Test of Vandiver's conjecture with Gauss sums – Heuristics

Georges Gras

TEST OF VANDIVER'S CONJECTURE WITH GAUSS SUMS – HEURISTICS

GEORGES GRAS

Abstract. The link between Vandiver's conjecture and Gauss sums is well-known since the papers of Iwasawa (1975) and Anglès–Nuccio (2010); this context has been considered by many authors with various purposes (Iwasawa theory, Galois cohomology, Fermat curves,...). We give again the interpretation of Vandiver's conjecture in terms of the minus part of the torsion group of the Galois group of the maximal abelian p-ramified pro-p-extension of the pth cyclotomic field, that we had published at the Laval University (1984). Then we provide a specific use of Gauss sums allowing a numerical test of Vandiver's conjecture (cf. Theorem 4.5 using both the set of exponents of p-irregularity and the sets of exponents of p-primarity of a suitable twist of Gauss sums giving Jacobi sums of characters of order p). Then we propose new heuristics for its rightness. We show that a counterexample to Vandiver's conjecture leads to a strange phenomenon on the congruential properties modulo p of Gauss sums and to an unusual complexity of algorithms. All the techniques used are basic and classic. Many tables are given to strength our arguments; the corresponding PARI programs may be copy and past by the reader.

Contents

Date: August 28, 2018.

1991 *Mathematics Subject Classification.* 11R37, 11R29, 11R18, 11T24.

Key words and phrases. Vandiver's conjecture; Gauss sums; Jacobi sums; Stickelberger's elements; class field theory; p-ramification.

1. Introduction

Let $K = \mathbb{Q}(\mu_p)$ be the field of pth roots of unity for a given prime $p > 2$ and let K_+ be its maximal real subfield. We denote by $\mathcal{C}\ell$ and $\mathcal{C}\ell_+$ the p-class groups of K and K_+, respectively, then by $\mathcal{C}\ell_-$ the relative p-class group. Let E and E_+ be the groups of units of K and K_+; we know that $E = E_+ \oplus \mu_p$.

The Vandiver (or Kummer–Vandiver) conjecture asserts that $\mathcal{C}\ell_+$ is trivial. This statement is equivalent to say that the group of real cyclotomic units is of prime to p index in E_+ [24, Theorem 8.14]. See numerical results using this property in [3, 6].

Many heuristics are known about this conjecture; see Washington's book [24, § 8.3, Corollary 8.19] for some history and criteria, then for probabilistic arguments. We have also given a probabilistic study in [10, II.5.4.9.2]. All these heuristics lead to the fact that the number of primes p less than p_0, giving a counterexample, can be of the form $c \cdot \log(\log(p_0))$, $c < 1$. These reasonings, giving the possible existence of infinitely many counterexamples to Vandiver's conjecture, are based on standard probabilities associated with the Borel–Cantelli heuristic, but many recent p-adic conjectures (on class groups and units) may contradict such approaches.

In this paper, we shall give numerical experiments in another direction using Gauss sums and Stickelberger annihilation of relative classes, together with a weaker form of the main theorem on abelian fields. Such a link of Vandiver's conjecture with Gauss sums and Galois p-ramification has been given first by Iwasawa [18] and applied by many authors in various directions (e.g., [1, 5, 13, 16, 17, 21]); we shall give a short survey about this in Section 3.

More precisely, we shall use the reflection principle to interprete a counterexample to Vandiver's conjecture in terms of non-trivial "p-primary relative pseudo-units" stemming from Gauss sums of the form $\sum_{x\in\mathbb{F}_\ell^\times} \psi(x)\,\xi_\ell^x$, for $\psi^p = 1$, ξ_ℓ of order $\ell \equiv 1 \pmod p$; this shall give the main test verifying the validity of the conjecture for a given p (Theorem 4.5 and Corollaries). Indeed, if $\#\mathcal{C}\ell_+ \equiv 0 \pmod p$, there exists a class $\gamma = c\ell(\mathfrak{A}) \in \mathcal{C}\ell_-$, of order p, such that $\mathfrak{A}^p = (\alpha)$, with α p-primary (to give the unramified extension $K(\sqrt[p]{\alpha})/K$, decomposed over K_+ into the cyclic unramified extension L_+/K_+ predicted by class field theory); since α can be obtained explicitely by means of twists of the above Gauss sums, giving products of Jacobi sums, we show that some assumption of *independence*, of the congruential properties (mod p) of these Jacobi sums, is an obstruction to any counterexample to Vandiver's conjecture or, at least, that the probability of such a counterexample is at most $\frac{O(1)}{p^2}$.

This method is different from those needing to prove that some cyclotomic units are not global pth powers, which does not give obvious probabilistic approaches.

Finally, we propose new heuristics (to our knowledge) and give substantial numerical experiments which confirm them. All the PARI [20] programs can be copy and paste by the reader for any further experience.

Definitions & Notations 1.1. Let $K := \mathbb{Q}(\mu_p)$ and $G = \mathrm{Gal}\,(K/\mathbb{Q})$.

(i) Let ζ_p be a primitive pth root of unity. We denote by ω the character of Teichmüller of G (i.e., the p-adic character with values in $\mu_{p-1}(\mathbb{Q}_p)$ such that $\zeta_p^s = \zeta_p^{\omega(s)}$ for all $s \in G$).

(ii) An irreducible p-adic character of G is of the form $\theta = \omega^k$, $1 \le k \le p-1$; we denote by 1 the unit character. We denote by $\mathscr{X}_+$ the set of even characters $\chi \ne 1$ (i.e., $\chi = \omega^n$, $n \in [2, p-3]$ even).

(iii) If $\theta = \omega^m$, we put $\theta^* := \omega\theta^{-1} = \omega^{p-m}$. This defines an involution on the group of characters which applies $\mathscr{X}_+$ onto the set $\mathscr{X}_-$ of odd characters distinct from ω.

(iv) For any character θ, we denote by $e_\theta := \frac{1}{p-1}\sum_{s\in G} \theta(s^{-1})\,s$ the associated idempotent in $\mathbb{Z}_p[G]$. Thus $s \cdot e_\theta = \theta(s)\cdot e_\theta$ for all $s \in G$.

(v) For a finite $\mathbb{Z}_p[G]$-module M, we put $M_\theta := M^{e_\theta}$. The operation of the complex conjugation $s_{-1} \in G$ gives rise to the obvious definition of the components M_+ and M_- such that $M = M_+ \oplus M_-$.

(vi) We denote by $\mathrm{rk}_p(A)$ the p-rank of any abelian group A (i.e., the $\mathbb{F}_p$-dimension of A/A^p).

(vii) Let F be a subgroup of $K^\times$; for $\alpha \in F$, considered modulo $K^{\times p}$, we denote, by abuse, by α_θ a representative of $\alpha^{e_\theta} \in F_\theta := (FK^{\times p}/K^{\times p})_\theta$.

(viii) For $\chi =: \omega^n \in \mathscr{X}_+$, denote by $b(\chi^*) = \frac{1}{p}\sum_{a=1}^{p-1}(\chi^*)^{-1}(s_a)\,a$ (where $s_a \in G$ is the Artin automorphism of a) the generalized Bernoulli number $B_{1,(\chi^*)^{-1}} = B_{1,\omega^{n-1}}$; it is an element of $\mathbb{Z}_p$ congruent modulo p to $\frac{B_n}{n}$, where B_n is the ordinary Bernoulli number of even index $n \in [2, p-3]$ (see [24, Proposition 4.1, Corollary 5.15]).

(ix) The index of p-irregularity $i(p)$ is the number of even $n \in [2, p-3]$ such that $B_n \equiv 0 \pmod p$; see [24, § 5.3 & Exercise 6.6] giving statistics and the heuristic $i(p) = O\big(\frac{\log(p)}{\log(\log(p))}\big)$.

Hypothesis 1.2. *To simplify and to be realistic in an heuristic point of view, we assume that each $\mathcal{C}\ell_{\chi^*}$ is trivial or cyclic of order p, for all $\chi \in \mathscr{X}_+$; in other words, we assume that $\mathcal{C}\ell_- \simeq (\mathbb{Z}/p\mathbb{Z})^{i(p)}$.*

Indeed, we know that $\#\mathcal{C}\ell_{\chi^*} \equiv 0 \pmod{p^2}$ has probability less than $\frac{O(1)}{p^2}$, especially for the case $\mathrm{rk}_p(\mathcal{C}\ell_{\chi^*}) \geq 2$, which may be considered as giving a finite number of counterexamples to Vandiver's conjecture, what can be discarded for our purpose, the general case giving only technical complications. The main theorem on abelian fields gives, under our assumption, $b(\chi^*) \sim p$ for each non-trivial component $\mathcal{C}\ell_{\chi^*}$, where $\sim$ means "equality up to a p-adic unit factor", but leads, in fact, to the classical Herbrand theorem "$p \mid \mathcal{C}\ell_{\chi^*}$ implies $p \mid b(\chi^*)$" (the numerical results [3, 6] are in complete accordance with this viewpoint).

2. Pseudo-units – Notion of p-primarity

Definitions 2.1. (i) We call *pseudo–unit* any $\alpha \in K^\times$, prime to p, such that (α) is the pth power of an ideal of K.

(ii) We say that an arbitrary $\alpha \in K^\times$, prime to p, is *p-primary* if the Kummer extension $K(\sqrt[p]{\alpha})/K$ is unramified at the unique prime ideal $\mathfrak{p}$ above p in K (but possibly ramified elsewhere).

Remarks 2.2. (i) Let A be the group of pseudo–units of K; then we have the exact sequence (where ${}_p\mathcal{C}\ell := \{\gamma \in \mathcal{C}\ell,\ \gamma^p = 1\}$):

$$1 \longrightarrow E/E^p \longrightarrow AK^{\times p}/K^{\times p} \longrightarrow {}_p\mathcal{C}\ell \longrightarrow 1,$$

giving $\mathrm{rk}_p(AK^{\times p}/K^{\times p}) = \frac{p-1}{2} + \mathrm{rk}_p(\mathcal{C}\ell)$.

(ii) The general condition of p-primarity for any $\alpha \in K^\times$ (prime to p but not necessarily pseudo-unit) is "α congruent to a pth power modulo $\mathfrak{p}^p = (p)\,\mathfrak{p}$" (e.g., [10, Ch. I, § 6, (b)], Theorem 6.3). Since in any case, we can suppose $\alpha \equiv 1 \pmod{\mathfrak{p}}$, the above condition is then equivalent to $\alpha \equiv 1 \pmod{\mathfrak{p}^p}$ (indeed, $x \equiv 1 \pmod{\mathfrak{p}}$ implies $x^p \equiv 1 \pmod{\mathfrak{p}^p}$).

For the pseudo-units, the p-primarity may be precised as follows:

Proposition 2.3. *Let $\alpha \in K^\times$ be a pseudo–unit. Then α is p-primary if and only if it is a local pth power at $\mathfrak{p}$.*

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 in H/K of the principal ideal $\mathfrak{p} = (1-\zeta_p)$ is trivial; so $\mathfrak{p}$ splits totally in H/K, thus in $K(\sqrt[p]{\alpha})/K$, proving the proposition. □

There is another analogous case when α, prime to p, is not necessarily a pseudo-unit, but when we look at the p-primarity of α_θ for $\theta \neq 1, \omega$:

Proposition 2.4. *Let $\alpha \equiv 1 \pmod{\mathfrak{p}} \in K^\times$ and let $m \in [2, p-2]$. Let $\theta = \omega^m$, and consider α_θ. Then $\alpha_\theta \equiv 1 \pmod{\mathfrak{p}^m}$ and α_θ is p-primary if and only if $\alpha_\theta \equiv 1 \pmod{p}$, in which case $\alpha_\theta \equiv 1 \pmod{\mathfrak{p}^{m+p-1} = (p)\mathfrak{p}^m}$.*

Proof. Consider the Dwork uniformizing parameter ϖ in $\mathbb{Z}_p[\mu_p]$ which has the following properties:
(i) $\varpi^{p-1} = -p$,
(ii) $s(\varpi) = \omega(s) \cdot \varpi$, for all $s \in G$.

Put $\alpha_\theta = 1 + \varpi^k u$, where u is a unit of $\mathbb{Z}_p[\varpi]$ and $k \geq 1$; let $u_0 \in \mathbb{Z} \setminus p\mathbb{Z}$ such that $u \equiv u_0 \pmod{\varpi}$. Since $\alpha_\theta^s = \alpha_\theta^{\theta(s)}$ in $K^\times/K^{\times p}$, we get, for all $s \in G$:

$$\begin{aligned} 1 + s(\varpi^k)\, u_0 &= 1 + \omega^k(s)\, \varpi^k u_0 \\ &\equiv (1+\varpi^k u_0)^{\theta(s)} \equiv 1 + \omega^m(s)\, \varpi^k u_0 \pmod{\varpi^{k+1}}, \end{aligned}$$

which implies $k \equiv m \pmod{p-1}$ and $\alpha_\theta = 1 + \varpi^k\, u$, $k \in \{m, m+p-1, \ldots\}$. The p-primarity condition for α_θ is $\alpha_\theta \equiv 1 \pmod{\varpi^p}$ giving the obvious direction since $\varpi^p \sim p\,\varpi$. Suppose $\alpha_\theta \equiv 1 \pmod{\varpi^{p-1}}$; so $k = m$ does not work since $m \leq p-2$, and necessarily k is at least $m + p - 1 \geq p + 1$ since $m \geq 2$ (which is also the local pth power condition). □

We shall apply this with $\theta = \chi^* = \omega^{p-n}$, $n \in [2, p-3]$ even, and for some $\alpha \equiv 1 \pmod{\mathfrak{p}}$ deduced from Gauss sums.

3. Abelian p-ramification – Gauss sums

3.1. **Vandiver's conjecture and abelian p-ramification.** Let $\mathcal{T}$ be the torsion group of the Galois group of the maximal abelian p-ramified (i.e., unramified outside p) pro-p-extension $H^{\rm pr}$ of K; since Leopoldt's conjecture holds for abelian number fields, we have $\mathrm{Gal}(H^{\rm pr}/K) \simeq \mathbb{Z}_p^{\frac{p+1}{2}} \oplus \mathcal{T}$ where the Galois group Γ of the compositum of the $\mathbb{Z}_p$-extensions of K is such that $\Gamma = \Gamma_+ \oplus \Gamma_-$, with $\Gamma_+ \simeq \mathbb{Z}_p$ and $\Gamma_- \simeq \mathbb{Z}_p^{\frac{p-1}{2}}$ (for more information, see [10, 11, 14] and their references).

Write $\mathcal{T} = \mathcal{T}_+ \oplus \mathcal{T}_-$ and define $H_-^{\rm pr} \subseteq H^{\rm pr}$, $H_+^{\rm pr} \subseteq H^{\rm pr}$ so that $\mathrm{Gal}(H_+^{\rm pr}/K) \simeq \mathbb{Z}_p \oplus \mathcal{T}_+$ and $\mathrm{Gal}(H_-^{\rm pr}/K) \simeq \mathbb{Z}_p^{\frac{p-1}{2}} \oplus \mathcal{T}_-$. Note that $H_+^{\rm pr}/K$ is decomposed over K_+ to give the maximal abelian p-ramified pro-p-extension of K_+. We then have the following interpretation [10, Proposition III.4.2.2]:

Theorem 3.1. *The Vandiver conjecture $\mathcal{C}\ell_+ = 1$ is equivalent to $\mathcal{T}_- = 1$.*

Proof. We will briefly prove this famous "global" reflection result as follows: The Kummer radical of the compositum of the cyclic extensions of degree p of K contained in $H_-^{\rm pr}$ is generated (modulo $K^{\times p}$) by the obvious part E_+ of real units, giving a p-rank $\frac{p-3}{2}$, then by the real p-unit $\eta_+ := \zeta_p + \zeta_p^{-1} - 2$, and by the pseudo-units α_+ comming from $\mathcal{C}\ell_+$, which gives the p-rank of this radical equal to $\frac{p-1}{2} + \mathrm{rk}_p(\mathcal{C}\ell_+)$. Since $\mathrm{rk}_p(\mathrm{Gal}(H_-^{\rm pr}/K)) = \frac{p-1}{2} + \mathrm{rk}_p(\mathcal{T}_-)$, we get $\mathrm{rk}_p(\mathcal{T}_-) = \mathrm{rk}_p(\mathcal{C}\ell_+)$. □

The proof for the isotypic components is similar, taking the θ or θ^*-components for each object which yields [10, Theorem II.5.4.5]:

$$\mathrm{rk}_p(\mathcal{T}_{\theta^*}) = \mathrm{rk}_p(\mathcal{C}\ell_\theta). \tag{1}$$

In particular, if $\chi \in \mathscr{X}_+$, we shall say that Vandiver's conjecture holds at χ (i.e., $\mathcal{C}\ell_\chi = 1$) if and only if $\mathcal{T}_{\chi^*} = 1$.

Remarks 3.2. (i) One says that K is p-rational if $\mathcal{T} = 1$ (the definition is the same for any number field fulfilling the Leopoldt conjecture at p; see [11] for more details and programs testing the p-rationality of any field). For the pth cyclotomic field K this is equivalent to its p-regularity [9, Théorème 4.1] (the relation $\mathcal{T}_- = 1$ may be interpreted as the conjectural "relative p-rationality" of K). We have conjectured that any given field is p-rational for all $p \gg 0$.

(ii) At each unramified cyclic extension L_+ of degree p of K_+ is associated a p-primary pseudo-unit $\alpha \in (K^\times/K^{\times p})_-$ such that $L_+K = K(\sqrt[p]{\alpha})$. Put $(\alpha) = \mathfrak{A}^p$, where the p-class of $\mathfrak{A}$ is in $\mathcal{C}\ell_-$; moreover $\mathfrak{A}$ is not p-principal, otherwise α should be, up to a pth power factor, a unit $\varepsilon \in (E/E^p)_-$, which gives $\varepsilon \in \mu_p$ (absurd). In the same way, if G operates via χ on $\mathrm{Gal}(L_+/K_+)$ then by Kummer duality G operates via χ^* on $\langle\alpha\rangle K^{\times p}$.

We shall prove that such pseudo-units α may be found by means of suitable twists $g_c(\ell)$ of the Gauss sums (Lemma 4.4).

3.2. **Vandiver's conjecture and Gauss sums.** Recall the formula (see [10, Corollary III.2.6.1, Remark III.2.6.5] for more details and references):

$$\#\mathcal{T}_- = \frac{\#\mathcal{C}\ell_-}{\#\big(\mathbb{Z}_p \log(I)/\mathbb{Z}_p \log(U)\big)_-},$$

where I is the group of prime to p ideals of K and U is the group of principal local units of $\mathbb{Q}_p(\mu_p)$ which is equal to $1 + \varpi\, \mathbb{Z}_p[\varpi]$. If $\mathfrak{A} \in I$, let e be such

that $\mathfrak{A}^e = (\alpha)$, then $\log(\mathfrak{A}) := \frac{1}{e}\log(\alpha)$ where log is the p-adic logarithm; taking the minus part, $\log(\mathfrak{A})$ becomes well-defined.

We obtain for all $\chi \in \mathscr{X}_+$ (noting that $\mathcal{T}_\omega = \mathcal{C}\ell_\omega = 1$):

$$\#\mathcal{T}_{\chi^*} = \frac{\#\mathcal{C}\ell_{\chi^*}}{\#\big(\mathbb{Z}_p \log(I)/\mathbb{Z}_p \log(U)\big)_{\chi^*}}\cdot \tag{2}$$

The following reasonning (from [13, § 3]) gives another, but similar, interpretation of the result of Iwasawa [18]. Consider the Stickelberger element:

$$S := \frac{1}{p}\sum_{a=1}^{p-1} a\, s_a^{-1} \in \mathbb{Q}[G];$$

it is such that $S\,.\,e_{\chi^*} = b(\chi^*)\,.\,e_{\chi^*} := B_{1,(\chi^*)^{-1}}\,.\,e_{\chi^*}$ for all $\chi \in \mathscr{X}_+$; then if $\chi =: \omega^n$, $\chi^* = \omega^{p-n}$ for which $\#\mathcal{C}\ell_{\chi^*}$ corresponds to the ordinary Berrnoulli numbers B_n giving the "exponents of p-irregularity n" when $B_n \equiv 0 \pmod p$ (see Definition 1.1 (viii)).

Let $\mathfrak{L} \neq \mathfrak{p}$ be a prime ideal of K, let $F_\mathfrak{L}$ of characteristic ℓ be its residue field and let ψ be a character of order p of $F_\mathfrak{L}^\times$. We define the Gauss sum:

$$\tau(\psi) := -\sum_{x\in F_\mathfrak{L}} \psi(x)\,\xi_\ell^{\mathrm{tr}(x)} \in \mathbb{Z}[\mu_{p\ell}], \tag{3}$$

where ξ_ℓ is a primitive ℓth root of unity and tr the trace in $F_\mathfrak{L}/\mathbb{F}_\ell$. We have the fundamental relation in K (see [24, §§ 6.1, 6.2, 15.1]):

$$\mathfrak{L}^{pS} = \tau(\psi)^p\,\mathbb{Z}[\zeta_p], \tag{4}$$

Remark 3.3. Since various choices of $\mathfrak{L}$, ξ_ℓ and ψ, from a given ℓ, correspond to Galois conjugations and/or products by a pth root of unity, we denote simply $\tau(\psi)$ such a Gauss sum, where ψ is for instance the canonical character of order p; for convenience, we shall have in mind that ℓ *defines* such a $\tau(\psi)$ (and some other forthcoming objects) in an obvious way.

Taking the logarithms in (4), we obtain, for all $\chi \in \mathscr{X}_+$:[1]

$$S\,.\,e_{\chi^*}\,.\log(\mathfrak{L}) = b(\chi^*)\,.\log(\mathfrak{L})\,.\,e_{\chi^*} = \log(\tau(\psi))\,.\,e_{\chi^*}.$$

Then $p^{v_p(b(\chi^*))}\,\mathbb{Z}_p \log(\mathfrak{L})\,.\,e_{\chi^*} = \mathbb{Z}_p \log(\tau(\psi))\,.\,e_{\chi^*}$, thus, from (2):

$$\#\mathcal{T}_{\chi^*} = \frac{p^{v_p(b(\chi^*))}}{\#\big(\mathbb{Z}_p \log(\mathcal{G})/p^{v_p(b(\chi^*))}\log(U)\big)_{\chi^*}},$$

where $\mathcal{G}$ is the group generated by all the Gauss sums. So, the Vandiver conjecture at $\chi \in \mathscr{X}_+$ (i.e., $\mathcal{T}_{\chi^*} = 1$) is equivalent to $\big(\mathbb{Z}_p \log(\mathcal{G})/\log(U)\big)_{\chi^*} = 1$,

[1] Only $\log(\tau(\psi)^p)$ makes sense in $\mathbb{Z}_p[\zeta_p]$, but allows to define $\log(\tau(\psi)) \in \mathbb{Z}_p[\zeta_p]$ via the functional property of the logarithm.

and is obviously fulfilled if $b(\chi^*)$ is a p-adic unit. 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.

It will appear that one can restrict ourselves to primes $\ell \equiv 1 \pmod p$, what we shall suppose in the sequel.

More precisely, assume the Hypothesis 1.2 and let $\chi \in \mathscr{X}_+$ be such that $b(\chi^*) \sim p$ (i.e., $\#\mathcal{C}\ell_{\chi^*} = p$); thus $\mathcal{T}_{\chi^*} = 1$ if and only if there exists a prime number ℓ such that the corresponding $\log(\tau(\psi)_{\chi^*})$ generates $\log(U_{\chi^*}) = \log(1 + \varpi^{p-n}\mathbb{Z}_p[\varpi])$ (Proposition 2.4).

There is also the fact that the Gauss sums, considered modulo pth powers and computed modulo p, are indexed by infinitely many ℓ; in other words there are some non-obvious periodicities in the numerical results as ℓ varies. This may be explained as follows under the Hypothesis 1.2:

Proposition 3.4. *Let $\mathcal{C}\ell^{(p)} := I/\{(x),\ x \equiv 1 \pmod p\}$ be the ray class group of modulus $(p)\,\mathbb{Z}[\zeta_p]$. Then for any $\chi \in \mathscr{X}_+$, we have the following properties:*

(i) $\#\mathcal{C}\ell^{(p)}_{\chi^*} = p \cdot \#\mathcal{C}\ell_{\chi^*} \in \{p, p^2\}$.

(ii) The condition $\mathcal{C}\ell_\chi = 1$ is equivalent to the cyclicity of $\mathcal{C}\ell^{(p)}_{\chi^*}$.

Proof. We have the exact sequence $1 \to (V/W)_{\chi^*} \to \mathcal{C}\ell^{(p)}_{\chi^*} \to \mathcal{C}\ell_{\chi^*} \to 1$, where $V := \{x \in K^\times,\ x \equiv 1 \pmod{\mathfrak{p}}\}$, $W := \{x \in K^\times,\ x \equiv 1 \pmod p\}$, giving (i). The statement (ii) is obvious if $\mathcal{C}\ell_{\chi^*} = 1$. Suppose $\#\mathcal{C}\ell_{\chi^*} = p$; then $\mathcal{C}\ell_\chi = 1$ is equivalent to $\mathcal{T}_{\chi^*} = 1$ which implies the cyclicity of $\mathcal{C}\ell^{(p)}_{\chi^*}$. Reciprocally, if $\mathcal{C}\ell^{(p)}_{\chi^*}$ is cyclic, there exists an ideal $\mathfrak{A}$ such that $\mathfrak{A}^p_{\chi^*} = (\alpha_{\chi^*})$ with $\alpha_{\chi^*} \not\equiv 1 \pmod p$ and α_{χ^*} defines the radical of the unique p-ramified (but not unramified) cyclic extension of degree p of K decomposed over K_+ (its Galois group defines the cyclic group $\mathcal{T}_\chi$). □

As soon as $\mathfrak{L}' \mid \ell'$ and $\mathfrak{L} \mid \ell$ are such that $\mathfrak{L}' \in \mathfrak{L} \cdot (1 + p\,\mathbb{Z}[\zeta_p])$ formula (4) shows that the χ^*-components of the logarithms of the two Gauss sums are congruent modulo p. But this does not give any obvious rule between ℓ' and ℓ.

4. Gauss sums associated to primes $\ell \equiv 1 \pmod p$

Let $\mathscr{L}$ be the set of primes ℓ totally split in K (i.e., $\ell \equiv 1 \pmod p$). For $\ell \in \mathscr{L}$, let $\mathfrak{L} \mid \ell$ in K and let $\psi : \mathbb{F}_\ell^\times \longrightarrow \mu_p$ be of order p; if g is a primitive root modulo ℓ, we put $\psi(\overline{g}) = \zeta_p$. Let ξ_ℓ be a primitive ℓ-th root of unity; then the Gauss sum associated to ℓ may be written in $\mathbb{Z}[\mu_{p\,\ell}]$:

$$\tau(\psi) := -\sum_{x \in \mathbb{F}_\ell^\times} \psi(x) \cdot \xi_\ell^x = -\sum_{k=0}^{\ell-2} \zeta_p^k \cdot \xi_\ell^{g^k}. \tag{5}$$

4.1. **Practical computation of** $\mathrm{g}_c(\ell) := \tau(\psi)^{c-\sigma_c}$**.** Let $c \geq 2$ be a primitive root modulo p; to get an element of K, one must use the twisted version $\tau(\psi)^{c-\sigma_c}$, where $\sigma_c \in \mathrm{Gal}(\mathbb{Q}(\mu_{p\,\ell})/\mathbb{Q})$ is the Artin automorphism of c (its restriction to K is $s_c \in G$). We put:

$$\mathrm{g}_c(\ell) := \tau(\psi)^{c-\sigma_c}. \tag{6}$$

This notation using $\ell \in \mathscr{L}$ is justified by the Remark 3.3, then formulas (3) and (4), giving, for all $\chi \in \mathscr{X}_+$:

$$\mathfrak{L}^{S_c} = \mathrm{g}_c(\ell)\,\mathbb{Z}[\zeta_p] \;\;\&\;\; \mathfrak{L}_{\chi^*}^{(c-\chi^*(s_c))\cdot b(\chi^*)} = \mathrm{g}_c(\ell)_{\chi^*}\,\mathbb{Z}[\zeta_p] \tag{7}$$

where $S_c := (c-s_c)\cdot S \in \mathbb{Z}[G]$ is the corresponding twist of the Stickelberger element and where $\mathrm{g}_c(\ell) \in \mathbb{Z}[\zeta_p]$ as one checks easily. For simplicity, put:

$$b_c(\chi^*) := (c - \chi^*(s_c)) \cdot b(\chi^*) \sim b(\chi^*). \tag{8}$$

Then:

$$\mathfrak{L}_{\chi^*}^{b_c(\chi^*)} = \mathrm{g}_c(\ell)_{\chi^*}\,\mathbb{Z}[\zeta_p]. \tag{9}$$

In the above definition (6) of $\mathrm{g}_c(\ell)$, $\tau(\psi)^{\sigma_c} = \tau(\psi^c)\cdot\zeta(c)$, where $\zeta(c) \in \mu_p$; but for all $\chi \neq 1$, $\zeta(c)^{e_{\chi^*}} = 1$, which defines $\mathrm{g}_c(\ell)_{\chi^*}$ without ambiguity.

Lemma 4.1. *Let $\ell \in \mathscr{L}$ be given. Then $\mathrm{g}_c(\ell)$ is, up to the product by a pth root of unity, a product of Jacobi sums and $\mathrm{g}_c(\ell) \equiv 1 \pmod{\mathfrak{p}}$.*

Proof. The classical formula [24, § 6.1] on Jacobi sums (for $\psi\,\psi' \neq 1$) is:

$$J(\psi,\psi') := \tau(\psi)\cdot\tau(\psi')\cdot\tau(\psi\,\psi')^{-1} = -\sum_{x\in\mathbb{F}_\ell\setminus\{0,1\}} \psi(x)\cdot\psi'(1-x).$$

By induction, we obtain:

$$\tau(\psi)^c = J_1\cdots J_{c-1}\cdot\tau(\psi^c), \;\text{ where } J_i = -\sum_{x\in\mathbb{F}_\ell\setminus\{0,1\}} \psi^i(x)\cdot\psi(1-x).$$

Concerning the congruence, we have:

$$\tau(\psi) = -\sum_{x\in\mathbb{F}_\ell^\times} \psi(x)\cdot\xi_\ell^x \equiv -\sum_{x\in\mathbb{F}_\ell^\times} \xi_\ell^x \pmod{\mathfrak{p}};$$

but since ℓ is prime, $\sum_{x\in\mathbb{F}_\ell^\times} \xi_\ell^x = -1$, whence the result for $\mathrm{g}_c(\ell)$. □

Thus, in the numerical computations, we shall use the relation $\mathrm{g}_c(\ell)_{\chi^*} = (J_1\cdots J_{c-1})_{\chi^*}$ for any $\chi \in \mathscr{X}_+$.

Definitions 4.2. (i) We call set of exponents of p-primarity, of a prime $\ell \in \mathscr{L}$, the set $\mathscr{E}_\ell(p)$ of even integers $n \in [2, p-3]$ such that $\mathrm{g}_c(\ell)_{\omega^{p-n}}$ is p-primary (see Definition 2.1 (ii)).

(ii) We call set of exponents of p-irregularity, the set $\mathscr{E}_0(p)$ of even integers $n \in [2, p-3]$ such that $B_n \equiv 0 \pmod{p}$ (i.e., $b(\omega^{p-n}) \equiv 0 \pmod{p}$; see Definition 1.1 (viii)).

Remark 4.3. Let $\chi =: \omega^n \in \mathscr{X}_+$. If $\mathrm{g}_c(\ell)_{\chi^*}$ is p-primary this does not give necessarily a counterexample to Vandiver's conjecture for the following possible reasons considering the expression $S_c\, e_{\chi^*} = b_c(\chi^*)\, e_{\chi^*}$ (recall that $b_c(\chi^*) = (c - \chi^*(s_c)) \cdot b(\chi^*) \sim b(\chi^*)$):

(i) The number $b_c(\chi^*)$ is a p-adic unit, so $\mathrm{g}_c(\ell)_{\chi^*}$ is not the pth power of an ideal and leads to a ℓ-ramified Kummer extension of K_+ (i.e., the character $\chi^* = \omega^{p-n}$ does not correspond to an exponent of p-irregularity). For instance, the program below gives, for $p = 11$ ($c = 2$), $\ell = 23$, the exponent of 11-primarity $n = 2$ so that $\alpha := \mathrm{g}_c(\ell)_{\chi^*}$ is the integer (where $x = \zeta_{11}$):

```
16313053108*x^9 + 14568599738*x^8 + 15188534416*x^7 + 12440402458*x^6
+ 11144637196*x^5 + 19451005706*x^4 + 16080428144*x^3 + 12836788646*x^2
+ 12505300522*x + 12784005125
```

for which $K(\sqrt[11]{\alpha})/K$ is a cyclic extension of degree 11 of K decomposed over K_+ into L_+/K_+ only ramified at 23; then α is a product of prime ideals above 23 and is not a 11th power, since:

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha) = 134768284860588469651366402896654188603790598857406250$$
$$99289939159401864703561440252197759503241482448 07 = 23^{75}.$$

Its decomposition in K is $(\alpha) = \mathfrak{L}_1^9 \cdot \mathfrak{L}_2^{10} \cdot \mathfrak{L}_3^{12} \cdot \mathfrak{L}_4^3 \cdot \mathfrak{L}_5^5 \cdot \mathfrak{L}_6^{15} \cdot \mathfrak{L}_7^6 \cdot \mathfrak{L}_8^8 \cdot \mathfrak{L}_9^7$.

(ii) The number $b_c(\chi^*)$ is divisible by p, but the ideal $\mathfrak{L}_{\chi^*}$ is p-principal and then $\mathrm{g}_c(\ell)_{\chi^*}$ is a pth power in $K^\times$ (numerical examples in § 4.5.2).

So, a *necessary and sufficient condition for a counterexample* to Vandiver's conjecture is that there exists $\chi \in \mathscr{X}_+$ such that $b_c(\chi^*) \equiv 0 \pmod p$, and $\ell \in \mathscr{L}$ such that $\mathrm{g}_c(\ell)_{\chi^*}$ be p-primary, non-pth power in $K^\times$ (this shall be precised in Lemma 4.4 to give Theorem 4.5).

4.2. **Program.** For $p \in [3, 199]$ and for the least $\ell \in \mathscr{L}$, the following program computes $\mathrm{g}_c(\ell)$ in $\mathsf{Mod}(\mathsf{J}, \mathsf{P})$, with $\mathsf{P} = \mathsf{polcyclo}(\mathsf{p})$, where the product J of Jacobi sums is written in $\mathbb{Z}[x]$; c is a primitive root modulo p. We shall take into account the relation $J^{1+s_{-1}} \equiv 1 \pmod p$.

Taking $\mathsf{n} = 2 * \mathsf{m}$, we consider $\chi = \omega^n$ & $\chi^* = \omega^{p-n}$. Then the polynomials Jj give the powers J^{j} modulo p, $j = 1, \ldots, p-1$, in LJ.

The computation of $\mathrm{g}_c(\ell)_{\chi^*}$ is given in $\mathsf{Sn} = \prod_{\mathsf{a}=1}^{\mathsf{p}-1} \mathsf{s_a}(\mathsf{J}^{\mathsf{a}^{n-1}})$ from the formula $\mathrm{g}_c(\ell)_{\chi^*} = \prod_{a=1}^{p-1} s_a(\mathrm{g}_c(\ell))^{\omega^{n-p}(a)} = \prod_{a=1}^{p-1} s_a(\mathrm{g}_c(\ell)^{a^{n-1}})$ up to a pth power factor; then a^{n-1} is computed modulo p in an and then J^{an} is given by $\mathsf{component}(\mathsf{LJ}, \mathsf{an})$. Finaly the conjugate $\mathsf{s_a}(\mathsf{J}^{\mathsf{an}})$ is computed in sJan via the conjugation $\mathsf{x} \mapsto \mathsf{x}^{\mathsf{a}}$ in J^{an}, whence the product in Sn.

```
{forprime(p=3,200,c=lift(znprimroot(p));P=polcyclo(p)+Mod(0,p);
X=Mod(x,P);L=1;while(isprime(L)==0,L=L+2*p);g=znprimroot(L);
print("p=",p," L=",L," c=",c," g=",g);J=1;for(i=1,c-1,Ji=0;
for(k=1,L-2,kk=znlog(1-g^k,g);e=lift(Mod(kk+i*k,p));Ji=Ji-X^e);J=J*Ji);
```

```
d=p-2;LJ=List;Jj=1;for(j=1,p-1,Jj=lift(Jj*J);listinsert(LJ,Jj,j));
for(m=1,(p-3)/2,n=2*m;Sn=Mod(1,P);for(a=1,(p-1)/2,
an=lift(Mod(a,p)^(n-1));Jan=component(LJ,an);sJan=Mod(0,P);
for(j=0,d,aj=lift(Mod(a*j,p));sJan=sJan+x^(aj)*component(Jan,1+j));
Sn=Sn*sJan);if(Sn==1,print("   exponents of p-primarity: ",n))))}
p=3   L=7      c=2  g=3
p=5   L=11     c=2  g=2
p=7   L=29     c=2  g=2
p=11  L=23     c=3  g=5    exponents of p-primarity: 2
p=13  L=53     c=2  g=2
p=17  L=103    c=3  g=5
p=19  L=191    c=4  g=19
p=23  L=47     c=2  g=5
p=29  L=59     c=2  g=2    exponents of p-primarity: 2
p=31  L=311    c=7  g=17
p=37  L=149    c=2  g=2
p=41  L=83     c=6  g=2
p=43  L=173    c=9  g=2    exponents of p-primarity: 26
p=47  L=283    c=2  g=3
p=53  L=107    c=2  g=2    exponents of p-primarity: 34, 10
p=59  L=709    c=3  g=2
p=61  L=367    c=2  g=6
p=67  L=269    c=4  g=2
p=71  L=569    c=2  g=3
p=73  L=293    c=5  g=2
p=79  L=317    c=2  g=2
p=83  L=167    c=3  g=5
p=89  L=179    c=3  g=2
p=97  L=389    c=5  g=2    exponents of p-primarity: 26
p=101 L=607    c=2  g=3    exponents of p-primarity: 10
p=103 L=619    c=5  g=3
p=107 L=643    c=2  g=11
p=109 L=1091   c=6  g=2    exponents of p-primarity: 14, 86
p=113 L=227    c=3  g=2
p=127 L=509    c=3  g=2
p=131 L=263    c=2  g=5    exponents of p-primarity: 16
p=137 L=823    c=3  g=3    exponents of p-primarity: 78
p=139 L=557    c=2  g=2
p=149 L=1193   c=2  g=3
p=151 L=907    c=6  g=2
p=157 L=1571   c=5  g=2    exponents of p-primarity: 94
p=163 L=653    c=2  g=2    exponents of p-primarity: 42
p=167 L=2339   c=5  g=2    exponents of p-primarity: 122
p=173 L=347    c=2  g=2
p=179 L=359    c=2  g=7    exponents of p-primarity: 138
p=181 L=1087   c=2  g=3    exponents of p-primarity: 114, 164
p=191 L=383    c=19 g=5
p=193 L=773    c=5  g=2    exponents of p-primarity: 108, 172
p=197 L=3547   c=2  g=2    exponents of p-primarity: 62
p=199 L=797    c=3  g=2
```

The program tests the "first" prime $\ell \in \mathscr{L}$ and we shall see § 4.4.2 that it is sufficient to try another ℓ to be successful in testing Vandiver's conjecture.

4.3. **Reciprocal study.** Recall, from Remark 4.3, that, for all $\chi \in \mathscr{X}_+$, $(\mathrm{g}_c(\ell)_{\chi^*}) = \mathfrak{L}^{S_c\, e_{\chi^*}} = \mathfrak{L}_{\chi^*}^{b_c(\chi^*)}$ and that the three conditions:

(a) $b_c(\chi^*) \equiv 0 \pmod p$,

(b) $\mathrm{g}_c(\ell)_{\chi^*}$ is p-primary,

(c) $\mathrm{g}_c(\ell)_{\chi^*}$ is not a pth power,

give rise to a counterexample to Vandiver's conjecture.

We still assume the Hypothesis 1.2 to obtain the reciprocal (to be put in relation with Proposition 3.4):

Lemma 4.4. *Let $\chi \in \mathscr{X}_+$ be such that $\mathcal{C}\ell_\chi \neq 1$ (i.e., we assume to have a counterexample to Vandiver's conjecture). Then $\mathcal{C}\ell_{\chi^*} \neq 1$, $b_c(\chi^*) \sim p$, and there exists a totally split prime ideal $\mathfrak{L}$ such that $\mathfrak{L}_{\chi^*}$ represents a generator of $\mathcal{C}\ell_{\chi^*}$; afterwards $\mathfrak{L}^{S_c\, e_{\chi^*}} = \mathfrak{L}_{\chi^*}^{b_c(\chi^*)} = (\alpha_{\chi^*})$, where α_{χ^*} is unique, thus equal to $\mathrm{g}_c(\ell)_{\chi^*}$ which is p-primary (i.e., $\mathrm{g}_c(\ell)_{\chi^*} \equiv 1 \pmod p$) and not a pth power in $K^\times$.*

Proof. The claim $\mathcal{C}\ell_{\chi^*} \neq 1$ is the consequence of the reflection theorem.

From the Chebotarev theorem in $H/\mathbb{Q}$, there exists a prime ℓ and $\overline{\mathfrak{L}} \mid \ell$ in H such that (in terms of Frobenius) $\left(\frac{H/\mathbb{Q}}{\overline{\mathfrak{L}}}\right)$ generates the subgroup of $\mathrm{Gal}(H/K)$ corresponding to $\mathcal{C}\ell_{\chi^*}$ by class field theory. So ℓ splits completely in $K/\mathbb{Q}$ (i.e., $\ell \in \mathscr{L}$) and the ideal $\mathfrak{L}$ of K under $\overline{\mathfrak{L}}$ is (as well as $\mathfrak{L}_{\chi^*}$) a representative of a generator of $\mathcal{C}\ell_{\chi^*}$.

Necessarily $b_c(\chi^*) = p\,u$ for a p-adic unit u, and $\mathfrak{L}_{\chi^*}^{pu} = (\alpha_{\chi^*})$; since $E_{\chi^*} = 1$ (except for $\chi^* = \omega$ excluded), α_{χ^*} is unique and not a pth power; in terms of Gauss sums, $\mathfrak{L}_{\chi^*}^{pu} = (\mathrm{g}_c(\ell)_{\chi^*})$ (see (7)), thus $\alpha_{\chi^*} = \mathrm{g}_c(\ell)_{\chi^*}$.

The p-primarity of α_{χ^*} is necessary to obtain the corresponding unramified Kummer extension $K\big(\sqrt[p]{\alpha_{\chi^*}}\big)$ of degree p of K, decomposed over K_+ into the unramified extension associated to $\mathcal{C}\ell_\chi$ by class field theory, whence the p-primarity of $\mathrm{g}_c(\ell)_{\chi^*}$. □

4.4. **The test of Vandiver's conjecture.** Drawing the consequences of the above, we shall get the main test for Vandiver's conjecture.

4.4.1. *Main theorem.* Recall that $\mathscr{L}$ is the set of primes $\ell \equiv 1 \pmod p$.

A necessary and sufficient condition, to have a counterexample to Vandiver's conjecture (under the Hypothesis 1.2), is that there exists $\chi \in \mathscr{X}_+$, such that $b_c(\chi^*) \sim p$, and $\ell \in \mathscr{L}$ such that $\mathrm{g}_c(\ell)_{\chi^*} := \tau(\psi)^{c-\sigma_c}$ (cf. (6), (7)) is p-primary and not a pth power (i.e., $\mathfrak{L}_{\chi^*}$ non-p-principal):

Theorem 4.5. *Let $\ell \in \mathscr{L}$ and let $\mathscr{E}_\ell(p)$ be the set of exponents of p-primarity of ℓ (i.e., the even $n \in [2, p-3]$, such that $\mathrm{g}_c(\ell)_{\omega^{p-n}} \equiv 1 \pmod p$), and let $\mathscr{E}_0(p)$ be the set of exponents of p-irregularity of K (i.e., the even $n \in [2, p-3]$, such that p divides the nth Bernoulli number B_n).*
Then, if $\mathscr{E}_\ell(p) \cap \mathscr{E}_0(p) = \emptyset$, the Vandiver conjecture holds for K.

Proof. Consider, for $\chi =: \omega^n \in \mathscr{X}_+$, and $\chi^* = \omega^{p-n}$, the relation (7) giving $\mathfrak{L}_{\chi^*}^{b_c(\chi^*)} = (\mathrm{g}_c(\ell)_{\chi^*})$, and examine the two possibilities for $n \in [2, p-3]$ even:
(i) If n is not an exponent of p-irregularity (i.e., $b_c(\chi^*) \not\equiv 0 \pmod p$ or $B_n \not\equiv 0 \pmod p$), then $\mathcal{C}\ell_{\chi^*} = 1$ and $\mathcal{C}\ell_\chi = 1$ from reflection theorem (we also have $\mathcal{T}_{\chi^*} = 1$, see § 3.2).
(ii) If n is an exponent of p-irregularity, then $b_c(\chi^*) \sim p$, giving, for some p-adic unit u, $\mathfrak{L}_{\chi^*}^{pu} = (\mathrm{g}_c(\ell)_{\chi^*})$; if $\mathfrak{L}_{\chi^*}$ is p-principal, then $\mathrm{g}_c(\ell)_{\chi^*}$ is a global pth power, hence p-primary (absurd by assumption). So $\mathfrak{L}_{\chi^*}$ defines a class of order p in $\mathcal{C}\ell_{\chi^*}$ for which $\mathrm{g}_c(\ell)_{\chi^*}$ is not p-primary, whence $\mathcal{C}\ell_\chi = 1$ by Kummer duality since $K(\sqrt[p]{\mathrm{g}_c(\ell)_{\chi^*}})/K$ is ramified at p. □

Corollary 4.6. *Let $\ell \in \mathscr{L}$. If, for all $\chi \in \mathscr{X}_+$, the numbers $\mathrm{g}_c(\ell)_{\chi^*}$ are not p-primary (i.e., $\mathscr{E}_\ell(p) = \emptyset$), then the Vandiver conjecture is true for p.*

4.4.2. *Minimal prime $\ell \in \mathscr{L}$ such that $\mathscr{E}_\ell(p) = \emptyset$.* The following program examines, for each p, the successive prime numbers $\ell_i \in \mathscr{L}$, $i \geq 1$, and returns the first one, ℓ_N (in L with its index N), such that $\mathscr{E}_{\ell_N}(p) = \emptyset$. Its existence is of course a strong conjecture, but the numerical results are extremely favorable to the existence of such primes; which strengthens the conjecture of Vandiver. Moreover, since the integer $i(p) = \#\mathscr{E}_0(p)$ is rather small regarding p, as doubtless for $\#\mathscr{E}_\ell(p)$, and can be both in $O\big(\frac{\log(p)}{\log(\log(p))}\big)$, the intersection of $\mathscr{E}_\ell(p) \cap \mathscr{E}_0(p)$ may be easily empty if these sets are independent; the experiments give the impression that the sets $\mathscr{E}_\ell(p)$ are random when ℓ varies and have no link with $\mathscr{E}_0(p)$

```
{forprime(p=3,700,c=lift(znprimroot(p));P=polcyclo(p)+Mod(0,p);X=Mod(x,P);
N=0;for(i=1,99,L=1+2*i*p;if(isprime(L)!=1,next);N=N+1;g=znprimroot(L);
J=1;for(i=1,c-1,Ji=0;for(k=1,L-2,kk=znlog(1-g^k,g);e=lift(Mod(kk+i*k,p));
Ji=Ji-X^e);J=J*Ji);d=p-2;LJ=List;Jj=1;for(j=1,p-1,Jj=lift(Jj*J);
listinsert(LJ,Jj,j));T=1;for(m=1,(p-3)/2,n=2*m;Sn=Mod(1,P);
for(a=1,(p-1)/2,an=lift(Mod(a,p)^(n-1));Jan=component(LJ,an);sJan=Mod(0,P);
for(j=0,d,aj=lift(Mod(a*j,p));sJan=sJan+x^(aj)*component(Jan,1+j));
Sn=Sn*sJan);if(Sn==1,T=0;break));if(T==1,print(p," ",L," ",N);break)))}
```

For $p < 400$, we only write the primes p, ℓ_N for which $N > 1$:

p	L	N	p	L	N	p	L	N	p	L	N	p	L	N
11	67	2	197	4729	2	409	4091	2	499	1997	1	601	25243	5
29	233	2	211	10973	4	419	839	1	503	3019	1	607	20639	3
43	431	2	223	6691	2	421	4211	1	509	4073	2	613	6131	1
53	743	2	227	5903	2	431	863	1	521	16673	1	617	30851	3

```
97  971   2   229 5039  2   433 5197  2   523 6277  2   619 17333  3
101 809   2   233 1399  2   439 4391  1   541 9739  1   631 6311   1
109 2399  2   251 4519  2   443 887   1   547 5471  1   641 1283   1
131 1049  3   277 4987  3   449 3593  1   557 24509 3   643 10289  2
137 1097  2   337 6067  3   457 21023 3   563 7883  1   647 9059   1
157 7537  5   349 8377  2   461 9221  2   569 6829  1   653 1307   1
163 5869  3   367 3671  2   463 5557  1   571 5711  1   659 1319   1
167 7349  3   383 16087 4   467 2803  1   577 3463  2   661 14543  3
179 1433  2   389 14783 2   479 3833  1   587 8219  1   673 2693   1
181 1811  2   397 6353  2   487 1949  1   593 1187  1   677 5417   1
193 1931  2   401 10427 4   491 983   1   599 4793  1   683 4099   2
```

The comparison with the table of exponents of p-irregularity does not show any relation. Moreover, this much stronger test of Vandiver's conjecture does not need the knowledge of $\mathscr{E}_0(p)$.

4.5. **What happens when $\ell \in \mathscr{L}$ varies with $\mathscr{E}_0(p) \neq \emptyset$?** Let n_0 even be an exponent of p-irregularity under the Hypothesis 1.2, and put $\chi_0 = \omega^{n_0}$; then $\#\mathcal{C}\ell_{\chi_0^*} = p$ and $b_c(\chi_0^*) = pu$, for a p-adic unit u.

4.5.1. *About the p-class of $\mathfrak{L} \mid \ell$.* Let $\ell \in \mathscr{L}$ with $\mathfrak{L} \mid \ell$, and let $\mathfrak{L}_{\chi_0^*}$ where $\chi_0^* = \omega^{p-n_0}$. There are two cases as we have seen previously:

(i) $\mathfrak{L}_{\chi_0^*}$ is p-principal; since $b_c(\chi_0^*) = p\,u$, $\mathrm{g}_c(\ell)_{\chi_0^*}$ is a pth power in $K^\times$, whence $\mathrm{g}_c(\ell)_{\chi_0^*}$ is p-primary and $n_0 \in \mathscr{E}_\ell(p)$, but this does not lead to an unramified cyclic extension of degree p of K_+ of character χ_0;

(ii) $\mathfrak{L}_{\chi_0^*}$ is not p-principal; thus it defines the non-trivial group $\mathcal{C}\ell_{\chi_0^*}$ and Vandiver's conjecture holds at $\chi_0 = \omega^{n_0}$ if and only if $\mathrm{g}_c(\ell)_{\chi_0^*}$ is not p-primary. If $\mathrm{g}_c(\ell)_{\chi_0^*} \equiv 1 \pmod p$, whatever the ideal $\mathfrak{L}'_{\chi_0^*}$, $\mathfrak{L}' \mid \ell' \in \mathscr{L}$, we have $\mathfrak{L}'_{\chi_0^*} = (z_{\chi_0^*}) \cdot \mathfrak{L}^r_{\chi_0^*}$, with $z \in K^\times$ and $r \in [0, p-1]$, so that:

$$\mathfrak{L}'^{pu}_{\chi_0^*} = (z^{pu}_{\chi_0^*}) \cdot \mathfrak{L}^{rpu}_{\chi_0^*} \quad \& \quad \mathrm{g}_c(\ell')_{\chi_0^*} \equiv \mathrm{g}_c(\ell)^r_{\chi_0^*} \equiv 1 \pmod p.$$

Whence, the index n_0 of p-irregularity is a common exponent of p-primarity for all $\ell \in \mathscr{L}$, giving $\mathscr{E}_0(p) \cap \Big(\bigcap\limits_{\ell \in \mathscr{L}} \mathscr{E}_\ell(p) \Big) \neq \emptyset$.

Thus we can state from Theorem 4.5 (under Hypothesis 1.2):

Corollary 4.7. *As soon as there exist distinct $\ell_1, \ldots, \ell_N \in \mathscr{L}$, $N \geq 1$, such that $\mathscr{E}_{\ell_1}(p) \cap \cdots \cap \mathscr{E}_{\ell_N}(p) = \emptyset$, the Vandiver conjecture holds.*

So it is fundamental to see if the sets $\mathscr{E}_\ell(p)$ are independent (or not) of the choice of $\ell \in \mathscr{L}$.

We analyse the case of $p = 37$ whose exponent of p-irregularity is $n_0 = 32$ giving $\#\mathcal{C}\ell_{\omega^5} = 37$ and compute (in expp) the sets $\mathscr{E}_\ell(37)$ when $\ell \in \mathscr{L}$ varies. We shall see that the results do no seem to depend on the order of magnitude of ℓ (the number of exponents of p-primarity grows in the same

proportion as, classically, for the exponents of p-irregularity); if $n_0 \in \mathscr{E}_\ell(37)$, this means that $\mathfrak{L}_{\chi^*}$ is necessarily p-principal:

```
{p=37;c=lift(znprimroot(p));P=polcyclo(p)+Mod(0,p);X=Mod(x,P);
for(i=1,100,L=1+2*i*p;if(isprime(L)==1,g=znprimroot(L);
print("L=",L," g=",g);J=1;for(i=1,c-1,Ji=0;for(k=1,L-2,kk=znlog(1-g^k,g);
e=lift(Mod(kk+i*k,p));Ji=Ji-X^e);J=J*Ji);d=p-2;LJ=List;Jj=1;
for(j=1,p-1,Jj=lift(Jj*J);listinsert(LJ,Jj,j));for(m=1,(p-3)/2,n=2*m;
Sn=Mod(1,P);for(a=1,(p-1)/2,an=lift(Mod(a,p)^(n-1));
Jan=component(LJ,an);sJan=Mod(0,P);for(j=0,d,aj=lift(Mod(a*j,p));
sJan=sJan+x^(aj)*component(Jan,1+j));Sn=Sn*sJan);
if(Sn==1,print("     exponent of p-primarity: ",n)))))}
```

```
L=149      g=2                      L=3331     g=3   expp: 22
L=223      g=3                      L=3701     g=2
L=593      g=3                      L=3923     g=2
L=1259     g=2                      L=4219     g=2   expp: 18,16
L=1481     g=3    expp: 30          L=4441     g=21
L=1777     g=5                      L=4663     g=3
L=1999     g=3                      L=5107     g=2
L=2221     g=2                      L=5477     g=2
L=2591     g=7    expp: 34          L=6143     g=5   expp: 28
L=2887     g=5                      L=6217     g=5
L=3109     g=6                      L=6661     g=6
L=3257     g=3                      L=6883     g=2
-----------------------------------------------------------------------
L=742073   g=3    expp: 12          L=768343   g=11  expp: 18
L=742369   g=7                      L=768491   g=10
L=742591   g=3                      L=768787   g=2   expp: 20
L=743849   g=3                      L=769231   g=11  expp: 24
L=743923   g=3    expp: 16          L=769453   g=2   expp: 30
L=744071   g=22                     L=772339   g=3
L=744811   g=10                     L=773153   g=3   expp: 14
L=744959   g=13   expp: 10          L=774337   g=5   expp: 28
L=745033   g=10   expp: 16          L=774929   g=3   expp: 18
L=745181   g=2                      L=775669   g=10  expp: 18
L=745477   g=2                      L=776483   g=2
L=745699   g=2                      L=776557   g=2   expp: 20
L=746069   g=2                      L=777001   g=31  expp: 18,28
L=746957   g=2                      L=778111   g=11
L=747401   g=3                      L=778333   g=2   expp: 28
L=747919   g=3                      L=778777   g=5
L=748807   g=6    expp: 22          L=779221   g=2
L=749843   g=2    expp: 34          L=779591   g=7
L=750287   g=5                      L=779887   g=10  expp: 18
L=750509   g=2    expp: 14,22       L=780257   g=3   expp: 8
L=751027   g=3                      L=780553   g=10
L=751841   g=3    expp: 14,16,24    L=781367   g=5   expp: 34
L=752137   g=10   expp: 8           L=781589   g=2   expp: 32
L=752359   g=3    expp: 18          L=782107   g=2
L=752581   g=2    expp: 16          L=782329   g=13  expp: 18
```

```
L=752803   g=2    expp: 22,32      L=782921   g=3   expp: 20
L=753617   g=3                     L=783143   g=5
L=753691   g=11   expp: 16         L=783661   g=2
L=753839   g=7    expp: 4,22       L=784327   g=3
L=754283   g=2                     L=784697   g=3
L=755171   g=6                     L=784919   g=7
L=755393   g=3    expp: 22         L=785363   g=2
L=756281   g=3    expp: 2          L=786251   g=2
L=756799   g=15   expp: 18         L=786547   g=2
L=757243   g=2                     L=787139   g=2   expp: 20
L=757909   g=2    expp: 16         L=787361   g=6
L=758279   g=7                     L=787879   g=6   expp: 10,18,20
L=758501   g=2    expp: 18         L=788027   g=2   expp: 34
L=759019   g=2                     L=789137   g=3   expp: 24
L=759167   g=5    expp: 12         L=790099   g=2
L=759463   g=3                     L=791209   g=7
L=759833   g=3    expp: 4          L=791431   g=12
L=760129   g=11                    L=791801   g=3
L=760499   g=2                     L=792023   g=5   expp: 32
L=762053   g=2                     L=792689   g=3
L=762571   g=10                    L=793207   g=5
L=763237   g=2                     L=795427   g=2
L=764051   g=2                     L=795649   g=22  expp: 2,32
L=764273   g=3                     L=795797   g=2
L=764717   g=2    expp: 2          L=795871   g=3
L=765383   g=5                     L=796759   g=3
L=765827   g=2    expp: 34         L=796981   g=7
L=766049   g=3    expp: 22         L=797647   g=3
L=766937   g=3    expp: 34         L=797869   g=10
L=767381   g=2    expp: 18         L=798461   g=2
L=767603   g=5    expp: 34         L=798757   g=2
L=767677   g=5                     L=800089   g=7   expp: 20
```

For $\ell = 149, 223, 593, 1259, 1777, \ldots$, $\mathscr{E}_\ell(37) = \emptyset$, which proves the Vandiver conjecture for $p = 37$ a great lot of times. For $\ell = 1481$ one finds a p-primarity for $\chi^* = \omega^7$ ($\chi = \omega^{30} \neq \omega^{32}$). Corollary 4.7 applies at will.

Remark 4.8. We remark that $\chi_0 = \omega^{32}$ gives $\chi_0^* = \omega^5$ which is a character of K, not the character of a strict subfield (the class of order 37 does not come from a strict subfield); then $\chi = \omega^{30}$ is a character of the real subfield k_6 of degree 6 which gives rise to a ℓ-ramified (i.e., unramified outside ℓ since the 37-primarity gives the non-ramification of p) cyclic extension of degree p of k_6. If the exponent of p-irregularity had been 30 instead of 32, this would have given an unramified cyclic extension of degree p of k_6, i.e., $\#\mathcal{C}\ell_{k_6} = 37$.

It remains to give statistics about the p-principality (or not) of the $\mathfrak{L}_{\chi_0^*}$ when $\ell \in \mathscr{L}$ varies. In the particular case $p = 37$, $\mathfrak{L}_{\chi_0^*}$ is p-principal if and

only if $\mathfrak{L}$ is principal since the exponent of p-irregularity $n_0 = 32$ is unique and the class number of K equal to $h = 37$.

4.5.2. *Table of the classes of $\mathfrak{L}$ for $p = 37$.* We give a table with a generator of $\mathfrak{L}$ in the principal cases (indicated by $*$). Otherwise, the class of $\mathfrak{L}$ is of order 37 in K. The exponents of p-primarity are denoted expp and we only write the cases where $\mathscr{E}_\ell(37) \neq \emptyset$:

```
{p=37;c=lift(znprimroot(p));P=polcyclo(p);K=bnfinit(P,1);P=P+Mod(0,p);
X=Mod(x,P);Lsplit=List;N=0;for(i=1,2000,L=1+2*i*p;if(isprime(L)==1,
N=N+1;listinsert(Lsplit,L,N)));for(j=1,N,L=component(Lsplit,j);
F=bnfisintnorm(K,L);if(F!=[],print("L=",L," ",component(F,1)));
g=znprimroot(L);J=1;for(i=1,c-1,Ji=0;for(k=1,L-2,kk=znlog(1-g^k,g);
e=lift(Mod(kk+i*k,p));Ji=Ji-X^e);J=J*Ji);d=p-2;LJ=List;
Jj=1;for(j=1,p-1,Jj=lift(Jj*J);listinsert(LJ,Jj,j));for(m=1,(p-3)/2,
n=2*m;Sn=Mod(1,P);for(a=1,(p-1)/2,an=lift(Mod(a,p)^(n-1));
Jan=component(LJ,an);sJan=Mod(0,P);for(j=0,d,aj=lift(Mod(a*j,p));
sJan=sJan+x^(aj)*component(Jan,1+j));Sn=Sn*sJan);
if(Sn==1,print("L=",L," expp:",n))))}
```

```
 L=1481    expp: 30               L=56167   expp: 10,14,26
 L=2591    expp: 34               L=57203   expp: 34
 L=3331    expp: 22               L=58313   expp: 28
 L=4219    expp: 16,18            L=58757   expp: 16,18
 L=6143    expp: 28               L=58831   expp: 24,30
 L=7993    expp: 16,20            L=59497   expp: 28
 L=8363    expp: 8                L=61051   expp: 10
 L=9769    expp: 20               L=62383   expp: 2
 L=10657   expp: 4,18,26          L=62753   expp: 2
 L=12433   expp: 20               L=63493   expp: 2
 L=13099   expp: 28              *L=64381   expp: 6,32 [x^20+x^9+x]
 L=14431   expp: 4,14,22          L=66749   expp: 30
 L=17021   expp: 6               *L=67489  expp: 30,32 [x^24-x^3-x^2]
 L=17909   expp: 30               L=67933   expp: 6
 L=18131   expp: 22              *L=68821  expp: 32    [x^15-x^9+x^4]
 L=19463   expp: 6                L=69931   expp: 12
 L=20129   expp: 6                L=71411   expp: 4
 L=21017   expp: 2,4              L=72817   expp: 28
 L=21313   expp: 18               L=74149   expp: 2
 L=21757   expp: 8                L=75407   expp: 10
 L=22349   expp: 8                L=75629   expp: 12, 20
 L=23459   expp: 6                L=76961   expp: 14
 L=23977   expp: 26               L=78737   expp: 28
 L=25087   expp: 26               L=79181   expp: 10
 L=25457   expp: 30               L=80513   expp: 16, 26
 L=29009   expp: 8,24             L=81031   expp: 18, 34
 L=30859   expp: 2                L=82067   expp: 34
*L=32783   expp: 32 [x^11+x^3+x]  L=83621   expp: 34
 L=33301   expp: 30               L=83843   expp: 2
 L=33967   expp: 26               L=84731   expp: 6
```

```
L=36187   expp: 8              L=85027   expp: 26
L=37889   expp: 16             L=86729   expp: 22
L=38629   expp: 22             L=86951   expp: 8
L=40627   expp: 30             L=87691   expp: 24
L=40849   expp: 6              L=91243   expp: 22, 34
L=42773   expp: 4              L=91909   expp: 30
L=45289   expp: 8              L=94351   expp: 10
L=45659   expp: 26             L=94573   expp: 18
L=48619   expp: 8              L=95239   expp: 18, 28
L=48989   expp: 20             L=96497   expp: 10
L=51283   expp: 14,16          L=98347   expp: 28
L=51431   expp: 20             L=98939   expp: 30
L=53281   expp: 16             L=99679   expp: 10, 22
L=55057   expp: 20             L=100049  expp: 14
```

This table shows the clear independence of the exponents of p-primarity regarding the set of *non-principal* $\mathfrak{L}$. Give some examples:

(i) Principal case $\mathfrak{L} \mid 32783$. The principal $\mathfrak{L}$ are rare (which comes from density theorems); the first one is $\mathfrak{L} = (\zeta_{37}^{11} + \zeta_{37}^{3} + \zeta_{37})$ where $\ell = 32783$. Thus in that case, in the relation $\mathfrak{L}_{\chi_0^*}^{b_c(\chi_0^*)} = (\mathrm{g}_c(\ell)_{\chi_0^*})$, the number $\mathrm{g}_c(\ell)_{\chi_0^*}$ must be a 37th power (which explain that one shall find the exponent of 37-primarity equal to that of 37-irregularity in any table); infortunately, the data are too large to be given. Nevertheless, the reader can easily compute $\mathsf{factor}(\mathsf{norm}(\mathsf{Sn})) = 32783^{37\cdot 16\cdot 9}$ and use $\mathsf{K} = \mathsf{bnfinit}(\mathsf{P},1); \mathsf{idealfactor}(\mathsf{K},\mathsf{Sn})$, which gives the 37th power of a principal ideal $\mathfrak{L} \mid 32783$.

(ii) Non-principal case $\mathfrak{L} \mid 149$. The instruction $\mathsf{bnfisintnorm}(\mathsf{K}, 149^{\mathsf{k}})$:

```
{P=polcyclo(37);K=bnfinit(P,1);for(k=1,2,print(bnfisintnorm(K,149^k)))}
```

yields an empty set for $k = 1$ (since $\mathfrak{L}$ is not principal) and, for $k = 2$, it gives (with $x = \zeta_{37}$) the 18 conjugates of:

```
-2*x^35-2*x^34-x^32-2*x^31+x^29-x^28-2*x^27-2*x^24-x^23+x^22-2*x^20
      -x^19-x^17-2*x^16+x^14-x^13-2*x^12-2*x^9-x^8+x^7-2*x^5-x^4-2*x^2-2*x
```

since $\mathrm{N}_{K/K_+}(\mathfrak{L})$ is always principal. This allows an easy characterization.

4.5.3. *Densities of the exponents of p-primarity.* The following program intends to show that all exponents of p-primarity are obtained, with some specific densities, taking sufficientely many $\ell \in \mathscr{L}$ (each even $n \in [2, p-3]$, such that $\mathrm{g}_c(\ell)_{\omega^{p-n}}$ is p-primary for some new ℓ, is counted in the $(n/2)$th component of the list EL).

At the beginning of the list, one finds the index i of the prime ℓ_i considered; if some index i is missing, this means that $\mathscr{E}_{\ell_i}(p) = \emptyset$. The second integer gives the whole number of exponents of p-primarity obtained at this step; then the third one is ℓ_i. In some cases, a prime ℓ gives rise to several exponents of p-primarity, as the following excerpt shows:

```
2757 1298 1289303  [76,88,78,88, 72,77,81,66,82, 78,85,69,76,72,73,65,72]
2757 1299 1289303  [76,88,78,89*,72,77,81,66,82, 78,85,69,76,72,73,65,72]
2757 1300 1289303  [76,88,78,89, 72,77,81,66,83*,78,85,69,76,72,73,65,72]
2757 1301 1289303  [76,88,78,89, 72,77,81,66,83, 78,85,69,76,72,73,65,73*]
```

(i) Program:

```
{p=37;c=lift(znprimroot(p));P=polcyclo(p)+Mod(0,p);X=Mod(x,P);
NL=0;Npp=0;EL=List;for(j=1,(p-3)/2,listput(EL,0,j));
for(i=1,1000,L=1+2*i*p;if(isprime(L)==1,g=znprimroot(L);NL=NL+1;
J=1;for(i=1,c-1,Ji=0;for(k=1,L-2,kk=znlog(1-g^k,g);e=lift(Mod(kk+i*k,p));
Ji=Ji-X^e);J=J*Ji);d=p-2;LJ=List;Jj=1;for(j=1,p-1,Jj=lift(Jj*J);
listinsert(LJ,Jj,j));for(m=1,(p-3)/2,n=2*m;Sn=Mod(1,P);
for(a=1,(p-1)/2,an=lift(Mod(a,p)^(n-1));Jan=component(LJ,an);sJan=Mod(0,P);
for(j=0,d,aj=lift(Mod(a*j,p));sJan=sJan+x^(aj)*component(Jan,1+j));
Sn=Sn*sJan);if(Sn==1,Npp=Npp+1;listput(EL,1+component(EL,n/2),n/2);
print(NL," ",Npp," ",L," ",EL)))))}
```

(ii) Results for $p = 37$. The end of the table for the selected interval is:

```
3012 1423 1413179   [83,94,84,91,80,80,86,82,92,82,97,76,83,78,85,74,76]
3012 1424 1413179   [83,94,84,91,80,80,86,82,92,83,97,76,83,78,85,74,76]
3014 1425 1413623   [83,95,84,91,80,80,86,82,92,83,97,76,83,78,85,74,76]
3015 1426 1414067   [83,95,84,91,80,80,86,83,92,83,97,76,83,78,85,74,76]
3015 1427 1414067   [83,95,84,91,80,80,86,83,92,83,97,76,83,78,86,74,76]
3027 1428 1419839   [83,95,84,91,80,80,86,83,92,83,98,76,83,78,86,74,76]
3030 1429 1420949   [83,95,84,91,80,80,86,83,92,83,98,76,83,78,86,75,76]
3032 1430 1421911   [83,95,85,91,80,80,86,83,92,83,98,76,83,78,86,75,76]
3033 1431 1422133   [83,95,86,91,80,80,86,83,92,83,98,76,83,78,86,75,76]
3042 1432 1428127   [83,96,86,91,80,80,86,83,92,83,98,76,83,78,86,75,76]
```

The penultimate column corresponds to the exponent of 37-irregularity $n_0 = 32$; since there is no counterexamples to Vandiver's conjecture, when this component increases, this means that the new ℓ gives rise to a principal $\mathfrak{L}$ for which $\mathrm{g}_c(\ell)_{\omega^5}$ is a 37th power.

(iii) Results for $p = 157$. For $p = 157$ (exponents of p-irregularity $62, 110$), one finds the partial analogous information after 590 distinct primes $\ell \in \mathscr{L}$ tested (proving also Vandiver's conjecture for a lot of times):

```
581 305 1140449   [9,3,2,6,8,3,1,4,5,9,3,1,3,1,5,3,4,4,
        2,2,1,2,5,5,3,2,2,1,5,7,6,2,2,1,5,5,5,4,4,3,3,4,5,4,5,5,
        5,5,5,3,6,1,5,3,5,4,5,0,2,3,5,7,3,3,3,2,4,4,7,6,6,5,6,1,7,4,6]
583 306 1142333   [9,3,2,6,8,3,1,4,5,9,3,1,3,1,5,3,4,4,
        2,2,1,2,5,5,3,2,2,1,5,7,6,2,2,1,5,5,5,4,4,3,3,4,5,4,5,5,
        5,5,5,3,6,1,5,3,5,4,5,0,2,3,5,7,3,3,3,2,4,4,7,6,6,5,6,1,7,4,7]
586 307 1150183   [9,3,2,6,8,3,1,4,5,9,3,1,3,1,6,3,4,4,
        2,2,1,2,5,5,3,2,2,1,5,7,6,2,2,1,5,5,5,4,4,3,3,4,5,4,5,5,
        5,5,5,3,6,1,5,3,5,4,5,0,2,3,5,7,3,3,3,2,4,4,7,6,6,5,6,1,7,4,7]
586 308 1150183   [9,3,2,6,8,3,1,4,5,9,3,1,3,1,6,3,4,4,
        2,2,1,2,5,5,3,2,2,1,5,7,6,2,2,1,5,5,5,4,4,3,3,4,5,4,5,5,
        5,5,5,3,6,1,6,3,5,4,5,0,2,3,5,7,3,3,3,2,4,4,7,6,6,5,6,1,7,4,7]
```

```
590 309 1161487   [9,3,2,6,8,3,1,4,5,10,3,1,3,1,6,3,4,4,
        2,2,1,2,5,5,3,2,2,1,5,7,6,2,2,1,5,5,5,4,4,3,3,4,5,4,5,5,
        5,5,5,3,6,1,6,3,5,4,5,0,2,3,5,7,3,3,3,2,4,4,7,6,6,5,6,1,7,4,7]
590 310 1161487   [9,3,2,6,8,3,1,4,5,10,3,1,3,1,6,3,4,4,
        2,2,1,2,5,5,3,2,2,1,5,7,6,2,2,1,5,5,5,4,4,3,3,4,5,4,5,6,
        5,5,5,3,6,1,6,3,5,4,5,0,2,3,5,7,3,3,3,2,4,4,7,6,6,5,6,1,7,4,7]
590 311 1161487   [9,3,2,6,8,3,1,4,5,10,3,1,3,1,6,3,4,4,
        2,2,1,2,5,5,3,2,2,1,5,7,6,2,2,1,5,5,5,4,4,3,3,4,5,4,5,6,
        5,5,5,3,6,1,6,3,5,4,5,0,2,3,5,7,3,3,3,2,4,5,7,6,6,5,6,1,7,4,7]
```

The remaining column of zeros (for $n/2 = 58$) stops at the following lines:

```
602 318 1185979   [9,3,2,6,8,3,2,4,6,10,3,1,
                    3,1,6,4,4,4,2,2,1,2,5,5,3,2,2,1,5,7,6,3,2,1,
                    5,5,5,4,4,3,3,4,5,4,5,6,5,5,5,3,6,1,6,4,5,4,6,0,
                    2,3,5,7,3,3,3,3,4,5,7,6,6,5,6,1,7,4,7]
602 319 1185979   [9,3,2,6,8,3,2,4,6,10,3,1,
                    3,1,6,4,4,4,2,2,1,2,5,5,3,2,2,1,5,7,6,3,2,1,
                    5,5,5,4,4,3,3,4,5,4,5,6,5,5,5,3,6,1,6,4,5,4,6,1,
                    2,3,5,7,3,3,3,3,4,5,7,6,6,5,6,1,7,4,7]
602 320 1185979   [9,3,2,6,8,3,2,4,6,10,3,1,
                    3,1,6,4,4,4,2,2,1,2,5,5,3,2,2,1,5,7,6,3,2,1,
                    5,5,5,4,4,3,3,4,5,4,5,6,5,5,5,3,6,1,6,4,5,4,6,1,
                   2,4,5,7,3,3,3,3,4,5,7,6,6,5,6,1,7,4,7]
```

One sees that these numbers depend on the orders of ω^n and/or ω^{p-n}, but this needs to be clarified taking a great lot of primes ℓ. The complete tables for $p = 37$ and $p = 157$ (40 pages) may be downloaded from:
https://www.dropbox.com/s/vs5eq6ornqx5922/vandiver.97.157.pdf?dl=0

4.5.4. *Vandiver's conjecture and p-adic regulator of K_+.* We return to the case $p = 37$ and $n_0 = 32$. From the relation (1), we see that ω^{32} is a character of order 9, hence a character of the real subfield k_9 of degree 9, which is such that $\mathcal{T}_{k_9} \neq 1$; so, k_9 admits a cyclic 37-ramified extension of degree 37 which is not unramified. To verify, we use [11, Program I], simplified for real fields, which indeed gives $\#\mathcal{T}_{k_9} = 37$ (take nt large enough):

```
{p=37;n=32;d=(p-1)/gcd(p-1,n);P=polsubcyclo(p,d);K=bnfinit(P,1);nt=6;
Kpn=bnrinit(K,p^nt);Hpn=component(component(Kpn,5),2);L=List;
e=component(matsize(Hpn),2);R=0;for(k=1,e-1,c=component(Hpn,e-k+1);
if(Mod(c,p)==0,R=R+1;listinsert(L,p^valuation(c,p),1)));
if(R>0,print("rk(T)=",R,"  K is not ",p,"-rational ",L));
if(R==0,print("rk(T)=",R,"  K is ",p,"-rational"))}

rk(T)=1 K is not 37-rational  List([37])
```

We find here another interpretation of the reflection theorem since we have the typical formula $\#\mathcal{T}_+ = \#\mathcal{C}\ell_+ \cdot \#\mathcal{R}$, where the p-group $\mathcal{R}$ is the normalized p-adic regulator of K_+ [14, Proposition 5.2]; thus the above data shows that the relation $\#\mathcal{T}_+ = 37$ comes from $\#\mathcal{R} = 37$, which is not surprising:

Remark 4.9. We have the analytic formula $\#\mathcal{C}\ell_{\chi_0} = \#(E_{\chi_0}/\langle\eta_{\chi_0}\rangle)$, where η is a suitable cyclotomic unit; so a classical method (explained in [24, Corollary 8.19] and applied in [3, 6]) consists in finding $\ell \in \mathscr{L}$ such that η_{χ_0} is not a local pth power at ℓ proving Vandiver's conjecture at χ_0; so when we find that $\mathcal{R} \neq 1$ (more precisely $\mathcal{R}_{\chi_0} \neq 1$), this means that η_{χ_0} generates E_{χ_0} and is a local pth power at p by p-primarity (whence $\#\mathcal{R} \equiv 0 \pmod p$).

5. Heuristics – Probability of a counterexample

5.1. **Standard probabilities.** We may suppose in a first approximation that, for a given p, the sets $\mathscr{E}_\ell(p)$ of exponents of p-primarity of primes $\ell \in \mathscr{L}$, are random with the same behavior as for the set $\mathscr{E}_0(p)$ of exponents of p-irregularity. More precisely, assume, as in Washington's book (see in [24], Theorem 5.17 and some statistical computations), that in terms of probabilities one has, for given primes p and $\ell \in \mathscr{L}$ (where $N := \frac{p-3}{2}$):

$$\begin{aligned}\text{Prob}(\#\mathscr{E}_0(p) = j) &= \tbinom{N}{j} \cdot \big(1 - \tfrac{1}{p}\big)^{N-j} \cdot \big(\tfrac{1}{p}\big)^{j},\\ \text{Prob}(\#\mathscr{E}_\ell(p) = k) &= \tbinom{N}{k} \cdot \big(1 - \tfrac{1}{p}\big)^{N-k} \cdot \big(\tfrac{1}{p}\big)^{k},\end{aligned}$$

this would imply that, for p given, $\mathscr{E}_\ell(p) \neq \emptyset$ for many $\ell \in \mathscr{L}$, but that $\mathscr{E}_\ell(p) = \emptyset$ in a proportion close to $e^{-\frac{1}{2}}$, which is in accordence with previous tables. Then the probability, for p and ℓ given, of $\mathscr{E}_0(p) \cap \mathscr{E}_\ell(p) \neq \emptyset$ with cardinalities $j \in [0, N]$ and $k \in [0, N]$ fixed, is $1 - \frac{(N-k)! \cdot (N-j)!}{N! \cdot (N-k-j)!}$. So, an approximation of the whole probability of $\mathscr{E}_0(p) \cap \mathscr{E}_\ell(p) \neq \emptyset$ is:

$$\sum_{j,k \geq 0} \tbinom{N}{j}\tbinom{N}{k} \cdot \big(1 - \tfrac{1}{p}\big)^{2N-j-k} \cdot \big(\tfrac{1}{p}\big)^{j+k} \cdot \big(1 - \tfrac{(N-k)!\cdot(N-j)!}{N!\cdot(N-k-j)!}\big). \tag{10}$$

The computations show that this expression is around $\frac{1}{2p}$, which does not allow to conclude easily for a single ℓ, but this does not take into account the infiniteness of $\mathscr{L}$ giving, a priori, independent information. The following program shows a rapid convergence as t grows taking j and k independent in $[0, t]$:

```
{p=1000003;N=(p-3)/2;for(t=1,30,S=0.0;for(k=0,t,Pk=binomial(N,k)*
(1-1/p)^(N-k)*(1/p)^k;for(j=0,t,S=S+Pk*binomial(N,j)*(1-1/p)^(N-j)*(1/p)^j*
(1-factorial(N-k)*factorial(N-j)/(factorial(N)*factorial(N-k-j)))));
print(t," ",S," ",0.5/p," ",0.5/p-S))}
```

$S = 4.9999687501 \times 10^{-7}$, $\frac{1}{2p} = 4.9999850000 \times 10^{-7}$, $\frac{1}{2p} - S = 1.6249892292 \times 10^{-12}$. for $t = 18$.

5.2. **New heuristics.** There are several reasons to say that the generic probability $\frac{1}{p}$ must be replaced by a much lower one:

(i) For some characters $\chi = \omega^n =: \omega^{p-(1+h)} \in \mathscr{X}_+$, $h = 2, 4, \ldots$, when $p \gg_h 0$, one may prove that $\mathcal{C}\ell_{\omega^{p-(1+h)}} = 1$, as the case of $\mathcal{C}\ell_{\omega^{p-3}} = 1$ proved

unconditionally by Kurihara (see [19, 8, 22, 23, 2] among other authors applying the same approach via K-theory) [2]; the order of ω^n is:

$$\frac{p-1}{\gcd\,(p-1,h)} = \frac{p-1}{h'},\ h' \mid h$$

(see the data of § 4.5.3 for $p = 37$ and 157).

(ii) At the opposite, for $\chi \in \mathscr{X}_+$ of small order, $\mathscr{C}\!\ell_\chi$ may be trivial because of the "archimedean" order of magnitude of the whole class group of the subfield of K_+ fixed by the kernel of χ (proved for the quadratic case when $p \equiv 1 \pmod 4$, the cubic case when $p \equiv 1 \pmod 3$, ...). Moreover, we have the ϵ-conjecture of [7], for p-class groups, that we state for the real abelian fields k_d *of constant* degree d, of discriminant $D = p^{d-1}$, when p increases:

For all $\epsilon > 0$ *there exists* $C_{\epsilon,p}$ *such that* $\log(\#\mathscr{C}\!\ell_{k_d}) \leq \log(C_{\epsilon,p}) + \epsilon \cdot \log(p)$,

which would give $\mathscr{C}\!\ell_{k_d} = 1$ for $\log(p) > \dfrac{\log(C_{\epsilon,p})}{1-\epsilon}$ and any $\epsilon < 1$.

(iii) The previous probabilities (10) assume that when $\ell \in \mathscr{L}$ varies, the sets $\mathscr{E}_\ell(p)$ are *random and independent*, which is not the case when p is irregular at some $\chi_0^* = \omega^{p-n_0}$ (for $\chi_0 = \omega^{n_0} \in \mathscr{X}_+$) as we have seen; to simplify we assume the Hypothesis 1.2 giving $b_c(\chi_0^*) = p\,u$, where u is a p-adic unit.

Fix $\ell \in \mathscr{L}$ such that $\mathfrak{L}_{\chi_0^*}$ generates $\mathscr{C}\!\ell_{\chi_0^*} \simeq \mathbb{Z}/p\mathbb{Z}$; put (Proposition 2.4):

$$\mathrm{g}_c(\ell)_{\chi_0^*} = 1 + \beta_0(\ell) \cdot \varpi^{p-n_0},\ \beta_0(\ell) \in \mathbb{Z}_p[\varpi],$$

where $\beta_0(\ell)$ is invertible modulo ϖ if and only if $\mathrm{g}_c(\ell)_{\chi_0^*}$ is non-p-primary.

Whatever ℓ' and $\mathfrak{L}' \mid \ell'$, one has, from the computations done in § 4.5.1 (ii) $\mathrm{g}_c(\ell')_{\chi_0^*} \equiv \mathrm{g}_c(\ell)^r_{\chi_0^*} \pmod p$, $r \in \mathbb{Z}/p\mathbb{Z}$, giving:

$$\mathrm{g}_c(\ell')_{\chi_0^*} =: 1 + \beta_0(\ell') \cdot \varpi^{p-n_0},\ \ \beta_0(\ell') \equiv r \cdot \beta_0(\ell) \pmod \varpi. \tag{11}$$

Contrary to the classical idea that the values of $\beta_0(\ell)$ modulo ϖ follow standard probabilities $\frac{1}{p}$, the heuristic that we propose is the following:

For each $\chi \in \mathscr{X}_+$, *the congruential values, at* $\chi^* = \omega\,\chi^{-1}$, *of the Gauss sums (more precisely of the* $\mathrm{g}_c(\ell)$ *as product* $J_1 \cdots J_{c-1}$ *of Jacobi sums), are independent of the p-class of* $\mathfrak{L} \mid \ell$ *and are uniformly (or at least with explicit non-trivial densities) distributed, when* $\ell \in \mathscr{L}$ *varies.*

Because of the density theorems on the ideal classes, we must examine two cases concerning the χ-components of $\mathscr{C}\!\ell$, for $\chi \in \mathscr{X}_+$, when there exists $\chi_0 = \omega^{n_0} \in \mathscr{X}_+$ such that $\mathscr{C}\!\ell_{\chi_0^*} \simeq \mathbb{Z}/p\mathbb{Z}$:

[2] I thank Christian Maire for pointing out to me the reference [2] improving the bounds of Soulé. Unfortunately these bounds are not usable in practice, but demonstrate the existence of a fundamental general principle

(a) $\chi \neq \chi_0$ and $\mathcal{C}\ell_{\chi^*} = 1$. The numerical experiments show that when $\ell \in \mathscr{L}$ varies, $\mathrm{g}_c(\ell)_{\chi^*} \equiv 1+\beta(\ell)\cdot\varpi^{p-n} \pmod p$, with random $\beta(\ell) \pmod\varpi$ in $\mathbb{Z}/p\mathbb{Z}$ (probabilities $\frac{O(1)}{p}$ depending on the orders of the characters).

(b) $\chi = \chi_0$ and $\mathcal{C}\ell_{\chi_0^*} \simeq \mathbb{Z}/p\mathbb{Z}$. If $\mathrm{g}_c(\ell)_{\chi_0^*}$ is p-primary for some given non-principal $\mathfrak{L}_{\chi_0^*}$, then from (11) all the $\mathrm{g}_c(\ell')_{\chi_0^*}$ are p-primary, whatever the class of $\mathfrak{L}'_{\chi_0^*}$ (p possibilities) because $\beta_0(\ell) \equiv 0 \pmod\varpi$. So, n_0 is always an exponent of p-primarity and $\mathscr{E}_0(p) \cap \mathscr{E}_\ell(p) \neq \emptyset$ for all $\ell \in \mathscr{L}$ (which corresponds to the non-cyclicity of $\mathcal{C}\ell^{(p)}_{\chi_0^*}$).

Thus, to have the same density of p-primarity on $\mathscr{L}$ (as for the p-principal case (a)), $\beta_0(\ell) \equiv 0 \pmod\varpi$ must occur p times less, giving the probability in $\frac{O(1)}{p^2}$ instead of $\frac{O(1)}{p}$; it is even possible that such a circumstance be of probability 0 depending on more precise properties of Gauss sums. Otherwise, their behaviour should be excessively disturbed and in an algorithmic framework, we suggest that the congruential properties of the Gauss sums (mod p) "determine" the properties of the p-class group of K instead of the contrary, and perhaps imply the cyclicity of each $\mathcal{C}\ell^{(p)}_{\chi^*}$ (see Proposition 3.4). Of course, the probabilities $\frac{O(1)}{p}$ and $\frac{O(1)}{p^2}$ are to be precised regarding the orders of the characters.

Otherwise, under the assumption $\mathrm{g}_c(\ell)_{\chi_0^*}$ p-primary, the corresponding component n_0 of the list counting the p-primarities, increases at each step. For instance, if for $p = 37$ the exponent $n_0 = 32$ of 37-irregularity was an exponent of p-primarity, then the last line of the data § 4.5.3 would be the awful result about the 16th component (equal to $75 + 1432 = 1507$):

```
L=[83,96,86,91,80,80,86,83,92,83,98,76,83,78,86,1507,76]
```

Let $x(\ell)$ be the mean value of the components of the list L and let N_ℓ be the number of primes ℓ tested at this step. Then from the above, $x(\ell) \approx 84$ and this would give a 16th component $x_0(\ell) \approx x(\ell) \cdot \frac{p-1}{2}$ as $\ell \to \infty$ (here, $\frac{75+1432}{84} \approx 17.94$). Then we may estimate $x(\ell)$ very approximatively equal to $\frac{2N}{p}$ where N is the number of exponents of p-primarity obtained in the selected interval of primes ℓ, and we may put $N_\ell \approx O(1)\cdot N$; whence $x(\ell) \approx \frac{2}{p}\cdot N_\ell \cdot (1+O(1))$ giving the pathological component $x_0(\ell) \approx N_\ell \cdot (1+O(1))$.

6. Conclusion

Under these experiments and heuristics, the existence of sets $\mathscr{E}_\ell(p)$, disjoint from $\mathscr{E}_0(p)$, or probably the existence of primes $\ell \in \mathscr{L}$ such that $\mathscr{E}_\ell(p) = \emptyset$ (see the numerical results § 4.4.2), may occur conjecturally for all p.

Let us define the "main algorithm", associated to the test of Vandiver's conjecture for p, as the passage from ℓ to the next ℓ' in $\mathscr{L}$, the crucial step

being the computation of the Jacobi sums ($1 \le i \le c-1$):

$$J_i = - \sum_{x \in \mathbb{F}_\ell \setminus \{0,1\}} \zeta_p^{i \cdot \mathrm{lg}(x) + \mathrm{lg}(1-x)} \quad \& \quad J'_i = - \sum_{x' \in \mathbb{F}_{\ell'} \setminus \{0,1\}} \zeta_p^{i \cdot \mathrm{lg}'(x') + \mathrm{lg}'(1-x')},$$

where lg and lg$'$ are the discrete logarithms for ℓ and ℓ'; then we have $\mathrm{g}_c(\ell) = J_1 \cdots J_{c-1}$. Since the $\mathrm{g}_c(\ell)$ have, a priori, no "algebraic link", this suggests randomness and applies for many independent primes ℓ.

Remark 6.1. There are two constraints, for the Gauss sums and Jacobi sums that we have considered, but they only concern the auxiliary numbers $\ell \in \mathscr{L}$:

(i) The ideal factorization of $\tau(\psi)$ *is related to congruences modulo the conjugates of a prime ideal* $\mathfrak{L} \mid \ell$ *and is canonical* (this yields to Stickelberger's theorem [24, § 15.1], [4]).

(ii) The p-classes (finite in number) of ideals $\mathfrak{L} \mid \ell$ for $\ell \in \mathscr{L}$ are all represented with standard densities (Lemma 4.4).

However, since we consider characters ψ of order p, the *p-adic congruential properties* of Gauss sums (or Jacobi sums) do not follow any law (in our opinion and according to classical literature), what explains that the negation of the distribution properties, for at least one irregular prime p, implies a very tricky complexity of the algorithm, as the fact that $\mathscr{E}_\ell(p) \cap \mathscr{E}_0(p) \ne \emptyset$ for all $\ell \in \mathscr{L}$ (or the weaker property $\mathscr{E}_\ell(p) \ne \emptyset$ for all $\ell \in \mathscr{L}$), which comes from the non-cyclicity of some $\mathcal{C}\ell^{(p)}_{\chi_0^*}$.

This may have crucial consequences in various domains:

(i) In a geometrical viewpoint, the Riemann hypothesis for Fermat curves [24, § 6.1] gives a basic link with Jacobi sums;

(ii) Vandiver's conjecture is often strongly necessary (e.g., in [5] about the Galois cohomology of the homology of Fermat curves, then in several papers on Galois p-ramification theory as in [21]).

Then it may be legitimate to think that all these numerous basic congruential aspects are (logically) governing principles of a wide part of algebraic number theory beyond the case of the pth cyclotomic field (not to mention all the geometrical aspects):

Gauss and Jacobi sums $\longrightarrow$ *Stickelberger element* $\longrightarrow$ *p-adic L-functions* $\longrightarrow$ *Herbrand theorem & Main theorems on abelian fields* $\longrightarrow$ *annihilation of the p-torsion group* $\mathcal{T} = \mathrm{H}^2(G_{S_p}, \mathbb{Z}_p)^*$ *of real abelian fields* $\longrightarrow$ *p-rationality of number fields ($\mathcal{T} = 1$)* $\longrightarrow$ *cohomological obstructions for Galois theory* $\longrightarrow \cdots$

Which gives again an example of a basic p-adic problem analogous to those we have analysed for various conjectures: Greenberg's conjectures

(in Iwasawa theory over totally real fields and representation theory), p-rationalities of a number field as p varies, existence of a p-adic Brauer–Siegel theorem (see [15] and its bibliography).

The truth of Vandiver's conjecture may come, for $p \gg 0$, from Borel–Cantelli heuristics on properties of probabilities much less than $\frac{O(1)}{p^2}$, but this point of view allows cases of failure of Vandiver's conjecture, which is not satisfactory for the theoretical fondations of the above subjects. Possibly, there is an universal property of the sets $\mathscr{E}_\ell(p)$ coming from the important fact that all primes $\ell \in \mathscr{L}$ intervene for each p.

To be very optimistic (but not very rigorous), one can perhaps say that Vandiver's conjecture is true because it has been verified for sufficiently many prime numbers [3, 6]. In a more serious statement, we may assert that Vandiver's conjecture holds for almost all primes; the precise finite cardinality of the set of counterexamples ($\emptyset$ or not) is (in our opinion) not of algebraic nature nor enlightened by class field theory or Iwasawa's theory, but is perhaps accessible by the way of analytical techniques or depends on an hypothetic "complexity theory" in algebraic number theory.

References

[1] B. Anglès and F.A.E. Nuccio, *On Jacobi Sums in* $\mathbb{Q}(\zeta_p)$, Acta Arithmetica **142** (2010), no. 3, 199–218. https://perso.univ-st-etienne.fr/nf51454h/PDF/jacobi.pdf

[2] E. Bayer–Fluckiger, V. Emery and J. Houriet, *Hermitian Lattices and Bounds in K-Theory of Algebraic Integers*, Documenta Math. Extra Volume Merkurjev (2015), 71–83. https://www.math.uni-bielefeld.de/documenta/vol-merkurjev/

[3] J.P. Buhler and D. Harvey, *Irregular primes to* 163 *million* Math. Comp. **80** (2011), no. 276, 2435–2444. http://www.ams.org/journals/mcom/2011-80-276/S0025-5718-2011-02461-0/

[4] K. Conrad, *Jacobi sums and Stickelberger's congruence*, Enseign. Math. **41** (1995), 141–153. http://www.math.uconn.edu/~kconrad/articles/jacobistick.pdf

[5] R. Davis and R. Pries, *Cohomology groups of Fermat curves via ray class fields of cyclotomic fields* (preprint 2018).

[6] W. Hart, D. Harvey and W. Ong, *Irregular primes to two billion* (2016). https://arxiv.org/abs/1605.02398

[7] J. S. Ellenberg and A. Venkatesh, *Reflection principles and bounds for class group torsion*, Int. Math. Res. Not. (1) (2007). http://math.stanford.edu/~akshay/research/sch.pdf

[8] E. Ghate, *Vandiver's Conjecture via K-theory*, Summer School on Cyclotomic fields, Pune (1999).http://www.math.tifr.res.in/%7Eeghate/vandiver.pdf

[9] G. Gras et J-F. Jaulent, *Sur les corps de nombres réguliers*, Math. Z. **202** (1989), 343–365. https://eudml.org/doc/174095

[10] G. Gras, *Class Field Theory: from theory to practice*, corr. 2nd ed., Springer Monographs in Mathematics, Springer, 2005, xiii+507 pages. https://www.researchgate.net/publication/268005797

[11] G. Gras, *On p-rationality of number fields. Applications – PARI/GP programs*, Publ. Math. Fac. Sci. Besançon (Théorie des Nombres), Années 2017/2018 (to appear). https://arxiv.org/pdf/1709.06388.pdf

[12] G. Gras, *Annihilation of* $\mathrm{tor}_{\mathbb{Z}_p}(\mathcal{G}_{K,S}^{\mathrm{ab}})$ *for real abelian extensions* $K/\mathbb{Q}$ (preprint 2018). https://arxiv.org/pdf/1806.03137.pdf
[13] G. Gras, *Sur la p-ramification abélienne*, Conférence donnée à l'University Laval, Québec, Mathematical series of the department of mathematics **20** (1984), 1–26. https://www.dropbox.com/s/hecx46bex3ptzdw/Conf%C3%A9rences1982.Canada.Univ.Laval.pdf?dl=0
[14] G. Gras, *The p-adic Kummer-Leopoldt Constant: Normalized p-adic Regulator*, Int. J. Number Theory **14** (2018), no. 2, 329–337. https://doi.org/10.1142/S1793042118500203
[15] G. Gras, *Heuristics and conjectures in direction of a p-adic Brauer–Siegel theorem*, Math. Comp. (to appear).https://doi.org/10.1090/mcom/3395
[16] R. Greenberg, *On the jacobian variety of some algebraic curves*, Compositio Math. **42** (1980), 345–359. http://www.numdam.org/article/CM_1980__42_3_345_0.pdf
[17] H. Ichimura, *Local Units Modulo Gauss Sums*, Journal of Number Theory **68** (1998), 36–56.https://doi.org/10.1006/jnth.1997.2206
[18] K. Iwasawa, *A note on Jacobi sums*, Symposia Mathematica **15**, Academic Press (1975), 447–459.
[19] M. Kurihara, *Some remarks on conjectures about cyclotomic fields and K-groups of* $\mathbb{Z}$, Compositio Math. **81** (1992), 223–236. http://www.numdam.org/item/CM_1992__81_2_223_0
[20] The PARI Group, *PARI/GP, version* `2.9.0`, Université de Bordeaux (2016). http://pari.math.u-bordeaux.fr/
[21] R. T. Sharifi, *Relationships between conjectures on the structure of pro-p Galois groups unramified outside p* (preprint 2018).
[22] C. Soulé, *Perfect forms and the Vandiver conjecture*, J. Reine Angew. Math. **517** (1999), 209–221. https://doi.org/10.1515/crll.1999.095
[23] C. Soulé, *A bound for the torsion in the K-theory of algebraic integers*, Documenta Math. Extra, vol. Kato (2003), 761–788.
[24] L.C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math. 83, Springer enlarged second edition 1997.

Villa la Gardette, Chemin Château Gagnière F–38520 Le Bourg d'Oisans, France, https://www.researchgate.net/profile/Georges_Gras
E-mail address: g.mn.gras@wanadoo.fr