Proc. Indian Acad. Sci. (Math. Sci.) (2020) 130:32
https://doi.org/10.1007/s12044-020-0561-1

New criteria for Vandiver's conjecture using Gauss sums – Heuristics and numerical experiments

GEORGES GRAS

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

MS received 6 June 2019; revised 4 December 2019; accepted 30 December 2019

Abstract. The link between Vandiver's conjecture and Gauss sums is well known since the papers of Iwasawa (Symposia Mathematica, vol 15, Academic Press, pp 447–459, 1975), Thaine (Mich Math J 42(2):311–344, 1995; Trans Am Math Soc 351(12):4769–4790, 1999) and Anglès and Nuccio (Acta Arith 142(3):199–218, 2010). This conjecture is required in many subjects and we shall give such examples of relevant references. In this paper, we recall our interpretation of Vandiver's conjecture in terms of minus part of the torsion of the Galois group of the maximal abelian p-ramified pro-p-extension of the p-th cyclotomic field (Sur la p-ramification abélienne (1984) vol. 20, pp. 1–26). Then we provide a specific use of Gauss sums of characters of order p of $\mathbb{F}_\ell^\times$ and prove new criteria for Vandiver's conjecture to hold (Theorem 2 (a) using both the sets of exponents of p-irregularity and of p-primarity of suitable twists of the Gauss sums, and Theorem 2 (b) which does not need the knowledge of Bernoulli numbers or cyclotomic units). We propose in §5.2 new heuristics showing that any counterexample to the conjecture leads to excessive constraints modulo p on the above twists as ℓ varies and suggests analytical approaches to evidence. We perform numerical experiments to strengthen our arguments in the direction of the very probable truth of Vandiver's conjecture and to inspire future research. The calculations with their PARI/GP programs are given in appendices.

Keywords. Cyclotomic field of p-th roots of unity; Vandiver's conjecture; Gauss sums; Jacobi sums; Kummer theory; class field theory; p-ramification.

Mathematics Subject Classification. 11R18, 11L05, 11R37, 11R29, 08-04.

1. Introduction

Let $K = \mathbb{Q}(\mu_p)$ be the field of p-th roots of unity for a given prime $p > 2$ and let K_+ be its maximal real subfield. Put $G = \mathrm{Gal}\,(K/\mathbb{Q})$.

We denote by $\mathcal{C}\ell$ and $\mathcal{C}\ell_+$ the p-class groups of K and K_+, then by $\mathcal{C}\ell_-$ the relative p-class group, so that $\mathcal{C}\ell = \mathcal{C}\ell_+ \oplus \mathcal{C}\ell_-$.

Let E and E_+ be the groups of units of K and K_+; then $E = E_+ \oplus \mu_p$ (Kummer). The conjecture of Vandiver (or Kummer–Vandiver) asserts that $\mathcal{C}\ell_+$ is trivial. This statement is equivalent to saying that the group of real cyclotomic units of K is of prime to p index in E_+ [55, Theorem 8.14]. One may refer to numerical tables using this property in [5,26] (verifying the conjecture up to $2 \cdot 10^9$), and to more general results in [50,51] where

Published online: 06 May 2020

some relations with Gauss and Jacobi sums are used to express the order of the isotypic components of $\mathcal{C}\ell_+$ (e.g., [50, Theorem 4]).

Many heuristics are proposed about this conjecture (see Washington's book [55, § 8.3, Corollary 8.19] for some history, criteria and for probabilistic arguments, then [39] assuming Greenberg's conjecture [22] for K_+).

We have also given a probabilistic study in [14, II.5.4.9.2]. All these heuristics lead to the fact that the number of primes p less than x, giving a counterexample, can be of the form $O(1) \cdot \log(\log(x))$.

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 heuristics and conjectures (on class groups and units) may contradict such unfounded approaches.

In this paper, we shall work in another direction, in the framework of 'abelian p-ramification', using Gauss sums together with the *main theorem on abelian number fields* restricted to $\mathcal{C}\ell_-$, and giving the order of its isotypic components by means of generalized Bernoulli numbers. Thus the annihilation of these components will be of significant importance for our method (this classical result is related by Ribet [40,41] and we shall call it 'main theorem' in short).

Such a link of Vandiver's conjecture with Gauss sums and abelian p-ramification has been given first by Iwasawa [29], then by Anglès–Nuccio [1], and encountered by many authors in various directions (Iwasawa's theory, Galois cohomology, Fermat curves, Galois representations, etc.), then often assuming Vandiver's conjecture (e.g., [8,23,24,27,28,32, 44–47,53,54]).

This link does exist also in the context of the classical conjecture of Greenberg [22] considered as a generalization of Vandiver's conjecture (e.g., [15,16,36]). We propose, in Section 3.1, to explain the links with p-ramification and prove again the reflection theorem (Theorem 8 and Corollary 9).

Then we shall interpret a counterexample to Vandiver's conjecture in terms of non-trivial 'p-primary pseudo-units' stemming from Gauss sums:

$$\tau(\psi) = -\sum_{x \in \mathbb{F}_\ell^\times} \psi(x)\, \xi_\ell^x,$$

for ψ of order p, ξ_ℓ of prime order $\ell \equiv 1 \pmod{p}$. 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 a cyclic unramified extension L_+/K_+ of degree p predicted by class field theory); the converse being obvious.

Since α can be obtained explicitly by means of twists (giving products of Jacobi sums) of the above Gauss sums:

$$\mathrm{g}_c(\ell) = \tau(\psi)^{c-\sigma_c} \in K^\times, \tag{1}$$

with Artin automorphisms σ_c attached to a primitive root c modulo p. This will yield the main test verifying the validity of the conjecture at p; this result is the object of Theorem 21, Corollary 22 and Theorem 23, that we can summarize, in Theorem 2 below, after the reminder of some notations and classical definitions.

DEFINITION 1

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

The irreducible p-adic characters of G are $\theta = \omega^m$, $1 \leq m \leq p-1$.

(ii) Let $e_\theta = \frac{1}{p-1}\sum_{s\in G} \theta(s^{-1})\, s$ be the associated idempotents in $\mathbb{Z}_p[G]$.

(iii) Let $\mathrm{g}_c(\ell)_\theta$ denote the θ-component of the twist $\mathrm{g}_c(\ell)$ defined by (1), as representative in $K^\times$ of the class $\overline{\mathrm{g}_c(\ell)}^{\,e_\theta} \in K^\times/K^{\times p}$.

Theorem 2 (Main results). *For a prime $\ell \equiv 1 \pmod p$, let $\mathscr{E}_\ell(p)$ be the set of exponents of p-primarity of ℓ (i.e., the even integers $n \in [2,\, p-3]$, such that $\mathrm{g}_c(\ell)_{\omega^{p-n}} \equiv 1 \pmod p$). Then let $\mathscr{E}_0(p)$ be the set of exponents of p-irregularity of K (i.e., the even integers $n \in [2,\, p-3]$, such that p divides the n-th Bernoulli number B_n).*

(a) *Vandiver's conjecture holds for K if and only if there exists $\ell \equiv 1 \pmod p$ such that $\mathscr{E}_\ell(p) \cap \mathscr{E}_0(p) = \emptyset$ (this is Theorem 21).*

(b) *Vandiver's conjecture holds for K if and only if there exist $N \geq 1$ primes $\ell_i \equiv 1 \pmod p$ such that $\bigcap_{i=1}^N \mathscr{E}_{\ell_i}(p) = \emptyset$ (this is Theorem 23).*

See the computational aspects of this theorem (heuristics, PARI/GP programs and tables) in "Appendix A".

Test (b) is numerically very frequent for $N = 1$ or N very small, *and does not need the knowledge of Bernoulli numbers*; in fact, it does not need to know if p is irregular or not.

We show that some assumption of *independence* of the congruential properties (mod p) of these twists, as ℓ varies, is an obstruction to any counterexample to Vandiver's conjecture.

This method is different from that needed to prove that some cyclotomic unit is not a global p-th power, which does not give obvious probabilistic approach (nevertheless, see § 5.2.4 for some complements).

Finally, we propose in § 5.2 and § 5.3, new heuristics (to our knowledge) and give substantial numerical experiments confirming them.

Now we give the main definitions and notations used throughout the rest of the article.

DEFINITION 3

(i) We denote by $\mathscr{X}_+$ the set of even characters $\theta \neq 1$ (i.e., $\theta = \omega^m$, $m \in [2,\, p-3]$ even), and by $\mathscr{X}_-$ the set of odd characters distinct from ω (i.e., $\theta = \omega^m$, $m \in [3,\, p-2]$ odd).

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 $\mathscr{X}_+^* = \mathscr{X}_-$.

(ii) For a finitely generated $\mathbb{Z}_p[G]$-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 $M = M_+ \oplus M_-$.

(iii) We denote by $\mathrm{rk}_p(A) = \dim_{\mathbb{F}_p}(A/A^p)$ the p-rank of any abelian group A.

(iv) For $\alpha \in K^\times$, prime to p, considered modulo $K^{\times p}$, we denote by α_θ a representative in $K^\times$ of the class $\overline{\alpha}^{\,e_\theta} \in K^\times/K^{\times p}$ (e.g., $\alpha_\theta = \alpha^{e'_\theta}$ where $e'_\theta \in \mathbb{Z}[G]$ approximates $e_\theta \bmod p$).

(v) Let I be the group of prime to p ideals of K. For any $\mathfrak{A} \in I$ such that $c\ell(\mathfrak{A}) \in \mathcal{C}\ell$, there exists an approximation $e'_\theta \in \mathbb{Z}[G]$ of e_θ modulo a sufficient high power of p such that $\mathfrak{A}_\theta = \mathfrak{A}^{e'_\theta}$ is defined up to a principal ideal of the form (x^p), $x \in K^\times$.

(vi) We say that $\mathfrak{A} \in I$ is p-principal if it is principal in $I \otimes \mathbb{Z}_p$; thus $\mathfrak{A} = (\alpha)$, with $\alpha \in K^\times \otimes \mathbb{Z}_p$, defined up to the product by $\varepsilon \in E \otimes \mathbb{Z}_p$. (The distinction between $\mathfrak{A}^{e_\theta} \in I \otimes \mathbb{Z}_p$ and $\mathfrak{A}^{e'_\theta} \in I$ ($e'_\theta \equiv e_\theta \pmod{p^N \mathbb{Z}_p[G]}$, N large enough) has some importance in practice and programming, provided of a definition of $\mathfrak{A}^{e'_\theta}$ up to a principal ideal of the form (x^p), for deciding, for instance, in the writing $\mathfrak{A}^{e_\theta} =: (\alpha_\theta)$ of the 'p-primarity' of $\alpha_\theta \in K^\times \otimes \mathbb{Z}_p$; whence $\mathfrak{A}^{e'_\theta} =: (\alpha')$ where $\alpha_\theta \cdot \alpha'^{-1} \in (K^\times \otimes \mathbb{Z}_p)^p \cdot E \otimes \mathbb{Z}_p$. This will be used for $\theta \in \mathscr{X}_+^*$ where θ-components of units do not intervene, giving $(\alpha_\theta) = (x)^p \Leftrightarrow \alpha_\theta \in K^{\times p}$.)

(vii) For $\chi =: \omega^n \in \mathscr{X}_+$, let $B_{1,(\chi^*)^{-1}} = B_{1,\omega^{n-1}} = \frac{1}{p} \sum_{a=1}^{p-1} (\chi^*)^{-1}(s_a)\, a$ be the generalized Bernoulli number of character $(\chi^*)^{-1}$ (where $s_a \in G$ is the Artin automorphism attached to a; it is the restriction of the Artin automorphism σ_a defined above in larger extensions). The Bernoulli number $B_{1,\omega^{n-1}}$ is an element of $\mathbb{Z}_p$ congruent modulo p to $\frac{B_n}{n}$, where B_n is the n-th ordinary Bernoulli number; see [55, Proposition 4.1, Corollary 5.15].

The index of p-irregularity $i(p)$ is the number of even $n \in [2, p-3]$ such that $B_n \equiv 0 \pmod{p}$; thus $i(p) = \#\mathscr{E}_0(p)$. See [55, § 5.3, Exercise 6.6] giving statistics and the heuristic $i(p) = O\big(\frac{\log(p)}{\log(\log(p))}\big)$.

(viii) We say that a finitely generated $\mathbb{Z}_p[G]$-module M is monogenous if it is generated over $\mathbb{Z}_p[G]$ by a single element; this is equivalent to $\mathrm{rk}_p(M_\theta) \leq 1$ for all irreducible p-adic characters θ of G.

In this context, if for $\theta \in \mathscr{X}_-$, $B_{1,\theta^{-1}}$ is of p-valuation e, we shall have (Main Theorem):

$$\#\mathcal{C}\ell_\theta = \big|B_{1,\theta^{-1}}\big|_p^{-1} = p^e.$$

For a more general history of Bernoulli–Kummer–Herbrand–Ribet, then Mazur–Wiles–Thaine–Kolyvagin–Rubin–Greither works on cyclotomy, see [12,41,55].

2. Pseudo-units: Notion of p-primarity

DEFINITION 4

(i) We call *pseudo-unit* for any $\alpha \in K^\times$, prime to p, such that (α) is the p-th 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).

Remark 5.

(i) Let A be the group of pseudo-units of K. If $\alpha \in A$, there exists an ideal $\mathfrak{a}$ such that $(\alpha) = \mathfrak{a}^p$; then if we associate with $\alpha K^{\times p}$ the class of $\mathfrak{a}$, we obtain 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

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

Thus the computation of $\dim_{\mathbb{F}_p}\big((AK^{\times p}/K^{\times p})_\theta\big)$ is immediate from the value of $\mathrm{rk}_p(\mathcal{C}\ell_\theta)$ and $\dim_{\mathbb{F}_p}\big((E/E^p)_\theta\big) = 1$ (resp. 0) if $\theta \in \mathscr{X}_+ \cup \{\omega\}$ (resp. $\theta \in \mathscr{X}_+^* \cup \{1\}$).

(ii) The general condition of p-primarity for any $\alpha \in K^\times$ (α prime to p but not necessarily a pseudo-unit) is 'α congruent to a p-th power modulo $\mathfrak{p}^p = (p)\,\mathfrak{p}$' (e.g., [14, Ch. I, § 6, (b), Theorem 6.3]). Since in any case (replacing α by α^{1-p}) we can assume $\alpha \equiv 1 \pmod{\mathfrak{p}}$, the above condition is then equivalent to $\alpha \equiv 1 \pmod{\mathfrak{p}^p}$ (indeed, for any $x \equiv 1 \pmod{\mathfrak{p}}$ we get $x^p \equiv 1 \pmod{\mathfrak{p}^p}$).

For the pseudo-units of K, the p-primarity may be characterized as follows.

PROPOSITION 6

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

Proof. One direction is trivial. Suppose that $K(\sqrt[p]{\alpha})/K$ is unramified at $\mathfrak{p}$; since $\alpha = \mathfrak{a}^p$, 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* $\mathfrak{p} = (\zeta_p - 1)$ is trivial; so $\mathfrak{p}$ totally splits in H/K, thus in $K(\sqrt[p]{\alpha})/K$, proving the proposition. □

When α is not necessarily a pseudo-unit, we have a similar result provided we only look at the p-primarity of α_θ for $\theta \neq 1, \omega$.

PROPOSITION 7

Let $\alpha \equiv 1 \pmod{\mathfrak{p}}$. Let $m \in [2, p-2]$ and let α_θ for $\theta = \omega^m$. Then $\alpha_\theta \equiv 1 \pmod{\mathfrak{p}^m}$; moreover α_θ is p-primary if and only if $\alpha_\theta \equiv 1 \pmod{p}$, in which case one gets $\alpha_\theta \equiv 1 \pmod{\mathfrak{p}^{m+p-1} = (p)\mathfrak{p}^m}$.

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 $u_0 \in \mathbb{Z} \backslash p\,\mathbb{Z}$ be such that $u \equiv u_0 \pmod{\varpi}$ giving $\alpha_\theta \equiv 1 + \varpi^k u_0 \pmod{\varpi^{k+1}}$. Since $\alpha_\theta^s = \alpha_\theta^{\theta(s)}$ in $K^\times \otimes \mathbb{Z}_p$, 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 $\alpha_\theta = 1 + \varpi^k u$, $k \in \{m, m+p-1, \ldots\}$; whence the first claim. The p-primarity condition for α_θ is $\alpha_\theta \equiv 1 \pmod{\varpi^p}$ giving the obvious direction 'α_θ p-primary $\Rightarrow \alpha_\theta \equiv 1 \pmod{p}$', since $(\varpi^p) = (p\,\varpi)$.

Suppose $\alpha_\theta \equiv 1 \pmod{\varpi^{p-1}}$; so $k = m$ does not work in the writing $\alpha_\theta = 1 + \varpi^k u$ since $m \leq p-2$, and necessarily k is at least $m + p - 1 \geq p + 1$, because $m \geq 2$ (which is also the local p-th power condition). □

3. Abelian p-ramification

Let us give an overview of the theory of abelian p-ramification, which is not our main purpose, but the natural framework for Vandiver's conjecture and Gauss sums.

3.1 *Vandiver's conjecture and abelian p-ramification*

Let U be the group of principal local units at p of K and let $\bar{E}$ be the closure of the image of E in U. 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. This extension contains the p-Hilbert class field H and the compositum $\tilde{K}$ of the $\mathbb{Z}_p$-extensions of K. In the case of $K = \mathbb{Q}(\mu_p)$, the theory is summarized by the following exact sequences (Leopoldt's conjecture holds for abelian fields, giving $\mathrm{tor}_{\mathbb{Z}_p}(\bar{E}) = \mathrm{tor}_{\mathbb{Z}_p}(E) = \mu_p$):

$$1 \longrightarrow \mathrm{tor}_{\mathbb{Z}_p}\big(U \big/ \bar{E}\big) \longrightarrow \mathcal{T} \longrightarrow \widetilde{\mathcal{C}\ell} \longrightarrow 1$$

$$1 \longrightarrow \mathrm{tor}_{\mathbb{Z}_p}(U)/\mathrm{tor}_{\mathbb{Z}_p}(\bar{E}) = 1 \longrightarrow \mathrm{tor}_{\mathbb{Z}_p}\big(U \big/ \bar{E}\big) \xrightarrow{\log} \mathcal{R} \longrightarrow 0,$$

where $\widetilde{\mathcal{C}\ell} \subseteq \mathcal{C}\ell$ corresponds, by class field theory, to the subgroup $\mathrm{Gal}(H/H \cap \tilde{K})$, and where $\mathcal{R} = \mathrm{tor}_{\mathbb{Z}_p}\big(\log\big(U\big)\big/\log(\bar{E})\big)$ is the normalized p-adic regulator [19, Proposition 5.2]. Taking the θ-components, we obtain the exact sequences (where $\mathcal{R}_\theta = 1$ for all odd θ):

$$1 \longrightarrow \mathcal{R}_\theta \longrightarrow \mathcal{T}_\theta \longrightarrow \widetilde{\mathcal{C}\ell}_\theta \longrightarrow 1.$$

For more information, see [14,17,19]. We then have $\mathrm{Gal}(H^{\rm pr}/K) \simeq \Gamma \oplus \mathcal{T} \simeq \mathbb{Z}_p^{\frac{p+1}{2}} \oplus \mathcal{T}$, where $\Gamma = \mathrm{Gal}(\tilde{K}/K)$ is such that $\Gamma_+ = \Gamma_1 \simeq \mathbb{Z}_p$ and $\Gamma_- \simeq \mathbb{Z}_p[G]_-$ giving $\Gamma_\theta \simeq \mathbb{Z}_p$ for all odd θ.

Write $\mathcal{T} = \mathcal{T}_+ \oplus \mathcal{T}_-$ and define $H_-^{\rm pr} \subseteq H^{\rm pr}$ (fixed by $\mathrm{Gal}(H^{\rm pr}/K)_+$), then $H_+^{\rm pr} \subseteq H^{\rm pr}$ (fixed by $\mathrm{Gal}(H^{\rm pr}/K)_-$). Thus $\mathrm{Gal}(H_+^{\rm pr}/K) \simeq \mathbb{Z}_p \oplus \mathcal{T}_+$ and $\mathrm{Gal}(H_-^{\rm pr}/K) \simeq \mathbb{Z}_p^{\frac{p-1}{2}} \oplus \mathcal{T}_-$.

One defines in the same way the fields $H_\theta^{\rm pr}$ for which $\mathrm{Gal}(H_\theta^{\rm pr}/K) \simeq \Gamma_\theta \oplus \mathcal{T}_\theta$ (reduced to $\mathcal{T}_\theta$ finite, for all $\theta \in \mathscr{X}_+$). We have $H_\theta \subset H_\theta^{\rm pr}$ in terms of components of H.

Note that $H_+^{\rm pr}/K$ is decomposed over K_+ to give the maximal abelian p-ramified pro-p-extension of K_+.

Theorem 8. *For all irreducible p-adic characters θ of K, we have* $\mathrm{rk}_p(\mathcal{T}_{\theta^*}) = \mathrm{rk}_p(\mathcal{C}\ell_\theta)$.

Proof. We will give an outline of this famous reflection result as follows, from classical Kummer duality between radicals and Galois groups (see, e.g., [14, Theorem I.6.2 and Corollary I.6.2.1]), using the fact that $K(\sqrt[p]{\beta})/K$, $\beta \in K^\times$ is p-ramified, if and only if $(\beta) = \mathfrak{p}^e \cdot \mathfrak{A}^p$, $e \geq 0$, $\mathfrak{A} \in I$ (group of prime to p ideals of K). We shall have to take the

θ or θ^*-components for each object considered in $K^\times \otimes \mathbb{Z}_p$, $I \otimes \mathbb{Z}_p, \ldots$, modulo p-th powers:

Let θ be even. The Kummer radical of the compositum of the cyclic extensions of degree p of K, contained in $H_{\theta^*}^{\rm pr}$, is generated (modulo $K^{\times p}$) by the part E_θ of real units, giving a p-rank 1 for $\theta \neq 1$ (and 0 for $\theta = 1$), by p (of character 1), and by the pseudo-units α_θ coming from the elements of order p of $\mathcal{C}\ell_\theta$, which gives a radical of p-rank $1 + {\rm rk}_p(\mathcal{C}\ell_\theta)$. Since ${\rm rk}_p({\rm Gal}(H_{\theta^*}^{\rm pr}/K)) = 1 + {\rm rk}_p(\mathcal{T}_{\theta^*})$, we get ${\rm rk}_p(\mathcal{T}_{\theta^*}) = {\rm rk}_p(\mathcal{C}\ell_\theta)$. Similarly, we have ${\rm rk}_p(\mathcal{T}_\theta) = {\rm rk}_p(\mathcal{C}\ell_{\theta^*})$. □

COROLLARY 9 (Hecke theorem or Leopoldt spiegelungssatz)

We have $\mathcal{T}_1 = \mathcal{T}_\omega = \mathcal{C}\ell_\omega = \mathcal{C}\ell_1 = 1$. *We also have* $\mathcal{R}_{\chi *} = 1$ *and* $\mathcal{T}_{\chi *} = \widetilde{\mathcal{C}\ell}_{\chi *} \subseteq \mathcal{C}\ell_{\chi *}$ *for all* $\chi \in \mathscr{X}_+$, *which implies* ${\rm rk}_p(\mathcal{C}\ell_{\chi *}) = {\rm rk}_p(\mathcal{C}\ell_\chi) + \delta_\chi$, $\delta_\chi \in \{0, 1\}$ *since* $\Gamma_{\chi *} \simeq \mathbb{Z}_p$ (*particular case of* [14, Theorem II.5.4.5, 5.4.9.2]).

Remark 10.

(i) One says that K is p-rational if $\mathcal{T} = 1$ (same definition for any number field fulfilling the Leopoldt conjecture at p; see [17,21] for more details and programs testing the p-rationality of any number field). For the p-th cyclotomic field K, this is equivalent to its 'p-regularity' in the more general context of 'regular kernel' given in [11, Théorème 4.1] ($\mathcal{T}_- = 1$ may be interpreted as the conjectural 'relative p-rationality' of K). Thus $\mathcal{C}\ell_\chi = 1$ if and only if $H_{\chi *}$ is contained in a $\mathbb{Z}_p$-extension.

(ii) As we have seen, 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 $c\ell(\mathfrak{A}) \in \mathcal{C}\ell_-$; moreover $\mathfrak{A}$ is not principal, otherwise α should be, up to a p-th power factor, a unit ε such that $\varepsilon^{1+s_{-1}} = 1$, which gives $\varepsilon \in \mu_p$ (absurd). In the same way, if G operates via χ on ${\rm Gal}(L_+/K_+)$, then by Kummer duality, G operates via χ^* on $\langle\alpha\rangle K^{\times p}/K^{\times p}$.

(iii) As explained in the Introduction, we shall prove in § 4.2 that such pseudo-units α may be found by means of twists $g_c(\ell) = \tau(\psi)^{c-\sigma_c}$ associated to primes $\ell \equiv 1 \pmod p$ and Artin automorphisms σ_c.

3.2 *Vandiver's conjecture and Gauss sums*

3.2.1 *Iwasawa's results.* Recall the formula [14, Corollary III.2.6.1]:

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

where I is the group of prime to p ideals of K and $U = 1 + \varpi\, \mathbb{Z}_p[\varpi]$. For any $\mathfrak{A} \in I$, let $m \geq 1$ be such that $\mathfrak{A}^m = (\alpha)$, then $\log(\mathfrak{A}) = \frac{1}{m}\log(\alpha)$ where log is the p-adic logarithm; taking the minus parts, $\log(\mathfrak{A})$ becomes well-defined since $\mathbb{Q}_p \log(E)_- = 0$. We obtain

$$\#\,\mathcal{T}_{\chi *} = \frac{\#\,\mathcal{C}\ell_{\chi *}}{\#\left(\mathbb{Z}_p \log(I)/\mathbb{Z}_p \log(U)\right)_{\chi *}}, \quad \text{for all } \chi =: \omega^n \in \mathscr{X}_+. \tag{2}$$

The following reasoning (from [13, § 3]) gives another interpretation of the result of Iwasawa [29]. 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 $S \cdot e_{\chi *} = B_{1,(\chi^*)^{-1}} \cdot e_{\chi *} \in \mathbb{Z}_p[G]$ for all $\chi \in \mathscr{X}_+$; then $\chi^* = \omega^{p-n}$ for which $\mathcal{C}\ell_{\chi *}$, annihilated by $B_{1,(\chi^*)^{-1}}$, corresponds to the ordinary Berrnoulli numbers B_n giving the 'exponents of p-irregularity' n for $B_n \equiv 0 \pmod{p}$ (see Definition 3(vii)).

Let ℓ be a prime number totally split in K (thus $\ell \equiv 1 \pmod{p}$). Let ψ be a character of order p of $\mathbb{F}_\ell^\times$. We define the Gauss sum (where ξ_ℓ is a primitive ℓ-th root of unity):

$$\tau(\psi) = -\sum_{x \in \mathbb{F}_\ell^\times} \psi(x)\, \xi_\ell^x \in \mathbb{Z}[\mu_{p\ell}]. \tag{3}$$

Lemma 11. *We have* $\tau(\psi)^{\sigma_a} = \psi(a)^{-a}\, \tau(\psi^a)$, *where* σ_a *is the Artin automorphism attached to* a *in* $\mathrm{Gal}(\mathbb{Q}(\mu_{p\ell})/\mathbb{Q})$, *and* $\tau(\psi)^p \in \mathbb{Z}[\zeta_p]$; *then* $\tau(\psi) \equiv 1 \pmod{\mathfrak{p}\,\mathbb{Z}[\mu_{p\ell}]}$.

Proof. By definition of σ_a, one has $\tau(\psi)^{\sigma_a} = -\sum_{x \in \mathbb{F}_\ell^\times} \psi(x)^a\, \xi_\ell^{a\,x} = -\psi^a(a^{-1}) \sum_{y \in \mathbb{F}_\ell^\times} \psi^a(y)\, \xi_\ell^y$; whence the second claim taking $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\mu_{p\ell})/K)$ (i.e., $a \equiv 1 \pmod{p}$). Then $\tau(\psi) \equiv -\sum_{x \in \mathbb{F}_\ell^\times} \xi_\ell^x \pmod{\mathfrak{p}\,\mathbb{Z}[\mu_{p\ell}]}$; since ℓ is prime, $\sum_{x \in \mathbb{F}_\ell^\times} \xi_\ell^x = -1$. □

We then have the fundamental classical relation in K (see [55, § 6.1, § 6.2, § 15.1]):

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

for $\mathfrak{L} \mid \ell$ such that ψ is defined on the multiplicative group of $\mathbb{Z}[\zeta_p]/\mathfrak{L} \simeq \mathbb{F}_\ell$.

Remark 12.

(i) Since various choices of $\mathfrak{L} \mid \ell$, ξ_ℓ and ψ, from a given ℓ, correspond to Galois conjugations and/or products by a p-th 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 objects) in an obvious way. One verifies that the forthcoming properties (p-primarities, Kummer radicals, …) do not depend on these choices.

(ii) If we consider $\alpha = \tau(\psi)^p \in K^\times$ as the Kummer radical of the cyclic extension $M_\ell = K(\tau(\psi))$ of K, we have $\alpha^{c-s_c} =: \mathrm{g}_c(\ell)^p$, where $\mathrm{g}_c(\ell) = \tau(\psi)^{c-\sigma_c} \in K^\times$; which gives $M_\ell = K(\sqrt[p]{\alpha}) = F_\ell K$, where F_ℓ is the subfield of $\mathbb{Q}(\mu_\ell)$ of degree p (the character of $\langle\alpha\rangle K^{\times p}/K^{\times p}$ is ω and that of $\mathrm{Gal}(M_\ell/K)$ is 1). Thus p is unramified in M_ℓ/K (which is coherent with $\tau(\psi) \equiv 1 \pmod{\mathfrak{p}\mathbb{Z}_p[\mu_{p\ell}]}$ implying $\tau(\psi)^p \equiv 1 \pmod{\mathfrak{p}^p}$); it splits if and only if $\tau(\psi)^p \equiv 1 \pmod{\mathfrak{p}^{p+1}}$.

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

$$\big(S \cdot e_{\chi *}\big) \cdot \log(\mathfrak{L}) = B_{1,(\chi^*)^{-1}} \cdot \log(\mathfrak{L}) \cdot e_{\chi *} = \log(\tau(\psi)) \cdot e_{\chi *},$$

where $\log(\tau(\psi)) = \frac{1}{p}\log(\tau(\psi)^p) \in \mathbb{Z}_p[\varpi]$. Put $B_{1,(\chi^*)^{-1}} \sim p^e$, $e \geq 0$, where $\sim$ means equality up to a p-adic unit. Then $p^e\, \mathbb{Z}_p \log(\mathfrak{L}) \cdot e_{\chi *} = \mathbb{Z}_p \log(\tau(\psi)) \cdot e_{\chi *}$, thus, from (2), since I/P may be represented by prime ideals of degree 1,

$$\#\,\mathcal{T}_{\chi *} = \frac{p^e}{\#\left(\mathbb{Z}_p \log(\mathscr{G}) \big/ p^e \log(U)\right)_{\chi *}}, \tag{5}$$

where $\mathscr{G}$ is the group generated by all the previous Gauss sums.

So, the 'Vandiver conjecture at $\chi \in \mathscr{X}_+$' is equivalent to $\left(\mathbb{Z}_p \log(\mathscr{G})/\log(U)\right)_{\chi *} = 1$, and is, as expected, obviously fulfilled if $e = 0$. 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 giving again Iwasawa's result [29].

3.2.2. *About the structure of $\mathcal{C}\ell_{\chi *}$: Strategy of the proofs.* We shall, from now on, make the following working hypothesis which corresponds to the more subtle case for testing Vandiver's conjecture with Theorems 21, 23 (or Theorem 2 in the Introduction), the case where some $\mathcal{C}\ell_{\chi *}$ are not cyclic, being obvious for all the forthcoming statements, as soon as one knows that $B_{1,(\chi^*)^{-1}} \sim p^e$ gives the order of $\mathcal{C}\ell_{\chi *}$, thus its annihilation.

Indeed, to explain briefly, consider the straightforward case where $\mathcal{C}\ell_{\chi *} \simeq \mathbb{Z}/p^{e_1}\mathbb{Z} \times \mathbb{Z}/p^{e_2}\mathbb{Z} =: \langle c\ell(\mathfrak{L}_1)\rangle \times \langle c\ell(\mathfrak{L}_2)\rangle$, $e_i \geq 1$, so that $B_{1,(\chi^*)^{-1}} \sim p^{e_1+e_2}$ annihilates $c\ell(\mathfrak{L}_i)$ for $i = 1, 2$; so we will obtain, from the relation (4), the fundamental relation:

$$\mathfrak{L}_i^{B_{1,(\chi *)^{-1}}} = (\alpha_i) \text{ with twists } \alpha_i = \mathrm{g}_c(\ell_i)_{\chi *} \text{ (referred later as relation (9))}$$

giving in the left member a generator of the ideal in $K^{\times p}$, thus $\mathrm{g}_c(\ell_i)_{\chi *} \in K^{\times p}$ since $E_{\chi *} = 1$ for odd characters distinct from ω (a fundamental fact; otherwise the generator would not be canonical). So, this will give $\mathscr{E}_\ell(p) \cap \mathscr{E}_0(p) \neq \emptyset$, *for all* $\ell \in \mathscr{L}_p$, whence the two main theorems for trivial reasons.

In the remaining cyclic case for $\mathcal{C}\ell_{\chi *}$, we shall have similar reasonings with the relations $\mathfrak{L}^{B_{1,(\chi *)^{-1}}} = (\mathrm{g}_c(\ell)_{\chi *})$ $(\mathfrak{L} \mid \ell \in \mathscr{L}_p)$ depending on the order of $c\ell(\mathfrak{L})$; but here we can use the Chebotarev density theorem to choose $\mathfrak{L}$ at will (all this will be used in full generality, with all details, in § 4.2).

Hypothesis 13 (*Cyclicity hypothesis*). We assume that, for all $\chi \in \mathscr{X}_+$, the component $\mathcal{C}\ell_{\chi *}$ of the p-class group is cyclic (which implies the cyclicity of $\mathcal{C}\ell_\chi$); in other words, we restrict ourselves to the case where $\mathcal{C}\ell$ is $\mathbb{Z}_p[G]$-monogenous (cf. Definition 3 (viii)), giving $\mathrm{rk}_p(\mathcal{C}\ell_-) = i(p)$, the index of p-irregularity.

3.3 *Vandiver's conjecture and ray class group modulo* (p)

Assume Hypothesis 13 and let $\chi = \omega^n \in \mathscr{X}_+$ be such that $B_{1,(\chi^*)^{-1}} \sim p^e$, $e \geq 1$ (i.e., $\mathcal{C}\ell_{\chi *} \simeq \mathbb{Z}/p^e\mathbb{Z}$); thus, from (5), we have $\mathcal{T}_{\chi *} = 1$ (i.e., $\mathcal{C}\ell_\chi = 1$) if and only if there exists a prime number $\ell \equiv 1 \pmod p$ such that the corresponding $\log(\tau(\psi)_{\chi *})$ generates $\log(U_{\chi *}) = \log(1 + \varpi^{p-n}\mathbb{Z}_p[\varpi]) = \varpi^{p-n}\mathbb{Z}_p[\varpi]$ (Proposition 7), which indicates analytically the non-p-primarity of $\tau(\psi)_{\chi *}$ in $\mathbb{Z}[\zeta_p]$, since $n > 1$.

There is also the fact that the Gauss sums (or the $\mathrm{g}_c(\ell) = \tau(\psi)^{c-\sigma_c}$), considered modulo p-th powers and computed modulo p, are indexed by infinitely many ℓ; in other words, there are some non-obvious large periodicities in the results as ℓ varies since numerical data are finite in number.

This may be explained as follows (giving also an interesting criterion which will imply new heuristics):

Theorem 14. *Let $\mathcal{C}\ell^{(p)}$ be the p-subgroup of the ray class group $I/\{(x),\ x \equiv 1 \pmod p\}$ of modulus $p\mathbb{Z}[\zeta_p]$. Then for any $\chi \in \mathscr{X}_+$, we have (under the cyclicity Hypothesis 13) the following properties*:

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

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

Proof. Let $V = \{x \in K^\times,\ x \equiv 1 \pmod{\mathfrak{p}}\}$ and $W = \{x \in K^\times,\ x \equiv 1 \pmod{p}\}$. Since $E_{\chi^*} = 1$, we have the exact sequence (using Proposition 7):

$$1 \to (V/W)_{\chi^*} \simeq \mathbb{F}_p \longrightarrow \mathcal{C}\ell_{\chi^*}^{(p)} \longrightarrow \mathcal{C}\ell_{\chi^*} \to 1,$$

giving (i). The statement (ii) is obvious if $\mathcal{C}\ell_{\chi^*} = 1$. Suppose $\#\mathcal{C}\ell_{\chi^*} = p^e$, with $e \geq 1$. Then $\mathcal{C}\ell_\chi = 1$ implies $\mathcal{T}_{\chi^*} = 1$ (from Theorem 8) which implies $\mathcal{C}\ell_{\chi^*}^{(p)} \simeq \mathbb{Z}/p^{e+1}\mathbb{Z}$: indeed, the χ^*-part $H_{\chi^*}^{\rm pr}/K$ of the pro-p-extension $H^{\rm pr}/K$ is a $\mathbb{Z}_p$-extension, thus the p-ray class field corresponding to $\mathcal{C}\ell_{\chi^*}^{(p)}$, contained in $H_{\chi^*}^{\rm pr}$, is a cyclic extension of K.

Reciprocally, if $\mathcal{C}\ell_{\chi^*}^{(p)} \simeq \mathbb{Z}/p^{e+1}\mathbb{Z}$, $e \geq 1$ (thus $\mathcal{C}\ell_{\chi^*} \simeq \mathbb{Z}/p^e\mathbb{Z}$), there exists $\mathfrak{A}$ (whose class generates $\mathcal{C}\ell_{\chi^*}^{(p)}$) such that $\mathfrak{A}_{\chi^*}^{p^e} = (\alpha_{\chi^*})$ (where α_{χ^*} is unique up to a p-th power since $E_{\chi^*} = 1$) with $\alpha_{\chi^*} \equiv 1 \pmod{\mathfrak{p}^{p-n}}$ ($\chi =: \omega^n$, $n \in [2,\ p-3]$ even), but $\alpha_{\chi^*} \not\equiv 1 \pmod{p}$. Note that $\mathrm{rk}_p(\mathcal{T}_\chi) = \mathrm{rk}_p(\mathcal{C}\ell_{\chi^*}) = 1$. Thus α_{χ^*} defines the radical of the unique p-ramified (but not unramified) cyclic extension of degree p of K decomposed over K_+ into L_+/K_+ and contained in $H_\chi^{\rm pr}$ (its Galois group is a quotient of order p of the *cyclic group* $\mathcal{T}_\chi$ since $\Gamma_\chi = 1$ for an even $\chi \neq 1$); thus $\mathcal{C}\ell_\chi = 1$. □

4. Twists of Gauss sums associated to primes $\ell \equiv 1 \pmod{p}$

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

$$\tau(\psi) = -\sum_{x \in \mathbb{F}_\ell^\times} \psi(x) \cdot \xi_\ell^x = -\sum_{k=0}^{\ell-2} \zeta_p^k \cdot \xi_\ell^{g^k}$$
$$\text{(with the relation } x \equiv g^k \pmod{\ell}). \tag{6}$$

4.1 *Computation and properties of the twists* $\mathrm{g}_c(\ell) = \tau(\psi)^{c-\sigma_c}$

4.1.1. *Main relation: Ideal decomposition of the twists.* Let $c \in [2,\ p-2]$ be a primitive root modulo p; to get an integer of K, one uses the twist $\tau(\psi)^{c-\sigma_c}$, where σ_c is the Artin automorphism attached to c in $\mathrm{Gal}(\mathbb{Q}(\mu_{p\,\ell})/\mathbb{Q})$ (independently of the theoretical interest of these twists, a PARI/GP program computing with Gauss sums in $\mathbb{Z}[\mu_{p\,\ell}]$ overflows as ℓ increases, even if $\tau(\psi)_{\chi^*} = \tau(\psi)^{e'_{\chi^*}}$ makes sense in $\mathbb{Z}[\zeta_p]$, a posteriori). We define for $\ell \in \mathscr{L}_p$ (cf. Lemma 11),

$$\mathrm{g}_c(\ell) = \tau(\psi)^{c-\sigma_c} \in \mathbb{Z}[\zeta_p] \ \text{(see formulas (3), (4) and Remark 12)}, \tag{7}$$

giving for all $\chi \in \mathscr{X}_+$, up to an element of $K^{\times p}$ for the generators of ideals:

$$\mathfrak{L}^{S_c} = \mathrm{g}_c(\ell)\,\mathbb{Z}[\zeta_p] \quad \text{and} \quad \mathfrak{L}_{\chi^*}^{(c-\chi^*(s_c))\cdot B_{1,(\chi^*)^{-1}}} = \mathrm{g}_c(\ell)_{\chi^*}\,\mathbb{Z}[\zeta_p],$$

where $\mathfrak{L} \mid \ell$ in K, $S_c = (c - s_c) \cdot S \in \mathbb{Z}[G]$ is the corresponding twist of the Stickelberger element and where $\mathrm{g}_c(\ell) \in \mathbb{Z}[\zeta_p]$. Put

$$b_c(\chi^*) = (c - \chi^*(s_c)) \cdot B_{1,(\chi^*)^{-1}} \sim B_{1,(\chi^*)^{-1}},\ \text{for all } \chi \in \mathscr{X}_+. \tag{8}$$

Then we obtain for all $\ell \equiv 1 \pmod{p}$ and for all $\chi \in \mathscr{X}_+$ *the main relations* that will be of a constant use, since we shall verify (Lemma 20 using Chebotarev density theorem) that any class in $\mathcal{C}\ell_{\chi *}$ may be put in the form $c\ell(\mathfrak{L}_{\chi *})$ such that

$$\mathfrak{L}_{\chi *}^{b_c(\chi *)} = \mathrm{g}_c(\ell)_{\chi *}\, \mathbb{Z}[\zeta_p], \quad \text{where } \mathfrak{L} \mid \ell \text{ and } \mathrm{g}_c(\ell)_{\chi *} = \left[\tau(\psi)^{c-\sigma_c}\right]_{\chi *}. \tag{9}$$

Remark 15.

(i) In the above definition (7) of $\mathrm{g}_c(\ell)$, $\tau(\psi)^{\sigma_c} = \tau(\psi^c) \cdot \psi^{-c}(c)$ (Lemma 11); but for all $\chi \neq 1$, $\mu_p^{e_{\chi *}} = 1$, defining $\mathrm{g}_c(\ell)_{\chi *}$ without ambiguity up to $K^{\times p}$, which does not change the p-primarity properties. But in some sense the best definition of the twists should be $\psi^{-c}(c) \cdot \mathrm{g}_c(\ell) = \psi^{-c}(c) \cdot \tau(\psi)^{c-\sigma_c}$.

(ii) Note that, since $\tau(\psi)^{1+s_{-1}} = \ell$, this yields $\mathrm{g}_c(\ell)_\chi \in K^{\times p}$ for all $\chi \in \mathscr{X}_+$.

4.1.2 *Computation of* $\mathrm{g}_c(\ell)$ *using Jacobi sums*

Lemma 16. *Let* $\ell \in \mathscr{L}_p$. *Then* $\psi^{-c}(c) \cdot \mathrm{g}_c(\ell)$ *is a product of Jacobi sums and* $\psi^{-c}(c) \cdot \mathrm{g}_c(\ell) \equiv \mathrm{g}_c(\ell) \equiv 1 \pmod{\mathfrak{p}}$.

Proof. The classical formula [55, § 6.1] for Jacobi sums (with $\psi\, \psi' \neq 1$) is

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

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

$$\tau(\psi)^{c-\sigma_c} = J_1 \cdots J_{c-1} \cdot \tau(\psi^c)\, \tau(\psi)^{-\sigma_c} = J_1 \cdots J_{c-1} \cdot \psi^c(c),$$

from Lemma 11. Then $\tau(\psi) \equiv 1 \pmod{\mathfrak{p}\, \mathbb{Z}[\mu_{p\ell}]}$ implies the result for $\mathrm{g}_c(\ell)$. □

Thus, in the numerical computations, we shall use the relation

$$\mathrm{g}_c(\ell)_{\chi *} = (J_1 \cdots J_{c-1})_{\chi *} \text{ for any } \chi \in \mathscr{X}_+. \tag{10}$$

4.1.3. *Exponents of p-primarity and p-irregularity.* The following definitions will be of constant use in the paper.

DEFINITION 17

(i) We call the set of exponents of p-primarity, of a prime $\ell \in \mathscr{L}_p$, 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, thus $\mathrm{g}_c(\ell)_{\omega^{p-n}} \equiv 1 \pmod{p}$ (Definition 4 (ii), Proposition 7).

(ii) We call the set of exponents of p-irregularity, the set $\mathscr{E}_0(p)$ of even integers $n \in [2,\ p-3]$ such that $B_n \equiv 0 \pmod{p}$. Thus, $B_{1,\omega^{n-1}} \equiv 0 \pmod{p}$ (see Definitions 3 (vii)).

4.1.4. *Sufficient condition for a counterexample to Vandiver's conjecture.* We know and we shall see in Lemma 20 that the existence of a degree p unramified cyclic extension of K_+, of character $\chi \in \mathscr{X}_+$, comes necessarily from a Kummer radical in $K^\times$ of the form $\langle \mathrm{g}_c(\ell)_{\chi *}\rangle$, where $\mathrm{g}_c(\ell)_{\chi *} = \left[\tau(\psi)^{c-\sigma_c}\right]_{\chi *}$ fulfills some conditions, of which the p-primarity is one of them. So we consider such a twist $\mathrm{g}_c(\ell)_{\chi *}$ with $\chi =: \omega^n \in \mathscr{X}_+$ and $\ell \in \mathscr{L}_p$.

If $\mathrm{g}_c(\ell)_{\chi *}$ is p-primary, the Kummer extension $K\big(\sqrt[p]{\mathrm{g}_c(\ell)_{\chi *}}\big)/K$ (decomposed over K_+) does not necessarily give a counterexample to Vandiver's conjecture for the following two possible reasons (recall that, from (8), (9), $\mathfrak{L}_{\chi^*}^{b_c(\chi^*)} = (\mathrm{g}_c(\ell)_{\chi^*})$, where $b_c(\chi^*) = (c - \chi^*(s_c)) \cdot B_{1,(\chi^*)^{-1}} \sim B_{1,(\chi^*)^{-1}}$ gives the order and annihilation of $\mathcal{C}\ell_{\chi^*}$):

(i) The number $b_c(\chi^*)$ is a p-adic unit ($n \notin \mathscr{E}_0(p)$), so the radical $\mathrm{g}_c(\ell)_{\chi *}$ is not the p-th power of an ideal (thus not a pseudo-unit, even if Proposition 7 applies) and leads to a cyclic ℓ-ramified Kummer extension of degree p of K_+. For instance, for $p = 11$ ($c = 2$), $\ell = 23$, the exponent of 11-primarity is $n = 2$ so that $\alpha = \mathrm{g}_c(\ell)_{\chi *}$ is the integer ($x = \zeta_{11}$):

```
-8491773970656065727678427465045288222*x^9
  -1963231019856677733688722439078492228*x^8
+1175752323219887315920581034885452632 0*x^7
  -5860674150310922200348907606983566648*x^6
-6440880061928168516081421235792769 62*x^5
  -6110740142892312843083868171996580 10*x^4
+2673005955545675004066087284224877298*x^3
  +1502302873783880915125184216661565 8188*x^2
+1520229819300797188419125563036321734*x
  +1783623855473216386893369378902567 9469
```

for which $K(\sqrt[11]{\alpha})/K$ is decomposed over K_+ into L_+/K_+, ℓ-ramified; then (α) is a product of prime ideals above ℓ ($s = s_2$): $(\alpha) = \mathfrak{L}^{1+2s+2^2s^2+2^3s^3+2^4s^4+2^5s^5+2^6s^6+2^7s^7+2^8s^8+2^9s^9}$, up to the 11-th power of an ℓ-ideal. We get $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \ell^{275}$ and $\mathrm{N}_{K/\mathbb{Q}}(\alpha - 1) \sim 11^{13}$.

(ii) We have $b_c(\chi^*) \sim p^e$, $e \geq 1$, but the ideal $\mathfrak{L}_{\chi *}^{p^{e-1}}$ is p-principal and then $\mathrm{g}_c(\ell)_{\chi *}$ is a p-th power in $K^\times$ since $E_{\chi *} = 1$; see numerical examples with $p = 37$ in "Appendix B".

So, from this reason, we can state about $\mathrm{g}_c(\ell)_{\chi *} = \left[\tau(\psi)^{c-\sigma_c}\right]_{\chi *}$ and $b_c(\chi^*) \sim B_{1,(\chi^*)^{-1}}$:

Lemma 18. *A sufficient condition giving a counterexample to Vandiver's conjecture is the existence of $\chi = \omega^n \in \mathscr{X}_+$ and $\ell \in \mathscr{L}_p$ such that the following three conditions hold*:

(a) $b_c(\chi^*) \equiv 0 \pmod p$ *(i.e., $n \in \mathscr{E}_0(p)$)*,
(b) $\mathrm{g}_c(\ell)_{\chi *}$ *is p-primary (i.e., $n \in \mathscr{E}_\ell(p)$)*,
(c) $\mathrm{g}_c(\ell)_{\chi *}$ *is not a global p-th power (i.e., $c\ell(\mathfrak{L}_{\chi *})$ is generator)*.

We shall see in the next section that the condition is necessary subject to reduction to the monogenous case (i.e., cyclicity of the $\mathcal{C}\ell_{\chi^*}$ for all $\chi \in \mathscr{X}_+$).

4.2 *First main theorem*

We once again state here the fundamental remark at the origin of the cyclicity hypothesis 13.

Remark 19. If $\mathrm{rk}_p(\mathcal{C}\ell_{\chi_0^*}) \geq 2$ for $\chi_0 = \omega^{n_0} \in \mathscr{X}_+$ (giving a counterexample to Vandiver's conjecture), we get from the Main Theorem $\#\mathcal{C}\ell_{\chi_0^*} \sim B_{1,(\chi_0^*)^{-1}} \sim b_c(\chi_0^*)$; then the p-part of $b_c(\chi_0^*)$ is strictly larger than the exponent of $\mathcal{C}\ell_{\chi_0^*}$ so, in every relation $\mathfrak{L}_{\chi_0^*}^{b_c(\chi_0^*)} = (\mathrm{g}_c(\ell)_{\chi_0^*})$, $\ell \in \mathscr{L}_p$ (relation (9)), necessarily $\mathrm{g}_c(\ell)_{\chi_0^*}$ is a global p-th power (condition (c) is *never* fulfilled, although conditions (a), (b) hold), whence the property:

$$n_0 \in \mathscr{E}_\ell(p) \cap \mathscr{E}_0(p), \quad \text{for all } \ell \in \mathscr{L}_p,$$

giving the non-empty sets $\mathscr{E}_\ell(p) \cap \mathscr{E}_0(p)$ (for all ℓ) and $\bigcap_\ell \mathscr{E}_\ell(p)$. Thus, as we have explained, Theorems 21 and 23 will apply for trivial reasons and we can go back to the cases $\mathrm{rk}_p(\mathcal{C}\ell_{\chi*}) \leq 1$ (Hypothesis 13) for the reciprocal: 'non-Vandiver implies conditions (a), (b), (c) of Lemma 18'. This is given by the following lemma in the cyclic case for $\mathcal{C}\ell_{\chi*}$.

Lemma 20. *Let $\chi \in \mathscr{X}_+$ be such that $\mathcal{C}\ell_\chi \neq 1$. There exists a totally split prime ideal $\mathfrak{L}$ such that $\mathfrak{L}_{\chi*}$ represents a generator of $\mathcal{C}\ell_{\chi*}$. Then $\mathfrak{L}_{\chi*}^{b_c(\chi*)} = (\alpha_{\chi*})$, where $\alpha_{\chi*}$ is unique (up to p-th power), thus it equals to $\mathrm{g}_c(\ell)_{\chi*}$ which is p-primary and not a global p-th power.*

Proof. From the Chebotarev density theorem in $H/\mathbb{Q}$, there exists a prime ℓ and $\bar{\mathfrak{L}} \mid \ell$ in H such that the Frobenius $\left(\frac{H/\mathbb{Q}}{\bar{\mathfrak{L}}}\right)$ generates the subgroup of $\mathrm{Gal}(H/K)$ corresponding to $\mathcal{C}\ell_{\chi*}$, by class field theory. So ℓ splits completely in $K/\mathbb{Q}$ ($\ell \in \mathscr{L}_p$) and the ideal $\mathfrak{L}$ of K under $\bar{\mathfrak{L}}$ is (as $\mathfrak{L}_{\chi*}$) a representative of a *generator* of $\mathcal{C}\ell_{\chi*} \simeq \mathbb{Z}_p/b_c(\chi^*)\,\mathbb{Z}_p$. Then $\mathfrak{L}_{\chi*}^{b_c(\chi^*)} = (\alpha_{\chi*})$ where $\alpha_{\chi*} \notin K^{\times p}$; $\alpha_{\chi*}$ is unique since $E_{\chi*} = 1$ for $\chi^* \neq \omega$. In terms of Gauss sums, $\mathfrak{L}_{\chi*}^{b_c(\chi^*)} = (\mathrm{g}_c(\ell)_{\chi*})$, thus $\alpha_{\chi*} = \mathrm{g}_c(\ell)_{\chi*}$. The p-primarity of $\alpha_{\chi*}$ is necessary to obtain the *unique* (thanks to Hypothesis 13) unramified Kummer extension $K(\sqrt[p]{\alpha_{\chi*}})/K$ of degree p, decomposed over K_+ into the unramified extension L_+/K_+ of degree p in H_χ, associated to $\mathcal{C}\ell_\chi/\mathcal{C}\ell_\chi^p$ by class field theory, whence the p-primarity of $\mathrm{g}_c(\ell)_{\chi*}$. □

Drawing the consequences of the above, we get, unconditionally, the main test for Vandiver's conjecture stated in the Introduction (Theorem 2 (a)). We refer to the relations (7), (8), (9) and Definition 17.

Theorem 21. *For any prime $\ell \equiv 1 \pmod p$, let $\mathscr{E}_\ell(p)$ be the set of exponents of p-primarity (even integers n such that $\mathrm{g}_c(\ell)_{\omega^{1-n}} \equiv 1 \pmod p$) and let $\mathscr{E}_0(p)$ be the set of exponents of p-irregularity (even integers n such that $B_n \equiv 0 \pmod p$). Vandiver's conjecture holds for $K = \mathbb{Q}(\mu_p)$ if and only if there exists $\ell \equiv 1 \pmod p$ such that $\mathscr{E}_\ell(p) \cap \mathscr{E}_0(p) = \emptyset$.*

Proof. As explained in Remark 19, we may assume the cyclicity Hypothesis 13.

(a) Suppose $\mathscr{E}_\ell(p) \cap \mathscr{E}_0(p) = \emptyset$ and consider, for $\chi =: \omega^n \in \mathscr{X}_+$ and $\chi^* = \omega^{p-n}$, the relation $\mathfrak{L}_{\chi*}^{b_c(\chi*)} = (\mathrm{g}_c(\ell)_{\chi*})$, where $\mathrm{g}_c(\ell) = \tau(\psi)^{c-\sigma_c}$, for the prime ℓ under consideration, and examine the two possibilities:

(i) If n is not an exponent of p-irregularity (namely, $b_c(\chi^*) \not\equiv 0 \pmod p$ or $B_n \not\equiv 0 \pmod p$), then $\mathcal{C}\ell_{\chi*} = 1$ and $\mathcal{C}\ell_\chi = 1$ from reflection theorem (Corollary 9).

(ii) If n is an exponent of p-irregularity, then $b_c(\chi^*) \sim p^e$, $e \geq 1$, giving, for some p-adic unit u, $\mathfrak{L}_{\chi*}^{p^e u} = (\mathrm{g}_c(\ell)_{\chi*})$; if $\mathfrak{L}_{\chi*}^{p^{e-1}u}$ is p-principal, then $\mathrm{g}_c(\ell)_{\chi*}$ is a global p-th power, hence p-primary (absurd by assumption). So $\mathfrak{L}_{\chi*}$ defines a class of order p^e in $\mathcal{C}\ell_{\chi*}$ for which the pseudo-unit $\mathrm{g}_c(\ell)_{\chi*}$ is not p-primary by assumption; since $\mathrm{Gal}(H_\chi^{\mathrm{pr}}/K_+) = \mathcal{T}_\chi$ is cyclic from Theorem 8, by Kummer duality, $K(\sqrt[p]{\mathrm{g}_c(\ell)_{\chi*}})$ is the unique extension cyclic of degree p, decomposed over K_+ and contained in H_χ^{pr}. Since it is ramified at p and since H_χ^{pr} contains the χ-component of the p-Hilbert class field of K_+, this implies $\mathcal{C}\ell_\chi = 1$.

(b) Reciprocally, if Vandiver's conjecture holds, then $\mathcal{C}\ell = \mathcal{C}\ell_-$ is $\mathbb{Z}_p[G]$-monogenous, thus the direct sum of non-trivial cyclic isotypic components generated by some p-classes $\gamma^{(n_i)} = c\ell(\mathfrak{L}_{\omega^{p-n_i}}^{(n_i)}) \in \mathcal{C}\ell_{\omega^{p-n_i}}$ ($n_i \in \mathscr{E}_0(p)$) related to non-p-primary $\mathrm{g}_c(\ell^{(n_i)})_{\omega^{p-n_i}}$; thus there exists, from density theorem, $\ell \in \mathscr{L}_p$ and $\mathfrak{L} \mid \ell$ such that $c\ell(\mathfrak{L})_{\omega^{p-n_i}} = \gamma^{(n_i)}$ for all i (e.g., $\mathfrak{L} = (z) \cdot \prod_i \mathfrak{L}_{\omega^{p-n_i}}^{(n_i)}$). So each $\mathrm{g}_c(\ell)_{\omega^{p-n_i}} = \mathrm{g}_c(\ell^{(n_i)})_{\omega^{p-n_i}}$ (up to p-th power) is non-p-primary, whence $\mathscr{E}_\ell(p) \cap \mathscr{E}_0(p) = \emptyset$ for this prime ℓ. □

COROLLARY 22 (Case $\mathscr{E}_\ell(p) = \emptyset$)

Let $\ell \in \mathscr{L}_p$. If, for all $\chi \in \mathscr{X}_+$, the numbers $\mathrm{g}_c(\ell)_{\chi*} = \left[\tau(\psi)^{c-\sigma_c}\right]_{\chi*}$ are not p-primary (i.e., $\mathscr{E}_\ell(p) = \emptyset$), then the Vandiver conjecture holds for p.

At this step, the reader may consider, in "Appendix A.1", the PARI/GP programs giving explicit computations of the sets $\mathscr{E}_\ell(p)$, and may examine the corresponding numerical results illustrating the previous statements (especially the corollary in "Appendix A.2").

4.3 *Second main theorem*

Let n_0 be an exponent of p-irregularity; put $\chi_0 = \omega^{n_0}$ and let $b_c(\chi_0^*) \sim p^e$, $e \geq 1$. If $\mathcal{C}\ell_{\chi_0^*}$ is not cyclic, Remark 19 implies $n_0 \in \cap_{\ell \in \mathscr{L}_p} \mathscr{E}_\ell(p)$ and Theorem 23 below will hold. Then we may assume $\mathcal{C}\ell_{\chi_0^*} \simeq \mathbb{Z}/p^e\mathbb{Z}$. We shall examine what happens when ℓ varies.

Let $\ell \in \mathscr{L}_p$ and let $\mathfrak{L}_{\chi_0^*}$ with $\mathfrak{L} \mid \ell$. Recall that there are two cases as we have seen previously (in Lemma 18 and Remark 19) in the monogenous case:

(i) $\mathfrak{L}_{\chi_0^*}^{p^{e-1}}$ is p-principal. Since $b_c(\chi_0^*) \sim p^e$, $e \geq 1$, $\mathrm{g}_c(\ell)_{\chi_0^*}$ is a global p-th 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 (i.e., it does not give a counterexample to Vandiver's conjecture at χ_0);

(ii) $\mathfrak{L}_{\chi_0^*}^{p^{e-1}}$ is not p-principal (from density theorem, such primes ℓ always exist). Thus it defines a generator of $\mathcal{C}\ell_{\chi_0^*}$, $\mathrm{g}_c(\ell)_{\chi_0^*} \notin K^{\times p}$, and Vandiver's conjecture holds at χ_0 *if*

and only if $\mathrm{g}_c(\ell)_{\chi_0^*}$ is not p-primary. If $\mathrm{g}_c(\ell)_{\chi_0^*} \equiv 1 \pmod p$ (whence a counterexample to Vandiver's conjecture at χ_0), we fix this ℓ once for all, and whatever the ideal $\mathfrak{L}' \mid \ell'$, for $\ell' \in \mathscr{L}_p$, we have $\mathfrak{L}'^{\chi_0^*} = (z) \cdot \mathfrak{L}^{r}_{\chi_0^*}$, with $z \in K^\times$ and $r \in [0, p^e - 1]$; so, this gives $\mathfrak{L}'^{p^e u}_{\chi_0^*} = (z^{p^e u}) \cdot \mathfrak{L}^{r p^e u}_{\chi_0^*}$ and $\mathrm{g}_c(\ell')_{\chi_0^*} \equiv \mathrm{g}_c(\ell)^r_{\chi_0^*} \equiv 1 \pmod p$.

Whence, the exponent n_0 of p-irregularity is a common exponent of p-primarity for all $\ell \in \mathscr{L}_p$, giving $n_0 \in \mathscr{E}_0(p) \cap \left(\cap_{\ell \in \mathscr{L}_p} \mathscr{E}_\ell(p) \right) \neq \emptyset$. In other words, the existence of an empty intersection $\mathscr{E}_{\ell_1}(p) \cap \cdots \cap \mathscr{E}_{\ell_N}(p)$ implies Vandiver's conjecture. We shall now prove the converse, which gives the new criterion.

Theorem 23. *For any prime* $\ell \equiv 1 \pmod p$, *let* $\mathscr{E}_\ell(p)$ *be the set of exponents of* p*-primarity* (*even integers* n *such that* $\mathrm{g}_c(\ell)_{\omega^{1-n}} \equiv 1 \pmod p$). *Vandiver's conjecture holds if and only if there exist* $N \geq 1$ *and* $\ell_1, \ldots, \ell_N \in \mathscr{L}_p$ *such that* $\mathscr{E}_{\ell_1}(p) \cap \cdots \cap \mathscr{E}_{\ell_N}(p) = \emptyset$.

Proof. It remains to prove that Vandiver's conjecture ($\mathcal{C}\ell_\chi = 1$ for all $\chi \in \mathscr{X}_+$) implies the existence of such an empty intersection. Assume, on the contrary, that for all $N \geq 1$ and all sets $\{\ell_1, \ldots, \ell_N\} \subset \mathscr{L}_p$, one has $\mathscr{E}_{\ell_1}(p) \cap \cdots \cap \mathscr{E}_{\ell_N}(p) \neq \emptyset$.

Since $\mathscr{X}_+$ is finite, there exists an n_0 in $\bigcap_{\ell \in \mathscr{L}_p} \mathscr{E}_\ell(p)$ (if $\cap_{\ell \in \mathscr{L}_p} \mathscr{E}_\ell(p) = \emptyset$, then for all even $n \in [2, p-3]$ there exists $\ell(n)$ such that $n \notin \mathscr{E}_{\ell(n)}(p)$ whence $\bigcap_{n \in [2, p-3] \text{ even}} \mathscr{E}_{\ell(n)}(p) = \emptyset$ (absurd)). This means that for the fixed character $\chi_0 = \omega^{n_0}$, we have the property:

$$\mathrm{g}_c(\ell)_{\chi_0^*} \equiv 1 \pmod p, \text{ for all } \ell \in \mathscr{L}_p.$$

To simplify, put $\alpha(\ell) = \mathrm{g}_c(\ell)_{\chi_0^*}$ and consider the extensions $K(\sqrt[p]{\alpha(\ell)})/K$; these extensions, with Galois groups of character χ_0, are decomposed over K_+ into cyclic extensions $L_+(\ell)/K_+$ (possibly trivial), and are ℓ-ramified since $(\alpha(\ell)) = \mathfrak{L}^{b_c(\chi_0^*)}_{\chi_0^*}$ with $\alpha(\ell) \equiv 1 \pmod p$ (non-ramification at p). Examine the two possibilities about $b_c(\chi_0^*)$:

(i) $b_c(\chi_0^*) \equiv 0 \pmod p$. Then $\alpha(\ell)$ is, for all ℓ, a p-primary pseudo-unit, and choosing ℓ such that $\mathfrak{L}_{\chi_0^*}$ generates $\mathcal{C}\ell_{\chi_0^*}$ (which is cyclic since $\mathcal{C}\ell_{\chi_0} = 1$), then $\alpha(\ell) \notin K^{\times p}$, and the extension $L_+(\ell)/K_+$ is unramified of degree p (absurd).

(ii) $b_c(\chi_0^*) \not\equiv 0 \pmod p$. Then $L_+(\ell)/K_+$ is, for all ℓ, a *ℓ-ramified degree p cyclic extension of character* χ_0. We restrict ourselves to primes $\ell \not\equiv 1 \pmod{p^2}$ and consider the p-ray class fields, $H_+(\ell)$ over K_+, of modulus (ℓ); we have $L_+(\ell) \subseteq H_+(\ell)$. Since $\mathcal{C}\ell_+ = 1$, $\mathrm{Gal}(H_+(\ell)/K_+) \simeq (P_+/P_+(\ell)) \otimes \mathbb{Z}_p$, where P_+ is the group of principal ideals prime to ℓ of K_+ and $P_+(\ell)$ the subgroup of P_+ of ideals generated by an element $x \equiv 1 \pmod \ell$.

From the G-modules exact sequence $1 \to E_+/E_+(\ell) \to \bigoplus_{\mathfrak{L}_+ \mid \ell} \mathbb{F}_\ell^\times \to P_+/P_+(\ell) \to 1$, where $E_+(\ell) = \{\varepsilon \in E_+,\ \varepsilon \equiv 1 \pmod \ell\}$, we get (for $\ell \not\equiv 1 \pmod{p^2}$):

$$1 \to (E_+/E_+(\ell))_{\chi_0} \longrightarrow (\mathbb{Z}/p\mathbb{Z})_{\chi_0} \longrightarrow \mathrm{Gal}(H_+(\ell)/K_+)_{\chi_0} \to 1.$$

Since $\mathrm{Gal}(H_+(\ell)/K_+)_{\chi_0}$ is, at least, of order p because of $L_+(\ell)/K_+$, the generating χ_0-unit, $\varepsilon_{\chi_0} =: \varepsilon$, is in $E_+(\ell)_{\chi_0}$, thus locally a p-th power at ℓ, for all $\ell \in \mathscr{L}_p$, $\ell \not\equiv 1 \pmod{p^2}$. Thus ℓ totally splits in $K(\sqrt[p]{\varepsilon})/K$. Let M be the compositum $K(\sqrt[p]{\varepsilon}) \cdot K_1$,

where $K_1 = \mathbb{Q}(\mu_{p^2})$; this Galois field M only depends on p and χ_0 and the primes $\ell \not\equiv 1 \pmod{p^2}$ are inert in K_1/K. Then choose ℓ such that the decomposition group of $\mathcal{L} \mid \ell$ does not fix $K(\sqrt[p]{\varepsilon})$ (since $\mathrm{Gal}(M/K) \simeq (\mathbb{Z}/p\mathbb{Z})^2$, this allows $p-1$ possibilities). Thus ℓ is inert in $K(\sqrt[p]{\varepsilon})/K$ (a contradiction).

Whence the existence of some $\bigcap_{i=1}^{N} \mathscr{E}_{\ell_i}(p) = \emptyset$, $N \geq 1$. □

Remark 24. This theorem suggests that if the sets $\mathscr{E}_\ell(p)$ are random when ℓ varies and are independent, the (conjectural) triviality of $\mathcal{C}\ell_+$ is *a consequence* of a natural p-adic property of Gauss sums and the statement does exist with $N = 1$.

On the contrary, the structure of $\mathcal{C}\ell_-$ is independent of the Gauss sums because the *even components* $\mathrm{g}_c(\ell)_\chi$ are global p-th powers for all $\ell \in \mathscr{L}_p$ (Remark 15 (ii)) and do not yield any obstruction! Thus the cases of non-triviality of $\mathcal{C}\ell_-$ may follow standard probabilities under the monogenous case.

As for the previous Theorem 21, the reader may look at some computations (with PARI/GP programs) illustrating, with the case $p = 37$, the statistical properties of the sets $\mathscr{E}_\ell(p)$ for the criteria about Vandiver's conjecture, in "Appendix B".

5. Heuristics: Probability of a counterexample

In this section, we examine some heuristics in various directions regarding our results.

5.1 *Use of classical 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 $\ell \in \mathscr{L}_p$, 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 [55], Theorem 5.17 and some statistical computations), that for given primes p and $\ell \in \mathscr{L}_p$, the probabilities of a cardinality k is $\binom{N}{j} \cdot \left(1 - \frac{1}{p}\right)^{N-j} \cdot \left(\frac{1}{p}\right)^{j}$ (where $N = \frac{p-3}{2}$). This would imply that, for a given p, $\mathscr{E}_\ell(p) \neq \emptyset$ for many $\ell \in \mathscr{L}_p$, but that $\mathscr{E}_\ell(p) = \emptyset$ in a proportion close to $e^{-\frac{1}{2}}$, which is in accordance 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 $1 - \dfrac{(N-k)! \cdot (N-j)!}{N! \cdot (N-k-j)!}$. So, an approximation of the whole probability of $\mathscr{E}_0(p) \cap \mathscr{E}_\ell(p) \neq \emptyset$ is

$$\sum_{j,\,k \geq 0} \binom{N}{j}\binom{N}{k} \cdot \left(1 - \frac{1}{p}\right)^{2N-j-k} \cdot \left(\frac{1}{p}\right)^{j+k} \cdot \left(1 - \frac{(N-k)! \cdot (N-j)!}{N! \cdot (N-k-j)!}\right). \tag{11}$$

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 $\mathscr{L}_p$ giving, *a priori*, *independent informations*, but limited by Theorem 14 on periodicities due to the density theorem (see the Weil interpretation of Jacobi sums defining Hecke Grössencharacters [56, Theorem, p. 489] where a module of definition of our Jacobi sums is p^2, which may give an order of magnitude of the cardinality of this 'infiniteness'). So this must be put in relation with Theorem 21 to characterize 'non-Vandiver'.

5.2 *New heuristics and probabilities*

Many reasons imply that the generic probability $\frac{1}{p}$ must be replaced by a much lower one.

5.2.1. *Results from K-theory.* For some characters $\chi \in \mathscr{X}_+$ of the form $\chi =: \omega^{p-(1+h)}$, for small $h = 2, 4, \ldots$, one may prove that $\mathcal{C}\ell_{\omega^{p-(1+h)}} = 1$, as in the case of $\mathcal{C}\ell_{\omega^{p-3}} = 1$, proved unconditionally by Kurihara [33]; then Soulé proved in [48] that for $n \in [2,\, p-3]$ even, $\mathcal{C}\ell_{\omega^{p-n}} = 1$ for all p large enough (see also [2,10,49] among other references applying the same approach via K-theory). Unfortunately these bounds are not usable in practice, but demonstrate the existence of a fundamental general principle.

5.2.2. *Archimedean aspects.* At the opposite, for $\chi \in \mathscr{X}_+$ of small order, $\mathcal{C}\ell_\chi$ may be trivial because of the 'archimedean' order of magnitude of the whole class number of the subfield of K_+ fixed by $\mathrm{Ker}(\chi)$ (which is proved for the quadratic case when $p \equiv 1 \pmod 4$, the cubic case when $p \equiv 1 \pmod 3$); see the tables of Schoof [42] for serious arguments about the order of magnitude of the whole class number. Moreover, we have the p-rank ϵ-conjecture for p-class groups [9] that we state for the real abelian fields k_d *of constant degree* d, of discriminant $D = p^{d-1}$, when $p \equiv 1 \pmod d$ increases:

For all $\epsilon > 0$ there exists $C_{d,p,\epsilon}$ such that $\log(\#\,(\mathcal{C}\ell_{k_d}/\mathcal{C}\ell_{k_d}^{p})) \le \log(C_{d,p,\epsilon}) + \epsilon \cdot \log(p)$, which would give $\mathcal{C}\ell_{k_d} = 1$ for $\log(p) > \frac{\log(C_{d,p,\epsilon})}{1-\epsilon}$ and any $\epsilon < 1$. But this does not apply for any p with 'small' d and the constant $C_{d,p,\epsilon}$ is not effective.

5.2.3 *Heuristics about Gauss sums*

The standard probabilities (11) assume that when $\ell \in \mathscr{L}_p$ varies, the sets $\mathscr{E}_\ell(p)$ are *random and independent*, giving probabilities close to 0, which is not the case when p is irregular at some $\chi_0^* = \omega^{p-n_0}$ with $\mathcal{C}\ell_{\chi_0^*} \simeq \mathbb{Z}/p^e\mathbb{Z}$, $e \ge 1$, and when $\mathrm{g}_c(\ell)_{\chi_0^*} = \left[\tau(\psi)^{c-\sigma_c}\right]_{\chi_0^*}$ is a global p-th power because $\mathfrak{L}_{\chi_0^*}^{p^{e-1}}$ is p-principal.

Fix $\ell \in \mathscr{L}_p$ such that $\mathfrak{L}_{\chi_0^*}$ generates $\mathcal{C}\ell_{\chi_0^*} \simeq \mathbb{Z}/p^e\mathbb{Z}$ (thus $\mathrm{g}_c(\ell)_{\chi_0^*}$ is not a global p-th power); put (Proposition 7) $\mathrm{g}_c(\ell)_{\chi_0^*} = 1 + \beta_0(\ell) \cdot \varpi^{\,p-n_0}$, $\beta_0(\ell) \in \mathbb{Z}_p[\varpi]$, where $\beta_0(\ell)$ is invertible modulo ϖ if and only if $\mathrm{g}_c(\ell)_{\chi_0^*}$ is not p-primary.

Whatever $\ell' \in \mathscr{L}_p$ and $\mathfrak{L}' \mid \ell'$, one has, from §4.3, case (ii), $\mathrm{g}_c(\ell')_{\chi_0^*} \equiv \mathrm{g}_c(\ell)_{\chi_0^*}^r \pmod p$, with $r \in [0,\, p^e - 1]$ ($r = 0$ if $\mathfrak{L}'_{\chi_0^*}$ is p-principal, thus $\mathrm{g}_c(\ell')_{\chi_0^*} \in K^{\times p}$), giving

$$\mathrm{g}_c(\ell')_{\chi_0^*} =: 1 + \beta_0(\ell') \cdot \varpi^{\,p-n_0},\quad \beta_0(\ell') \equiv r \cdot \beta_0(\ell) \pmod \varpi. \tag{12}$$

Contrary to the classical idea that $\beta_0(\ell) \pmod \varpi$ follow standard probabilities $\frac{O(1)}{p}$ (even under the condition $\mathrm{g}_c(\ell)_{\chi_0^*} \notin K^{\times p}$), we propose the following heuristic:

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

Because of the density theorems on the ideal classes when ℓ varies in $\mathscr{L}_p$ and χ in $\mathscr{X}_+$, we must examine two cases concerning the χ-components of $\mathcal{C}\ell$ when there exists $\chi_0 = \omega^{n_0} \in \mathscr{X}_+$ such that $\mathcal{C}\ell_{\chi_0^*} \simeq \mathbb{Z}/p^e\mathbb{Z}$, $e \ge 1$:

(a) $\chi \neq \chi_0$ and $\mathcal{C}\ell_{\chi *} = 1$. The numerical experiments show that when $\ell \in \mathscr{L}_p$ varies, $\mathrm{g}_c(\ell)_{\chi *} = 1 + \beta(\ell) \cdot \varpi^{p-n}$, with random $\beta(\ell) \pmod{\varpi}$ (probabilities $\frac{O(1)}{p}$).
(b) $\chi = \chi_0$ (and $\mathcal{C}\ell_{\chi_0^*} \neq 1$). If $\mathrm{g}_c(\ell)_{\chi_0^*}$ is p-primary for some given generator $\mathfrak{L}_{\chi_0^*}$, then from (12), all the $\mathrm{g}_c(\ell')_{\chi_0^*}$ are p-primary, whatever the class of $\mathfrak{L}'_{\chi_0^*}$ (p^e possibilities) because $\beta_0(\ell') \equiv 0 \pmod{\varpi}$. So, n_0 is always in $\mathscr{E}_\ell(p)$ and $\mathscr{E}_0(p) \cap \mathscr{E}_\ell(p) \neq \emptyset$ for all $\ell \in \mathscr{L}_p$, which corresponds to $\mathcal{C}\ell_{\chi_0} \neq 1$ and the non-cyclicity of $\mathcal{C}\ell_{\chi_0^*}^{(p)}$ (Theorem 14).

Thus, to have analogous densities of p-primarity on $\mathscr{L}_p$ (as for the p-principal case (a)), $\beta_0(\ell) \equiv 0 \pmod{\varpi}$ (*under the condition* $\mathrm{g}_c(\ell)_{\chi_0^*} \notin K^{\times p}$) must occur at least p times less, giving a 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 accurate properties of Gauss or Jacobi sums; for this, the computation of $\beta(\ell)$ should be very interesting (see [51] where, for any $\ell \equiv 1 \pmod{p}$, the coefficients $d_{i,k}$ of $J_i = \sum_{k=0}^{p-1} d_{i,k}\, \zeta_p^k$, with $\sum_{k=0}^{p-1} d_{i,k} = 1$, are studied and the starting point of future investigations, in relation with the other heuristics).

5.2.4. *Use of p-th power residue symbols and cyclotomic units.* We refer to [55, § 8.3] for the classical p-adic interpretation of the numbers $\#\mathcal{C}\ell_\chi$, for $\chi \in \mathscr{X}_+$, as indices of the form $(E_\chi : F_\chi)$, where F is the group of cyclotomic units. We need the following p-th power criterion (from [14, II.6.3.8]).

Lemma 25. *Let $\alpha \in K^\times$ be a pseudo-unit (namely, α is prime to p and $(\alpha) = \mathfrak{a}^p$). Let any set $\mathscr{S}$ of places $\mathfrak{q}$ of K such that $\langle c\ell(\mathscr{S})\rangle_{\mathbb{Z}} = \mathcal{C}\ell$ (or such that $\langle c\ell(\mathscr{S})\rangle_{\mathbb{Z}[G]} = \mathcal{C}\ell$ if $K(\sqrt[p]{\alpha})/\mathbb{Q}$ is Galois). Then $\alpha \in K^{\times p}$ if and only if α is p-primary and locally a p-th power at $\mathscr{S}$ (i.e., $\alpha \in K_\mathfrak{q}^{\times p}$ for all $\mathfrak{q} \in \mathscr{S}$ where $K_\mathfrak{q}$ is the $\mathfrak{q}$-completion of K).*

Proof. Consider the non-trivial direction, in the Galois case, assuming that α is p-primary and such that $\alpha \in K_\mathfrak{q}^{\times p}$ for all $\mathfrak{q} \in \mathscr{S}$. So $K(\sqrt[p]{\alpha})/K$ is unramified and $\mathscr{S}$-split; thus, due to the Galois condition, all the conjugates of $\mathfrak{q} \in \mathscr{S}$ are split and the Galois group of $K(\sqrt[p]{\alpha})/K$ corresponds, by class field theory, to a quotient of $\mathcal{C}\ell/\langle c\ell(\mathscr{S})\rangle_{\mathbb{Z}[G]}$, trivial by assumption. □

Theorem 26. *Let $\chi_0 = \omega^{n_0} \in \mathscr{X}_+$ with $n_0 \in \mathscr{E}_0(p)$ (set of exponents of p-irregularity) and $\mathcal{C}\ell_{\chi_0^*} \simeq \mathbb{Z}/p^e\mathbb{Z}$, $e \geq 1$ (i.e., $b_c(\chi_0^*) \sim p^e$). Let $\eta = \zeta_p^{\frac{1-c}{2}} \frac{1-\zeta_p^c}{1-\zeta_p}$ be a generating real cyclotomic unit, where c is a primitive root modulo p (cf.* [55, Proposition 8.11]).

(*i*) *There exists an infinite subset $\mathscr{L}_p(\chi_0) \subseteq \mathscr{L}_p$ of primes ℓ such that the G-module generated by the p-class of $\mathfrak{L} \mid \ell$ is $\mathcal{C}\ell_{\chi_0} \oplus \mathcal{C}\ell_{\chi_0^*}$.*
(*ii*) *$\mathcal{C}\ell_{\chi_0} \neq 1$ if and only if $\mathrm{g}_c(\ell)_{\chi_0^*}$ is locally a p-th power at $\mathfrak{p}$ but not at $\mathfrak{L}$ ($\ell \in \mathscr{L}_p(\chi_0)$).*
(*iii*) *$\mathcal{C}\ell_{\chi_0} \neq 1$ if and only if η_{χ_0} is locally a p-th power at $\mathfrak{p}$ and at $\mathfrak{L}$ ($\ell \in \mathscr{L}_p(\chi_0)$).*

Proof.

(i) In the $\mathbb{Z}_p[G]$-monogenous case, the ideals $\mathfrak{L}$ are of the form $(z) \cdot \mathfrak{A} \cdot \mathfrak{A}^*$, $z \in K^\times$, where $c\ell(\mathfrak{A})$ generates $\mathcal{C}\ell_{\chi_0}$ and $c\ell(\mathfrak{A}^*)$ generates $\mathcal{C}\ell_{\chi_0^*}$. (If, for instance, $\mathcal{C}\ell_{\chi_0} \simeq \mathcal{C}\ell_{\chi_0^*} \simeq \mathbb{Z}/p\mathbb{Z}$, these prime ideals $\mathfrak{L}$ have density $\left(1 - \frac{1}{p}\right)^2$; otherwise, if $\mathcal{C}\ell_{\chi_0} = 1$ and $\mathcal{C}\ell_{\chi_0^*} \simeq \mathbb{Z}/p\mathbb{Z}$, the density is $1 - \frac{1}{p}$.)

(ii) and (iii) Define the p-th power residue symbol $\left(\frac{\alpha}{\mathfrak{L}}\right) = \alpha^{\frac{\ell-1}{p}} \pmod{\mathfrak{L}}$ for $\mathfrak{L} \mid \ell \in \mathscr{L}_p$ when $\alpha \in K^\times$ is prime to $\mathfrak{L}$. By abuse of notation, we shall write $\left(\frac{\alpha}{p}\right) = 1$ if α is p-primary and $\left(\frac{\alpha}{\mathfrak{L}}\right) = 1$ if $\alpha \in K_{\mathfrak{L}}^{\times p}$ is not prime to $\mathfrak{L}$. Take $\ell \in \mathscr{L}_p(\chi_0)$:

(a) Consider $\alpha = \mathrm{g}_c(\ell)_{\chi_0^*} = [\tau(\psi)^{c-\sigma_c}]_{\chi_0^*}$, where $\left(\mathrm{g}_c(\ell)_{\chi_0^*}\right) = \mathfrak{L}_{\chi_0^*}^{b_c(\chi_0^*)}$ for a prime ideal $\mathfrak{L} \mid \ell$ (cf. (9)). This gives rise to a counterexample to Vandiver's conjecture at χ_0 if and only if α is p-primary, since $c\ell(\mathfrak{L}_{\chi_0^*})$ is a generator of $\mathcal{C}\ell_{\chi_0^*}$; it follows that $\left(\frac{\alpha}{\mathfrak{L}}\right) \neq 1$, otherwise, from Lemma 25 applied in H_{χ_0}, $\alpha = \mathrm{g}_c(\ell)_{\chi_0^*}$ should be a global p-th power (contradiction).

(b) Consider $\alpha = \eta_{\chi_0}$. Thus $b_c(\chi_0^*) \equiv 0 \pmod{p}$ is equivalent to the p-primarity of η_{χ_0}; so a counterexample to Vandiver's conjecture at χ_0, equivalent to $\eta_{\chi_0} \in E_{\chi_0}^p$, is equivalent to $\left(\frac{\eta_{\chi_0}}{\mathfrak{L}}\right) = 1$ since $\left(\frac{\eta_{\chi_0}}{p}\right) = 1$. Whence, with a prime $\mathfrak{L} \mid \ell \in \mathscr{L}_p(\chi_0)$:

$$\mathcal{C}\ell_{\chi_0} \neq 1 \Leftrightarrow \left(\frac{\mathrm{g}_c(\ell)_{\chi_0^*}}{\mathfrak{L}}\right) \neq 1 \;\&\; \left(\frac{\mathrm{g}_c(\ell)_{\chi_0^*}}{p}\right) = 1 \quad \text{and}$$

$$\mathcal{C}\ell_{\chi_0} \neq 1 \Leftrightarrow \left(\frac{\eta_{\chi_0}}{\mathfrak{L}}\right) = \left(\frac{\eta_{\chi_0}}{p}\right) = 1.$$

□

Let $\chi \in \mathscr{X}_+$ and $\ell \in \mathscr{L}_p(\chi)$ fixed. If $\mathrm{Prob}\left(\left(\frac{\mathrm{g}_c(\ell)_{\chi^*}}{\mathfrak{L}}\right) \neq 1\right)$ is close to 1, this suggests a probability around $\frac{O(1)}{p^2}$ for the p-primarity of $\mathrm{g}_c(\ell)_{\chi^*}$ if the above two symbols of η_χ are independent with probabilities $\frac{O(1)}{p}$ for a single ℓ.

So it is necessary to compute the symbol $\left(\frac{\mathrm{g}_c(\ell)_{\chi_0^*}}{\mathfrak{L}}\right)$ since $\mathrm{g}_c(\ell)_{\chi_0^*}$ and $\mathfrak{L}$ are non-independent data. For $\chi_0 = \omega^{n_0}$, $n_0 \in \mathscr{E}_0(p)$, the primes ℓ of the theorem are not effective, but experiments with random ℓ seem sufficient for statistics. Then a first condition for $\left(\frac{\mathrm{g}_c(\ell)_{\chi_0^*}}{\mathfrak{L}}\right) = 1$ is that $\mathrm{g}_c(\ell)_{\chi_0^*}$ be the p-th power of an ℓ-ideal, which is fulfilled since $b_c(\chi_0^*) \equiv 0 \pmod{p}$. Then, using a modification of the general program ("Appendix A.1"), computing $\mathrm{g}_c(\ell)_{\chi_0^*}$ in $\mathsf{Sn} \in \mathbb{Z}[\zeta_p]$ (in other words, *not reduced modulo* p), we divide this integer by the maximal power ℓ^v, so that there exists a prime ideal $\mathfrak{L} \mid \ell$ which does not divide this new integer (still denoted by Sn and the p-th power of an ℓ-ideal); the computation reduces to R, prime to $\mathfrak{L}$ and most likely random, whose symbol $\left(\frac{R}{\mathfrak{L}}\right) = R^{\frac{\ell-1}{p}} \pmod{\mathfrak{L}}$, computed in u, is immediate and gives the statistics. For a PARI/GP program computing these symbols and for numerical results, refer to § (d) of "Appendix B".

5.2.5. *Classical heuristics on class groups.* A first important reason for a very rare occurrence of the non-cyclic case for $\mathcal{C}\ell_{\chi*}^{(p)}$ may come from classical heuristics on p-class groups, assuming that they can be applied to ray class groups as $\mathcal{C}\ell_{\chi*}^{(p)}$ when it is, for instance, of order p^2.

Whatever the (numerous) references concerning this subject and independently of some improvements or questions on the relevance of the formulas giving $\mathrm{Prob}(\mathrm{rk}_p(C) = r)$ for such a p-group C, we observe that the quotient of the two probabilities for $r = 2$ and $r = 1$ (for instance, under the condition $\#C = p^2$) is at most $\frac{O(1)}{p}$ giving probabilities in $\frac{O(1)}{p^2}$ to have $\mathcal{C}\ell_{\chi *}^{(p)} \simeq (\mathbb{Z}/p\mathbb{Z})^2$. Since $\mathrm{rk}_p(\mathcal{C}\ell_\chi) = 1$ splits in the two cases of the reflection theorem, $\mathrm{rk}_p(\mathcal{C}\ell_\chi \oplus \mathcal{C}\ell_{\chi *}) = 2$ or $\mathrm{rk}_p(\mathcal{C}\ell_{\chi *}) = 2$, the above applies. As Nguyen Quang Do pointed out, this may come from the cohomological relation $\mathrm{H}^2(\mathcal{C}\ell_{\chi *}, (V/W)_{\chi *}) \simeq \mathbb{F}_p$, assuming the uniform randomness of the exact sequences

$$1 \to (V/W)_{\chi *} \simeq \mathbb{F}_p \to \mathcal{C}\ell_{\chi *}^{(p)} \to \mathcal{C}\ell_{\chi *} \simeq \mathbb{F}_p \to 1$$

(see the proof of Theorem 14 for notations and structure of $\mathcal{C}\ell_{\chi *}^{(p)}$), the non-cyclic case corresponding to the single cohomology class 0.

5.2.6. *Heuristics from p-ramification theory.* Another possible investigation is about the groups $\mathcal{T}_\chi$, $\chi \in \mathscr{X}_+$, and the formula $\#\mathcal{T}_\chi = \#\mathcal{C}\ell_\chi \cdot \#\mathcal{R}_\chi$ with the equivalence given by Theorem (8) of reflection, $\mathcal{C}\ell_{\chi *} \neq 1$ if and only if $\mathcal{T}_\chi \neq 1$.

Indeed, it is interesting to estimate in what proportions the relation $\#\mathcal{C}\ell_\chi \cdot \#\mathcal{R}_\chi \neq 1$ is due to $\mathcal{C}\ell_\chi$ or $\mathcal{R}_\chi$. Of course, it is impossible to experiment with the cyclotomic fields K; so, since this problem must be considered as general and may result from some insights in p-ramification theory as done in our articles (see [21] and its bibliography), we give some examples with quadratic and cyclic cubic fields in "Appendix C". The fact that $\mathcal{R}_\chi$ is much often non-trivial than $\mathcal{C}\ell_\chi$, in a computable proportion, is a positive argument for Vandiver's conjecture.

5.2.7. *Folk heuristic.* Consider $\tau(\psi) = -\sum_{k=0}^{\ell-2} \zeta_p^k \cdot \xi_\ell^{g^k}$ (where g is a primitive root mod ℓ, $\zeta_p = \psi(g)$, see (6)), and put $k = a\,p + b$, $0 \leq a \leq \frac{\ell-1}{p} - 1$, $0 \leq b \leq p-1$. Whence

$$\tau(\psi) = -\sum_{b=0}^{p-1} \zeta_p^b \cdot \left[\mathrm{Tr}_{\mathbb{Q}(\xi_\ell)/F_\ell}(\xi_\ell)\right]^{\sigma(b)}, \tag{13}$$

where F_ℓ is the cyclic sub-extension of degree p of $\mathbb{Q}(\xi_\ell)$, where $\sigma(b)$ is the automorphism acting trivially on ζ_p and such that $\xi_\ell \mapsto \xi_\ell^{g^b}$, giving an exact system of representatives for $\mathrm{Gal}(F_\ell/\mathbb{Q})$ independent of the choice of g.

From Remark 12 (ii), we know that F_ℓ is obtained as the decomposition over $\mathbb{Q}$ of the extension $K(\sqrt[p]{\alpha})/K$, with $\alpha = \tau(\psi)^p \in \mathbb{Z}[\zeta_p]$, and it is immediate to see that the p-class group of F_ℓ is trivial because of Chevalley's formula on invariant classes giving here $\#\mathcal{C}\ell_{F_\ell}^{\mathrm{Gal}(F_\ell/\mathbb{Q})} = 1$ since ℓ is the unique ramified prime in $F_\ell/\mathbb{Q}$.

(i) The first observation is that the p-class group of F_ℓ does not depend on that of K as ℓ varies! Indeed, this context is neither more nor less than class field theory over $\mathbb{Q}$ giving the existence of a unique cyclic extension F_ℓ of conductor $\ell \equiv 1 \pmod{p}$, for which one considers the set of conjugates of the relative trace of ξ_ℓ which moreover defines a normal basis of F_ℓ; then the unique link with the arithmetic of K is the linear combination (13) involving the traces to built α, but the character of $\langle\alpha\rangle_{\mathbb{Z}[G]} K^{\times p}/K^{\times p}$ is ω which gives, as we know, a 'poor' information on the arithmetic of K.
Thus, the relationship of $\alpha = \tau(\psi)^p$ (whence of $\tau(\psi)$) with class field theory over K (namely, with p-classes and units of K) is tenuous, possibly empty; which is quite

the opposite for the twists $\mathrm{g}_c(\ell) = \tau(\psi)^{c-\sigma_c}$ because of the relations $\alpha^{c-s_c} = \mathrm{g}_c(\ell)^p$ and the fact that the $\mathrm{g}_c(\ell)_{\chi^*}$ are radicals defining non-trivial (arithmetically) cyclic extensions of degree p of K_+ for any even character χ.

(ii) In another direction, suggested by the work of Lecouturier [34] generalizing results of Calegari–Emerton and Iimura, consider the non-Galois extension $\tilde{F}_\ell = \mathbb{Q}(\sqrt[p]{\tilde{\alpha}})$, where $\tilde{\alpha} = \ell$; of course, $K(\sqrt[p]{\tilde{\alpha}})/K$ is a cyclic extension of degree p (non-decomposed over a strict subfield of K), ramified at $p-1$ primes $\mathfrak{L} \mid \ell$ and at p if and only if $\ell \not\equiv 1 \pmod{p^2}$. On the contrary, as shown by many results of [21,34], the p-class group of $\tilde{F}_\ell$ strongly depends on the arithmetic of K while the radical $\tilde{\alpha}$ does not.

This second observation comes from the fact that, for $\tilde{M} = K(\sqrt[p]{\tilde{\alpha}})$,

$$\#\mathcal{C}\ell_{\tilde{M}}^{\mathrm{Gal}(\tilde{M}/K)} = \#\mathcal{C}\ell_K \cdot \frac{p^{p-2+\delta}}{(E_K : E_K \cap \mathrm{N}_{\tilde{M}/K}(\tilde{M}^\times))} \leq \#\mathcal{C}\ell_K \cdot p^{\frac{p-1}{2}},$$

where $\delta = 1$ or 0 according as p ramifies or not and where ζ_p is norm for $\delta = 0$; but the non-abelian Galois structure yields various non-trivial p-class groups for $\tilde{F}_\ell$ as ℓ varies, and the genera theory implies $\mathrm{rk}_p(\mathcal{C}\ell_{\tilde{F}_\ell}) \geq 1$ for all ℓ (for the metabelian genera theory, see [30]). However, for $M = K(\sqrt[p]{\alpha}) = F_\ell K$,

$$\#\mathcal{C}\ell_M^{\mathrm{Gal}(M/K)} = \#\mathcal{C}\ell_K \cdot \frac{p^{p-2}}{(E_K : E_K \cap \mathrm{N}_{M/K}(M^\times))} \leq \#\mathcal{C}\ell_K \cdot p^{\frac{p-1}{2}},$$

and we leave to the reader the computation of the (non-trivial) order of the minus part; but M/K decomposes into $F_\ell/\mathbb{Q}$ and only the isotopic component for the unit character is concerned, which gives in fact a trivial part of the above Chevalley's formula (contrary to the metabelian case $\tilde{M}/\mathbb{Q}$). So the 'folk heuristic' should be as follows:

Because of $F_\ell/\mathbb{Q}$ defined via the radical $\alpha = \tau(\psi)^p$, the p-adic properties of the Gauss sums are independent of the arithmetic of K as ℓ varies (despite the apparent complexity of the radical $\alpha = \tau(\psi)^p$), while the properties of $\tilde{F}_\ell/\mathbb{Q}$ are strongly dependent (despite the obvious simplicity of the radical $\tilde{\alpha} = \ell$).

In other words, we have probably some Galois 'dualities' about the arithmetic complexity of Kummer theory in the comparison 'radicals versus extensions'.

5.3 *Additive p-adic statistics*

Of course, we are only concerned with the multiplicative p-adic properties of the Gauss sums $\tau(\psi)$ and mainly of the twists $\mathrm{g}_c(\ell) = \tau(\psi)^{c-\sigma_c}$, and these are given by their χ^*-components for $\chi \in \mathscr{X}_+$. Nevertheless, the additive properties seem to follow more explicit rules, which is an interesting information about the numerical repartition and the independence as ℓ varies, and this probably has an impact on the multiplicative properties regarding the results of § 4.2 and § 4.3. We shall examine the case of the twists $\mathrm{g}_c(\ell)$ (more precisely, of $\psi^{-c}(c)\,\mathrm{g}_c(\ell)$), and then the case of the original Gauss sums $\tau(\psi)$ from the arithmetic of the fields F_ℓ.

5.3.1. *$\mathbb{Z}$-rank of the family $\left(\psi^{-c}(c)\,\mathrm{g}_c(\ell)\right)_{\ell \in \mathscr{L}_p}$.* Put, for p and c fixed,

$$\mathbf{J}(\ell) = \psi^{-c}(c)\,\mathrm{g}_c(\ell) = \psi^{-c}(c)\,\tau(\psi)^{c-\sigma_c} = J_1 \cdots J_{c-1} \text{ (see (10))} \tag{14}$$

written on the basis of $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$, under the form $\mathbf{J}(\ell) = \sum_{k=0}^{p-2} a_k(\ell)\,\zeta_p^k$, the integers $a_k(\ell)$ being considered modulo p.

A first information about the p-adic repartition of the $\mathbf{J}(\ell)$ as ℓ varies, is to compute the $\mathbb{F}_p$-rank of the $\mathbb{F}_p$-matrix $\big(a_k(\ell)\big)_{k,\ell}$. The following program gives *systematically*

$$\mathrm{Rank}_{\mathbb{F}_p}\big[\big(a_k(\ell)\big)_{\ell,k}\big] = p-4,$$

for all the primes $p \geq 7$ tested (rank 1 for $p=3$ and rank 2 for $p=5$), *despite the fact that the lines are not canonical* (up to circular permutations of their elements since $\mathbf{J}(\ell)$ is defined up to conjugation). We have verified it up to $p \leq 331$, an interval which contains 16 irregular primes.

The program gives p (in p), the $\mathbb{F}_p$-rank of the matrix (in rank) and the least ℓ_p (in elp) for which the sub-matrix built from $\{\ell \in \mathscr{L}_p,\ \ell \leq \ell_p\}$ has rank $p-4$:

```
{forprime(p=7,500,c=lift(znprimroot(p));P=polcyclo(p)+Mod(0,p);M=matrix(0,p-1);
r=0;for(i=1,10^8,el=1+2*i*p;if(isprime(el)!=1,next);g=znprimroot(el);J=1;
for(i=1,c-1,Ji=0;for(k=1,el-2,kk=znlog(1-g^k,g);e=lift(Mod(kk+i*k,p));
Ji=Ji-x^e);J=J*Ji);J=lift(Mod(J,P));V=vector(p-1,j,component(J,j));
A=concat(M,V);rr=matrank(A);if(rr==r,next);r=rr;M=A;
if(r==p-4,print("p=",p," r=",r," elp=",el);break)))}
```

```
p  rank  elp        p   rank  elp        p   rank   elp        p   rank   elp
7   3    113        11   7    397        13   9     599        17   13    1259
(...)
71  67   42743      73   69   48473      79   75    50087      83   79    65239
151 147  247943     157  153  273181     163  159   294053     167  163   305611
```

We have $\mathbf{J}(\ell) \equiv 1 \pmod{\mathfrak{p}}$, in other words, $\sum_{k=0}^{p-2} a_k(\ell) \equiv 1 \pmod{p}$, and we can write

$$\mathbf{J}(\ell) = 1 + \sum_{k=1}^{p-2} a_k(\ell)\,(\zeta_p^k - 1)$$

depending on $p-2$ parameters; then, due to the relations $\mathbf{J}(\ell)^{1+s_{-1}} \equiv 1 \pmod{p}$ and $\mathbf{J}(\ell)^{e_\omega} \in K^{\times p}$ (because $\omega(c-s_c) \equiv 0 \pmod{p}$), this yields the three relations of 'derivation' (for $p \geq 7$) $\sum_{k=1}^{p-2} k^\delta \cdot a_k(\ell) \equiv 0 \pmod{p}$, $\delta \in \{1,2,4\}$, for any $\ell \in \mathscr{L}_p$. Whence a $\mathbb{F}_p$-rank at most $p-4$, but we have no proof of the equality.

The order of magnitude of ℓ_p seems to be

$$\ell_p = O(1)\, p^2 \log(p^2), \tag{15}$$

which is in agreement with a 'conductor' p^2 for these Hecke Grössencharacters [56, Theorem, p. 489], but the program slows down very much as p increases, to be more accurate.

Moreover, the number of consecutive primes ℓ needed to reach the rank $p-4$ is equal to $p-4$, except probably for finitely many cases, which confirms the above order.

Give now the end of the above table with an estimation of the $O(1)$ in (15):

```
p    elp     O(1)     p    elp    O(1)     p    elp    O(1)     p    elp    O(1)
211 517373  1.0856   223 628861  1.1693   227 604729  1.0816   229  631583  1.1082
233 642149  1.0849   239 695491  1.1116   241 684923  1.0750   251  784627  1.1269
257 862493  1.1766   263 819509  1.0631   269 928051  1.1461   271  906767  1.1019
277 925181  1.0719   281 1055437 1.1853   283 979747  1.0834   293  988583  1.0136
307 1174583 1.0881   311 1214767 1.0941   313 1203799 1.0692   317  1276243 1.1026
```

The $\mathbb{F}_p$-rank $r_p(\ell)$ of the $p-1$ conjugates of $\mathbf{J}(\ell) \pmod{p}$, $\ell \in \mathscr{L}_p$, is close to $p-4$ (e.g., for $p=37$, $r_{37}(\ell) \in \{33, 32, 31, 30\}$ in similar proportions, and we only have the local minimum $(r_{37}(\ell), \ell) = (29, 2591)$ for ℓ up to 37000.

5.3.2. *Repartition of the conjugates of the traces* $\mathrm{Tr}_{\mathbb{Q}(\xi_\ell)/F_\ell}(\xi_\ell)$. Let Z_{F_ℓ} be the ring of integers of the degree p subfield F_ℓ of $\mathbb{Q}(\mu_\ell)$ and let $Z_{F_\ell}/p\,Z_{F_\ell}$ be the residue ring mod p. These residue rings are isomorphic to $\mathbb{F}_{p^p}$ or to $\mathbb{F}_p^p$, but there is no canonical map between them as $\ell \in \mathscr{L}_p$ varies. Thus, in (13), giving $\tau(\psi) = -\sum_{b=0}^{p-1} \zeta_p^b \cdot \left[\mathrm{Tr}_{\mathbb{Q}(\xi_\ell)/F_\ell}(\xi_\ell)\right]^{\sigma(b)}$, the images in $Z_{F_\ell}/p\,Z_{F_\ell}$ of the conjugates of the relative traces $\mathrm{Tr}(\xi_\ell) = \mathrm{Tr}_{\mathbb{Q}(\xi_\ell)/F_\ell}(\xi_\ell)$ may be easily analyzed and compared, for $\ell \in \mathscr{L}_p$, by means of the image R_ℓ in $\mathbb{F}_p[x]$ of the polynomial $Q_\ell = \prod_{\bar\sigma \in \mathrm{Gal}(F_\ell/\mathbb{Q})} \left(x - \mathrm{Tr}(\xi_\ell)^{\bar\sigma}\right) \in \mathbb{Z}[x]$.

PROPOSITION 27

Let $\ell_1, \ell_2 \in \mathscr{L}_p$ and let $\tau(\psi_1)$, $\tau(\psi_2)$ be the corresponding Gauss sums normalized via $\psi_1(g_1) = \psi_2(g_2) = \zeta_p$. Let $F = F_{\ell_1}F_{\ell_2}$. If $R_{\ell_1} \neq R_{\ell_2}$, then for all $\sigma \in \mathrm{Gal}(FK/\mathbb{Q})$, $\tau(\psi_2) \not\equiv \tau(\psi_1)^\sigma \pmod{\mathfrak{p}^p Z_{FK}}$.

Proof. Suppose there exists $\sigma \in \mathrm{Gal}(FK/\mathbb{Q})$ such that $\tau(\psi_2) \equiv \tau(\psi_1)^\sigma \pmod{\mathfrak{p}^p Z_{FK}}$; recall that $\tau(\psi_1)^\sigma = \zeta_\sigma\, \tau(\psi_1^e)$, $\zeta_\sigma \in \mu_p$, $e \in (\mathbb{Z}/p\mathbb{Z})^\times$. Then

$$\tau(\psi_2) = -\sum_{b=0}^{p-1} \zeta_p^b \cdot \mathrm{Tr}(\xi_{\ell_2})^{\sigma_2(b)} \quad \text{and} \quad \tau(\psi_1)^\sigma = -\sum_{b=0}^{p-1} \zeta_p^b \cdot \mathrm{Tr}(\xi_{\ell_1})^{\pi(\sigma_1(b))},$$

where π is a permutation of the $\sigma_1(b)$. Using $\mathrm{Tr}_{\mathbb{Q}(\xi_{\ell_i})/\mathbb{Q}}(\xi_{\ell_i}) = -1$, we get

$$\tau(\psi_2) = 1 - \sum_{b=1}^{p-1} (\zeta_p^b - 1) \cdot \mathrm{Tr}(\xi_{\ell_2})^{\sigma_2(b)},$$
$$\tau(\psi_1)^\sigma = 1 - \sum_{b=1}^{p-1} (\zeta_p^b - 1) \cdot \mathrm{Tr}(\xi_{\ell_1})^{\pi(\sigma_1(b))},$$

whence

$$\begin{aligned}\tau(\psi_1)^\sigma - \tau(\psi_2) &= \sum_{b=1}^{p-1} (\zeta_p^b - 1) \cdot \left(\mathrm{Tr}(\xi_{\ell_2})^{\sigma_2(b)} - \mathrm{Tr}(\xi_{\ell_1})^{\pi(\sigma_1(b))}\right) \\ &\equiv 0 \pmod{\mathfrak{p}^p Z_{FK}}.\end{aligned}$$

Since $\zeta_p^b - 1$, $b \in [1, p-1]$, define a $\mathbb{Z}$-basis of $\mathfrak{p}\,Z_K$, then a Z_F-basis of $\mathfrak{p}\,Z_{FK}$. This relation implies $\mathrm{Tr}(\xi_{\ell_2})^{\sigma(b)} \equiv \mathrm{Tr}(\xi_{\ell_1})^{\pi'(\sigma(b))} \pmod{p}$ for all b, which yields $R_{\ell_1} = R_{\ell_2}$ in $\mathbb{F}_p[x]$ (a contradiction). □

Since $\tau(\psi_2) \not\equiv \tau(\psi_1)^\sigma \pmod{\mathfrak{p}^p}$ for all σ implies $\mathrm{g}_c(\ell_2) \not\equiv \mathrm{g}_c(\ell_2)^\sigma \pmod{\mathfrak{p}^p}$ for all σ (except for the ω-components because $\omega(c - \sigma_c) \equiv 0 \pmod{p}$), we can say that the number of distinct polynomials R_ℓ, $\ell \in \mathscr{L}_p$ gives a partial idea of the repartition modulo p of the sets $\mathscr{E}_\ell(p)$ as ℓ varies. As p increases, the number of distinct R_ℓ seems to be $O(p^2 \cdot \log(p^2))$.

The following program, computing the monic polynomial $\mathsf{R} = R_\ell \in \mathbb{F}_p[x]$ returns: $\mathsf{el} = \ell$, the residue degree $\mathsf{f} = f$ of p in $F_\ell/\mathbb{Q}$, and R.

```
{p=7;B=5*10^3;el=1;while(el<B,el=el+2*p;if(isprime(el)!=1,next);g=znprimroot(el);
h=g^p;g=lift(g);h=lift(h);P=polcyclo(el);z=Mod(x,P);Q=1;e=1;for(k=1,p,Tr=0;e=e*g;
for(j=1,(el-1)/p,e=e*h;e=lift(Mod(e,el));Tr=Tr+z^e);Q=Q*(T-Tr));
Q=component(lift(Q),1);R=0; for(i=0,p,C=component(Q,i+1);C=lift(Mod(C,p));
R=R+x^i*C);F=znorder(Mod(p,el));f=1;v=valuation(F,p);w=valuation(el-1,p);
if(w==v,f=p);print("el=",el," f=",f," R=",R))}

el=29    f=7     R=x^7 + x^6 + 2*x^5 + 5*x + 1
el=43    f=1     R=x^7 + x^6 + 3*x^5 + 3*x^3 + 6*x^2
el=71    f=7     R=x^7 + x^6 + 5*x^5 + 3*x^4 + 2*x^3 + 6*x^2 + 4
el=4943  f=7     R=x^7 + x^6 + 3*x^5 + x^4 + x^3 + 3*x + 5
el=4957  f=7     R=x^7 + x^6 + 4*x^5 + 2*x^4 + 5*x^3 + 3*x^2 + 2*x + 1
el=4999  f=7     R=x^7 + x^6 + 4*x^3 + 5*x^2 + 2*x + 6
```

It is hopeless to write wide lists of polynomials R_ℓ for large p, but any experiment suggests a random distribution of the (non-independent) coefficients (except that of x^{p-1} since $\mathrm{Tr}_{\mathbb{Q}(\xi_\ell)/\mathbb{Q}}(\xi_\ell) = -1$). For $p = 3$, the six possible polynomials are of the form R_ℓ. For $p = 5$ (resp. $p = 7$), there are 150 (resp. 17192) possible polynomials.

(i) For $p = 5$, we obtain the following end of the calculations (two days of computer; it seems that only 35 distinct polynomials R_ℓ are available):

```
el=5591   f=5     R=x^5 + x^4 + 4*x^3 + x^2 + 4*x + 2
el=6211   f=1     R=x^5 + x^4 + x^3 + x^2 + x
el= 6271  f=1     R=x^5 + x^4 + 2*x^3 + 4*x^2 + 3*x + 4
el=1345   f=1     R=x^5 + x^4
```

(ii) For $p = 7$, ℓ up to 17977, we get painfully a little more than 250 distinct R_ℓ, but the exact number is unknown.

Remark 28. It is clear that a large number of polynomials R_ℓ strengthens Vandiver's conjecture since the corresponding $\mathbf{J}(\ell) = \psi^{-c}(c)\, \mathrm{g}_c(\ell)$ cover sufficiently possibilities modulo p, especially since we know that the $\mathbb{F}_p$-rank associated to the family of $\big(\mathbf{J}(\ell)\big)_{\ell\in\mathscr{L}_p}$ is probably always $p-4$, but these informations are not 'equivalent'. Moreover, an assumption about the order of magnitude of $\mathscr{N}_p = \#\{R_\ell,\ \ell \in \mathscr{L}_p\}$ *is not necessary* to obtain Vandiver's conjecture for p; indeed, a *single* suitable ℓ may ensure a positive test for Vandiver's conjecture as shown by the table given in "Appendix A.2".

We propose the following heuristic about the sets $\mathscr{E}_\ell(p)$ of exponents of p-primarity for which the reference [25] may be useful:

The probability of $\mathscr{E}_\ell(p) = \emptyset$, for a single $\ell \in \mathscr{L}_p$, is $(1 + o(1)) \cdot e^{-\frac{1}{2}}$; that of at least a counterexample to Vandiver's conjecture is of the form $O(1)\left(1 - e^{-\frac{1}{2}}\right)^{\mathscr{N}_p}$, where $\mathscr{N}_p = \#\{R_\ell,\ \ell \in \mathscr{L}_p\}$, with the polynomial $R_\ell = \prod_{\bar\sigma\in\mathrm{Gal}(F_\ell/\mathbb{Q})}\left(x - \mathrm{Tr}_{\mathbb{Q}(\xi_\ell)/F_\ell}(\xi_\ell)^{\bar\sigma}\right)$ seen in $\mathbb{F}_p[x]$.

6. Conclusion

Under these experiments and heuristics, and those given in the appendices, the existence of sets $\mathscr{E}_\ell(p)$, disjoint from $\mathscr{E}_0(p)$, or probably the existence of primes $\ell \in \mathscr{L}_p$ such that $\mathscr{E}_\ell(p) = \emptyset$, may occur conjecturally for all p. Possibly, our computations in "Appendix

A.2" show the existence of general properties of the sets $\mathscr{E}_\ell(p)$ coming from the fact that *all* $\ell \in \mathscr{L}_p$ *intervene* (and that these primes are probably independent), which is a new argument compared with classical ones. This is strengthened by the computation of the conjugates of the traces $\mathrm{Tr}_{\mathbb{Q}(\xi_\ell)/F_\ell}(\xi_\ell)$, as $\ell \in \mathscr{L}_p$ varies (coefficients of the Gauss sums), the fields $\mathbb{Q}(\mu_\ell)$ being, *a priori*, independent of the arithmetic of K.

Remark 29. There are two constraints for the Gauss and Jacobi sums that we have considered, but they only concern the auxiliary prime numbers $\ell \in \mathscr{L}_p$:

(i) The p-classes of ideals $\mathfrak{L} \mid \ell$, $\ell \in \mathscr{L}_p$, are all represented with standard densities.
(ii) The ideal factorization of $\tau(\psi)^p$ is related to *congruences modulo the conjugates of a prime ideal* $\mathfrak{L} \mid \ell$ *and is canonical* (this yields Stickelberger's theorem and its consequences [55, § 15.1], [7,43,56] for the annihilation of $\mathcal{C}\ell_{\chi_0^*}^{(p)}$ with generalizations of the Stickelberger ideal). A similar context is that of the ℓ-adic Γ-function of Morita.

However, since we consider characters ψ of order p, the *p-adic congruential properties* of Gauss sums (or Jacobi sums) do not follow any known law (in our opinion, the classical literature being mute about this).

These fundamental p-adic properties of Gauss sums may have crucial consequences in various domains since Vandiver's conjecture is often required; for instance: in [8] about the Galois cohomology of Fermat curves, in [47] for the root numbers of the Jacobian varieties of Fermat curves, then in several papers on Galois p-ramification theory as in [37,44–46] or [53,54] in relation with modular forms, then in numerous papers and books on the theory of deformations of Galois representations as in [4,38], Iwasawa's theory context and cyclotomy, as in [6] on Ihara series, [3] for μ-invariants in Hida families, [31] for the main conjecture of the Iwasawa theory.

Then it may be legitimate to think that all these numerous basic congruential aspects of Gauss sums are (logically) governing principles of a wide part of algebraic number theory, as follows: beyond the case of the p-th cyclotomic field (not to mention all the geometrical aspects as the theory of elliptic curves where some analogies can be found, and all the generalizations of the present abelian case over a number field $k \neq \mathbb{Q}$):

Gauss and Jacobi sums $\longrightarrow$ Hecke Grössencharacters $\longrightarrow$ Stickelberger element $\longrightarrow$ p-adic L-functions $\longrightarrow$ Herbrand–Ribet theorem $\longrightarrow$ Main Theorem on abelian fields $\longrightarrow$ annihilation of the p-torsion group $\mathcal{T}$ of real abelian fields $\longrightarrow$ universal isomorphism $\mathcal{T} \simeq \mathrm{H}^2(G_{S_p}, \mathbb{Z}_p)^* \longrightarrow$ p-rationality of fields ($\mathcal{T} = 1$) $\longrightarrow$ cohomological obstructions in Galois theory $\longrightarrow \cdots$

which gives again an example of a *basic p-adic problem*, analogous to those we have analyzed about deep conjectures: Greenberg's conjectures (on Iwasawa theory over totally real fields [22] and on representation theory [24]), p-rationalities of a number field as $p \to \infty$, generalizations of the conjecture of Ankeny–Artin–Chowla from the conjectural existence of a p-adic Brauer–Siegel theorem [20].

As shown by the evidences given in § 5.2, Vandiver's conjecture may be justified, for $p \gg 0$, by the Borel–Cantelli heuristic, on exceptional features of Gauss sums; but this point of view allows cases of failure of the conjecture, which is not satisfactory for the theoretical foundations of the above quoted fundamental subjects.

To be optimistic (but not very rigorous), one can say that Vandiver's conjecture is true because it holds for sufficiently many prime numbers [5,26] since probabilities may be in

$\frac{O(1)}{p^{\lambda(p)}}$, $\lambda(p) \to \infty$. In a more serious claim, we can say that Vandiver's conjecture holds for almost all prime numbers; the accurate cardinality of the finite set of counterexamples ($\emptyset$ or not) is (in our opinion) not of algebraic nature nor enlightened by class field theory, Galois cohomology or Iwasawa's theory, but is perhaps accessible by the way of analytical/geometrical techniques or depends on a more general hypothetic 'complexity theory' in number theory.

Acknowledgements

The author is very grateful to the referee for many linguistic corrections and valuable suggestions which have improved the presentation of the paper in various aspects.

7. Appendices

Appendix A: Illustration of the first Theorem 21

*Appendix A.*1: *Program computing* $\mathscr{E}_\ell(p)$

For $p \in [3, 199]$ and for the least $\ell \in \mathscr{L}_p$, the program computes $\mathsf{g}_c(\ell) = \tau(\psi)^{c-\sigma_c}$ in mod(J,P) with P=polcyclo(p), where $\mathsf{J} = \mathsf{J}_1 \cdots \mathsf{J}_{\mathsf{c}-1}$ is written in $\mathbb{Z}[x]$ modulo $p\,\mathbb{Z}[x]$; c is a primitive root (mod p) (see the relation (10)). For the computation of J_i, we use the discrete logarithm znlog to interprete the $1 - g^k$ in $g^{\mathbb{Z}/(\ell-1)\mathbb{Z}}$. We put $\chi = \omega^n$ and $\chi^* = \omega^{1-n}$, taking n=2*m for m in $[1, (p-3)/2]$.
The program takes into account the relation $J^{1+s_{-1}} \equiv 1 \pmod{p}$ in the action of the idempotents and drops the coefficient $\frac{1}{p-1}$ in $e_{\chi*}$ (in which $\chi^*(s_a^{-1})$ is replaced by the residue of a^{n-1} modulo p), thus computes in reality $\mathsf{g}_c(\ell)^{-1/2}$ up to p-th powers. Then the polynomials Jj give, in the list LJ, the powers J^j modulo p, $j = 1, \ldots, p-1$.
The result is given in $\mathsf{Sn} = \prod_{\mathsf{a}=1}^{(\mathsf{p}-1)/2} \mathsf{s}_\mathsf{a}(\mathsf{J}^{\mathsf{an}})$, from $\mathsf{g}_c(\ell)_{\chi*}^{-1/2} = \prod_{a=1}^{(p-1)/2} s_a\big(\mathsf{g}_c(\ell)^{\omega^{n-1}(a)}\big)$ (up to a p-th power), where $\omega^{n-1}(a) \equiv a^{n-1} \pmod{p}$ is computed in an and J^{an} is given by component(LJ,an). The conjugate $\mathsf{s}_\mathsf{a}(\mathsf{J}^{\mathsf{an}})$ is computed in sJan via the conjugation $\mathsf{x} \mapsto \mathsf{x}^\mathsf{a}$ in J^{an}, whence the product in Sn (the exponents of p-primarity are denoted expp). Thus a line such as p = 109 el = 1091 c = 6 g = 2 expp: 14, 86 means that for $p = 109$, $\ell = 1091$ is the least prime number $\equiv 1 \pmod{p}$, c, g are the primitive roots, then $n = 14$ and $n = 86$ are the exponents of p-primarity of the twists $\mathsf{g}_c(\ell)_{\chi*}$, for $\chi = \omega^n$:

```
{forprime(p=3,200,c=lift(znprimroot(p));P=polcyclo(p)+Mod(0,p);
X=Mod(x,P);el=1;while(isprime(el)==0,el=el+2*p);g=znprimroot(el);
print("p=",p," el=",el," c=",c," g=",g);J=1;for(i=1,c-1,Ji=0;
for(k=1,el-2,kk=znlog(1-g^k,g);e=lift(Mod(kk+i*k,p));Ji=Ji-X^e);J=J*Ji);
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,p-2,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   el=7   c=2  g=3                p=97  el=389  c=5  g=2 expp:26
p=5   el=11  c=2  g=2                p=101 el=607  c=2  g=3 expp:10
p=7   el=29  c=2  g=2                p=103 el=619  c=5  g=3
```

```
p=11  el=23  c=3  g=5 expp:2          p=107 el=643  c=2  g=11
p=13  el=53  c=2  g=2                 p=109 el=1091 c=6  g=2 expp:14,86
p=17  el=103 c=3  g=5                 p=113 el=227  c=3  g=2
p=19  el=191 c=4  g=19                p=127 el=509  c=3  g=2
p=23  el=47  c=2  g=5                 p=131 el=263  c=2  g=5 expp:16
p=29  el=59  c=2  g=2 expp:2          p=137 el=823  c=3  g=3 expp:78
p=31  el=311 c=7  g=17                p=139 el=557  c=2  g=2
p=37  el=149 c=2  g=2                 p=149 el=1193 c=2  g=3
p=41  el=83  c=6  g=2                 p=151 el=907  c=6  g=2
p=43  el=173 c=9  g=2 expp:26         p=157 el=1571 c=5  g=2 expp:94
p=47  el=283 c=2  g=3                 p=163 el=653  c=2  g=2 expp:42
p=53  el=107 c=2  g=2 expp:34,10      p=167 el=2339 c=5  g=2 expp:122
p=59  el=709 c=3  g=2                 p=173 el=347  c=2  g=2
p=61  el=367 c=2  g=6                 p=179 el=359  c=2  g=7 expp:138
p=67  el=269 c=4  g=2                 p=181 el=1087 c=2  g=3 expp:114,164
p=71  el=569 c=2  g=3                 p=191 el=383  c=19 g=5
p=73  el=293 c=5  g=2                 p=193 el=773  c=5  g=2 expp:108,172
p=79  el=317 c=2  g=2                 p=197 el=3547 c=2  g=2 expp:62
p=83  el=167 c=3  g=5                 p=199 el=797  c=3  g=2
p=89  el=179 c=3  g=2
```

For large p, the computations are slower, but the number of exponents of p-primarity remains small.

Appendix A.2: Minimal prime $\ell \in \mathscr{L}_p$ such that $\mathscr{E}_\ell(p) = \emptyset$

The following program examines, for each p, the successive prime numbers $\ell_i \in \mathscr{L}_p$, $i \geq 1$, 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 $O\left(\dfrac{\log(p)}{\log(\log(p))}\right)$, the intersection $\mathscr{E}_\ell(p) \cap \mathscr{E}_0(p)$ 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=3,100,c=lift(znprimroot(p));P=polcyclo(p)+Mod(0,p);
N=0;T=1;el=1;while(T==1,el=el+2*p;if(isprime(el)==1,N=N+1;g=znprimroot(el);
J=Mod(1,P);for(i=1,c-1,Ji=0;for(k=1,el-2,kk=znlog(1-g^k,g);
e=lift(Mod(kk+i*k,p));Ji=Ji-x^e);J=J*Ji);LJ=List;Jj=1;
for(j=1,p-1,Jj=lift(Jj*J);listinsert(LJ,Jj,j));T=0;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=0;for(j=0,p-2,aj=lift(Mod(a*j,p));sJan=sJan+x^(aj)*component(Jan,1+j));
Sn=Sn*sJan);if(Sn==1,T=1;break));if(T==0,print(p," ",el," ",N);break))))}
```

Thus, a line such as 601 25243 5 gives, for $p = 601$, the least prime $\ell = \ell_N \equiv 1 \pmod{p}$ such that $\mathscr{E}_\ell(p) = \emptyset$; the integer $N = 5$ means that the previous primes $\ell = 3607, 6011, 7213, 16829$ in the list are such that $\mathscr{E}_\ell(p) \neq \emptyset$. For $p < 400$, we only write the primes p, ℓ_N for which $N > 1$, then a complete list for $p \in [409, 683]$:

p	el	N	p	el	N	p	el	N	p	el	N	p	el	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.

Appendix B: Illustration of the theorems with $p = 37$

(*a*) *Computation of the sets* $\mathscr{E}_\ell(p)$. So it is fundamental to see if the sets $\mathscr{E}_\ell(p)$ are independent (or not) of the choice of $\ell \in \mathscr{L}_p$ for $\mathscr{E}_0(p) \neq \emptyset$. We analyze the case of $p = 37$ ($n_0 = 32$) giving $\#\mathcal{C}\ell_{\omega^5} = 37$ and compute (in expp) the sets $\mathscr{E}_\ell(37)$ when $\ell \in \mathscr{L}_{37}$ varies. If $n_0 = 32 \in \mathscr{E}_\ell(37)$, then $\mathfrak{L}_{\chi *}$ is necessarily 37-principal and $\mathrm{g}_c(\ell)_{\omega^5} \in K^{\times 37}$:

```
{p=37;c=lift(znprimroot(p));P=polcyclo(p)+Mod(0,p);X=Mod(x,P);
for(i=1,100,el=1+2*i*p;if(isprime(el)!=1,next);g=znprimroot(el);
print("el=",el," g=",lift(g));J=1;for(i=1,c-1,Ji=0;for(k=1,el-2,kk=znlog(1-g^k,g);
e=lift(Mod(kk+i*k,p));Ji=Ji-X^e);J=J*Ji);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,p-2,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)))))}
```

```
Table I: 149<el<7000
el=149      g=2                          el=3331     g=3   expp: 22
el=223      g=3                          el=3701     g=2
el=593      g=3                          el=3923     g=2
el=1259     g=2                          el=4219     g=2   expp: 18,16
el=1481     g=3    expp: 30              el=4441     g=21
el=1777     g=5                          el=4663     g=3
el=1999     g=3                          el=5107     g=2
el=2221     g=2                          el=5477     g=2
el=2591     g=7    expp: 34              el=6143     g=5   expp: 28
el=2887     g=5                          el=6217     g=5
el=3109     g=6                          el=6661     g=6
el=3257     g=3                          el=6883     g=2

Table II:  742073 <el<800000
el=742073   g=3    expp: 12              el=768343   g=11  expp: 18
el=742369   g=7                          el=768491   g=10
el=742591   g=3                          el=768787   g=2   expp: 20
el=743849   g=3                          el=769231   g=11  expp: 24
el=743923   g=3    expp: 16              el=769453   g=2   expp: 30
el=744071   g=22                         el=772339   g=3
el=744811   g=10                         el=773153   g=3   expp: 14
el=744959   g=13   expp: 10              el=774337   g=5   expp: 28
el=745033   g=10   expp: 16              el=774929   g=3   expp: 18
el=745181   g=2                          el=775669   g=10  expp: 18
```

```
el=745477   g=2
el=745699   g=2
el=746069   g=2
el=746957   g=2
el=747401   g=3
el=747919   g=3
el=748807   g=6    expp: 22
el=749843   g=2    expp: 34
el=750287   g=5
el=750509   g=2    expp: 14,22
el=751027   g=3
el=751841   g=3    expp: 14,16,24
el=752137   g=10   expp: 8
el=752359   g=3    expp: 18
el=752581   g=2    expp: 16
el=752803   g=2    expp: 22,32
el=753617   g=3
el=753691   g=11   expp: 16
el=753839   g=7    expp: 4,22
el=754283   g=2
el=755171   g=6
el=755393   g=3    expp: 22
el=756281   g=3    expp: 2
el=756799   g=15   expp: 18
el=757243   g=2
el=757909   g=2    expp: 16
el=758279   g=7
el=758501   g=2    expp: 18
el=759019   g=2
el=759167   g=5    expp: 12
el=759463   g=3
el=759833   g=3    expp: 4
el=760129   g=11
el=760499   g=2
el=762053   g=2
el=762571   g=10
el=763237   g=2
el=764051   g=2
el=764273   g=3
el=764717   g=2    expp: 2
el=765383   g=5
el=765827   g=2    expp: 34
el=766049   g=3    expp: 22
el=766937   g=3    expp: 34
el=767381   g=2    expp: 18
el=767603   g=5    expp: 34
el=767677   g=5
el=776483   g=2
el=776557   g=2    expp: 20
el=777001   g=31   expp: 18,28
el=778111   g=11
el=778333   g=2    expp: 28
el=778777   g=5
el=779221   g=2
el=779591   g=7
el=779887   g=10   expp: 18
el=780257   g=3    expp: 8
el=780553   g=10
el=781367   g=5    expp: 34
*el=781589  g=2    expp: 32
 el=782107  g=2
 el=782329  g=13   expp: 18
 el=782921  g=3    expp: 20
 el=783143  g=5
 el=783661  g=2
 el=784327  g=3
 el=784697  g=3
 el=784919  g=7
 el=785363  g=2
 el=786251  g=2
 el=786547  g=2
 el=787139  g=2    expp: 20
 el=787361  g=6
 el=787879  g=6    expp: 10,18,20
 el=788027  g=2    expp: 34
 el=789137  g=3    expp: 24
 el=790099  g=2
 el=791209  g=7
 el=791431  g=12
 el=791801  g=3
*el=792023  g=5    expp: 32
 el=792689  g=3
 el=793207  g=5
 el=795427  g=2
*el=795649  g=22   expp: 2,32
 el=795797  g=2
 el=795871  g=3
 el=796759  g=3
 el=796981  g=7
 el=797647  g=3
 el=797869  g=10
 el=798461  g=2
 el=798757  g=2
 el=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 number of times. For $\ell = 1481$, one finds a p-primarity for $\chi^* = \omega^7$ ($\chi = \omega^{30} \neq \omega^{32}$). Theorem 23 applies at will.

It remains to give statistics about the p-principality (or not) of the $\mathfrak{L}_{\chi_0^*}$ when $\ell \in \mathscr{L}_p$ varies. For $p = 37$, $\mathfrak{L}_{\chi_0^*}$ is 37-principal if and only if $\mathfrak{L}$ is principal since the class number of K is $h = 37$.

(*b*) *Table of the classes of ideals* $\mathfrak{L}$ *in* $\mathbb{Q}(\mu_{37})$. 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. We only write the cases where $\mathscr{E}_\ell(37) \neq \emptyset$.

For instance, the line el = 64381 ∗ expp : 6, 32 [x^20 + x^9 + x] means that for $\ell = 64381$, the exponents of 37-primarity are $n = 6$, $n = 32$, and that any prime ideal $\mathfrak{L} \mid \ell$ in $K = \mathbb{Q}(x)$ (with $x = \zeta_{37}$) is principal and generated by the integer $x^{20} + x^9 + x$ (as given by PARI/GP):

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

```
el=1481    expp: 30
el=2591    expp: 34
el=3331    expp: 22
el=4219    expp: 16,18
el=6143    expp: 28
el=7993    expp: 16,20
el=8363    expp: 8
el=9769    expp: 20
el=10657   expp: 4,18,26
el=12433   expp: 20
el=13099   expp: 28
el=14431   expp: 4,14,22
el=17021   expp: 6
el=17909   expp: 30
el=18131   expp: 22
el=19463   expp: 6
el=20129   expp: 6
el=21017   expp: 2,4
el=21313   expp: 18
el=21757   expp: 8
el=22349   expp: 8
el=23459   expp: 6
el=23977   expp: 26
el=25087   expp: 26
el=25457   expp: 30
el=29009   expp: 8,24
el=30859   expp: 2
el=32783*  expp: 32 [x^11+x^3+x]
el=33301   expp: 30
el=33967   expp: 26
el=36187   expp: 8
el=37889   expp: 16
el=38629   expp: 22
el=40627   expp: 30
el=40849   expp: 6
el=42773   expp: 4
el=45289   expp: 8
el=45659   expp: 26
el=48619   expp: 8
el=48989   expp: 20
el=51283   expp: 14,16
el=51431   expp: 20
el=56167   expp: 10,14,26
el=57203   expp: 34
el=58313   expp: 28
el=58757   expp: 16,18
el=58831   expp: 24,30
el=59497   expp: 28
el=61051   expp: 10
el=62383   expp: 2
el=62753   expp: 2
el=63493   expp: 2
el=64381*  expp: 6,32  [x^20+x^9+x]
el=66749   expp: 30
el=67489*  expp: 30,32 [x^24-x^3-x^2]
el=67933   expp: 6
el=68821*  expp: 32    [x^15-x^9+x^4]
el=69931   expp: 12
el=71411   expp: 4
el=72817   expp: 28
el=74149   expp: 2
el=75407   expp: 10
el=75629   expp: 12, 20
el=76961   expp: 14
el=78737   expp: 28
el=79181   expp: 10
el=80513   expp: 16, 26
el=81031   expp: 18, 34
el=82067   expp: 34
el=83621   expp: 34
el=83843   expp: 2
el=84731   expp: 6
el=85027   expp: 26
el=86729   expp: 22
el=86951   expp: 8
el=87691   expp: 24
el=91243   expp: 22, 34
el=91909   expp: 30
el=94351   expp: 10
el=94573   expp: 18
el=95239   expp: 18, 28
el=96497   expp: 10
el=98347   expp: 28
el=98939   expp: 30
```

```
el=53281   expp: 16                    el=99679   expp: 10, 22
el=55057   expp: 20                    el=100049  expp: 14
```

We give some examples ($\mathfrak{L}^{1+s_{-1}}$ is always principal giving an easy characterization):

(*i*) *Non-principal case* $\mathfrak{L} \mid 149$. The instruction bnfisintnorm(K, 149^{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 the real integer:

```
-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
```

(*ii*) *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 global 37-th power (which explains that one shall find the exponent of 37-primarity $n_0 = 32$ equal to that of 37-irregularity in the table); unfortunately, the data are too large to be given.
Nevertheless, the reader can easily compute factor(norm(Sn)) $= 32783^{37\cdot 16\cdot 9}$ and use K=bnfinit(P,1); idealfactor(K,Sn), which gives the 37-th power of $\mathfrak{L} \mid 32783$.
We obtain the following excerpts of the table (up to 10^6) of principal cases (i.e., for $p = 37$, the line el $= 64381$ expp : 6, 32 indicates that the exponents of 37-primarity are 6 and 32 and that the prime ideals above 64381 are principal):

```
el=32783    expp:32       el=64381    expp:6,32          el=67489    expp:30,32
el=68821    expp:32       el=108929   expp:32            el=132313   expp:32
el=325379   expp:10,32    el=332039   expp:6,10,14,32    el=351797   expp:32
el=364451   expp:28,32    el=387169   expp:32            el=396937   expp:32
el=960151   expp:32       el=973397   expp:32            el=983239   expp:32
el=1000777  expp:32       el=1002109  expp:2,32          el=1040959  expp:20,32
```

(*c*) *Densities of the exponents of p-primarity in* $\mathbb{Q}(\mu_{37})$ *and* $\mathbb{Q}(\mu_{157})$. The following program intends to show that all exponents of p-primarity are obtained, with (perhaps) some specific densities, taking sufficiently many $\ell \in \mathscr{L}_p$ (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 Eel).

```
{p=37;c=lift(znprimroot(p));P=polcyclo(p)+Mod(0,p);X=Mod(x,P);Nel=0;Npp=0;Eel=List;
for(j=1,(p-3)/2,listput(Eel,0,j));for(i=1,1000,el=1+2*i*p;if(isprime(el)!=1,next);
g=znprimroot(el);Nel=Nel+1;J=1;for(i=1,c-1,Ji=0;for(k=1,el-2,kk=znlog(1-g^k,g);
e=lift(Mod(kk+i*k,p));Ji=Ji-X^e);J=J*Ji);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=LJ[an];sJan=Mod(0,P);for(j=0,p-2,
aj=lift(Mod(a*j,p));sJan=sJan+x^(aj)*component(Jan,1+j));Sn=Sn*sJan);
if(Sn==1,Npp=Npp+1;listput(Eel,1+Eel[n/2],n/2);print(Nel," ",Npp," ",el," ",Eel))))}
```

In the first column, one shall find the index i (in Nel) 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 (in Npp); then the third one is ℓ_i (in el). In some cases, a prime ℓ gives rise to several exponents of p-primarity:

(*i*) *Results for* $p = 37$. The end of the table for the selected interval is (two excerpts):

```
Nel  Npp    el
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]

3889 1819 1863913[106,114,108,113,99,111,115,100,117,113,116,93,103,97,108,103,103]
3894 1820 1865911[106,114,108,114,99,111,115,100,117,113,116,93,103,97,108,103,103]
3898 1821 1868501[106,114,108,114,100,111,115,100,117,113,116,93,103,97,108,103,103]
3900 1822 1869389[106,114,108,114,100,112,115,100,117,113,116,93,103,97,108,103,103]
3900 1823 1869389[106,114,108,114,100,112,115,101,117,113,116,93,103,97,108,103,103]
3900 1824 1869389[106,114,108,114,100,112,115,101,117,113,116,93,104,97,108,103,103]
```

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 37-th power.

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

```
Nel Npp   el
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,
               5,3,2,2,1,5,7,6,2,2,1,5,5,5,4,4,3,3,4,5,4,5,5,5,5,3,6,1,6,3,5,4,5,
                                          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:

```
Nel Npp   el
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]
```

These numbers may depend on the orders of ω^n and/or ω^{p-n}, but this needs to be clarified taking much $\ell \in \mathscr{L}_p$.

(*d*) *Symbols computations for* $\mathrm{g}_c(\ell)_{\chi_0^*}$. The program computes the symbol $\left(\frac{\mathrm{g}_c(\ell)_{\chi_0^*}}{\mathfrak{L}}\right)$ in the field $\mathbb{Q}(\mu_{37})$ (see § 5.2.4):

```
{p=37;n=32;print("p=",p," n=",n);c=lift(znprimroot(p));P=polcyclo(p);X=Mod(x,P);
for(i=1,100,el=1+2*i*p;if(isprime(el)!=1,next);g=znprimroot(el);M=(el-1)/p;J=1;
for(i=1,c-1,Ji=0;for(k=1,el-2,kk=znlog(1-g^k,g);e=lift(Mod(kk+i*k,p));
Ji=Ji-X^e);J=J*Ji);LJ=List;Jj=1;for(j=1,p-1,Jj=lift(Jj*J);listinsert(LJ,Jj,j));
Sn=1;for(a=1,p-1,an=lift(Mod(a,p)^(n-1));Jan=LJ[an];sJan=Mod(0,P);
```

```
for(j=0,p-2,aj=lift(Mod(a*j,p));sJan=sJan+X^(aj)*component(Jan,1+j));Sn=Sn*sJan);
Sn=lift(Sn);s=valuation(Sn-1,p);v=valuation(Sn,el);Sn=Sn/el^v;ro=g^M;
for(b=1,p-1,r=lift(ro^b);R=0;for(k=0,p-2,R=R+component(Sn,k+1)*r^k);
if(valuation(R,el)==0,y=R;break));u=lift(Mod(y,el)^M);
print("p=",p," el=",el," v=",v," u=",u);if(s!=0,print("Sn local pth power at P"));
if(Mod(v,p)==0 & u==1,print("Sn local pth power at L"));
if(Mod(v,p)!=0 || u!=1,print("Sn NON local pth power at L"));
if(Mod(v,p)==0 & u==1 & s!=0,print("Sn GLOBAL pth power"))))}

p=37  n=32
el=149     v=259   u=102    Sn NON local pth power at L
el=223     v=259   u=132    Sn NON local pth power at L
el=6883    v=259   u=6850   Sn NON local pth power at L
el=7253    v=259   u=4947   Sn NON local pth power at L
el=32783   v=259   u=1      Sn local pth power at P
el=32783   v=259   u=1      Sn local pth power at L
el=32783   v=259   u=1      Sn GLOBAL pth power
```

We found $u = \left(\frac{\mathrm{g}_c(\ell)_{\chi_0^*}}{\mathfrak{L}}\right) = 1$ for the following ℓ (including the underlined numbers corresponding to primes $\ell \notin \mathscr{L}_p(\chi_0)$ such that $\mathrm{g}_c(\ell)_{\chi_0^*} \in K^{\times p}$, i.e., $\mathcal{L}$ p-principal):

$\ell \in \{22571;\ \underline{32783};\ 46103;\ 53503;\ 57943;\ \underline{64381};\ \underline{67489};\ \underline{68821};\ 79847;\ 83177;\ 96497;\ 98939;\ 104933;\ \underline{108929};\ 117883;\ \underline{132313};\ 146521;\ \underline{146891};\ 151553;\ 151849;\ 158657;\ 158731;\ \underline{167759};\ \underline{172717};\ 197359;\ \underline{198839};\ \underline{207497}\}$

confirming the existence and rarity of primes ℓ in the interval [149; 207497] such that $u = 1$, by accident ($\mathrm{g}_c(\ell)_{\chi_0^*} \notin K^{\times p}$, i.e., $\mathcal{L}$ non-p-principal).

For $n = 22 \notin \mathscr{E}_0(37)$, we found $u = 1$ for few examples (up to $2 \cdot 10^5$):

$\ell \in \{2221; 2887; 3923; 49211; 51283; 69709; 147779; 164503; 170497; 179969;\ 192697; 197803\}$,

but $\mathrm{g}_c(\ell)_{\chi^*}$ is not the p-th power of an ℓ-ideal, whence it is never in $K_{\mathfrak{L}}^{\times p}$. One finds an exponent of p-primarity 22 for $\ell = 3331$, then 14, 16 for $\ell = 51283$, 10 for $\ell = 147779$, and 28 for $\ell = 164503$. In the exceptional case $\ell = 3331$, $\mathrm{g}_c(\ell)_{\chi^*}$ is p-primary.

This confirms the expected properties of the symbol $\left(\frac{\mathrm{g}_c(\ell)_{\chi_0^*}}{\mathfrak{L}}\right)$. A similar program computing the two symbols of η_{χ_0} gives all the expected results.

(*e*) *Vandiver's conjecture and the* 37*-adic regulator of* $\mathbb{Q}(\mu_{37})_+$. We return to the case $p = 37$ and $n_0 = 32$. 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 $\mathcal{T}_{k_9} \neq 1$ from the reflection relation of Theorem (8); so, k_9 admits a cyclic 37-ramified extension of degree 37 which is not unramified. To verify, we use [17, Program I], for real fields, which indeed gives $\#\,\mathcal{T}_{k_9} = 37$ (nt must verify $\mathsf{p}^{\mathsf{nt}} > p^t$, the exponent of $\mathcal{T}$):

```
{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=Kpn[5][2];L=List;
e=matsize(Hpn)[2];R=0;for(k=1,e-1,c=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_+ [19, Proposition 5.2]. Whence $\#\mathcal{T}_\chi = \#\mathcal{C}\ell_\chi \cdot \#\mathcal{R}_\chi$ and $\mathcal{R}_{\chi*} = 1$, for all $\chi \in \mathscr{X}_+$; but we have $\#\mathcal{T}_{\chi*} = \#\tilde{\mathcal{C}}\ell_{\chi*}$ for the subgroup $\tilde{\mathcal{C}}\ell_{\chi*}$ of $\mathcal{C}\ell_{\chi*}$. The above data shows that the relation $\#\mathcal{T}_{\chi_0} = 37$ comes from $\#\mathcal{R}_{\chi_0} = 37$, which is not surprising because of the following:

*Remark B*1. 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 [55, Corollary 8.19], applied in [5,26] and developed in [50,51]) consists in finding $\ell \in \mathscr{L}_p$ such that η_{χ_0} is not a local p-th power at ℓ proving Vandiver's conjecture at χ_0; so when we find that $\mathcal{R}_{\chi_0} \neq 1$ (with $\mathcal{C}\ell_{\chi_0} = 1$), this means that η_{χ_0} generates E_{χ_0} and is a local p-th power at p by p-primarity, so that $K\left(\sqrt[p]{\eta_{\chi_0}}\right)$ is contained in the χ_0^*-component of the p-Hilbert class field of K. From § 5.2.4, the probability of p-primarity of $\mathrm{g}_c(\ell)_{\chi_0^*}$ may be at most $\frac{O(1)}{p^2}$.

Appendix C: Heuristics from p-ramification theory

We give the two examples of real quadratic fields and cyclic cubic fields. This suggests that for totally real fields (like K_+), abelian p-ramification is essentially governed by the normalized p-adic regulator and that the p-class group is in some sense a 'secondary' invariant.

(*a*) *Real quadratic fields and* $p \geq 3$ *fixed.* For each of the ND real quadratic field of discriminant D ∈ [bD, BD], for which $\mathcal{T} \neq 1$ (counted in Nt), we compute the proportions of cases for which this is due to $\#\mathcal{C}\ell$ or $\#\mathcal{R}$. We favor the case $\mathcal{C}\ell \neq 1$ (counted in Nh) even if the two groups $\mathcal{C}\ell$ and $\mathcal{R}$ are both non-trivial; this may give a slightly larger proportion for $\frac{\mathsf{Nh}}{\mathsf{Nt}}$ but a much faster program:

```
{p=3;bD=10^6;BD=10^6+5*10^4;ND=0;Nh=0;Nt=0;
for(D=bD,BD,e=valuation(D,2);M=D/2^e;
if(core(M)!=M,next);if((e==1||e>3)||(e==0&Mod(M,4)!=1)||(e==2&Mod(M,4)==1),next);
m=D;if(e!=0,m=D/4);ND=ND+1;P=x^2-m;K=bnfinit(P,1);Kpn=bnrinit(K,p^2);
Hpn0=Kpn.no;Hpn=Kpn.cyc;Hpn1=Hpn[1];vptor=valuation(Hpn0/Hpn1,p);
if(vptor>=1,Nt=Nt+1;h=K.no;vph= valuation(h,p);
if(vph>=1,Nh=Nh+1)));print("[",bD,", ",BD,"]");print
("p=",p," ND=",ND," Nt=",Nt," Nh=",Nh," Nh/Nt=",Nh/Nt+0.," 1/p=",1./p)}
[bD, BD]=[1000000, 1050000]
p=3   ND=15204   Nt=7308   Nh=2050   Nh/Nt=0.28051450  1/p=0.33333333
p=5   ND=15204   Nt=3522   Nh=634    Nh/Nt=0.18001135  1/p=0.20000000
p=7   ND=15204   Nt=2464   Nh=331    Nh/Nt=0.13433441  1/p=0.14285714
p=11  ND=15204   Nt=1497   Nh=97     Nh/Nt=0.06479625  1/p=0.09090909
[bD, BD]=[10000000, 10050000]
p=3   ND=15198   Nt=7516   Nh=2161   Nh/Nt=0.28751995  1/p=0.33333333
p=5   ND=15198   Nt=3597   Nh=720    Nh/Nt=0.20016680  1/p=0.20000000
p=7   ND=15198   Nt=2443   Nh=347    Nh/Nt=0.14203847  1/p=0.14285714
p=11  ND=15198   Nt=1512   Nh=122    Nh/Nt=0.08068783  1/p=0.09090909
```

```
[bD, BD]=[100000000, 100100000]
p=3   N=30410    Nt=15133  Nh=4456   Nh/Nt=0.29445582  1/p=0.33333333
p=5   N=30410    Nt=7122   Nh=1502   Nh/Nt=0.21089581  1/p=0.20000000
```

The proportion Nh/Nt becomes close to $\frac{1}{p}$ for intervals with large discriminants.

(*b*) *Cyclic cubic fields and* $p \equiv 1 \pmod 3$ *fixed.* We obtain analogous results with the same rough calculation (e.g., we may have $\mathcal{C}\ell_{\chi_1} \neq 1$ and $\mathcal{R}_{\chi_1} \neq 1$ or $\mathcal{R}_{\chi_2} \neq 1$), but this does not affect the statistics (f ∈ [bf, Bf] denotes the conductor); the program uses the classical representation of f, under the form $\frac{a^2+27b^2}{4}$ with some congruences on a and b, and the corresponding defining polynomials:

```
{p=7;bf=10^5;Bf=5*10^5;Nf=0;Nh=0;Nt=0;for(f=bf,Bf,e=valuation(f,3);
if(e!=0 & e!=2,next);F=f/3^e;if(Mod(F,3)!=1||core(F)!=F,next);F=factor(F);
D=component(F,1);d=component(matsize(F),1);for(j=1,d-1,l=component(D,j);
if(Mod(l,3)!=1,break));for(b=1,sqrt(4*f/27),if(e==2 & Mod(b,3)==0,next);
A=4*f-27*b^2;if(issquare(A,&a)==1,if(e==0,if(Mod(a,3)==1,a=-a);
P=x^3+x^2+(1-f)/3*x+(f*(a-3)+1)/27);if(e==2,if(Mod(a,9)==3,a=-a);
P=x^3-f/3*x-f*a/27);Nf=Nf+1;K=bnfinit(P,1);Kpn=bnrinit(K,p^2);
Hpn0=Kpn.no;Hpn=Kpn.cyc;Hpn1=Hpn[1];vptor=valuation(Hpn0/Hpn1,p);
if(vptor>=1,Nt=Nt+1;h=K.no;vph= valuation(h,p);
if(vph>=1,Nh=Nh+1)))));print("[",bf,", ",Bf,"]");print
("p=",p," Nf=",Nf," Nt=",Nt," Nh=",Nh," Nh/Nt=",Nh/Nt+0.0," 1/p=",1./p)}
```

```
[bf, Bf]=[50000, 100000]
p=7   Nf=7928   Nt=2302   Nh=344    Nh/Nt=0.14943527   1/p=0.14285714
[bf, Bf]=[100000, 500000]
p=7   Nf=63427  Nt=18533  Nh=2690   Nh/Nt=0.14514649   1/p=0.14285714
[bf, Bf]=[100000, 500000]
p=13  Nf=63427  Nt=9979   Nh=754    Nh/Nt=0.07555867   1/p=0.07692307
[bf, Bf]=[100000, 500000]
p=19  Nf=63427  Nt=6850   Nh=389    Nh/Nt=0.05678832   1/p=0.05263157
[bf, Bf]=[100000, 500000]
p=31  Nf=63427  Nt=4316   Nh=139    Nh/Nt=0.03220574   1/p=0.03225806
```

References

[1] Anglès B and Nuccio FAE, On Jacobi sums in $\mathbb{Q}(\zeta_p)$, *Acta Arithmetica* **142(3)** (2010) 199–218, https://perso.univ-st-etienne.fr/nf51454h/PDF/jacobi.pdf

[2] Bayer–Fluckiger E, Emery V and Houriet J, 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] Bellaïche J and Pollack R, Congruences with Eisenstein series and μ-invariants, *Compositio Mathematica* **155(5)** (2019) 863–901, https://doi.org/10.1112/S0010437X19007127

[4] Berger T, Oddness of residually reducible Galois representations, *Int. J. Number Theory* **14(5)** (2018) 1329–1345, https://doi.org/10.1142/S1793042118500835

[5] Buhler J P and Harvey D, Irregular primes to 163 million, *Math. Comp*. **80(276)** (2011) 2435–2444, https://doi.org/10.1090/S0025-5718-2011-02461-0

[6] Coleman R F, Anderson–Ihara theory: Gauss sums and circular units, Algebraic number theory, Adv. Stud. Pure Math., vol. 17 (1989) (Boston, MA: Academic Press) pp. 55–72, https://doi.org/10.2969/aspm/01710055

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

[8] Davis R and Pries R, Cohomology groups of Fermat curves via ray class fields of cyclotomic fields (2018) https://arxiv.org/pdf/1806.08352

[9] Ellenberg J S and Venkatesh A, Reflection principles and bounds for class group torsion, *Int. Math. Res. Not.* **2007(1)** (2007) https://doi.org/10.1093/imrn/rnm002
[10] Ghate E, Vandiver's conjecture via K-theory, Summer School on Cyclotomic Fields, Pune (1999) http://www.math.tifr.res.in/%7Eeghate/vandiver.pdf
[11] Gras G and Jaulent J-F, Sur les corps de nombres réguliers, *Math. Z.* **202(2)** (1989) 343–365, https://eudml.org/doc/174095
[12] Gras G, Étude d'invariants relatifs aux groupes des classes des corps abéliens, Journées Arithmétiques de Caen (Univ. Caen, Caen, 1976) pp. 35–53, Astérisque, No. 41–42, Soc. Math. France, Paris (1977) http://www.numdam.org/book-part/AST_1977__41-42__35_0/
[13] Gras G, Sur la p-ramification abélienne, Conférence donnée à l'University Laval, Québec, Mathematical Series of the Department of Mathematics vol. 20 (1984) pp. 1–26, https://www.dropbox.com/s/fusia63znk0kcky/Lectures1982.pdf?dl=0
[14] Gras G, Class Field Theory: From Theory to Practice, corr. 2nd ed., Springer Monographs in Mathematics (2005) (Springer) xiii+507 pages, https://doi.org/10.1007/978-3-662-11323-3
[15] Gras G, Approche p-adique de la conjecture de Greenberg pour les corps totalement réels, *Ann. Math. Blaise Pascal* **24(2)** (2017) 235–291, http://ambp.cedram.org/item?id=AMBP_2017__24_2_235_0
[16] Gras G, Normes d'idéaux dans la tour cyclotomique et conjecture de Greenberg, *Ann. Mathématiques du Québec* **43(2)** (2019) 249–280, https://doi.org/10.1007/s40316-018-0108-3
[17] Gras G, On p-rationality of number fields, Applications – PARI/GP Programs, Publ. Math. Fac. Sci. Besançon (Algèbre et Théorie des Nombres) no. 2 (2019), pp. 29–51. https://pmb.centre-mersenne.org/item/PMB_2019___2_29_0/
[18] Gras G, Annihilation of $\mathrm{tor}_{\mathbb{Z}_p}(\mathcal{G}_{K,S}^{\mathrm{ab}})$ for real abelian extensions $K/\mathbb{Q}$, *Commun. Adv. Math. Sci*. **1(1)** (2018) 5–34, http://dergipark.gov.tr/download/article-file/543993
[19] Gras G, The p-adic Kummer–Leopoldt constant: Normalized p-adic regulator, *Int. J. Number Theory* **14(2)** (2018) 329–337, https://doi.org/10.1142/S1793042118500203
[20] Gras G, Heuristics and conjectures in direction of a p-adic Brauer–Siegel theorem, *Math. Comp*. **88(318)** (2018)–(2019) 1929–1965, https://doi.org/10.1090/mcom/3395
[21] Gras G, Practice of the incomplete p-ramification over a number field – History of abelian p-ramification, *Commun. Adv. Math. Sci*. **2(4)** (2019) 251–280, https://dergipark.org.tr/en/download/article-file/906434
[22] Greenberg R, On the Iwasawa invariants of totally real number fields, *Amer. J. Math*. **98(1)** (1976) 263–284, http://www.jstor.org/stable/2373625?
[23] Greenberg R, On the Jacobian variety of some algebraic curves, *Compositio Math*. **42(3)** (1980) 345–359, http://www.numdam.org/article/CM_1980__42_3_345_0.pdf
[24] Greenberg R, Galois representations with open image, *Ann. de Mathématiques du Québec* **40(1)** (2016) 83–119, https://doi.org/10.1007/s40316-015-0050-6
[25] Gupta S and Don Zagier, On the coefficients of the minimal polynomials of Gaussian periods, *Math. Comp*. **60(201)** (1993) 385–398, https://www.jstor.org/stable/2153175
[26] Hart W, Harvey D and Ong W, Irregular primes to two billion, *Math. Comp*. **86(308)** (2017) 3031–3049, https://doi.org/10.1090/mcom/3211
[27] Ichimura H and Kaneko M, On the universal power series for Jacobi sums and the Vandiver conjecture, *J. Number Theory* **31(3)** (1989) 312–334, https://core.ac.uk/download/pdf/81986387.pdf
[28] Ichimura H, Local units modulo Gauss sums, *J. Number Theory* **68(1)** (1998) 36–56, https://doi.org/10.1006/jnth.1997.2206
[29] Iwasawa K, A note on Jacobi sums, *Symposia Mathematica* vol. 15 (1975) (Academic Press) pp. 447–459
[30] Jaulent J-F, Unités et classes dans les extensions métabéliennes de degré $n\ell^s$ sur un corps de nombres algébriques, *Ann. Inst. Fourier (Grenoble)* **31(1)** (1981) 39–62, http://www.numdam.org/article/AIF_1981__31_1_39_0.pdf/
[31] Kakde M and Wojtkowiak Z, A note on the main conjecture over $\mathbb{Q}$ (2018) https://arxiv.org/pdf/1812.04360

[32] Kersten I and Michaličeк J, On Vandiver's conjecture and $\mathbb{Z}_p$-extensions of $\mathbb{Q}(\zeta_{p^n})$, *J. Number Theory* **32(3)** (1989) 371–386, https://doi.org/10.1016/0022-314X(89)90091-7

[33] Kurihara M, Some remarks on conjectures about cyclotomic fields and K-groups of $\mathbb{Z}$, *Compositio Math*. **81(2)** (1992) 223–236, http://www.numdam.org/item/CM_1992__81_2_223_0

[34] Lecouturier E, On the Galois structure of the class group of certain Kummer extensions, *J. London Math. Soc*. **98(2)** (2018) 35–58, https://doi.org/10.1112/jlms.12123

[35] Maire C, Genus theory and governing fields, *New York J. Math*. **24** (2018) 1056–1067, https://www.emis.de/journals/NYJM/NYJM/nyjm/j/2018/24-50v.pdf

[36] McCallum W G, Greenberg's conjecture and units in multiple $\mathbb{Z}_p$-extensions, *Amer. J. Math*. **123(5)** (2001) 909–930, https://www.jstor.org/stable/25099088

[37] McCallum W G and Sharifi R T, A cup product in the Galois cohomology of number fields, *Duke Math. J*. **120(2)** (2003) 269–310, http://math.ucla.edu/~sharifi/pairing.pdf

[38] Mézard A, Obstructions aux déformations de représentations galoisiennes réductibles et groupes de classes, *Journal de théorie des nombres de Bordeaux* **17(2)** (2005) 607–618, https://doi.org/10.5802/jtnb.510

[39] Mihăilescu P, Turning Washington's Heuristics in Favor of Vandiver's Conjecture, in: Essays in Mathematics and its Applications in Honor of Stephen Smale's 80th Birthday, edited by P Pardalos and T Rassias (2012) (Springer-Verlag) pp. 287–294, http://poivs.tsput.ru/en/Biblio/Publication/11335

[40] Ribet K A, A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$, *Invent. Math*. **34(3)** (1976) 151–162, https://math.berkeley.edu/~ribet/Articles/invent_34.pdf

[41] Ribet K A, Bernoulli numbers and ideal classes, in: L'héritage scientifique de Jacques Herbrand, Gaz. Math. vol. 118 (2008) pp. 42–49, https://smf.emath.fr/publications/la-gazette-des-mathematiciens-118-octobre-2008

[42] Schoof R, Class numbers of real cyclotomic fields of prime conductor, *Math. Comp*. **72(242)** (2003) 913–937, https://doi.org/10.1090/S0025-5718-02-01432-1

[43] Schmidt C G, On ray class annihilators of cyclotomie fields, *Invent. Math*. **66(2)** (1982) 215–230, https://eudml.org/doc/142878

[44] Sharifi R T, On Galois groups of unramified pro-p extensions, *Math. Ann*. **342(2)** (2008) 297–308, https://doi.org/10.1007/s00208-008-0236-1

[45] Sharifi R T, A reciprocity map and the two-variable p-adic L-function, *Ann. Math. (2)* **173(1)** (2011) 251–300, https://www.jstor.org/stable/29783202

[46] Sharifi R T, Relationships between conjectures on the structure of pro-p Galois groups unramified outside p, in: Arithmetic Fundamental Groups and Noncommutative Algebra (Berkeley, CA, 1999) Proc. Sympos. Pure Math., vol. 70 (2002) (Providence, RI: Amer. Math. Soc.) pp. 275–284

[47] Shu J, Root numbers and Selmer groups for the Jacobian varieties of Fermat curves (2018) https://arxiv.org/pdf/1809.09285

[48] Soulé C, Perfect forms and the Vandiver conjecture, *J. Reine Angew. Math*. **517** (1999) 209–221, https://doi.org/10.1515/crll.1999.095

[49] Soulé C, A bound for the torsion in the K-theory of algebraic integers, *Documenta Math*. **Extra Vol. Kato** (2003) 761–788, http://preprints.ihes.fr/M02/M02-82.pdf

[50] Thaine F, On the p-part of the ideal class group of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and Vandiver's conjecture, *Michigan Math. J*. **42(2)** (1995) 311–344, https://projecteuclid.org/euclid.mmj/1029005231

[51] Thaine F, On the coefficients of Jacobi sums in prime cyclotomic fields, *Trans. Amer. Math. Soc*. **351(12)** (1999) 4769–4790, https://doi.org/10.1090/S0002-9947-99-02223-0

[52] The PARI Group, PARI/GP, version `2.9.0` (2016) (Université de Bordeaux)

[53] Wake P and Erickson C W, Ordinary pseudorepresentations and modular forms, *Proc. Amer. Math. Soc. Ser. B* **4** (2017) 53–71, https://doi.org/10.1090/bproc/29

[54] Wake P and Erickson C W, Pseudo-modularity and Iwasawa theory, *Amer. J. Math*. **140(4)** (2018) 977–1040, https://doi.org/10.1353/ajm.2018.0022

[55] Washington L C, Introduction to cyclotomic fields, Graduate Texts in Mathematics, vol. 83 (1997) (New York: Springer-Verlag) xiv+487 pp.
[56] Weil A, Jacobi sums as "Grössencharaktere", *Trans. Amer. Math. Soc*. **73** (1952) 487–495 https://www.jstor.org/stable/1990804

COMMUNICATING EDITOR: U K Anandavardhanan