_2^+\,| = \frac{24\,p}{2^{\frac{p-1}{2}}}\,\left|\,\zeta_{K^+}(-1)\,\right|$$

(see Washington′s book [Wa, Ch. IV] to compute the analytic expression of $|\,\mathrm{R}_2^+\,|$). For the minus part $|\,\mathrm{R}_2^-\,|$, we don′t know convenient analytic formula as for $|\,\mathcal{T}^-\,|$; we only have the isomorphism ${}_p\mathrm{R}_2^- \simeq (\langle\,\zeta\,\rangle \otimes_{\mathbb{Z}_p} \mathcal{C}\!\ell)^-$.

3. Some classical local considerations revisited (first case of FLT)

To study the p-rank of the radical W we begin with the partial radical W_c, in the first case of FLT, or the radical generated by W_c and the units.

Thus in this Section we suppose that $p \nmid c$; so we will have similar results by permutations of $\{a,\, b,\, c\}$ with no more global informations as explained in Section 2; moreover, since $a + b\,\zeta = \zeta\,(b + a\,\zeta^{-1})$, the radical W contains the conjugates of $b + a\,\zeta^{-1}$ and we can add the transpositions of the set $\{a,\, b,\, c\}$, so that the reasonings (in the first case of FLT) are valid for any $(x,\, y) \in \{(a,\, b),\, (b,\, a),\, (b,\, c),\, (c,\, b),\, (c,\, a),\, (a,\, c)\}$.

3.1. Logarithmic derivative: Mirimanoff′s polynomials. — We need, *once for all*, a convenient characterization of p-primarity; the best way is to use the method of derivation of Eichler. Everything depends on this.

From a solution (a, b, c) in the first case of Fermat′s equation, we study the relation:

$$\prod_{i=1}^{p-1} (a + b\,\zeta^i)^{\lambda_i} = \alpha^p,\ \ \lambda_i \in \{0, \ldots, p-1\},\ \ \alpha \in \mathbb{Z}[\zeta].\ ^{(11)}$$

Since $a + b$ is a pth power (Lem. 1.1), it is equivalent to consider, for $e := \frac{b}{a+b}$:

$$\prod_{i=1}^{p-1} (1 + e\,(\zeta^i - 1))^{\lambda_i} = \beta^p,\ \ \lambda_i \in \{0, \ldots, p-1\},\ \ \beta \in \mathbb{Z}_{(p)}[\zeta].$$

This relation is equivalent to the polynomial relation:

$$F(X) := \prod_{i=1}^{p-1} (1 + e\,(X^i - 1))^{\lambda_i} = G(X)^p + A(X)\,\Phi_p(X),\ \ G,\, A \in \mathbb{Z}_{(p)}[X],$$

where $\Phi_p(X)$ is the pth cyclotomic polynomial.

(11) Without any change, we can study the same relation in $\mathbb{Z}_p[\zeta]$ instead of $\mathbb{Z}[\zeta]$; in that case, we will obtain a N.S.C. (see Th. 3.5).

Lemma 3.1. — *We can choose $G(X)$ modulo $\Phi_p(X)$ such that:*

$$F(X) = \prod_{i=1}^{p-1} (1 + e\,(X^i - 1))^{\lambda_i} = H(X)^p + B(X)\,(X^p - 1), \ \ H,\, B \in \mathbb{Z}_{(p)}[X].$$

Proof. — Since $F(1) = 1$, $G(1)^p + A(1)\,p = 1$, thus $G(1)^p \equiv G(1) \equiv 1 \bmod (p)$ and $G(1) = 1 + \Lambda\,p$, $\Lambda \in \mathbb{Z}_{(p)}$. Put $G_1(X) := G(X) - \Lambda\,\Phi_p(X)$; this yields to $G_1(1) = G(1) - \Lambda\,p = 1$.
We have $F(X) = G_1(X)^p + A_1(X)\,\Phi_p(X)$ for some $A_1(X)$.
We obtain $F(1) = 1 = G_1(1)^p + A_1(1)\,p = 1 + A_1(1)\,p$, in other words $A_1(1) = 0$. Thus $A_1(X) = (X - 1)\,B(X)$. We then put $H(X) := G_1(X)$. □

By logarithmic derivation, since $e \not\equiv 0 \bmod (p)$ in the first case of FLT and since $F(X)$ is invertible modulo $(p, X^p - 1)$, this gives:

$$\sum_{i=1}^{p-1} \frac{\lambda_i\, i\, X^{i-1}}{1 + e\,(X^i - 1)} \in (p, X^p - 1)_{\mathbb{Z}_{(p)}[[X]]}. \tag{1}$$

Remark 3.2. — From this formula we deduce (taking $X = 1$) the necessary condition $\sum_{i=1}^{p-1} \lambda_i\, i \equiv 0 \bmod (p)$, which gives one nontrivial relation between the λ_i. This relation is due to an obstruction on the ω-component (see Rem. 3.4).
The interest of Lemma 3.1 is that $(p, X^p - 1)' \subseteq (p, X^p - 1)$.

The series $\dfrac{1}{1 + e\,(X^i - 1)} = \sum_{j \geq 0} (-1)^j\, e^j\, (X^i - 1)^j$ are convergent for the $(X - 1)$-adic topology and, since $(X^i - 1)^p \in (p, X^p - 1) = (p, (X - 1)^p)$, we obtain, after multiplication by X, the equivalent condition:

$$\sum_{i=1}^{p-1} \lambda_i\, i\, X^i \sum_{j=0}^{p-1} (-1)^j\, e^j\, (X^i - 1)^j \in (p, (X - 1)^p).$$

Thus, using $(X^i - 1)^j = \sum_{k \geq 0} (-1)^{j-k} \binom{j}{k} X^{ik}$, with $\binom{j}{k} = 0$ for $k > j$, this yields:

$$\sum_{k \geq 0} \sum_{i=1}^{p-1} \lambda_i\, i\, X^{i(k+1)} \,.\, (-1)^k \sum_{j=k}^{p-1} \binom{j}{k}\, e^j \in (p, (X - 1)^p).$$

Since $j \leq p - 1$ and $\binom{j}{k} = 0$ for $k > j$, we can limit k to the value $p - 1$; for $k = p - 1$ we get the term $\sum_{i=1}^{p-1} \lambda_i\, i\, X^{ip}\, e^{p-1} \equiv \sum_{i=1}^{p-1} \lambda_i\, i \equiv 0 \bmod (p, X^p - 1)$.
Then, under the condition $\sum_{i=1}^{p-1} \lambda_i\, i \equiv 0 \bmod (p)$, we can suppose that k varies from 0 to $p - 2$. Put:

$$\varphi_{k+1}(X) := \sum_{i=1}^{p-1} \lambda_i\, i\, X^{i(k+1)}, \quad k = 0, \ldots, p - 2.$$

We obtain the following condition (2), equivalent to (1) under the condition $\sum_{i=1}^{p-1} \lambda_i\, i \equiv 0 \bmod (p)$:

$$\sum_{k=0}^{p-2} \varphi_{k+1}(X) \,.\, A_k \in (p, (X - 1)^p), \ \text{ with } A_k := (-1)^k \sum_{j=k}^{p-1} \binom{j}{k}\, e^j. \tag{2}$$

Lemma 3.3. — *We have* $A_k \equiv (-1)^k \frac{e^k}{k!} D^{(k)}(e) \equiv \big(\frac{-b}{a}\big)^k \bmod (p)$, $k = 0, \ldots, p-2$, *where* $D(Y) := 1 + Y + \ldots + Y^{p-1}$.

Proof. — We have $A_0 = D(e) = \frac{e^p-1}{e-1} \equiv 1 \bmod (p)$ since $e \not\equiv 1 \bmod (p)$ (otherwise $a \equiv 0 \bmod (p)$). The first general relation giving A_k is immediate by induction, using $\binom{j}{k} = \frac{j!}{k!\,(j-k)!}$ and $D^{(k)}(Y) = \frac{k!}{0!} + \frac{(k+1)!}{1!}\,Y + \ldots + \frac{(k+p-1-k)!}{(p-1-k)!}\,Y^{p-1-k}$.

Since $D(Y) = 1 + Y + \ldots + Y^{p-1} = \frac{Y^p-1}{Y-1} \equiv (Y-1)^{p-1} \bmod p\,\mathbb{Z}[Y]$, we have $D^{(k)}(e) \equiv (p-1)\ldots(p-k)\,.\,(e-1)^{p-1-k} \equiv (-1)^k\,k!\,(e-1)^{-k} \bmod (p)$.
Then $A_k \equiv (-1)^k \frac{e^k}{k!} D^{(k)}(e) \equiv \big(\frac{e}{e-1}\big)^k = \big(\frac{-b}{a}\big)^k \bmod (p)$, hence the result. □

We intend to use this formula in the case of the action of the idempotents $e_\chi \in \mathbb{Z}_p[g]$, $\chi = \omega^m$ (where $g = \mathrm{Gal}\,(K/\mathbb{Q})$) on the previous pseudo-unit $1 + e\,(\zeta - 1)$ (see Not. 2.7).

The formulation of the condition $F(X) = H(X)^p + B(X)(X^p - 1)$ corresponds to the choice $\lambda_i \equiv \frac{1}{p-1}\omega^{-m}(i)$ modulo $p\,\mathbb{Z}_p[\zeta]$; the necessary condition $\sum_{i=1}^{p-1} \lambda_i\, i \equiv 0 \bmod (p)$ (see Rem. 3.2) is satisfied for any $m \in \{1, \ldots, p-1\}$, except $m = 1$ (i.e., $\chi = \omega$).
For $m \neq 1$ we obtain from the above:

$$\varphi_{k+1}(\zeta) = \tfrac{1}{p-1} \sum_{i=1}^{p-1} \omega^{-m}(i)\, i\, \zeta^{i(k+1)} \equiv \tfrac{1}{p-1} \sum_{i=1}^{p-1} \omega^{1-m}(i)\, \zeta^{i(k+1)} \bmod (p),$$

$$\sum_{k=0}^{p-2} \varphi_{k+1}(\zeta)\,.\,A_k = \sum_{k=1}^{p-1} \varphi_k(\zeta)\,.\,A_{k-1} \equiv \tfrac{1}{p-1} \sum_{k=1}^{p-1} \Big(\sum_{i=1}^{p-1} \omega^{1-m}(i)\, \zeta^{ik} \Big)\,.\,A_{k-1} \bmod (p).$$

We have obtained the necessary condition (put $j := i\,k$ modulo p):

$$-\sum_{k=1}^{p-1}\sum_{j=1}^{p-1} \omega^{1-m}(jk^{-1})\, \zeta^j\,.\,A_{k-1} = \Big(\sum_{k=1}^{p-1} \omega^{m-1}(k)\,.\,A_{k-1} \Big)\Big(-\sum_{j=1}^{p-1} \omega^{1-m}(j)\, \zeta^j \Big) \equiv 0 \bmod (p),$$

where:

$$-\sum_{j=1}^{p-1} \omega^{1-m}(j)\, \zeta^j =: \tau(\omega^{1-m}),$$

is the Gauss sum of ω^{1-m}, for which:

$$\tau(\omega^{1-m})\,.\,\overline{\tau}(\omega^{m-1}) = p, \quad \text{where } \overline{\tau}(\varphi) := -\sum_{k=1}^{p-1} \varphi(k)\zeta^{-k} = \varphi(-1)\,\tau(\varphi)$$

for any character φ.

But $\tau(\omega^{1-m})$, as element of $\mathbb{Z}_p[\zeta]$, is of $\mathfrak{p}$-valuation $m-1$, $m \in \{1, \ldots, p-1\}$ (see Prop. 3.17 in Subsec. 3.4). The final necessary condition is thus, for $m \neq 1$:

$$\sum_{k=1}^{p-1} \omega^{m-1}(k)\,.\,A_{k-1} \equiv 0 \bmod p\,\mathbb{Z}_p[\zeta]. \tag{3}$$

Remark 3.4. — For $m = 1$ (i.e., $\chi = \omega$) a direct computation gives:

$$\begin{aligned}(1+e\,(\zeta-1))^{e_\omega} &= \prod_{i=1}^{p-1}\big(1+e\,(\zeta^i-1)\big)^{\frac{\omega^{-1}(i)}{p-1}} \equiv \prod_{i=1}^{p-1}\big(1+e\,\omega^{-1}(i)\,(\zeta^i-1)\big)^{\frac{1}{p-1}}\\ &\equiv \prod_{i=1}^{p-1}\big(1+e\,(\zeta-1)\big)^{\frac{1}{p-1}} \equiv 1+e\,(\zeta-1) \bmod \mathfrak{p}^2,\end{aligned}$$

using $\zeta^i - 1 = \frac{\zeta^i-1}{\zeta-1}\,(\zeta-1) \equiv i\,(\zeta-1) \bmod \mathfrak{p}^2$.

Theorem 3.5. — *Let (a,b,c) be a solution in the first case of Fermat's equation; put $e = \frac{b}{a+b}$. Let $\chi = \omega^m$ be a p-adic character of g distinct from ω.*
Then the pseudo-unit $(a+b\,\zeta)^{e_\chi}$ or $(1+e\,(\zeta-1))^{e_\chi}$ is a pth power in $K_\mathfrak{p}$ if and only if:

$$\sum_{k=1}^{p-1}\omega^{m-1}(k)\big(\tfrac{-b}{a}\big)^k \equiv 0 \bmod (p).$$

Proof. — We have to prove the sufficiency of the condition. We note that this congruential condition is (for $\chi \neq \omega$) only equivalent to $F'(X) \in (p, \Phi_p(X)) = (p, (X-1)^{p-1})$ in $\mathbb{Z}_p[X]$, since $(X-1)\Phi_p(X) = X^p - 1 \equiv (X-1)^p \bmod (p)$ (see (1), (2), (3)).
Suppose that the condition $F'(X) \in (p, (X-1)^{p-1})$ is satisfied for the coefficients $\lambda_i = \frac{1}{p-1}\chi^{-1}(i)$ in $F(X) = \prod_{i=1}^{p-1}(1+e\,(X^i-1))^{\lambda_i}$.
Write $F(X) = \sum_{n=0}^{p-1} u_n\,(X-1)^n + U(X)\,(X-1)^p$ in $\mathbb{Z}_p[X]$; since:

$$F'(X) = \sum_{n=1}^{p-1} n\,u_n(X-1)^{n-1} + p\,U(X)\,(X-1)^{p-1} + U'(X)\,(X-1)^p$$

is in $(p, (X-1)^{p-1})$, this yields to $u_n \equiv 0 \bmod (p)$ for $n = 1, \ldots, p-1$.
Then $F(\zeta) \equiv u_0 \bmod (p)$; from Theorem 2.2, $F(\zeta)$ being a pseudo-unit congruent to a rational modulo p is a local pth power. Which proves the theorem obtained by Thaine [Th3] using generalized binomial computations. □

Remark 3.6. — (i) We have obtained that in our viewpoint using radicals, the p-primarity of the pseudo-unit $(1+e\,(\zeta-1))^{e_\chi}$, $\chi \neq \omega$, is directly characterized by means of the polynomial:

$$M_m(Z) := \sum_{k=1}^{p-1}\omega^{m-1}(k)Z^k.$$

As the reader can see, this polynomial is a variant of the classical polynomial of Mirimanoff $\widetilde{M}_m(Z) := \sum_{k=1}^{p-1} k^{m-1}Z^k$ and is congruent modulo p to it (see [R, VIII.1] for more information; see [A1] for the use of Mirimanoff's polynomials in Iwasawa theory over K; see [Th2, I] for the definition of polynomial congruences equivalent to Mirimanoff's congruences and giving a direct proof of some Wieferich's criteria).

(ii) We see that $M_m(Z)$ comes from the Gauss sum $\tau(\omega^{m-1})$ that we have encountered before (put $Z = \zeta$), and this has probably a deep signification (see Subsec. 3.4 for some insights).

This shows that this indexation is not convenient; we observe that $M_m(Z)$ must be denoted $M_{\chi^*}(Z)$, where $\chi^* = \omega\chi^{-1} = \omega^{1-m}$, and more generally $M_\varphi(Z) := \sum_{k=1}^{p-1} \varphi^{-1}(k)\, Z^k$ for any character φ.

Thus, to summarize:

$$\begin{aligned} M_{\chi^*}(Z) &:= \sum_{k=1}^{p-1} (\chi^*)^{-1}(k)\, Z^k \\ M_{\chi^*}(\zeta) &= \sum_{k=1}^{p-1} (\chi^*)^{-1}(k)\, \zeta^k = -\tau((\chi^*)^{-1}); \end{aligned}$$

for convenience, we will use the two notations, the rule being $M_{\omega^h} = M_{p-h}$.

We see also that by all permutations of a, b, c, the p-primarity of the corresponding pseudo-units $(x + y\,\zeta)^{e_\chi}$, $\chi \neq \omega$ (i.e., $\chi^* \neq \chi_0$), is equivalent to the congruence:

$$M_{\chi^*}\Big(\frac{-y}{x}\Big) = \sum_{k=1}^{p-1} (\chi^*)^{-1}(k) \Big(\frac{-y}{x}\Big)^k \equiv 0 \bmod (p).$$

This notation which associates χ (for $(x + y\,\zeta)^{e_\chi}$) and χ^* (for $M_{\chi^*}\big(\frac{-y}{x}\big)$) anticipates the use of reflection theorems.

(iii) The advantage of this definition of Mirimanoff′s polynomials, indexed by the characters of g, is that they may be related to characters of some subfields of K, giving a more precise information (use Th. 2.8, (i)), and the knowledge of the p-class groups of the subfields may have suitable consequences for the properties of these polynomials (e.g. $\chi = \omega^{\frac{p-1}{2}}$, $\chi^* = \omega^{\frac{p+1}{2}}$).

***Theorem 3.7* (algebraic form of Kummer′s congruences)**. — *Let (a, b, c) be a solution in the first case of Fermat′s equation.*

If for an odd character $\chi \neq \omega$, $M_{\chi^*}\big(\frac{-b}{a}\big) \not\equiv 0 \bmod (p)$ (where $\chi^* = \omega\chi^{-1}$), then the χ-component $\mathcal{C}\ell_\chi := \mathcal{C}\ell^{e_\chi}$ of the p-class group is nontrivial.

Proof. — We have $(1 + e\,(\zeta - 1))^{e_\chi} \notin K^{\times p}$ since this pseudo-unit is not a local pth power at $\mathfrak{p}$. Put $(1 + e\,(\zeta - 1))^{e_\chi}\, \mathbb{Z}_{(p)}[\zeta] = \mathfrak{z}^p$; if the ideal $\mathfrak{z}$ is principal, say $\mathfrak{z} = (z)$, then:

$$(1 + e\,(\zeta - 1))^{e_\chi} = \varepsilon\, z^p, \ \text{ where } \varepsilon \in E_\chi := E^{e_\chi};$$

since χ is odd and distinct from ω (the character of $\langle\,\zeta\,\rangle$), $\varepsilon = 1$, giving a global pth power for $(1 + e\,(\zeta - 1))^{e_\chi}$ (contradiction). Thus $c\ell(\mathfrak{z}) \in \mathcal{C}\ell_\chi$ is nontrivial. □

From the main theorem on cyclotomic fields (see Th. 2.8, (iii))), the p-valuation of $|\,\mathcal{C}\ell_\chi\,|$ is that of the generalized Bernoulli number:

$$b_\chi := \tfrac{1}{p} \sum_{k=1}^{p-1} \chi^{-1}(k) k;$$

so $b_\chi \equiv 0 \bmod (p)$ or, equivalentely since $\chi = \omega^m$, $m \neq 1$ odd, the ordinary Bernoulli number B_{p-m} is congruent to 0 modulo p (see [W, Cor. 5.15]).

Actually Stickelberger′s theorem is sufficient to get $b_\chi \equiv 0 \bmod (p)$; if we want the reciprocal of " Herbrand′s theorem", we can use [Ri], [Th4] to get that $b_\chi \equiv 0 \bmod (p)$ is equivalent to $\mathcal{C}\!\ell_\chi \neq 1$.

We find again in a more precise way the classical situation of Kummer′s congruences which are:

$$b_\chi \cdot M_{\chi^*}\big(\tfrac{-b}{a}\big) \equiv 0 \bmod (p).$$

If $M_{\chi^*}\big(\frac{-b}{a}\big) \not\equiv 0 \bmod (p)$, then $\mathcal{C}\!\ell_\chi \neq 1$ and for χ^* (even and nontrivial), we know by reflection (see Exa. 2.9) that the χ^*-cyclotomic unit $\eta_{\chi^*} := (1-\zeta)^{e_{\chi^*}}$ is a *local* pth power at $\mathfrak{p}$. It is a global pth power if and only if $\mathcal{C}\!\ell_{\chi^*}$ is nontrivial (Vandiver′s conjecture false at χ^*).

Remark 3.8. — If $\chi \neq \chi_0$ is even, if $M_{\chi^*}\big(\frac{-b}{a}\big) \not\equiv 0 \bmod (p)$, and if the ideal $\mathfrak{z}$ is principal (in the wtiting $(1+e\,(\zeta-1))^{e_\chi}\,\mathbb{Z}[\zeta] = \mathfrak{z}^p$), we only obtain the relation $(1+e\,(\zeta-1))^{e_\chi} = \varepsilon_\chi\, z^p$, where $\varepsilon_\chi \in E_\chi$ is not a local pth power at $\mathfrak{p}$.
The basic example for this is $\mathcal{C}\!\ell_{\chi^*} = 1$, thus $\mathcal{C}\!\ell_\chi = 1$ (Vandiver′s conjecture true at χ); we then have $b_{\chi^*} \not\equiv 0 \bmod (p)$ thus $M_\chi\big(\frac{-b}{a}\big) \equiv 0 \bmod (p)$, which implies that $(1+e\,(\zeta-1))^{e_{\chi^*}}$ is a global pth power since $\mathcal{C}\!\ell_\chi = 1$.
If $\mathfrak{z}$ is nonprincipal, then $\mathcal{C}\!\ell_\chi \neq 1$ (counterexample to Vandiver′s conjecture), $\mathcal{C}\!\ell_{\chi^*} \neq 1$, $b_{\chi^*} \equiv 0 \bmod (p)$, and $M_\chi\big(\frac{-b}{a}\big)$ is a priori arbitrary (see Rem. 3.11 for improvements of these reasonings).

Theorem 3.9 **(algebraic form of Mirimanoff′s congruences: the reflection theorem)** *Let $\chi \neq \chi_0$ be even, and let $\chi^* = \omega\chi^{-1}$ (χ^* is odd distinct from ω).*
Then we have $M_{\chi^*}\big(\frac{-y}{x}\big) \,.\, M_\chi\big(\frac{-y}{x}\big) \equiv 0 \bmod (p)$ for any of the six pairs (x,y) corresponding to a solution in the first case of Fermat′s equation.

Proof. — To prove this congruence, we suppose that both $M_{\chi^*}\big(\frac{-y}{x}\big)$ and $M_\chi\big(\frac{-y}{x}\big)$ are not congruent to 0 modulo p to obtain a contradiction.

From the Theorem 2.8, (ii), or [Gr1, II.5.4.9.2], the analysis of the reflection theorem in K leads to the following equalities (χ even):

$$\mathrm{rk}_p((Y/Y_{\mathrm{prim}})_{\chi^*}) = \mathrm{rk}_p(\mathcal{C}\!\ell_{\chi^*}) - \mathrm{rk}_p(\mathcal{C}\!\ell_\chi) = 1 - \mathrm{rk}_p((Y/Y_{\mathrm{prim}})_\chi),$$

where Y is the group of pseudo-units of K, and where Y_{prim} is the subgroup of p-primary pseudo-units.

The condition $M_\chi\big(\frac{-y}{x}\big) \not\equiv 0 \bmod (p)$ is thus equivalent to $(x+y\,\zeta)^{e_{\chi^*}} \in Y\backslash Y_{\mathrm{prim}}$ giving $\mathrm{rk}_p((Y/Y_{\mathrm{prim}})_{\chi^*}) = 1$, and similarly the condition $M_{\chi^*}\big(\frac{-y}{x}\big) \not\equiv 0 \bmod (p)$ is equivalent to $(x+y\,\zeta)^{e_\chi} \in Y\backslash Y_{\mathrm{prim}}$, giving $\mathrm{rk}_p((Y/Y_{\mathrm{prim}})_\chi) = 1$ (contradiction). $\square$

Corollary 3.10. — *Let $\chi \neq \chi_0$ (i.e., $\chi^* \neq \omega$) be even. Suppose that $\mathcal{C}\!\ell_\chi$ is trivial (Vandiver′s conjecture true at χ).*
If $M_\chi\big(\frac{-y}{x}\big) \not\equiv 0 \bmod (p)$, then $M_{\chi^*}\big(\frac{-y}{x}\big) \equiv 0 \bmod (p)$ and the fundamental χ-unit ε_χ is p-primary as well as the χ-cyclotomic unit $\eta_\chi := (1-\zeta)^{e_\chi}$.

Proof. — From $M_\chi\big(\frac{-y}{x}\big) \not\equiv 0 \bmod (p)$ and Theorem 3.7 we get that ${\mathcal{C}\ell}_{\chi^*}$ is of p-rank ≥ 1, hence equal to 1 since ${\mathcal{C}\ell}_\chi = 1$; so by Kummer duality (see Th. 2.8, (i)), the radical of the corresponding unramified χ^*-extension of K is given by the fundamental χ-unit ε_χ which is thus p-primary. By hypothesis, E_χ is also generated by the χ-cyclotomic unit η_χ. This is the result obtained in [Th2, II] via congruential computations. $\square$

So, Mirimanoff's congruences, obtained by ugly computations, are nothing but the reflection principle in class field theory.

Remark 3.11. — Let χ be even distinct from χ_0.

(i) If $M_\chi\big(\frac{-y}{x}\big) \not\equiv 0 \bmod (p)$, then from the proof of Theorem 3.9 we have $\mathrm{rk}_p((Y/Y_{\mathrm{prim}})_{\chi^*}) = 1$, $\mathrm{rk}_p((Y/Y_{\mathrm{prim}})_\chi) = 0$ (all the χ-pseudo-units are p-primary, especially ε_χ), and for the class group we get $\mathrm{rk}_p({\mathcal{C}\ell}_\chi) + 1 = \mathrm{rk}_p({\mathcal{C}\ell}_{\chi^*})$, which means that the χ^*-class group is nontrivial. Then $(x + y\,\zeta)^{e_\chi}$ is p-primary (which is coherent with $M_{\chi^*}\big(\frac{-y}{x}\big) \equiv 0 \bmod (p)$) but can be a global pth power.

(ii) If $M_{\chi^*}\big(\frac{-y}{x}\big) \not\equiv 0 \bmod (p)$, $\mathrm{rk}_p((Y/Y_{\mathrm{prim}})_\chi) = 1$, $\mathrm{rk}_p((Y/Y_{\mathrm{prim}})_{\chi^*}) = 0$ (all the χ^*-pseudo-units are p-primary), and $\mathrm{rk}_p({\mathcal{C}\ell}_{\chi^*}) = \mathrm{rk}_p({\mathcal{C}\ell}_\chi)$.

(iii) If $M_{\chi^*}\big(\frac{-y}{x}\big) \equiv M_\chi\big(\frac{-y}{x}\big) \equiv 0 \bmod (p)$, then $(x + y\,\zeta)^{e_\chi}$ and $(x + y\,\zeta)^{e_{\chi^*}}$ are p-primary, but we dont know if they are global pth powers or not; if for instance $(x + y\,\zeta)^{e_\chi} = z^p$ then the ideal $\mathfrak{c}_1^{e_\chi}$ is principal. If $(x + y\,\zeta)^{e_\chi}$ is not of the form $\varepsilon_\chi\, z^p$, $\mathfrak{c}_1^{e_\chi}$ is not principal (the χ-class group is nontrivial), and $(x + y\,\zeta)^{e_\chi}$ defines the radical of a χ^*-unramified extension of K (the χ^*-class group is of course nontrivial).
If $(x + y\,\zeta)^{e_{\chi^*}}$ is not a pth power, $\mathfrak{c}_1^{e_{\chi^*}}$ is nonprincipal (because $E_{\chi^*} = 1$) and defines the radical of a χ-unramified extension of K, giving ${\mathcal{C}\ell}_\chi \neq 1$ (Vandiver's conjecture false at χ), hence also ${\mathcal{C}\ell}_{\chi^*} \neq 1$.

(iv) If ${\mathcal{C}\ell}_{\chi^*}$ is trivial, then the unit ε_χ is not p-primary and all the χ^*-pseudo-units are p-primary (hence global pth powers); then we get $M_\chi\big(\frac{-y}{x}\big) \equiv 0 \bmod (p)$.

(v) For $\chi = \chi_0$, we know that ${\mathcal{C}\ell}_{\chi^*} = {\mathcal{C}\ell}_\omega$ is trivial; in this case, $M_{\chi_0}\big(\frac{-y}{x}\big) = \sum_{k=1}^{p-1} \big(\frac{-y}{x}\big)^k$ takes always the value 0 for $\frac{-y}{x} \not\equiv 1 \bmod (p)$.

For $\chi = \chi_0$, ${\mathcal{C}\ell}_\chi$ is trivial and in this case we obtain the supplementary Mirimanoff congruence:

$$M_{\chi^*}\Big(\frac{-y}{x}\Big) = M_\omega\Big(\frac{-y}{x}\Big) = \sum_{k=1}^{p-1} \omega^{-1}(k)\Big(\frac{-y}{x}\Big)^k \equiv 0 \bmod (p)$$

since it corresponds to the p-primarity of $\mathrm{N}_{K/\mathbb{Q}}(x + y\,\zeta) = z_1^p$.

3.2. Derivation technics: the method of Eichler. — We begin with a particular case of this method to analyze a global approach to the computation of the p-rank of the radicals W_a, W_b, W_c, and W.

We consider the necessary condition of the previous subsection, concerning the first case of FLT, to have $\prod_{i=1}^{p-1}(1+e\,(\zeta^i-1))^{\lambda_i} \in K^{\times p}$, for $e := \frac{b}{a+b}$:

$$\sum_{i=1}^{p-1} \frac{\lambda_i\, i\, X^{i-1}}{1+e(X^i-1)} \in (p, X^p-1).$$

The trick is to suppose that the support S of the set of integers λ_i (that is the set of indices i such that $\lambda_i \not\equiv 0 \bmod (p)$) is not too big in the expression:

$$\sum_{i\in S} \lambda_i\, i\, X^{i-1} \prod_{j\in S, j\neq i} (1-e+e\,X^j) \in (p, X^p-1),$$

so that there is no reduction by X^p-1 in the computation of the products:

$$X^{i-1} \prod_{j\in S, j\neq i} (1-e+e\,X^j), \ \text{ for } i \in S.$$

For this, the condition is that $i-1+\sum_{j\in S, j\neq i} j < p$, equivalent to $\sum_{i\in S} i \leq p$. If we suppose that $S \subseteq \{1, 2, \ldots, \rho := [\sqrt{2p}\,-0.5]\}$, the condition is satisfied.

We thus have the congruence:

$$\sum_{i\in S} \lambda_i\, i\, X^{i-1} \prod_{j\in S, j\neq i} (1-e+e\,X^j) \equiv 0 \bmod p\,\mathbb{Z}_{(p)}[X].$$

The (unique) term of minimal degree is obtained for the minimal value i_0 of $i \in S$ and gives $\lambda_{i_0} \,.\, (1-e)^{\rho-1} \equiv 0 \bmod (p)$, then $\lambda_{i_0} \equiv 0 \bmod (p)$ (contradiction). We have obtained:

Theorem 3.12. — *Let (a, b, c) be a solution in the first case of Fermat's equation. Then each of the three radicals $W_a = \langle\, b + c\,\zeta^j\,\rangle.K^{\times p}/K^{\times p}$, $W_b = \langle\, c + a\,\zeta^k\,\rangle.K^{\times p}/K^{\times p}$, $W_c = \langle\, a + b\,\zeta^i\,\rangle.K^{\times p}/K^{\times p}$, $j, k, i = 1, \ldots, p-1$, is of p-rank at least $\rho := [\sqrt{2p}\,-0.5]$. Same conclusion replacing K by $K_{\mathfrak{p}}$ (local radicals).*

But as is always the case, the conclusion of the proof is of a local nature.

Remark 3.13. — (i) The monogenic $\mathbb{F}_p[g]$-module W_c generated by $a + b\,\zeta$ defines a subrepresentation of the regular one; thus there exist at least ρ distinct characters χ such that $(a + b\,\zeta)^{e_\chi}$ is not a global (or local) pth power.

(ii) Let $(x_i, y_i) \in \{(a, b), (b, c), (c, a)\}$, $i = 1, \ldots, \rho$; then by the same method it is easy to prove that the pseudo-units $x_i + y_i\,\zeta^i$ are independent in $K^\times/K^{\times p}$, giving by conjugation many subradicals in W of p-rank ρ.

Now we give a variant of the theorem of Eichler from a solution (a, b, c) in the first case of the Fermat equation. We study the relation, where $e := \frac{b}{a+b}$ (still for the support S of the λ_i):

$$\prod_{i\in S} \Big(\frac{a + b\zeta^{-i}}{a + b\zeta^i}\Big)^{\lambda_i} = \prod_{i\in S} \Big(\frac{(1 + e\,(\zeta^{-i}-1))}{(1 + e\,(\zeta^i-1))}\Big)^{\lambda_i} = \beta^p, \ \ \beta \in \mathbb{Z}_{(p)}[\zeta].$$

Put $(a + b\,\zeta^i)\,\mathbb{Z}[\zeta] = \mathfrak{c}_i^p$ and $(a + b\,\zeta^{-i})\,\mathbb{Z}[\zeta] = \overline{\mathfrak{c}}_i^p$. From the above relation we deduce:

$$\prod_{i\in S} \Big(\frac{\overline{\mathfrak{c}}_i}{\mathfrak{c}_i}\Big)^{\lambda_i} = (\beta)\,\mathbb{Z}_{(p)}[\zeta].$$

Reciprocally, any relation of principality $\prod_{i\in S}\Big(\frac{\overline{\mathfrak{c}}_i}{\mathfrak{c}_i}\Big)^{\lambda_i} = (\beta')\,\mathbb{Z}_{(p)}[\zeta]$ gives:

$$\prod_{i\in S}\Big(\frac{(1+e\,(\zeta^{-i}-1))}{(1+e\,(\zeta^{i}-1))}\Big)^{\lambda_i} = \zeta^h\,\varepsilon^+\,\beta'^p,\ \ \varepsilon^+\in E^+,\ h\geq 0;$$

we suppose that $\sum_{i\in S}\lambda_i\,i\equiv 0 \bmod (p)$; this implies easily $h=0$. Then the relative norm $\mathrm{N}_{K/K^+}(\varepsilon^+\,\beta'^p)$ must be 1, so that $(\varepsilon^+)^2\,\mathrm{N}_{K/K^+}(\beta'^p)=1$ giving $\varepsilon^+=(\eta^+)^p$ for a real unit η^+; this yields the first relation with $\beta=\eta^+\,\beta'$.

Write $(1+e\,(\zeta^{-i}-1))^{\lambda_i}=\zeta^{-\lambda_i\,i}(e+(1-e)\,\zeta^i))^{\lambda_i}$. The first relation is thus equivalent to the relation (reutilizing by abuse the same notations for F, H, B in $\mathbb{Z}_{(p)}[[X]]$):

$$F(X) := \prod_{i\in S}(e+(1-e)X^i)^{\lambda_i}\,(1+e(X^i-1))^{-\lambda_i} = H(X)^p + B(X)(X^p-1),$$

giving by logarithmic derivation, F being invertible modulo (p, X^p-1):

$$(1-e)\sum_{i\in S}\frac{\lambda_i\,i\,X^{i-1}}{e+(1-e)X^i} - e\sum_{i\in S}\frac{\lambda_i\,i\,X^{i-1}}{1+e(X^i-1)}\in (p, X^p-1),$$

and finally:

$$(1-2e)\sum_{i\in S}\frac{\lambda_i\,i\,X^{i-1}}{(e+(1-e)X^i)(1+e(X^i-1))}\in (p, X^p-1).$$

If $2e\equiv 1 \bmod (p)$ we get $a\equiv b \bmod (p)$ and by circular permutations, the analogous congruences would give $a\equiv b\equiv c \bmod (p)$, thus $0\equiv a+b+c\equiv 3a \bmod (p)$ (absurd for $p>3$); so we may suppose that $2e\not\equiv 1 \bmod (p)$.

As before we obtain:

$$\sum_{i\in S}\lambda_i\,i\,X^{i-1}\prod_{j\in S, j\neq i}(e+(1-e)X^j)(1-e+e\,X^j)\in (p, X^p-1).$$

If $2\sum_{j\in S} j\leq p+1$ there is no reduction modulo X^p-1 in the computation of this expression.

Then, for $S\subseteq\{1,\ldots,[\sqrt{p+1}\,-0.5]\}$, the (unique) term of minimal degree is obtained for the minimum i_0 of S, giving immediately $\lambda_{i_0}\equiv 0 \bmod (p)$ (contradiction).

Since the classes $\mathcal{C}\!\ell(\overline{\mathfrak{c}}_i\,.\,{\mathfrak{c}_i}^{-1})$ are relative classes, we have proved (taking in account that we have imposed a relation on the λ_i):

Theorem 3.14 **(Eichler's theorem)**. — *Let $p>2$ be prime. If the p-rank of the relative class group of K satisfies* $\mathrm{rk}_p(\mathcal{C}\ell^-)\leq\rho' := [\sqrt{p+1}\,-1.5]$ *then the first case of FLT holds for the prime p.* (12)

(12) Since $\mathcal{C}\!\ell\big(\frac{\overline{\mathfrak{c}}_i}{\mathfrak{c}_i}\big) = s_i.\mathcal{C}\!\ell\big(\frac{\overline{\mathfrak{c}}_1}{\mathfrak{c}_1}\big)$, $i\in S$, the monogenic g-module generated by $\mathcal{C}\!\ell\big(\frac{\overline{\mathfrak{c}}_1}{\mathfrak{c}_1}\big)$ contains the $\mathcal{C}\!\ell\big(\frac{\overline{\mathfrak{c}}_i}{\mathfrak{c}_i}\big)$ and is contained in the regular representation $\mathbb{F}_p[g]$; this means that at least ρ' different characters χ give a nontrivial $\mathcal{C}\ell_\chi$ and the statement is true with the index of irregularity $i(p)$ instead of $\mathrm{rk}_p(\mathcal{C}\ell^-)$.

3.3. Some other p-adic technics. — Now we consider the Dwork uniformizing parameter ϖ in $K_{\mathfrak{p}}$ which has the following characteristic properties (see e.g. [Gr1, Exer. II.1.8.3]):

(i) $\varpi^{p-1} = -p$,

(ii) $s_k(\varpi) = \omega(k)\varpi$, $k = 1, \dots, p-1$.

In the following lemma we suppose that $1 + e\,(\zeta - 1)$ is a pseudo-unit, so that p-primarity and local pth power property are equivalent (see Lem. 2.1, Th. 2.2). We compute in $\mathbb{Z}_p[\zeta] = \mathbb{Z}_p[\varpi]$.

Lemma 3.15. — *Let $\chi = \omega^m$, $m \in \{1, \dots, p-1\}$; then for $e \not\equiv 0 \bmod (p)$ we have the relation $(1 + e\,(\zeta - 1))^{e_\chi} = 1 + \varpi^m \varphi_\chi$, where $\varphi_\chi \in \mathbb{Z}_p[\varpi]$.*

Then $(1 + e\,(\zeta - 1))^{e_\chi}$ is a local pth power if and only if $\varphi_\chi \equiv 0 \bmod (\varpi)$.

Proof. — Suppose that $(1 + e\,(\zeta - 1))^{e_\chi} = 1 + \varpi^n v$, where v is a unit of $K_{\mathfrak{p}}$ and $n \geq 1$; put $v \equiv v_0 \bmod (\varpi)$, $v_0 \in \mathbb{Z} \backslash p\,\mathbb{Z}$.
Applying e_χ we have:

$$\begin{aligned} & (1 + e\,(\zeta - 1))^{e_\chi} \equiv (1 + \varpi^n v_0)^{e_\chi} \equiv 1 + e_\chi(\varpi^n v_0) \\ \equiv \ & 1 + \tfrac{1}{p-1} \sum_{j=1}^{p-1} \omega^{-m}(j)\, s_j(\varpi^n v_0) \equiv 1 + \tfrac{1}{p-1} \sum_{j=1}^{p-1} \omega^{-m}(j)\, \omega^n(j)\, \varpi^n v_0 \\ \equiv \ & 1 + \tfrac{\varpi^n v_0}{p-1} \sum_{j=1}^{p-1} \omega^{n-m}(j) \equiv 1 + \varpi^n v \mod (\varpi^{n+1}), \end{aligned}$$

which is absurd except if $n \equiv m \bmod (p-1)$. Thus $(1 + e\,(\zeta - 1))^{e_\chi} = 1 + \varpi^m\, \varphi_\chi$.

If $m = p-1$, we know that the norm of such a pseudo-unit is of the form n^p with $n \equiv 1 \bmod (p)$, hence $(1 + e\,(\zeta - 1))^{e_{\chi_0}} \equiv 1 \bmod (p^2)$, proving the lemma in this case; suppose $m < p-1$.

The pth power condition is $\varphi_\chi \equiv 0 \bmod (\varpi^{p-m-1})$ (apply Th. 2.2), with $p - m - 1 > 0$. Suppose that $\varphi_\chi \equiv 0 \bmod (\varpi)$; then we get $(1 + e\,(\zeta - 1))^{e_\chi} = 1 + \varpi^{m+1}\varphi'_\chi$, for $\varphi'_\chi \in \mathbb{Z}_p[\varpi]$. Then applying again the idempotent e_χ, the first part of the proof gives $\varphi'_\chi \equiv 0 \bmod (\varpi)$, then inductively the result up to $(1 + e\,(\zeta - 1))^{e_\chi} \in 1 + (\varpi^{m+p-1})$. □

The value $m = 1$ does not work here since we know that $(1 + e\,(\zeta - 1))^{e_\omega} \equiv 1 + e\,\varpi \mod (\varpi^2)$ (see Rem. 3.4) and since we have supposed $p \nmid e$.

Corollary 3.16. — *Write $\log(1 + e\,(\zeta - 1)) = e_2\,\varpi^2 + \ldots + e_{p-1}\,\varpi^{p-1}$, $e_i \in \mathbb{Z}_p$. Then the set of characters $\chi = \omega^m$, $m \in \{2, \dots, p-1\}$, such that $(1 + e\,(\zeta - 1))^{e_\chi}$ is p-primary, is $\{m \in \{2, \dots, p-1\},\ e_m \equiv 0 \bmod (p)\}$.*

Proof. — Left to the reader. □

We see that the condition depends on a single congruence to 0 modulo ϖ, whose probability may be $\frac{1}{p}$, giving another aspect of the rarity of such a condition for many values of m (at least $\frac{p-1}{2}$ from Mirimanoff's congruences).

3.4. p-adic Gauss sums and Mirimanoff's polynomials. — We use the context of the previous Subsection 3.3, especially the Dwork uniformizing parameter $\varpi \in \mathbb{Q}_p(\zeta)$ such that $\varpi^{p-1} = -p$ and $s_k(\varpi) = \omega(k)\, \varpi$ for $k = 1, \ldots, p-1$.

Let $\chi = \omega^m$, here indexed by $m \in \{0, \ldots, p-2\}$. We note that (additively):

$$e_\chi \,.\, \zeta = \frac{1}{p-1} \sum_{k=1}^{p-1} \chi^{-1}(k) \zeta^k = \frac{-1}{p-1} \tau(\chi^{-1}).$$

Now put:

$$\zeta = \frac{-1}{p-1} \big(u_0 + u_1\, \varpi + \ldots + u_{p-2}\, \varpi^{p-2}\big),$$

where $u_k \in \mathbb{Z}_p$, with $u_0 \equiv 1 \bmod (p)$. We know that $e_\chi \,.\, \varpi^j = 0$ if $j \not\equiv m$ modulo $(p-1)$ and $e_\chi \,.\, \varpi^m = \varpi^m$, so that $e_\chi \,.\, \zeta = \frac{-1}{p-1} u_m\, \varpi^m$ and $\tau(\chi^{-1}) = u_m\, \varpi^m$, for all $m \in \{0, \ldots, p-2\}$.[13] Then, since for $\overline{\tau}(\chi) := \chi(-1)\, \tau(\chi)$, we have $\tau(\chi^{-1})\, \overline{\tau}(\chi) = p$ for $\chi \neq \chi_0$, we obtain for $m \neq 0$:

$$u_m\, \varpi^m\, (-1)^m\, u_{p-1-m}\, \varpi^{p-1-m} = (-1)^m\, u_m\, u_{p-1-m}\, (-p) = p,$$

giving the relation $u_m\, u_{p-1-m} = (-1)^{m+1}$, for $m \neq 0$. For the unit character, $\tau(\chi_0) = 1$ and we find $u_0 = 1$.

We have obtained a classical result:

Proposition 3.17. — *Let $\chi = \omega^m$, $m \in \{0, \ldots, p-2\}$, $\tau(\chi^{-1}) := -\sum_{k=1}^{p-1} \chi^{-1}(k)\, \zeta^k$ the Gauss sum of χ^{-1}; put $\overline{\tau}(\chi) := -\sum_{k=1}^{p-1} \chi(k)\, \zeta^{-k} = \chi(-1)\, \tau(\chi)$.*
Then we have $\tau(\chi^{-1}) = u_m\, \varpi^m$, $\overline{\tau}(\chi) = \chi(-1)\, u_{p-1-m}\, \varpi^{p-1-m}$, which implies the relation $u_m\, u_{p-1-m} = (-1)^{m+1}$, for all $m \in \{1, \ldots, p-2\}$, and $u_0 = 1$.

The modified Mirimanoff polynomial is, for $\chi^* = \omega\chi^{-1}$ (see Rem. 3.6, (ii)):

$$M_{\chi^*}(Z) := \sum_{k=1}^{p-1} (\chi^*)^{-1}(k)\, Z^k,$$

and in the first case of FLT we must compute $M_{\chi^*}(\frac{-x}{y})$ modulo (p) for the usual (x, y) depending of a solution and its permutations.

We suppose now that ω takes its values in the field F of $(p-1)$th roots of unity. We consider the ideal $\mathfrak{p}_0 \,|\, p$ of F such that $\omega(k) \equiv k \bmod \mathfrak{p}_0$ for all k. All the computations take place in the compositum FK in which we denote by $\mathfrak{P}$ the (unique) prime ideal above $\mathfrak{p}_0$.

The condition of p-primarity of $(a + b\,\zeta)^{e_\chi}$, for $\chi = \omega^m$, $m \in \{1, \ldots, p-1\}$, $\chi \neq \omega$ (see Subsec. 3.1) becomes, in FK with $\chi^* = \omega^{1-m}$:

$$M_{\chi^*}\Big(\frac{-b}{a}\Big) \,.\, \tau(\chi^*) \equiv 0 \bmod \mathfrak{P}^{p-1},$$

[13] In these computations, we must write the unit character ω^0 instead of ω^{p-1} because of the expression of ζ since $\varpi^{p-1} = -p$ and $\tau(\omega^0) = 1$.

where $M_{\chi^*}\big(\frac{-b}{a}\big) \in F$ and $\tau(\chi^*) := -\sum_{k=1}^{p-1} \chi^*(k)\zeta^k \in FK$ is of $\mathfrak{P}$-valuation $m-1$, giving $M_{\chi^*}\big(\frac{-b}{a}\big) \equiv 0 \bmod \mathfrak{p}_0$, and where we have:

$$M_{\chi^*}(\zeta) = -\tau((\chi^*)^{-1}).$$

The above properties of Gauss sums lead to the following, where we only suppose that a and b are coprime integers.

Put $(a + b\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{C}_1$, thus $\zeta \equiv \frac{-a}{b} \bmod \mathfrak{C}_1$ seen in FK. This gives:

$$-M_{\chi^*}\Big(\frac{-a}{b}\Big) = -\sum_{k=1}^{p-1} (\chi^*)^{-1}(k)\,\Big(\frac{-a}{b}\Big)^k \equiv \tau((\chi^*)^{-1}) \bmod \mathfrak{C}_1.$$

Thus in the same way (using $\zeta^{-1} \equiv \frac{-b}{a} \bmod \mathfrak{C}_1$):

$$-M_{(\chi^*)^{-1}}\Big(\frac{-b}{a}\Big) \equiv \overline{\tau}(\chi^*) \bmod \mathfrak{C}_1,$$

which yields, in F, for any $\chi \neq \omega$ (i.e., $\chi^* \neq \chi_0$):

$$M_{\chi^*}\Big(\frac{-a}{b}\Big) \,.\, M_{(\chi^*)^{-1}}\Big(\frac{-b}{a}\Big) \equiv \tau((\chi^*)^{-1}) \,.\, \overline{\tau}(\chi^*) \equiv p \bmod \mathfrak{C}_1.$$

Let σ be an element of $\mathrm{Gal}\,(FK/K)$; for any $(p-1)$th root of unity ξ, $\sigma(\xi) = \xi^t$ with a suitable t prime to $p-1$, so that the action of σ on the powers of ω preserves the relation $\varphi \,.\, \varphi^{-1} = \chi_0$ between the characters, and preserves the ideal $\mathfrak{C}_1$ which is in K; thus the expressions $M_{\chi^*}\big(\frac{-a}{b}\big) \,.\, M_{(\chi^*)^{-1}}\big(\frac{-b}{a}\big)$ are conjugated by Galois so that the p-adic study [(14)] of the products $M_{\omega^d}\big(\frac{-a}{b}\big) \,.\, M_{\omega^{-d}}\big(\frac{-b}{a}\big)$, $d \,|\, p-1$, is sufficient.

The congruence modulo $\mathfrak{C}_1$ in FK is now in F, thus it is actually modulo the ideal $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{C}_1)$ seen in F. Since it is the norm of $a + b\,\zeta$, it is the homogeneous form in a, b:

$$\Phi_p(a, b) := a^{p-1} - a^{p-2}b + \ldots - a\,b^{p-2} + b^{p-1}.$$

Put $M_{\chi^*}\big(\frac{-a}{b}\big) \,.\, M_{(\chi^*)^{-1}}\big(\frac{-b}{a}\big) - p = \Phi_p(a, b) \,.\, \frac{\Psi_\chi(a, b)}{a^{p-2}\,b^{p-2}}$, then $\Psi_\chi(a, b)$ is an homogeneous form of degree $p-3$.

We have, for any character φ, $M_\varphi(Z) = \varphi(-1)\,Z^p\,M_\varphi(Z^{-1})$, which gives $M_\varphi(Z)\,M_{\varphi^{-1}}(Z^{-1}) = M_\varphi(Z^{-1})\,M_{\varphi^{-1}}(Z)$, hence proves the symmetry between a and b, and the invariance of $M_{\chi^*}\big(\frac{-a}{b}\big) \,.\, M_{(\chi^*)^{-1}}\big(\frac{-b}{a}\big)$ by complex conjugation in $F/\mathbb{Q}$. So these expressions have coefficients in the maximal real subfield F^+ of F.

To summarize, we have obtained:

Proposition 3.18. — *Let x, y be indeterminates and put $M_\varphi(Z) := \sum_{k=1}^{p-1} \varphi^{-1}(k)\,Z^k$ for any character φ. Then for all $\chi \neq \omega$, we have the relation:*

$$M_{\chi^*}\Big(\frac{-x}{y}\Big) \,.\, M_{(\chi^*)^{-1}}\Big(\frac{-y}{x}\Big) = p + \Phi_p(x, y) \,.\, \frac{\Psi_\chi(x, y)}{x^{p-2}\,y^{p-2}}\,,$$

where $\Psi_\chi(x, y)$ is a symmetrical homogeneous form of degree $p-3$ with coefficients in F^+.

[(14)] More precisely the knowledge of the $\mathfrak{p}'_0$-valuations, for all the prime ideals $\mathfrak{p}'_0$ of F above p.

Now we suppose that (x, y, z) is a solution in the first case of the Fermat equation. Recall that the condition of p-primarity of $(x + y\,\zeta)^{e_\chi}$ which was modulo $\mathfrak{P}^{p-1}$ in FK is now, because of the total ramification in FK/F, modulo the prime ideal $\mathfrak{p}_0$ of F under $\mathfrak{P}$, and is $M_{\chi^*}\big(\frac{-y}{x}\big) \equiv 0 \bmod \mathfrak{p}_0$.

From the above we obtain that:

$$M_{\chi^*}\Big(\frac{-x}{y}\Big) \,.\, M_{(\chi^*)^{-1}}\Big(\frac{-y}{x}\Big) \equiv 0 \bmod \mathfrak{p}_0$$

is equivalent to $\Psi_\chi(x, y) \equiv 0 \bmod \mathfrak{p}_0$.

For instance, for $p = 5$ we have (noting that $F^+ = \mathbb{Q}$ and $\mathfrak{p}_0 = (5)$):

$$\begin{aligned} M_{\omega^{-1}}\Big(\frac{-x}{y}\Big) \,.\, M_{\omega}\Big(\frac{-y}{x}\Big) &= 5 + \Phi_5(x, y) \,.\, \frac{x^2 + x\,y + y^2}{x^3\,y^3}, \\ M_{\omega^2}\Big(\frac{-x}{y}\Big) \,.\, M_{\omega^2}\Big(\frac{-y}{x}\Big) &= 5 - \Phi_5(x, y) \,.\, \frac{x^2 + 3\,x\,y + y^2}{x^3\,y^3}. \end{aligned}$$

Of course these forms Ψ do not represent 0 in $\mathbb{F}_5$.

Remark 3.19. — (i) Notice that these congruences have nothing to do with Mirimanoff′s congruences despite the fact that as soon as one of the factors $M_{\chi^*}\big(\frac{-x}{y}\big)$, $M_{(\chi^*)^{-1}}\big(\frac{-y}{x}\big)$ is congruent to 0 modulo $\mathfrak{p}_0$, this is the case of the expression $\Psi_\chi(x, y)$ and reciprocally.

More precisely, $M_{\chi^*}\big(\frac{-x}{y}\big) \equiv 0 \bmod \mathfrak{p}_0$ is equivalent to $(y+x\,\zeta)^{e_\chi}$ p-primary, hence to $(x+y\,\zeta)^{e_\chi}$ p-primary (since $\chi \neq \omega$), thus to $M_{\chi^*}\big(\frac{-y}{x}\big) \equiv 0 \bmod \mathfrak{p}_0$.

Similarly, $M_{(\chi^*)^{-1}}\big(\frac{-y}{x}\big) \equiv 0 \bmod \mathfrak{p}_0$ is equivalent to the p-primarity of the two pseudo-units $(x + y\,\zeta)^{e_{\widetilde{\chi}}}$ and $(y + x\,\zeta)^{e_{\widetilde{\chi}}}$, then to $M_{(\chi^*)^{-1}}\big(\frac{-x}{y}\big) \equiv 0 \bmod \mathfrak{p}_0$, where $\widetilde{\chi} := \omega^2\,\chi^{-1}$, which may have some interest (see in Subsec. 2.5, (b), the reflection between $R_{2,\chi}$ and $\mathcal{T}_{\omega^2\chi^{-1}}$).

(ii) It would be interesting to perform the same study with the Davenport–Hasse relations between Gauss sums, for two characters:

$$\prod_{\chi,\,\chi^d=\chi_0} \tau(\chi\,.\,\psi) = \psi^{-d}(d)\,.\,\tau(\psi^d)\,.\prod_{\chi,\,\chi^d=\chi_0} \tau(\chi),$$

for any divisor d of $p-1$, and with the Jacobi sums given by the relation:

$$\frac{\tau(\chi)\,\tau(\psi)}{\tau(\chi\,\psi)} = -\sum_{k=1}^{p-1} \chi(k)\,\psi(1-k).$$

3.5. Mirimanoff′s sums. — We still consider the context of the previous Subsection 3.4, for which ω takes its values in the field F of $(p-1)$th roots of unity. We fix the prime ideal $\mathfrak{p}_0$ of F above p in the following way: fix a primitive $(p-1)$th root of unity $\xi_0 \in F$ and a primitive $(p-1)$th root $r_0 \in \mathbb{Z}$ modulo p; then we decrete that $\xi_0 \equiv r_0 \bmod \mathfrak{p}_0$.

Since for any character φ of $g := \mathrm{Gal}\,(K/\mathbb{Q})$, $M_\varphi(Z) = \sum_{k=1}^{p-1} \varphi^{-1}(k)\,Z^k$, if we put, for a solution (x, y, z) in the first case of Fermat′s equation:

$$\frac{-y}{x} \equiv r_0^t \equiv \xi_0^t =: \xi \bmod \mathfrak{p}_0,$$

we have in F the congruence:

$$M_\varphi\Big(\frac{-y}{x}\Big) \equiv M_\varphi(\xi) \bmod \mathfrak{p}_0;$$

hence the congruences $M_\varphi\big(\frac{-y}{x}\big) \equiv 0 \bmod (p)$ in $\mathbb{Q}_p$ and $M_\varphi(\xi) \equiv 0 \bmod \mathfrak{p}_0$ in F are equivalent.
We propose to call the sums of roots of unity:

$$\mu_\varphi(\xi) := \sum_{k=1}^{p-1} \varphi^{-1}(k)\, \xi^k \ \in\ F,$$

the Mirimanoff sums attached to the character φ and the $(p-1)$th root of unity ξ.
It is clear that the algebraic numbers:

$$\mu_\varphi(\xi)\,.\,\mu_{\varphi^*}(\xi),\ \ \varphi \neq \chi_0, \omega \ \text{ and }\ \mu_\varphi(\xi)\,.\,\mu_{\varphi^{-1}}(\xi^{-1}),\ \ \varphi \neq \chi_0,$$

give the easy way to study the congruences of Mirimanoff and the congruences given in Proposition 3.18.
Unfortunately, the root ξ is uneffective and the properties of the sums $\mu_\varphi(\xi)$ depend largely of the order of ξ (i.e., the order of $\frac{-x}{y}$ modulo p); hence we must envisage all the possibilities.

Warning: in the factor $\varphi^{-1}(k)$, k is considered modulo p, but in the factor ξ^k, k is considered modulo $p-1$, under the condition that $k \in \{1, \ldots, p-1\}$.
In a more numerical setting, put $\varphi = \omega^h$ and $\xi = \xi_0^t$; then, writing $k \equiv r_0^j \bmod (p)$, we get:

$$\begin{aligned}\mu_\varphi(\xi) =: \mu_h(t) \ &= \ \sum_{k=1}^{p-1} \omega^{-h}(k)\, \xi_0^{\,t\,k} = \sum_{j=1}^{p-1} \xi_0^{-h\,j}\, \xi_0^{\,t\,[r_0^j]_p} \\ &= \ \sum_{j=1}^{p-1} \xi_0^{-h\,j\,+\,t\,[r_0^j]_p},\ \ h,\, t \in \{1, \ldots, p-1\},\end{aligned}$$

where $[r_0^j]_p$ is the unique residue modulo p of r_0^j in the set $\{1, \ldots, p-1\}$.
Then let Φ_{p-1} be the $(p-1)$th cyclotomic polynomial, of degree $\nu := \phi(p-1)$; after reduction modulo Φ_{p-1}, we obtain: $\mu_h(t) = q_0 + q_1\xi_0 + \ldots + q_{\nu-1}\xi_0^{\nu-1}$, $q_i \in \mathbb{Z}$, which can be studied modulo $\mathfrak{p}_0$ in an easy way.

Naturally, these sums are completely analogous to Mirimanoff's polynomials specialized at suitable classes modulo p, but we hope that the formulation in terms of sums of roots of unity is likely of a better understanding.

3.6. Wieferich's criterion: a local consequence of the reciprocity law. — As indicated in Ribenboim's book, the Wieferich criterion may be deduced from the law of reciprocity (this has been done first by Furtwängler from Eisenstein's reciprocity law [R, IX.3]). For this purpose, an explicit formula of Hasse may also be used [R, IX.5].

Here we propose a more basic proof using the $\mathfrak{p}$-conductor of a Kummer extension in the following way, where $\big(\frac{\bullet}{\bullet}\big)_p$ is the pth power residue symbol, with values in $\langle\, \zeta\, \rangle$.

***Theorem 3.20* (Wieferich′s criterion).** — *Let ℓ be a prime number, $\ell \neq p$, and suppose that $x + y\,\zeta$ is a pseudo-unit (i.e., $(x + y\,\zeta)$ is the pth power of an ideal of K prime to $\mathfrak{p}$).*
(i) Then $\Big(\dfrac{\zeta^x\, y + \zeta^{-y}\, x}{\ell}\Big)_p = 1$.
(ii) If $\ell \,|\, y$ with $p \nmid y$ and if (x, y, z) is a solution of Fermat′s equation(15)*, then* $\ell^{\,p-1} \equiv 1 \bmod (p^2)$.

Proof. — The expression of $\alpha := \zeta^x\, y + \zeta^{-y}\, x$ is such that α is still a pseudo-unit, and $\alpha \equiv x + y \equiv (x + y)^p \bmod (1 - \zeta)^2$.
The general law of reciprocity (see e.g. [Gr1, Th. II.7.4.4]) yields to:

$$\Big(\frac{\alpha}{\ell}\Big)_p \Big(\frac{\ell}{\alpha}\Big)_p^{-1} = (\ell, \alpha)_{\mathfrak{p}}$$

where $(\bullet, \bullet)_{\mathfrak{p}}$ is the Hilbert′s symbol at the place $\mathfrak{p}$. This symbol is equal to 1 if and only if ℓ is a local norm in the Kummer extension $K_{\mathfrak{p}}(\sqrt[p]{\alpha}\,)/K_{\mathfrak{p}}$; the conductor of this extension divides $\mathfrak{p}^{p-1}$ since α is congruent to a pth power modulo $\mathfrak{p}^2$ (see the general conductor formula in [Gr1, Prop. II.1.6.3]). Since $\ell^{\,p-1} \equiv 1 \bmod (p)$ the normic condition is satisfied for ℓ.

But the symbol $\big(\frac{\ell}{\alpha}\big)_p^{-1}$ is tivial since (α) is the pth power of an ideal; thus:

$$\Big(\frac{\zeta^x\, y + \zeta^{-y}\, x}{\ell}\Big)_p = 1.$$

If $\ell \,|\, y$, we have $\zeta^x\, y + \zeta^{-y}\, x \equiv \zeta^{-y}\, x \mod (\ell)$ and $1 = \big(\frac{\zeta^{-y}\, x}{\ell}\big)_p = \big(\frac{\zeta}{\ell}\big)_p^{-y} \big(\frac{x}{\ell}\big)_p$; but $x = z_0^p - y \equiv z_0^p \bmod (\ell)$ giving $\big(\frac{x}{\ell}\big)_p = 1$ and $\big(\frac{\zeta}{\ell}\big)_p = 1$ since $p \nmid y$.
If $(\ell) = \mathfrak{l}_1 \ldots \mathfrak{l}_d$ in K, then $\prod_{i=1}^{d} \big(\frac{\zeta}{\mathfrak{l}_i}\big) = 1$, but we have $\big(\frac{\zeta}{\mathfrak{l}_1}\big)^k = s_k \big(\frac{\zeta}{\mathfrak{l}_1}\big) = \big(\frac{\zeta^k}{\mathfrak{l}_k}\big) = \big(\frac{\zeta}{\mathfrak{l}_k}\big)^k$, so that $\big(\frac{\zeta}{\mathfrak{l}_k}\big)$ does not depend on k, giving $\big(\frac{\zeta}{\mathfrak{l}_1}\big) = 1$; thus the multiplicative group of the residue field of $\mathfrak{l}_1$ contains an element of order p^2, proving the point (ii) of the theorem. □

Then the discovery of Wieferich′s criteria consists in proving that small prime numbers ℓ (e.g. $\ell = 2$) divide $a\,b\,c$ (see [GM], [Th2], for a study of Fermat′s quotients in relation with FLT); in the second case, the hypothesis $\ell \,|\, y$, $p \nmid y$ may be inaccurate, so the Wieferich criterion is uneffective in the second case.

It is clear that the prime numbers $\ell \equiv 1 \bmod (p)$, such that Fermat′s equation $u^p + v^p + 1 = 0$ has no nontrivial solutions in the finite field $\mathbb{F}_\ell$, are divisors of $a\,b\,c$ (where (a, b, c) is a global solution in any case of Fermat′s equation); then experimental computations show that many such primes do exist. One may conjecture that their number tends to infinity with p, which gives many uneffective Wieferich′s criteria.

In this direction we have the following interesting approach.

(15) So that $x + y = z_0^p$ as usual; the second case of FLT being equivalent here to $p \,|\, x$.

3.7. Wendt's criterion: a non modulo p local–global result. — Let ℓ be a prime number of the form $1 + n\,p$, $n \geq 2$, and let $\mathfrak{l}$ be an ideal above ℓ in K. We consider the algebraic number $\theta_n := \prod_{i,\,j=1}^{n}(\xi_i + \xi_j + 1)$, where the ξ_k, $k = 1, \ldots, n$, are the nth roots of unity.

We have $\theta_n \in \mathbb{Z}\backslash\{0\}$; this number has been used for instance in the following papers : [LS] (for a similar purpose as us) and [A-HB], [F] to prove that the first case of FLT holds for infinitely many primes p.

See [R, IV.4] for its explicit computation via Wendt's determinant. If $\ell \nmid \theta_n$ this means that Fermat's equation in the residue field $\mathbb{F}_\ell$ of $\mathfrak{l}$ has no nontrivial solutions; thus if a, b, c is a solution in $\mathbb{Z}$ of Fermat's equation, necessarily ℓ divides one of these numbers, say $\ell \,|\, c$.

Now we state the following result (in the spirit of Germain's theorem).

Theorem 3.21 **(Wendt's criterion).** — *Let $\ell = 1 + n\,p$ be a prime number which does not divide the natural integer θ_n. Moreover, we suppose that p is not a pth power modulo ℓ.*

Then the first case of FLT holds for p.

Proof. — Suppose that $\ell \,|\, c$ for a solution in the first case of Fermat's equation. We have $a + b = c_0^p$, $\mathrm{N}_{K/\mathbb{Q}}(a + b\,\zeta) = c_1^p$ with $-c = c_0\, c_1$ (see Rem. 1.4, (i)).
If $\ell \,|\, c_0$ then $b \equiv -a \bmod (\ell)$, giving:

$$c_1^p = \mathrm{N}_{K/\mathbb{Q}}(a + b\,\zeta) \equiv a^{p-1} \prod_{i=1}^{p-1}(1 - \zeta^i) = a^{p-1}\, p \mod (\ell)$$

(a contradiction since $a + c \equiv a \equiv b_0^p \bmod (\ell)$, giving that p is a local pth power at ℓ).

So $\ell \,|\, c_1$; from Lemma 1.2, $\ell \nmid c_0$ giving, from $a + b = c_0^p$, $a + c = b_0^p$, and $b + c = a_0^p$, the relation $0 = a + b - c_0^p \equiv b_0^p + a_0^p + (-c_0)^p \bmod (\ell)$ which defines a non trivial solution in $\mathbb{F}_\ell$ (absurd).

The conclusion of the theorem is the same if we replace the hypothesis "p is not a pth power modulo ℓ", by "$p \nmid n$" since in that case, Wieferich's criterion is not satisfied for ℓ. □

Appendix. Wieferich's criterion without reciprocity law (from a proof rediscovered by Roland Quême). [16]

We use the same notations as in Subsection 3.6. See also Notations 2.7.
Let $\ell \neq p$ be a prime number. We suppose that by choosing suitable x, y among a, b, c, we have $\ell \,|\, y$ and $p \nmid x + y$ in the writing $(x + y\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{z}_1^p$ (valid in any case of Fermat's equation). Consider $e_\omega \in \mathbb{Z}[g]$ modulo p.

We know that $\mathcal{C}\!\ell(\mathfrak{z}_1)^{e_\omega} = 1$ (another application of the reflection theorem; see [Gr1, II.5.4.6.3]), so that $(x + y\,\zeta)^{e_\omega} = \varepsilon_\omega\, \delta_\omega^p$, $\varepsilon_\omega \in E_\omega = \langle \zeta \rangle$, $\delta_\omega \in K^\times$; hence $\varepsilon_\omega = \zeta^h$ for $h \geq 0$.
Thus this yields:

$$(x + y\,\zeta)^{e_\omega} \in \zeta^h \,.\, K^{\times p},$$

[16] Adress: Roland Quême, 13 Avenue du château d'eau, 31490 Brax, Url: http://roland.queme.free.fr/, email: roland.queme@wanadoo.fr

hence the relation $\big(\frac{(x+y\,\zeta)^{e_\omega}}{\ell}\big)_p = \big(\frac{\zeta}{\ell}\big)_p^h$ where $(x+y\,\zeta)^{e_\omega} \equiv x^{e_\omega}$ (a pth power) modulo ℓ, proving that:

$$\Big(\frac{\zeta}{\ell}\Big)_p^h = 1.$$

But $(x+y\,\zeta)^{e_\omega} \in \zeta^h \,.\, K^{\times p}$ is equivalent to $(1+\frac{y}{x+y}(\zeta-1))^{e_\omega} \in \zeta^h \,.\, K^{\times p}$; using Remark 3.4 $(\,(1+\frac{y}{x+y}(\zeta-1))^{e_\omega} \equiv 1+\frac{y}{x+y}(\zeta-1) \bmod \mathfrak{p}^2)$ we get immediately $h \equiv \frac{y}{x+y} \bmod (p)$.

If moreover $y \not\equiv 0 \bmod (p)$ (e.g. first case of FLT, or second case with $x \equiv 0 \mod (p)$) we obtain the result on Wieferich′s criterion in the same way as in Subsection 3.6, without any use of the reciprocity law.

4. Conclusion

We have shown that much of the classical literature on FLT has been concerned with very basic facts of class field theory, often rediscovered by means of painful congruential computations; but recall that class field theory is essentially algebraic as soon as, for instance, Čebotarev′s density theorem is not used (among other analytic tools), and that, algebrically, all is " possible ". So it appears that this approach is relatively poor, despite the power of class field theory to enunciate technical properties.

Moreover, most of the arguments are local, especially *local at p*.[(17)]

The fact that the relative class group takes place in these studies does not change our point of view since it is utilized without serious analytic arguments (except the unusable upperbound $\log(h^-) < \frac{p}{4}\log(p)$ and the ingenious but elementary derivation technic of Eichler). Moreover the analytic class number formula for the relative class group is not really analytic since it is, roughly speaking, equivalent to Stickelberger′s theorem and is, in some sense, algebraic (the main theorem on cyclotomic fields gives a better knowledge of the class field theory aspects, but it is not really necessary).

It is likely that the most serious *cyclotomic* approaches are the study of " Mirimanoff′s sums ", since at least half of them must be zero modulo $\mathfrak{p}_0$, and that of Wendt′s criterion since it is connected with the theory of prime numbers; but all this only concerns the first case of FLT, which is unnatural.

Still in the first case, from the well-known class field theory exact sequence of $\mathbb{Z}_p$-modules:

$$1 \longrightarrow U/\overline{E} \longrightarrow \mathrm{Gal}(H_{Pl_p}/K) \longrightarrow \mathcal{C}\ell \longrightarrow 1,$$

where H_{Pl_p} is the maximal abelian p-ramified pro-p-extension of K, U the group of principal units of $K_\mathfrak{p}$, $\overline{E}$ the closure in U of the group of global units $\varepsilon \equiv 1 \bmod \mathfrak{p}$, we get for any *even* character $\chi \neq \chi_0$:

$$1 \longrightarrow U_\chi/\overline{E}_\chi \longrightarrow \mathcal{T}_\chi \longrightarrow \mathcal{C}\ell_\chi \longrightarrow 1,$$

(17) Recall that a pseudo-unit α of K is in $K^{\times p}$ if and only if $\alpha \in K_\mathfrak{q}^{\times p}$ for all $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{l}_1, \dots \mathfrak{l}_r\}$, where the prime ideals $\mathfrak{l}_1, \dots \mathfrak{l}_r$ generate the p-class group of K (see [Gr1, Exer. II.6.3.8]); but this criterion is not effective.

where all groups are p-torsion groups since $\chi \neq \chi_0$ is even. For p large enough, the result of Kurihara–Soulé is $\mathcal{C}\ell_{\omega^{p-3}} = 1$; suppose that it is possible to extend it to $\mathcal{T}_{\omega^{p-3}} = 1$ (taking "p-ramification" instead of "nonramification"), then $\overline{E}_{\omega^{p-3}} = U_{\omega^{p-3}}$ which means that the fundamental ω^{p-3}-unit $\varepsilon_{\omega^{p-3}}$ is not a local pth power and that the fundamental ω^{p-3}-cyclotomic unit $\eta_{\omega^{p-3}}$ (equal to $\varepsilon_{\omega^{p-3}}$ since $\mathcal{C}\ell_{\omega^{p-3}} = 1$) is not a local pth power, which is equivalent to $b_{\chi^*} = b_{\omega^3} \not\equiv 0 \bmod (p)$, in other words to $B_{p-3} \not\equiv 0 \bmod (p)$, which would contradict the first case of FLT (at least for p large enough).

We believe more in the possibility of a *nonalgebraic* study of the radical generated by ζ, $1-\zeta$, $a+b\,\zeta$, $b+c\,\zeta$, $c+a\,\zeta$ and their conjugates, which would be independent of the considered case of FLT, and which is not equivalent to a general study of the group ${}_p\mathcal{C}\ell$ because as a matter of fact we are concerned with very specific p-classes, the same remark being valid for the utilization of other arithmetical invariants of K. As the Referee mentions, all these invariants are isomorphic or dual to adequate Tate twists of the cohomology group $\mathrm{H}^2(\mathcal{G}, \mathbb{Z}/p\mathbb{Z})$ (where $\mathcal{G}$ is the Galois group of the maximal p-ramified pro-p-extension of K) which relativizes the interest, but we don't know if the use of the pseudo-units $x + y\,\zeta$ in these contexts leads, in practice, to the same "numerical" criteria and to the same diophantine approach.

It is indeed surprising that, to our knowledge, there is no important diophantine results on the mixed radical W, using simultaneously a, b, c, and possibly the cyclotomic numbers, which constitutes a particular case of the study of the polynomial identity, in the polynomial ring $\mathbb{Z}[X]$:

$$\prod_{i=1}^{n} (u_i + v_i\, X^{d_i})^{\lambda_i} = H(X)^p + B(X)\,(X^p - 1), \quad 0 \leq d_i,\, \lambda_i \leq p-1.$$

References

[A1] B. Anglès, On some p-adic power series attached to the arithmetic of $\mathbb{Q}(\zeta_p)$, J. Number Theory 122 (2007), 1, 221–246.

[A2] B. Anglès, Norm residue symbol and the first case of Fermat's equation, J. Number Theory 91,2 (2001), 297–311.

[A3] B. Anglès, Units and norm residue symbol, Acta Arith. 98, 1 (2001), 33–51.

[A-HB] L.M. Adleman and D.R. Heath-Brown, The first case of Fermat's last theorem, Invent. Math. 79 (1985), 409–416.

[AN] J. Assim and T. Nguyen Quang Do, On the Kummer–Leopoldt constant of a number field, Manuscripta Math. 115, 1 (2004), 55–72.

[Br1] H. Brückner, Zum ersten Fall der Fermatschen Vermutung, J. Reine Angew. Math. 274/275 (1975), 21–26.

[Br2] H. Brückner, Zum Beweis des ersten Falles der Fermatschen Vermutung für pseudoreguläre Primzahlen ℓ (Bemerkungen zur vorstehenden Arbeit von L. Skula.), J. Reine Angew. Math. 253 (1972), 15–18.

[E1] M. Eichler, Zum 1. Fall der Fermatschen Vermutung. Eine Bemerkung zu zwei Arbeiten von L. Skula und H. Brückner, J. Reine Angew. Math. 260 (1973), 214.

[E2] M. Eichler, Eine Bemerkung zur Fermatschen Vermutung, Acta Arith. 11 (1965), 129–131; Errata. Ibid. ohne Seitenzahl, p. 261.

[F] E. Fouvry, Théorème de Brun-Titchmarsh; application au théorème de Fermat, Invent. Math. 79 (1985), 383–407.

[G1] A. Granville, The Kummer–Wieferich–Skula approach to the first case of Fermat′s Last Theorem, Gouvêa, Fernando (ed.) et al., Advances in number theory, The proceedings of the third conference of the Canadian Number Theory Association, Oxford: Clarendon Press 1993, 479–497.

[G2] A. Granville, On Krasner′s criteria for the first case of Fermat′s last theorem, Manuscr. Math. 56 (1986), 67–70.

[G3] A. Granville, On the size of the first factor of the class number of a cyclotomic field, Invent. Math. 100 (1990), 321–338.

[GM] 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. Am. Math. Soc. 306, 1 (1988), 329–359.

[Gr1] G. Gras, Class Field Theory: from theory to practice, SMM second corrected printing 2005.

[Gr2] G. Gras, Théorèmes de réflexion, J. Théorie des Nombres de Bordeaux 10, 2 (1998), 399–499.

[GJ] G. Gras et J-F. Jaulent, Sur les corps de nombres réguliers, Math. Z. 202 (1989), 343–365.

[Gre] C. Greither, Class groups of abelian fields, and the main conjecture, Ann. Inst. Fourier 42, 3 (1992), 449–499.

[Hel] Y. Hellegouarch, Invitation aux mathématiques de Fermat–Wiles, Masson, Paris 1997.

[He1] C. Helou, Norm residue symbol and cyclotomic units, Acta Arith. 73 (1995), 147–188.

[He2] C. Helou, Proof of a conjecture of Terjanian for regular primes, C. R. Math. Rep. Acad. Sci. Canada 18 (1996), 5, 193–198.

[Iw] K. Iwasawa, A note on Jacobi sums, Symposia Mathematica 15, Academic Press (1975), 447–459.

[J] J-F. Jaulent, Sur le noyau sauvage des corps de nombres, Acta Arith. 67 (1994), 335–348.

[JN] J-F. Jaulent et T. Nguyen Quang Do, Corps p-rationnels, corps p-réguliers et ramification restreinte, J. Théorie des Nombres de Bordeaux 5 (1993), 343–365.

[Kr] M. Krasner, Sur le premier cas du théorème de Fermat, C. R. Acad. Sci., Paris 199 (1934), 256–258.

[Ku] M. Kurihara, Some remarks on conjectures about cyclotomic fields and K-groups of $\mathbb{Z}$, Compos. Math. 81, 2 (1992), 223–236.

[LS] H.W. Lenstra jun. and P. Stevenhagen, Class field theory and the first case of Fermat′s last theorem, Cornell, Gary (ed.) et al., Modular forms and Fermat′s last theorem. Papers from a conference, Boston 1995, New York, Springer (1997), 499–503.

[MN] A. Movahhedi et T. Nguyen Quang Do, Sur l'arithmétique des corps de nombres p-rationnels, Sém. Th. Nombres Paris (1987/1988), Prog. in Math. 89 (1990), 155–200.

[R] P. Ribenboim, 13 Lectures on Fermat′s Last Theorem, Springer, New York 1979.

[Ri] K. Ribet, A modular construction of unramified p-extensions of $\mathbb{Q}_p$, Invent. Math. 34 (1976), 151–162.

[Sk1] L. Skula, Some historical aspects of the Fermat problem, Pokroky Mat. Fyz. Astron. 39, 6 (1994), 318–330.

[Sk2] L. Skula, Eine Bemerkung zu dem ersten Fall der Fermatschen Vermutung, J. Reine Angew. Math. 253 (1972), 1–14.

[S] C. Soulé, Perfect forms and the Vandiver conjecture, J. Reine Angew. Math. 517 (1999), 209–221.

[Ta] J. Tate, Relations between K_2 and Galois cohomology, Invent. Math. 36 (1976), 257–274.

[Te] G. Terjanian, Sur la loi de réciprocité des puissances ℓ-èmes, Acta Arith. 54, 2 (1989), 8-125.

[Th1] F. Thaine, On Fermat′s last theorem and the arithmetic of $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$, J. Number Theory 29, 3 (1988), 297–299.

[Th2] F. Thaine, On the first case of Fermat′s last theorem, J. Number Theory 20 (1985), 128–142.

[Th3] F. Thaine, Polynomials generalizing binomial coefficients and their application to the study of Fermat′s last theorem, J. Number Theory 15 (1982), 304–317.

[Th4] F. Thaine, On the ideal class groups of real abelian number fields, Ann. Math. (2) 128, 1 (1988), 1–18.

[Wa] L.C. Washington, Introduction to cyclotomic fields, Graduate Texts in Math. 83, Springer-Verlag 1982, enlarged second edition 1997.

March 14, 2010

Georges Gras, Villa la Gardette, chemin Château Gagnière, F-38520 Le Bourg d'Oisans
E-mail : g.mn.gras@wanadoo.fr • *Url :* http://monsite.orange.fr/maths.g.mn.gras/