# 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), Anglès–Nuccio (2010) and has been considered by many authors with various purposes (e.g., Iwasawa theory). In this article, we give again the interpretation of Vandiver's conjecture in terms of the minus part of the torsion group of the Galois group of the maximal abelian $p$-ramified pro-$p$-extension of the $p$th cyclotomic field, that we had published at the Laval University (1984), in relation with the result of Iwasawa. Then we provide a specific use of Gauss sums that allows a new numerical test of Vandiver's conjecture (see Theorem 4.5 using both the set of exponents of $p$-irregularity and the set of exponents of $p$-primarity of the Gauss sum associated to a totally split prime number). Then we propose new favorable heuristics for its rightness. We show that a counterexample to Vandiver's conjecture leads to a totally strange phenomenon on the congruential properties of Gauss sums and to an unusual complexity of some classical algorithms. Some tables with PARI programs are given to strength our arguments.

## Contents



*Date*: August 9, 2018.

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

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

## 1. Introduction

Let $K = \mathbb{Q}(\mu_p)$ be the field of $p$th roots of unity for the 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. Then let $E$ and $E_+$ be the groups of units of $K$ and $K_+$, respectively; 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 $E_+$ [18, Theorem 8.14]. See numerical results for instance in [2, 3].

Many heuristics are known about this conjecture; see Washington's book [18, § 8.3, Corollary 8.19] for some history and criteria, then for probabilistic arguments. We have also given a probabilistic study in [6, II.5.4.9.2]. All these heuristics lead to the fact that the number of primes $p$ less than $p_0$, giving a counterexample, can be of the form $c \cdot \log(\log(p_0))$, $c < 1$.

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

In this paper, we shall give numerical experiments in another direction using Gauss sums and Stickelberger annihilation of relative classes, together with the Thaine–Ribet–Mazur–Wiles–Kolyvagin–Greither main theorem on cyclotomic fields. Such a link with Gauss sums has been given first by Iwasawa [14] and applied by many authors in various directions (e.g., [1, 9, 12, 13]). We shall give a short survey about this in Section 3.

Then we shall use the reflection principle to interprete a counterexample to Vandiver's conjecture in terms of non-trivial "$p$-primary relative pseudo-units" stemming from Gauss sums; this shall give the main test verifying the validity of the conjecture for a given $p$ (Theorem 4.5).

More precisely, if $\#\mathcal{C}\ell_+ \equiv 0 \pmod p$, there exists a class $\gamma = cl(\mathfrak{A}) \in \mathcal{C}\ell_-$, of order $p$, such that $\mathfrak{A}^p = (\alpha)$, with $\alpha$ $p$-primary (to give the unramified extension $K(\sqrt[p]{\alpha})/K$, decomposed over $K_+$ into the cyclic unramified extension $L_+/K_+$ predicted by class field theory); since $\alpha$ can be obtained explicitely by means of infinitely many Gauss sums associated to the prime numbers $\ell \equiv 1 \pmod p$, we show that some assumtion of independence, of the congruential properties of these Gauss sums, is an obstruction to any counterexample to Vandiver's conjecture or, at least, that the probability of such a counterexample is at most $\frac{O(1)}{p^2}$.

This method is different from those needing to prove that some cyclotomic units are not global $p$th powers, which is more complicated and does not give natural probabilistic approaches.

Finally, we propose (see § 5.2), from the properties of these Gauss sums, new heuristics (to our knowledge) and give substantial numerical experiments which confirms them. All the PARI [16] programs can be copy and paste by the reader for any further experience.

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

(i) We denote by $\omega$ the character of Teichmüller of $G$ (i.e., the $p$-adic character with values in $\mu_{p-1}(\mathbb{Q}_p)$ such that $\zeta^s = \zeta^{\omega(s)}$ for all $\zeta \in \mu_p$ and $s \in G$).

(ii) An irreducible $p$-adic character of $G$ is of the form $\theta = \omega^n$, $1 \leq n \leq p-1$; we denote by 1 the unit character ($n = p-1$).

(iii) If $\theta = \omega^n$, we put $\theta^* := \omega\theta^{-1} = \omega^{p-n}$.

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

(v) For a finite $\mathbb{Z}_p[G]$-module $M$, we shall write $M_\theta := M^{e_\theta}$ for the $\theta$-component of $M$. This gives rise to the obvious definition of parity of the characters and that of the components $M_+$ and $M_-$ such that $M = M_+ \oplus M_-$.

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

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

(viii) For $\chi = \omega^n \neq 1$, $n$ even, denote by $b(\chi^*) = \frac{1}{p} \sum_{a=1}^{p-1} (\chi^*)^{-1}(s_a)\, a$ the generalized Bernoulli number $B_{1,(\chi^*)^{-1}} = B_{1,\omega^{n-1}}$; it is an element of $\mathbb{Z}_p$ congruent modulo $p$ to $\frac{B_n}{n}$, where $B_n$ is the ordinary Bernoulli number of index $n$ [18, Proposition 4.1, Corollary 5.15].

(ix) The index of $p$-irregularity $i(p)$ is the number of even $n \in [2, p-3]$ such that $B_n \equiv 0 \pmod p$ (see [18, § 5.3] for some statistics about $i(p)$).

**Working Hypothesis 1.2.** *To simplify and to be realistic in an heuristic point of view, we assume that each $\mathcal{C}\ell_{\chi^*}$ is trivial or cyclic of order $p$, for the even characters $\chi \neq 1$; in other words, we assume that $\mathcal{C}\ell_- \simeq (\mathbb{Z}/p\mathbb{Z})^{i(p)}$.*

Indeed, we know that $\#\mathcal{C}\ell_{\chi^*} \equiv 0 \pmod{p^2}$ has probability less than $\frac{O(1)}{p^2}$, and may be considered as giving a finite number of counterexamples to Vandiver's conjecture, what can be discarded for our purpose.

The Thaine–Ribet–Mazur–Wiles–Kolyvagin main theorem on abelian fields is in $K$:

$$\#\mathcal{C}\ell_{\chi^*} = p^{v_p(b(\chi^*))}$$

(the $p$-part of $b(\chi^*)$), giving, under our assumption, $b(\chi^*) \sim p$ for each non-trivial component $\mathcal{C}\ell_{\chi^*}$, where $\sim$ means "equality up to a $p$-adic unit factor". But this main theorem is not necessary in our context and leads to the classical Herbrand theorem "$p \mid \mathcal{C}\ell_{\chi^*}$ implies $p \mid b(\chi^*)$" (the numerical results [2, 3] are in complete accordance with this viewpoint).

## 2. Pseudo-units – Notion of $p$-primarity

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

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

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

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

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

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

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

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

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

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

**Proposition 2.4.** *Let $\alpha \equiv 1 \pmod{\mathfrak{p}} \in K^\times$ and let $m \in [2, p-2]$. Let $\theta = \omega^m$, and consider $\alpha_\theta$. Then $\alpha_\theta \equiv 1 \pmod{\mathfrak{p}^m}$ and $\alpha_\theta$ 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 $\varpi$ in $\mathbb{Z}_p[\mu_p]$ which has the following properties (see, e.g., [6, Exercise II.1.8.3]):

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

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

We shall prove first that $\alpha_\theta = 1 + \varpi^m \beta$, $\beta \in \mathbb{Z}_p[\varpi]$, then that $\alpha_\theta$ is $p$-primary (i.e., $\beta \equiv 0 \pmod{\varpi^{p-m}}$) if and only if $\beta \equiv 0 \pmod{\varpi^{p-1}}$.

Put $\alpha_\theta = 1 + \varpi^k u$, where $u$ is a unit of $\mathbb{Z}_p[\varpi]$ and $k \geq 1$; let $u_0 \in \mathbb{Z} \setminus p\mathbb{Z}$ such that $u \equiv u_0 \pmod{\varpi}$. Since $\alpha_\theta^s = \alpha_\theta^{\theta(s)}$, 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 $\alpha_\theta = 1 + \varpi^k u$, $k \in \{m, m+p-1, \ldots\}$, with $m \in [2, p-2]$.

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

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

## 3. Link with $p$-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 $H^{\mathrm{pr}}$ of $K$ (for more information, see [6, 7, 10]).

Write $\mathcal{T} = \mathcal{T}_+ \oplus \mathcal{T}_-$; then we difine, in an obvious way, $H_-^{\rm pr} \subseteq H^{\rm pr}$ (fixed by $\mathcal{T}_+$) and $H_+^{\rm pr} \subseteq H^{\rm pr}$ (fixed by $\mathcal{T}_-$). Considering any character $\theta$ of $G$, we have, from the reflection theorem [6, Theorem II.5.4.5]:

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

which gives the following interpretation:

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

*Proof.* We shall justify this well-known "global" reflection result as follows (the proof for the isotypic components being similar, taking the $\theta$ or $\theta^*$-components for each object).

The Kummer radical of the compositum of the cyclic extensions of degree $p$ of $K$ contained in $H_-^{\rm pr}$ is generated (modulo $K^{\times p}$) by the obvious part $E_+$ of real units, giving a $p$-rank $\frac{p-3}{2}$, then by the real $p$-unit $\eta_+ := \zeta_p + \zeta_p^{-1} - 2$, and by the pseudo-units $\alpha_+$ comming from $\mathcal{C}\ell_+$, which gives the $p$-rank of this radical equal to $\frac{p-1}{2} + \mathrm{rk}_p(\mathcal{C}\ell_+)$.

Since $\mathrm{rk}_p(\mathrm{Gal}(H_-^{\rm pr}/K)) = \frac{p-1}{2} + \mathrm{rk}_p(\mathcal{T}_-)$ ($\frac{p-1}{2}$ corresponds to the compositum of the non-cyclotomic $\mathbb{Z}_p$-extensions), we get $\mathrm{rk}_p(\mathcal{T}_-) = \mathrm{rk}_p(\mathcal{C}\ell_+)$. □

*Remark* 3.2. At each unramified cyclic extension $L_+$ of degree $p$ of $K_+$ is associated a $p$-primary pseudo-unit $\alpha \in K^\times \backslash K^{\times p}$ such that $\alpha^{1+s_{-1}} \in K^{\times p}$ and such that $L_+K = K(\sqrt[p]{\alpha})$. Put $(\alpha) = \mathfrak{A}^p$, where $\mathfrak{A}$ is an ideal of $K$ such that $\mathfrak{A}^{1+s_{-1}}$ is $p$-principal (i.e., the image of its class in $\mathcal{C}\ell$ is trivial); moreover $\mathfrak{A}$ is not $p$-principal, otherwise $\alpha$ should be, up to a $p$th power factor, a unit $\varepsilon \in E$ such that $\varepsilon^{1+s_{-1}} \in E^p$, which gives $\varepsilon \in \mu_p$ (absurd). In the same way, if $G$ operates via $\chi$ on $\mathrm{Gal}(L_+/K_+)$ then by Kummer duality $G$ operates via $\chi^*$ on $\langle\alpha\rangle K^{\times p}$.

We shall prove that such pseudo-units $\alpha$ may be found by means of Gauss sums (Lemma 4.4).

3.2. **Vandiver's conjecture and Gauss sums.** Recall the formula (see [6, 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 $K$; if $\mathfrak{A} \in I$, let $e$ be such that $\mathfrak{A}^e = (\alpha)$, then $\log(\mathfrak{A}) := \frac{1}{e}\log(\alpha)$ where log is the $p$-adic logarithm, then $U$ is the group of principal local units of $\mathbb{Q}_p(\mu_p)$ which is equal to $1 + \varpi\, \mathbb{Z}_p[\varpi]$. Taking the minus part, $\log(\mathfrak{A})$ becomes well-defined.

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

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

Mention the following reasonning (from [9, § 3]) giving another interpretation of the result of Iwasawa [14]. Let $S := \frac{1}{p}\sum_{a=1}^{p-1} a\, s_a^{-1} \in \mathbb{Q}[G]$ be the Stickelberger element of $K$; it is such that $S\,.\,e_{\chi^*} = b(\chi^*)\,.\,e_{\chi^*} := B_{1,(\chi^*)^{-1}}\,.\,e_{\chi^*}$ for all even $\chi \neq 1$; then if $\chi = \omega^n$, $\chi^* = \omega^{p-n}$ for which $\#\mathcal{C}\ell_{\chi^*}$ corresponds to the ordinary Berrnoulli numbers $B_n$ giving the "exponents of $p$-irregularity $n$" when $B_n \equiv 0 \pmod p$ (see Definition 1.1 (viii)).

Now we know that for any prime ideal $\mathfrak{L}$ of $K$, $\mathfrak{L} \neq \mathfrak{p}$, we have the fundamental relation in $K$ (see [18, §§ 6.1, 6.2, 15.1]):

$$\mathfrak{L}^{pS} = \tau(\psi)^p\, \mathbb{Z}[\zeta_p], \tag{2}$$

where $\tau(\psi)$ is the Gauss sum:

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

where $F_{\mathfrak{L}}$ is the residue field of $\mathfrak{L}$, $\psi$ a character of order $p$ of $F_{\mathfrak{L}}^\times$, $\xi_\ell$ a primitive $\ell$th root of unity for $\ell = \mathfrak{L} \cap \mathbb{Z}$, and tr the trace in $F_{\mathfrak{L}}/\mathbb{F}_\ell$. Since the choices of $\mathfrak{L}$, $\psi$ and $\xi_\ell$, from a given $\ell$, correspond to Galois conjugations, we denote simply $\tau(\psi)$ such a Gauss sum; this has some importance since once the prime ideal $\mathfrak{L}$ and $\xi_\ell$ are fixed, up to conjugation, we shall consider the powers $\psi^c$ of $\psi$, for $c$ prime to $p$, and the Gauss sums $\tau(\psi^c)$.

Taking the logarithms in (2) and dividing by $p$ we obtain:

$$S\,.\,e_{\chi^*}\,.\log(\mathfrak{L}) = b(\chi^*)\,.\log(\mathfrak{L})\,.\,e_{\chi^*} = \log(\tau(\psi))\,.\,e_{\chi^*}, \text{ for all even } \chi \neq 1.$$

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

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

where $\mathcal{G}$ is the group generated by all the Gauss sums. So, the Vandiver conjecture for the $\chi$-component of $\mathcal{C}\ell$ (i.e., $\mathcal{T}_{\chi^*} = 1$) is equivalent to $\big(\mathbb{Z}_p \log\left(\mathcal{G}\right)/\log(U)\big)_{\chi^*} = 1$, and the whole Vandiver conjecture is equivalent to the fact that the images of the Gauss sums in $U$ generate the minus part of this $\mathbb{Z}_p$-module.

More precisely, assume the Hypothesis 1.2 and let $\chi$ even be such that $b(\chi^*) \sim p$; thus $\mathcal{T}_{\chi^*} = 1$ if and only if there exists at least a prime number $\ell$ such that the corresponding $\tau(\psi)_{\chi^*}$ generates $U_{\chi^*} \simeq 1 + \varpi^{p-n}\mathbb{Z}_p[\varpi]$, which needs only congruences modulo $p$; indeed, from Proposition 2.4 all is clear (we shall prove that this is equivalent to a property of non-$p$-primarity of a particular elements deduced from $\tau(\psi)_{\chi^*}$ in a suitable context, giving an explicit test for Vandiver's conjecture).

## 4. Gauss sums associated to ideals $\mathfrak{L}$ of residue degree 1

Let $\ell$ be a prime number totally split in $K$ (i.e., $\ell \equiv 1 \pmod p$). Let $\mathfrak{L} \mid \ell$ in $K$ and let $\psi : \mathbb{F}_{\mathfrak{L}}^{\times} \simeq \mathbb{F}_{\ell}^{\times} \longrightarrow \mu_p$ be a character of order $p$; if $g$ is a primitive root modulo $\ell$, one may put $\psi(\overline{g}) = \zeta_p$ to define $\psi$ on $\mathbb{F}_{\ell}^{\times}$. Let $\xi_\ell$ be a primitive $\ell$-th root of unity; then the Gauss sum associated to $\psi$ may be written in $\mathbb{Z}[\mu_p\,\ell]$:

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

4.1. **Practical computation of $\tau(\psi)^{c-\sigma_c}$.** Let $c \geq 2$ be a primitive root modulo $p$; to get an element of $K$, one must use the twisted version $\tau(\psi)^{c-\sigma_c}$, where $\sigma_c \in \mathrm{Gal}(\mathbb{Q}(\mu_p\,\ell)/\mathbb{Q})$ is the Artin automorphism of $c$ (its restriction to $K$ is $s_c \in G$). We put (still assuming $\ell \equiv 1 \pmod p$):

$$\tau_c(\mathfrak{L}) := \tau(\psi)^{c-\sigma_c} \text{ for } \psi : F_{\ell}^{\times} \longrightarrow \mu_p. \tag{4}$$

This notation using $\mathfrak{L} \mid \ell$ is justified by (2) and (3) giving, for all even $\chi$:

$$\mathfrak{L}^{S_c} = \tau_c(\mathfrak{L})\,\mathbb{Z}[\zeta_p] \;\;\&\;\; \mathfrak{L}_{\chi^*}^{(c-\chi^*(s_c))\cdot b(\chi^*)} = \tau_c(\mathfrak{L})_{\chi^*}\,\mathbb{Z}[\zeta_p] \tag{5}$$

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

$$b_c(\chi^*) := (c - \chi^*(s_c)) \cdot b(\chi^*) \sim b(\chi^*). \tag{6}$$

**Lemma 4.1.** *Let $\ell \equiv 1 \pmod p$ prime and let $\mathfrak{L} \mid \ell$ be a prime ideal in $K$. Then $\tau_c(\mathfrak{L})$ is a product of Jacobi sums and $\tau_c(\mathfrak{L}) \equiv 1 \pmod{\mathfrak{p}}$.*

*Proof.* We have the classical formula using Jacobi sums (for $\psi\,\psi' \neq 1$):

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

By induction, we obtain:

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

Concerning the congruence, we have:

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

but since $\ell$ is prime, $\displaystyle\sum_{x \in \mathbb{F}_{\ell}^{\times}} \xi_\ell^x = -1$, whence the result for $\tau_c(\mathfrak{L})$. □

Put $J = J_1 \cdots J_{c-1}$. Then in the above definition (4) of $\tau_c(\mathfrak{L})$, $\tau(\psi)^{\sigma_c} = \tau(\psi^c)\cdot\zeta(c)$, where $\zeta(c) \in \mu_p$; but for all $\chi \neq 1$, $\zeta(c)^{e_{\chi^*}} = 1$, which defines $\tau_c(\mathfrak{L})_{\chi^*} := J_{\chi^*}$ without ambiguity.

**Definitions 4.2.** (i) We call set of exponents of $p$-primarity, of a prime $\ell \equiv 1 \pmod p$, the set $\mathcal{E}_\ell(p) := \{n_1, \ldots, n_s\}$, $s \geq 0$, of even integers $n$ in $[2, p-3]$ such that $\tau_c(\mathfrak{L})_{\omega^{p-n}}$ is $p$-primary (this set does not depend on the choice of $\mathfrak{L} \mid \ell$).

(ii) We call set of exponents of $p$-irregularity, the set $\mathcal{E}_0(p) := \{\nu_1, \ldots, \nu_t\}$, $t \geq 0$, of even integers $\nu$ in $[2, p-3]$ such that $B_\nu \equiv 0 \pmod p$ (i.e., $b(\omega^{p-\nu}) \equiv 0 \pmod p$; see Definition 1.1 (viii)).

*Remark* 4.3. Let $\chi \neq 1$ be even. If $\tau_c(\mathfrak{L})_{\chi^*}$ is $p$-primary this does not give necessarily a counterexample to Vandiver's conjecture for the following possible reasons considering the expression $S_c\, e_{\chi^*} = b_c(\chi^*)\, e_{\chi^*}$ (recall that $b_c(\chi^*) \sim b(\chi^*)$):

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

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

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

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha) = 13476828486058846965136640289665418860379059885740625099289939159401864703561440252197759503241482448 07 = 23^{75}.$$

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

(ii) The number $b_c(\chi^*)$ is divisible by $p$, but the ideal $\mathfrak{L}_{\chi^*}$ is $p$-principal and then $\tau_c(\mathfrak{L})_{\chi^*}$ is a $p$th power in $K^\times$.

So, the best *necessary condition for a counterexample* is that there exists an even character $\chi \neq 1$ such that $\tau_c(\mathfrak{L})_{\chi^*}$ is $p$-primary and $b_c(\chi^*) \equiv 0 \pmod p$ (this shall be precised in Lemma 4.4 to give Theorem 4.5). The condition is not sufficient because of the case where $\mathfrak{L}_{\chi^*}$ is $p$-principal (which is not easy to verify).

4.2. **Program.** For the least prime $\ell \equiv 1 \pmod p$, the following program computes $\tau_c(\mathfrak{L})$ in $\mathsf{Mod}(\mathsf{J}, \mathsf{P})$, with $\mathsf{P} = \mathsf{polcyclo}(\mathsf{p})$, where the product $\mathsf{J}$ of Jacobi sums is written in $\mathbb{Z}[x]$; $\mathsf{c}$ is a primitive root modulo $\mathsf{p}$.

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

The computation of $\tau_c(\mathfrak{L})_{\chi^*}$ is given in $\mathsf{Sn} = \prod_{\mathsf{a}=1}^{\mathsf{p}-1} \mathsf{s_a}(\mathsf{J}^{\mathsf{a}^{\mathsf{n}-1}})$ from the formula $\tau_c(\mathfrak{L})_{\chi^*} = \prod_{a=1}^{p-1} \sigma_a(\tau_c(\mathfrak{L}))^{\omega^{n-p}(a)} = \prod_{a=1}^{p-1} \sigma_a(\tau_c(\mathfrak{L})^{a^{n-1}})$ up to a $p$th

power factor; then $a^{n-1}$ is computed modulo $p$ in $\mathsf{an}$ and then $\mathsf{J}^{\mathsf{an}}$ is given by $\mathsf{component}(\mathsf{LJ},\mathsf{an})$.

Finaly the conjugate $\mathsf{s}_{\mathsf{a}}(\mathsf{J}^{\mathsf{an}})$ is computed in $\mathsf{sJan}$ via the conjugation $\mathsf{x}\mapsto\mathsf{x}^{\mathsf{a}}$ in $\mathsf{J}^{\mathsf{an}}$, whence the product in $\mathsf{Sn}$.

```
{forprime(p=3,200,c=lift(znprimroot(p));
P=polcyclo(p)+Mod(0,p);X=Mod(x,P);ell=1;
while(isprime(ell)==0,ell=ell+2*p);g=znprimroot(ell);
print("p=",p," ell=",ell," c=",c," g=",g);J=1;for(i=1,c-1,Ji=0;
for(k=1,ell-2,kk=znlog(1-g^k,g);e=lift(Mod(kk+i*k,p));Ji=Ji-X^e);J=J*Ji);
d=p-2;LJ=listcreate;Jj=1;for(j=1,p-1,Jj=lift(Jj*J);listinsert(LJ,Jj,j));
for(m=1,(p-3)/2,n=2*m;pn=p-n;Sn=Mod(1,P);
for(a=1,(p-1)/2,an=lift(Mod(a,p)^(n-1));Jan=component(LJ,an);sJan=0;
for(j=0,d,aj=lift(Mod(a*j,p));sJan=sJan+x^(aj)*component(Jan,1+j));
Sn=Sn*sJan);if(Sn==1,print("     exponents of p-primarity: ",n))))}

p=3  ell=7      c=1  g=3
p=5  ell=11     c=2  g=2
p=7  ell=29     c=2  g=2
p=11 ell=23     c=3  g=5    exponents of p-primarity: 2
p=13 ell=53     c=2  g=2
p=17 ell=103    c=3  g=5
p=19 ell=191    c=4  g=19
p=23 ell=47     c=2  g=5
p=29 ell=59     c=2  g=2    exponents of p-primarity: 2
p=31 ell=311    c=7  g=17
p=37 ell=149    c=2  g=2
p=41 ell=83     c=6  g=2
p=43 ell=173    c=9  g=2    exponents of p-primarity: 26
p=47 ell=283    c=2  g=3
p=53 ell=107    c=2  g=2    exponents of p-primarity: 34, 10
p=59 ell=709    c=3  g=2
p=61 ell=367    c=2  g=6
p=67 ell=269    c=4  g=2
p=71 ell=569    c=2  g=3
p=73 ell=293    c=5  g=2
p=79 ell=317    c=2  g=2
p=83 ell=167    c=3  g=5
p=89 ell=179    c=3  g=2
p=97 ell=389    c=5  g=2    exponents of p-primarity: 26
p=101 ell=607   c=2 g=3     exponents of p-primarity: 10
p=103 ell=619   c=5 g=3
p=107 ell=643   c=2 g=11
p=109 ell=1091  c=6 g=2     exponents of p-primarity: 14, 86
p=113 ell=227   c=3 g=2
p=127 ell=509   c=3 g=2
p=131 ell=263   c=2 g=5     exponents of p-primarity: 16
p=137 ell=823   c=3 g=3     exponents of p-primarity: 78
p=139 ell=557   c=2 g=2
p=149 ell=1193  c=2 g=3
```

```
p=151 ell=907   c=6 g=2
p=157 ell=1571  c=5 g=2     exponents of p-primarity: 94
p=163 ell=653   c=2 g=2     exponents of p-primarity: 42
p=167 ell=2339  c=5 g=2     exponents of p-primarity: 122
p=173 ell=347   c=2 g=2
p=179 ell=359   c=2 g=7     exponents of p-primarity: 138
p=181 ell=1087  c=2 g=3     exponents of p-primarity: 114, 164
p=191 ell=383   c=19 g=5
p=193 ell=773   c=5 g=2     exponents of p-primarity: 108, 172
p=197 ell=3547  c=2 g=2     exponents of p-primarity: 62
p=199 ell=797   c=3 g=2
```

We shall see that, when the list of exponents of $p$-primarity is empty, this implies Vandiver's conjecture for $p$ (Corollary 4.6). Moreover this program only test the "first" prime $\ell$ and we shall see later that it is sufficient to try another $\ell$ to be successfull.

4.3. **Stickelberger element and Bernoulli numbers.** Recall that from § 4.1 we have, for all even $\chi \neq 1$, $(\tau_c(\mathfrak{L})_{\chi^*}) = \mathfrak{L}^{S_c\, e_{\chi^*}} = \mathfrak{L}_{\chi^*}^{b_c(\chi^*)}$. We still assume the Hypothesis 1.2.

**Lemma 4.4.** *Let $\chi \neq 1$ even be such that $\mathcal{C}\ell_\chi \neq 1$ (i.e., we assume to have a counterexample to Vandiver's conjecture). Then $\mathcal{C}\ell_{\chi^*} \neq 1$ and there exists a totally split prime ideal $\mathfrak{L}$ such that $\mathfrak{L}^{S_c\, e_{\chi^*}} = (\alpha_{\chi^*})$, where $\alpha_{\chi^*}$ is unique, equal to $\tau_c(\mathfrak{L})_{\chi^*}$ which is $p$-primary (i.e., $\tau_c(\mathfrak{L})_{\chi^*} \equiv 1 \pmod p$) and not a $p$th power in $K^\times$.*

*Proof.* The claim $\mathcal{C}\ell_{\chi^*} \neq 1$ is the consequence of the reflection theorem. Let $\gamma \in \mathcal{C}\ell_{\chi^*}$ be of order $p$. From the Chebotarev theorem in $H_K/\mathbb{Q}$, there exists a prime $\ell$ such that (in terms of Frobenius) $\left(\frac{H_K/\mathbb{Q}}{\mathfrak{L}'}\right)$ is of order $p$, for $\mathfrak{L}' \mid \ell$ in $H_K$. So $\ell$ splits completely in $K/\mathbb{Q}$ and the ideal $\mathfrak{L}$ of $K$ under $\mathfrak{L}'$ is (as well as $\mathfrak{L}_{\chi^*}$) a representative of $\gamma$. Since $b_c(\chi^*) = p\,u$ for a $p$-adic unit $u$, we can put $\mathfrak{L}_{\chi^*}^{pu} = (\alpha_{\chi^*})$; since $E_- = 1$ (except for $\chi^* = \omega$ excluded), $\alpha_{\chi^*}$ is unique and not a $p$th power; in terms of Gauss sums, $\mathfrak{L}_{\chi^*}^{pu} = (\tau_c(\mathfrak{L})_{\chi^*})$ (see (5)), thus $\alpha_{\chi^*} = \tau_c(\mathfrak{L})_{\chi^*}$. The $p$-primarity of $\alpha_{\chi^*}$ is necessary to obtain the corresponding unramified Kummer extension $K\big(\sqrt[p]{\alpha_{\chi^*}}\big)$ of degree $p$ of $K$, decomposed over $K_+$ into the unramified extension associated to $\mathcal{C}\ell_\chi$ by class field theory, whence the $p$-primarity of $\tau_c(\mathfrak{L})_{\chi^*}$ for any $\ell \equiv 1 \pmod p$ such that $\mathfrak{L} \mid \ell$ leads to a generator $\mathfrak{L}_{\chi^*}$ of $\mathcal{C}\ell_{\chi^*}$. □

4.4. **Main test for Vandiver's conjecture.** Drawing the consequences of the above (under the Hypothesis 1.2), we shall get the main test for Vandiver's conjecture.

4.4.1. *Main theorem.* A *necessary condition* to have a counterexample to Vandiver's conjecture, is that there exists an even character $\chi \neq 1$ such that $b_c(\chi^*) \sim p$ and a prime number $\ell \equiv 1 \pmod p$ such that $\tau_c(\mathfrak{L})_{\chi^*}$ is

$p$-primary, where $\mathfrak{L}$ is any prime ideal of $K$ dividing $\ell$ (the condition is sufficient as soon as $\mathfrak{L}$ is not $p$-principal). Thus the main statement for $K=\mathbb{Q}(\mu_p)$:

**Theorem 4.5.** *Let $\ell$ be any prime number totally split in $K/\mathbb{Q}$ (i.e., $\ell\equiv 1 \pmod p$). Let $\mathcal{E}_\ell(p)$ be the set of exponents of $p$-primarity of $\ell$ (i.e., the even $n\in[2,p-3]$ such that $\tau_c(\mathfrak{L})_{\omega^{p-n}}\equiv 1 \pmod p$ for any choice of $\mathfrak{L}\mid\ell$ in $K$), and let $\mathcal{E}_0(p)$ be the set of exponents of $p$-irregularity of $K$ (i.e., the even $n\in[2,p-3]$ such that $b(\omega^{p-n})\equiv 0 \pmod p$ or $B_n\equiv 0 \pmod p$). Then, if $\mathcal{E}_\ell(p)\cap\mathcal{E}_0(p)=\emptyset$, the Vandiver conjecture holds for $K$.*

*Proof.* Consider, for $\chi=\omega^n\neq 1$ even, and $\chi^*=\omega^{p-n}$, the relation (5) giving $\mathfrak{L}_{\chi^*}^{b_c(\chi^*)}=(\tau_c(\mathfrak{L})_{\chi^*})$, and examine the two possibilities:

(i) If $n$ is not an exponent of $p$-irregularity, then $\mathcal{C}\ell_{\chi^*}=1$ and $b_c(\chi^*)\not\equiv 0 \pmod p$, giving $\mathcal{T}_{\chi^*}=1$, whence $\mathcal{C}\ell_\chi=1$ (see § 3.2).

(ii) If $n$ is an exponent of $p$-irregularity, then $b_c(\chi^*)\sim p$, giving, for some $p$-adic unit $u$, $\mathfrak{L}_{\chi^*}^{pu}=(\tau_c(\mathfrak{L})_{\chi^*})$; if $\mathfrak{L}_{\chi^*}$ is $p$-principal, then $\tau_c(\mathfrak{L})_{\chi^*}$ is a global $p$th power, hence $p$-primary (absurd by assumption). So $\mathfrak{L}_{\chi^*}$ is not $p$-principal and defines the class of order $p$ in $\mathcal{C}\ell_{\chi^*}$ for which $\tau_c(\mathfrak{L})_{\chi^*}$ is not $p$-primary, whence $\mathcal{C}\ell_\chi=1$ (Kummer duality with Hypothesis 1.2). □

**Corollary 4.6.** *Let $\ell$ be a prime number totally split in $K$ and $\mathfrak{L}\mid\ell$ in $K$. If, for all even characters $\chi\neq 1$, the numbers $\tau_c(\mathfrak{L})_{\chi^*}$ are not $p$-primary (i.e., $\mathcal{E}_\ell(p)=\emptyset$), then the Vandiver conjecture is true for $p$.*

4.4.2. *Research of the minimal prime $\ell$ allowing the test.* The following program examines, for each $p$, the successive prime numbers $\ell_i\equiv 1 \pmod p$, for $i=1,\dots,N$, and return the first one, $\ell_N$ (in ell), with its index N, such that $\mathcal{E}_{\ell_N}(p)=\emptyset$. Its existence is of course a strong conjecture, but the results are extremely favorable to the existence of infinitely many such primes; which strengthens the conjecture of Vandiver.

Moreover, since the integer $i(p)=\#\mathcal{E}_0(p)$ is rather small regarding $p$ (as doubtless for $\#\mathcal{E}_\ell(p)$), the intersection of $\mathcal{E}_\ell(p)$ with $\mathcal{E}_0(p)$ may be empty for all $\ell$. Warning: we shall see that if $\mathcal{E}_\ell(p)\cap\mathcal{E}_0(p)\neq\emptyset$ (i.e., existence of a counterexample), this occurs for all $\ell$, which is terrific since the experiments give the impression that these two sets are independent, as well the sets $\mathcal{E}_\ell(p)$ when $\ell$ varies.

```
{forprime(p=3,200,c=lift(znprimroot(p));P=polcyclo(p)+Mod(0,p);X=Mod(x,P);
N=0;for(i=1,99,L=1+2*i*p;if(isprime(L)!=1,next);N=N+1;g=znprimroot(L);
J=1;for(i=1,c-1,Ji=0;for(k=1,L-2,kk=znlog(1-g^k,g);e=lift(Mod(kk+i*k,p));
Ji=Ji-X^e);J=J*Ji);d=p-2;LJ=listcreate;Jj=1;for(j=1,p-1,Jj=lift(Jj*J);
listinsert(LJ,Jj,j));T=1;for(m=1,(p-3)/2,n=2*m;pn=p-n;Sn=Mod(1,P);
for(a=1,(p-1)/2,an=lift(Mod(a,p)^(n-1));Jan=component(LJ,an);sJan=0;
for(j=0,d,aj=lift(Mod(a*j,p));sJan=sJan+x^(aj)*component(Jan,1+j));
Sn=Sn*sJan);if(Sn==1,T=0;break));if(T==1,print(p," ",L," ",N);break)))}
```

In the results, we only write the primes $p, \ell_N$, for which $N > 1$:

| p | ell | N | p | ell | N |
|---|---|---|---|---|---|
| 11 | 67 | 2 | 197 | 4729 | 2 |
| 29 | 233 | 2 | 211 | 10973 | 4 |
| 43 | 431 | 2 | 223 | 6691 | 2 |
| 53 | 743 | 2 | 227 | 5903 | 2 |
| 97 | 971 | 2 | 229 | 5039 | 2 |
| 101 | 809 | 2 | 233 | 1399 | 2 |
| 109 | 2399 | 2 | 251 | 4519 | 2 |
| 131 | 1049 | 3 | 277 | 4987 | 3 |
| 137 | 1097 | 2 | 337 | 6067 | 3 |
| 157 | 7537 | 5 | 349 | 8377 | 2 |
| 163 | 5869 | 3 | 367 | 3671 | 2 |
| 167 | 7349 | 3 | 383 | 16087 | 4 |
| 179 | 1433 | 2 | 389 | 14783 | 2 |
| 181 | 1811 | 2 | 397 | 6353 | 2 |
| 193 | 1931 | 2 | 401 | 10427 | 4 |

The comparison with the table of exponents of $p$-irregularity does not show any relation with the above study. Moreover, this test of Vandiver's conjecture does not need the knowledge of $\mathcal{E}_0(p)$ since when this set is empty, the existence of a suitable $\ell$ with $\mathcal{E}_\ell(p) = \emptyset$ does exist in all circumstance (in the selected interval).

4.5. **What happens when $\ell$ varies ?** Let $n_0$ even in $[2, p-3]$ be an exponent of $p$-irregularity under the Hypothesis 1.2, and put $\chi_0 = \omega^{n_0}$.

4.5.1. *About the $p$-principality or not of $\mathfrak{L}$.* Let $\mathfrak{L} \mid \ell$, $\ell \equiv 1 \pmod p$, be any totally split prime ideal, and let $\mathfrak{L}_{\chi_0^*}$ where $\chi_0^* = \omega^{p-n_0}$. There are two cases as we have seen in the proof of Theorem 4.5:

(i) The component $\mathfrak{L}_{\chi_0^*}$ is $p$-principal; thus since $b_c(\chi_0^*) = p\,u$, $\tau_c(\mathfrak{L})_{\chi_0^*}$ is a $p$th power in $K^\times$, whence $\tau_c(\mathfrak{L})_{\chi_0^*}$ is $p$-primary, but this does not lead to an unramified cyclic extension of degree $p$ of $K_+$ of character $\chi_0$;

(ii) The component $\mathfrak{L}_{\chi_0^*}$ is not $p$-principal; thus it defines the non-trivial component $\mathcal{C}\ell_{\chi_0^*}$ and the Vandiver conjecture holds at $\chi = \omega^{n_0}$ if and only if $\tau_c(\mathfrak{L})_{\chi_0^*}$ is not $p$-primary. In this case, if $\tau_c(\mathfrak{L})_{\chi_0^*}$ is $p$-primary, whatever the ideal $\mathfrak{L}'_{\chi_0^*}$, $\mathfrak{L}' \mid \ell'$, we have $\mathfrak{L}'_{\chi_0^*} = (z_{\chi_0^*})\mathfrak{L}^r_{\chi_0^*}$, with $z \in K^\times$ and $r \in [0, p-1]$, so that:

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

Whence a common exponent $n_0$ of $p$-primarity giving $\bigcap\limits_{\ell \equiv 1 \,(\mathrm{mod}\ p)} \mathcal{E}_\ell(p) \neq \emptyset$.

So it is fundamental to see if the sets $\mathcal{E}_\ell(p)$ are in general independent (or not) of the choice of the ideals $\mathfrak{L}$ in a given class; from the density theorems, there exist infinitely many $\ell$ for which the class of $\mathfrak{L}_{\chi^*}$ has a given order (1 or $p$). We shall do this § 4.5.2.

Now we analyse the case of $p = 37$ whose exponent of $p$-irregularity is $n_0 = 32$ giving $\#\mathcal{C}\ell_{\omega^5} = 37$ and compute in expp) the sets $\mathcal{E}_\ell(37)$ when $\ell$ varies; we shall see that the results do no seem to depend on the order of magnitude of $\ell$; if $n_0 \in \mathcal{E}_\ell(37)$, this means that $\mathfrak{L}_{\chi^*}$ is $p$-principal:

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

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

```
ell=752137   g=10   expp: 8          ell=781589   g=2   expp: 32
ell=752359   g=3    expp: 18         ell=782107   g=2
ell=752581   g=2    expp: 16         ell=782329   g=13  expp: 18
ell=752803   g=2    expp: 22,32      ell=782921   g=3   expp: 20
ell=753617   g=3                     ell=783143   g=5
ell=753691   g=11   expp: 16         ell=783661   g=2
ell=753839   g=7    expp: 4,22       ell=784327   g=3
ell=754283   g=2                     ell=784697   g=3
ell=755171   g=6                     ell=784919   g=7
ell=755393   g=3    expp: 22         ell=785363   g=2
ell=756281   g=3    expp: 2          ell=786251   g=2
ell=756799   g=15   expp: 18         ell=786547   g=2
ell=757243   g=2                     ell=787139   g=2   expp: 20
ell=757909   g=2    expp: 16         ell=787361   g=6
ell=758279   g=7                     ell=787879   g=6   expp: 10,18,20
ell=758501   g=2    expp: 18         ell=788027   g=2   expp: 34
ell=759019   g=2                     ell=789137   g=3   expp: 24
ell=759167   g=5    expp: 12         ell=790099   g=2
ell=759463   g=3                     ell=791209   g=7
ell=759833   g=3    expp: 4          ell=791431   g=12
ell=760129   g=11                    ell=791801   g=3
ell=760499   g=2                     ell=792023   g=5   expp: 32
ell=762053   g=2                     ell=792689   g=3
ell=762571   g=10                    ell=793207   g=5
ell=763237   g=2                     ell=795427   g=2
ell=764051   g=2                     ell=795649   g=22  expp: 2,32
ell=764273   g=3                     ell=795797   g=2
ell=764717   g=2    expp: 2          ell=795871   g=3
ell=765383   g=5                     ell=796759   g=3
ell=765827   g=2    expp: 34         ell=796981   g=7
ell=766049   g=3    expp: 22         ell=797647   g=3
ell=766937   g=3    expp: 34         ell=797869   g=10
ell=767381   g=2    expp: 18         ell=798461   g=2
ell=767603   g=5    expp: 34         ell=798757   g=2
ell=767677   g=5                     ell=800089   g=7   expp: 20
```

For $\ell = 149, 223, 593, 1259, 1777, \ldots$, $\mathcal{E}_\ell(37) = \emptyset$, which proves the Vandiver conjecture for $p = 37$. Consider a case where $\mathcal{E}_\ell(p) \neq \emptyset$:

For $\ell = 1481$ one finds a $p$-primarity for $\chi^* = \omega^7$ ($\chi = \omega^{30} \neq \omega^{32}$); we may think that for small primes $p$, some coincidences may be possible (i.e., $\mathcal{E}_\ell(p) \cap \mathcal{E}_0(p) \neq \emptyset$), despite the fact that this must arrive for all $\ell$ as we have just seen.

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 (in other words, the class of order 37 does not come from a strict subfield); then $\chi = \omega^{30}$ is a character of the real subfield $k_6$ of degree 6 of $\mathbb{Q}$ which gives rise to a $\ell$-ramified (i.e., unramified outside $\ell$ since the 37-primarity gives the non-ramification of $p$) cyclic extension of degree $p$ of $k_6$ (in other words, if the exponent of $p$-irregularity had been

30 instead of 32, this would have given an unramified cyclic extension of degree $p$ of $k_6$, i.e., $\#\mathcal{C}\ell_{k_6} = 37$). It remains the question of the principality (or not) of the $\mathfrak{L}_{\chi_0^*}$, where $\chi_0^* = \omega^5$.

In the particular case $p = 37$, $\mathfrak{L}_{\chi_0^*}$ is principal if and only if $\mathfrak{L}$ is principal since the exponent of $p$-irregularity $n_0 = 32$ is unique with a class number $h = 37$.

(i) Principal case. The principal $\mathfrak{L}$ are rare; the first one is $\mathfrak{L} = (x^{11}+x^3+x)$ where $\ell = 32783$ and $x = \zeta_{37}$.

Thus in that case, in the relation $\mathfrak{L}^{b_c(\chi_0^*)} = (\tau_c(\mathfrak{L})_{\chi_0^*})$, $\tau_c(\mathfrak{L})_{\chi_0^*}$ must be a 37th power (which explain that one finds the exponent of 37-primarity equal to that of 37-irregularity in the forthcomming table); but infortunately, the data are too large to be given. Nevertheless, the reader can easily compute $\mathsf{factor}(\mathsf{norm}(\mathsf{Sn})) = 32783^{37\cdot 16\cdot 9}$ and use the instructions $\mathsf{K} = \mathsf{bnfinit}(\mathsf{P}, 1)$; $\mathsf{idealfactor}(\mathsf{K}, \mathsf{Sn})$, which give the 37th power of a principal ideal $\mathfrak{L} \mid 32783$.

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

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

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

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

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

4.5.2. *Table of the classes of* $\mathfrak{L}$ *for* $p = 37$. We give a table with a generator of $\mathfrak{L}$ in the principal cases (indicated by $*$). Otherwise, the class of $\mathfrak{L}$ is of order 37 in $K$. The exponents of $p$-primarity are denoted $\mathsf{expp}$:

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

```
ell=1481    expp: 30          ell=56167   expp: 10,14,26
ell=2591    expp: 34          ell=57203   expp: 34
ell=3331    expp: 22          ell=58313   expp: 28
ell=4219    expp: 16,18       ell=58757   expp: 16,18
```

```
 ell=6143    expp: 28               ell=58831   expp: 24,30
 ell=7993    expp: 16,20            ell=59497   expp: 28
 ell=8363    expp: 8                ell=61051   expp: 10
 ell=9769    expp: 20               ell=62383   expp: 2
 ell=10657   expp: 4,18,26          ell=62753   expp: 2
 ell=12433   expp: 20               ell=63493   expp: 2
 ell=13099   expp: 28              *ell=64381   expp: 6,32 [x^20+x^9+x]
 ell=14431   expp: 4,14,22          ell=66749   expp: 30
 ell=17021   expp: 6               *ell=67489  expp: 30,32 [x^24-x^3-x^2]
 ell=17909   expp: 30               ell=67933   expp: 6
 ell=18131   expp: 22              *ell=68821  expp: 32    [x^15-x^9+x^4]
 ell=19463   expp: 6                ell=69931   expp: 12
 ell=20129   expp: 6                ell=71411   expp: 4
 ell=21017   expp: 2,4              ell=72817   expp: 28
 ell=21313   expp: 18               ell=74149   expp: 2
 ell=21757   expp: 8                ell=75407   expp: 10
 ell=22349   expp: 8                ell=75629   expp: 12, 20
 ell=23459   expp: 6                ell=76961   expp: 14
 ell=23977   expp: 26               ell=78737   expp: 28
 ell=25087   expp: 26               ell=79181   expp: 10
 ell=25457   expp: 30               ell=80513   expp: 16, 26
 ell=29009   expp: 8,24             ell=81031   expp: 18, 34
 ell=30859   expp: 2                ell=82067   expp: 34
*ell=32783   expp: 32 [x^11+x^3+x]  ell=83621   expp: 34
 ell=33301   expp: 30               ell=83843   expp: 2
 ell=33967   expp: 26               ell=84731   expp: 6
 ell=36187   expp: 8                ell=85027   expp: 26
 ell=37889   expp: 16               ell=86729   expp: 22
 ell=38629   expp: 22               ell=86951   expp: 8
 ell=40627   expp: 30               ell=87691   expp: 24
 ell=40849   expp: 6                ell=91243   expp: 22, 34
 ell=42773   expp: 4                ell=91909   expp: 30
 ell=45289   expp: 8                ell=94351   expp: 10
 ell=45659   expp: 26               ell=94573   expp: 18
 ell=48619   expp: 8                ell=95239   expp: 18, 28
 ell=48989   expp: 20               ell=96497   expp: 10
 ell=51283   expp: 14,16            ell=98347   expp: 28
 ell=51431   expp: 20               ell=98939   expp: 30
 ell=53281   expp: 16               ell=99679   expp: 10, 22
 ell=55057   expp: 20               ell=100049  expp: 14
```

This table shows the clear independence of the exponents of $p$-primarity regarding the choice of *non-principal* $\mathfrak{L}$.

4.5.3. *Densities of the exponents of p-primarity.* The following program may be used to see that all exponents of $p$-primarity are obtained, with some specific densities, taking sufficientely many primes $\ell \equiv 1 \pmod{p}$ and a $\mathfrak{L} \mid \ell$ (each even $n \in [2, p-3]$, such that $\tau_c(\mathfrak{L})_{\omega^{p-n}}$ is $p$-primary for some new $\ell$, is counted in the $(n/2)$th component of the list $\mathsf{L}$).

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

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

(i) Program:

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

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

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

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

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

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

```
        5,5,5,3,6,1,5,3,5,4,5,0,2,3,5,7,3,3,3,2,4,4,7,6,6,5,6,1,7,4,7]
586 307 1150183   [9,3,2,6,8,3,1,4,5,9,3,1,3,1,6,3,4,4,
        2,2,1,2,5,5,3,2,2,1,5,7,6,2,2,1,5,5,5,4,4,3,3,4,5,4,5,5,
        5,5,5,3,6,1,5,3,5,4,5,0,2,3,5,7,3,3,3,2,4,4,7,6,6,5,6,1,7,4,7]
586 308 1150183   [9,3,2,6,8,3,1,4,5,9,3,1,3,1,6,3,4,4,
        2,2,1,2,5,5,3,2,2,1,5,7,6,2,2,1,5,5,5,4,4,3,3,4,5,4,5,5,
        5,5,5,3,6,1,6,3,5,4,5,0,2,3,5,7,3,3,3,2,4,4,7,6,6,5,6,1,7,4,7]
590 309 1161487   [9,3,2,6,8,3,1,4,5,10,3,1,3,1,6,3,4,4,
        2,2,1,2,5,5,3,2,2,1,5,7,6,2,2,1,5,5,5,4,4,3,3,4,5,4,5,5,
        5,5,5,3,6,1,6,3,5,4,5,0,2,3,5,7,3,3,3,2,4,4,7,6,6,5,6,1,7,4,7]
590 310 1161487   [9,3,2,6,8,3,1,4,5,10,3,1,3,1,6,3,4,4,
        2,2,1,2,5,5,3,2,2,1,5,7,6,2,2,1,5,5,5,4,4,3,3,4,5,4,5,6,
        5,5,5,3,6,1,6,3,5,4,5,0,2,3,5,7,3,3,3,2,4,4,7,6,6,5,6,1,7,4,7]
590 311 1161487   [9,3,2,6,8,3,1,4,5,10,3,1,3,1,6,3,4,4,
        2,2,1,2,5,5,3,2,2,1,5,7,6,2,2,1,5,5,5,4,4,3,3,4,5,4,5,6,
        5,5,5,3,6,1,6,3,5,4,5,0,2,3,5,7,3,3,3,2,4,5,7,6,6,5,6,1,7,4,7]
```

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

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

One sees that these numbers seem to depend on the order $\dfrac{p-1}{\gcd(p-1,n)}$ of $\omega^n$, but this needs to be clarified taking a great lot of primes $\ell$. The complete tables for $p = 37$ and $p = 157$ (40 pages) may be downloaded from:
https://www.dropbox.com/s/vs5eq6ornqx5922/vandiver.97.157.pdf?dl=0

4.5.4. *Link with the non-p-rationality.* We return to the case $p = 37$ and $n_0 = 32$. From the reflection relation (1), we see that $\omega^{32}$ is a character of order 9, hence a character of the real subfield $k_9$ of degree 9 which is such that $\mathcal{T}_{k_9} \simeq \mathbb{Z}/37\mathbb{Z}$; so, $k_9$ admits a cyclic 37-ramified extension of degree 37 which is not unramified. To verify, we use the program [7, Program I] simplified for real fields, which gives $\#\mathcal{T}_{k_9} = 37$ (take nt large enough):

```
{P=polsubcyclo(37,9);K=bnfinit(P,1);p=37;nt=6;Kpn=bnrinit(K,p^nt);
Hpn=component(component(Kpn,5),2);L=listcreate;e=component(matsize(Hpn),2);
R=0;for(k=1,e,c=component(Hpn,e-k+1);if(Mod(c,p)==0,R=R+1;
listinsert(L,p^valuation(c,p),1)));print("Structure of T: ",L);
if(R>1,print("rk(T)=",R-1,"  K is not ",p,"-rational"));
if(R==1,print("rk(T)=",R-1,"  K is ",p,"-rational"))}
```

```
37-rank of the compositum of the Z_37-extensions: 1
Structure of the 37-ray class group: List([69343957, 37])
rk(T)=1 K is not 37-rational
```

We find here another interpretation of the reflection theorem since we have the typical formula (for totally real number fields) $\#\mathcal{T}_+ = \#\mathcal{C}\ell_+ \cdot \#\mathcal{R}$, where the $p$-group $\mathcal{R}$ is the normalized $p$-adic regulator of $K_+$ [10, Proposition 5.2]; thus the above data shows that the relation $\#\mathcal{T}_+ = 37$ comes from $\#\mathcal{R} = 37$.

*Remark* 4.7. We have the analytic formula $\#\mathcal{C}\ell_{\chi_0^*} = \#(E_{\chi_0^*}/\langle\eta_{\chi_0^*}\rangle)$, where $\eta$ is a suitable cyclotomic unit; so a classical method (explained in [18, Corollary 8.19] and applied in [2, 3]) consists in finding a prime $\ell \equiv 1 \pmod p$ such that $\eta_{\chi_0^*}$ is not a local $p$th power at $\ell$ proving Vandiver's conjecture at $\chi_0^*$; so when we find that $\mathcal{R} \neq 1$, this means that $\eta_{\chi_0^*}$ generates $E_{\chi_0^*}$ and is a local $p$th power at $p$.

## 5. Heuristics

5.1. **Standard probabilities.** We may conjecture that, for $p$ fixed, the sets $\mathcal{E}_\ell(p)$ of exponents of $p$-primarity of primes $\ell \equiv 1 \pmod p$, are random with the same behavior as for the set $\mathcal{E}_0(p)$ of exponents of $p$-irregularity of $K$ (see in [18], after Theorem 5.17, the comments and the statistical computations). This should imply that, for $p$ fixed, $\mathcal{E}_\ell(p) \neq \emptyset$ for infinitely many $\ell$.

More precisely, if we assume, as in Washington's book [18], that in terms of probabilities one has for $p$ and $\ell$ fixed (where $N := \frac{p-3}{2}$ is the number of even characters $\chi \neq 1$):

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

the probability of a non-empty intersection $\mathcal{E}_0(p) \cap \mathcal{E}_\ell(p)$, for $j \in [0, N]$ and $k \in [0, N]$ fixed, is $1 - \frac{(N-k)! \cdot (N-j)!}{N! \cdot (N-k-j)!}$. So, a first approximation of the whole probability for $\mathcal{E}_0(p) \cap \mathcal{E}_\ell(p) \neq \emptyset$ is:

$$\sum_{j,k \geq 0} \tbinom{N}{j}\tbinom{N}{k} \cdot \big(1 - \tfrac{1}{p}\big)^{2N-j-k} \cdot \big(\tfrac{1}{p}\big)^{j+k} \cdot \big(1 - \tfrac{(N-k)!\cdot(N-j)!}{N!\cdot(N-k-j)!}\big). \tag{7}$$

Some computations show that this expression is around $\frac{1}{2p}$, which does not allow to conclude easily. The following program shows a rapid convergence obtained still for $t = 18$ (i.e., $j$ and $k$ independent in $[0, t]$):

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

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

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

(i) For some even characters $\chi = \omega^n =: \omega^{p-1-h}$, $\chi^* = \omega^{h+1}$, $h = 2, 4, \ldots$, when $p \gg_h 0$, one may prove that $\mathcal{C}\ell_\chi = 1$ (see [5, 15, 17] among other authors applying the same approach via K-theory); the order of $\omega^n$ is $\dfrac{p-1}{\gcd(p-1,n)}$ which only concerns subfields of $K_+$ of great degree since $\gcd(p-1,n) = \gcd(p-1,h)$ giving the order of $\omega^n$ equal to:

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

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

In another direction, for the even $\chi$ of small orders, $\mathcal{C}\ell_\chi$ may be trivial because of the "archimedean" order of magnitude of $\#\mathcal{C}\ell_+$ (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 $\epsilon$-conjecture of [4], for $p$-class groups, that we state for the real abelian fields $k_d$ *of fixed degree* $d$, of discriminant $D = p^{d-1}$, when $p$ 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 $\epsilon < 1$.

(ii) The previous probabilities (7) assume that when $\ell$ varies, the sets $\mathcal{E}_\ell(p)$ are *random and independent*, which is not the case when $p$ is irregular at some $\chi_0^* = \omega^{p-n_0}$ (for even $\chi_0 = \omega^{n_0}$) as we shall see; to simplify we assume the Hypothesis 1.2 giving $b_c(\chi_0^*) = p\,u$, where $u$ is a $p$-adic unit.

Indeed, if $\mathfrak{L}_{\chi_0^*}$ generates $\mathcal{C}\ell_{\chi_0^*} \simeq \mathbb{Z}/p\mathbb{Z}$, for any $\mathfrak{L}'_{\chi_0^*}$ one has:

$$\mathfrak{L}'_{\chi_0^*} = (z_{\chi_0^*}) \cdot \mathfrak{L}^r_{\chi_0^*},\ \ r \in \mathbb{Z}/p\mathbb{Z},\ z \in K^\times,$$

then $\mathfrak{L}'^{pu}_{\chi_0^*} = \mathfrak{L}^{rpu}_{\chi_0^*} \cdot (z^{pu}_{\chi_0^*})$, giving, since $E_{\chi_0^*} = 1$:

$$\tau_c(\mathfrak{L}')_{\chi_0^*} = z^{pu}_{\chi_0^*} \cdot \tau_c(\mathfrak{L})^r_{\chi_0^*} \equiv \tau_c(\mathfrak{L})^r_{\chi_0^*} \pmod p.$$

Fix $\ell$ and $\mathfrak{L} \mid \ell$, then put:

$$\tau_c(\mathfrak{L})_{\chi_0^*} = 1 + \beta_0 \cdot \varpi^{p-n_0};$$

then $\beta_0$ only depends on $\chi_0^*$. From Proposition 2.4, $\beta_0$ is invertible modulo $\varpi$ if and only if $\tau_c(\mathfrak{L})_{\chi_0^*}$ is non-$p$-primary, or is not invertible if and only if $\tau_c(\mathfrak{L})_{\chi_0^*}$ is $p$-primary. This relation gives, whatever $\mathfrak{L}'_{\chi_0^*}$, *but under the non-p-principality of* $\mathfrak{L}_{\chi_0^*}$:

$$\tau_c(\mathfrak{L}')_{\chi_0^*} = 1 + r \cdot \beta'_0 \cdot \varpi^{p-n_0},\ \ \beta'_0 \equiv \beta_0 \pmod \varpi,\ r \in \mathbb{Z}/p\mathbb{Z}. \tag{8}$$

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

*For each even character $\chi \neq 1$, the congruential values, at $\chi^* = \omega\,\chi^{-1}$, of the Gauss sums (more precisely of the $\tau_c(\mathfrak{L})_{\chi^*} = (\tau(\psi)^{c-\sigma_c})_{\chi^*}$), are independent of the $p$-class of $\mathfrak{L} \mid \ell$ and are uniformly distributed, when $\ell \equiv 1 \pmod p$ varies.*

Because of the uniform distribution of the ideals $\mathfrak{L}$ in the $p$-classes (density theorems), we must examine two cases for any even $\chi$ when there exists $\chi_0 = \omega^{n_0}$ 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 the $\tau_c(\mathfrak{L}')_{\chi^*}$, when $\mathfrak{L}'$ varies, are of the form $\tau_c(\mathfrak{L}')_{\chi^*} \equiv 1 + \beta' \cdot \varpi^{p-n} \pmod p$, with uniformly random $\beta' \pmod \varpi$ in $\mathbb{Z}/p\mathbb{Z}$ (usual heuristics and probabilities $\frac{1}{p}$).

(b) $\chi = \chi_0$ and $\mathcal{C}\ell_{\chi_0^*} \simeq \mathbb{Z}/p\mathbb{Z}$. If $\tau_c(\mathfrak{L})_{\chi_0^*}$ is $p$-primary for some fixed non-principal $\mathfrak{L}_{\chi_0^*}$, then from (8) all the $\tau_c(\mathfrak{L}')_{\chi_0^*}$ are $p$-primary, whatever the class of $\mathfrak{L}'_{\chi_0^*}$ ($p$ possibilities) because $\beta_0 \equiv 0 \pmod \varpi$. So, $n_0$ is always an exponent of $p$-primarity; in other words $\mathcal{E}_0(p) \cap \mathcal{E}_\ell(p) \neq \emptyset$ for all prime $\ell \equiv 1 \pmod p$.

Thus, to have the same density $\frac{1}{p}$ of $p$-primary $\tau_c(\mathfrak{L}')_{\chi_0^*}$ (as in the $p$-principal case (a)), $\beta_0 \equiv 0 \pmod \varpi$ must occur $p$ times less, giving the probability $\frac{1}{p^2}$ instead of $\frac{1}{p}$; it is even possible that such a circumstance is of probability 0 depending on more precise properties of Gauss sums. Otherwise, the behaviour of the Gauss sums should be excessively disturbed and in an algorithmic framework, we suggest that the congruential properties of the Gauss sums "determine" the properties of the $p$-class group of $K$ instead of the contrary.

Precisely, under the assumption $\tau_c(\mathfrak{L})_{\chi_0^*}$ $p$-primary, the corresponding component $n_0$ of the list counting the $p$-primarities, increases at each step. For instance, if for $p = 37$ the exponent 32 of 37-irregularity was an exponent of $p$-primarity, then the last line of the data § 4.5.3 would be the awful result about the 16th component:

```
L=[83,96,86,91,80,80,86,83,92,83,98,76,83,78,86, {75+1432}, 76]
```

The quotient $\dfrac{1432}{75}$ looks like $\frac{p}{2}$; this is in accordance with the previous heuristics and would give a 16th component:

$$x_0(\ell) \approx x(\ell) \cdot \big(1 + \tfrac{p}{2}\big), \ \text{ as } \ell \to \infty,$$

where $x(\ell)$ is the mean of the other components (very approximatively equal to $\dfrac{2\,N}{p}$ where $N$ is the number of exponents of $p$-primarity obtained

in the selected interval). Let $N_\ell$ be the number of prime numbers $\ell$ tested; then $\frac{N_\ell}{N}$ seems to be $O(1)$ giving:

$$x(\ell) \approx \frac{2}{p} \cdot N_\ell \cdot (1 + O(1))$$

and the pathological component:

$$x_0(\ell) \approx N_\ell \cdot (1 + O(1)).$$

## 6. Conclusion

Under these experiments and heuristics, the existence of disjoint sets $\mathcal{E}_\ell(p)$ and $\mathcal{E}_0(p)$, or perhaps the existence of $\ell$ such that $\mathcal{E}_\ell(p) = \emptyset$ (see the numerical results § 4.4.2), may occur conjecturally for all $p \gg 0$ and possibly for all $p$.

Note that the "algoritm" associated to the test of Vandiver's conjecture is the passage from $\ell$ to the next $\ell'$ in the sequence of totally split primes, the crucial step being the computation of the Jacobi sums:

$$J_i = -\sum_x \zeta_p^{\lg(x)+\lg(1-x)} \quad \& \quad J'_i = -\sum_{x'} \zeta_p^{\lg'(x')+\lg'(1-x')},$$

where lg and lg′ are the discrete logarithms for $\ell$ and $\ell'$, respectively. Since they have, a priori, no "algebraic link", this suggests randomness and applies for infinitely many primes.

Of course, there are two constraints: the fact that each Jacobi sum is of module $\ell$ and that the $p$-classes of the associated ideals $\mathcal{L}$ (finite in number) are all represented with standard densities; but the *congruential properties* of Gauss sums do not follow any law (in our opinion), what explains that the negation of the above properties, for at least one prime $p$, implies a very tricky complexity of the algoritms, as the fact that, for all $\ell \equiv 1 \pmod p$, $\mathcal{E}_\ell(p) \cap \mathcal{E}_0(p) \neq \emptyset$ (or the weaker property $\mathcal{E}_\ell(p) \neq \emptyset$ for all $\ell \equiv 1 \pmod p$).

Which gives again an example of $p$-adic problem analogous to those we have analysed for various conjectures: Greenberg's conjectures, $p$-rationalities of a number field, existence of a $p$-adic Brauer–Siegel theorem governing many number theory problems (see [11] and its bibliography).

In other words, the truth of Vandiver's conjecture for "small" primes $p$ may be a non-theoretical coincidence and may come, for $p \gg 0$, from Borel–Cantelli heuristics on properties of probabilities much less than $\frac{O(1)}{p^2}$. Possibly, there is an universal obstruction for the above phenomena on the sets $\mathcal{E}_\ell(p)$ comming from Gauss sums theory.

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 [2, 3]. In a more serious statement, we may conjecture that Vandiver's conjecture holds for almost all primes, the precise finite

cardinality of the set of counterexamples ($\emptyset$ or not) being (in our opinion) not of algebraic nature nor enlightened by Iwasawa's theory, is perhaps accessible by the way of analytical techniques or depends on an 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] J.P. Buhler and D. Harvey, *Irregular primes to* 163 *million* Math. Comp. **80** (2011), no. 276, 2435–2444. http://www.ams.org/journals/mcom/2011-80-276/S0025-5718-2011-02461-0/

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

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

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

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

[7] 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

[8] G. Gras, *Annihilation of* $\mathbf{tor}_{\mathbb{Z}_p}(\mathcal{G}_{K,S}^{\mathrm{ab}})$ *for real abelian extensions* $K/\mathbb{Q}$ (preprint 2018). https://arxiv.org/pdf/1806.03137.pdf

[9] G. Gras, *Sur la p-ramification abélienne*, Conférence donnée à l'University Laval, Québec, Mathematical series of the department of mathematics **20** (A) (1984), 1–26. https://www.dropbox.com/s/hecx46bex3ptzdw/Conf%C3%A9rences1982.Canada.Univ.Laval.pdf?dl=0

[10] 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

[11] G. Gras, *Heuristics and conjectures in direction of a p-adic Brauer–Siegel theorem*, Math. Comp. (to appear).https://doi.org/10.1090/mcom/3395 https://arxiv.org/pdf/1801.04214.pdf

[12] 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

[13] H. Ichimura, *Local Units Modulo Gauss Sums*, Journal of Number Theory **68** (1998), 36–56.https://doi.org/10.1006/jnth.1997.2206

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

[15] 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

[16] The PARI Group, *PARI/GP, version 2.9.0*, Université de Bordeaux (2016). http://pari.math.u-bordeaux.fr/

[17] C. Soulé, *Perfect forms and the Vandiver conjecture*, Journal de Crelle **517** (1999), 209–221. https://doi.org/10.1515/crll.1999.095

[18] L.C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math. 83, Springer enlarged second edition 1997.

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