Test of Vandiver's conjecture with Gauss sums – Heuristics

Georges Gras

TEST OF VANDIVER'S CONJECTURE WITH GAUSS SUMS – HEURISTICS

GEORGES GRAS

Abstract. The link between Vandiver's conjecture and Gauss sums is well-known since the papers of Iwasawa (1975) and Anglès–Nuccio (2010); this context has been considered by many authors with various purposes (Iwasawa theory, Galois cohomology, Fermat curves,...). We prove again the 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 pth cyclotomic field, from a lecture we gave at the Laval University (1984). Then we provide a specific use of Gauss sums of characters of order p of $\mathbb{F}_\ell^\times$ allowing a necessary and sufficient condition for Vandiver's conjecture (Theorem 4.6 and corollaries 4.7, 4.8, using both the sets of exponents of p-irregularity and of p-primarity of suitable products of Jacobi sums obtained as twists of Gauss sums). We propose § 5.2 new heuristics and numerical experiments to strengthen our arguments in direction of Vandiver's conjecture and we show that any counterexample leads to excessive constraints modulo p on the above twists as ℓ varies. All the calculations are given with their PARI/GP programs.

Contents

Date: September 25, 2018 – November 14, 2018 – December 6, 2018.

1991 *Mathematics Subject Classification.* 11R18, 11L05, 11R37, 11R29, 08-04.

Key words and phrases. Cyclotomic fields; Vandiver's conjecture; Gauss sums; Jacobi sums; Kummer theory; Stickelberger's theorem; Class field theory; p-ramification.

1. Introduction

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

The Vandiver (or Kummer–Vandiver) conjecture asserts that $\mathcal{C}\ell_+$ is trivial. This statement is equivalent to say that the group of real cyclotomic units is of prime to p index in E_+ [43, Theorem 8.14]. See numerical tables using this property in [4, 8] (verifying the conjecture up to $2 \cdot 10^9$), and more general results in [41, 42] where some relations with Gauss and Jacobi sums are used, in a different framework, to determine the order of the isotypic components of $\mathcal{C}\ell_+$ (e.g., [41, Theorem 4]).

Many heuristics are known about this conjecture; see Washington's book [43, § 8.3, Corollary 8.19] for some history, criteria, and for probabilistic arguments, then see [32]. We have also given a probabilistic study in [12, II.5.4.9.2]. All these heuristics lead to the fact that the number of primes p less than p_0, giving a counterexample, can be of the form $O(1)\cdot\log(\log(p_0))$.

These reasonings, giving the possible existence of infinitely many counterexamples to Vandiver's conjecture, are based on standard probabilities associated with the Borel–Cantelli heuristic, but many recent p-adic conjectures (on class groups and units) may contradict such approaches.

In this paper, we shall give numerical experiments in another direction using Gauss sums and Stickelberger annihilation of relative classes, together with a weaker form of the main theorem on abelian fields. Such a link of Vandiver's conjecture with Gauss sums and abelian p-ramification has been given first by Iwasawa [24] and applied by many authors in various directions, often needing Vandiver's conjecture (e.g., [1, 7, 15, 20, 21, 22, 23, 27, 36, 37, 38, 44, 45]), or in the context of Greenberg's conjecture considered as a generalization of Vandiver's conjecture (e.g., [19], [30]); we shall give Section 3 a short survey, explain the links with p-ramification and prove again the Theorem of reflection 3.1, not so well known in the literature.

Then we shall interprete 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 $\psi^p = 1$, 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 an 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 reciprocal being obvious. Since α can be obtained explicitely by means of twists $\mathrm{g}_c(\ell) = \tau(\psi)^{c-\sigma_c}$ with Artin automorphisms σ_c (by definition $\zeta_p^{\sigma_a} = \zeta_p^a$ for all $a \not\equiv 0 \pmod p$), of the above Gauss sums, giving products of Jacobi sums, this shall give the main test verifying the validity of the conjecture for a given p (Theorem 4.6 and Corollaries 4.7, 4.8).

We show that some assumption of *independence*, of the congruential properties (mod p) of these products of Jacobi sums as ℓ varies, is an obstruction to any counterexample to Vandiver's conjecture or, at least, that the probability of such a counterexample is at most $\frac{O(1)}{p^2}$.

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

Finally, we propose, §§ 5.2, 5.3, new heuristics (to our knowledge) and give substantial numerical experiments confirming them. PARI/GP programs [33] can be copy and paste by the reader for any further experience. [1]

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

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

[1] Verbatim characters are compatible for copy and past, except sometimes, in some Journals, for the power symbol ^ to be replaced by the PARI/GP one. We give a copy of our programs at: https://www.dropbox.com/s/y57jdgv4thyx0tb/Vandiver.Prog.pdf?dl=0

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

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

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

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

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

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

For any ideal $\mathfrak{A}$ (prime to p) such that $\mathscr{cl}(\mathfrak{A}) \in \mathcal{C}\ell$, there exists an approximation $e'_\theta \in \mathbb{Z}[G]$ of e_θ modulo a sufficient power of p such that $\mathfrak{A}_\theta := \mathfrak{A}^{e'_\theta}$ is defined up to a principal ideal of the form (x^p), $x \in K^\times$. If $\mathfrak{A} = (\alpha)$, then $\mathfrak{A}_\theta = (\alpha'_\theta)$ with $\alpha'_\theta = \alpha^{e'_\theta}$.

(viii) For $\chi =: \omega^n \in \mathscr{X}_+$, denote by $b(\chi^*) = \frac{1}{p}\sum_{a=1}^{p-1}(\chi^*)^{-1}(s_a)\,a$ (where $s_a \in G$ is the Artin automorphism of a) the generalized Bernoulli number $B_{1,(\chi^*)^{-1}} = B_{1,\omega^{n-1}}$; it is an element of $\mathbb{Z}_p$ congruent modulo p to $\dfrac{B_n}{n}$, where B_n is the ordinary Bernoulli number of even index $n \in [2, p-3]$; see [43, 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 $B_n \equiv 0 \pmod p$; see [43, § 5.3 & Exercise 6.6] giving statistics and the heuristic $i(p) = O\big(\frac{\log(p)}{\log(\log(p))}\big)$.

(ix) We say that $\mathfrak{A}$ is p-principal if its class is of order prime to p; considering $\mathfrak{A}$ in $I \otimes \mathbb{Z}_p$, where I is the group of prime to p ideals of K, this means that $\mathfrak{A} = (\alpha)$, with $\alpha \in K^\times \otimes \mathbb{Z}_p$, defined up to $\varepsilon \in E \otimes \mathbb{Z}_p$.

We shall often write in this context for which $\mathfrak{A}_\theta := \mathfrak{A}^{e_\theta}$ and $\alpha_\theta := \alpha^{e_\theta}$ make sense, then use the practical writing defined in (vii) for programming.

Remark 1.2. We shall say that a $\mathbb{Z}_p[G]$-module M is monogenous (or G-monogenous) if it is generated, over $\mathbb{Z}_p[G]$, by a single element. One verifies that M is monogenous if and only if $\mathrm{rk}_p(M_\theta) \leq 1$ for all irreducible p-adic character θ of G (indeed, in our context, $\mathbb{Z}_p[G] \cdot e_\theta \simeq \mathbb{Z}_p$).

For a nice presentation on the history of Bernoulli–Kummer–Herbrand's works on cyclotomy, see [34].

2. Pseudo-units – Notion of p-primarity

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

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

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

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

giving $\mathrm{rk}_p(AK^{\times p}/K^{\times p}) = \frac{p-1}{2} + \mathrm{rk}_p(\mathcal{C}\ell)$. Thus $\mathrm{rk}_p\big((AK^{\times p}/K^{\times p})_\theta\big)$ is immediate from $\mathrm{rk}_p(\mathcal{C}\ell_\theta)$ and $\mathrm{rk}_p\big((E/E^p)_\theta\big) = 1$ (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 $\alpha \in K^\times$ (prime to p but not necessarily pseudo-unit) is "α congruent to a pth power modulo $\mathfrak{p}^p = (p)\,\mathfrak{p}$" (e.g., [12, Ch. I, § 6, (b), Theorem 6.3]). Since in any case (replacing α by α^{p-1}) we can suppose $\alpha \equiv 1 \pmod{\mathfrak{p}}$, 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 precised as follows:

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

Proof. One direction is trivial. Suppose that $K(\sqrt[p]{\alpha})/K$ is unramified at $\mathfrak{p}$; since α is a pseudo-unit, this extension is unramified as a global extension and is contained in the p-Hilbert class field H of K. The Frobenius automorphism in H/K of the *principal ideal* $\mathfrak{p} = (\zeta_p - 1)$ is trivial; so $\mathfrak{p}$ totally splits in H/K, thus in $K(\sqrt[p]{\alpha})/K$, proving the proposition. □

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

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

Proof. Consider the Dwork uniformizing parameter ϖ in $\mathbb{Z}_p[\mu_p]$ which has the following properties:

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

(ii) $s(\varpi) = \omega(s) \cdot \varpi$, for all $s \in G$.

Put $\alpha_\theta = 1 + \varpi^k u$, where u is a unit of $\mathbb{Z}_p[\varpi]$ and $k \geq 1$; let $u_0 \in \mathbb{Z} \setminus p\mathbb{Z}$ such that $u \equiv u_0 \pmod{\varpi}$ 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 $\alpha_\theta = 1 + \varpi^k\, u$, $k \in \{m, m+p-1, \ldots\}$. The p-primarity condition for α_θ is $\alpha_\theta \equiv 1 \pmod{\varpi^p}$ giving the obvious direction since $(\varpi^p) = (p\,\varpi)$. Suppose $\alpha_\theta \equiv 1 \pmod{\varpi^{p-1}}$; so $k = m$ does not work since $m \leq p-2$, and necessarily k is at least $m + p - 1 \geq p + 1$ since $m \geq 2$ (which is also the local pth power condition). □

3. Abelian p-ramification and Gauss sums

3.1. **Vandiver's conjecture and abelian p-ramification.** Let $\mathcal{T}$ be the torsion group of the Galois group of the maximal abelian p-ramified (i.e., unramified outside p) pro-p-extension $H^{\rm pr}$ of K; since Leopoldt's conjecture holds for abelian number fields, we have $\mathrm{Gal}(H^{\rm pr}/K) = \Gamma \oplus \mathcal{T} \simeq \mathbb{Z}_p^{\frac{p+1}{2}} \oplus \mathcal{T}$ where the Galois group $\Gamma = \Gamma_+ \oplus \Gamma_-$, of the compositum of the $\mathbb{Z}_p$-extensions of 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 (for more information, see [12, 13, 16] and their references).

Write $\mathcal{T} = \mathcal{T}_+ \oplus \mathcal{T}_-$ and define $H_-^{\rm pr} \subseteq H^{\rm pr}$ (fixed by $\mathrm{Gal}(H^{\rm pr}/K)_+$), $H_+^{\rm pr} \subseteq H^{\rm pr}$ (fixed by $\mathrm{Gal}(H^{\rm pr}/K)_-$); then $\mathrm{Gal}(H_+^{\rm pr}/K) \simeq \mathbb{Z}_p \oplus \mathcal{T}_+$ 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 $\theta = \chi \in \mathscr{X}_+$).

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

We then have unconditionally the following interpretation for K (particular case of [12, Theorem II.5.4.5]):

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

Proof. We will briefly prove this famous "global" reflection result as follows from classical Kummer duality between radicals and Galois groups, using the fact that $K(\sqrt[p]{\beta})/K$, $\beta \in K^\times$, is p-ramified if and only if $(\beta) = \mathfrak{p}^e \cdot \mathfrak{A}^p$, $e \geq 0$, $\mathfrak{A} \in I$ (see, e.g., [12, Theorem I.6.2 & Corollary I.6.2.1]):

The Kummer radical of the compositum of the cyclic extensions of degree p of K contained in $H_-^{\rm pr}$ is generated (modulo $K^{\times p}$) by the part E_+ of real units, giving a p-rank $\frac{p-3}{2}$, by the real p-unit $\eta_+ := \zeta_p + \zeta_p^{-1} - 2$, and by the pseudo-units α_+ comming from the elements of order p of $\mathcal{C}\ell_+$, which gives the p-rank of this radical equal to $\frac{p-1}{2} + \mathrm{rk}_p(\mathcal{C}\ell_+)$. Since $\mathrm{rk}_p(\mathrm{Gal}(H_-^{\rm pr}/K)) = \frac{p-1}{2} + \mathrm{rk}_p(\mathcal{T}_-)$, we get the more precise information $\mathrm{rk}_p(\mathcal{T}_-) = \mathrm{rk}_p(\mathcal{C}\ell_+)$. □

Similarly, $\mathrm{rk}_p(\mathcal{T}_+) = \mathrm{rk}_p(\mathcal{C}\ell_-)$, and the proof for the isotypic components is obtained taking the θ or θ^*-components for each object, which yields:

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

Note that $\mathcal{T}_1 = \mathcal{T}_\omega = \mathcal{C}\ell_\omega = \mathcal{C}\ell_1 = 1$.

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

Remarks 3.2. (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 [13] for more details and programs testing the p-rationality of any number field). For the pth 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).

(ii) As we have seen, at each unramified cyclic extension L_+ of degree p of K_+ is associated a p-primary pseudo-unit $\alpha \in (K^\times/K^{\times p})_-$, with $\alpha^{1+s_{-1}} \in K_+^{\times p}$ and $L_+K = K(\sqrt[p]{\alpha})$. Put $(\alpha) = \mathfrak{A}^p$, where $\mathfrak{cl}(\mathfrak{A}) \in \mathcal{C}\ell_-$ (giving $\mathfrak{A}^{1+s_{-1}} = (\beta_+)$, $\beta_+ \in K_+^\times$); moreover $\mathfrak{A}$ is not principal, otherwise α should be, up to a pth 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 $\mathrm{Gal}(L_+/K_+)$ then by Kummer duality G operates via χ^* on $\langle\alpha\rangle_{\mathbb{Z}[G]}K^{\times p}/K^{\times p}$.

As explained in the Introduction, we shall prove that such pseudo-units α may be found by means of twists $\mathrm{g}_c(\ell) := \tau(\psi)^{c-\sigma_c}$ associated to primes $\ell \equiv 1 \pmod p$ and Artin automorphisms σ_c (tese twists shall be defined and studied Section 4 and used in Lemma 4.5 to obtain the main Theorem 4.6).

3.2. **Vandiver's conjecture and Gauss sums.** Recall, for the field K, the formula (see [12, Corollary III.2.6.1, Remark III.2.6.5] for more details and references):

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

where I is the group of prime to p ideals of K and U the group of principal local units of $\mathbb{Q}_p(\mu_p)$ which is equal to $1 + \varpi\,\mathbb{Z}_p[\varpi]$. 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 for all $\chi \in \mathscr{X}_+$:

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

The following reasonning (from [15, § 3]) gives another, but similar, interpretation of the result of Iwasawa [24]. Consider the Stickelberger element:

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

it is such that:

$$S\,.\,e_{\chi^*} = b(\chi^*)\,.\,e_{\chi^*} := B_{1,(\chi^*)^{-1}}\,.\,e_{\chi^*} \in \mathbb{Z}_p[G] \text{ for all } \chi \in \mathscr{X}_+;$$

then if $\chi = \omega^n$, $\chi^* = \omega^{p-n}$ for which $\#\mathcal{C}\ell_{\chi^*}$ corresponds to the ordinary Berrnoulli numbers B_n giving the "exponents of p-irregularity" n for $B_n \equiv 0 \pmod p$ (see Definitions 1.1 (viii)).

Let ℓ be a prime number totally split in K (i.e., $\ell \equiv 1 \pmod p$). Let ψ be a character of order p of $\mathbb{F}_\ell^\times$. We define the Gauss sum:

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

where ξ_ℓ is a primitive ℓth root of unity.

Lemma 3.3. *We have $\tau(\psi)^{\sigma_a} = \psi(a)^{-a}\,\tau(\psi^a)$ for any Artin automorphism σ_a of $\mathrm{Gal}(\mathbb{Q}(\mu_{p\,\ell})/\mathbb{Q})$ 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 relation in K (see [43, §§ 6.1, 6.2, 15.1]):

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

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

Remarks 3.4. (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 pth root of unity, we denote simply $\tau(\psi)$ such a Gauss sum, where ψ is for instance the canonical character of order p; for convenience, we shall have in mind that ℓ *defines* such a $\tau(\psi)$ (and some other forthcoming objects) in an obvious way.

(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 we have put $\mathrm{g}_c(\ell) := \tau(\psi)^{c-\sigma_c} \in K^\times$, for all $c \in [1, p-1]$ (see (7) and Lemma 4.2 using Jacobi sums); 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 $\langle\alpha\rangle_{\mathbb{Z}[G]}K^{\times p}/K^{\times p}$ 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 $\chi \in \mathscr{X}_+$:

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

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

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

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

We shall from now make in general the following working hypothesis which corresponds to the more subtle case for testing Vandiver's conjecture by means of Theorem 4.6, the general case (i.e., when some $\mathcal{C}\ell_{\chi^*}$ are not cyclic) being obvious as soon as one knows that $b(\chi^*)$ gives the order of $\mathcal{C}\ell_{\chi^*}$, thus its annihilation:

Hypothesis 3.5. *We assume that, for all $\chi \in \mathscr{X}_+$, the component $\mathcal{C}\ell_{\chi^*}$ of the p-class group is cyclic; in other words, we restrict ourselves to the case where $\mathcal{C}\ell$ is G-monogenous (cf. Remark 1.2), giving* $\mathrm{rk}_p(\mathcal{C}\ell_-) = i(p)$.

Moreover, we know that $\#\mathcal{C}\ell_{\chi^*} \equiv 0 \pmod{p^2}$ has probability less than $\frac{O(1)}{p^2}$, especially for the case $\mathrm{rk}_p(\mathcal{C}\ell_{\chi^*}) \geq 2$ which may be considered as giving a finite number of counterexamples to Vandiver's conjecture, what can be discarded for our purpose (the numerical results [4, 8] are in complete accordance with this viewpoint). The main theorem on abelian fields gives, under our assumption, $b(\chi^*) \sim p^e$, $e \geq 1$, for each non-trivial component $\mathcal{C}\ell_{\chi^*}$ of order p^e, where $\sim$ means "equality up to a p-adic unit factor", but leads, in fact, to the classical Herbrand theorem "$\#\mathcal{C}\ell_{\chi^*} \sim p^e$ implies $b(\chi^*) \sim p^e$".

3.3. **Vandiver's conjecture and ray class group modulo** (p)**.** Assume the Hypothesis 3.5 and let $\chi = \omega^n \in \mathscr{X}_+$ be such that $b(\chi^*) \sim p^e$, $e \geq 1$ (i.e., $\#\mathcal{C}\ell_{\chi^*} = p^e$); thus, from (5), $\mathcal{T}_{\chi^*} = 1$ (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 2.4), which indicates analytically the non-p-primarity of $\tau(\psi)_{\chi^*}$ in $\mathbb{Z}[\zeta_p]$.

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

Theorem 3.6. *Let $\mathcal{C}\ell^{(p)} := I/\{(x),\ x \equiv 1 \pmod{p}\}$ be the ray class group of modulus $p\,\mathbb{Z}[\zeta_p]$. Then for any $\chi \in \mathscr{X}_+$, we have the following properties (under the Hypothesis 3.5):*

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

Proof. Let $V := \{x \in K^\times, x \equiv 1 \,(\mathrm{mod}\ \mathfrak{p})\}, W := \{x \in K^\times, x \equiv 1 \,(\mathrm{mod}\ p)\}$. Since $(E/E^p)_{\chi^*} = 1$, we have the exact sequence (using Proposition 2.4):

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

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 equality (1)) which implies $\mathcal{C}\ell_{\chi^*}^{(p)} \simeq \mathbb{Z}/p^{e+1}\mathbb{Z}$ (indeed, the χ^*-part $H^{\rm pr}_{\chi^*}/K$ 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 $H^{\rm pr}_{\chi^*}$, is cyclic).

Reciprocally, if $\mathcal{C}\ell_{\chi^*}^{(p)}$ is cyclic of order p^{e+1}, $e \geq 1$ (so $\mathcal{C}\ell_{\chi^*} \simeq \mathbb{Z}/p^e\mathbb{Z}$), there exists an ideal $\mathfrak{A}$ (whose class is of order p^{e+1} in $\mathcal{C}\ell_{\chi^*}^{(p)}$) such that $\mathfrak{A}^{p^e}_{\chi^*} = (\alpha_{\chi^*})$ (up to a pth power, see Definitions 1.1 (ix)), with $\alpha_{\chi^*} \equiv 1 \pmod{\mathfrak{p}^{p-n}}$ if $\chi = \omega^n$, $n \in [2, p-3]$, but $\alpha_{\chi^*} \not\equiv 1 \pmod p$.
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 $H^{\rm pr}_\chi$ (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 (i.e., $\ell \equiv 1 \pmod p$). For $\ell \in \mathscr{L}_p$, let $\psi : \mathbb{F}_\ell^\times \longrightarrow \mu_p$ be of order p; if g is a primitive root modulo ℓ, we put $\psi(\overline{g}) = \zeta_p$. Let ξ_ℓ be a primitive ℓ-th root of unity; then the Gauss sum associated to ℓ may be written in $\mathbb{Z}[\mu_{p\,\ell}]$:

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

4.1. **Practical computation of** $\mathrm{g}_c(\ell) := \tau(\psi)^{c-\sigma_c}$**.** Let $c \in [2, p-2]$ be a primitive root modulo p; to get an element of K (a PARI/GP program in $\mathbb{Z}[\mu_{p\,\ell}]$ overflows as ℓ increases arbitrarily, even if $\tau(\psi)_{\chi^*} = \tau(\psi)^{e'_{\chi^*}}$ (defined up to $K^{\times p}$) makes sense in $\mathbb{Z}[\zeta_p]$, a posteriori), one use the twist $\tau(\psi)^{c-\sigma_c}$ where $\sigma_c \in \mathrm{Gal}(\mathbb{Q}(\mu_{p\,\ell})/\mathbb{Q})$ is the Artin automorphism of c (its restriction to K is $s_c \in G$). We define (using Lemma 3.3):

$$\mathrm{g}_c(\ell) := \tau(\psi)^{c-\sigma_c} \in \mathbb{Z}[\zeta_p]. \tag{7}$$

This notation using $\ell \in \mathscr{L}_p$ is justified by the Remark 3.4, then formulas (3) and (4), giving, up to $K^{\times p}$ (see Definitions 1.1 (vii, ix, x)):

$$\mathfrak{L}^{S_c} = \mathrm{g}_c(\ell)\,\mathbb{Z}[\zeta_p] \ \ \&\ \ \mathfrak{L}_{\chi^*}^{(c-\chi^*(s_c))\cdot b(\chi^*)} = \mathrm{g}_c(\ell)_{\chi^*}\,\mathbb{Z}[\zeta_p], \text{ for all } \chi \in \mathscr{X}_+, \tag{8}$$

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 we know that $\mathrm{g}_c(\ell) \in \mathbb{Z}[\zeta_p]$. Put:

$$b_c(\chi^*) := (c - \chi^*(s_c)) \cdot b(\chi^*) \sim b(\chi^*), \text{ for all } \chi \in \mathscr{X}_+. \tag{9}$$

Then:

$$\mathfrak{L}_{\chi^*}^{b_c(\chi^*)} = \mathrm{g}_c(\ell)_{\chi^*}\, \mathbb{Z}[\zeta_p]. \tag{10}$$

Remark 4.1. In the above definition (7) of $\mathrm{g}_c(\ell)$, $\tau(\psi)^{\sigma_c} = \tau(\psi^c) \cdot \psi^{-c}(c)$ (Lemma 3.3); 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 $\psi^{-c}(c) \cdot \tau(\psi)^{c-\sigma_c}$. Note that, since $\tau(\psi)^{1+s_{-1}} = \ell$, $\mathrm{g}_c(\ell)_\chi \in K^{\times p}$ for all $\chi \in \mathscr{X}_+$.

Lemma 4.2. *Let $\ell \in \mathscr{L}_p$ be given. 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 [43, § 6.1] for Jacobi sums (for $\psi\,\psi' \neq 1$) is $J(\psi, \psi') := \tau(\psi) \cdot \tau(\psi') \cdot \tau(\psi\,\psi')^{-1} = -\sum_{x \in \mathbb{F}_\ell \setminus \{0,1\}} \psi(x) \cdot \psi'(1-x)$. 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:

$$\tau(\psi)^{c-\sigma_c} = J_1 \cdots J_{c-1} \cdot \tau(\psi^c)\, \tau(\psi)^{-\sigma_c} = J_1 \cdots J_{c-1} \cdot \psi^c(c). \tag{11}$$

From Lemma 3.3, $\tau(\psi) \equiv 1 \pmod{\mathfrak{p}\, \mathbb{Z}[\mu_{p\,\ell}]}$ implies the result for $\mathrm{g}_c(\ell)$. □

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

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

Definitions 4.3. (i) We call 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 2.1 (ii), Proposition 2.4).
(ii) We call set of exponents of p-irregularity, the set $\mathscr{E}_0(p)$ of even integers $n \in [2, p-3]$ such that $B_n \equiv 0 \pmod{p}$ (i.e., $b(\omega^{p-n}) \equiv 0 \pmod{p}$; see Definitions 1.1 (viii)).

Remark 4.4. Let $\chi =: \omega^n \in \mathscr{X}_+$. If $\mathrm{g}_c(\ell)_{\chi^*}$ is p-primary (i.e., $n \in \mathscr{E}_\ell(p)$) this does not give necessarily a counterexample to Vandiver's conjecture for the two following possible reasons considering the expression $S_c\, e_{\chi^*} = b_c(\chi^*)\, e_{\chi^*}$ (recall from (9) that $b_c(\chi^*) = (c - \chi^*(s_c)) \cdot b(\chi^*) \sim b(\chi^*)$):
(i) The number $b_c(\chi^*)$ is a p-adic unit (i.e., $n \notin \mathscr{E}_0(p)$), so the radical $\mathrm{g}_c(\ell)_{\chi^*}$ is not the pth power of an ideal (thus not a pseudo-unit, even if Proposition 2.4 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 (where $x = \zeta_{11}$):

```
-84917739706560657276784274650452882 22*x^9-19632310198566777336887224 3
9078492228*x^8+11757523232198873159205810348854526320*x^7-586067415031
09222003489076069835666 48*x^6-64408800619281685160814212357927696 2*x^5
-61107401428923128430838681719965801 0*x^4+26730059555456750040660872 84
224877298*x^3+15023028737838809151251842166615658188*x^2+1520229819300
797188419125563036321734*x+17836238554732163868933693789025679469
```

for which $K(\sqrt[11]{\alpha})/K$ is decomposed over K_+ into L_+/K_+ only ramified at ℓ; then (α) is a product of prime ideals above ℓ:

$$(\alpha) = \mathfrak{L}^{1+2s+2^2s^2+2^3s^3+2^4s^4+2^5s^5+2^6s^6+2^7s^7+2^8s^8+2^9s^9}$$

up to the 11th power of an ℓ-ideal ($s = s_2$). We obtain $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \ell^{275}$ and $\mathrm{N}_{K/\mathbb{Q}}(\alpha - 1) \sim 11^{13}$. In fact the program gives:

$$(\alpha) = \mathfrak{L}_1^{25} \cdot \mathfrak{L}_2^{27} \cdot \mathfrak{L}_3^{31} \cdot \mathfrak{L}_4^{24} \cdot \mathfrak{L}_5^{28} \cdot \mathfrak{L}_6^{15} \cdot \mathfrak{L}_7^{30} \cdot \mathfrak{L}_8^{23} \cdot \mathfrak{L}_9^{32} \cdot \mathfrak{L}_{10}^{40}$$

and one must discover the significance given above ! Here, we get $b_c(\chi^*) \equiv 1 \pmod{11}$.

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

So, a *sufficient condition for a counterexample* to Vandiver's conjecture is the existence of $\chi \in \mathscr{X}_+$ such that $b_c(\chi^*) \equiv 0 \pmod{p}$, and $\ell \in \mathscr{L}_p$ such that $\mathrm{g}_c(\ell)_{\chi^*}$ is p-primary and $\mathrm{g}_c(\ell)_{\chi^*} \notin K^{\times p}$ (ie., a non-trivial p-primary pseudo-unit). The *necessity* shall be given in Lemma 4.5 and Theorem 4.6.

4.2. **Program computing $\mathscr{E}_\ell(p)$.** For $p \in [3, 199]$ and for the least $\ell \in \mathscr{L}_p$, the program computes $\mathrm{g}_c(\ell)$ in $\mathsf{Mod}(\mathsf{J}, \mathsf{P})$, with $\mathsf{P} = \mathsf{polcyclo}(\mathsf{p})$, 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 modulo p. 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 $\chi = \omega^n$ & $\chi^* = \omega^{1-n}$, taking $\mathsf{n} = 2 * \mathsf{m}$.

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_{χ^*} (in which $\chi^*(s_a^{-1})$ is replaced by the residue of a^{n-1} modulo p), thus computes in reality $\mathrm{g}_c(\ell)^{-1/2}$ up to pth 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 $\mathsf{Sn} = \prod_{\mathsf{a}=1}^{(\mathsf{p}-1)/2} \mathsf{s}_\mathsf{a}(\mathsf{J}^{\mathsf{a}^{\mathsf{n}-1}})$ from:

$$\mathrm{g}_c(\ell)_{\chi^*}^{-1/2} = \prod_{a=1}^{(p-1)/2} s_a(\mathrm{g}_c(\ell))^{\omega^{n-1}(a)}$$

(up to a pth power); then $\omega^{n-1}(a) \equiv a^{n-1} \pmod{p}$ is computed in an and then J^an is given by $\mathsf{component}(\mathsf{LJ}, \mathsf{an})$. 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):

```
{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
```

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

4.3. **Reciprocal study.** Recall, from formula (10) and Remark 4.4, that, for all $\chi \in \mathscr{X}_+$, $(\mathrm{g}_c(\ell)_{\chi^*}) = \mathfrak{L}^{S_c\, e_{\chi^*}} = \mathfrak{L}_{\chi^*}^{b_c(\chi^*)}$ and that the union of the following conditions gives rise to a counterexample to Vandiver's conjecture:

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

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

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

We still assume the Hypothesis 3.5 to obtain the reciprocal (to be put in relation with Theorem 3.6 (ii)); otherwise, if for instance $\mathrm{rk}_p(\mathcal{C}\ell_{\chi_0^*}) \geq 2$ for some $\chi_0 = \omega^{n_0} \in \mathscr{X}_+$ (giving a counterexample to Vandiver's conjecture), we get, from the main theorem on abelian fields, $\#\mathcal{C}\ell_{\chi_0^*} \sim b_c(\chi_0^*)$; then the p-part of $b_c(\chi_0^*)$ is strictely larger than the exponent of $\mathcal{C}\ell_{\chi_0^*}$ so that, in

any relation $\mathfrak{L}_{\chi_0^*}^{b_c(\chi_0^*)} = (\mathrm{g}_c(\ell)_{\chi_0^*})$ (cf. (10)), necessarily $\mathrm{g}_c(\ell)_{\chi_0^*}$ is a global pth power (condition (c) is never fulfilled), whence the property $\mathscr{E}_\ell(p) \cap \mathscr{E}_0(p) \neq \emptyset$ for all $\ell \in \mathscr{L}_p$; thus Theorem 4.6 and Corollaries 4.7, 4.8 shall apply for trivial reasons.

Lemma 4.5. *Let $\chi \in \mathscr{X}_+$ be such that $\mathcal{C}\ell_\chi \neq 1$ (i.e., we assume to have a counterexample to Vandiver's conjecture).*

Then $\mathcal{C}\ell_{\chi^*} \neq 1$, thus $b_c(\chi^*) \equiv 0 \pmod p$, and there exists a totally split prime ideal $\mathfrak{L}$ such that $\mathfrak{L}_{\chi^*}$ represents a generator of $\mathcal{C}\ell_{\chi^*}$.

Afterwards $\mathfrak{L}^{S_c\, e_{\chi^*}} = \mathfrak{L}_{\chi^*}^{b_c(\chi^*)} = (\alpha_{\chi^*})$, where the generator α_{χ^*} is unique (up to a pth power), thus equal to $\mathrm{g}_c(\ell)_{\chi^*}$ which is p-primary (i.e., $\mathrm{g}_c(\ell)_{\chi^*} \equiv 1 \pmod p$) and not a global pth power in $K^\times$.

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

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

Necessarily $b_c(\chi^*) \equiv 0 \pmod p$, and $\mathfrak{L}_{\chi^*}^{b_c(\chi^*)} = (\alpha_{\chi^*})$; since $E_{\chi^*} = 1$ (except for $\chi^* = \omega$ excluded), α_{χ^*} is unique and not a pth power; in terms of Gauss sums, $\mathfrak{L}_{\chi^*}^{b_c(\chi^*)} = (\mathrm{g}_c(\ell)_{\chi^*})$, thus $\alpha_{\chi^*} = \mathrm{g}_c(\ell)_{\chi^*}$.

The p-primarity of α_{χ^*} is necessary to obtain the *unique* (thanks to Hypothesis 3.5) corresponding unramified Kummer extension $K(\sqrt[p]{\alpha_{\chi^*}})/K$ of degree p, decomposed over K_+ into the unramified extension L_+/K_+ associated to $\mathcal{C}\ell_\chi$ by class field theory, whence the p-primarity of $\mathrm{g}_c(\ell)_{\chi^*}$. □

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

4.4.1. *Main theorem.* A necessary and sufficient condition, to have a counterexample to Vandiver's conjecture, is that there exists $\chi \in \mathscr{X}_+$, such that $b_c(\chi^*) \equiv 0 \pmod p$, and $\ell \in \mathscr{L}_p$ such that $\mathrm{g}_c(\ell)_{\chi^*} := \tau(\psi)^{c-\sigma_c}$ (cf. (7), (8)) be p-primary and not a global pth power (i.e., $\mathfrak{L}_{\chi^*}$ non-p-principal):

Theorem 4.6. *For any $\ell \in \mathscr{L}_p$ (the set of primes $\ell \equiv 1 \pmod p$) let $\mathscr{E}_\ell(p)$ be the set of exponents of p-primarity of ℓ (i.e., the even $n \in [2, p-3]$, such that $\mathrm{g}_c(\ell)_{\omega^{p-n}} \equiv 1 \pmod p$); let $\mathscr{E}_0(p)$ be the set of exponents of p-irregularity of K (i.e., the even $n \in [2, p-3]$, such that $p \mid B_n$).*

Then, Vandiver's conjecture holds for K if and only if there exists $\ell \in \mathscr{L}_p$ such that $\mathscr{E}_\ell(p) \cap \mathscr{E}_0(p) = \emptyset$.

Proof. As we have explain § 4.3, we may assume to be in the context of Hypothesis 3.5. 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 (10) giving $\mathfrak{L}_{\chi^*}^{b_c(\chi^*)} = (\mathrm{g}_c(\ell)_{\chi^*})$, and examine the two possibilities:

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

(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 pth power, hence p-primary (absurd by assumption).

So $\mathfrak{L}_{\chi^*}$ defines a class of order p^e in $\mathscr{C}\!\ell_{\chi^*}$ for which $\mathrm{g}_c(\ell)_{\chi^*}$ is not p-primary by assumption, whence $\mathscr{C}\!\ell_\chi = 1$ by Kummer duality since $K(\sqrt[p]{\mathrm{g}_c(\ell)_{\chi^*}})/K$ (unique extension cyclic of degree p, decomposed over K_+ and contained in H_χ^{pr} since $\mathrm{Gal}(H_\chi^{\mathrm{pr}}/K_+) = \mathcal{T}_\chi$ is cyclic), is ramified at p.

Reciprocally, if Vandiver's conjecture holds, $\mathscr{C}\!\ell = \mathscr{C}\!\ell_-$ is G-monogenous, i.e., the direct sum of non-trivial cyclic isotypic components generated by some $\gamma^{(n_0)} = \mathscr{A}(\mathfrak{L}_{\omega^{p-n_0}}^{(n_0)}) \in \mathscr{C}\!\ell_{\omega^{p-n_0}}$ ($n_0 \in \mathscr{E}_0(p)$) related to non-p-primary $\mathrm{g}_c(\ell^{(n_0)})_{\omega^{p-n_0}}$; thus there exists, from density theorem, $\ell \in \mathscr{L}_p$ and $\mathfrak{L} \mid \ell$ such that $\mathscr{A}(\mathfrak{L})_{\omega^{p-n_0}} = \gamma^{(n_0)}$ for all $n_0 \in \mathscr{E}_0(p)$ (e.g., $\mathfrak{L} = (z) \cdot \prod_{n_0} \mathfrak{L}_{\omega^{p-n_0}}^{(n_0)}$). So each $\mathrm{g}_c(\ell)_{\omega^{p-n_0}} = \mathrm{g}_c(\ell^{(n_0)})_{\omega^{p-n_0}}$ (up to a pth power) is non-p-primary, whence $\mathscr{E}_\ell(p) \cap \mathscr{E}_0(p) = \emptyset$ for this prime ℓ. □

Corollary 4.7. *Let $\ell \in \mathscr{L}_p$. If, for all $\chi \in \mathscr{X}_+$, the numbers $\mathrm{g}_c(\ell)_{\chi^*}$ are not p-primary (i.e., $\mathscr{E}_\ell(p) = \emptyset$), then the Vandiver conjecture is true for p.*

4.4.2. *Minimal prime $\ell \in \mathscr{L}_p$ 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 $O\big(\frac{\log(p)}{\log(\log(p))}\big)$, 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=3,700,c=lift(znprimroot(p));P=polcyclo(p)+Mod(0,p);X=Mod(x,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=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));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=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,T=1;break));if(T==0,print(p," ",el," ",N);break))))}
```

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

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. Moreover, this much stronger test of Vandiver's conjecture does not need the knowledge of $\mathscr{E}_0(p)$ nor that of the whole class number h.

4.5. **What happens when $\ell \in \mathscr{L}_p$ varies with $\mathscr{E}_0(p) \neq \emptyset$?** Let n_0 even be an exponent of p-irregularity; put $\chi_0 = \omega^{n_0}$ and $b_c(\chi_0^*) \sim p^e$, $e \geq 1$; then $\#\mathcal{C}\ell_{\chi_0^*} = p^e$.

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

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

(ii) $\mathfrak{L}_{\chi_0^*}^{p^{e-1}}$ is not p-principal (such a prime ℓ does exist from density theorem). Thus it defines a generator of $\mathcal{C}\ell_{\chi_0^*}$ and Vandiver's conjecture holds at $\chi_0 = \omega^{n_0}$ if and only if $\mathrm{g}_c(\ell)_{\chi_0^*}$ is not p-primary.

Otherwise, if $\mathrm{g}_c(\ell)_{\chi_0^*} \equiv 1 \pmod p$, whatever the ideal $\mathfrak{L}'_{\chi_0^*}$, $\mathfrak{L}' \mid \ell' \in \mathscr{L}_p$, we have $\mathfrak{L}'_{\chi_0^*} = (z_{\chi_0^*}) \cdot \mathfrak{L}_{\chi_0^*}^r$, with $z \in K^\times$ and $r \in [0, p^e - 1]$, so:

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

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

Thus, from Theorem 4.6:

Corollary 4.8. *As soon as there exist distinct $\ell_1, \ldots, \ell_N \in \mathscr{L}_p$, $N \geq 1$, such that $\mathscr{E}_{\ell_1}(p) \cap \cdots \cap \mathscr{E}_{\ell_N}(p) = \emptyset$, the Vandiver conjecture holds.*

So it is fundamental to see if the sets $\mathscr{E}_\ell(p)$ are independent (or not) of the choice of $\ell \in \mathscr{L}_p$ for p fixed and $\mathscr{E}_0(p) \neq \emptyset$. We analyse the case of $p = 37$ whose exponent of p-irregularity is $n_0 = 32$ giving $\#\mathscr{C}\ell_{\omega^5} = 37$ and compute (in expp) the sets $\mathscr{E}_\ell(37)$ when $\ell \in \mathscr{L}_p$ varies. We shall see that the number of exponents of p-primarity grows, with ℓ, in the same proportion as, classically, for the exponents of p-irregularity; if $n_0 \in \mathscr{E}_\ell(37)$, this means that $\mathfrak{L}_{\chi*}$ is necessarily p-principal and then $\mathrm{g}_c(\ell)_{\omega^5} \in K^{\times 37}$:

```
{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,g=znprimroot(el);
print("el=",el," 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("     exponent of p-primarity: ",n)))))}
```

```
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
-----------------------------------------------------------------------
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=776483   g=2
el=745699   g=2                     el=776557   g=2   expp: 20
el=746069   g=2                     el=777001   g=31  expp: 18,28
el=746957   g=2                     el=778111   g=11
el=747401   g=3                     el=778333   g=2   expp: 28
el=747919   g=3                     el=778777   g=5
el=748807   g=6    expp: 22         el=779221   g=2
el=749843   g=2    expp: 34         el=779591   g=7
```

```
el=750287   g=5                      el=779887   g=10  expp: 18
el=750509   g=2    expp: 14,22       el=780257   g=3   expp: 8
el=751027   g=3                      el=780553   g=10
el=751841   g=3    expp: 14,16,24    el=781367   g=5   expp: 34
el=752137   g=10   expp: 8           *el=781589  g=2   expp: 32
el=752359   g=3    expp: 18          el=782107   g=2
el=752581   g=2    expp: 16          el=782329   g=13  expp: 18
el=752803   g=2    expp: 22,32       el=782921   g=3   expp: 20
el=753617   g=3                      el=783143   g=5
el=753691   g=11   expp: 16          el=783661   g=2
el=753839   g=7    expp: 4,22        el=784327   g=3
el=754283   g=2                      el=784697   g=3
el=755171   g=6                      el=784919   g=7
el=755393   g=3    expp: 22          el=785363   g=2
el=756281   g=3    expp: 2           el=786251   g=2
el=756799   g=15   expp: 18          el=786547   g=2
el=757243   g=2                      el=787139   g=2   expp: 20
el=757909   g=2    expp: 16          el=787361   g=6
el=758279   g=7                      el=787879   g=6   expp: 10,18,20
el=758501   g=2    expp: 18          el=788027   g=2   expp: 34
el=759019   g=2                      el=789137   g=3   expp: 24
el=759167   g=5    expp: 12          el=790099   g=2
el=759463   g=3                      el=791209   g=7
el=759833   g=3    expp: 4           el=791431   g=12
el=760129   g=11                     el=791801   g=3
el=760499   g=2                      *el=792023  g=5   expp: 32
el=762053   g=2                      el=792689   g=3
el=762571   g=10                     el=793207   g=5
el=763237   g=2                      el=795427   g=2
el=764051   g=2                      *el=795649  g=22  expp: 2,32
el=764273   g=3                      el=795797   g=2
el=764717   g=2    expp: 2           el=795871   g=3
el=765383   g=5                      el=796759   g=3
el=765827   g=2    expp: 34          el=796981   g=7
el=766049   g=3    expp: 22          el=797647   g=3
el=766937   g=3    expp: 34          el=797869   g=10
el=767381   g=2    expp: 18          el=798461   g=2
el=767603   g=5    expp: 34          el=798757   g=2
el=767677   g=5                      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 great lot of times. For $\ell = 1481$ one finds a p-primarity for $\chi^* = \omega^7$ ($\chi = \omega^{30} \neq \omega^{32}$). Corollary 4.8 applies at will.

Remark 4.9. We remark that $\chi_0 = \omega^{32}$ gives $\chi_0^* = \omega^5$ which is a character of K, not the character of a strict subfield (the class of order 37 does not come from a strict imaginary subfield). Let $\ell = 1481$; then $\chi = \omega^{30}$ is a character of the real subfield k_6 of degree 6 which gives rise to a ℓ-ramified (i.e., unramified outside ℓ since the 37-primarity gives the non-ramification of 37) cyclic extension of degree 37 of k_6. If the exponent of p-irregularity had

been 30 instead of 32, this would have given an unramified cyclic extension of degree 37 of k_6, i.e., $\#\mathcal{C}l_{k_6} = 37$ (but we would have in the previous table an $\mathsf{expp} = 30$ at each line).

It remains to give statistics about the p-principality (or not) of the $\mathfrak{L}_{\chi_0^*}$ when $\ell \in \mathscr{L}_p$ varies. In the particular case $p = 37$, $\mathfrak{L}_{\chi_0^*}$ is 37-principal if and only if $\mathfrak{L}$ is principal since the exponent of 37-irregularity $n_0 = 32$ is unique and the whole class number of K equal to $h = 37$.

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

```
{p=37;c=lift(znprimroot(p));P=polcyclo(p);K=bnfinit(P,1);P=P+Mod(0,p);
X=Mod(x,P);Lsplit=List;N=0;for(i=1,2000,el=1+2*i*p;if(isprime(el)==1,
N=N+1;listinsert(Lsplit,el,N)));for(j=1,N,el=component(Lsplit,j);
F=bnfisintnorm(K,el);if(F!=[],print("el=",el," ",component(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=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("el=",el," expp:",n))))}
```

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

```
 el=25457   expp: 30                el=80513   expp: 16, 26
 el=29009   expp: 8,24              el=81031   expp: 18, 34
 el=30859   expp: 2                 el=82067   expp: 34
*el=32783   expp: 32 [x^11+x^3+x]   el=83621   expp: 34
 el=33301   expp: 30                el=83843   expp: 2
 el=33967   expp: 26                el=84731   expp: 6
 el=36187   expp: 8                 el=85027   expp: 26
 el=37889   expp: 16                el=86729   expp: 22
 el=38629   expp: 22                el=86951   expp: 8
 el=40627   expp: 30                el=87691   expp: 24
 el=40849   expp: 6                 el=91243   expp: 22, 34
 el=42773   expp: 4                 el=91909   expp: 30
 el=45289   expp: 8                 el=94351   expp: 10
 el=45659   expp: 26                el=94573   expp: 18
 el=48619   expp: 8                 el=95239   expp: 18, 28
 el=48989   expp: 20                el=96497   expp: 10
 el=51283   expp: 14,16             el=98347   expp: 28
 el=51431   expp: 20                el=98939   expp: 30
 el=53281   expp: 16                el=99679   expp: 10, 22
 el=55057   expp: 20                el=100049  expp: 14
```

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

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

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

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

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

(i) Principal case $\mathfrak{L} \mid 32783$. The principal $\mathfrak{L}$ are rare (which comes from density theorems); the first one is $\mathfrak{L} = (\zeta_{37}^{11} + \zeta_{37}^{3} + \zeta_{37})$ where $\ell = 32783$. Thus in that case, in the relation $\mathfrak{L}_{\chi_0^*}^{b_c(\chi_0^*)} = (\mathrm{g}_c(\ell)_{\chi_0^*})$, the number $\mathrm{g}_c(\ell)_{\chi_0^*}$ must be a global 37th 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 $\mathsf{factor}(\mathsf{norm}(\mathsf{Sn})) = 32783^{37 \cdot 16 \cdot 9}$ and use $\mathsf{K} = \mathsf{bnfinit}(\mathsf{P}, 1); \mathsf{idealfactor}(\mathsf{K}, \mathsf{Sn})$, which gives the 37th power of a principal ideal $\mathfrak{L} \mid 32783$. We obtain the following excerpts of the table (up to 10^6) of principal cases:

```
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
```

4.5.3. *Densities of the exponents of p-primarity.* The following program intends to show that all exponents of p-primarity are obtained, with (perhaps) some specific densities, taking sufficientely 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).

(i) Program (choose p; here the results are for $p = 37$):

```
{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,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=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,Npp=Npp+1;listput(Eel,1+component(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, as the following excerpt for $p = 37$ shows:

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

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

```
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]
```

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

(iii) Results for $p = 157$. For $p = 157$ (exponents of p-irregularity $62, 110$), one finds the partial analogous information after 590 distinct primes $\ell \in \mathscr{L}_p$ 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,
       5,5,5,3,6,1,6,3,5,4,5,0,2,3,5,7,3,3,3,2,4,4,7,6,6,5,6,1,7,4,7]
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 $\ell \in \mathscr{L}_p$, since for $p = 1 + 2\,q$, q prime, where the elements of $\mathscr{X}_+$ are indistinguishable, there is some gap for few ℓ. The complete tables for $p = 37, 157$ and $59 = 1 + 2{\cdot}29$ may be downloaded from: https://www.dropbox.com/s/vs5eq6ornqx5922/vandiver.97.157.pdf?dl=0.

4.5.4. *Vandiver's conjecture and p-adic regulator of K_+.* We return to the case $p = 37$ and $n_0 = 32$. 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 (1); so, k_9 admits a cyclic 37-ramified extension of degree 37 which is not unramified. To verify, we use [13, Program I], simplified for real fields, which indeed gives $\#\mathcal{T}_{k_9} = 37$ (nt must verify $\mathsf{p}^{\mathsf{nt}} > p^t$, the exponent of $\mathcal{T}$; here $\mathsf{nt} = 2$ would be sufficient):

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

We find here another interpretation of the reflection theorem since we have the typical formula:

$$\#\mathcal{T}_+ = \#\mathcal{C}\ell_+ \cdot \#\mathcal{R}_+,$$

where the p-group $\mathcal{R}_+$ is the normalized p-adic regulator of K_+ [16, Proposition 5.2] (whence $\#\mathcal{T}_\chi = \#\mathcal{C}\ell_\chi \cdot \#\mathcal{R}_\chi$ for all $\chi \in \mathscr{X}_+$); the above data shows that the relation $\#\mathcal{T}_{\chi_0} = 37$ comes from $\#\mathcal{R}_{\chi_0} = 37$, which is not surprising:

Remark 4.10. 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 [43, Corollary 8.19], applied in [4, 8] and developped in [41, 42]) consists in finding $\ell \in \mathscr{L}_p$ such that η_{χ_0} is not a local pth power at ℓ proving Vandiver's conjecture at χ_0; so when we find that $\mathcal{R}_{\chi_0} \neq 1$ (with $\mathcal{C}\ell_{\chi_0} = 1$), this means that η_{χ_0} generates E_{χ_0} and is a local pth power at p by p-primarity. We shall give in § 5.2.4 some insights in this direction to obtain new heuristics for the probability of p-primarity of $\mathrm{g}_c(\ell)_{\chi_0^*}$ to be in $\frac{O(1)}{p^2}$.

5. Heuristics – Probability of a counterexample

5.1. **Standard probabilities.** We may suppose in a first approximation that, for a given p, the sets $\mathscr{E}_\ell(p)$ of exponents of p-primarity of primes $\ell \in \mathscr{L}_p$, 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 [43], the Theorem 5.17 and some statistical computations), that in terms of probabilities one has, for given primes p and $\ell \in \mathscr{L}_p$ (where $N := \frac{p-3}{2}$):

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

this would imply that, for p given, $\mathscr{E}_\ell(p) \neq \emptyset$ 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 accordence with previous tables. Then the probability, for p and ℓ given, of $\mathscr{E}_0(p) \cap \mathscr{E}_\ell(p) \neq \emptyset$ with cardinalities $j \in [0, N]$ and $k \in [0, N]$ fixed, is $1 - \dfrac{(N-k)! \cdot (N-j)!}{N! \cdot (N-k-j)!}$. So, an approximation of the whole probability of $\mathscr{E}_0(p) \cap \mathscr{E}_\ell(p) \neq \emptyset$ is:

$$\sum_{j,\,k \geq 0} \tbinom{N}{j}\tbinom{N}{k} \cdot \left(1 - \tfrac{1}{p}\right)^{2N-j-k} \cdot \left(\tfrac{1}{p}\right)^{j+k} \cdot \left(1 - \tfrac{(N-k)!\cdot(N-j)!}{N!\cdot(N-k-j)!}\right). \tag{12}$$

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 the Theorem 3.6 on periodicities due to the density theorem (see the Weil interpretation of Jacobi sums defining Hecke Grössencharacters [46, Theorem, p. 489] where the module of definition of our Jacobi sums is p^2).

5.2. **New heuristics and probabilities.** There are several reasons to say 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 $h = 2, 4, \ldots$, for $p \gg_h 0$, one may prove that $\mathcal{C}\ell_{\omega^{p-(1+h)}} = 1$, as the case of $\mathcal{C}\ell_{\omega^{p-3}} = 1$ proved unconditionally by Kurihara [26] (see [10, 39, 40, 3] 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 the kernel of χ (which is proved for the quadratic case when $p \equiv 1 \pmod 4$, the cubic case when $p \equiv 1 \pmod 3$, ...). Moreover, we have the ϵ-conjecture for p-class groups of [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* $C_{\epsilon,p}$ *such that* $\log(\#\mathcal{C}\ell_{k_d}) \leq \log(C_{\epsilon,p}) + \epsilon \cdot \log(p)$,

which would give $\mathcal{C}\ell_{k_d} = 1$ for $\log(p) > \dfrac{\log(C_{\epsilon,p})}{1-\epsilon}$ and any $\epsilon < 1$. But this does not apply for any p with "small" d and the constant $C_{\epsilon,p}$ is not effective.

5.2.3. *Heuristics about Gauss sums.* The previous probabilities (12) assume that when $\ell \in \mathscr{L}_p$ varies, the sets $\mathscr{E}_\ell(p)$ are *random and independent*, which is not the case when p is irregular at some $\chi_0^* = \omega^{p-n_0}$ ($\chi_0 = \omega^{n_0} \in \mathscr{X}_+$) as we have seen when $\mathrm{g}_c(\ell)_{\chi_0^*}$ is a global pth power. We assume the Hypothesis 3.5 giving $b_c(\chi_0^*) \sim p^e$, $e \geq 1$, and $\mathcal{C}\ell_{\chi_0^*} \simeq \mathbb{Z}/p^e\mathbb{Z}$; to simplify the comments hereafter, we assume that $e = 1$.

Fix $\ell \in \mathscr{L}_p$ such that $\mathfrak{L}_{\chi_0^*}$ generates $\mathcal{C}\ell_{\chi_0^*} \simeq \mathbb{Z}/p\mathbb{Z}$ (thus $\mathrm{g}_c(\ell)_{\chi_0^*}$ is not a global pth power); put (Proposition 2.4):

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

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

Whatever $\ell' \in \mathscr{L}_p$ and $\mathfrak{L}' \mid \ell'$, one has, from the computations done in § 4.5.1 (ii) $\mathrm{g}_c(\ell')_{\chi_0^*} \equiv \mathrm{g}_c(\ell)^r_{\chi_0^*} \pmod p$, $r \in [0, p-1]$ ($r = 0$ if $\mathfrak{L}'_{\chi_0^*}$ is p-principal, i.e., $\mathrm{g}_c(\ell')_{\chi_0^*} \in K^{\times p}$), giving:

$$\mathrm{g}_c(\ell')_{\chi_0^*} =: 1 + \beta_0(\ell') \cdot \varpi^{p-n_0},\ \beta_0(\ell') \equiv r \cdot \beta_0(\ell) \pmod \varpi. \tag{13}$$

Contrary to the classical idea that $\beta_0(\ell) \pmod \varpi$ follow standard probabilities $\frac{1}{p}$ (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 congruential values modulo* p *at* $\chi^* = \omega\,\chi^{-1}$ *of the Gauss sums (more precisely of the* $\psi^{-c}(c) \cdot \mathrm{g}_c(\ell)$ *as product* $J_1 \cdots J_{c-1}$ *of*

Jacobi sums), 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 $\mathscr{L}_p$, we must examine two cases concerning the χ-components of $\mathcal{C}\ell$, for $\chi \in \mathscr{X}_+$, when there exists $\chi_0 = \omega^{n_0} \in \mathscr{X}_+$ such that $\mathcal{C}\ell_{\chi_0^*} \simeq \mathbb{Z}/p\mathbb{Z}$:

(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 $\frac{O(1)}{p}$ depending on the orders of the characters).

(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 non-principal $\mathfrak{L}_{\chi_0^*}$, then from (13) all the $\mathrm{g}_c(\ell')_{\chi_0^*}$ are p-primary, whatever the class of $\mathfrak{L}'_{\chi_0^*}$ (p possibilities) because $\beta_0(\ell') \equiv 0 \pmod{\varpi}$. So, n_0 is always an exponent of p-primarity and $\mathscr{E}_0(p) \cap \mathscr{E}_\ell(p) \neq \emptyset$ for all $\ell \in \mathscr{L}_p$, which corresponds to $\mathcal{C}\ell_{\chi_0} \neq 1$ and the non-cyclicity of $\mathcal{C}\ell^{(p)}_{\chi_0^*}$ (Theorem 3.6).

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 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 precise properties of Gauss or Jacobi sums; for this, the computation of $\beta(\ell)$ should be very interesting (see [42] 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). Otherwise, their behaviour should be excessively disturbed and, in an algorithmic framework, we suggest that the congruential properties of the Gauss sums (mod p) "determine" the properties of the p-class group of K instead of the contrary, and perhaps imply the cyclicity of each $\mathcal{C}\ell^{(p)}_{\chi *}$ or $\mathrm{g}_c(\ell)_{\chi_0^*} \in K^{\times p}$ as soon as $\mathrm{g}_c(\ell)_{\chi_0^*} \equiv 1 \pmod{p}$, what we intend to examine hereafter.

5.2.4. *Use of pth power residue symbols and cyclotomic units.* We refer to [43, § 8.3] for the classical p-adic interpretation of the numbers $\#\mathcal{C}\ell_\chi$, for $\chi \in \mathscr{X}_+$, as indices $(E_\chi : F_\chi)$, where F is the group of cyclotomic units. We shall need the following pth power criterion [12, II.6.3.8]:

Lemma 5.1. *Let $\alpha \in K^\times$ be a pseudo-unit (i.e., the pth power of an ideal prime to p). Then $\alpha \in K^{\times p}$ if and only if α is p-primary and locally a pth power at any set $\mathscr{S}$ of places $\mathfrak{q}$ of K whose classes generate (over $\mathbb{Z}$) the p-class group $\mathcal{C}\ell$ (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). If $K(\sqrt[p]{\alpha})/\mathbb{Q}$ is Galois, the condition becomes $\langle cl(\mathscr{S})\rangle_{\mathbb{Z}[G]} = \mathcal{C}\ell$.*

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

Theorem 5.2. *Let $\chi_0 = \omega^{n_0} \in \mathscr{X}_+$ with $n_0 \in \mathscr{E}_0(p)$ 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 $\eta := \zeta_p^{\frac{1-c}{2}} \dfrac{1-\zeta_p^c}{1-\zeta_p}$ be the canonical cyclotomic unit, where c is a primitive root modulo p (cf.* [43, Proposition 8.11]*).*
(i) There exist 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) Then $\mathcal{C}\ell_{\chi_0} \neq 1$ if and only if $\mathrm{g}_c(\ell)_{\chi_0^*}$ is locally a pth power at $\mathfrak{p}$ but not at $\mathfrak{L}$, or if and only if η_{χ_0} is locally a pth power at $\mathfrak{p}$ and $\mathfrak{L} \mid \ell$ ($\ell \in \mathscr{L}_p(\chi_0)$).

Proof. (i) In the G-monogenous case, the ideals $\mathfrak{L}$ are of the form $(z)\cdot\mathfrak{A}\cdot\mathfrak{A}'$, $z \in K^\times$, where $\mathscr{A}(\mathfrak{A})$ generates $\mathcal{C}\ell_{\chi_0}$ and $\mathscr{A}(\mathfrak{A}')$ 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) Define the pth power residue symbol $\left(\frac{\alpha}{\mathfrak{L}}\right) := \alpha^{\frac{\ell-1}{p}} \pmod{\mathfrak{L}}$, for any $\mathfrak{L} \mid \ell \in \mathscr{L}_p$ and any $\alpha \in K^\times$ prime to $\mathfrak{L}$. By abuse of notation, we shall write $\left(\frac{\alpha}{p}\right) = 1$ if α is p-primary.

Consider $\alpha = \mathrm{g}_c(\ell)_{\chi_0^*}$, where $\left(\mathrm{g}_c(\ell)_{\chi_0^*}\right) = \mathfrak{L}_{\chi_0^*}^{b_c(\chi_0^*)}$. This gives rise to a counterexample to Vandiver's conjecture at χ_0 if and only if α is p-primary (i.e., $\left(\frac{\alpha}{p}\right) = 1$) since $\mathscr{A}(\mathfrak{L}_{\chi_0^*})$ is of order p^e; it follows that $\left(\frac{\alpha}{\mathfrak{L}}\right) \neq 1$, otherwise, from Lemma 5.1, $\alpha = \mathrm{g}_c(\ell)_{\chi_0^*}$ should be a global pth power (contradiction). Consider $\alpha = \eta_{\chi_0}$. It is well-known that $b_c(\chi_0^*) \equiv 0 \pmod{p}$ is equivalent to the p-primarity of η_{χ_0}; thus 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 $\mathfrak{L} \mid \ell$ fulfilling the point (i) of the theorem:

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

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 in $\dfrac{O(1)}{p^2}$ for the p-primarity of $\mathrm{g}_c(\ell)_{\chi^*}$ ($\chi \in \mathscr{X}_+$ and $\ell \in \mathscr{L}_p$) if the two symbols of η_χ are independent with probabilities $\dfrac{O(1)}{p}$. So it is necessary to compute this symbol $\left(\frac{\mathrm{g}_c(\ell)_{\chi^*}}{\mathfrak{L}}\right)$ since $\mathrm{g}_c(\ell)_{\chi^*}$ 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 seems 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 pth power of an ℓ-ideal, which is fulfilled since $b_c(\chi_0^*) \equiv 0 \pmod{p}$. Then, from the general program computing $\mathrm{g}_c(\ell)_{\chi_0^*}$ in Sn (*not 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 Sn and pth power of an ℓ-ideal); the computation reduces to R prime to $\mathfrak{L}$ (in R) whose symbol $\left(\frac{R}{\mathfrak{L}}\right)$ (in u) is immediate.

```
{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=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);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>=1,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
```

But with the primes $\ell \in \{32783, 64381, 67489, \ldots\}$ the program writes, for instance for $\ell = 32783$:

```
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 $u = 1$ for the following ℓ (including the underlined numbers corresponding to primes $\ell \notin \mathscr{L}_p(\chi_0)$ such that $\mathrm{g}_c(\ell)_{\chi_0^*} \in K^{\times p}$ or $\mathcal{L}$ p-principal):

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

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

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

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

but $\mathrm{g}_c(\ell)_{\chi^*}$ is not the pth power of an 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.

A similar program computing the two symbols of η_{χ_0} gives all expected results (distribution, independence as $\chi \in \mathscr{X}_+$ and $\ell \in \mathscr{L}_p$ vary).

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 used on this subject and independently of some improvements or questions on the relevance of the formulas giving the probability $\mathrm{Prob}(\mathrm{rk}_p(C) = r)$ 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 $\mathcal{C}\ell_{\chi^*}^{(p)} \simeq (\mathbb{Z}/p\mathbb{Z})^2$. As Nguyen Quang Do pointed out to me, this may come, algebraically, from the relation $\mathrm{H}^2(\mathcal{C}\ell_{\chi^*}, (V/W)_{\chi^*}) \simeq \mathbb{F}_p$, assuming the uniform randomness of the exact sequences (proof of Theorem 3.6): $1 \to (V/W)_{\chi^*} \simeq \mathbb{F}_p \to \mathcal{C}\ell_{\chi^*}^{(p)} \to \mathcal{C}\ell_{\chi^*} \simeq \mathbb{F}_p \to 1$, knowing that the non-cyclic case corresponds to the single cohomology class 0.

5.2.6. *Heuristics from p-ramification theory.* Another observation concerns the groups $\mathcal{T}_\chi$ for $\chi \in \mathscr{X}_+$ and the formula $\#\mathcal{T}_\chi = \#\mathcal{C}\ell_\chi \cdot \#\mathcal{R}_\chi$ with the equivalence (1) of reflection, $\mathcal{C}\ell_{\chi^*} \neq 1$ if and only if $\mathcal{T}_\chi \neq 1$ (illustrated in the § 4.5.4). Thus 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 a number of our articles (see [17] and its bibliography), we give first a poor example with real quadratic fields and some $p \geq 3$.

For each of the ND real quadratic field of discriminant $\mathsf{D} \in [\mathsf{bD}, \mathsf{BD}]$, 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 privilegiate 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 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);
C5=component(Kpn,5);Hpn0=component(C5,1);Hpn=component(C5,2);
Hpn1=component(Hpn,1);vptor=valuation(Hpn0/Hpn1,p);if(vptor>=1,
Nt=Nt+1;C8=component(K,8);h=component(component(C8,1),1);
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)}
```

It appears that the proportion increases for intervals with large discriminants and becomes close to $\frac{1}{p}$:

```
[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
```

For cyclic cubic fields with primes $p \equiv 1 \pmod 3$ (to get two irreducible p-adic characters of degree 1) 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 ($\mathsf{f} \in [\mathsf{bf}, \mathsf{Bf}]$ denotes the conductor):

```
{p=7;bf=10^5;Bf=5*10^5;Nf=0.0;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);
C5=component(Kpn,5);Hpn0=component(C5,1);Hpn=component(C5,2);
Hpn1=component(Hpn,1);vptor=valuation(Hpn0/Hpn1,p);
if(vptor>=1,Nt=Nt+1;C8=component(K,8);h=component(component(C8,1),1);
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," 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
```

Thus, the fact that, in general, $\mathcal{R}_\chi$ 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 the general Gauss sum under the expression: $\tau(\psi) = -\sum_{k=0}^{\ell-2} \zeta_p^k \cdot \xi_\ell^{g^k}$ (relation (6), where g is a primitive root modulo ℓ),

and put $k = a\,p + b$, $0 \leq a \leq \frac{\ell-1}{p} - 1$, $0 \leq b \leq p-1$. Then one gets easily:

$$\tau(\psi) = -\sum_{b=0}^{p-1} \zeta_p^b \cdot \big[\mathrm{Tr}_{\mathbb{Q}(\xi_\ell)/F_\ell}(\xi_\ell)\big]^{\overline{\sigma}_{g^b}}, \tag{14}$$

where F_ℓ is the cyclic subextension of degree p of $\mathbb{Q}(\xi_\ell)$ and where $\overline{\sigma}_{g^b}$ is the automorphism acting trivially on ζ_p and such that $\xi_\ell \mapsto \xi_\ell^{g^b}$, which gives an exact system of representatives for $\mathrm{Gal}(F_\ell/\mathbb{Q})$.

From Remark 3.4 (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 $F_\ell/\mathbb{Q}$ (see a survey in [18, Remark 3.10]).

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 (14) 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 a "poor" information. Thus, the relationship of $\alpha = \tau(\psi)^p$ (whence of $\tau(\psi)$) with class field theory over K (i.e., with p-classes and units of K) is tenuous, possibly empty; which is quite the opposite for the twists $\mathrm{g}_c(\ell)$ because of the relation $\alpha^{c-s_c} = \mathrm{g}_c(\ell)^p$ and the fact that the $\mathrm{g}_c(\ell)$ are radicals defining non-trivial (arithmetically) cyclic extensions of degree p of K_+.

In another direction, suggested by the work of Lecouturier [28] among others, consider the non-Galois extension $\widetilde{F}_\ell := \mathbb{Q}(\sqrt[p]{\widetilde{\alpha}})$, where $\widetilde{\alpha} = \ell$; of course, $K(\sqrt[p]{\widetilde{\alpha}})/K$ is a cyclic extension of degree p (undecomposed over a strict subfield of K), ramified at the $p-1$ primes $\mathfrak{L} \mid \ell$ and at p if and only if $\ell \not\equiv 1 \pmod{p^2}$. Then [28] shows on the contrary that the p-class group of $\widetilde{F}_\ell$ strongly depends on the arithmetic of K while the radical $\widetilde{\alpha}$ does not.

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

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

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 $\widetilde{F}_\ell$ as ℓ varies, and genera theory implies $\mathrm{rk}_p(\mathcal{C}\ell_{\widetilde{F}_\ell}) \geq 1$ for all ℓ (for the metabelian genera theory, see [25]). However, for $M = K(\sqrt[p]{\alpha})$:

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

but in this case, M/K decomposes into F_ℓ and only the isotopic component for the unit character is concerned, which gives in fact a trivial part of the Chevalley's formula (contrary to the metabelian case $\widetilde{M}/\mathbb{Q}$).

So the "folk heuristic" shall be to say that, because of F_ℓ defined by the radical $\alpha = \tau(\psi)^p$, the p-adic properties of the Gauss sums are independent of the arithmetic of K (i.e., random) as ℓ varies (despite the apparent complexity of the radical $\alpha = \tau(\psi)^p$), while the properties of $\widetilde{F}_\ell$ are strongly dependent (despite the obvious simplicity of the radical $\widetilde{\alpha} = \ell$). In other words we have probably some 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 $\mathrm{g}_c(\ell)$, 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 § 4.5.

We shall examine the case of the twists, $\mathrm{g}_c(\ell)$ (more precisely of $\psi^{-c}(c)\,\mathrm{g}_c(\ell)$ as product of Jacobi sums), then the case of the original Gauss sums $\tau(\psi)$ from the arithmetic of the fields F_ℓ.

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

$$J(\ell) := \psi^{-c}(c)\,\mathrm{g}_c(\ell) = \psi^{-c}(c)\,\tau(\psi)^{c-\sigma_c} = J_1\cdots J_{c-1} \text{ (see (11))} \tag{15}$$

written on the basis $\{1,\zeta_p,\dots,\zeta_p^{p-2}\}$, under the form $J(\ell) = \sum_{k=0}^{p-2} a_k(\ell)\,\zeta_p^k$, the integers $a_k(\ell)$ being considered modulo p. A first information, about the p-adic repartition of the $J(\ell)$ 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:

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

for all the primes $p \geq 7$ tested (rank 1 for $p = 3$ and rank 2 for $p = 5$). We have verified it up to $p \leq 300$, an interval which contains 14 irregular primes. The program gives 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);M=matrix(1,p-1);r=0;
for(i=1,10^8,el=1+2*i*p;if(isprime(el)==0,next);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);J=lift(Mod(J,P));V=vector(p-1,j,component(J,j));
MM=concat(M,V);rr=matrank(MM);if(rr==r,next);r=rr;M=MM;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 $J(\ell) \equiv 1 \pmod{\mathfrak{p}}$, whence $\sum_{k=0}^{p-2} a_k(\ell) \equiv 1 \pmod{p}$, and we can write $J(\ell) = 1 + \sum_{k=1}^{p-2} a_k(\ell)\,(\zeta_p^k - 1)$ depending on $p-2$ parameters; then, due to the relations $J(\ell)^{1+s_{-1}} \equiv 1 \pmod{p}$ and $J(\ell)^{e_\omega} \in K^{\times p}$ (because $\omega(c - s_c) \equiv 0 \pmod{p}$), this yields the three relations of "derivation" ($p \geq 7$):

$$\sum_{k=1}^{p-2} k^\delta \cdot a_k(\ell) \equiv 0 \pmod{p},\ \delta \in \{1,2,4\},\ \text{ for any } \ell \in \mathscr{L}_p.$$

This explains a $\mathbb{F}_p$-rank at most $p-4$, but we have no proof of the fact that the rank is not less than $p-4$.

The order of magnitude of ℓ_p seems to be $O(1)\,p^2 \log(p^2)$, but the program slows down very much as p increases, which prevents to be more precise; give now the end of the computations with an estimation of the $O(1)$:

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

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 F_ℓ and let $Z_{F_\ell}/p\,Z_{F_\ell}$ be the residue ring modulo 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 the expression (14) giving $\tau(\psi) = -\sum_{b=0}^{p-1} \zeta_p^b \cdot \big[\mathrm{Tr}_{\mathbb{Q}(\xi_\ell)/F_\ell}(\xi_\ell)\big]^{\sigma(b)}$, where $\sigma(b) := \overline{\sigma}_{g^b}$ and $\psi(g) = \zeta_p$, the images in $Z_{F_\ell}/p\,Z_{F_\ell}$ of the conjugates of the $\mathrm{Tr}(\xi_\ell) := \mathrm{Tr}_{\mathbb{Q}(\xi_\ell)/F_\ell}(\xi_\ell)$ may be easily analysed and compared, for $\ell \in \mathscr{L}_p$, by means of the image R_ℓ in $\mathbb{F}_p[x]$ of the polynomial:

$$Q_\ell = \prod_{\overline{\sigma} \in \mathrm{Gal}(F_\ell/\mathbb{Q})} \big(x - \mathrm{Tr}(\xi_\ell)^{\overline{\sigma}}\big) \in \mathbb{Z}[x].$$

Proposition 5.3. *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 $\tau(\psi_2) \equiv \tau(\psi_1)^\sigma \pmod{\mathfrak{p}^p Z_{FK}}$; we recall that $\tau(\psi_1)^\sigma = \zeta_\sigma\, \tau(\psi_1^e)$, $\zeta_\sigma \in \mu_p$, $e \in \mathbb{Z}/p\mathbb{Z}$. 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:

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

$$\tau(\psi_1)^\sigma - \tau(\psi_2) = \sum_{b=1}^{p-1} (\zeta_p^b - 1) \cdot \big(\mathrm{Tr}(\xi_{\ell_2})^{\sigma_2(b)} - \mathrm{Tr}(\xi_{\ell_1})^{\pi(\sigma_1(b))} \big) \equiv 0 \,(\mathrm{mod}\ \mathfrak{p}^p Z_{FK}).$$

Since the $\zeta_p^b - 1$, $b \in [1, p-1]$, define a $\mathbb{Z}$-basis of $\mathfrak{p}\, Z_K$, then a Z_F-basis of 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 $\mathbb{F}_p[x]$ (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.

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)==0,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))}
```

Give a short excerpt of the table of the R_ℓ for $p = 7$ with $\ell \in [1,\, 5{\cdot}10^3]$:

```
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=113   f=7  R=x^7 + x^6 + x^5 + 2*x^4 + 4*x^3 + 2*x^2 + 6
(...)
el=4831  f=7  R=x^7 + x^6 + 2*x^5 + 5*x^4 + 3*x^3 + 6*x^2 + 3*x + 1
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 coefficients (except that of x^{p-1} since $\mathrm{Tr}_{\mathbb{Q}(\xi_\ell)/\mathbb{Q}}(\xi_\ell) = -1$).

We verify that for $p = 3$ the six possible polynomials are of the form R_ℓ. For $p = 5$ there are 150 possible polynomials. For $p = 7$, there are 17192 possible polynomials. But to establish the list of the *distinct* polynomials R_ℓ, the program becomes very slow as ℓ increases:

(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):

```
{p=5;B=10^7;L=List;N=0;el= 1;while(el<B,el=el+2*p;if(isprime(el)==0,next);
P=polcyclo(el);g=znprimroot(el);h=g^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+x^e);Tr=Mod(Tr,P);
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);t=0;for(m=1,N,S=component(L,m);
if(S==R,t=1;break));if(t==0,listput(L,R);N=N+1;print(N," ",el," ",R)))}
(...)
32   5591     x^5 + x^4 + 4*x^3 + x^2 + 4*x + 2
33   6211     x^5 + x^4 + x^3 + x^2 + x
34   6271     x^5 + x^4 + 2*x^3 + 4*x^2 + 3*x + 4
35   13451    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.

Remarks 5.4. (i) One verifies (using the program of § 4.5.1) that, as expected, if two primes ℓ give the same R, the lists of exponents of p-primarity are identical (e.g., $p = 5$, $R = x^5 + x^4 + 4$ obtained for $\ell = 1151$, 1601, 1951, 3001, 3251, 3851, 4651, 4751, up to 5000, with exponent of p-primarity 2).

(ii) If $n_0 \in \mathscr{E}_\ell(p) \cap \mathscr{E}_0(p)$ when the class of $\mathcal{L} \mid \ell$ generates $\mathcal{C}\ell_{\chi_0^*}$, then we get $\mathrm{g}_c(\ell)_{\chi_0^*} \equiv 1 \pmod p$ for all $\ell \in \mathscr{L}_p$ (see § 4.5); this gives (non-linear) relations modulo p between the conjugates of the traces $\mathrm{Tr}_{\mathbb{Q}(\xi_\ell)/F_\ell}(\xi_\ell)$ for all $\ell \in \mathscr{L}_p$, which may seem excessive.

(iii) It is clear that a large number of polynomials R_ℓ strengthens Vandiver's conjecture since the corresponding $J(\ell) = \psi^{-c}(c)\,\mathrm{g}_c(\ell)$ (see (15)) cover sufficiently possibilities modulo p, especially since we know that the $\mathbb{F}_p$-rank associated to the family of $\big(J(\ell)\big)_{\ell \in \mathscr{L}_p}$ 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; indeed, a *single* suitable ℓ may ensure a positive test for Vandiver's conjecture as shown by the table given in § 4.4.2.

We propose the following heuristic, about the sets $\mathscr{E}_\ell(p)$ of exponents of p-primarity, using the number $\mathscr{N}_p$:

Heuristic 5.5. *For any given p, the probability of $\mathscr{E}_\ell(p) = \emptyset$, for a single $\ell \in \mathscr{L}_p$, is $(1 + o(1)) \cdot e^{-\frac{1}{2}}$; the probability of at least a counterexample to Vandiver's conjecture is $O(1)\left(1 - e^{-\frac{1}{2}}\right)^{\mathscr{N}_p}$, with $\mathscr{N}_p := \#\{R_\ell,\ \ell \in \mathscr{L}_p\}$, where $R_\ell = \prod_{\overline{\sigma} \in \mathrm{Gal}(F_\ell/\mathbb{Q})} \left(x - \mathrm{Tr}_{\mathbb{Q}(\xi_\ell)/F_\ell}(\xi_\ell)^{\overline{\sigma}}\right)$ seen in $\mathbb{F}_p[x]$.*

It will be necessary to confirm these facts, to estimate $\mathscr{N}_p$ and prove the independence of the p-adic properties of the sets of traces as ℓ varies, in which case Vandiver's conjecture is very credible. Such a goal may perhaps be accessible by specialists of analytic number theory.

5.4. **Consequences of a failure of Vandiver's conjecture.** We have seen that under the p-primarity of $\mathrm{g}_c(\ell)_{\chi_0^*}$ for the exponent of p-irregularity

n_0, the corresponding component of the list counting the p-primarities, increases at each step. For instance, if for $p = 37$ the exponent $n_0 = 32$ of 37-irregularity was an exponent of p-primarity, the last line of the data § 4.5.3 would be the awful result (16th component equal to $75 + 1432 = 1507$):

$$L = [83, 96, 86, 91, 80, 80, 86, 83, 92, 83, 98, 76, 83, 78, 86, \mathbf{1507}, 76].$$

Let $x(\ell)$ be the mean value of the components of the list L and let N_ℓ be the number of primes ℓ tested at this step. Then from the above, $x(\ell) \approx 84$ and this would give a 16th component $x_0(\ell) \approx x(\ell) \cdot \frac{p-1}{2}$ as $\ell \to \infty$ (here, $\frac{75+1432}{84} \approx 17.94$).

Then we may estimate $x(\ell)$ very approximatively equal to $\frac{2\,N}{p}$ where N is the number of exponents of p-primarity obtained in the selected interval of primes ℓ, and we may put $N_\ell \approx O(1) \cdot N$; whence $x(\ell) \approx \frac{2}{p} \cdot N_\ell \cdot (1 + O(1))$ giving the pathological component $x_0(\ell) \approx N_\ell \cdot (1 + O(1))$.

6. Conclusion

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

Let us define a "main algorithm", associated to the test of Vandiver's conjecture for p, as the passage from ℓ to the next ℓ' in $\mathscr{L}_p$, the crucial step being the computation of the Jacobi sums ($1 \leq i \leq c-1$):

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

where lg and lg′ are the discrete logarithms for the primes ℓ and ℓ'; then we have $\psi^{-c}(c) \cdot \mathrm{g}_c(\ell) = J_1 \cdots J_{c-1}$. Since the Jacobi sums have, a priori, no p-adic "algebraic link", this suggests randomness and applies for many independent primes ℓ. Another possibility of "algorithm" should be 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, giving the coefficients of the Gauss sums, the fields $\mathbb{Q}(\mu_\ell)$ being, a priori, independent of the arithmetic of K.

Remark 6.1. There are two constraints, for 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 (finite in number) of ideals $\mathfrak{L} \mid \ell$ for $\ell \in \mathscr{L}_p$ are all represented with standard densities.

(ii) The ideal factorization of $\tau(\psi)^p$, $\psi : \mathbb{F}_\ell^\times \to \mu_p$, is related to *congruences modulo the conjugates of a prime ideal* $\mathfrak{L} \mid \ell$ *and is canonical* (this yields to Stickelberger's theorem and its consequences [43, § 15.1], [6, 46]); the reference [35] may give some help for the annihilation of $\mathcal{C}\ell_{\chi_0^*}^{(p)}$. A similar context is that of the ℓ-adic Γ-function of Morita (do not confuse p and ℓ,

often permuted in the literature). However, since we consider characters ψ of order p, the *p-adic congruential properties* of Gauss sums (or Jacobi sums) do not follow any law (in our opinion and according to classical literature), what explains that the negation of the distribution properties (i.e., randomness), for at least one irregular prime p, implies a very tricky complexity of the above "algorithms", as the fact that $\mathscr{E}_\ell(p) \cap \mathscr{E}_0(p) \neq \emptyset$ (or the weaker property $\mathscr{E}_\ell(p) \neq \emptyset$), for all $\ell \in \mathscr{L}_p$, which comes from the non-cyclicity of $\mathcal{C}\ell_{\chi_0^*}^{(p)}$ for some χ_0^*.

These fundamental p-adic properties of Gauss sums may have crucial consequences in various domains:

Vandiver's conjecture is often strongly necessary (e.g., in [7] about the Galois cohomology of Fermat curves, in [38] for the root numbers of the Jacobian varieties of Fermat curves, then in several papers on Galois p-ramification theory as in [36, 37], or [44, 45] in relation with modular forms, then in numerous papers and books on the theory of deformations of Galois representations as in [2, 31], Iwasawa's theory context as in [5] for μ-invariants in Hida families). In a geometrical viewpoint, the Riemann hypothesis for Fermat curves [43, § 6.1] gives a basic link with Jacobi sums.

Then it may be legitimate to think that all these numerous basic congruential aspects are (logically) governing principles of a wide part of algebraic number theory, as follows, beyond the case of the pth 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, Hecke Grössencharacters $\longrightarrow$ *Stickelberger element* $\longrightarrow$ *p-adic L-functions* $\longrightarrow$ *Herbrand theorem & Main theorems on abelian fields* $\longrightarrow$ *annihilation of the p-torsion group $\mathcal{T}$ of real abelian fields* $\longrightarrow$ *universal isomorphism $\mathcal{T} \simeq \mathrm{H}^2(G_{S_p}, \mathbb{Z}_p)^*$* $\longrightarrow$ *p-rationality of number 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 analysed about various deep conjectures: Greenberg's conjectures (in Iwasawa theory over totally real fields [19] and on representation theory [21]), p-rationalities of a number field as $p \to \infty$, Ankeny–Artin–Chowla conjecture fromthe conjectural existence of a p-adic Brauer–Siegel theorem [17]... All these questions being related to the deep invariant $\mathcal{T}$ that may be considered as an ultimate information beyond Leopoldt's conjecture.

As shown by the numerous evidences given in § 5.2, Vandiver's conjecture may come, for $p \gg 0$, from Borel–Cantelli heuristic, on exceptional features of Gauss sums of probabilities much less than $\frac{O(1)}{p^2}$; but this point of view allows cases of failure of the conjecture, which is not satisfactory for the

theoretical fundations of the above subjects. Possibly, there is an universal property of the sets $\mathscr{E}_\ell(p)$ coming from the fact that all $\ell \in \mathscr{L}_p$ intervene.

To be very optimistic (but not very rigorous), one can perhaps say that Vandiver's conjecture is true because it has been verified for sufficiently many prime numbers [4, 8]. In a more serious statement, we may assert that Vandiver's conjecture holds for almost all primes; the precise finite cardinality of the set of counterexamples ($\emptyset$ or not) is (in our opinion) not of algebraic nature nor enlightened by class field theory, 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.

References

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

[2] T. Berger, *Oddness of residually reducible Galois representations*, International Journal of Number Theory **14** (2018), no. 5, 1329–1345. https://doi.org/10.1142/S1793042118500835

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

[4] J.P. Buhler and D. Harvey, *Irregular primes to* 163 *million* Math. Comp. **80** (2011), no. 276, 2435–2444. https://doi.org/10.1090/S0025-5718-2011-02461-0

[5] J. Bellaïche and R. Pollack, *Congruences with Eisenstein series and mu-invariants* (preprint 2018). https://arxiv.org/abs/1806.04240

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

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

[8] W. Hart, D. Harvey and W. Ong, *Irregular primes to two billion*, Math. Comp. **86** (2017), 3031–3049 (2016). https://doi.org/10.1090/mcom/3211

[9] J. S. Ellenberg and A. Venkatesh, *Reflection principles and bounds for class group torsion*, Int. Math. Res. Not. **2007**, no. 1. https://doi.org/10.1093/imrn/rnm002

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

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

[12] G. Gras, *Class Field Theory: from theory to practice*, corr. 2nd ed., Springer Monographs in Mathematics, Springer, 2005, xiii+507 pages. https://doi.org/10.1007/978-3-662-11323-3 https://www.researchgate.net/publication/268005797

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

[14] G. Gras, *Annihilation of* $\mathrm{tor}_{\mathbb{Z}_p}(\mathcal{G}_{K,S}^{\mathrm{ab}})$ *for real abelian extensions* $K/\mathbb{Q}$, Communications in Advanced Mathematical Sciences **1** (2018), no. 1, 5–34. http://dergipark.gov.tr/download/article-file/543993

[15] G. Gras, *Sur la p-ramification abélienne*, Conférence donnée à l'University Laval, Québec, Mathematical series of the department of mathematics **20** (1984), 1–26. https://www.dropbox.com/s/fusia63znk0kcky/Lectures1982.pdf?dl=0
[16] G. Gras, *The p-adic Kummer-Leopoldt Constant: Normalized p-adic Regulator*, Int. J. Number Theory **14** (2018), no. 2, 329–337. https://doi.org/10.1142/S1793042118500203
[17] G. Gras, *Heuristics and conjectures in direction of a p-adic Brauer–Siegel theorem*, Math. Comp. (2018). https://doi.org/10.1090/mcom/3395
[18] G. Gras, *Invariant generalized ideal classes–Structure theorems for p-class groups in p-extensions*, Proc. Math. Sci. **127** (2017), no. 1, 1–34. https://doi.org/10.1007/s12044-016-0324-1
[19] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), no. 1, 263–284. http://www.jstor.org/stable/2373625?
[20] R. Greenberg, *On the jacobian variety of some algebraic curves*, Compositio Math. **42** (1980), 345–359. http://www.numdam.org/article/CM_1980__42_3_345_0.pdf
[21] R. Greenberg, *Galois representations with open image*, Annales de Mathématiques du Québec **40** (2016), no. 1, 83–119. https://doi.org/10.1007/s40316-015-0050-6
[22] H. Ichimura, *Local Units Modulo Gauss Sums*, Journal of Number Theory **68** (1998), 36–56. https://doi.org/10.1006/jnth.1997.2206
[23] H. Ichimura and M. Kaneko, *On the Universal Power Series for Jacobi Sums and the Vandiver Conjecture*, Journal of Number Theory **31** (1989), 312–334. https://core.ac.uk/download/pdf/81986387.pdf
[24] K. Iwasawa, *A note on Jacobi sums*, Symposia Mathematica **15**, Academic Press (1975), 447–459. https://mathscinet.ams.org/mathscinet-getitem?mr=1275719
[25] J.-F. Jaulent, *Unités et classes dans les extensions métabéliennes de degré $n\ell^s$ sur un corps de nombres algébriques*, Ann. Inst. Fourier (Grenoble) **31** (1981) 39–62. http://www.numdam.org/article/AIF_1981__31_1_39_0.pdf/
[26] M. Kurihara, *Some remarks on conjectures about cyclotomic fields and K-groups of* $\mathbb{Z}$, Compositio Math. **81** (1992), 223–236. http://www.numdam.org/item/CM_1992__81_2_223_0
[27] I. Kersten and J. Michaliček, *On Vandiver's conjecture and $\mathbb{Z}_p$-extensions of $\mathbb{Q}(\zeta_{p^n})$*, Journal of Number Theory **32** (1989), no. 3, 371–386. https://doi.org/10.1016/0022-314X(89)90091-7
[28] E. Lecouturier, *On the Galois structure of the class group of certain Kummer extensions*, J. London Math. Soc. **98** (2018), no. 2, 35–58. https://doi.org/10.1112/jlms.12123
[29] C. Maire, *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
[30] W. G. Mc Callum, *Greenberg's conjecture and units in multiple $\mathbb{Z}_p$-extensions*, American Journal of Mathematics **123** (2001), no. 5, 909–930. https://www.jstor.org/stable/25099088
[31] A. Mézard, *Obstructions aux déformations de représentations galoisiennes réductibles et groupes de classes*, Journal de théorie des nombres de Bordeau **17** (2005), no. 2, 607–618.https://doi.org/10.5802/jtnb.510
[32] P. Mihăilescu, *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, P. Pardalos, T. Rassias (Eds.), Springer-Verlag (2012), pp. 287–294. http://poivs.tsput.ru/en/Biblio/Publication/11335
[33] The PARI Group, *PARI/GP, version `2.9.0`*, Université de Bordeaux (2016). http://pari.math.u-bordeaux.fr/

[34] K. A. Ribet, *Bernoulli numbers and ideal classes*, Gaz. Math. **118** (2008), 42–49. https://mathscinet.ams.org/mathscinet-getitem?mr=MR2459143
[35] C.-G. Schmidt, *On Ray Class Annihilators of Cyclotomie Fields*, Invent. math. **66** (1982), 215–230. https://eudml.org/doc/142878
[36] R.T. Sharifi *A reciprocity map and the two-variable p- adic L-function*, Ann. of Math. (2), **173** (2011), no. 1, 251–300. https://arxiv.org/pdf/0709.3591v3.pdf
[37] R.T. Sharifi, *Relationships between conjectures on the structure of pro-p Galois groups unramified outside p* (preprint 2018).http://math.ucla.edu/~sharifi/galstr.pdf
[38] J. Shu, *Root numbers and Selmer groups for the Jacobian varieties of Fermat curves* (preprint 2018). https://arxiv.org/pdf/1809.09285v2.pdf
[39] C. Soulé, *Perfect forms and the Vandiver conjecture*, J. Reine Angew. Math. **517** (1999), 209–221. https://doi.org/10.1515/crll.1999.095
[40] C. Soulé, *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
[41] F. Thaine, *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** (1995), no. 2, 311–344. https://projecteuclid.org/euclid.mmj/1029005231
[42] F. Thaine, *On the coefficients of Jacobi sums in prime cyclotomic fields*, Transactions of the Amer. Math. Soc. **351** (1999), no. 12, 4769–4790. https://www.ams.org/journals/tran/1999-351-12/S0002-9947-99-02223-0/S0002-9947-99-02223-0.pdf
[43] L.C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math. 83, Springer enlarged second edition 1997.
[44] P. Wake and C.W. Erickson, *Ordinary pseudorepresentations and modular forms*, Proc. Amer. Math. Soc. Ser. B, **4** (2017), 53–71.https://arxiv.org/pdf/1510.01661.pdf
[45] P. Wake and C.W. Erickson, *Pseudo-modularity and Iwasawa theory*, Amer. J. Math. **140** (2018), no. 4, 977–1040. https://arxiv.org/pdf/1505.05128.pdf
[46] A. Weil, *Jacobi sums as "Grössencharaktere"*, Trans. Amer. Math. Soc. **73** (1952), 487–495.https://www.jstor.org/stable/1990804

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